Academic program description form

University name: *Northern Technical University*
College/Institute: **Technical Engineering College for computer and AI** */ Mosul*

Scientific Department: *Department of* **Cyber Security and Cloud Computing Techniques Engineering**

Name of the academic or professional program: *Bachelor of Engineering techniques, cybersecurity and cloud computing*

Name of final degree: *Bachelor of engineering techniques Cybersecurity*

School system: *Bologna*
Description preparation date: *1/12/2024*

Date of filling the file: *28/12/2024*

The signature:
Name of head of department:

Dr. Nawar A. Sultan

The date: 28/12/2024

The signature:
Name of the scientific assistant:

Dr. Zakaria N. Mahmood

The date: 28/12/2024

The file was audited by the Quality Assurance and University Performance Division

Name of the Director of the Quality Assurance and University Performance Division: *Nour Qahtan Younis*

The date: 28/12/2024

The signature:

Authentication of the Dean Dr.

28/12/2024

Ministry of Higher Education and Scientific Research Scientific supervision and evaluation device
Department of Quality Assurance and Academic Accreditation
Accreditation Department

Academic Program and course description guide

2024

introduction:

The educational program is considered a coordinated and organized package of academic courses that includes procedures and experiences organized in the form of academic vocabulary, the main purpose of which is to build and refine the skills of graduates, making them qualified to meet the requirements of the labor market. It is reviewed and evaluated annually through internal or external audit procedures and programs such as the external examiner program.

The description of the academic program provides a brief summary of the main features of the program and its courses, indicating the skills that students are working to acquire based on the objectives of the academic program. The importance of this description is evident because it represents the cornerstone of obtaining program accreditation, and the teaching staff participates in writing it under the supervision of the scientific committees in the scientific departments. This guide, in its second edition, includes a description of the academic program after updating the vocabulary and paragraphs of the previous guide in light of the latest developments in the educational system in Iraq, which included a description of the academic program in its traditional form (annual, quarterly), in addition to adopting the description of the academic program circulated according to the book of the Department of Studies 3/2906. On 5/3/2023 with regard to programs that adopt the Bologna Process as a basis for their work.

In this area, we can only emphasize the importance of writing descriptions of academic programs and courses to ensure the smooth conduct of the educational process.

Concepts and terminology:

Academic Program Description: *The academic program description provides a brief summary of its vision, mission, and goals, including an accurate description of the targeted learning outcomes according to the identified learning strategies.* ***Course Description:*** *Provides a necessary summary of the most important course characteristics and learning outcomes that the student is expected to achieve, indicating whether they have made the most of the learning opportunities available. It is derived from the program description.*

Program Vision: *An ambitious picture for the future of the academic program to be a developed, inspiring, motivating, realistic and applicable program.* ***Program mission:*** *It briefly explains the objectives and activities necessary to achieve them, and also specifies the developmental paths and directions of the program.*

Program objectives: *These are statements that describe what the academic program intends to achieve within a specific period of time and are measurable and observable.*

Curriculum structure: *All courses/study subjects included in the academic program according to the approved learning system (semester, annual, Bologna track), whether it is a requirement (ministry, university, college, or scientific department), in addition to the number of courses and study units.*

Learning Outcomes: *A fixed set of knowledge, skills, and values that a student has acquired after successfully completing an academic program. The learning outcomes for each course must be defined in a way that achieves the program objectives.*

Teaching and learning strategies: *These are the strategies that a faculty member uses to develop the student's teaching and learning process, and they are the plans that are followed to reach learning goals. That is, it describes all curricular and extracurricular activities to achieve the learning outcomes of the program.*

Academic program description form

University name: *Northern Technical University*
College/Institute: **Technical Engineering College for computer and AI** */ Mosul*

Scientific Department: *Department of* **Cyber Security and Cloud Computing Techniques Engineering**

Name of the academic or professional program: *Bachelor of Engineering techniques, cybersecurity and cloud computing*

Name of final degree: *Bachelor of engineering techniques Cybersecurity*

School system: *Bologna*
Description preparation date: *1/10/2024*

Date of filling the file: *7/10/2024*

The signature:
Name of head of department:

Dr. Nawar A. Sultan

The date:

The signature:
Name of the scientific assistant:

Dr. Zakaria N. Mahmoud

The date:

The file was audited by the Quality Assurance and University Performance Division

Name of the Director of the Quality Assurance and University Performance Division: ***Nour Qahtan Younis***

The date:

The signature:

Authentication of the Dean Dr.

1. program vision

The vision of the Department of Cybersecurity and Cloud Computing Technology Engineering is a world where digital security is a top priority and cloud computing is used to its full potential. The department's vision recognizes the importance of both areas and their unique responsibilities. While cybersecurity seriously protects against unauthorized access, cyber threats, and network and data compromise, cloud computing represents a transformative force, using the Internet to easily access scalable computing resources.

In this department, students are taught the importance of cybersecurity and cloud computing and how to apply cybersecurity and cloud computing techniques to solve cybersecurity and cloud computing problems. And also how to analyze cybersecurity and cloud computing and how to apply cybersecurity techniques and cloud computing to solve cybersecurity and cloud computing problems. Students can also learn how to develop and apply cybersecurity and cloud computing techniques to help solve cybersecurity and cloud computing problems. Graduates of the department will be responsible for planning, implementing, updating and monitoring security measures to protect computer and information networks, assessing vulnerabilities in computer and electronic systems with regard to security risks, and proposing and implementing risk mitigation. They may ensure that appropriate security controls are in place that will protect digital files and vital information and respond to computer breaches and viruses. Cloud computing is a transformative force, using the Internet to easily access scalable computing resources.

2. Program message

The mission of the Department of Cybersecurity and Cloud Computing Technologies Engineering is one of the important messages in the field of cybersecurity and cloud computing. This department aims to train students on the use of modern technologies to protect systems and data from cyber attacks and security threats. The department includes the study of topics such as security analysis, encryption, virus protection, identity verification, access control, network control, and cloud computing. These topics are taught using the latest technologies and software tools, giving students the skills to work in cybersecurity and cloud computing. Thus, the mission of the Department of Cybersecurity and Cloud Computing Engineering Technologies is to train students to protect systems and data from cyberattacks and security threats using modern technologies and software tools.

3. Program Objectives

1. Graduating engineering cadres capable of designing and implementing secure systems that protect against cyber threats and vulnerabilities. Develop and implement secure network solutions, design, engineer and convert reliable systems into secure systems, manage audit/intrusion and security technology systems, conduct assessments and penetration testing, understand successful cyberattacks and their impacts on the operational mission of various digital systems, and build the Iraqi state's long-term resilience and work through cyber incidents.
2. Preparing engineering cadres with a high level of understanding, knowledge and academic and technical preparation that combine engineering perceptions, technical creativity, scientific skill and quality of implementation in the field of cybersecurity and cloud computing engineering technologies.
3. Graduating engineering cadres who are responsible for building, designing and protecting information technology systems in institutions to prevent data breaches, keep them safe from hackers, viruses and other potential problems, supervise and build network infrastructure of various types and available systems.
4. Graduating engineering cadres with the scientific and technical skill that enables him to master dealing with cloud computing operations and using vulnerability examination tools to detect various technical problems, follow up on the failure and evaluation of security patches, mitigate security vulnerabilities, and provide assistance in security documentation and disaster recovery solutions.
5. Preparing engineering cadres with the technical and scientific skill that

enables him to analyze data records and conduct risk assessments in the event of security breaches to know the parts of the system that have been penetrated and where the danger lies. Data breaches and secure systems to explore potential vulnerabilities in order to ensure the integrity of network systems.
6. Providing experts in the field of cybersecurity to help achieve the long-term plan of the Iraqi state with the presence of experts in the field of cybersecurity.
7. Empower students with soft skills and values to communicate and collaborate effectively with others professionally, ethically and legally.
8. Ensure that students' knowledge and skills are in line with the latest cybersecurity technologies
9. Achieving greater interaction between the Technical College of Engineering for Computer and Artificial Intelligence and the community in all its institutions for the purpose of experiencing the circumstances and reality and finding appropriate solutions to the problems that are identified.

4. Programmatic accreditation

nothing

5. Other external influences

nothing

6. *Program structure*

Program structure	Number of courses	Study unit	percentage	comments
Enterprise requirements	9	18	17 %	Basic course
College requirements	12	34	24 %	Secondary course
Department requirements	30	83	59 %	Major course
Summer training	exists		---	
Other				

*Notes may include whether the course is core or elective.

7. Program description

Year/level	Course code	Name of the course	Credit hours	
Level 1 – First Semester	**BCYSCE100-S1**	**Mathematic**	٢	٢
	BCYSCE105-S1	**Linux Administration**	**2**	**2**
	BCYSCE102-S1	**Fundamentals of Programming**	**2**	**2**
	BCYSCE104-S1	**Fundamentals of Electrical Engineering**	**2**	**2**
	NTU 101	**English language**	**2**	–
	BCYSCE103-S1	**Introduction to Sociology**	**2**	–

	NTU100	**Human rights and Democracy**	**2**	–
Level 1 – Second Semester	**BCYSCE101-S2**	**Digital Electronics**	3	2
	BCYSCE106-S2	**Introduction to Probability and Statistics**	2	2
	BCYSCE107-S2	**Object oriented programming**	2	2
	NTU102	**Computer**	2	1
	BCYSCE108-S2	**Introduction to Cyber security Engineering**	2	2
	NTU103	**Arabic Language**	-	2
Level 2 – First Semester	**BCYSCE200-S1**	**Computer Electronics**	2	2
	BCYSCE205-S1	**Discrete Math**	3	-
	BCYSCE202-S1	**Database systems**	2	2
	BCYSCE204-S1	**Python Programming for Cybersecurity**	2	2
	BCYSCE203-S1	**Operating Systems**	1	2
	NTU203	**Bath Party Crimes**	2	-
	NTU200	**English language**	2	-
	BCYSCE200-S1	**Computer Networks**	2	2
Level 2 – Second	**BCYSCE205-S2**	**Data structures**	2	2

Semester	**BCYSCE202-S2**	**Database security**	2	2
	BCYSCE204-S2	**Computer Organization and Architectures**	2	2
	BCYSCE203-S2	**Networks Security**	2	2
	NTU202	**Arabic Language**	2	-
	NTU 204	**Cybersecurity Professional ethics**	2	-
	BCYSCE201-S1	**Network Administration and Infrastructure**	1	2
	NTU201	**Computer**	1	2
Level 3 – First Semester	**BCYSCE203-S1**	**Introduction to Cryptography**	2	2
	BCYSCE305-S1	**Introduction to Hardware security**	2	2
	BCYSCE302-S1	**Digital Signal Processing**	2	2
	BCYSCE304-S1	**Mobile and wireless networks**	2	2
	BCYSCE303-S1	**Fundamentals of Cloud computing**	2	2
Level 3 – Second Semester	**BCYSCE300-S2**	**Mobile and wireless networks security**	2	2
	BCYSCE305-S2	**Secure software development**	2	2
	BCYSCE302-S2	**Operating system security**	2	2

	BCYSCE304-S2	**Practicing cybersecurity: Attacks and Countermeasures**	2	2
	BCYSCE303-S2	**Engineering Analysis**	2	2
	BCYSCE301-S2	**Cloud Computing security**	2	2
Level 4 – First Semester	**BCYSCE400-S1**	**Intrusions Detection and prevention System**	2	2
	BCYSCE405-S1	**Research Methodology**	2	2
	BCYSCE402-S1	**AI for Cybersecurity Engineering**	2	2
	BCYSCE404-S1	**Practicing cybersecurity: Ethical Hacking and Vulnerability Analysis**	2	2
	BCYSCE403-S1	**Cloud Application**	2	2
	BCYSCE401-S1	**Graduation Project Design**	0	2
Level ٤ – Second Semester	**BCYSCE400-S2**	**IT Project Management**	2	-
	BCYSCE405-S2	**Graduation Project Implementation**	-	2
	BCYSCE402-S2	**Digital Forensics**	2	2
	BCYSCE404-S2	**IoTs and Cybersecurity**	2	2
	BCYSCE403-S2	**Reverse Engineering-Malwares Analysis**	2	2

8. Expected learning outcome of the program

knowledge

A. Cognitive Objectives

1. Evaluate computer systems, networks and software applications for vulnerabilities.
2. Design and implement cybersecurity measures to protect systems and data from cyberattacks.
3. Data analysis and verification of illegal activities on networks and systems.
4. Understand and deal with cloud computing concepts and applications.
5. Maintain the confidentiality and security of data and detect breaches that occur.
6. Take countermeasures to unauthorized intrusions and countermeasures through data protection

skills

B. Skills objectives of the program

1. Critical thinking: The ability to analyze complex problems, evaluate different solutions, and make informed decisions based on evidence and logic is critical in cybersecurity engineering.
2. Problem-solving skills: The ability to identify security vulnerabilities, develop effective solutions, and efficiently troubleshoot problems is an essential skill for a cybersecurity engineer.
3. Analytical skills: The ability to examine data, detect patterns, and interpret trends is essential to understanding cyber threats and developing effective defensive strategies.
4. Attention to detail: Developing a keen eye on details is vital to ensure the security of systems and networks
5. Creativity: Thinking outside the box and coming up with innovative solutions to combat evolving cyber threats is a valuable skill for cybersecurity engineers
6. Risk assessment skills: The ability to assess and prioritize potential risks based on their impact and develop risk mitigation strategies is critical in cybersecurity.
7. Adaptability: Being adaptable and wanting to learn new techniques and techniques is essential to stay ahead of cyber threats.
8. Collaborative skills: Working effectively in teams, communicating ideas clearly, and collaborating with colleagues from diverse backgrounds are important skills to address complex cybersecurity challenges.
9. Continuous learning: Having a continuous learning mindset and staying up-to-date Trends and technologies are essential to succeed in this critical in cybersecurity.
7. Adaptability: Being adaptable and willing to learn new techniques and techniques is essential to stay ahead of threats

value

- Value objectives

1. Teamwork: Ability to work collaboratively with colleagues, share knowledge, and contribute effectively to group projects or incident response teams.
2. Time Management: Skill in prioritizing tasks, meeting deadlines, and efficiently managing workload to handle multiple projects simultaneously.
3. Ethical mindset: Commitment to upholding ethical standards, maintaining confidentiality, and adhering to legal regulations in cybersecurity practices.
4. Research and Commitment to Learning: A strong dedication to continuous learning and survival Updating with the latest trends is vital to success in cybersecurity.
5. Resilience: Ability to deal with high-stress situations, recover from setbacks, and persevere in finding solutions in the middle of evolving cyber threats.
6. English and Arabic speaking skills
7. Leadership and Communication: Developing leadership skills and building a professional network can enhance career opportunities and facilitate collaboration in cybersecurity.

9. Teaching and learning strategies

1. Explain the scientific material to students in detail.

2. Participation of students in solving scientific and mathematical problems related to the specific scientific material

3. Discussion and dialogue on vocabulary related to the topic and scientific material

4. Blended learning (online learning material with online interaction, with classroom methods).

5. Science films, educational videos

6. Labs

7. Summer training
8. Graduation Projects

1

10. Education institution

Students' participation in solving mathematical problems is an important process that contributes to enhancing their understanding of mathematical subjects and developing their mental skills. Here are some ways in which students can be encouraged to participate in solving mathematical problems:

1. Providing a supportive atmosphere:

• Create a classroom environment that encourages the use of mathematical problems as a learning opportunity.

• Encouraging students to exchange ideas and cooperate in solving problems with each other.

2. Presenting issues in an exciting way:

• Choose problems that are stimulating and arouse curiosity, so that students feel a desire to solve them.

• Use everyday issues or applied examples to capture students' interest.

3. Provide various challenges:

• Providing a variety of problems at different difficulty levels, so that each student finds a challenge appropriate to his level.

11. Evaluation method

Daily tests, mid-term exams, final exams, descriptive homework assignments Weekly reports on the subject and seminars.

Faculty members

no	Name	Certificate	Academic title/ job title	General	Exact	Position/responsibility	Permanent/ contract
1	**Farqad Hamed Abdul Rahim Abdullah**	Ph.D	Assistant Professor	Computer Science	Security Information	Teaching	permanent
2	**Asif Abdulelah Saleh Mehidi**	Ph.D	Assistant Professor	Power Electronics	Electronics Power	Studies and Planning Division manager	Permanent
3	**Kafaa Hadi Thanoon Younis**	Master's	Assistant Professor	Computer Science	Image Processing and Digital Signal	Teaching	Permanent
4	**Nawar Abdul Ghani Sultan Elias**	Ph.D	Lecturer	Philosophy of Computer Science	Computer Science	Head of Department	Permanent
5	**Zakaria Noureddine Mahmoud Abdullah**	Ph.D	Lecturer	Computer Science	Artificial Intelligence	Scientific Assistant of the College	Permanent
6	**Younis Anas Younis Hassan**	Ph.D	Lecturer	Computer Engineering	Computer Engineering	Teaching	Permanent
7	**Razan Abdul jawad Abdul Hamid**	Ph.D	Lecturer	Computer Engineering	Computer Engineering	Teaching	Permanent
8	**Fadwa Subhi Mustafa Yahya**	Ph.D	Lecturer	Electrical Engineering	Image Processing	Teaching	Permanent
9	**Rabie Raad Ali Ahmed**	Ph.D	Lecturer	Computer Science	Information Technology	Technology Incubator Unit Officer	Permanent
10	**Arwa Hamed Saleh Ahmed**	Ph.D	Lecturer	Computer Engineering	Computer Engineering	Teaching	Permanent
11	**Afaf Nasser Yousef Abdullah**	Ph.D	Lecturer	Philosophy of Mathematics	Computational Mathematics	Studies and Planning Division	Permanent
12	**Lubab Harith Sami Ahmed**	Master	Lecturer	Computer Engineering Techniques	Computer Engineering Techniques	Teaching	Permanent
13	**Shaima Miqdad Muhammad Najib**	Master	Lecturer	Computer Engineering Techniques	Computer Engineering	Teaching	Permanent
14	**Omar Muhammad Jihad Mahmoud**	Master	Assistant Lecturer	Mathematics	Computational Mathematics	Department rapporteur	Permanent
15	**Marwa Younis Abdullah Jassim Mohammed**	Master	Assistant Lecturer	Sciences in Communications Engineering	Sciences in Communication Engineering	Teaching	Permanent
١٦	**Ammar Abdul Majeed Gharbi Nasser**	Master	Assistant Lecturer	Computer Science	Security Data	Teaching	Permanent
١٧	**Rana Khaled Sabry Abdullah Mohammed**	Master	Assistant Lecturer	Computer Engineering	Computer Engineering	Continuing Education Unit Officer	Permanent
١٨	**Mahmoud Shaker Mahmoud Ahmed**	Master	Assistant Lecturer	Communications Engineering	Communications Engineering	M. Student Affairs Division	Permanent

١٩	**Abdul Rahman Shakib Muhammad Yahya**	Master	Assistant Lecturer	Communications Engineering	Communications Engineering	Missions and Cultural Relations Unit	Permanent
٢٠	**Roaa Wael Hassan Youssef**	Master	Assistant Lecturer	Mathematics	Mathematics	Teaching	Permanent
٢١	**Areej Mahmoud Asaad Aide**	Master	Assistant Lecturer	Computer Technology Engineering	Computer Technology Engineering	Information Technology Division	Permanent
٢٢	**Abdulrahman Abdulqader Ahmed Mohammed**	Bachelor's	M. Technical engineer	Electrical Power	Electrical Power	Computer lab administrator	Permanent
٢٣	**Ziad Shro Khudida Qasim**	Bachelor's	Assistant Programmer	Computer Science	Computer Science	Website Unit Officer	Permanent
٢٤	**Abdulrahman Anmar Sharaf Eddin Muhammad**	Bachelor's	Assistant Engineer	Electrical Engineering	Electronics and Communications	Engineer	Permanent
٢٥	**Omar Shehab Ahmed Gharbi**	Bachelor's	Assistant Engineer	Computer Engineering	Computer Engineering	Engineer	Permanent
٢٦	**Mohammed Basil Yousef Jassim**	Bachelor's	Assistant Engineer	Computer Engineering and Informatics	Computer Engineering and Informatics	Engineer	Permanent
٢٧	**Sayda'a al-Din Siddiq Nayef Ali**	Bachelor's	Assistant Chief Engineer	Electrical Power Techniques Engineering	Electrical Power	Engineer	Permanent
٢٨	**Doha Fathi Ibrahim Hussein**	Bachelor's	Technical Engineer Assistant	Computer Technology Engineering	Networks and Communications Branch	Laboratory	Permanent
٢٩	**Hamza Faris Abdulaziz**	Bachelor's	Assistant Programmer	Computer Science	Computer Science	Computer lab administrator	Permanent
٣٠	**Amira Wasfi Mustafa Suleiman**	Bachelor's	Assistant Programmer	Computer Science	Computer Science	Computer lab administrator	Permanent
٣١	**Saad Jabr Mahmoud Ali**	Technical diploma	Assistant Technical Manager	Electrical	Electricity	Department secretariat	Permanent
٣٢	**Faisal Saado Saleh Saado**	diploma	Data Logger	Informatics Technology	Informatics Technology	technical	permanent

Professional development

Orienting new faculty members

1. Develop an orientation program to introduce new faculty members to the institution and its policies and procedures.

2. Pair new faculty with experienced mentors to provide guidance, support, and advice

3. Organize regular training workshops on teaching methodologies, assessment and research technique

s 4. Establish a feedback mechanism for new faculty members to receive constructive feedback on their performance and areas of improvement

5. Encourage participation in conferences, seminars and research projects to promote professional growth

6. Provide ongoing support through regular meetings, resources and access to professional development materials

Professional development for faculty members

1. Faculty skills should be assessed to study their educational and technical needs.

2. Provide training courses to help develop faculty skills in areas such as advanced education, educational technologies, and rigorous assessment.

3. Encourage teamwork among faculty members to share experiences and knowledge.

4. Provide continuous updates on the latest in the fields of education and educational technologies.

5. Provide continuous support to faculty members to help solve the problems and challenges they face.

6. Conduct periodic evaluations to review the professional development of faculty members and identify advantages and disadvantages

12. ***Acceptance criterion***

• Scientific section.
• Professional study.

13. The most important sources of information about the program

1. University website.
2. The location of the department.
3. Academic description files and program specifications.
4. Academic Program Review Form.
5. Research sites in the college.

14. Program development plan

Curriculum Improvement:
1. One of the future plans is the development of cybersecurity laboratories as well as the development of the curriculum to keep pace with modern technological development through addition and deletion.
2. Provide advanced courses in cybersecurity, cloud computing, artificial intelligence and data analytics to keep pace with industry requirements
3. Include hands-on training in network security, threat detection and secure infrastructure design
4. Provide specialized courses in cloud security, encryption techniques and risk assessment.

Faculty Development:
1. Employ experienced professionals in cybersecurity and cloud computing to enhance the quality of teaching and the relevance of the industry.
2. Encourage faculty research in advanced cybersecurity technologies and cloud computing developments.

Industrial Partnerships:
1. Collaborate with cybersecurity companies, cloud service providers, and

technology companies for in-house training, guest lectures, and real-world projects

2. Create a strong network with industry experts to ensure curriculum alignment with current industry trends and practices.

Student Engagement:

1. Organize cybersecurity competitions and cloud computing workshops to enhance practical skills and innovation among students

2. Encourage student participation in research projects related to cybersecurity, cloud security and emerging technologies. Infrastructure

Development:

1. Invest in state-of-the-art cybersecurity labs, cloud computing resources, and simulation environments for hands-on and experiential training

2. Provide access to industry-standard tools and software used in cybersecurity and computing.

Curriculum skills chart

				Learning outcomes required from the program											
Year/level	**Course Code**	**Course Name**	**Core or basic**	**Knowledge**				**Skills**				**the value**			
2024-2025				A1	A2	A3	A4	B1	B2	B3	B4	C1	C2	C3	C4
Level 1 – First Semester	**BCYSCE100-S1**	**Mathematic**	secondary	TH	P	TH		TH		B		TH	P		
	BCYSCE105-S1	**Linux Administration**	essential	TH	P			TH		P			R		R
	BCYSCE102-S1	**Fundamentals of Programming**	essential	TH	P			p							
	BCYSCE104-S1	**Fundamentals of Electrical Engineering**	secondary	TH	P										
	NTU 101	**English language**	essential	TH	P			TH					P		E
	BCYSCE103-S1	**Introduction to Sociology**	secondary	TH	P										R
	NTU100	**Human rights and Democracy**	optional	TH				P					R		B
Level 1 – Second	**BCYSCE101-S2**	**Digital Electronics**	secondary	TH	p	B		E			TH		P		

Semester	**BCYSCE106-S2**	**Introduction to Probability and Statistics**	secondary	TH	B										TH
	BCYSCE107-S2	**Object oriented programming**	essential	TH	p			S			R		E		
	NTU102	**Computer**	main	TH	P			B			P				TH
	BCYSCE108-S2	**Introduction to Cyber security Engineering**	secondary	TH	E			B			E				
	NTU103	**Arabic Language**	main	TH	E	B									
Level ٢ – First Semester	**BCYSCE200-S1**	**Computer Electronics**	secondary	TH	B	P									TH
	BCYSCE205-S1	**Discrete Math**	essential	TH	p			S			R		E		
	BCYSCE202-S1	**Database systems**	secondary	TH	P			B			P				TH
	BCYSCE204-S1	**Python Programming for Cybersecurity**	essential	TH	p			B			E				
	BCYSCE203-S1	**Operating Systems**	essential	TH	p	B									
	NTU203	**Bath Party Crimes**	main	TH	E	B					R				
	NTU200	**English language**	main	TH	E	B									

	BCYSCE205-S2	**Computer Networks**	essential	TH	P		R								
Level 2 – Second Semester	**BCYSCE205-S2**	**Data structures**	secondary	TH	p	B		E					P		
	BCYSCE202-S2	**Database security**	essential	TH	B										E
	BCYSCE204-S2	**Computer Organization and Architectures**	secondary	TH	p			S			R		E		PR
	BCYSCE203-S2	**Networks Security**	essential	TH	P			B			P				S
	NTU202	**Arabic Language**	main	TH	E			B			E				PR
	NTU 204	**Cybersecurity Professional ethics**	main	TH	E	B									S
	BCYSCE201-S1	**Network Administration and Infrastructure**	essential	TH	p	B		E			PR		P		S
	NTU201	**Computer**	main	TH	B					R					E
Level 3 – First Semester	**BCYSCE203-S1**	**Introduction to Cryptography**	essential	TH	P		R				B				
	BCYSCE305-S1	**Introduction to Hardware security**	essential	TH	p	B		E					P		
	BCYSCE302-S1	**Digital Signal Processing**	secondary	TH	B										E

	BCYSCE304-S1	**Mobile and wireless networks**	essential	TH	p			S			R		E		PR
	BCYSCE303-S1	**Fundamentals of Cloud computing**	essential	TH	P			B			P				S
Level ٣ – Second Semester	**BCYSCE300-S2**	**Mobile and wireless networks security**	essential	TH	P			B			P				S
	BCYSCE305-S2	**Secure software development**	essential	TH	E			B			E				PR
	BCYSCE302-S2	**Operating system security**	essential	TH	E	B									S
	BCYSCE304-S2	**Practicing cybersecurity: Attacks and Countermeasures**	essential	TH	p	B		E			PR		P		S
	BCYSCE303-S2	**Engineering Analysis**	secondary	TH	P					R					E
	BCYSCE301-S2	**Cloud Computing security**	essential	TH	P		R					B			
Level٤ – First Semester	**BCYSCE400-S1**	**Intrusions Detection and prevention System**	essential	TH	P			B			P				S
	BCYSCE405-S1	**Research Methodology**	secondary	TH	E			B			E				PR
	BCYSCE402-S1	**AI for Cybersecurity Engineering**	essential	TH	E	B									S
	BCYSCE404-S1	**Practicing cybersecurity: Ethical Hacking and**	essential	TH	p	B		E			PR		P		S

		Vulnerability Analysis													
	BCYSCE403-S1	**Cloud Application**	secondary	TH	P					R					E
	BCYSCE401-S1	**Graduation Project Design**	essential	TH	P		R			B					
Level 4– Second Semester	**BCYSCE400-S2**	**IT Project Management**	Essential	TH	P			B			P				S
	BCYSCE405-S2	**Graduation Project Implementation**	Essential	TH	E			B			E				PR
	BCYSCE402-S2	**Digital Forensics**	Essential	TH	E	B									S
	BCYSCE404-S2	**IoTs and Cybersecurity**	Essential	TH	p	B		E			PR		P		S
	BCYSCE403-S2	**Reverse Engineering-Malwares Analysis**	Essential	TH	P					R					E

P/Practice Pr/Project S/Seminar R/ report TH/ theoretical
B/Book E/Externa

Course Description Form

This course description provides a summary of the most important course characteristics and the learning outcomes expected of the student to achieve, demonstrating whether the student has made the most of the learning opportunities available. It must be linked to the program description.

1. Educational institution

Northern Technical University / Technical Engineering College for computer and AI / Mosul

2. Scientific department/center

Cyber Security and Cloud Computing Techniques Engineering Dept.

3. Course name/code

Mathematics	**BCYSCE100-S1**

4. Available attendance forms

daily

5. Semester/year

Semester

6. Number of study hours (total)

125 H

7. Date the description was prepared

25/10/2024

8. Course objectives

1. Enhance Problem-Solving Skills: Develop the ability to analyze and solve mathematical problems using appropriate strategies, techniques, and mathematical reasoning.
2. Foster Mathematical Thinking: Cultivate critical thinking and logical reasoning skills necessary for understanding and applying mathematical concepts and principles.
3. Promote Conceptual Understanding: Develop a deep understanding of mathematical concepts, including algebra, geometry, statistics, and probability, by exploring their properties, relationships, and applications.
4. Cultivate Mathematical Modeling Skills: Apply mathematical concepts and techniques to real-world problems, formulate mathematical models, and interpret and analyze the results.
5. Promote Mathematical Technology Literacy: Utilize technology tools, such as calculators, graphing software, and spreadsheets, to enhance mathematical understanding, visualization, and problem solving.

MODULE DESCRIPTION FORM
MATHEMATICS

Module Information					
Module Title	**MATHEMATICS**			**Module Delivery**	
Module Type	**Core**			**☒Theory** **☒ Lecture** **☒ Lab** **☒Tutorial** **☐ Practical** **☒ Seminar**	
Module Code	**BCYSCE100-S1**				
ECTS Credits	٥				
SWL (hr/sem)	١٢٥				
Module Level	UGx11_1		**Semester of Delivery**	1	
Administering Department	Cyber Security and Cloud Computing Techniques Engineering		**College**	Technical Engineering College for computer and AI / Mosul	
Module Leader	**Asst. Lecturer Afaf Nasser**		**e-mail**	E-mail	
Module Leader's Acad. Title	Lecturer		**Module Leader's Qualification**	MSc	
Module Tutor			**e-mail**	Afaf.nasser@ntu.edu.iq	
Peer Reviewer Name			**e-mail**		
Scientific Committee Approval Date	25/10/2024		**Version Number**	1.0	

Relation with other Modules			
Prerequisite module		**Semester**	
Co-requisites module	Discrete Math (BCYSCE205-S1)	**Semester**	\

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	6. Enhance Problem-Solving Skills: Develop the ability to analyze and solve mathematical problems using appropriate strategies, techniques, and mathematical reasoning. 7. Foster Mathematical Thinking: Cultivate critical thinking and logical reasoning skills necessary for understanding and applying mathematical concepts and principles. 8. Promote Conceptual Understanding: Develop a deep understanding of mathematical concepts, including algebra, geometry, statistics, and probability, by exploring their properties, relationships, and applications. 9. Cultivate Mathematical Modeling Skills: Apply mathematical concepts and techniques to real-world problems, formulate mathematical models, and interpret and analyze the results. 10. Promote Mathematical Technology Literacy: Utilize technology tools, such as calculators, graphing software, and spreadsheets, to enhance mathematical understanding, visualization, and problem solving.
Module Learning Outcomes	1. Numeracy Skills: Develop the ability to work with numbers, perform calculations, and solve mathematical problems accurately and efficiently. 2. Mathematical Reasoning: Develop logical thinking and problem-solving skills to analyze and solve mathematical problems using appropriate strategies and techniques. 3. Mathematical Communication: Express mathematical ideas and concepts clearly and effectively using mathematical language, symbols, and diagrams. 4. Mathematical Modeling: Apply mathematical concepts and techniques to real-world situations and formulate and solve problems using mathematical models. 5. Algebraic Reasoning: Understand and apply algebraic concepts and methods to analyze patterns, relationships, and functions. 6. Geometric and Spatial Reasoning: Understand and analyze geometric shapes, properties, and spatial relationships using visual representations, diagrams, and proofs.

Learning and Teaching Strategies	
Strategies	1. Lectures and Presentations: Lectures are commonly used to present foundational

	concepts, theories, and methodologies in engineering analysis. 2. Practical Assignments and Problem-Solving Exercises: Hands-on assignments and problem-solving exercises allow students to apply the concepts learned in class to real-world engineering problems. 3. Case Studies and Real-World Examples: Presenting case studies and real-world examples helps students connect theoretical concepts with practical applications. By analyzing and discussing real-world engineering 4. Group Projects and Collaborative Learning: Group projects encourage collaboration and teamwork among students.

Student Workload (SWL)			
Structured SWL (h/sem)	64	**Structured SWL (h/w)**	4
Unstructured SWL (h/sem)	61	**Unstructured SWL (h/w)**	4
Total SWL (h/sem)	**125**		

Module Evaluation

As		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	4	10% (10)	2,4,6,7	LO #1, #2 and #9
	Assignments	9	10% (10)	1,2,3,4,5,6, 7,8,9	LO #1, #4,#5, #6,#7,#8,#9 and #6, #7
	Reading	2	5% (5)	5,7	LO #10, #12,#13
	Report	1	5% (5)	2	LO #5, #8 and #10
	Web Based Learning	4	5% (5)	1,5,8,10	LO #5, #8 ,#9 and #10
	Seminar	1	5% (5)	8	LO #9, #13
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Deliv ery Plan (Weekly Syllabus)

Week	Material Covered
Week 1	Matrix and Determinants • Matrix, properties, and operations • Determinants and properties of determinants
Week 2	**Matrix and Determinants**

	• Inverse of square matrix by determinants. • Solving linear System equations using the inverse of the coefficient matrix and Cramer's rule.
Week 3	**Review of Functions** • Algebraic functions. • Review of natural logarithm, the exponential function, trigonometric functions, inverse trigonometric functions and hyperbolic functions.
Week 4	**Derivatives** • Derivatives formula and chain rule. • Derivatives of natural logarithm, the exponential function.
Week 5	**Derivatives** • trigonometric functions , inverse trigonometric functions and hyperbolic functions • Applications of differentiation.
Week 6	**Integration** • Review of Integration, Indefinite and Definite Integral • Applications of integration.
Week 7	**Integration** • approximation (trapezoidal rule, Simpson's rule) • Area between curves.
Week 8	**Techniques of integration** • Basic integration formulas. • Integration by parts.
Week 9	**Techniques of integration** • Partial fractions. • Trigonometric substitutions. • Improper integral.
Week 10	**Applications of integration** • Volume and solid revolution • Length of plane curves.
Week 11	**Vectors** • Vectors – The Basics • Vector Arithmetic
Week 12	**Vectors** • Dot product • Cross product • Applications.
Week 13	**Complex numbers** • Complex numbers in Cartesian coordinates and polar from. • linear algebra for complex number in polar and Cartesian.
Week 14	**Linear Algebra** • Euler's formula. • DeMoivre's theorem to find powers and the nth roots of given complex numbers.
Week 15	**Review**
Week 16	**Final Exam**

Learning and Teaching Resources		
	Text	**Available in the Library?**

Required Texts	Calculus I, Paul Dawkins, 2007.	Yes
Recommended Texts	Advance Engineering Mathematics, Alan Jeffrey, 2002.	Yes
Websites		

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Fundamentals of Programming

Module Information

Module Title	**Fundamentals of Programming**	**Module Delivery**	
Module Type	**Core**	☒ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**BCYSCE102-S1**		
ECTS Credits	**7**		
SWL (hr/sem)	**175**		
Module Level	1	**Semester of Delivery**	1
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Zakaria Noor Aldeen Mahmood	**e-mail**	E-mail

Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	Ph.D.
Module Tutor		**e-mail**	zakaria@ntu.edu.iq
Peer Reviewer Name		**e-mail**	
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules

Prerequisite module	Object oriented Programming (BCYSCE107-S2)	**Semester**	2
Co-requisites module		**Semester**	

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	1. Introducing the fundamentals and principles of programming in C++ language. 2. Teaching the concept of Procedure Oriented Programming. 3. Starts from scratch to advance programing by improving the skills of the students through several program implementation and code writing. 4. The students should be able to define programming purposes & the required code lines to perform the needed works. 5. as well as qualifying him to use the different kinds of programming style and program functions in building & executing the projects of cyber security engineering.
Module Learning Outcomes	1. Understanding the fundamentals of programming in C++ language. 2. Mastering C++ programming tools and techniques, including common integrated development environment (IDE) such as visual studio. 3. Becoming familiar with the C++ concepts such as Variables, assignments, Simple input, Main program and functions. 4. Being competent in common If-statement,Loops, Boolean Expressions & Logical operators. 5. Being able to perform Function call, Parameters, return values. 6. Being able to write C++ codes, Basics of program design & Programming style.

Module Evaluation

		Time/Number	Weight (Marks)	Week Due
Formative assessment	Quizzes	٤	10% (10)	٣,6,9,12
	Assignments	8	5% (5)	Every other week
	Projects / Lab.	14	10% (10)	Continuous
	Report	2	5% (5)	7, 14
	Seminar	1	10% (10)	15
Summative assessment	Midterm Exam	2hr	10% (10)	7
	Final Exam	3hr	50% (50)	16
Total assessment			100% (100 Marks)	

Learning and Teaching Strategies

Strategies	The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)

Structured SWL (h/sem)	79	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	96	**Unstructured SWL (h/w)**	6
Total SWL (h/sem)	**175**		

FUNDAMENTALS OF PROGRAMMING - PROGRAMME COURSE DESCRIPTION

Code BCYSCE ١٠٢-S١	Name of the Course Unit	Semester	In-Class Hours (T+P)	Credit	ECTS Credit
	Fundamentals of Programming	2	2+3		7

GENERAL INFORMATION	
Language of Instruction :	**English**
Level of the Course Unit :	**BACHELOR'S DEGREE**
Type of the Course :	**Compulsory**
Mode of Delivery of the Course Unit	**Face to Face**
Coordinator of the Course Unit	**Dr. Zakaria Noor Aldeen Mahmood**
Instructor(s) of the Course Unit	**Dr. Zakaria Noor Aldeen Mahmood**

OBJECTIVES AND CONTENTS	
Objectives of the Course Unit:	Introducing the fundamentals and principles of programming in C++ language. Starts from scratch to advance programing by improving the skills of the students through several program implementation and code writing. The students should be able to define programming purposes & the required code lines to perform the needed works as well as qualifying him to use the different kinds of programming style and program functions in building & executing the projects of cyber security engineering.
Contents of the Course Unit:	1. Procedure Oriented Programming 2. Structure of a program 3. Flow Chart. 4. Variables, assignments, Simple input, Main program If-statement If-else, Boolean Expressions & Logical operators 5. Output formatting. 6. Pointers. 7. Dynamic Memory.

Delivery Plan (Weekly Syllabus)

WEEK	KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)
1	Introduction to C++ (Structure of a program), Flow Chart.
2	Variables, assignments, Simple input, Main program.
3	If-statement If-else, Boolean Expressions & Logical operators.
4	Loops Nested Loops, and program Design.
5	Output formatting.
6	Functions, Parameters, return values.
7	Debugger.
8	Lists Methods, Nesting, Slicing, and Comprehension.

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
9	Strings and String Formatting.
10	Dictionary and Handle Exceptions.
11	Values and references.
12	Basics of program design & Programming style.
13	Pointers (Reference operator, dereference operator, Declaring variables of pointer types, Pointers and arrays, Pointers to pointers, void pointers, and Pointers to functions).
14	Dynamic Memory (Operators new, check if the allocation memory is successful and Operators delete).
15	review/seminar
16	Final Exam.

Delivery Plan (Weekly Lab. Syllabus)	
	Material Covered
Week 1	Lab 1: Getting started - Structure of a program- Flow Chart.
Week 2	Lab 2: Variables, assignments, Simple input, Main program - Examples and Problems
Week 3	Lab 3: If-statement If-else, Boolean Expressions & Logical operators - Examples and Problems.
Week 4	Lab 4: Loops Nested Loops, and program Design - Examples and Problems.
Week 5	Lab 5: Loops Nested Loops, and program Design - Examples and Problems.
Week 6	Lab 6: Functions, Parameters, return values - Examples and Problems.

Week 7	Lab 7: Debugger - Examples and Problems.
Week 8	Lab 8: Lists Methods, Nesting, Slicing, and Comprehension - Examples and Problems.
Week 9	Lab 9: Dictionary and Handle Exceptions - Examples and Problems.
Week 10	Lab 10: Pointers - Examples and Problems.
Week 11	Lab 11: Strings and String Formatting - Examples and Problems.
Week 12	Lab 12: Programming style.
Week 13	Lab 13: Values and references.
Week 14	Lab 14: Dynamic Memory - Examples and Problems.
Week15	Lab 15: Review
Week 16	**Final Exam**

WORKLOAD & ECTS CREDITS OF THE COURSE UNIT Fundamentals of Programming			
Workload for Learning & Teaching Activities			
Type of the Learning Activates	**Learning Activities (# of week)**	**Duration (hours, h)**	**Workload (h)**
Lecture & In-Class Activities	15	2	30
Preliminary & Further Study	NA	NA	NA
Land Surveying	NA	NA	NA
Group Work	NA	NA	NA
Laboratory	15	3	45
Reading	6	1	6
Assignment (Homework)	8	2	16
Project Work	NA	NA	NA
Seminar	1	1	1
Internship	NA	NA	NA
Technical Visit	NA	NA	NA
Web Based Learning	6	2	12
Implementation/Application/Practice	NA	NA	NA
Practice at a workplace	NA	NA	NA
Occupational Activity	NA	NA	NA
Social Activity	NA	NA	NA
Thesis Work	NA	NA	NA
Field Study	NA	NA	NA
Report Writing	2	2	4
Final Exam -Theory	1	3	3
Final Exam - Practical	1	1	1
Preparation for the Final Exam- Theory	1	20	20
Preparation for the Final Exam -Practical	1	15	15
Mid-Term Exam - Theory	1	2	2
Mid-Term Exam - Practical	1	1	1
Preparation for the Mid-Term Exam	1	15	15
Short Exam (Quizzes)	4	0.5	2
Preparation for the Short Exam (Quizzes)	4	2	8

Total Workload of the Course Unit			175

Learning and Teaching Resources

	Text	Available in the Library?
Required Texts	1. **Choudhary, H. (2013). C++ Programming-Final Golden Edition. Beginners To Experts Approach Guide-With Easy Learning & Problem Analysis to Program Design & Development.**	no
Recommended Texts	2. **Farrell, J. (2008). Object-oriented programming using C++. Cengage Learning.** 3. **Object-Oriented Programming in C++, Fourth Edition.**	no
Websites	4. **https://www.geeksforgeeks.org/cpp** 5. https://www.w3schools.com/cpp	

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Linux Administration

Module Information					
Module Title	**Linux Administration**			**Module Delivery**	
Module Type	**Core**			☒ **Theory**	
Module Code	**BCYSCE105-S1**			☒ **Lecture**	
ECTS Credits	**7**			☒ **Lab**	
SWL (hr/sem)	**175**			☐ **Tutorial**	
				☐ **Practical**	
				☒ **Seminar**	
Module Level		UGx11 1	**Semester of Delivery**		1
Administering Department		Cyber Security and Cloud Computing Techniques Engineering	**College**		Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Zakaria Noor Aldeen Mahmood		**e-mail**		E-mail
Module Leader's Acad. Title		Lecturer	**Module Leader's Qualification**		Ph.D.
Module Tutor			**e-mail**		zakaria@ntu.edu.iq
Peer Reviewer Name			**e-mail**		
Scientific Committee Approval Date		25/10/2024	**Version Number**		1.0

Relation with other Modules			
Prerequisite module	Introduction to Cyber Security Engineering (BCYSCE107-S2)	**Semester**	2
Co-requisites module		**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	1. Introducing the fundamentals and principles of Linux administration using Linux operating system. 2. starts from scratch to network monitoring applications. 3. Improving the skills of the students through several Linux implementations and scripts writing. 4. The students should be able to understand the uses and purpose of using scripts and retrieve important network settings and packets sending and receiving information. 5. Help the students perform the needed cyber security works as well as qualifying him to use the different kinds of shell scripting style and instructions to build & execute the projects of cyber security engineering.
Module Learning Outcomes	1. Understanding the fundamentals of Linux administration. 2. Mastering Linux Instructions and commands, including common users administration & Permissions. 3. Becoming familiar with the Linux operating system and its distributions. 4. Being competent in common Networking & Configuring Network Settings and Package Management. 5. Being able to perform Bash Scripting and Execute shell command. 6. Being able to write complete shell scripts to perform I/O Manipulation and I/O Redirections
Learning and Teaching Strategies	

Strategies	The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.
Student Workload (SWL)	
Structured SWL (h/sem)	
Unstructured SWL (h/sem)	
Total SWL (h/sem)	

Module Evaluation				
As		**Time/Number**	**Weight (Marks)**	**Week Due**
Formative assessment	**Quizzes**	٤	10% (10)	٣,6,9,12
	Assignments	8	5% (5)	Every other week
	Projects / Lab.	14	10% (10)	Continuous
	Report	2	5% (5)	7
Summative assessment	**Midterm Exam**	2hr	10% (10)	7
	Final Exam	3hr	50% (50)	15
Total assessment			100% (100 Marks)	

Code BCYSCE 403-S2	**Name of the Course Unit**	**Semester**	**In-Class Hours (T+P)**	**Credit**	**ECTS Credit**
LINUX	**Linux Administration**	**2**	**2+3**		**7**

ADMINISTRATION - PROGRAMME COURSE DESCRIPTION

GENERAL INFORMATION	
Language of Instruction :	**English**
Level of the Course Unit :	**BACHELOR'S DEGREE**
Type of the Course :	**Compulsory**
Mode of Delivery of the Course Unit	**Face to Face**
Coordinator of the Course Unit	**Dr. Zakaria Noor Aldeen Mahmood**
Instructor(s) of the Course Unit	**Dr. Zakaria Noor Aldeen Mahmood**

OBJECTIVES AND CONTENTS	
Objectives of the Course Unit:	Introducing the fundamentals and principles of Linux administration using Linux operating system. starts from scratch to network monitoring applications. Improving the skills of the students through several Linux implementations and scripts writing. The students should be able to understand the uses and purpose of using scripts and retrieve important network settings and packets sending and receiving information. Help the students perform the needed cyber security works as well as qualifying him to use the different kinds of shell scripting style and instructions to build & execute the projects of cyber security engineering.
Contents of the Course Unit:	• Linux Fundamentals • Users & Permissions • Networking & Package Groups • Linux Services • Bash Scripting • Shell script • I/O Manipulation and I/O Redirections

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	Linux Fundamentals: Linux Distros & History, Debian vs RedHat, Basic Commands.
2	Linux Fundamentals: Debian vs RedHat.
3	Linux Fundamentals: Basic Commands.
4	Users & Permissions: File System & File Structure
5	Users & Permissions: Users & Groups, Permissions
6	Networking & Package Groups: Package Management.
7	Networking & Package Groups: Configuring Network Settings.
8	Linux Services: Apache, Creating a Basic Website
9	Linux Services: SSH & Telnet
10	Linux Services: FTP, SMB
11	Bash Scripting, Data types and variables, Execute shell command
12	Shell Scripting, Loops function
13	Shell conditions, and arithmetic comparisons
14	I/O Manipulation, I/O Redirections
15	Review
16	Final Exam

Delivery Plan (Weekly Lab. Syllabus)	
Week	**Material Covered**
Week 1	Lab1: Installation of Linux OS.
Week 2	Lab2 : Basic Command 1
Week 3	Lab 3: Visual interface (VI Editor)
Week 4	Lab 4: User Administration and Group Administration
Week 5	Lab5: Permissions and Access control List
Week 6	Lab 6: Change ownership of files and directories and Change group owner of files and directories
Week 7	Lab 7: Partitions and Swap partition (Virtual memory)
Week 8	Lab 8: Disk Quotas and Logical Volume Manager (LVM)
Week 9	Lab 9: Redundant party of independent disks (RPID) and Backup and restore using CPIO Command
Week 10	Lab 10: Backup and restore using TAR and Filter the Archive through BZIP2(-J) and Backup and restore using TAR and Filter the Archive through GZIP2(-z)
Week 11	Lab 11: Redundant party of independent disks (RPID)
Week 12	Lab 12: Backup and restore using CPIO Command
Week 13	Lab 13: Backup and restore using TAR and Filter the Archive through BZIP2(-J)
Week 14	Lab 14: Review
Week 15	**Final Exam**

WORKLOAD & ECTS CREDITS OF THE COURSE UNIT

Linux Administration

Workload for Learning & Teaching Activities

Type of the Learning Activates	Learning Activities (# of week)	Duration (hours, h)	Workload (h)
Lecture & In-Class Activities	15	2	30
Preliminary & Further Study	NA	NA	NA
Land Surveying	NA	NA	NA
Group Work	NA	NA	NA
Laboratory	15	3	45
Reading	6	1	6
Assignment (Homework)	8	2	16
Project Work	NA	NA	NA
Seminar	1	1	1
Internship	NA	NA	NA
Technical Visit	NA	NA	NA
Web Based Learning	6	2	12
Implementation/Application/Practice	NA	NA	NA
Practice at a workplace	NA	NA	NA
Occupational Activity	NA	NA	NA
Social Activity	NA	NA	NA
Thesis Work	NA	NA	NA

Field Study	NA	NA	NA
Report Writing	2	2	4
Final Exam -Theory	1	3	3
Final Exam - Practical	1	1	1
Preparation for the Final Exam-Theory	1	20	20
Preparation for the Final Exam - Practical	1	15	15
Mid-Term Exam - Theory	1	2	2
Mid-Term Exam - Practical	1	1	1
Preparation for the Mid-Term Exam	1	15	15
Short Exam (Quizzes)	4	0.5	2
Preparation for the Short Exam (Quizzes)	4	2	8
Total Workload of the Course Unit			175

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	**1.** Unix And Linux®System Administration Handbook. Fourth Edition, Evi Nemeth Garth Snyder,Trent R. Hein and Ben Whaley	yes
Recommended Texts	1. Modern Linux Administratio (2016) by Sam R. Alapati. 2. LINUX SYSTEM ADMINISTRATION by *Tom Adelstein and Bill Lubanovic*	yes
Websites		
Grading Scheme		

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D -Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group	**FX –** Fail	(45-49)	More work required but credit awarded
(0 – 49)	**F –** Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Introduction to Sociology

Module Information			
Module Title	**Introduction to Sociology**	**Module Delivery**	
Module Type	**Core**	☐ **Theory** ☒ **Lecture** ☐ **Lab** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**BCYSCE103-S1**		
ECTS Credits	**4**		
SWL (hr/sem)	**100**		
Module Level	1	**Semester of Delivery**	1
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Razan Abdulhammed	**e-mail**	E-mail

Module Leader's Acad. Title	Assistant Professor	**Module Leader's Qualification**	Ph.D.
Module Tutor	Name (if available)	**e-mail**	rabdulhammed@ntu.edu.iq
Peer Reviewer Name	Name	**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	11. Examining legal and regulatory requirements, ethical issues, and the development of cybersecurity policy for commercial and government organizations. 12. Introduce students to the field of sociology and its central theoretical perspectives from Cybersecurity perspective. Provide students with basic ideas and knowledge in the science of sociology. 13. Help students understand the similarities and differences between different sociological paradigms. 14. provide students with basic ideas and knowledge in the science of sociology and how cybersecurity issues effects society. 15. Introduce student to terminology related to cybersecurity such as Cybercrime and deviance, Globalization. 16. Explore the development of organizational cybersecurity policy that meets an organization's compliance requirements and business goals. 17. Introduce students to new ways of thinking about race, ethnicity, and culture from the perspectives of sociology. 18. Use computational social science techniques to identify, counter, and measure the impact of communication in social cybersecurity.
Module Learning Outcomes	1. Understanding the impact of technology on society: Students will be able to analyze the effects of technology on social structures, institutions, and relationships, and identify potential cybersecurity risks associated with technological advancements. Students can explain the sociological significance of social identity groups and the processes that create them; determine the historical and contemporary factors that shape social inequality; and analyze the relationship between social structure and individual agency. 2. Students will be able to define and explain sociological concepts and explain social facts and society-related concepts. 3. Students will be able to effectively engage with and apply their “sociological imagination” to think critically about the social world and what separates sociology from other social science disciplines. 4. Students will be able to construct relevant arguments using data from credible sources and demonstrate familiarity with basic statistical concepts. 5. help students to develop critical thinking skills, understand sociological concepts and theories, and analyze social phenomena from a sociological perspective. 6. Help students to develop communication and research skills, as well as their ability to engage with diverse perspectives and apply sociological concepts to real-world issues.
Indicative Contents	Indicative content includes the following. Introduction to Sociology and Cybersecurity. (3hrs) Cybersecurity Fundamentals. (2hrs) Sociology Fundamentals. (10hrs) Cybersecurity and Society. (3hrs) Cybercrime and Deviance. (2hrs)

	Cybersecurity and Social Change. (2hrs) Cybersecurity and Globalization. (2hrs) Cybersecurity and Ethics. (1hrs) Introduction to Cyberbullying(2hrs) Effects of Cyberbullying (1hrs) Human-factors, Cyber security, and sociology. (3hrs) Risks and cybersecurity incidents and how society should deal with them. (3hrs)

Learning and Teaching Strategies

Strategies	Type something like: The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive learning and by considering types of simple case study discussions involving some sampling activities that are interesting to the students.

Student Workload (SWL)

Structured SWL (h/sem)	33	**Structured SWL (h/w)**	2
Unstructured SWL (h/sem)	67	**Unstructured SWL (h/w)**	4
Total SWL (h/sem)	**200**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	2	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

Week	Material Covered
1	• Introduction to Sociology and Cybersecurity: • Overview of the course • Introduction to sociology and cybersecurity • The importance of cybersecurity in modern society
2	**Cybersecurity Fundamentals.** • Cybersecurity basics • Cyber threats and vulnerabilities • Cybersecurity best practices
3	**Sociology Fundamentals**. • Introduction to sociology. • Social structures and institutions. • Social norms and values.
4	**Cybersecurity and Society** • The impact of cybersecurity on society. • Social and cultural factors that influence cybersecurity practices. • Privacy and security policy. • social, political, legal, criminological, and economic dimensions of cybersecurity through a social science framework
5	**Cybercrime and Deviance** • Types of cybercrime. • Theories of deviance and cybercrime. • The impact of cybercrime on society.
6	**Cybersecurity and Social Change** • Cybersecurity and social change • The role of technology in social change • Cybersecurity and activism
7	Cybersecurity and Globalization. • Cybersecurity and globalization • The impact of globalization on cybersecurity • Cybersecurity and international relations
8	**Cybersecurity and Ethics** • Ethical issues in cybersecurity • Cybersecurity and social responsibility • Cybersecurity and the future of society
9	**Introduction to Cyberbullying** • Definition of cyberbullying • Types of cyberbullying • How cyberbullying differs from traditional bullying
10	**Effects of Cyberbullying.** • Emotional and psychological impact on victims • Impact on academic performance • Legal and social consequences
11	**Responding to Cyberbullying.** • How to identify cyberbullying. • Legal and ethical considerations • Reporting cyberbullying incidents**.**

	Supporting victims of cyberbullying.
12	**Human-factors and Cyber security** • Human-factors approach to understanding cybersecurity threats, social factors that contribute to cyber incidents
13	**Risks and cybersecurity incidents** • The political and legal mechanisms that are developed to control the behaviors of those who create risks and cybersecurity incidents.
14	**Review and Student Presentation**
15	**Final Exam**

Learning and Teaching Resources

	Text	Available in the Library?
Required Texts	Introduction to Sociology" by George Ritzer.	Yes
Recommended Texts	1. "Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer and Allan Friedman 3. "The Cybersecurity Canon: Must-Read Books" by Palo Alto Networks	No
Websites		

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Fundamentals of Electrical Engineering

Module Information					
Module Title	**Fundamentals of Electrical Engineering**			**Module Delivery**	
Module Type	**Core**			✓ **Theory** ✓ **Lecture** ✓ **Lab** ✓ **Tutorial** ✓ **Practical** ✓ **Seminar**	
Module Code	**BCYSCE104-S1**				
ECTS Credits	**5**				
SWL (hr/sem)	**125**				
Module Level		UGx11 1	**Semester of Delivery**		1
Administering Department		Cyber Security and Cloud Computing Techniques Engineering	**College**		Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Thabat F. Thabet		**e-mail**		thabat.tfy@ntu.edu.iq
Module Leader's Acad. Title		Professor	**Module Leader's Qualification**		Ph.D.
Module Tutor	Name (if available)		**e-mail**		E-mail
Peer Reviewer Name		Name	**e-mail**		E-mail
Scientific Committee Approval Date		25/10/2024	**Version Number**		1.0

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	1. To learn the basics of electrical elements (Symbols and Abbreviations, Units, Electric Circuit and Direct Current). 2. Study Ohm's law 3. To learn Kirchhoff's Laws 4. Network Analysis Methods 5. Study The Alternating Current Network 6. Phase Diagram
Module Learning Outcomes	Important: Write at least 6 Learning Outcomes, better to be equal to the number of study weeks. 1. Recognize how electricity works in electrical circuits. 2. List the various terms associated with electrical circuits. 3. Summarize what is meant by a basic electric circuit. 4. Define Ohm's law. 5. Explain the two Kirchoff's laws used in circuit analysis.

	6. Use different Network Analysis Methods to analyze and solve the electrical circuits 7. Discuss the various properties of resistors, capacitors, and inductors. 8. Discuss the operations of sinusoid and phasors in an electric circuit. 9. Identify the capacitor and inductor phasor relationship with respect to voltage and current.
Indicative Contents	Indicative content includes the following. <u>Part A - Introduction to electrical circuits</u> Symbols And Abbreviations, Units, Electric Circuit & It's Element. The Direct Current Network. Ohm's law, Series Circuits, Parallel Circuits, Series-Parallel Circuits, Open and Short Circuits, Source Transformation Conversion Of Delta to Star Connection And Vice Versa [15 hrs] <u>Part B - Kirchhoff's Laws</u> How to use in Network Analysis. [5 hrs] <u>Part C - Network Analysis Methods</u> Loop (mesh) Current Method. Superposition Method. Thevenin's Theorem Norton's Theorem Maximum Power Transfer Theorem Nodal Voltage Method. [30 hrs] <u>Part D - The Alternating Current Network</u> Types of Alternating Waveforms, Generation of Alternating Current, and Definitions related to Alternating Waveforms. The Mean Values of Current and Voltage the Effective Vales of Current and Voltage Circuit Elements in the Phase Domain The Vector Diagram Series Ac Circuits and Parallel Ac Circuits Using Kirchhoff's laws to solve AC circuits [20 hrs] <u>Revision problem classes</u> [5 hrs]

Learning and Teaching Strategies	
Strategies	Type something like: The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)			
Structured SWL (h/sem)	75	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	50	**Unstructured SWL (h/w)**	2
Total SWL (h/sem)	**125**		

Module Evaluation

As		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	6	10% (10)	4, 5, 6, 8, 11 and 12	LO #4, #5, #6, #7, #8 and #9
	Assignments	7	10% (10)	3, 4, 5, 6, 8, 11 and 12	LO #4, #5, #6, #7, #8 and #9
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	6	10% (10)	13	LO #4, #5, #6, #7, #8 and #9
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

Week	Material Covered
Week 1	**Symbols And Abbreviations, Units, Electric Circuit & It's Element. The Direct Current Network.**
Week 2	**Ohm's law, Series Circuits, Parallel Circuits, Series-Parallel Circuits, Open and Short Circuits, Source Transformation**
Week 3	**Conversion Of Delta to Star Connection And Vice Versa**
Week 4	**Kirchhoff's Laws How to use in Network Analysis..**
Week 5	**Loop (mesh) Current Method.**
Week 6	**Superposition Method.**
Week 7	**Thevenin's Theorem**
Week 8	**Norton's Theorem**
Week 9	**Maximum Power Transfer Theorem**
Week 10	**Nodal Voltage Method**
Week 11	**Types of Alternating Waveforms, Generation of Alternating Current, and Definitions related to Alternating Waveforms.** **The Mean Values of Current and Voltage the Effective Vales of Current and Voltage**
Week 12	**Circuit Elements in the Phase Domain**

	The Vector Diagram
Week 13	**Series Ac Circuits and Parallel Ac Circuits**
Week 14	**Using Kirchhoff's laws to solve AC circuits**
Week 15	**Preparatory week before the final Exam**
Week 16	**Final Exam**

Delivery Plan (Weekly Lab. Syllabus)	
Week	**Material Covered**
Week 1	**Basic information**
Week 2	**Color of resistance**
Week 3	**Ohm's law and resister in series and parallel**
Week 4	**Star and delta connection**
Week 5	**Kirchhoff's law**
Week 6	**Superposition theorem**
Week 7	**Thevenin's Theorem**
Week 8	**Maximum Power Transfer**
Week 9	**Norton's Theorem**
Week 10	**Operating of Oscilloscope (CRO)**
Week 11	**Utilization of Oscilloscope**
Week 12	**The Sine wave**
Week 13	**Application of AC signal**
Week 14	**Time constant**

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Electric Circuits, by: James W. Nilsson and Susan A. Riedel Pearson Education Limited 10th edition 2015	Yes
Recommended Texts	FUNDAMENTALS OF ELECTRICAL ENGINEERING, by: Giorgio Rizzoni, McGraw-Hill, 1st edition, 2009.	No
Websites	https://www.coursera.org/browse/physical-science-and-engineering/electrical-engineering	

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 – 100	Outstanding Performance
	B - Very Good	80 – 89	Above average with some errors
	C - Good	70 – 79	Sound work with notable errors
	D - Satisfactory	60 – 69	Fair but with major shortcomings
	E - Sufficient	50 – 59	Work meets minimum criteria
Fail Group	**FX –** Fail	(45-49)	More work required but credit awarded

(0 – 49)	**F –** Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Introduction to Probability and Statistics

Module Information					
Module Title	**Introduction to Probability and Statistics**			**Module Delivery**	
Module Type	**Core**			☒**Theory**	
Module Code	**BCYSCE106-S2**			☒ **Lecture**	
ECTS Credits	**5**			☒ **Lab**	
SWL (hr/sem)	**125**			☐ **Tutorial**	
				☐ **Practical**	
				☒**Seminar**	
Module Level		UGx11 1	**Semester of Delivery**		2
Administering Department		Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul	
Module Leader	Asst. Lecturer Afaf Nasser		**e-mail**	E-mail	
Module Leader's Acad. Title		Lecturer	**Module Leader's Qualification**		MSc
Module Tutor			**e-mail**	Afaf.nasser@ntu.edu.iq	
Peer Reviewer Name			**e-mail**	E-mail	
Scientific Committee Approval Date		25/10/2024	**Version Number**	1.0	

Relation with other Modules			
Prerequisite module	MATHEMATICS (BCYSCE100-S1)	**Semester**	1
Co-requisites module		**Semester**	
Module Aims, Learning Outcomes and Indicative Contents			
Module Objectives	1. Understand the basic concepts: Students should be able to define and understand key concepts in probability, such as events, outcomes, sample space, probability, and random variables.		

	2. Comprehend probability laws: Students should become familiar with the laws and rules of probability. 3. Solve probability problems: Students should be able to solve probability problems using both theoretical calculations and practical applications, such as calculating probabilities of events, determining expected values, and understanding the law of large numbers. 4. Understand independence and dependence: Students should learn the concepts of independence and dependence between events and random variables, and how they affect probability calculations.
Module Learning Outcomes	7. Understand the basic concepts and terminology used in probability and statistics. 8. Comprehend the fundamental principles of probability theory, including probability axioms, random variables, and probability distributions. 9. Analyze and interpret data using descriptive statistics, including measures of central tendency (mean, median, mode) and variability (variance, standard deviation). 10. Understand the concept of sampling and its importance in statistical inference. 11. Apply basic regression analysis techniques to examine relationships between variables. 12. Understand the limitations and assumptions associated with various statistical methods. 13. Use statistical software or programming languages to analyze and visualize data.

Learning and Teaching Strategies	
Strategies	1. Understanding the problem: Begin by reading and understanding the problem statement carefully and identifying key information, variables, and what is required. 2. Define the problem in probabilistic terms: Determine how the problem can be translated into a probabilistic framework. 3. Use appropriate probability models: Determine the appropriate probability model or distribution that best represents the problem at hand. 4. Break down complex problems: If a problem seems complex, it should be broken down into smaller, easier-to-handle parts.

Student Workload (SWL)			
Structured SWL (h/sem)	64	**Structured SWL (h/w)**	4
Unstructured SWL (h/sem)	61	**Unstructured SWL (h/w)**	4
Total SWL (h/sem)	**125**		

Module Evaluation

As		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	Quizzes	3	10% (10)	5 ,8 and 10	LO #1, #2 and #10, #11
	Assignments	5	10% (10)	2,4,8,9,10	LO #3, #4 and #6, #7
	Projects / Lab.	15	10% (10)	Continuous	All
	Report	1	5% (5)	13	LO #5, #8 and #10
	Seminar	1	5% (5)	10	LO #7, #9 and #13
Summative assessment	Midterm Exam	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

Week	Material Covered
Week 1	**Introduction to Statistics** • An overview of the role of statistics in science. • types of statistics (descriptive and inferential).
Week 2	**Introduction to Statistics** • data presentation. • (arithmetical mean, median, mode).
Week 3	**Introduction to Statistics** • exploring Univariate Data, types of data. • mean and median, standard Deviation and Variance.
Week 4	**Introduction to Statistics** • range, IQR and Finding Outliers. • graphs and Describing Distributions. • Overview of software security and defense practices
Week 5	**Introduction to Probability** • Introduction to Probability. • Counting Techniques. • combinations and Permutations
Week 6	**Introduction to Probability** • sets and Venn Diagrams. • basic probability models. • general probability rules.
Week 7	**probabilistic models** • Introduction to discrete distributions. • random variables. • binomial distributions.
Week 8	**probabilistic models** • geometric distributions. • continuous distributions.

	• density curves.
Week 9	**probabilistic models** • Introduction to Suricata. • Installation and configuration of Suricata. • Rulesets, and signatures. • Understanding the rules and rule management
Week 10	**Normal Distribution** • Introduction to normal distribution. • Standard Normal Calculations. • density curves. • bivariate data.
Week 11	**Axioms of probability** • Scatter plots, the least squares regression line, residuals, nonlinear models. • relations in categorical data, Samples and experiments: sampling, designing experiments. • simulating experiments, estimation: margins of error and estimates.
Week 12	**Confidence Interval** • confidence interval for a proportion, confidence interval for the difference of two proportions. • confidence interval for a mean, confidence interval for the difference of two means.
Week 13	**Axioms of probability** • Tests of significance, inference for the mean of a population. • sample proportions. • inference for a population proportion.
Week 14	**Comparing Two Means, comparing two proportions, goodness of fit test and two-way tables, inference for regression, confidence intervals, test for slope of regression lines.**
Week 15	**Review**
Week 16	**Final Exam**

Delivery Plan (Weekly Lab. Syllabus)	
Week	**Material Covered**
Week 1	Lab 1: Introduction to R
Week 2	Lab 2: Data structures in R programming (Vectors, Matrices, Array)
Week 3	Lab 3: Data structures in R programming (Lists, Data Frame, Factor)
Week 4	Lab 4: Data type
Week 5	Lab 5: R-decision making, R-loops, loop control statements
Week 6	Lab 6: Functions in R.
Week 7	Lab 7: R-Operators (Arithmetic operators, Relational operators, Logical operators, Assignment Operator
Week 8	Lab 8: Graphics

Week 9	Lab 9: Importing and Exporting Data.
Week 10	Lab 10: Distribution types
Week 11	Lab 11: Package Building
Week 12	Lab 12: Advanced package Building
Week 13	Lab 13: Data Manipulation
Week 14	Lab 1٤: Data Transformation
Week 15	Lab 1٥: Review and presentation
Week 16	Final Exam

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Freund, J. E. (2012). *Introduction to probability*. Courier Corporation.	Yes
Recommended Texts	Pishro-Nik, H. (2016). Introduction to probability, statistics, and random processes.	Yes
Websites		

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Object Oriented Programming

Module Information		
Module Title	**Object Oriented Programming**	**Module Delivery**
Module Type	**Core**	☒ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial**
Module Code	**BCYSCE107-S2**	
ECTS Credits	**7**	

SWL (hr/sem)	**175**	☐ **Practical** ☒ **Seminar**	
Module Level	1	**Semester of Delivery**	2
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Zakaria Noor Aldeen Mahmood	**e-mail**	E-mail
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	Ph.D.
Module Tutor		**e-mail**	zakaria@ntu.edu.iq
Peer Reviewer Name		**e-mail**	
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules

Prerequisite module	Fundamentals of Programming (BCYSCE102-S1)	**Semester**	1
Co-requisites module		**Semester**	

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	1. Introduction to OOP and its application. 2. OOP vs Procedure Oriented Programming. 3. Starts from building Classes and member function to advance implementation of OOP programing. 4. Improving the skills of the students through several OOP program implementation and code writing. 5. The students should be able to Identify the OOP uses and purpose of using classes and derived classes, inheritance and polymorphism & the required code lines to perform the needed works 6. as well as qualifying him to use the different kinds of programming style and program functions in building & executing the projects of cyber security engineering.
Module Learning Outcomes	1. Understanding the fundamentals of OOP programming. 2. Mastering OOP programming tools and techniques, including common class inheritance techniques such as multi-level inheritance. 3. Becoming familiar with the OOP concepts such as abstraction, constructor, destructor, *this* pointer and virtual function.

	4. Being competent in common file Input/output with Streams techniques, such as File Stream Class Hierarchy, Opening and Closing files, Read/Write from File. 5. Being able to perform Templates: Function Template, Overloading Function Template, Overloading with Functions. 6. Being able to write Exception Handling: Error Handling, Exception Handling Constructs (try, catch, throw).

Learning and Teaching Strategies	
Strategies	The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)			
Structured SWL (h/sem)	79	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	96	**Unstructured SWL (h/w)**	6
Total SWL (h/sem)	**175**		

Module Evaluation				
		Time/Number	**Weight (Marks)**	**Week Due**
Formative assessment	**Quizzes**	4	10% (10)	3,6,9,12
	Assignments	8	5% (5)	Every other week
	Projects / Lab.	14	10% (10)	Continuous
	Report	2	5% (5)	7, 14
	Seminar	1	10% (10)	15
	Midterm Exam	2hr	10% (10)	7

Summative assessment	**Final Exam**	3hr	50% (50)	15
Total assessment			100% (100 Marks)	

OBJECT ORIENTED PROGRAMMING - PROGRAMME COURSE DESCRIPTION

Code BCYSCE 107-S2	Name of the Course Unit	Semester	In-Class Hours (T+P)	Credit	ECTS Credit
	Object Oriented Programming	2	2+3	4	7

GENERAL INFORMATION	
Language of Instruction :	English
Level of the Course Unit :	BACHELOR'S DEGREE
Type of the Course :	Compulsory
Mode of Delivery of the Course Unit	Face to Face
Coordinator of the Course Unit	Dr. Zakaria Noor Aldeen Mahmood
Instructor(s) of the Course Unit	Dr. Zakaria Noor Aldeen Mahmood

OBJECTIVES AND CONTENTS	
Objectives of the Course Unit:	Introducing the fundamentals and principles of OOP programming in C++ language. Starts from building Classes and member function to advance implementation of OOP programing. Improving the skills of the students through several OOP program implementation and code writing. The students should be able to

OBJECTIVES AND CONTENTS	
	Identify the OOP uses and purpose of using classes and derived classes, inheritance and polymorphism & the required code lines to perform the needed works as well as qualifying him to use the different kinds of programming style and program functions in building & executing the projects of cyber security engineering.
Contents of the Course Unit:	OOP programing OOP concepts Inheritance types and implementation Runtime Polymorphism Compile-time Polymorphism File Input/output Exception Handling

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	• Issues with Procedure Oriented Programming
2	• Basic of Object-Oriented Programming (OOP)
3	Procedure Oriented versus Object Oriented Programming
4	Concept of Object-Oriented Programming: Object, Class, Abstraction, Encapsulation, Inheritance, Polymorphism
5	Objects and Classes: C++ Classes, Access Specifiers, Objects and the Member Access, Defining Member Function, Constructor: Default Constructor, Parameterized Constructor, Copy Constructor
6	Destructors, Object as Function Arguments and Return Type, Array of Objects, Pointer to Objects and Member Access, Dynamic Memory Allocation for Objects and Object Array.
7	this Pointer static Data Member and static Function, Constant Member Functions and Constant Objects, Friend Function and Friend Classes
8	Operator Overloading, Overloadable Operators, Syntax of Operator Overloading, Rules of Operator Overloading, Unary Operator Overloading, Binary Operator Overloading, Operator Overloading with Member and Non-Member Functions, Data Conversion: Basic – User Defined and User Defined – User Defined, Explicit Constructors
9	Inheritance: Base and Derived Class, protected Access Specifier, Derived Class Declaration, Member Function Overriding, Forms of Inheritance: single, multiple, multilevel, hierarchical, hybrid, multipath, Multipath Inheritance and Virtual Base Class, Constructor Invocation in Single and Multiple Inheritances, Destructor in Single and Multiple Inheritances
10	Polymorphism and Dynamic Binding: Need of Virtual Function, Pointer to Derived Class, Definition of Virtual Functions, Array of Pointers to Base Class, Pure Virtual functions and

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
	Abstract Class, Virtual Destructor, reinterpret cast Operator, Run-Time Type Information, dynamic cast Operator, typed Operator
11	Stream Computation for Console and File Input /Output : Stream Class Hierarchy for Console Input /Output, Testing Stream Errors, Unformatted Input /Output, Formatted Input /Output with iOS Member functions and Flags, Formatting with Manipulators, Stream Operator Overloading
12	File Input/output with Streams, File Stream Class Hierarchy, Opening and Closing files, Read/Write from File, File Access Pointers and their Manipulators, Sequential and Random Access to File, Testing Errors during File Operations
13	Templates: Function Template, Overloading Function Template, Overloading with Functions, Overloading with other Template, Class Template, Function Definition of Class Template, On-Template Type, Arguments, Default Arguments with Class Template, Derived Class Template, Introduction to Standard Template Library, Containers, Algorithms, Iterators
14	Exception Handling: Error Handling, Exception Handling Constructs (try, catch, throw), Advantage over Conventional Error Handling, Multiple Exception Handling, Rethrowing Exception, Catching All Exceptions, Exception with Arguments, Exceptions Specification for Function, Handling Uncaught and Unexpected Exceptions.
15	Review/ preparation for final exam
16	Final Exam

Delivery Plan (Weekly Lab. Syllabus)	
	Material Covered
Week 1	Lab 1: Getting started - Object-Oriented Programming.
Week 2	Lab 2: Object, Class, Abstraction, Encapsulation, Inheritance, Polymorphism - Examples and Problems
Week 3	Lab 3: Destructors - Examples and Problems.

Week 4	Lab 4: Virtual Destructor
Week 5	Lab 5：Operator Overloading - Examples and Problems.
Week 6	Lab 6: Inheritance - Examples and Problems.
Week 7	Lab 7: Polymorphism and Dynamic Binding - Examples and Problems.
Week 8	Lab 8: Stream Computation for Console and File Input /Output - Examples and Problems.
Week 9	Lab 9: Templates - Examples and Problems.
Week 10	Lab 10: Exception Handling - Examples and Problems.
Week 11	Lab 11: Debugging - Examples and Problems.
Week 12	Lab 12: Containers, Algorithms, Iterators - Examples and Problems.
Week 13	Lab 13. Conventional Error Handling - Examples and Problems
Week 14	Lab 14: Dynamic Memory - Examples and Problems.
Week 15	Lab 15: review/preparation for final exam
Week 16	**Final Exam**

WORKLOAD & ECTS CREDITS OF THE COURSE UNIT Object Oriented Programming			
Workload for Learning & Teaching Activities			
Type of the Learning Activates	**Learning Activities (# of week)**	**Duration (hours, h)**	**Workload (h)**
Lecture & In-Class Activities	15	2	30
Preliminary & Further Study	NA	NA	NA
Land Surveying	NA	NA	NA
Group Work	NA	NA	NA
Laboratory	15	3	45
Reading	6	1	6
Assignment (Homework)	8	2	16
Project Work	NA	NA	NA
Seminar	1	1	1
Internship	NA	NA	NA
Technical Visit	NA	NA	NA
Web Based Learning	6	2	12
Implementation/Application/Practice	NA	NA	NA
Practice at a workplace	NA	NA	NA
Occupational Activity	NA	NA	NA
Social Activity	NA	NA	NA
Thesis Work	NA	NA	NA
Field Study	NA	NA	NA
Report Writing	2	2	4
Final Exam -Theory	1	3	3
Final Exam - Practical	1	1	1
Preparation for the Final Exam- Theory	1	20	20
Preparation for the Final Exam -Practical	1	15	15
Mid-Term Exam - Theory	1	2	2
Mid-Term Exam - Practical	1	1	1
Preparation for the Mid-Term Exam	1	15	15
Short Exam (Quizzes)	4	0.5	2
Preparation for the Short Exam	4	2	8

			175

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	1. **Choudhary, H. (2013). C++ Programming-Final Golden Edition. Beginners To Experts Approach Guide-With Easy Learning & Problem Analysis to Program Design & Development.**	no
Recommended Texts	2. **Farrell, J. (2008). Object-oriented programming using C++. Cengage Learning.** 3. **Object-Oriented Programming in C++, Fourth Edition.**	no
Websites	4. https://www.geeksforgeeks.org/object-oriented-programming-in-cpp/ 5. https://www.w3schools.com/cpp	

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Digital Electronics

Module Information		
Module Title	**Digital Electronics**	**Module Delivery**
Module Type	**Core**	☒ **Theory**
Module Code	**BCYSCE101-S2**	

ECTS Credits	**7**		☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
SWL (hr/sem)	**175**			
Module Level		**Semester of Delivery**	2	
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul	
Module Leader	Lubab H.Samy	**e-mail**	E-mail	
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**		
Module Tutor		**e-mail**	Lubab_harith @ntu.edu.iq	
Peer Reviewer Name		**e-mail**		
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0	

Relation with other Modules

Prerequisite module		**Semester**	
Co-requisites module	Computer Electronics BCYSCE200-S1 Computer Organization and Architectures BCYSCE204-S2	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	1. Understanding the principles of digital electronics: This includes understanding the properties of digital signals, logic gates, Boolean algebra, and other fundamental concepts. 2. Designing digital circuits: This involves designing and analyzing digital circuits using various tools and techniques such as truth tables, Karnaugh maps, and circuit simulation software. 3. Implementing digital circuits: This includes building digital circuits using electronic components such as logic gates, flip-flops, and counters. 4. Troubleshooting digital circuits: This involves identifying and diagnosing problems in digital circuits using various diagnostic tools and techniques. 5. Understanding digital systems: This includes understanding how digital circuits are combined to create digital systems such as computers, microcontrollers, and other digital devices. 6. Applying digital electronics to real-world problems: This involves using digital electronics to solve real-world problems such as designing control systems, communication systems, and data processing systems.
Module Learning Outcomes	1.Students should be able to describe the basics of digital electronics, including binary arithmetic, logic gates, Boolean algebra, and digital circuits. 2. Analyzing and designing digital circuits: Students should be able to analyze and design combinational and sequential digital circuits using various tools and techniques, including truth tables, Karnaugh maps, and state diagrams. 3. Understanding the operation of digital devices: Students should be able to explain the operation of digital devices such as flip-flops, counters, registers, and memory devices. 4. Applying digital electronics to real-world problems: Students should be able to apply their knowledge of digital electronics to solve real-world problems, such as designing a digital system to control a traffic light or implementing a digital filter for audio signal processing. 5. Understanding the limitations of digital electronics: Students should be able to identify the limitations of digital electronics, such as timing constraints, noise, and power consumption, and suggest appropriate solutions. .

Learning and Teaching Strategies

Strategies	1-Boolean Algebra: This is a mathematical system that allows digital signals to be represented and manipulated using a set of logical operations such as AND, OR, and NOT. Boolean algebra can be used to simplify complex digital circuits and to derive expressions for the output of a circuit. 2-Karnaugh Maps: Karnaugh maps are graphical tools that can be used to simplify Boolean expressions and to derive the minimal sum of products (MSP) or product of sums (POS) expressions for a digital circuit. 3-Combinational Logic Design: Combinational logic circuits are digital circuits whose outputs depend only on the current input values. Strategies for designing combinational logic circuits include Boolean algebra, Karnaugh maps, and the use of standard logic gates. 4-Sequential Logic Design: Sequential logic circuits are digital circuits whose outputs depend on both the current input values and the previous state of the circuit. Strategies for 5-designing sequential logic circuits include state diagrams, state tables, and the use of flip-flops and registers.

Student Workload (SWL)

Structured SWL (h/sem)	79	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	96	**Unstructured SWL (h/w)**	6
Total SWL (h/sem)	**175**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due
Formative assessment	**Quizzes**	6	10% (10)	3,5,7,9,10,13
	Assignments	10	10% (5)	2 ,4,5,6,7,8,9,10,11,13
	Projects / Lab.	15	10% (5)	Continuous
	Report	15	10% (5)	Continuous
Summative assessment	**Midterm Exam**	2hr	10% (10)	7
	Final Exam	3hr	50% (50)	15

Total assessment	100% (100 Marks)	

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	• Introduction to system numbers and Logic Law • Logic gates AND, OR, NOT, NAND • Logic gates NOR, XOR, XNOR.
2	• logic simplification using Boolean functions • logic simplification using DE Morgan's theorem
3	• Karnaugh maps definition: Karnaugh maps of 2-variables and 3-variables • Karnaugh maps of 4-variables and 5-variables
4	• Sum of Product (SOP) definition: logic circuit design using SOP • Product of Sum (POS) definition: logic circuit design using POS
5	• Adder digital circuit design and Application with examples, parallel binary adder and Application with examples • Parallel binary adder circuit design and Application with examples • Subtracter digital circuit design and Application with examples
6	• Multiplier digital circuit design and Application with examples • Divider digital circuit design and Application with examples
7	• Decoder definition and Types: Decoder digital circuit design and Application with examples • Encoder definition and Types: Encoder digital circuit design and Application with examples
8	• Multiplexer definition and Types, Multiplexer digital circuit design and Application with examples • Demultiplexer definition and Types: Demultiplexer digital circuit design and Application with examples.
9	• Comparator definition and Types: Comparator digital circuit design and Application with examples • Code conversion definition and Types: Code conversion digital circuit design and Application with examples
10	• Flip-flops definition and Types: Flip-flops digital circuit design and Application with examples. (SR latch, D latch)-Edge triggered and conversion from one type to another)

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
	• Flip-flops definition and Types: Flip-flops digital circuit design and Application with examples. (T-latch, and J-K F.F)-Edge triggered and conversion from one type to another)
11	• Counters (asynchronous, synchronous, decade, up/down, cascade, counter decoding)
12	• Asynchronous Counters Design and Application • Synchronous Counters Design and Application
13	• Shift-registers: serial in and serial out registers Design and Application • Shift-registers: serial in and parallel out Design and Application.
14	• Timer: Definition, 555 Timer Design and Application
15	**review**
16	**Final Exam**

Delivery Plan (Weekly Lab. Syllabus)	
Week 1	**Lab 1:** Connect different logic gates AND, OR, NOT, NAND, NOR
Week 2	**Lab 2: EX-OR gate and EX-NOR gates, Design AND & OR and NOT gates by using NAND and NOR gates.**
Week 3	**Lab3: De-Morgan's theorems.**
Week 4	**Lab 4: Designing a combinational logic circuit (SOP) and (POS), The realization of the Boolean equation.**
Week 5	**Lab 5: Half binary Adder.**
Week 6	**Lab 6: Full binary Adder.**
Week 7	**Lab 7: Half binary subtractor.**
Week 8	**Lab 8: Full binary subtractor ,2'S complement Adder-subtractor**
Week 9	**Lab 9: Design Binary comparator.**
Week 10	**Lab 10: Decoders digital circuit.**
Week 11	**Lab 11: Encoders digital circuit.**
Week 12	**Lab 12: Digital Multiplexer.**
Week 13	**Lab 13: Demultiplexer digital circuit.**

Week 14	**Lab 14: J-K flip flop.**
Week 15	**review**
Week 16	**Final Exam**

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Digital Fundamentals ELEVENTH EDITION Thomas L. Floyd	Yes
Recommended Texts	"Digital Design" by M. Morris Mano and Michael Ciletti Fundamentals of Digital Logic and Microcontrollers" by M. Rafiquzzaman	yes
Websites		

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Introduction to Sociology

Module Information		
Module Title	**Introduction to Sociology**	**Module Delivery**

Module Type	**Core**	☐ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**
Module Code	**BCYSCE 108-S2**	
ECTS Credits	**4**	
SWL (hr/sem)	**100**	

Module Level	1	**Semester of Delivery**	1
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Name	**e-mail**	E-mail
Module Leader's Acad. Title	Professor	**Module Leader's Qualification**	Ph.D.
Module Tutor	Name (if available)	**e-mail**	E-mail
Peer Reviewer Name	Name	**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

79	96

Relation with other Modules

Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	19. Examining legal and regulatory requirements, ethical issues, and the development of cybersecurity policy for commercial and government organizations. 20. Introduce students to the field of sociology and its central theoretical perspectives from Cybersecurity perspective. Provide students with basic ideas and knowledge in the science of sociology. 21. Help students understand the similarities and differences between different sociological paradigms. 22. provide students with basic ideas and knowledge in the science of sociology and how cybersecurity issues effects society.

	23. Introduce student to terminology related to cybersecurity such as Cybercrime and deviance, Globalization. 24. Explore the development of organizational cybersecurity policy that meets an organization's compliance requirements and business goals.
Module Learning Outcomes	10. Describe the fundamental concepts and principles of cybersecurity. Students should be able to explain the basic terminology, models, and frameworks used in cybersecurity, such as confidentiality, integrity, availability, risk management, and threat modeling. 11. Identify common cybersecurity threats and attacks. Students should be able to recognize the most common types of cyber threats and attacks, such as malware, phishing, social engineering, and denial-of-service, and understand their impact on individuals, organizations, and society. 12. Apply cybersecurity best practices and tools. Students should be able to apply basic cybersecurity best practices and tools to protect their own devices and data, such as strong passwords, encryption, firewalls, and antivirus software. 13. Analyze cybersecurity incidents and breaches. Students should be able to analyze real-world cybersecurity incidents and breaches, such as data breaches, ransomware attacks, and cyber espionage, and understand their causes, consequences, and mitigation strategies. 14. Evaluate ethical and legal issues in cybersecurity. Students should be able to evaluate ethical and legal issues related to cybersecurity, such as privacy, surveillance, intellectual property, and cybercrime, and understand their implications for individuals, organizations, and society. 15.
Indicative Contents	Indicative content includes the following. Introduction to Cybersecurity (4 HOURS) Cybersecurity Fundamentals (6HOURS) Cybersecurity Operations (4 HOURS) Cybersecurity Ethics and Law (4 HOURS) Incident Response and Recovery. (4 HOURS) Threat Analysis Mode . (4 HOURS) Introduction to Security Policy (4 HOURS) Disaster Recovery and Business Continuity (4 HOURS) Security policy management and maintenance (4 HOURS)

Learning and Teaching Strategies

Strategies	Type something like: The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)

Structured SWL (h/sem)	79	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	96	**Unstructured SWL (h/w)**	6
Total SWL (h/sem)	**175**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	3	10% (10)	5, 8, and 10	LO #1, #2, #5 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

KEY LEA

RNING OUTCOMES OF THE COURSE UNIT

	Material Covered
Week 1	1. **Introduction to Cybersecurity** • Definition of cybersecurity • Importance of cybersecurity • Cybersecurity threats and attacks • Cybersecurity best practices
Week 2	**Introduction to Cybersecurity** • Cybersecurity threats and attacks • Cybersecurity best practices
Week 3	**Cybersecurity Fundamentals** • Security models and frameworks • Risk management
Week 4	**Cybersecurity Fundamentals** • Security policies and procedures • Security controls and countermeasures
Week 5	**Cybersecurity Operations** • Incident response and management • Security monitoring and analysis • Vulnerability assessment and management • Penetration testing and ethical hacking
Week 6	**Cybersecurity Ethics and Law** • Ethical and legal issues in cybersecurity • Cybercrime and cyber law
Week 7	**Cybersecurity Ethics and Law** • Cybersecurity regulations and standards • Cybersecurity career paths and opportunities
Week 8	**Incident Response and Recovery.** • Incident Response and Recovery • Incident response planning
Week 9	**Incident Response and Recovery** • Incident detection and analysis • Incident containment and eradication
Week 10	**Incident Response and Recovery** • Business continuity and disaster recovery
Week 11	**Threat Analysis Mode** • , Categorization of threats. • Analysis of threats.
Week 12	**Introduction to Security Policy** • Overview of security policy development and implementation • Why security policy is important.

	• Risk assessment and analysis • Hands-on exercises in developing security policies
Week 13	**Disaster Recovery and Business Continuity**
	Security Policy Implementation • Best practices for implementing security policies. • Developing and implementing security protocols. • Incident response planning. • Hands-on exercises in implementing security policies.
Week 14	**Security policy management and maintenance** • Security policy auditing and compliance • Security policy training and awareness
Week 15	**Review and Presentation**
Week 16	**Preparatory week before the final Exam**

Delivery Plan (Weekly Lab. Syllabus)

	Material Covered
Week 1	Lab 1: Network Security Monitoring Software
Week 2	Lab 2: Vulnerability Assessment Software
Week 3	Lab 3: Packet Sniffer Software
Week 4	Lab 4: Encryption Tools
Week 5	Lab 5: Web Vulnerability Scanning Tools
Week 6	Lab 6: Penetration Testing Tools
Week 7	Lab 7: Antivirus Software
Week 8	Lab 8: Network Intrusion Detection Tools
Week 9	Lab 9: Keylogger Software
Week 10	Lab 10: Threat Intelligence Enrichment Tools
Week 11	Lab 11: Threat Identification in the Network
Week 12	Lab 12: Packet Sniffing Tools
Week 13	Lab 13: Network Security Monitoring Software
Week 14	Lab 14: Vulnerability Assessment Software
Week 15	Review and Students presentation
Week 16	Final Exam

Learning and Teaching Resources

	Text	**Available in the Library?**
Required Texts	Introduction to Computer Networks and Cybersecurity by Chwan-Hwa (John) Wu and J. David Irwin, 2013	Yes

Recommended Texts	1. Guide to Cyber Security for Beginners 2. Cybersecurity Essentials by Charles J. Brooks and Christopher Grow	No
Websites		

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Human rights and Democracy

Module Information			
Module Title	**Human rights and Democracy**	**Module Delivery**	
Module Type	Suplement	✓ **Theory** ✓ **Lecture** **Lab** **Tutorial** **Practical** ✓ **Seminar**	
Module Code	BCYSCE109-S2		
ECTS Credits	4		
SWL (hr/sem)	100		
Module Level	UGx11 1	**Semester of Delivery**	2
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	**Dr. Eesha I. Mohammed**	**e-mail**	aysha.ibrahim@ntu.edu.iq
Module Leader's Acad. Title	Assist Prof.	**Module Leader's Qualification**	PHD

Module Tutor	None	**e-mail**	None
Peer Reviewer Name	None	**e-mail**	None
Review Committee Approval	25/10/2024	**Version Number**	1.0

Relation With Other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	Democracy and human rights aim to preserve and promote the dignity of the individual and his fundamental rights, achieve social justice, encourage the economic and social development and cohesion of society, consolidate national security and establish a climate conducive to international peace, because human rights and democracy are an essential reference for all to protect human rights; Today, some time after democracy was achieved around the world, many democracies seem to be in decline. Some governments appear to be deliberately weakening independent checks of their powers, eliminating any criticism, dismantling democratic oversight and ensuring its long-term governance, with a negative impact on people's rights.
Module Learning Outcomes	1- Understand, know and realize his rights that God has approved for him and for all human beings, and therefore they are a gift and not a gain from anyone and no one has the right to take them away. ٢- The student expresses these rights in his own way and defends them. ٣- Explaining the phenomena and giving explanations for the violation of human rights and freedoms by identifying the deficiencies or gaps in the light of the information available to him ٤- Understanding the most important political systems, which are a guarantee of human rights and political freedoms, and trying to apply them on the ground, which is the democratic system.
Indicative Contents	❖ Human Rights in Contemporary and Modern History: International Recognition of Human Rights since World War I and the League of Nations (4 hours) ❖ Human rights, definition, objectives and human rights in ancient civilizations, especially the civilization of Mesopotamia (6 hours) ❖ International guarantees, respect for and protection of human rights: ❖ - Role of the United Nations and its specialized agencies in providing safeguards ❖ - Role of regional organizations (Arab League, European Union, African Union, Organization of American States, ASEAN) ❖ The role of international, regional non-governmental organizations and public opinion in respecting and protecting human rights (12 hours) ❖ Problems, obstacles and student discussions (6 hours)

Learning and Teaching Strategies	
Strategies	1-Thinking strategy according to the student's ability ٢- High thinking skill strategy ٣- Critical Thinking Strategy in Learning ٤- Brainstorming

Student Workload (SWL)			
Structured SWL (h/sem)	33	**Structured SWL (h/w)**	2
Unstructured SWL (h/sem)	67	**Unstructured SWL (h/w)**	4
Total SWL (h/sem)	100		

Module Evaluation					
As		**Time/Number**	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	4	10% (10)	5, 10	LO #1, 2, 10 and 11
	Assignments	·	0	Continuous	All
	Projects / Lab.	0	0		
	Report	4	10% (10)		
Summative assessment	**Midterm Exam**	2 hr	20% (20)	7	LO # 1-7
	Final Exam	3 hr	60% (60)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)	
Week	**Material Covered**
Week 1	Human rights, definition, objectives Human rights in ancient civilizations, especially the civilization of Mesopotamia
Week 2	Human rights in heavenly laws with a focus on human rights in Islam. Discussing whether heavenly laws can be protection and follow-up of cybersecurity and its effects on humans
Week 3	Human Rights in Contemporary and Modern History: International Recognition of Human Rights Since World War I and the League of Nations
Week 4	Regional recognition of human rights: European Convention on Human Rights 1950, American Convention on Human Rights 1969, African Charter of Human Rights 1981, Arab Charter on Human Rights 1994
Week 5	Human Rights in Contemporary and Modern History: International Recognition of Human Rights Since World War I and the League of Nations
Week 6	Human rights in Iraqi constitutions between theory and reality Iraqi human rights in cyberspace
Week 7	Economic, social and cultural human rights and civil and political human rights. Cybersecurity Impact on These Rights
Week 8	Modern human rights: facts in development, the right to a clean environment, the right to solidarity, the right to religion
Week 9	Guarantees of respect and protection of human rights at the national level, guarantees in the Constitution and laws

	Guarantees in constitutional oversight, guarantees in freedom of the press and public opinion, the role of non-governmental organizations in respecting and protecting human rights. Constitutional guarantees related to cybersecurity and their impact on the individual and society
Week 10	Guarantees, respect and protection of human rights at the international level: - Role of the United Nations and its specialized agencies in providing safeguards - The role of regional organizations (Arab League, European Union, African Union, Organization of American States, ASEAN) The role of international, regional non-governmental organizations and public opinion in respecting and protecting human rights The role of international and regional non-governmental organizations in national and global cybersecurity Human Safeguards, Rights and Protection in Cyberspace
Week 11	The term democracy, its origin, its significance, the history of democracy. The relationship of democracy with cybersecurity and its impact on cybersecurity
Week 12	Islam - democracy and the disadvantages of authoritarian rule.
Week 13	Criticisms of democracy, and the merits of the democratic system.
Week 14	Democracies in the world/Democracies in the Third World/Problems Facing Arab Countries in Democratic Transition
Week 15	**Review and presentations**
Week 16	**Final Exam**

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Human Rights and Democracy - Concepts and Foundations of Dr. Samah Mahdi Al-Alawi and Dr. Salman Kazem Al-Bahadli	Yes
Recommended Texts	Democracy and Human Rights in Islam by Dr. Rashid Ghannouchi	No
Websites	https://www.neelwafurat.com https://studies.aljazeera.ne	

GRADING SCHEME				
Group	**Grade**	**Marks (%)**	**Definition**	
Success Group (50 - 100)	**A –** Excellent	90 - 100	Outstanding Performance	
	B - Very Good	80 - 89	Above average with some errors	
	C – Good	70 - 79	Sound work with notable errors	
	D - Satisfactory	60 - 69	Fair but with major shortcomings	
	E – Sufficient	50 - 59	Work meets minimum criteria	
Fail Group	**FX –** Fail	(45-49)	More work required but credit awarded	

(0 – 49)	**F –** Fail	(0-44)		Considerable amount of work required	
Note:					
NB Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.					

Database System

Module Information					
Module Title	**Database System**			**Module Delivery**	
Module Type	**Core**			☒ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**BCYSCE202-S1**				
ECTS Credits	**5**				
SWL (hr/sem)	**125**				
Module Level		UGx11 ٢	**Semester of Delivery**		3
Administering Department		Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul	
Module Leader	Dr. Zakaria Noor Aldeen Mahmood		**e-mail**	E-mail	
Module Leader's Acad. Title		Lecturer	**Module Leader's Qualification**		Ph.D.
Module Tutor			**e-mail**	zakaria@ntu.edu.iq	
Peer Reviewer Name			**e-mail**		
Scientific Committee Approval Date		25/10/2024	**Version Number**	1.0	

Relation with other Modules			
Prerequisite module		**Semester**	
Co-requisites module	Database Security (BCYSCE202-S2)	**Semester**	2

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives أهداف المادة الدراسية	1. To learn the fundamental concepts of database systems. 2. To learn data models (ER, relational, and others); query languages (relational algebra, SQL, and others). 3. To learn implementation techniques of database management systems 4. The students should be able to understand the uses and purpose of using Database application and database settings, send and retrieve important information and data through SQL queries. 5. Help the students perform the needed cyber security database works as well as qualifying him to use the different kinds of database tools and instructions to build & execute the projects of cyber security engineering.
Module Learning Outcomes	14. Understanding the fundamentals of database system. 15. Mastering SQL Queried and commands, including common input/output application and data manipulation. 16. Becoming familiar with the Linux operating system and its distributions. 17. Being competent in common Networking & Configuring Network Settings and Package Management. 18. Being able to perform Bash Scripting and Execute shell command. 19. Being able to write complete shell scripts to perform I/O Manipulation and I/O Redirections

Learning and Teaching Strategies	
Strategies	The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes,

	interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)			
Structured SWL (h/sem)	78	Structured SWL (h/w)	٥
Unstructured SWL (h/sem)	47	Unstructured SWL (h/w)	3
Total SWL (h/sem)	125		

Module Evaluation				
As		Time/Number	Weight (Marks)	Week Due
Formative assessment	Quizzes	2	10% (10)	6, ١٤
	Assignments	1	10% (10)	14
	Projects / Lab.	1٤	10% (10)	Continuous
	Report	1	10% (10)	10
Summative assessment	Midterm Exam	2hr	10% (10)	7
	Final Exam	3hr	50% (50)	15
Total assessment			100% (100 Marks)	

Code BCYSCE202-S1	Name of the Course Unit	Semester	In-Class Hours (T+P)	Credit	ECTS Credit
	Database System	1	2+2		5

GENERAL INFORMATION	
Language of Instruction :	English
Level of the Course Unit :	BACHELOR'S DEGREE
Type of the Course :	Compulsory
Mode of Delivery of the Course Unit	Face to Face
Coordinator of the Course Unit	Dr. Zakaria Noor Aldeen Mahmood

Instructor(s) of the Course Unit	Dr. Zakaria Noor Aldeen Mahmood

OBJECTIVES AND CONTENTS	
Objectives of the Course Unit:	Introducing the fundamentals and principles of database system using SQL. starts from scratch to database building and applications. Improving the skills of the students through several Database implementations and queries writing. The students should be able to understand the uses and purpose of using SQL Queries through sending and receiving information. Help the students perform the needed cyber security works as well as qualifying him to use the different kinds of Database style and instructions to build & execute the projects of cyber security engineering.
Contents of the Course Unit:	• Introduction to the Relational Model • SQL Language • Formal Relational Query Languages • Database and Relational Database Design • Application Design

	• Storage and File Structure • Indexing and Hashing • Query Processing & Optimization • Transactions & Concurrency Control • Recovery System & Database System Architectures.

DATABASE SYSTEM - PROGRAMME COURSE DESCRIPTION

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	Introduction to the Relational Model: Introduce class and overview of course topics
2	SQL Language: Introduction to SQL; Intermediate SQL, Advanced SQL
3	Formal Relational Query Languages: Relational Algebra; Tuple Relational Calculus; Domain Relational Calculus
4	Database Design: The Entity-Relationship Approach; ER Design; Reduction to Relational Model
5	Relational Database Design: Functional Dependency; Multivalued Dependency; Normal Forms
6	Application Design: Web Architectures
7	Storage and File Structure: Physical Storage; Record Organization
8	Indexing and Hashing; Ordered Indices; Hashed Indices
9	Indexing and Hashing; Bitmap Indices
10	Query Processing & Optimization: Query Processing
11	Query Processing & Optimization: Query Optimization
12	Transactions & Concurrency Control: ACID Properties; Transaction Management
13	Recovery System & Database System Architectures: Locks; Deadlocks; Snapshot Isolation
14	Student Presentations: Presentations and reviews
15	Review/preparation for final exam
16	Final Exam

Delivery Plan (Weekly Lab. Syllabus)	
Week	**Material Covered**
Week 1	Lab1: Getting started.
Week 2	Lab 2: Introducing Database framework
Week 3	Lab ٣ : Basic of SQL Language- 1
Week 4	Lab 4: Basic of SQL Language -2
Week 5	Lab 5: Basic of SQL Language -3
Week 6	Lab 6: Formal Relational Query Languages
Week 7	Lab 7: Storage and File Structure: Physical Storage
Week 8	Lab 8: Storage and File Structure: Record Organization
Week 9	Lab ٩: Ordered Indices
Week 10	Lab ١٠: Hashed Indices
Week 11	Lab ١١: Locks
Week 12	Lab ١٢: Deadlocks
Week 13	Lab 1٣: Snapshot Isolation
Week 14	Review
Week 15	**Final Exam**

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Beginning SQL Server 2008 Express for Developers From Novice to Professional. By Robin Dewson, 2008	yes
Recommended Texts	Learning SQL Master SQL Fundamentals By Alan Beaulieu · 2009	yes
Websites		

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	8 0 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Discrete Mathematics

Module Information

Module Title	**Discrete Mathematics**	**Module Delivery**	
Module Type	**Core**		☒ **Theory** ☒ **Lecture** ☐**Lab** ☒ **Tutorial** ☐ **Practical** ☐**Seminar**
Module Code	**BCYSCE205-S1**		
ECTS Credits	٤		
SWL (hr/sem)	١٠٠		
Module Level	٢	**Semester of Delivery**	1
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Asst. Lecturer Afaf Nasser	**e-mail**	E-mail
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	MSc
Module Tutor		**e-mail**	Afaf.nasser@ntu.edu.iq
Peer Reviewer Name		**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules

Prerequisite module	Mathematics (BCYSCE100-S1)	**Semester**	١
Co-requisites module		**Semester**	

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	25. Understanding Fundamental Concepts: The primary objective of studying discrete mathematics is to develop a solid understanding of fundamental concepts and structures in discrete mathematics. 26. Developing Problem-Solving Skills: Discrete mathematics aims to cultivate problem-solving skills. 27. Enhancing Mathematical Reasoning: Discrete mathematics promotes the development of mathematical reasoning skills. 28. Applying Mathematics to Real-World Situations: Discrete mathematics aims to enable students to apply mathematical concepts and techniques to real-world problems. 29. Promoting Mathematical Communication: Discrete mathematics aims to improve students' ability to communicate mathematical ideas effectively.
Module Learning Outcomes	1. Problem-Solving Skills: Discrete mathematics helps develop problem-solving skills by exposing students to a wide range of mathematical problems and teaching them techniques to approach and solve them. 2. Logical Reasoning: Discrete mathematics emphasizes logical reasoning and critical thinking. Students learn how to construct logical arguments, analyze logical statements, and use deductive and inductive reasoning to prove mathematical theorems and solve problems. 3. Mathematical Modeling: Discrete mathematics provides a foundation for mathematical modeling, where real-world problems are represented and solved using mathematical structures such as graphs, networks, and algorithms. 4. Algorithmic Thinking: Discrete mathematics introduces students to algorithmic thinking.

Learning and Teaching Strategies

Strategies	1. Mathematical Induction: This strategy is often used to prove statements about sequences, sets, or mathematical structures that have a recursive or inductive nature. 2. Graph Theory: Graph theory is concerned with the study of graphs, which are mathematical structures consisting of vertices (nodes) and edges. 3 Logic and Propositional Calculus: Logic is an essential part of discrete mathematics. 4. Number Theory: Number theory is the study of properties and relationships of integers. 5. Probability Theory: Probability theory deals with the study of random events and uncertainty.

Student Workload (SWL)

Structured SWL (h/sem)	٤٨	**Structured SWL (h/w)**	٣

Unstructured SWL (h/sem)	٥٢	**Unstructured SWL (h/w)**	٣
Total SWL (h/sem)	١٠٠		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	5	10% (10)	2,4,6,8,10	LO #1, #2 and #10, #11
	Assignments	6	10% (10)	1,2,3,4,5,6,	LO #3, #4 and #6, #7
	Reading	4	10% (10)	3,5,8,10	LO #3, #4
	Report	3	10% (10)	2,9,11	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)	
	Material Covered
Week 1	**Introduction to Discrete Mathematics** • Introduction to Discrete Mathematics • Sets and Relations • Functions.
Week 2	**Introduction to Discrete Mathematics** • introduction to Discrete Mathematics: Propositional Logic • Predicate Logic.
Week 3	**Combinatorics** • Counting Principles • Permutations and Combinations.
Week 4	**Combinatorics** • Binomial Coefficients • Inclusion-Exclusion Principle
Week 5	**Graph Theory** • Basic Concepts • Trees
Week 6	**Graph Theory** • Connectivity Cycles • Euler
Week 7	**Graph Theory** • Hamilton Paths • Cycles.
Week 8	**Number Theory** • Divisibility • Modular Arithmetic, Greatest Common Divisor • Least Common Multiple, RSA Cryptography from Math perspective
Week 9	Euclidean algorithm, Chinese remainder theorem.
Week 10	Fermat's little theorem.
Week 11	Discrete Probability, Sample Spaces and Events, Probability Axioms.
Week 12	Conditional Probability, Bayes' Theorem.

Week 13	Algorithms and Complexity, Algorithm Analysis.
Week 14	Big-O Notation: Sorting and Searching Algorithms, NP-Completeness.
Week 15	**Review**

Learning and Teaching Resources

	Text	Available in the Library?
Required Texts	*Discrete Mathematics* by Richard Johnson Baugh., 8thEd.	Yes
Recommended Texts	Rosen, K. H. (2007). *Discrete mathematics and its applications*. The McGraw Hill Companies,.	Yes
Websites		

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Computer Electronics

Module Information					
Module Title	**Computer Electronics**			**Module Delivery**	
Module Type	**Core**			☐ **Theory**	
Module Code	**BCYSCE200-S1**			☒ **Lecture**	
ECTS Credits	**5**			☒ **Lab**	
SWL (hr/sem)	**125**			☐ **Tutorial**	
				☐ **Practical**	
				☒ **Seminar**	
Module Level		UGx11 2	**Semester of Delivery**		1
Administering Department		Cyber Security and Cloud Computing Techniques Engineering	**College**		Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Thabat F. Thabet		**e-mail**		Thabet.tfy@ntu.edu.iq
Module Leader's Acad. Title		Lecturer	**Module Leader's Qualification**		PhD.
Module Tutor	None		**e-mail**		None
Peer Reviewer Name		Name	**e-mail**		None
Scientific Committee Approval Date		25/10/2024	**Version Number**		1.0

Relation with other Modules			
Prerequisite module	Fundamentals of Electrical Engineering(BCYSCE104-S1)	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	30. 1. Understanding the fundamental principles of electronic devices and circuits. 31. Learning about digital electronics and microprocessors. 32. Developing skills in circuit design and analysis. 33. Learning about the practical applications of computer electronics. Overall, the objectives of a module in computer electronics are to provide students with a foundational knowledge of electronic devices and systems, as well as the skills and tools necessary to design, analyze, and implement electronic circuits and systems.
Module Learning Outcomes	1. Understanding the principles of electronic devices and circuits: Students should be able to demonstrate a basic understanding of the behavior and operation of electronic components such as resistors, capacitors, diodes, and transistors, as well as the design and analysis of electronic circuits. 2. Applying principles of digital electronics: Students should be able to apply the principles of digital logic and the design and operation of digital circuits, as well as the use of microprocessors and microcontrollers in electronic systems. 3. Working effectively in a team: Students should be able to work effectively in a team to design and implement electronic circuits and systems. 4. Applying knowledge to practical applications: Students should be able to apply their knowledge and skills to practical applications of computer electronics.
Learning and Teaching Strategies	
Strategies	The learning and teaching strategies for a course in computer electronics will depend on a variety of factors, including the level of study, course objectives, and student needs. However, some common learning and teaching strategies for computer electronics may include: 1. Lectures: Lectures are a common teaching strategy for introducing students to new concepts and theories in computer electronics. Lectures may be delivered in person or online, and may include multimedia such as slides and videos.

	2. Laboratory sessions: Laboratory sessions provide students with hands-on experience in designing, building, and testing electronic circuits and systems. These sessions may be conducted in a physical laboratory or through online simulation tools. 3. Group projects: Group projects are a common teaching strategy for developing students' teamwork skills and providing them with practical experience in designing and implementing electronic circuits and systems. Projects may involve designing and building electronic circuits, or developing software for controlling electronic systems. 4. Online resources: Online resources such as interactive simulations, virtual labs, and video tutorials can be used to supplement lectures and provide students with additional opportunities to practice and apply their knowledge. 5. Assignments and assessments: Assignments and assessments such as quizzes, exams, and design projects can be used to evaluate students' understanding of the course material and their ability to apply their knowledge and skills to practical problems.

Student Workload (SWL)			
Structured SWL (h/sem)	78	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	47	**Unstructured SWL (h/w)**	3
Total SWL (h/sem)	**125**		

Module Evaluation

As		**Time/Number**	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	2	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All

	Report	1	10% (10)	13	LO #6
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	**Introduction to electronic devices** • Physics of material, atoms. • electrons and energy bands. • types of material (insulators, conductors, and semiconductors). • N-type and P-type semiconductor. • Diodes(forward bias, reverse bias, V-I characteristics)
2	**Applications of diodes** • Half-wave rectifier. • average value. • r.m.s. value. • capacitor filter. • ripple voltage
3	**Applications of diodes** • Full-wave rectifier. • Diode limiters. • Clampers and Voltage Doubler.
4	**Applications of diodes** • Other types of diodes
5	**Bipolar junction transistor BJT** • BJT biasing. • cutoff. • Saturation. • operating point.
6	**Bipolar junction transistor BJT**

	• Applications • Amplifiers
7	**Bipolar junction transistor BJT,** • Frequency response
8	**Midterm Exam**
9	**Bipolar junction transistor BJT.** • Operational amplifier OPAMP
10	**Field Effect Transistors (FET)** • JFET. • MOSFET
11	**Field Effect Transistors (FET)** • MOSFET Biasing
12	**Field Effect Transistors (FET)** • Introduction to VLSI
13	**Field Effect Transistors (FET)** • NMOS. • PMOS. • CMOS Inverter
14	**Field Effect Transistors (FET)** • MOSFET DIGITAL Gates
15	Review and Student presentation
16	**Final Exam**

	Delivery Plan (Weekly Lab. Syllabus)
	Material Covered
1	**Lab1: Diode characteristics**
2	**Lab2: Half-wave rectifiers and with filter**
3	**Lab3: Full-wave rectifiers and with filter**
4	**Lab4: Zener diode characteristics and regulators**
5	**Lab5: BJT Characteristics**
6	**Lab6: Transistor Biasing (part 1)**
7	**Lab7: Transistor Biasing (part 2)**
8	**Lab8: BJT Amplifier and Frequency response**
9	**Lab9: Inverting and Non-inverting OPAMPs**
10	**Lab10: Analogue Comparator (OPAMP)**
11	**Lab11: FET Biasing**
12	**Lab12: CMOS Invertor**
13	**Lab13: Nand Gate**
14	**Lab14:Nor Gate**
15	**Review and Student presentation**
16	**Final Exam**

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	"Electronic Devices Conventional Current Version " by FLOYD	Yes
Recommended Texts	"Electronics for computer Technology " by Terrell, David	No

Websites	

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Computer Networks

Module Information		
Module Title	Computer Networks	**Module Delivery**
Module Type	**Core**	☒ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical**
Module Code	**BCYSCE201-S1**	
ECTS Credits	5	

Relation with other Modules

Prerequisite module	Network infrastructure and administration lab (BCYSCE201-S1)	**Semester**	1
Co-requisites module	Network Security (BCYSCE203-S2)	**Semester**	2

SWL (hr/sem)	**125**	☒ **Seminar**	
Module Level	2	**Semester of Delivery**	2
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Lecturer Assist. Rana Kh. Sabri	**e-mail**	E-mail
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	$MS_{C.}$
Module Tutor		**e-mail**	mti.lec39.rana@ntu.edu.iq
Peer Reviewer Name		**e-mail**	
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	1. Knowledge of Network Fundamentals. 2. Ability to Design and Implement Networks. 3. Understanding of Network Protocols and Services. 4. Effective Communication and Collaboration: Students should be able to effectively communicate and collaborate with others in the context of computer networks. This includes clear and concise documentation, presenting technical information, and working in teams to solve network-related problems.
Module Learning Outcomes	1. Understanding Network Fundamentals. 2. Exploring Network Protocols and Services: The module typically covers various network protocols and services, such as Ethernet, TCP/IP, DHCP , DNS, HTTP and FTP Students learn how these protocols enable communication and data transfer across networks. 3. Configure network devices 4. Design and plan network architectures
Learning and Teaching Strategies	
Strategies	1. Lectures and Presentations: Lectures and presentations are often used to deliver theoretical concepts, principles, and foundational knowledge related to computer networking. 2. Hands-on Lab Sessions: Practical lab sessions are essential for allowing students to apply theoretical knowledge and gain hands-on experience in configuring, troubleshooting, and managing computer networks. 3. Group Projects and Collaborative Learning: Group projects and collaborative learning activities promote teamwork, communication, and the exchange of ideas among students. 4. Online Discussion Forums: Online discussion forums or platforms provide an opportunity for students to engage in asynchronous discussions, ask questions, and share knowledge and resources related to computer networking. 5. Simulations and Virtual Environments: Network simulation tools and virtual environments can be used to create simulated network scenarios, allowing students to experiment and practice without the need for physical equipment.

	6. Continuous Learning Resources: Providing additional resources, such as textbooks, online tutorials, reference materials, and interactive learning modules, supports students' independent learning and exploration of advanced networking topics beyond the scope of the module.

Student Workload (SWL)

Structured SWL (h/sem)	79	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	46	**Unstructured SWL (h/w)**	3
Total SWL (h/sem)	**125**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
ormative ssessment	**Quizzes**	4	10% (10)	3, 5 , 10, 12	LO #2, #5 and #10, #11
	Assignments	5	10% (10)	2 ,4, 8, 12	LO #3, #4 and #6, #7
	Projects / Lab.	15	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #6
ummative ssessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
otal assessment			100% (100 Marks)		

Learning and Teaching Resources

	Text	Available in the Library?
Required Texts	Computer Networking: A Top-Down Approach, 8th edition" by James Krose and Keith Ross.	Yes
Recommended Texts	Data Communications and Networking: Forouzan, Behrouz A.	Yes
Websites	https://www.youtube.com/playlist?list=PL4IvPhAsvnPtkIJ3uV-pazx7XQ1God5OT	

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	**Computer Networks and the Internet** • What Is the Internet • A Nuts-and-Bolts Description • A Services Description • What Is a Protocol? • The Network Edge, Access Networks , Physical Media, The Network Core, Packet Switching, Circuit Switching, A Network of Networks, Delay, Loss, and Throughput in Packet-Switched Networks
2	**Computer Networks and the Internet** • Overview of Delay in Packet-Switched Networks, Queuing Delay and Packet Los, End-to-End Delay ,Throughput in Computer Networks • Protocol Layers and Their Service Models, Layered Architecture, Encapsulation, Networks Under Attack
3	**Application Layer** • Principles of Network Applications • Network Application Architectures • Processes Communicating • Transport Services Available to Applications • Transport Services Provided by the Internet • Application-Layer Protocols • Network Applications
4	**Application Layer** • The Web and HTTP , Overview of HTTP , Non-Persistent and Persistent Connections , HTTP Message Format • User-Server Interaction: Cookies , Web Caching, DNS—The Internet's Directory Service , Services Provided by DNS , Overview of How DNS Works , DNS Records and Messages
5	**Application Layer** • Peer-to-Peer Applications , P2P File Distribution • Video Streaming and Content Distribution Networks , Internet Video , HTTP Streaming and DASH , Content Distribution Networks • Case Studies: Netflix, YouTube, and Kankan • Socket Programming: Creating Network Applications ,Socket Programming with UDP , Socket Programming with TCP
6	**Transport Layer Introduction and Transport-Layer Services** • Relationship Between Transport and Network Layers • Overview of the Transport Layer in the Internet , Multiplexing and Demultiplexing
7	**Transport Layer Introduction and Transport-Layer Services** • Connectionless Transport: UDP , UDP Segment Structure , UDP Checksum

	• Principles of Reliable Data Transfer , Building a Reliable Data Transfer Protocol , Pipelined Reliable Data Transfer Protocols , Go-Back-N (GBN) , Selective Repeat (SR)
8	**Transport Layer Introduction and Transport-Layer Services** • Connection-Oriented Transport: TCP • The TCP Connection • TCP Segment Structure • Round-Trip Time Estimation and Timeout • Reliable Data Transfer • Flow Control • TCP Connection Management , Principles of Congestion Control , The Causes and the Costs of Congestion , Approaches to Congestion Control , TCP Congestion Control , Classic TCP congestion Control , Network-Assisted Explicit Congestion Notification and Delay-based Congestion Control , Fairness , Evolution of transport-layer functionality
9	**The Network Layer:** • Overview of Network Layer , Forwarding and Routing: The Network Data and Control Planes • Network Service Models , What's Inside a Router? , Input Port Processing and Destination-Based Forwarding , Switching , Output Port Processing , Where Does Queuing Occur? , Packet Scheduling
10	**The Network Layer:** • The Internet Protocol (IP): IPv4, Addressing, IPv6, and More • IPv4 Datagram Format , IPv4 Addressing • Network Address Translation (NAT) ,
11	**The Network Layer:** • IPv6 4.4 Generalized Forwarding and SDN , Match , Action , OpenFlow Examples of Match-plus-action in Action, Middleboxes
12	**The Network Layer:** • Control Plane Introduction • Routing Algorithms • The Link-State (LS) Routing Algorithm • The Distance-Vector (DV) Routing Algorithm • Intra-AS Routing in the Internet: OSPF • Routing Among the ISPs: BGP • The Role of BGP , Advertising BGP Route Information , Determining the Best Rou tes , IP-Anycast , Routing Policy , Putting the Pieces Together: Obtaining Internet Presence
13	**The Network Layer:** • The SDN Control Plane: SDN Controller and SDN Control Applications • OpenFlow Protocol • Data and Control Plane Interaction: An Example , SDN: Past and Future • ICMP: The Internet Control Message Protocol , Network Management, SNMP, and NETCONF/YANG ,The Network Management Framework

	• The Simple Network Management Protocol (SNMP) and the Management Information Base (MIB) , NETCONF and YANG
14	**The Link Layer and LANs** • Virtual Local Area Networks (VLANs) , Link Virtualization: A Network as a Link Layer • Multiprotocol Label Switching (MPLS) , Data Center Networking , Data Center Architectures • Trends in Data Center Networking, Retrospective: A Day in the Life of a Web Page Request • Getting Started: DHCP, UDP, IP, and Ethernet , Still Getting Started: DNS and ARP , Still • Getting Started: Intra-Domain Routing to the DNS Server • Web Client-Server Interaction: TCP and HTTP
15	**The Link Layer and LANs** • Introduction to the Link Layer • The Services Provided by the Link Layer • Where Is the Link Layer Implemented? , Error-Detection and -Correction Techniques , Parity Checks , Check summing Methods , Cyclic Redundancy Check (CRC) • Multiple Access Links and Protocols , Channel Partitioning Protocols , Random Access Protocols , Taking-Turns Protocols • DOCSIS: The Link-Layer Protocol for Cable Internet Access , Switched Local Area Networks , Link-Layer Addressing and ARP , Ethernet , Link-Layer Switches
16	**Final Exam**

	Delivery Plan (Weekly Lab. Syllabus)
	Material Covered
1	**Lab 1: Getting Started**
2	**Lab 2: Introduction to Wireshark**
3	**Lab 3: Setting Up Network**
4	**Lab 4: Wireshark_DHCP**
5	**Lab 5: Wireshark_DNS**
6	**Lab 6: Wireshark_Ethernet_ARP**
7	**Lab7: Wireshark_HTTP**
8	**Lab 8: Wireshark_ICMP**
9	**Lab 9: Wireshark IP**
10	**Lab 10: Wireshark NAT**
11	**Lab 11: Wireshark_SSL**
12	**Lab 12: Wireshark_TCP**
13	**Lab 13Wireshark_UDP**
14	**Lab14: Project and Presentation**
15	**Review**
16	**Final exam**

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Network infrastructure and Administration Lab

Module Information			
Module Title	**Network infrastructure and Administration Lab**	**Module Delivery**	
Module Type	**Supported**	☐ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**BCYSCE201-S2**		
ECTS Credits	**4**		
SWL (hr/sem)	**100**		
Module Level	1	**Semester of Delivery**	4
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Razan Abdulhammed	**e-mail**	rabdulhammed@ntu.edu.iq
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	Ph.D.
Module Tutor	Name (if available)	**e-mail**	E-mail
Peer Reviewer Name	Name	**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	Introducing students to fundamental, vendor-independent system and networking administration concepts. Building on students' existing knowledge of networks and systems administration. Providing students with knowledge of network basics and administration, including scope, goals, and best practices. 34. Teaching students how to configure, maintain, and Helping students develop skills in IP addressing, TCP/IP operation.
Module Learning Outcomes	16. Configure and manage network infrastructure devices, including routers, switches, firewalls, and wireless access points. 17. Troubleshoot network problems using appropriate tools and techniques. 18. Build multiple host and network architectures, given business requirements and constraints; configure operating systems, network-specific services, routing, switching, and remote access solutions. 19. Apply networking skills related to server operating systems, directory services, and administrative network. 20. Configure and manage network Cables and connecters, including twisted pair, Coaxial cables, optical fiber cables. 21. Configure and manage Different types of Antennas.
Indicative Contents	Indicative content includes the following. Cabling and Connectivity. Testing equipment. Connectivity devices – Repeater Connectivity devices – Modems Connectivity devices – Switches Connectivity devices – Routers Connectivity devices – Wireless Access point Antennas

Learning and Teaching Strategies	
Strategies	The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students. In addition to

	hands-on learning experiences that allow students to explore and learn through trial and error.

Student Workload (SWL)

Structured SWL (h/sem)	48	**Structured SWL (h/w)**	3
Unstructured SWL (h/sem)	52	**Unstructured SWL (h/w)**	3
Total SWL (h/sem)	**100**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	2	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

	Material Covered
Week 1	Cabling and Connectivity: Explain the key differences between cables and connector types.
Week 2	copper; 10Base2; 10BaseT. fiber – glass / plastic; multi-modal single-mode. connectors; RJ45; BNC; Straight Tip (ST); Subscriber Connector (SC); Local Connector (LC).

Week 3	Cabling and Connectivity: Describe the key features of Cat1-6 cables. identify Cat1-4 cable as older types of cable. describe the main features of Cat5, 5A, 6, 6A; (capacity; maximum distance; (network application (10BastT; 100Base-TX; 1000Base-T; 10GBase-T)).
Week 4	Cabling and Connectivity: Explain the different antenna types. directional; omni directional; point-to-point; point-to-multipoint; mobile.
Week 5	Identify testing equipment used with wired and wireless networks. Wired; multimeter; wire map tester; cable testers; tone generator and probe; loopback plug. Wireless; wireless locator / Wi-Fi analyzer; wireless heat maps.
Week 6	Repeater building component blocks, how to install, configure, and maintenance, Security configuration on repeater.
Week 7	Modems, function, types, building component blocks, how to install, configure, and maintenance Modems, Security configuration on Modems.
Week 8	Hub, function, types, building component block, how to install, configure, and maintenance Hubs, Security configuration on Hubs.
Week 9	Bridge, function, types, building component blocks, how to install, configure, and maintenance Bridges, Security configuration on Bridges.
Week 10	switches, function, types, how to install, configure, and maintenance switches, internal components, connectors, ports, and hardware specifications, Security configuration on Switches.
Week 11	Firewalls, function, types, how to install, configure, and maintenance Firewalls, internal components, connectors, ports, and hardware specifications, Security configuration on Firewalls
Week 12	wireless access points, function, types, how to install, configure, and maintenance wireless access points, internal components, connectors, ports, and hardware specifications, Security configuration on wireless access points.
Week 13	routers, function, types, how to install, configure, and maintenance routers, The router chassis, internal components, connectors, ports, and hardware specifications, Security configuration on Routers.
Week 14	Configure

Delivery Plan (Weekly Lab. Syllabus)

	Material Covered
Week 1	Lab1: Connectivity Cables
Week 2	Lab2: Connectivity devices -Modem -Repeater
Week 3	Lab 3: Network Configuration -IP address

	Week 4	Lab 4: Package management (RPM Command)
	Week 5	Lab 5: Package management (YUM Command)
	Week 6	Lab 6: DHCP Server
	Week 7	Lab7: FTP Server
	Week 8	Lab 8: YUM Server
	Week 9	Lab 9: NFS Server
	Week 10	Lab 10: DNS Sever
	Week 11	Lab 11: POST FIX Mail Server
	Week 12	Lab 12: Apache Web server
	Week 13	Lab 13: Authentication on Apache Web server
	Week 14	Lab 14: WEBMIN Administration
	Week 15	Final Project
	routers using the CLI, Configuring static routes.	
Week 15	Configuring router interfaces with IPv4 addresses, configuring clients with IPv4 addresses using DHCP.	
Week 16	**Preparatory week before the final Exam**	

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Linux Network Administrator's Guide: Infrastructure, Services, and Security by Tony Bautts , Terry Dawson, et al.	Yes
Recommended Texts		No
Websites		

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Operating Systems

Module Information			
Module Title	**Operating Systems**	**Module Delivery**	
Module Type	**Core**	☒ **Theory** ☒ **Lecture** ☒ **Lab** ☒ **Tutorial** ☒ **Practical** ☒ **Seminar**	
Module Code	**BCYSCCTE307-S1**		
ECTS Credits	**6**		
SWL (hr/sem)	**150**		
Module Level	2	**Semester of Delivery**	2
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Zakaria Noor Aldeen Mahmood	**e-mail**	E-mail
Module Leader's Acad. Title	Lecture	**Module Leader's Qualification**	Ph.D.
Module Tutor	Name (if available)	**e-mail**	E-mail
Peer Reviewer Name	Name	**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	35. To study, learn, and understand the main concepts of advanced operating systems, including parallel processing systems. 36. To gain a basic understanding of operating systems, including their role, types, and batch systems 37. To describe the services an operating system provides to users, processes, and other systems, and to discuss the various ways of structuring an operating system. 38. To acquire the basic operating system concepts such as processes and threads. 39. To understand the fundamental concepts of operating systems, including OS structures, processes/threads, memory management, and file systems. 40. To gain a general understanding of the structure of modern computers, the purpose, structure, and functions of operating systems, and to illustrate key OS concepts.
Module Learning Outcomes	22. Understand the main concepts of advanced operating systems, including parallel processing systems. 23. Acquire a basic understanding of operating systems, including their role, types, and batch systems. 24. Describe the services an operating system provides to users, processes, and other systems, and discuss the various ways of structuring an operating system. 25. Acquire the basic operating system concepts such as processes and threads. 26. Understand the fundamental concepts of operating systems, including OS structures, processes/threads, memory management, and file systems. 27. Gain a general understanding of the structure of modern computers, the purpose, structure, and functions of operating systems, and illustrate key OS concepts.
Indicative Contents	Indicative content includes the following. - Introduction to the operating system The basics of operating systems, including their role, types, and batch systems. Types of operating systems (Windows, Linux, MacOS, Unix). Processes and Threads (address spaces, system calls, scheduling).

	Threads and concurrency. [15 hrs] – The design and implementation of modern operating systems Memory management File systems and storage management Input/output (I/O) management. [15 hrs] - Synchronization Algorithms, Structures- semaphores, and monitors, Virtual Memory- Paging, Page tables, Eviction, Segmentation. [15 hrs] Revision problem classes [6 hrs] - File Systems File Abstraction, Directory Structures, Disk I/O. [12 hrs] Virtualization and cloud computing Virtualization in cloud computing is used to replace physical files, servers, networks, files, applications, devices, and infrastructure with computer-generated versions, which are hosted and managed by a service provider. [15 hrs]

Learning and Teaching Strategies

Strategies	Type something like: The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials, and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)

Structured SWL (h/sem)	78	**Structured SWL (h/w)**	5.2
Unstructured SWL (h/sem)	72	**Unstructured SWL (h/w)**	4.8
Total SWL (h/sem)	**200**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Assignments**	4	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Seminar	3	10% (10)	2 and 12	LO #3, #4 and #6, #7

	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

	Material Covered
Week 1	Introduction to the operating system
Week 2	Types of operating systems (Windows, Linux, MacOS, Unix)
Week 3	Process management and scheduling
Week 4	Processes and Threads (address spaces, system calls, scheduling)
Week 5	Threads and concurrency
Week 6	Memory management
Week 7	File systems and storage management
Week 8	Input/Output (I/O) management
Week 9	Synchronization (algorithms and structures like locks, semaphores, and monitors)
Week 10	Virtual Memory (paging, page tables, eviction, segmentation)
Week 11	File Systems (the file abstraction, directory structures)
Week 12	File Systems (disk I/O)
Week 13	Virtualization and cloud computing
Week 14	**The preparatory week before the Final Exam**
Week 15	Final Exam
Week 16	

Delivery Plan (Weekly Lab. Syllabus)

	Material Covered
Week 1	Lab1: Getting Started.
Week 2	Lab2: Process Scheduling Simulation
Week 3	Lab 3: Building a Simple Operating System - bootstrapping
Week 4	Lab 4: Building a Simple Operating System - memory management
Week 5	Lab5: Building a Simple Operating System - process management

Week 6	Lab 6: File System Implementation - FAT or EXT.
Week 7	Lab 7: File System Implementation – EXT.
Week 8	Lab 8: Virtual Memory Simulation - virtual memory management - page replacement algorithms.
Week 9	Lab 9: Kernel Debugging -Linux
Week 10	Lab 10: Kernel Debugging - Windows
Week 11	Lab 11: Concurrency Control - synchronization primitives, semaphores
Week 12	Lab 12: Concurrency Control - synchronization primitives, monitors
Week 13	Lab 13: Device Driver Development - keyboard or mouse driver
Week 14	Review
Week 15	Final Exam

Learning and Teaching Resources

	Text	**Available in the Library?**
Required Texts	Abraham Silberschatz-"Operating System Concepts" ,9th Edition,	No
Recommended Texts	William Stalling "Operating System- Internals and Design Principles", 7th Edition.	No
Websites	https://www.coursera.org/browse/physical-science-and-engineering/opreating system	

Grading Scheme

Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Programming Python for Cybersecurity

Module Information			
Module Title	**Python for Cybersecurity Programming**	**Module Delivery**	
Module Type	**Core**	☐ **Theory** ☒ **Lecture** ☒ **Lab** ☒ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**BCYSCE204-S1**		
ECTS Credits	6		
SWL (hr/sem)	**150**		
Module Level	2	**Semester of Delivery**	1
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Rabei Raad Ali	**e-mail**	rabei@ntu.edu.iq
Module Leader's Acad. Title	Professor	**Module Leader's Qualification**	Ph.D.
Module Tutor	Name (if available)	**e-mail**	E-mail
Peer Reviewer Name	Name	**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules			
Prerequisite module	Network security (**BCYSCE 203-S2)**	**Semester**	١
Co-requisites module	Computer Networks (**BCYSCCET 200-S2)**	**Semester**	1

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	Python is an advantageous programming language for cybersecurity because it can perform many cybersecurity functions, including malware analysis, scanning, and penetration testing. It is user-friendly and has an elegant simplicity, making it the perfect language choice for many cybersecurity professionals. Using Python's base programming, developers can do any of the following without using any other third-party tools: Web server fingerprinting, Simulation of attacks, Port scanning, Website cloning, Load generation and testing of a website, Creating intrusion detection and prevention systems, Wireless network scanning, Transmission of traffic in the network and Accessing mail server.
Module Learning Outcomes	1. Understand the fundamentals of Python programming. 2. Develop custom Python scripts to automate cybersecurity tasks. 3. Apply Python to meet objectives through the cybersecurity attack lifecycle. 4. Automate common cyberattack and defense activities with Python. 5. Use Python for monitoring and defense activities.

Learning and Teaching Strategies

Strategies	This course is designed with a learn by doing approach that focuses on creation of fully functional scripts. Instead of being stuck learning the details of the programming or scripting language to create the "optimal" solution, we focus on "what works" instead. Once complete, we can then extend what we have to build bigger and better solutions We will introduce the basic concepts of Python and how it can be used to facilitate cybersecurity initiatives. Additionally, we will introduce other tools such as Microsoft Visual Studio Code, Git and GitHub, various Linux commands, and

Student Workload (SWL)

Structured SWL (h/sem)	78	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	72	**Unstructured SWL (h/w)**	5
Total SWL (h/sem)	**150**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	2	10% (10)	5 and 14	LO #1, #2, #3, and #4
	Assignments	4	10% (10)	4 and 10	LO #2 #3, and #4
	Projects / Lab.	1	10% (10)	All	LO #1, #2, #3 and #4
	Report	1	10% (10)	15	LO #4 and #6
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	All
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

	Material Covered
Week 1	Overview of the course format and learning objectives Why Python is one of the most in-demand skills among cybersecurity recruits. Introduction to Python syntax and data types
Week 2	Automating Cybersecurity Tasks with Python Using Python to automate common cyberattack and defense activities. Writing custom Python scripts to automate cybersecurity tasks. Applying Python to meet objectives through the cybersecurity attack lifecycle. Using Python to monitor and detect security threats
Week 3	Advanced Python Concepts for Cybersecurity Advanced Python syntax and data structures Object-oriented programming in Python Using Python libraries for cybersecurity tasks Debugging and error handling in Python
Week 4	Python for Network Security Using Python to analyze network traffic. Writing Python scripts to detect and prevent network attacks. Using Python to secure network infrastructure
Week 5	Python for Web Security Using Python to analyze web traffic. Writing Python scripts to detect and prevent web attacks. Using Python to secure web applications
Week 6	Human security: identity management; personal awareness, understanding and compliance; human behavioral factors; personal data privacy and security. Automating Cybersecurity Tasks with Python Using Python to automate common cyberattack and defense activities. Applying Python to meet objectives through the cybersecurity attack lifecycle Developing custom Python scripts to automate cybersecurity tasks
Week 7	Mid-term Exam + Python Libraries for Cybersecurity Overview of Python libraries commonly used in cybersecurity, such as Scapy, Nmap, and Requests Using Python libraries to perform network scanning and reconnaissance. Using Python libraries to analyze network traffic and detect anomalies
Week 8	advanced Topics in Python for Cybersecurity Persistence, privilege escalation, and evasion techniques

	Active defense techniques using Python. Best practices for secure coding in Python
Week 9	Python libraries for cybersecurity
Week 10	Python for Pre-ATT&CK Introduction to Pre-ATT&CK Using Python for Pre-ATT&CK
Week 11	Python for ATT&CK Introduction to ATT&CK Using Python for ATT&CK
Week 12	Python for Monitoring Introduction to monitoring Using Python for monitoring
Week 13	Other forms of Overflow Attacks Ethical Issues
Week 14	Python for Defense Introduction to defense activities
Week 15	Using Python for defense activities

Delivery Plan (Weekly Lab. Syllabus)

	Material Covered
Week 1	Lab 1: Getting Started- Introduction to Python for cybersecurity.
Week 2	Lab 2: Installing Python and setting up the development environment.
Week 3	Lab 3: Python for PRE-ATT&CK
Week 4	Lab 4: Python for monitoring
Week 5	Lab 5: Cryptography in Python -Creaser
Week 6	Lab 6: Cyber security threats
Week 7	Lab7: Cyber security attacks
Week 8	Lab 8: Network security libraries in Python
Week 9	Lab 9: Automating cybersecurity tasks with Python
Week 10	Lab 10: Cybersecurity attack and defense activities with Python
Week 11	Lab 11: Developing custom Python scripts to automate cybersecurity tasks
Week 12	Lab 12: MITRE ATT&CK and Shield cybersecurity use cases drawn from Python code
Week 13-15	Lab 13 -15: Persistence, privilege escalation, and evasion in Python

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Python for Cybersecurity Using Python for Cyber Offense and Defense By Howard E. Poston · 2022	Yes
Websites	https://www.youtube.com/watch?v=4pe1fn3Gus0 https://www.youtube.com/c/googlecareercertificates	

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Database Security

Module Information		
Module Title	**Database Security**	**Module Delivery**
Module Type	**Core**	☒ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**
Module Code	**BCYSCE202-S2**	
ECTS Credits	**6**	
SWL (hr/sem)	**150**	

Module Level	٢	**Semester of Delivery**	4
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Zakaria Noor Aldeen Mahmood	**e-mail**	E-mail
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	Ph.D.
Module Tutor		**e-mail**	zakaria@ntu.edu.iq
Peer Reviewer Name		**e-mail**	
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules

Prerequisite module	Database Security (BCYSCE202-S1)	**Semester**	1
Co-requisites module		**Semester**	

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	1. To learn the basic understanding of database security concepts, principles, and practices. 2. To learn design, implement, and manage secure databases. 3. To learn how to protect sensitive data from unauthorized access, modification, and disclosure. 4. To learn implementation techniques of database security systems 5. The students should be able to understand the uses and purpose of using secure database application and database settings, send and retrieve secured information. 6. Help the students perform the needed cyber security database works as well as qualifying him to use the different kinds of database security tools and instructions to build & execute the projects of cyber security engineering.
Module Learning Outcomes	20. Understanding the fundamentals of database security system and concepts. 21. Mastering of secure database design and management. 22. Becoming familiar with protecting sensitive data.

	23. Being competent in common users authorized accessing and prevent data. 24. Being able to perform database security settings through encryption and Data protection. 25. Being able to write complete code to securely connect the database tools and avoid database software vulnerabilities for cyber security application programs.

Student Workload (SWL)

Structured SWL (h/sem)	79	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	71	**Unstructured SWL (h/w)**	4
Total SWL (h/sem)	**150**		

Learning and Teaching Strategies

Strategies	The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Module Evaluation

		Time/Number	Weight (Marks)	Week Due
Formative assessment	**Quizzes**	٤	10% (10)	2,6,10,١٤
	Assignments	5	10% (10)	2 ,6,8,10,١٢
	Projects / Lab.	1٤	10% (10)	Continuous
	Seminar	1	10% (10)	14
Summative assessment	**Midterm Exam**	2hr	10% (10)	7
	Final Exam	3hr	50% (50)	15
Total assessment			100% (100 Marks)	

DATABASE SECURITY - PROGRAMME COURSE DESCRIPTION

Code BCYSCE202-S2	Name of the Course Unit	Semester	In-Class Hours (T+P)	Credit	ECTS Credit
	Database Security	2	2+2		6

GENERAL INFORMATION	
Language of Instruction :	English
Level of the Course Unit :	BACHELOR'S DEGREE
Type of the Course :	Compulsory
Mode of Delivery of the Course Unit	Face to Face
Coordinator of the Course Unit	Dr. Zakaria Noor Aldeen Mahmood
Instructor(s) of the Course Unit	Dr. Zakaria Noor Aldeen Mahmood

OBJECTIVES AND CONTENTS	
Objectives of the Course Unit:	Introducing the fundamentals and principles of database security systems. starts from scratch to build a secure database and applications. Improving the skills of the students through understanding of database security concepts, principles, and practices. The students should be able to learn design, implement, and manage secure databases. Help the students perform the needed cyber security works as well as qualifying him to learn how to protect sensitive data from unauthorized access, modification, and disclosure.
Contents of the Course Unit:	• Introduction to Database Security • Access Control and Authentication • Encryption and Data Protection • Auditing and Compliance • Virtual Private Database • Attacks against Database systems • Database Software Vulnerabilities • Database Protection

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	Introduction to the Relational Model: Introduce class and overview of course topics
2	Introduction to Database Security: Overview of database security concepts and principles, Threats and vulnerabilities to database security, Legal and ethical issues in database security
3	Access Control and Authentication: User authentication and authorization, Role-based access control (RBAC), 3. Database privileges and permissions
4	Encryption and Data Protection: Cryptography and encryption algorithms, Data masking and obfuscation, Secure data transmission and storage

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
5	Auditing and Compliance: Database auditing and monitoring, Compliance regulations and standards, Incident response and disaster recovery
6	Database Security Best Practices: Secure coding practices for database applications, Database security testing and assessment, Emerging trends and technologies in database security
7	Virtual Private Database
8	Buffer overflows attacks and Query optimization
9	How the Virtual Private Database Works
10	Database injection attacks, Cross-site scripting (XSS) attacks, Privilege escalation attacks,
11	Encryption with Oracle
12	SQL/NoSQL Injection attacks, Testing input variables for SQL injection
13	Database Software Vulnerabilities: Deployment failures: Broken databases, Database inconsistencies, Misconfigurations
14	Database Software Vulnerabilities: Carelessness or misuse, Weaknesses in computational logic
15	Review/preparation for final exam
16	Final Exam

Delivery Plan (Weekly Lab. Syllabus)	
	Material Covered
Week 1	Lab 1: Getting started with Database Tools.
Week 2	Lab 2: Database Legal and ethical issues.
Week 3	Lab 3: Database Threats and vulnerabilities.
Week 4	Lab 4: Role-based access control.
Week 5	Lab 5: Database masking and obfuscation.
Week 6	Lab 6: Implementing Virtual Private Database.
Week 7	Lab 7: Buffer overflows attacks in Database.
Week 8	Lab 8: Injection attacks in Database.
Week 9	Lab 9: Cross-site scripting (XSS) attacks in Database.
Week 10	Lab 10: Protection against misuse in Database.
Week 11	Lab 11: Protection against damage in Database.

Week 12	Lab 12: Database Vulnerabilities – Misconfigurations.
Week 13	Lab 13: Database Vulnerabilities
Week 14	Lab 14: Deployment failures and Broken databases.
Week 15	Lab 15: Review/Preparation for final exam
Week 16	**Final Exam**

Learning and Teaching Resources

	Text	Available in the Library?
Required Texts	**2.** Database Security 1st Edition (2011) by Melissa Zgola	yes
Recommended Texts	3. Pfleeger, C. P. & Pfleeger, S. L. (2018). Security in Computing. Publisher: Pearson India	no
Websites		

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Computer Networks

Module Information

Module Title	Computer Networks	**Module Delivery**	
Module Type	**Core**	☒ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**BCYSCE200-S2**		
ECTS Credits	5		
SWL (hr/sem)	**125**		
Module Level	2	**Semester of Delivery**	2
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Lecturer Assist. Rana Kh. Sabri	**e-mail**	E-mail
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	$MS_{C.}$
Module Tutor		**e-mail**	mti.lec39.rana@ntu.edu.iq
Peer Reviewer Name		**e-mail**	
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules

Prerequisite module	Network infrastructure and administration lab (BCYSCE201-S1)	**Semester**	1
Co-requisites module	Network Security (BCYSCE203-S2)	**Semester**	2

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	5. Knowledge of Network Fundamentals. 6. Ability to Design and Implement Networks. 7. Understanding of Network Protocols and Services. 8. Effective Communication and Collaboration: Students should be able to effectively communicate and collaborate with others in the context of computer networks. This includes clear and concise documentation, presenting technical information, and working in teams to solve network-related problems.
Module Learning Outcomes	5. Understanding Network Fundamentals. 6. Exploring Network Protocols and Services: The module typically covers various network protocols and services, such as Ethernet, TCP/IP, DHCP , DNS, HTTP and FTP Students learn how these protocols enable communication and data transfer across networks. 7. Configure network devices 8. Design and plan network architectures
Learning and Teaching Strategies	
Strategies	7. Lectures and Presentations: Lectures and presentations are often used to deliver theoretical concepts, principles, and foundational knowledge related to computer networking. 8. Hands-on Lab Sessions: Practical lab sessions are essential for allowing students to apply theoretical knowledge and gain hands-on experience in configuring, troubleshooting, and managing computer networks. 9. Group Projects and Collaborative Learning: Group projects and collaborative learning activities promote teamwork, communication, and the exchange of ideas among students. 10. Online Discussion Forums: Online discussion forums or platforms provide an opportunity for students to engage in asynchronous discussions, ask questions, and share knowledge and resources related to computer networking. 11. Simulations and Virtual Environments: Network simulation tools and virtual environments can be used to create simulated network scenarios, allowing students to experiment and practice without the need for physical equipment. 12. Continuous Learning Resources: Providing additional resources, such as textbooks, online tutorials, reference materials, and

	interactive learning modules, supports students' independent learning and exploration of advanced networking topics beyond the scope of the module.

Student Workload (SWL)

Structured SWL (h/sem)	79	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	46	**Unstructured SWL (h/w)**	3
Total SWL (h/sem)	**125**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	4	10% (10)	3, 5 , 10, 12	LO #2, #5 and #10, #11
	Assignments	5	10% (10)	2 ,4, 8, 12	LO #3, #4 and #6, #7
	Projects / Lab.	15	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #6
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Learning and Teaching Resources

	Text	Available in the Library?
Required Texts	Computer Networking: A Top-Down Approach, 8th edition" by James Krose and Keith Ross.	Yes
Recommended Texts	Data Communications and Networking: Forouzan, Behrouz A.	Yes
Websites	https://www.youtube.com/playlist?list=PL4IvPhAsvnPtkIJ3uV-pazx7XQ1God5OT	

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	**Computer Networks and the Internet** • What Is the Internet • A Nuts-and-Bolts Description • A Services Description • What Is a Protocol? • The Network Edge, Access Networks , Physical Media, The Network Core, Packet Switching, Circuit Switching, A Network of Networks, Delay, Loss, and Throughput in Packet-Switched Networks
2	**Computer Networks and the Internet** • Overview of Delay in Packet-Switched Networks, Queuing Delay and Packet Los, End-to-End Delay ,Throughput in Computer Networks • Protocol Layers and Their Service Models, Layered Architecture, Encapsulation, Networks Under Attack
3	**Application Layer** • Principles of Network Applications • Network Application Architectures • Processes Communicating • Transport Services Available to Applications • Transport Services Provided by the Internet • Application-Layer Protocols • Network Applications
4	**Application Layer** • The Web and HTTP , Overview of HTTP , Non-Persistent and Persistent Connections , HTTP Message Format • User-Server Interaction: Cookies , Web Caching, DNS—The Internet's Directory Service , Services Provided by DNS , Overview of How DNS Works , DNS Records and Messages
5	**Application Layer** • Peer-to-Peer Applications , P2P File Distribution • Video Streaming and Content Distribution Networks , Internet Video , HTTP Streaming and DASH , Content Distribution Networks • Case Studies: Netflix, YouTube, and Kankan • Socket Programming: Creating Network Applications ,Socket Programming with UDP , Socket Programming with TCP
6	**Transport Layer Introduction and Transport-Layer Services** • Relationship Between Transport and Network Layers • Overview of the Transport Layer in the Internet , Multiplexing and Demultiplexing
7	**Transport Layer Introduction and Transport-Layer Services** • Connectionless Transport: UDP , UDP Segment Structure , UDP Checksum

	• Principles of Reliable Data Transfer , Building a Reliable Data Transfer Protocol , Pipelined Reliable Data Transfer Protocols , Go-Back-N (GBN) , Selective Repeat (SR)
8	**Transport Layer Introduction and Transport-Layer Services** • Connection-Oriented Transport: TCP • The TCP Connection • TCP Segment Structure • Round-Trip Time Estimation and Timeout • Reliable Data Transfer • Flow Control • TCP Connection Management , Principles of Congestion Control , The Causes and the Costs of Congestion , Approaches to Congestion Control , TCP Congestion Control , Classic TCP congestion Control , Network-Assisted Explicit Congestion Notification and Delay-based Congestion Control , Fairness , Evolution of transport-layer functionality
9	**The Network Layer:** • Overview of Network Layer , Forwarding and Routing: The Network Data and Control Planes • Network Service Models , What's Inside a Router? , Input Port Processing and Destination-Based Forwarding , Switching , Output Port Processing , Where Does Queuing Occur? , Packet Scheduling
10	**The Network Layer:** • The Internet Protocol (IP): IPv4, Addressing, IPv6, and More • IPv4 Datagram Format , IPv4 Addressing • Network Address Translation (NAT) ,
11	**The Network Layer:** • IPv6 4.4 Generalized Forwarding and SDN , Match , Action , OpenFlow Examples of Match-plus-action in Action, Middleboxes
12	**The Network Layer:** • Control Plane Introduction • Routing Algorithms • The Link-State (LS) Routing Algorithm • The Distance-Vector (DV) Routing Algorithm • Intra-AS Routing in the Internet: OSPF • Routing Among the ISPs: BGP • The Role of BGP , Advertising BGP Route Information , Determining the Best Rou tes , IP-Anycast , Routing Policy , Putting the Pieces Together: Obtaining Internet Presence
13	**The Network Layer:** • The SDN Control Plane: SDN Controller and SDN Control Applications • OpenFlow Protocol • Data and Control Plane Interaction: An Example , SDN: Past and Future • ICMP: The Internet Control Message Protocol , Network Management, SNMP, and NETCONF/YANG ,The Network Management Framework

	• The Simple Network Management Protocol (SNMP) and the Management Information Base (MIB) , NETCONF and YANG
14	**The Link Layer and LANs** • Virtual Local Area Networks (VLANs) , Link Virtualization: A Network as a Link Layer • Multiprotocol Label Switching (MPLS) , Data Center Networking , Data Center Architectures • Trends in Data Center Networking, Retrospective: A Day in the Life of a Web Page Request • Getting Started: DHCP, UDP, IP, and Ethernet , Still Getting Started: DNS and ARP , Still • Getting Started: Intra-Domain Routing to the DNS Server • Web Client-Server Interaction: TCP and HTTP
15	**The Link Layer and LANs** • Introduction to the Link Layer • The Services Provided by the Link Layer • Where Is the Link Layer Implemented? , Error-Detection and -Correction Techniques , Parity Checks , Check summing Methods , Cyclic Redundancy Check (CRC) • Multiple Access Links and Protocols , Channel Partitioning Protocols , Random Access Protocols , Taking-Turns Protocols • DOCSIS: The Link-Layer Protocol for Cable Internet Access , Switched Local Area Networks , Link-Layer Addressing and ARP , Ethernet , Link-Layer Switches
16	**Final Exam**

	Delivery Plan (Weekly Lab. Syllabus)
	Material Covered
1	**Lab 1: Getting Started**
2	**Lab 2: Introduction to Wireshark**
3	**Lab 3: Setting Up Network**
4	**Lab 4: Wireshark_DHCP**
5	**Lab 5: Wireshark_DNS**
6	**Lab 6: Wireshark_Ethernet_ARP**
7	**Lab7: Wireshark_HTTP**
8	**Lab 8: Wireshark_ICMP**
9	**Lab 9: Wireshark IP**
10	**Lab 10: Wireshark NAT**
11	**Lab 11: Wireshark_SSL**

12	**Lab 12: Wireshark_TCP**
13	**Lab 13Wireshark_UDP**
14	**Lab14: Project and Presentation**

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Network infrastructure and Administration Lab

Module Information			
Module Title	**Network infrastructure and Administration Lab**	**Module Delivery**	
Module Type	**Supported**	☐ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**BCYSCE201-S2**		
ECTS Credits	**4**		
SWL (hr/sem)	**100**		
Module Level	1 1	**Semester of Delivery**	4
Administering Department	Cyber Security and Cloud Computing	**College**	Technical Engineering College for computer and AI / Mosul

	Techniques Engineering		
Module Leader	Dr. Razan Abdulhammed	**e-mail**	rabdulhammed@ntu.edu.iq
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	Ph.D.
Module Tutor	Name (if available)	**e-mail**	E-mail
Peer Reviewer Name	Name	**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules

Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	Introducing students to fundamental, vendor-independent system and networking administration concepts. Building on students' existing knowledge of networks and systems administration. Providing students with knowledge of network basics and administration, including scope, goals, and best practices. 41. Teaching students how to configure, maintain, and Helping students develop skills in IP addressing, TCP/IP operation.
Module Learning Outcomes	28. Configure and manage network infrastructure devices, including routers, switches, firewalls, and wireless access points. 29. Troubleshoot network problems using appropriate tools and techniques. 30. Build multiple host and network architectures, given business requirements and constraints; configure operating systems, network-specific services, routing, switching, and remote access solutions. 31. Apply networking skills related to server operating systems, directory services, and administrative network. 32. Configure and manage network Cables and connecters, including twisted pair, Coaxial cables, optical fiber cables. 33. Configure and manage Different types of Antennas.
Indicative Contents	Indicative content includes the following. Cabling and Connectivity. Testing equipment. Connectivity devices – Repeater

	Connectivity devices – Modems

Learning and Teaching Strategies

Strategies	Connectivity devices – Wireless Access point Antennas The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students. In addition to hands-on learning experiences that allow students to explore and learn through trial and error.

Student Workload (SWL)

Structured SWL (h/sem)	48	**Structured SWL (h/w)**	3
Unstructured SWL (h/sem)	52	**Unstructured SWL (h/w)**	3
Total SWL (h/sem)	**100**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	2	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)	
	Material Covered
Week 1	Cabling and Connectivity: Explain the key differences between cables and connector types.
Week 2	copper; 10Base2; 10BaseT. fiber – glass / plastic; multi-modal single-mode. connectors; RJ45; BNC; Straight Tip (ST); Subscriber Connector (SC); Local Connector (LC).
Week 3	Cabling and Connectivity: Describe the key features of Cat1-6 cables. identify Cat1-4 cable as older types of cable. describe the main features of Cat5, 5A, 6, 6A; (capacity; maximum distance; (network application (10BastT; 100Base-TX; 1000Base-T; 10GBase-T)).
Week 4	Cabling and Connectivity: Explain the different antenna types. directional; omni directional; point-to-point; point-to-multipoint; mobile.
Week 5	Identify testing equipment used with wired and wireless networks. Wired; multimeter; wire map tester; cable testers; tone generator and probe; loopback plug. Wireless; wireless locator / Wi-Fi analyzer; wireless heat maps.
Week 6	Repeater building component blocks, how to install, configure, and maintenance, Security configuration on repeater.
Week 7	Modems, function, types, building component blocks, how to install, configure, and maintenance Modems, Security configuration on Modems.
Week 8	Hub, function, types, building component block, how to install, configure, and maintenance Hubs, Security configuration on Hubs.
Week 9	Bridge, function, types, building component blocks, how to install, configure, and maintenance Bridges, Security configuration on Bridges.
Week 10	switches, function, types, how to install, configure, and maintenance switches, internal components, connectors, ports, and hardware specifications, Security configuration on Switches.
Week 11	Firewalls, function, types, how to install, configure, and maintenance Firewalls, internal components, connectors, ports, and hardware specifications, Security configuration on Firewalls
Week 12	wireless access points, function, types, how to install, configure, and maintenance wireless access points, internal components, connectors, ports, and hardware specifications, Security configuration on wireless access points.
Week 13	routers, function, types, how to install, configure, and maintenance routers, The router chassis, internal components, connectors, ports, and hardware specifications, Security configuration on Routers.
Week 14	Configure routers using the CLI, Configuring static routes.

Week 15	Configuring router interfaces with IPv4 addresses, configuring clients with IPv4 addresses

Delivery Plan (Weekly Lab. Syllabus)

	Material Covered
Week 1	Lab1: Connectivity Cables
Week 2	Lab2: Connectivity devices -Modem -Repeater
Week 3	Lab 3: Network Configuration -IP address
Week 4	Lab 4: Package management (RPM Command)
Week 5	Lab 5: Package management (YUM Command)
Week 6	Lab 6: DHCP Server
Week 7	Lab7: FTP Server
Week 8	Lab 8: YUM Server
Week 9	Lab 9: NFS Server
Week 10	Lab 10: DNS Sever
Week 11	Lab 11: POST FIX Mail Server
Week 12	Lab 12: Apache Web server
Week 13	Lab 13: Authentication on Apache Web server
Week 14	Lab 14: WEBMIN Administration
Week 15	Final Project

Learning and Teaching Resources

	Text	**Available in the Library?**
Required Texts	Linux Network Administrator's Guide: Infrastructure, Services, and Security by Tony Bautts , Terry Dawson, et al.	Yes
Recommended Texts		No
Websites		

Grading Scheme

Group	**Grade**	**Marks %**	**Definition**
Success Group	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors

(50 - 100)	**C -** Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Cybersecurity Professional ethics

Module Information

Module Title	**Cybersecurity Professional ethics**	**Module Delivery**	
Module Type	**Basic**	☐ **Theory** ☒ **Lecture** ☐ **Lab** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**BCYSCE201-S2**		
ECTS Credits	**3**		
SWL (hr/sem)	**75**		
Module Level	1	**Semester of Delivery**	4
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Name	**e-mail**	E-mail
Module Leader's Acad. Title	Professor	**Module Leader's Qualification**	Ph.D.
Module Tutor	Name (if available)	**e-mail**	E-mail
Peer Reviewer Name	Name	**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	42. To provide students with an understanding of ethical issues and dilemmas that arise in the field of cybersecurity. 43. To develop critical ethical reasoning skills in addition to skills vital for cybersecurity professionals. 44. To engage students in open dialogue and debate within a safe and respectful environment.
Module Learning Outcomes	1. Understand the important ethical issues in cybersecurity. 2. Recognize that cybersecurity is intimately entangled with ethics. 3. Emphasize the social and ethical aspects of the work of cybersecurity, rather than the potential for technical fixes. 4. Develop ethical reasoning and professional conduct skills. 5. Understand how to overcome common psychological and contextual impediments for taking ethical action. 6. Adopt strategies for taking ethical action that have been developed in different sectors and areas. Practice as a competent professional in Cybersecurity or enrolled in an appropriate graduate program. 7. Demonstrate leadership by positive influence on others. 8. Understand the social and ethical aspects of the work of cybersecurity. 9. Recognize and analyze ethical issues in cybersecurity. 10. Apply ethical theories to cybersecurity situations. 11. Identify technical quandaries that have ethical implications. 12. Develop solutions to ethical issues in cybersecurity. 13. Apply rules and regulations to cybersecurity situations.
Indicative Contents	The concept of cybersecurity ethics (6hrs) The ethical issues related to cybersecurity and privacy. (2hrs) Ethical issues related to cybersecurity and society. (2hrs) Cybersecurity and national Business. (3hrs) Cybersecurity and national intellectual property. (3hrs)

	Ethical issues related to cybersecurity and national law enforcement. (3hrs) Cybersecurity and the national legal system (2hrs) The ethical issues related to Data breaches and data protection. (2hrs) Cybersecurity and International Business. (2hrs) Cybersecurity and international intellectual property (3hrs) Ethical issues related to cybersecurity and national international law enforcement (3hrs)

Learning and Teaching Strategies

Strategies	• Provide personalized guidance to encourage students to grow and carve their own path forward. • Instill outside-the-box thinking and encourage constant tinkering. • Prioritize ethics in the cyber community, despite their often being overlooked. • Leverage the online cybersecurity community, which has traditionally been accepting legitimate debates. • Focus on foundational building blocks and avoid rabbit holes. Cybersecurity requires life-long learning to stay up to date. • Personalize and individualize the teaching approach for each student to encourage outside-the-box thinking and constant tinkering. • Introduce some cybersecurity best practices, such as avoiding sharing sensitive data publicly, creating secure passwords, and not opening links from untrustworthy sources. • Integrate current events into lessons and classroom discussions.

Student Workload (SWL)

Structured SWL (h/sem)	33	**Structured SWL (h/w)**	2
Unstructured SWL (h/sem)	42	**Unstructured SWL (h/w)**	3
Total SWL (h/sem)	**75**		

Module Evaluation

		Time/Number	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	2	10% (10)	5 and 10	LO #3, #4 and #9, #11
	Assignments	2	10% (10)	2 and 12	LO #2, #7 and #13, #7
	Projects / Lab.	-	10% (10)	Continuous	All

	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

	Material Covered
Week 1	The concept of cybersecurity ethics, Introduction to cybersecurity ethics, Ethical theories and principles, Ethical decision-making frameworks.
Week 2	The ethical issues related to cybersecurity and privacy, Privacy and surveillance, Data breaches and data protection, Cyberstalking, and cyberbullying.
Week 3	Ethical issues related to cybersecurity and society, Cybercrime, and cyberterrorism, Cyberwarfare and cyberconflict, Cybersecurity and human rights
Week 4	Cybersecurity and Business, the ethical issues related to cybersecurity and business, Cybersecurity, and corporate responsibility.
Week 5	Cybersecurity and intellectual property, Cybersecurity, and the global economy
Week 6	Ethical issues related to cybersecurity and law enforcement from national perspective, Cybersecurity, and national law enforcement,
Week 7	Cybersecurity and the legal system, Cybersecurity and the criminal justice system, what ethical frameworks can guide cybersecurity practice
Week 8	What are the important ethical issues in cybersecurity? Common ethical challenges for cybersecurity professionals و What are cybersecurity professionals' obligations to the public
Week 9	The ethical issues related to cybersecurity and privacy, Privacy and surveillance in national sectors.
Week 10	The ethical issues related to Data breaches and data protection, Cyberstalking, and cyberbullying.
Week 11	Ethical issues related to cybersecurity and society, Cybercrime, and cyberterrorism
Week 12	Ethical issues related to Cyberwarfare and cyberconflict, Cybersecurity and human rights.
Week 13	Cybersecurity and Business, the ethical issues related to cybersecurity and business, Cybersecurity and corporate responsibility
Week 14	Cybersecurity and International Business, the International ethical issues related to cybersecurity and international business, Cybersecurity, and corporate responsibility. Cybersecurity and international intellectual property, Cybersecurity, and the global economy.
Week 15	**Review and Student Presentation.**
Week 16	**The final Exam**

Learning and Teaching Resources

	Text	Available in the Library?
Required Texts	Cybersecurity Ethics: An Introduction - Mary Manjikian	Yes

Recommended Texts	Cyberethics: Morality and Law in Cyberspace: Morality and Law in Cyberspace 7th Edition, by Richard A. Spinello	No
Websites		

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Network Security

Module Information

Module Title	**Network Security**	**Module Delivery**	
Module Type	**Core**	☐ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**BCYSCE203-S2**		
ECTS Credits	6		
SWL (hr/sem)	**150**		
Module Level	1 2	**Semester of Delivery**	2
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul

Module Leader	Dr. Rabei Raad Ali	**e-mail**	rabei@ntu.edu.iq
Module Leader's Acad. Title	Professor	**Module Leader's Qualification**	Ph.D.
Module Tutor	Name (if available)	**e-mail**	E-mail
Peer Reviewer Name	Name	**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules

Prerequisite module	Network infrastructure and administration (**BCYSCE 201-S1)**	**Semester**	١
Co-requisites module	Computer Networks (**BCYSCE 200-S2)**	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	This course examines information security services and mechanisms in a network context. Cryptographic tools such as message authentication codes, hash functions, digital signatures, and digital certificates are covered. Also, the course includes other topics such as access control, intrusion detection, database security, Internet security, and common threats on them.
Module Learning Outcomes	6. Use basic cryptographic techniques in software and system design 7. Apply security methods for authentication, access control, intrusion detection, and prevention 8. Identify and mitigate security vulnerabilities in existing systems 9. Evaluate the security risks of systems and perform security audits 10. Identify and critique the ethical and legal issues in system security 11. Work efficiently in a team

Learning and Teaching Strategies

Strategies	1- Provide students with opportunities to engage in realistic scenarios and apply their knowledge to solve security challenges. By actively participating in simulated attacks, vulnerability assessments, and defensive strategies, students can gain practical experience and develop problem-solving skills. 2- The integration of case studies and real-world examples. Network security is a constantly evolving field and learning from real-life incidents and breaches can help students understand the implications of security vulnerabilities and the importance of proactive measures. Analyzing case studies can enhance critical thinking abilities, risk assessment, and decision-making skills in the context of network security. 3- The context of network security should encompass hands-on experiences, real-world examples, collaboration, interactive methods, and industry

	involvement. By incorporating these strategies, educators can empower students to develop the knowledge, skills, and mindset necessary to navigate the complex and ever-changing landscape of network security.

Student Workload (SWL)

Structured SWL (h/sem)	79	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	71	**Unstructured SWL (h/w)**	5
Total SWL (h/sem)	**150**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	6	10% (10)	5 and 12	LO #1 and #3
	Assignments	4	10% (10)	3 and 10	LO #1 and #2
	Projects / Lab.	1	10% (10)	Continuous	All
	Report/ Seminar	1	10% (10)	4 and 13	LO #4 and #6
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	All
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

	Material Covered
Week 1	Security Overview
Week 2	Security Overview Wrap-up Cryptographic Tools
Week 3	Security Overview Wrap-up Cryptographic Tools
Week 4	User Authentication
Week 5	Authorization and Access Control
Week 6	Database Security

Week 7	Mid-term Exam + Denial of Service Attacks.
Week 8	Intrusion Detection
Week 9	Firewall and Intrusion Prevention.
Week 10	Internet Security Protocols and Standards (IPSec and Oakley).
Week 11	Internet Security Protocols and Standards (SSL / TLS; S/MIME), Internet Authentication (Kerberos, X.509)
Week 12	Stack Overflow Buffer Overflow
Week 13	Other forms of Overflow Attacks Ethical Issues
Week 14	Wireless Network Security

Delivery Plan (Weekly Lab. Syllabus)

	Material Covered
Week 1	Lab 1: Introducing Network Security.
Week 2	Lab 2: IP and ICMP Attacks Lab
Week 3	Lab 3: Linux Firewall Exploration Lab
Week 4	Lab 4: Web Security lab
Week 5	Lab 5: TCP Attacks Lab Packet Sniffing
Week 6	Lab 6: Social media forensics
Week 7	Lab 7: TCP Attacks Lab Packet Spoofing
Week 8	Lab 8: Intelligence gathering
Week 9	Lab 9: VLAN
Week 10	Lab 10: VPN
Week 11	Lab 11: DNS protocol attacks
Week 12	Lab 12: Detecting Data leaks using Internet Border Patrol
Week 13-15	Report and presentation

Learning and Teaching Resources

	Text	**Available in the Library?**
Required Texts	William Stallings and Lawrie Brown. Computer Security: Principles and Practice (4th Edition). 2017. Pearson, ISBN 9780134794105	Yes
Websites	https://seedsecuritylabs.org/Labs_16.04/Networking/	

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Computer Organization and Architectures

Module Information			
Module Title	**Computer Organization and Architectures**	**Module Delivery**	
Module Type	**Core**	☒ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**BCYSCE204-S2**		
ECTS Credits	**5**		
SWL (hr/sem)	**125**		
Module Level	1 2	**Semester of Delivery**	2

Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Lubab H.Samy	**e-mail**	E-mail
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	
Module Tutor		**e-mail**	Lubab_harith @ntu.edu.iq
Peer Reviewer Name		**e-mail**	
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules

Prerequisite module	**Digital electronics** BCYSCE101-S2	**Semester**	
Co-requisites module	Computer Electronics BCYSCE200-S1	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	1. Understanding the basic principles of computer organization: Students should be able to describe the fundamental concepts of computer organization such as memory hierarchy, input/output systems, and instruction execution. 2. Understanding the organization of computer systems: Students should be able to explain the organization of computer systems, including the CPU, memory, and I/O subsystems, and understand their interconnections and interactions. 3. Understanding the various instruction set architectures: Students should be able to compare and contrast different instruction set architectures (ISAs) and understand their trade-offs in terms of performance, complexity, and ease of programming. 4. Designing and analyzing computer systems: Students should be able to design and analyze computer systems based on their knowledge of computer organization and architecture principles and evaluate their performance using benchmarks. 5. Understanding the impact of emerging technologies: Students should be able to understand the impact of emerging technologies on computer architectures, such as the use of parallelism, virtualization, and cloud computing, and their implications for computer system design. Overall, the module objectives of Computer Organization and Architectures aim to provide students with a solid foundation in the principles of computer organization and architecture, as well as the ability to apply this knowledge to practical engineering problems.
Module Learning Outcomes	1. Understanding computer system organization: Students should be able to describe the organization of a computer system, including the CPU, memory, and I/O subsystems, and understand their interactions and trade-offs. 2. Understanding the instruction set architecture: Students should be able to compare and contrast different instruction set architectures (ISAs) and understand their impact on performance, power consumption, and ease of programming. 3. Understanding memory hierarchy: Students should be able to explain the concept of memory hierarchy and its impact on computer system performance, including cache memory, virtual memory, and secondary storage. 4. Understanding I/O systems: Students should be able to describe the principles of I/O

	systems, including device controllers, interrupt handling, and DMA. 5. Designing and analyzing computer systems: Students should be able to design and analyze computer systems based on their knowledge of computer organization and architecture principles, and evaluate their performance using benchmarks. 6. Understanding emerging technologies: Students should be able to understand the impact of emerging technologies on computer architectures, such as multicore processors, GPU computing, and cloud computing. .

Learning and Teaching Strategies	
Strategies	There are several strategies that can be used in Computer Organization and Architectures to design and analyze computer systems. Some of these strategies include: 1. Instruction Set Architecture (ISA) Design: This involves designing the instruction set and programming model of a computer system, which determines the operations that the CPU can perform and the interface between the CPU and the software. 2. Memory Hierarchy Design: This involves designing the memory hierarchy of a computer system, which includes cache memory, main memory, and secondary storage. Strategies such as cache optimization, virtual memory management, and data prefetching can be used to improve system performance. 3. I/O System Design: This involves designing the input/output (I/O) subsystem of a computer system, which allows the system to interact with external devices. Strategies such as interrupt handling, DMA, and device drivers can be used to optimize I/O system performance. 4. Parallelism and Concurrency: This involves designing computer systems to take advantage of parallelism and concurrency, which can improve system performance and energy efficiency. Strategies such as SIMD, MIMD,

Student Workload (SWL)			
Structured SWL (h/sem)	78	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	47	**Unstructured SWL (h/w)**	3
Total SWL (h/sem)	**125**		

Module Evaluation				
		Time/Number	**Weight (Marks)**	**Week Due**
Formative assessment	**Quizzes**	2	10% (10)	4,10
	Assignments	5	10% (5)	2 ,5,8,10,13
	Projects / Lab.	15	105% (5)	Continuous
	Report	15	10% (5)	Continuous
Summative assessment	**Midterm Exam**	2hr	10% (10)	7
	Final Exam	3hr	50% (50)	16
Total assessment			100% (100 Marks)	

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	Internal Architecture of 8086/8088, Register Organization, Pin Descriptions of 8086/8088
2	Physical Memory Organization, Timing diagrams, and General Bus Operations
3	Addressing Capability, Minimum Mode 8086 System and Timings, Maximum Mode 8086 System and Timings,8086/8088 Instruction Set: Arithmetic and logical instructions Shift instructions, Rotate instructions, Control Flow instructions, LOOPS instructions, String instructions
4	The 8284-clock generator and 8288 Bus Controller
5	Memory interfacing: Types of semiconductor memories. The internal structure of ROMs and RAMs, Memory Address Decoding, EPROM and static RAM interfacing (examples), Memory expansion (in word and size)

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
6	I/O interfacing: I/O bus cycles, Memory mapped I/O, Isolated mapped I/O,I/O instructions and data transfers, I/O Port Address Decoding, I/O interfacing examples (LEDs and switches)
7	PIO 8255 [Programmable Input-Output Port]: Modes of Operation of 8255
8	Interfacing Analog to Digital Data Converters, Interfacing Digital to Analog Converters
9	keyboard and 7-segment display Interfacing
10	Interrupts and stack operations: Stack Structure of 8086/88, Basic Interrupt Processing
11	Interrupt Cycle of 8086/8088, Interrupt Vector Table, Interrupt Instructions: BOUND, INTO, INT, INT 3, and IRET, Hardware Interrupts, Expanding the Interrupt Structure (examples)
12	8259A Programmable Interrupt Controller (pin diagram and internal structure
13	Connecting a Single 8259A ; Cascading Multiple 8259As
14	Direct memory access: Basic DMA Operation, The 8237 DMA Controller, Pin Definitions and internal structure
15	review
16	Final Exam

Delivery Plan (Weekly Lab. Syllabus)

Week 1	Lab 1: Introduction to Proteus simulator for digital systems
Week 2	Lab 2: Microprocessor interfacing Circuit Design in Proteus (Leds and Switches)
Week 3	Lab 3: Introduction to Memory Type and Organization
Week 4	Lab 4: SRAM interfacing
Week 5	Lab 5: ROM interfacing
Week 6	Lab 6: Expanding ROM and RAM
Week 7	Lab 7: Interfacing LEDs and switches to the microprocessor
Week 8	Lab 8: Interfacing Keyboard to the microprocessor
Week 9	Lab 9: Interfacing 7-segment display to the microprocessor
Week 10	Lab 10: Programmable Interrupt Controller
Week 11	Lab 11: Microprocessor Interrupts Design

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
Week 12	Lab 12: Interfacing ADC to the microprocessor
Week 13	Lab 13: Interfacing DAC to the microprocessor
Week 14	Review
Week 15	**presentation**
Week16	**Final Exam**

Learning and Teaching Resources

	Text	Available in the Library?
Required Texts	• 8085 Microprocessor by Ramesh Goankar • 8086 Microprocessor by John Uffenbeck. • Fundamentals of Microprocessors and Microcontrollers by B Ram	Yes
Recommended Texts		
Websites		

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Data Structure

Module Information

Module Title	**Data Structure**	**Module Delivery**	
Module Type	**Core**	✓ **Theory** ✓ **Lecture** ✓ **Lab** x **Tutorial** ✓ **Practical** ✓ **Seminar**	
Module Code	**BCYSCCTE104-S2**		
ECTS Credits	**5**		
SWL (hr/sem)	**125**		
Module Level	2	**Semester of Delivery**	1
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Shaima Miqdad Mohamed Najeeb	**e-mail**	shaimamiqdad76@ntu.edu.iq
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	M.Sc.
Module Tutor	None	**e-mail**	None
Peer Reviewer Name	None	**e-mail**	None
Review Committee Approval	25/10/2024	**Version Number**	1.0

Relation With Other Modules

Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives أ	1. Understanding the basic concepts of Data structures such as arrays, stacks, queues, trees, graphs, and so on. for building blocks of algorithms and programs.. 2. Analyzing the algorithms that are used to manipulate data. By analyzing algorithms, we can determine their efficiency and optimize them to make them faster and more efficient. 3. Choosing the right data structure is essential for developing efficient programs. The study of data structures helps in choosing the right data structure for a particular problem. 4. The study of data structures helps in implementing data structures such as linked lists, trees, and graphs. By implementing data structures, we can create efficient programs that can handle large amounts of data.
Module Learning Outcomes	1. Understanding the fundamental concepts of data structures. 2. Analyzing the performance of algorithms 3. Choosing appropriate data structures. 4. Implementing data structures. 5. Designing algorithms. 6. Applying data structures to real-world problems

Indicative Contents	Indicative content includes the following: • Part A – Introduction to data structures: Overview of data structures, their types, and applications. .[8 hrs] • Part B- Arrays and Linked lists:: One-dimensional and multi-dimensional arrays, array operations, and applications. Linked lists: Singly linked lists, doubly linked lists, circular linked lists, and their operations.[12hrs] • Part C -: Stacks and Queues Array-based and linked-list based implementation of stacks and queues, their operations, and applications.. [12 hrs] • Part D - Trees: Binary trees, binary search trees, AVL trees, red-black trees, and their operations. [14 hrs] • Part E – Graphs: Graph representation, graph traversal algorithms, shortest path algorithms, and minimum spanning tree algorithms..[10 hrs] • Revision problem classes [4 hrs]

Learning and Teaching Strategies

Strategies	The main strategy that will be used in Data structure courses to introduce the concepts of data structures and explain the theoretical aspects of algorithms that operate on data structures,provide hands-on exercises to help students implement data structures and algorithms using programming languages such as C++, Java, or Python, provide practice problems to help students improve their problem-solving skills and prepare for exams and assess students' understanding of data structures and algorithms through quizzes, exams, programming assignments, and group projects..

Student Workload (SWL)

Structured SWL (h/sem)	62	**Structured SWL (h/w)**	4.13
Unstructured SWL (h/sem)	63	**Unstructured SWL (h/w)**	4.2
Total SWL (h/sem)	125		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	4	10% (10)	5, 10	LO #1, 2, 10 and 11
	Assignments	4	10% (10)	2, 12	LO # 3, 4, 6 and 7
	Projects / Lab.	15	10% (10)	Continuous	All
	Report	14	10% (10)	1-14	LO#1-LO14
Summative assessment	**Midterm Exam**	1 hr	10% (10)	7	LO # 1-7
	Final Exam	3 hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

	Material Covered

Week 1	Introduction to Data Structure
Week 2	Algorithm Analysis
Week 3	Encapsulation, Inheritance
Week 4	Polymorphism, Generics
Week 5	Interfaces, Iterators
Week 6	Abstract Classes
Week 7	Maps and Sets, Linked Lists
Week 8	Recursion, Recursive Backtracking
Week 9	Searching and Simple Sorts, Fast Sorting
Week 10	Stacks and Queues
Week 11	Trees and Binary Search Trees, Red-Black Trees, and Huffman Code Trees
Week 12	Graphs and Hash tables, Heaps and Tries
Week 13	Dynamic Programming and Functional Programming
Week 14	Future trends in Data structure for Cyber security engineering Application
Week 15	Review
Week 16	Final Exam

Delivery Plan (Weekly Lab. Syllabus)

	Material Covered
Week 1	Lab1: Implementation of searching and sorting techniques.
Week 2	Lab2: Implementation of list using array and linked list.
Week 3	Lab 3: Implementation of push and pop operation on stack
Week 4	Lab 4: Implementation of polish notation and its conversion
Week 5	Lab5: Solve the problems using iteration/recursion
Week 6	Lab 6: Implementation of Maps and Sets.
Week 7	Lab 7: Implementation of Linked Lists.
Week 8	Lab 8: Recursion removal using stack
Week 9	Lab 9: Insertion /deletion operation on various queue
Week 10	Lab 10: Implementation of priority queue for process scheduling
Week 11	Lab 11: Storing data as a tree structure and implementation of various traversal techniques(part1).
Week 12	Lab 12: Storing data as graph structure and implementation of various traversal techniques (part2).
Week 13	Lab 13: Finding the shortest path in a graph.(part1)
Week 14	Lab 14: Finding the shortest path in a graph.(part2)
Week 15	Review
Week 16	Final Exam

Learning and Teaching Resources

	Text	**Available in the Library?**
Required Texts	1- Data Structures And Algorithms Made Easy	YES

	by Narasimha Karumanch (Author)	
Recommended Texts	data structure, algorithm and application in c++ by Sartaj sahni	No
Websites	https://opendatastructures.org/	

APPENDIX:

GRADING SCHEME			
Group	**Grade**	**Marks (%)**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note:

NB Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

ADVANCED ENGLISH SKILLS-I

Module Information		
Module Title	**ADVANCED ENGLISH SKILLS-I**	**Module Delivery**
Module Type	**Core**	**☒Theory** **☒ Lecture**
Module Code	**BCYSCE301-S1**	
ECTS Credits	**3**	

SWL (hr/sem)	**75**			☐**Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Level		UGx11 3	**Semester of Delivery**		1
Administering Department		Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul	
Module Leader	Dr. Razan Abdulhammed		**e-mail**	E-mail	
Module Leader's Acad. Title		Lecturer	**Module Leader's Qualification**		Ph.D.
Module Tutor			**e-mail**	rabdulhammed@ntu.edu.iq	
Peer Reviewer Name			**e-mail**	E-mail	
Scientific Committee Approval Date		25/10/2024	**Version Number**		1.0

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	45. Identify advanced level of grammar structure. 46. Criticize and interpret the advanced level of reading passages. 47. Develop listening skills. 48. Develop the ability to expand their vocabulary through multiple methods. 49. Compose an essay by developing content, using specific grammatical structures and giving thematically related examples about the given topic.
Module Learning Outcomes	1. Understand and use common everyday expressions and simple sentences. 2. Advanced Proficiency: Understand and actively participate in complex discussions. 3. Demonstrate grammatical accuracy and fluency in both spoken and written English. 4. Develop specialized vocabulary, terminology, and communication strategies relevant to the chosen field. 5. Understand and produce professional documents, presentations, and reports in English. 6. Engage in effective communication within professional contexts.

Learning and Teaching Strategies	
Strategies	Type something like: The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)			
Structured SWL (h/sem)	33	**Structured SWL (h/w)**	2
Unstructured SWL (h/sem)	42	**Unstructured SWL (h/w)**	3
Total SWL (h/sem)	**75**		

Module Evaluation					
As		**Time/Number**	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	6	10% (10)	1,3,4,7,8,9,	LO #1, #2 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Preliminary & further study	٢	10% (10)	3,7	LO #6, #10
	Report	٢	10% (10)	6,13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)	
Week	**Material Covered**
Week 1	Introduction to the Course Goals, Assignments, Schedule, Criteria, Policies
Week 2	**Unit 1**: The Way We Are Talking about the dysfunctional families, telling and writing a story about an unusual person from the past with Narrative Tenses.
Week 3	Managing conversation: Agreeing, Disagreeing and Partially Agreeing

Week 4	**Unit 2**: Wild World Listening conversations and reading a text about animals and their characteristics and human's attitudes to animals.
Week 5	Managing conversations on similarities and differences between humans and chimpanzees with using a wide range of Verbs of Senses and Articles.
Week 6	**Unit 3**: On the Money Listening to people talking about how they spend money and writing a web article called 'How to be rich'
Week 7	Reading an article about money trends, giving and responding to opinions about money issues with the use of Future Forms.
Week 8	MID-TERM EXAM
Week 9	Reading and analyzing movie review; Hobbits and Other Creatures Studying on Adjective Clauses with Prepositions.
Week 10	**Unit 4**: Through The Ages Giving a talk about the uses of and history of plastic. The Passive Structure.
Week 11	Using Compound Nouns and Possessive's Writing a paragraph about advantages and disadvantages of internet.
Week 12	**Unit 5**: Island Hopping Managing conversations using Discourse Markers.
Week 13	Listening of an interview about a survival TV show Reading the text 'An Unexplained Mystery' Studying on Past Deduction and Speculation.
Week 14	Talking about utopian and dystopian stories, films and games. Listening a conversation about dystopian fiction as a study of Pronouns and Substitution and Writing a paragraph comparing science fiction and reality.
Week 15	**Review**
Week 16	**Final Exam**

Learning and Teaching Resources

	Text	**Available in the Library?**
Required Texts	McCarthy, M., McCarten, J., & Sandiford, H. (2014). Touchstone series. Cambridge: Cambridge University Press.	Yes
Recommended Texts	McCarthy, M., McCarten, J., & Sandiford, H. (2014). Touchstone series. Cambridge: Cambridge University Press.	Yes
Websites		

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Introduction to cryptography

Module Information			
Module Title	**Introduction to cryptography**	**Module Delivery**	
Module Type	**Core**	☒ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**BCYSCE300-S1**		
ECTS Credits	6		
SWL (hr/sem)	**150**		
Module Level	3	**Semester of Delivery**	1

Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Razan Abdulhammed	**e-mail**	E-mail
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	Ph.D.
Module Tutor		**e-mail**	rabdulhammed@ntu.edu.iq
Peer Reviewer Name		**e-mail**	
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	1. Understanding Cryptographic Concepts 2. Learning Cryptographic Algorithms 3. Exploring Cryptographic Protocols 4. Understanding Cryptanalysis Techniques 5. Knowledge of Cryptographic Applications 6. Familiarity with Key Management and Distribution 7. Awareness of Cryptographic Standards and Regulations 8. Practical Skills in Cryptographic Implementation
Module Learning Outcomes	1. Students should acquire a fundamental understanding of what cryptography is and its role in securing information 2. Students should become familiar with various cryptographic algorithms used in practice, such as symmetric encryption (e.g., AES, DES) and asymmetric encryption. 3. Students should gain knowledge about cryptographic protocols used for secure communication 4. Students should learn about practical cryptographic tools and techniques used in real-world scenarios 5. Students should develop an understanding of basic cryptanalysis techniques 6. Students should explore various applications of cryptography beyond traditional encryption 7. Practical Skills: Depending on the nature of the course, students may also gain hands-on experience with implementing cryptographic algorithms, using cryptographic libraries or tools

Learning and Teaching Strategies

Strategies	13. Lectures and Presentations: Lectures and presentations are often used to deliver theoretical concepts, principles, and foundational knowledge related to computer networking. 14. Hands-on Lab Sessions: Practical lab sessions are essential for allowing students to apply theoretical knowledge and gain hands-on experience in configuring, troubleshooting, and managing computer networks. 15. Group Projects and Collaborative Learning: Group projects and collaborative learning activities promote teamwork, communication, and the exchange of ideas among students. 16. Online Discussion Forums: Online discussion forums or platforms provide an opportunity for students to engage in asynchronous discussions, ask

	questions, and share knowledge and resources related to computer networking. 17. Simulations and Virtual Environments: Network simulation tools and virtual environments can be used to create simulated network scenarios, allowing students to experiment and practice without the need for physical equipment. 18. Continuous Learning Resources: Providing additional resources, such as textbooks, online tutorials, reference materials, and interactive learning modules, supports students' independent learning and exploration of advanced networking topics beyond the scope of the module.

Student Workload (SWL)			
Structured SWL (h/sem)	63	**Structured SWL (h/w)**	4
Unstructured SWL (h/sem)	87	**Unstructured SWL (h/w)**	6
Total SWL (h/sem)	**150**		

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	**Overview of cryptography**: • what is a cipher? Introduction • symmetric ciphers model: plaintext, encryption algorithm, secret key, cipher text, decryption algorithm, a model of conventional encryption. • cryptanalysis, security against chosen plaintext attacks (cpa).
2	**Block ciphers**: • how to use a block cipher: pseudo random permutations (PRP) • pseudo random functions (PRF) • basic modes of operation: counter mode and CBC. • Iterated even-MANSOUR ciphers and the AES block cipher, arithmetic modulo primes and finite cyclic groups.
3	**Block ciphers**: • mono alphabetic substitution • ciphers shift ciphers • Caesar cipher • the affine cipher • Playfair cipher • polyalphabetic ciphers Vigenère cipher • the transposition cipher, one time pad cipher.
4	**El Gamal public key encryption semantically secure El Gamal encryption; CCA security**
5	**public key encryption using a trapdoor function**
6	**Message integrity:** • definition and applications CBC-MAC and PMAC.
7	**Digital signatures:** • definitions and applications: how to sign using RSA. • hash-based signatures; • certificates, certificate transparency, certificate revocation.
8	**Collision resistant hashing:** • MERKLE-DAMGARD and DAVIES-MEYER; • macs from collision resistance; case studies: SHA and Hmac.
9	**Symmetric-key algorithms** • DES—the data encryption standard, hers -16 round FEISTEL system, cryptanalysis of a symmetric key algorithms

10	**Public-key algorithms** • -RSA • - other public-key algorithms
11	**Identification protocols password protocols** • salts; • one-time passwords (s/key and SECUR-ID); • challenge response authentication.
12	**Authentication protocols** • -authentication based on a shared secret key, • -establishing a shared key: the DIFFIE -HELLMAN key exchange, -authentication using a key distribution center, -authentication using KERBEROS, -authentication using public-key cryptography,
13	**Authenticated key exchange and SSL/TLS session setup**
14	**Cryptography in the age of quantum computers**; • GROVER'S algorithm and symmetric crypto; • SHOR'S algorithm and public key crypto; • post-quantum crypto: signatures and key exchange
15	**Review**
16	**Final Exam**

Delivery Plan (Weekly Lab. Syllabus)

	Material Covered
1	Lab 1: Shift ciphers - Caesar cipher- the affine cipher
2	Lab 2: - Playfair cipher- ciphers Vigenère cipher
3	Lab 3: CBC-MAC and PMAC.
4	Lab 4: El Gamal.
5	Lab 5: MERKLE-DAMGARD and DAVIES-MEYER
6	Lab 6: SHA and HMAC
7	Lab 7: DES.
8	Lab 8: RSA.
9	Lab 9: SSL/TLS session
10	Lab 10: DIFFIE -HELLMAN
11	Lab 11: one-time passwords (s/key and SECUR-ID).
12	Lab 12: KERBEROS.
13	Lab 13: GROVER'S and SHOR'S algorithms
14	Lab 14: Review 1
15	Lab 14: Review 2
16	Final Exam

Learning and Teaching Resources

	Text	Available in the Library?

Required Texts	1. **Cryptography and Network Security: Principles and Practice, William Stallings , Jan 1, 1900** 2. **Cryptography and Network Security: Principles and Practice, Global Edition, Douglas R. Stinson , Nov 1, 2005** 3. **Workbook for ICD-10-CM/PCS Coding: Theory and Practice, 2018 Edition, Karla R. Lovaasen RHIA CCS CCS-P | Aug 25, 2017**	Yes
Recommended Texts	Cryptography & Network Security (McGraw-Hill Forouzan Networking) 1st Edition, Behrouz A. Forouzan	Yes
Websites		

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Digital Signal Processing

Module Information		
Module Title	**Digital Signal Processing**	**Module Delivery**
Module Type	**Core**	☒ **Theory** ☒ **Lecture**
Module Code	**BCYSCE302-S1**	
ECTS Credits	**4**	

SWL (hr/sem)	**100**	**☒ Lab** **☐ Tutorial** **☐ Practical** **☒ Seminar**

Module Level	UGx11 3	**Semester of Delivery**	2
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Fadwa Alezzo	**e-mail**	E-mail
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	
Module Tutor		**e-mail**	
Peer Reviewer Name		**e-mail**	
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules

Prerequisite module	**Digital electronics** BCYSCE101-S2	**Semester**	
Co-requisites module	AI for cybersecurity engineering BCYSCE402-S1	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	1-Understanding the basic principles of DSP: Students should be familiar with the fundamental concepts of DSP, including sampling, quantization, filtering, and spectral analysis. .2-Developing theoretical knowledge: Students should understand the mathematical foundations of DSP, including the Fourier transform, z-transform, and digital filter design.

	.3-Applying DSP techniques: Students should be able to apply DSP techniques to analyze and process digital signals for a range of applications, such as audio and image processing, telecommunications, and control systems. .4-Practical implementation: Students should be able to implement DSP algorithms using software tools such as MATLAB, and be familiar with common DSP hardware platforms
Module Learning Outcomes	1-Understanding of DSP fundamentals: Students should be able to demonstrate an understanding of the fundamental concepts and principles of DSP, including sampling, quantization, filtering, and spectral analysis. 2- Students should be able to apply mathematical techniques such as the Fourier transform, z-transform, and digital filter design to analyze and solve problems related to DSP. 3- Students should be able to analyze and interpret the results of DSP algorithms and experiments, and apply critical thinking skills to evaluate the effectiveness and limitations of different techniques.

Learning and Teaching Strategies	
Strategies	1. Start with the basics: Before diving into DSP, it's important to have a strong foundation in mathematics, particularly in calculus, linear algebra, and Fourier analysis. These concepts form the building blocks of DSP and will help you understand the fundamental principles. 2. Learn the theory: DSP is based on mathematical principles and concepts. Therefore, it is important to have a clear understanding of the theory behind signal processing. You can start by studying books, online courses, or attending lectures on signal processing theory 3. 3. Practice with real-world examples: DSP is widely used in many applications, such as audio processing, image processing, and control systems. Practicing with real-world examples can help you understand how DSP is applied in different fields. 4. Use software tools: There are many software tools available for DSP, such as MATLAB, Octave, and Python. These tools can help you implement and test different signal processing algorithms.

Student Workload (SWL)			
Structured SWL (h/sem)	63	**Structured SWL (h/w)**	4
Unstructured SWL (h/sem)	37	**Unstructured SWL (h/w)**	3
Total SWL (h/sem)	**100**		

Module Evaluation

As		Time/Number	Weight (Marks)	Week Due
Formative assessment	**Quizzes**	4	10% (10)	3,5,8,12
	Assignments	3	5% (5)	2,5,10
	Projects / Lab.	15	10% (5)	Continuous
	Report	11	10% (5)	Continuous
Summative assessment	**Midterm Exam**	2hr	10% (10)	7
	Final Exam	3hr	50% (50)	16
Total assessment			100% (100 Marks)	

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	Introduction to Continuous-time and Discrete-time signals and systems.
2	Numerical Integral compared to Integral with limits in Continuous-Time Signals.
3	Converting Continuous-time signals to discrete- time signals – sampling calculation and finding the number of samples in discrete-time signals.
4	Unit-Step and Unit-Impulse Functions in Continuous and Discrete versions.
5	Discrete-Time Signal Transformations: Time –Reversal, Time – Scaling, Time –Shifting
6	Discrete-Time Signal Amplitude Transformation: Amplitude – Reversal, Amplitude – Scaling, Amplitude – Shifting.
7	Plotting Discrete –time signal with both Time and Amplitude Transformations, Signals Periodic in $\boldsymbol{n}$ Signals Periodic in Ω
8	Discrete –Time Systems Interconnected System: Definition, Types of Interconnected Systems and their mathematical Models
9	Properties of Discrete-Time Systems: System with Memory, Causality, Time –Invariant System, Inverse of Systems, Time Invariance, Stability, Linearity
10	Impulse Representation of Discrete-time Signals, Calculating the Total impulse response in interconnected systems, Convolution of Discrete-Time Systems with impulse response
11	Convolution of Discrete-Time Systems for definite discrete-time signals, Properties of Discrete-time systems with convolution
12	Discrete-Time Fourier Transform and Linear Time Invariant Systems, Discrete-Time Fourier Transform for periodic Functions
13	Decomposition in time Fast Fourier Transform Algorithm, Decomposition in Fequency Fast Fourier Transform
14	Digital Filters: Properties, Averaging filter. Recursive smoother
15	review
16	Final Exam
WEEK	**Delivery Plan (Weekly Lab. Syllabus)**
Week 1	Lab 1: Getting started with MATLAB.

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
Week 2	Lab 2: Continuous-time and Discrete-time signals.
Week 3	Lab 3: Numerical Integral.
Week 4	Lab 4: Converting Signals.
Week 5	Lab 5: Signal Transformation and Plotting
Week 6	Lab 6: Impulse representation
Week 7	Lab 7: Convolution.
Week 8	Lab 8: Fourier Transform.
Week 9	Lab 9: Fast Fourier Transform part 1.
Week 10	Lab 10: Fast Fourier Transform part 2
Week 11	Lab 11: Recursive smoother.
Week 12	Lab 12: Averaging filter.
Week 13	Lab 13: Recursive smoother.
Week 14	Lab 14: Review
Week 15	presentation
Week 16	**Final Exam**

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	BASIC digital signal processing (GB Lockhart &BMG CHeetham Digital signal processing (Alan V. Oppenheim	Yes
Recommended Texts		

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D -Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Fundamentals of Cloud Computing

Module Information			
Module Title	**Fundamentals of Cloud Computing**	**Module Delivery**	
Module Type	**Core**	☐ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**BCYSCE303-S1**		
ECTS Credits	**6**		
SWL (hr/sem)	**150**		
Module Level	1	**Semester of Delivery**	1
Administering Department	Cyber Security and Cloud Computing	**College**	Technical Engineering College for computer and AI / Mosul

		Techniques Engineering			
Module Leader	Name		**e-mail**	E-mail	
Module Leader's Acad. Title		Professor	**Module Leader's Qualification**		Ph.D.
Module Tutor	Name (if available)		**e-mail**	E-mail	
Peer Reviewer Name		Name	**e-mail**	E-mail	
Scientific Committee Approval Date		25/10/2024	**Version Number**		1.0

Relation with other Modules			
Prerequisite module	**Cloud computing security** **BCYSCCET301-S2**e	**Semester**	
Co-requisites module	**Cloud application** **BCYSCCET403-S1**	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	1. Understanding the basic concepts and components of cloud computing, such as virtualization, scalability, and on-demand self-service. 2. Familiarizing with various deployment models of cloud computing, such as public, private, and hybrid clouds, and their advantages and disadvantages. 3. Exploring the different service models of cloud computing, such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), and when to use each of them. 4. Understanding the security, privacy, and compliance issues related to cloud computing and the measures taken to mitigate them. 5. Understanding the economic and business aspects of cloud computing, such as cost-benefit analysis, pricing models, and vendor lock-in. 6. Familiarizing with the different cloud providers and their specific features and services.
Module Learning Outcomes	1-Explain the basic concepts and components of cloud computing, 2-Differentiate between various deployment models of cloud computing, such as public, private, and hybrid clouds, and identify their advantages and disadvantages. 3- Compare and contrast the features and services of different cloud providers and select the appropriate provider for a given scenario. 4- Evaluate the key trends and latest developments in cloud computing, such as serverless computing, edge computing, and multi-cloud strategies, and identify their potential applications in various industries.

Learning and Teaching Strategies

Strategies	1-Starting with the basics: Cloud computing can be a complex topic, so it's important to start with the basics. This includes understanding the key concepts and terminology, such as virtualization, scalability, elasticity, and service models. 2. Hands-on experience: One of the most effective ways to learn cloud computing is through hands-on experience. This can involve setting up and using cloud services, experimenting with different configurations, and troubleshooting issues. 3-Establishing cloud security and compliance: Cloud security and compliance are critical considerations when deploying cloud solutions. Establishing the appropriate security measures and compliance standards can help you protect your data and meet regulatory requirements.

Student Workload (SWL)

Structured SWL (h/sem)	64	**Structured SWL (h/w)**	4
Unstructured SWL (h/sem)	86	**Unstructured SWL (h/w)**	6
Total SWL (h/sem)	**150**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	4	10% (10)	5 ,8,10,13	LO #1, #2 and #10, #11
	Assignments	7	10% (10)	2 ,4,5,8,9,11,12	LO #3, #4 and #6, #7
	Projects / Lab.	15	10% (10)	Continuous	All
	Report	14	10% (10)	Continuous	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

	Material Covered
Week 1	Introduction - Difference between Circuit Theory and Field Theory
Week 2	Basics of Network Elements
Week 3	Resistance and Resistivity, Ohm's Law and Inductance, Capacitance
Week 4	Review of Kirchhoff's Laws, Circuit Analysis - Nodal and Mesh
Week 5	Linearity and Superposition, Source Transformations, Thévenin and Norton Equivalents

Week 6	Review of Inductor and Capacitor as Circuit Elements, Source-free RL and RC Circuits, Transient Response
Week 7	Mid-term Exam + Unit-Step Forcing, Forced Response, the RLC Circuit
Week 8	Sinusoidal Forcing, Complex Forcing, Phasors, and Complex Impedance, Sinusoidal Steady State Response
Week 9	Nodal and Mesh Revisited, Average Power, RMS, Introduction to Polyphase Circuits
Week 10	Mutual Inductance, Linear and Ideal Transformers, Circuits with Mutual Inductance
Week 11	Frequency Response of Series/Parallel Resonances, High-Q Circuits
Week 12	Complex Frequency, s-Plane, Poles and Zeros, Response Function, Bode Plots
Week 13	Two Port Networks, Admittance, Impedance, Hybrid, and Transmittance Parameters
Week 14	Two Port Networks, Admittance, Impedance, Hybrid, and Transmittance Parameters

Delivery Plan (Weekly Lab. Syllabus)

Week 1	**Lab 1: Getting Started**
Week 2	**Lab 2: Virtual Machine concept**
Week 3	**Lab 3: Cloud Computing Framework**
Week 4	**Lab 4: Configuration of Virtual Machine.**
Week 5	**Lab 5: virtual block to virtual machines**
Week 6	**Lab 6: Hadoop Concept**
Week 7	**Lab 7: Installation and configuration with Hadoop**
Week 8	**Lab 8: Cloud Computing Services - Software as a Service (SaaS) - Case study.**
Week 9	**Lab 9: Cloud Computing Services - Infrastructure as a Service (IaaS) - Case study.**
Week 10	**Lab 10: Cloud Computing Services - Platform as a Service (PaaS) Case study.**
Week 11	**Lab 11: Virtualization**
Week 12	**Lab 12: Case Study: Software Defined Networks (SDN) Software Defined Storage (SDS)**
Week 13	**Lab 13: Case Study: Software Defined Storage (SDS)**
Week 14	**Lab 14: Project and Presentation**
Week15	**review**
Week16	**Final Exam**

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Fundamentals of Electric Circuits, C.K. Alexander and M.N.O Sadiku, McGraw-Hill Education	Yes
Recommended Texts	DC Electrical Circuit Analysis: A Practical Approach Copyright Year: 2020, dissidents.	No
Websites	https://www.coursera.org/browse/physical-science-and-engineering/electrical-engineering	

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Mobile and Wireless Networks

Module Information		
Module Title	**Mobile and Wireless Networks**	**Module Delivery**
Module Type	**Core**	☒ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical**
Module Code	**BCYSCE304-S1**	
ECTS Credits	5	

SWL (hr/sem)	**125**	**☒ Seminar**	
Module Level	3	**Semester of Delivery**	2
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Lecturer Assist. Rana Kh. Sabri	**e-mail**	E-mail
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	$MS_{C.}$
Module Tutor		**e-mail**	mti.lec39.rana@ntu.edu.iq
Peer Reviewer Name		**e-mail**	
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules			
Prerequisite module		**Semester**	
Co-requisites module	Mobile and Wireless Networks Security (BCYSCE300-S2)	**Semester**	2

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	1. Understanding Mobile and Wireless Network Architectures 2. Learning Wireless Communication Technologies 3. Exploring Mobile Network Protocols 4. Understanding Mobile IP and Mobile Routing 5. Learning Mobile Application Development 6. Practical skills are essential in understanding mobile and wireless networks.
Module Learning Outcomes	1. Understanding of Wireless Communication Technologies 2. Knowledge of Mobile Network Architectures 3. Proficiency in Mobile IP and Mobile Routing 4. Familiarity with Network Protocols and Standards 5. Proficiency in Mobile Application Development 6. Practical Skills in Configuring and Managing Mobile and Wireless Networks 7. Effective Communication and Collaboration
Learning and Teaching Strategies	
Strategies	1. Lectures and Presentations: Lectures and presentations are often used to deliver theoretical concepts, principles, and foundational knowledge related to computer networking. 2. Hands-on Lab Sessions: Practical lab sessions are essential for allowing students to apply theoretical knowledge and gain hands-on experience in configuring, troubleshooting, and managing computer networks. 3. Group Projects and Collaborative Learning: Group projects and collaborative learning activities promote teamwork, communication, and the exchange of ideas among students. 4. Online Discussion Forums: Online discussion forums or platforms provide an opportunity for students to engage in asynchronous discussions, ask questions, and share knowledge and resources related to computer networking. 5. Simulations and Virtual Environments: Network simulation tools and virtual environments can be used to create simulated network scenarios, allowing students to experiment and practice without the need for physical equipment. 6. Continuous Learning Resources: Providing additional resources, such as textbooks, online tutorials, reference materials, and interactive learning modules, supports students' independent learning and exploration of advanced networking topics beyond the scope of the module.

Student Workload (SWL)			
Structured SWL (h/sem)	64	**Structured SWL (h/w)**	4
Unstructured SWL (h/sem)	61	**Unstructured SWL (h/w)**	4
Total SWL (h/sem)	**125**		

Module Evaluation					
As		**Time/ Number**	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	6	10% (10)	3, 5, 10, 12	LO #2, #5 and #10, #11
	Assignments	2	10% (10)	2 ,4, 8, 12	LO #3, #4 and #6, #7
	Projects / Lab.	15	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #6
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	**Wireless local area networks**
2	**Fundamental concepts of wireless networks**
3	**Wireless LANs** • The 802.11 Architecture, The 802.11 MAC Protocol, The IEEE 802.11 Frame, Mobility in the Same IP Subnet, Advanced Features in 802.11
4	**Wireless and Mobile Networks** • Introduction, Wireless Links and Network Characteristics, CDMA
5	**Mobile device communications and characteristics** • Components of a digital communications system • Digital Signaling • Spread Spectrum Signals • Multi-User Communication Access Techniques • CDMA, TDMA, FDMA, SDMA, PDMA
6	**Bluetooth**
7	**RFIDs**
8	**Cellular Networks**: • 4G and 5G, An Overview of Cellular Network Architecture, 4G: LTE, 5G
9	**Mobility Management**: • Principles, Device mobility: a network-layer perspective, Home Networks and Roaming on Visited Networks, Direct and Indirect Routing to/from a Mobile Device
10	**Mobility Management** • Mobility Management in Practice, Mobility Management in 4G/5G Networks, Mobile IP
11	**Wireless and Mobility**: • Impact on Higher-Layer Protocols
12	**Wireless sensor networks**
13	**Telecommunication architectures and protocols for wireless sensor network**
14	**Issues in ad-hoc and sensor networks** • including power management, coverage, topology, and location discovery
15	**Review**
16	**Final Exam**
	Delivery Plan (Weekly Lab. Syllabus)
	Material Covered

1	**Lab 1: Getting Started**
2	**Lab2: Introduction to packet tracer**
3	**Lab 3: Setting up Wireless Network**
4	**Lab 4: Wireless networks Example 1**
5	**Lab 5: Wireless networks Example 2**
6	**Lab 6: Establishing a 4G & 5G mobile network**
7	**Lab 7: Wireless and Mobile Networks**
8	**Lab 8: Bluetooth**
9	**Lab 9: RFIDs**
10	**Lab 10: Wireless sensor networks**
11	**Lab 11: Creating Ad-Hok Network**
12	**Lab 12: Home Networks and Roaming**
13	**Lab 13: Communication Access Techniques**
14	**Lab 14: location discovery**
15	**Lab 15: Review**
16	**Final Exam**

earning and Teaching Resources		
	Text	**Available in the Library?**
equired Texts	1. Computer Networking: A Top-Down Approach, 8th edition" by James Krose and Keith Ross. 2. Wireless and Mobile Network Architectures by Yi-Bing Lin and Imrich Chlamtac 3. Wireless Networks and Mobile Computing by Asoke K. Talukder and Roopa R. Yavagal 4. Wireless and Mobile Network Security by Hakima Chaouchi	Yes
Websites	https://www.youtube.com/playlist?list=PL8z1B2A0yYsEOSDpZ1cVg3TpwJxxUxtGE	

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Introduction to Hardware security

Module Information					
Module Title	**Introduction to Hardware security**			**Module Delivery**	
Module Type	**Core**			☐ **Theory** ☒ **Lecture** ☐ **Lab** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**BCYSCE305-S1**				
ECTS Credits	**6**				
SWL (hr/sem)	**150**				
Module Level	4		**Semester of Delivery**	5	
Administering Department	Cyber Security and Cloud Computing Techniques Engineering		**College**	Technical Engineering College for computer and AI / Mosul	
Module Leader	Name		**e-mail**	rabdulhammed@ntu.edu.iq	
Module Leader's Acad. Title	Lecturer		**Module Leader's Qualification**	Ph.D.	
Module Tutor	Name (if available)		**e-mail**	E-mail	
Peer Reviewer Name	Name		**e-mail**	E-mail	
Scientific Committee Approval Date	25/10/2024		**Version Number**	1.0	

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	To learn Fundamentals of hardware security and trust for integrated circuits and systems, cryptographic hardware, invasive and non-invasive attacks, side-channel attacks, physically unclonable functions (PUFs), true random number generation (TRNG), watermarking of Intellectual Property (IP) blocks, counterfeit ICs, hardware Trojans in electronic circuits (IP cores and ICs).
Module Learning Outcomes	34. Describe in-depth a trustworthy security system for hardware and its constituent components. 35. Develop a security system for hardware. 36. Understand the topics of digital and analog hardware. 37. Understand physical attacks and tamper resistance. 38. Gain knowledge of the reverse engineering of embedded microcontroller devices. 39. Understand how to teach FPGA security to electrical engineering students. 40. Understand the foundational course for Information Technology, including hardware technology
Indicative Contents	Indicative content includes the following. Introduction to hardware security Users & Permissions Security Based on PUFs and TRNGs Linux Services Physical Attacks and Fault Injection Attacks PCB Security Hardware Trojans Physical unclonable functions VLSI Testing

Learning and Teaching Strategies	
Strategies	The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)			
Structured SWL (h/sem)	64	**Structured SWL (h/w)**	4
Unstructured SWL (h/sem)	86	**Unstructured SWL (h/w)**	6
Total SWL (h/sem)	**150**		

Module Evaluation				
As	**Time/Number**	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**

Formative assessment	**Quizzes**	2	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus) Key Learning Outcomes	
Week	**Material Covered**
Week 1	Introduction to hardware security, Emerging applications and the new threats, Basics of VLSI Design
Week 2	Security Based on PUFs and TRNGs, Hardware Metering, Watermarking of HW Ips
Week 3	Physical Attacks and Fault Injection Attacks
Week 4	PCB Security, Basics of PCB Security
Week 5	Side Channel Attacks and Countermeasures
Week 6	Hardware Trojans: IC Trust (Taxonomy and Detection
Week 7	Hardware Trojans: IP Trust (Detection) + Design for Hardware Trust
Week 8	Counterfeit Detection and Avoidance
Week 9	Protecting against Scan-based Side Channel Attacks
Week 10	Physical unclonable functions: design principles and applications;
Week 11	Physical unclonable functions: Random Number Generators: design principles and applications Design and Evaluate PUFs and Random Number Generators
Week 12	Side Channel Attacks and Countermeasures: Overview; Fault attacks and countermeasures; Power attacks and countermeasures, Design a fault attack and evaluate a countermeasure, Countermeasures for Embedded Microcontrollers
Week 13	VLSI Testing is a portal for hackers: attacks
Week 14	VLSI Testing is a portal for hackers: countermeasures
Week 15	Review
Week 16	**Preparatory week before the final Exam**

Delivery Plan (Weekly Lab. Syllabus)	
Week	**Material Covered**
Week 1	Lab 1: Introduction to Agilent VEE and PSPICE
Week 2	Lab 2: Thévenin's / Norton's Theorem and Kirchhoff's Laws
Week 3	Lab 3: First-Order Transient Responses
Week 4	Lab 4: Second-Order Transient Responses
Week 5	Lab 5: Frequency Response of RC Circuits
Week 6	Lab 6: Frequency Response of RLC Circuits
Week 7	Lab 7: Filters

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Introduction to Hardware Security and Trust by Mohammad Tehrani poor and Cliff Wan.	Yes
Recommended Texts		No
Websites		

Grading Scheme مخطط الدرجات			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Engineering Analysis

Module Information				
Module Title	**Engineering Analysis**		**Module Delivery**	
Module Type	**Core**		☒**Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☐**Seminar**	
Module Code	**BCYSCE303-S2**			
ECTS Credits	**4**			
SWL (hr/sem)	**100**			
Module Level	UGx11 3	**Semester of Delivery**	2	
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul	
Module Leader	Asst. Lecturer Afaf Nasser	**e-mail**	E-mail	
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	MSc	
Module Tutor		**e-mail**	Afaf.nasser@ntu.edu.iq	

Peer Reviewer Name		**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules			
Prerequisite module	Math (BCYSCE100-S1) Discrete Math (BCYSCE205-S1)	**Semester**	1
Co-requisites module		**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	6. Understanding of mathematical and statistical concepts relevant to engineering analysis. 7. Learning Analytical Techniques: Students should learn various analytical techniques used in engineering analysis. 8. Familiarity with Simulation and Modeling: Students should gain knowledge and skills in developing engineering models and simulations. 9. Proficiency in Data Analysis: Students should learn how to collect, organize, and analyze data relevant to engineering problems. 10. Application of Engineering Principles: Students should be able to apply engineering principles. 11. Awareness of Error and Uncertainty: Students should develop an understanding of the sources of error and uncertainty in engineering analysis. 12. Effective Communication of Analysis Results: Students should be able to effectively communicate their analysis results to technical and non-technical audiences. 13. Ethical Considerations: Students should be aware of the ethical considerations in engineering analysis.
Module Learning Outcomes	26. Understanding the fundamentals of Engineering Analysis including terminology and processes. 27. Proficiency in Numerical Methods and Computational Techniques. 28. Understanding of Uncertainty and Error Analysis in engineering. 29. Ability to Interpret and Communicate Analysis Results in the context of engineering problems. 30. Critical Thinking and Problem-Solving Skills and the ability to approach engineering problems analytically.

Learning and Teaching Strategies

Strategies	1. Lectures and Presentations: Lectures are commonly used to present foundational concepts, theories, and methodologies in engineering analysis. 2. Practical Assignments and Problem-Solving Exercises: Hands-on assignments and problem-solving exercises allow students to apply the concepts learned in class to real-world engineering problems. 3. Case Studies and Real-World Examples: Presenting case studies and real-world examples helps students connect theoretical concepts with practical applications. By analyzing and discussing real-world engineering 4. Group Projects and Collaborative Learning: Group projects encourage collaboration and teamwork among students.

Student Workload (SWL)			
Structured SWL (h/sem)	63	**Structured SWL (h/w)**	4
Unstructured SWL (h/sem)	37	**Unstructured SWL (h/w)**	2
Total SWL (h/sem)	**100**		

Module Evaluation

As		**Time/ Number**	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	2	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Assignments	5	10% (10)	2,4,8,9,10	LO #3, #4 and #6, #7
	Projects / Lab.	15	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)	
Week	**Material Covered**
Week 1	**Fourier transform** • Introduction to Fourier transform • Definition and properties
Week 2	**Fourier transform** • theorems • applications**.**
Week 3	**Z-transform** • Introduction to Z-transform • Definition and properties
Week 4	**Z-transform** • Theorems • applications
Week 5	**Numerical computations** • Introduction to numerical computations. • bisection method.
Week 6	**Numerical computations** • false position method • Newton-Raphson method
Week 7	**solution of algebraic and transcendental equations**
Week 8	**solution of linear simultaneous equations** • Introduction to the solution of linear simultaneous equations • Direct methods
Week 9	**Direct methods** • Gauss elimination • Gauss Jordan
Week 10	**Iterative method** • Introduction to Iterative method • Jacobi’s • Gauss-seidel iteration
Week 11	**Solution of nonlinear equation** • Introduction to the solution of nonlinear equation. • Newton-Raphson method.
Week 12	**Numerical solution of ordinary differential equation** • Introduction to Numerical solution of ordinary differential equation. • Picard's method. • Euler's method.
Week 13	**Matrices** • Introduction to Matrices • Matrix operations • related matrices
Week 14	**solution of a linear system of equations**

	• Introduction to solution of a linear system of equations. • linear transformations • Cayley-Hamilton theorem
Week 15	**Review**
Week 16	**Final Exam**

Delivery Plan (Weekly Lab. Syllabus)	
Week	**Material Covered**
Week 1	Lab 1: Getting Started
Week 2	Lab 2: Exploring MATLAB environment
Week 3	Lab 3: Introduction to MATLAB
Week 4	Lab 4: Exploring Fourier transform in MATLAB
Week 5	Lab 5: Fourier transform Applications in solving Engineering problem
Week 6	Lab 6: Exploring Z-transform
Week 7	Lab 7: Z-transform Application in solving Engineering problem
Week 8	Lab 8: solving Engineering problem using Gauss elimination
Week 9	Lab 9: solving Engineering problem using Gauss Jordan.
Week 10	Lab 10: solving Engineering problem using Jacobi's
Week 11	Lab 11: Solving equation using Gauss-seidel iteration
Week 12	Lab 12: Matrixes in MATLAB
Week 13	Lab 13: Matrixes operation in MATLAB
Week 14	Lab ١٤: Cayley-Hamilton theorem
Week 15	Lab ١٥: Review and presentation
Week 16	**Final Exam**

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Applied Engineering Analysis by Tai-Ran Hsu	Yes
Recommended Texts	Bolz, R. E. (1973). CRC handbook of tables for applied engineering science.	Yes
Websites		

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors

	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Wireless and Mobile Network security

Module Information					
Module Title	**Wireless and Mobile Network security**			**Module Delivery**	
Module Type	**Core**			☒**Theory** ☐**Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**BCYSCE300-S2**				
ECTS Credits	**5**				
SWL (hr/sem)	**125**				
Module Level		UGx11 3	**Semester of Delivery**		2
Administering Department		Cyber Security and Cloud Computing Techniques Engineering	**College**		Technical Engineering College for computer and AI / Mosul
Module Leader	Dr.Razan Abdulhammed		**e-mail**		rabdulhammed@ntu.edu.iq
Module Leader's Acad. Title		Lecturer	**Module Leader's Qualification**		PhD.
Module Tutor	None		**e-mail**		None
Peer Reviewer Name		Name	**e-mail**		None
Scientific Committee Approval Date		25/10/2024	**Version Number**		1.0

Relation with other Modules			
Prerequisite module	Mobile and wireless Networks (BCYSCE304-S1)	**Semester**	1
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	1. Understanding the concepts of mobile and wireless networks. 2. Understanding the security threats and attacks in mobile and wireless networks. 3. Understanding the security mechanisms and protocols in mobile and wireless networks. 4. Developing skills in mobile and wireless network security. 5. Understanding the legal and ethical issues in mobile and wireless network security.
Module Learning Outcomes	1. Communicating mobile and wireless network security concepts: Students should be able to communicate mobile and wireless network security concepts effectively through written reports, presentations, and other forms of communication. 2. Identifying security threats and attacks in mobile and wireless networks: Students should be able to identify and describe the various types of security threats and attacks that can occur in mobile and wireless networks, such as eavesdropping, man-in-the-middle attacks, denial-of-service attacks, and malware attacks. 3. Understanding security mechanisms and protocols in mobile and wireless networks: Students should be able to describe the security mechanisms and protocols used to protect mobile and wireless networks, such as encryption, authentication, access control, and firewalls. 4. Applying security principles to mobile and wireless network design: Students should be able to design and implement secure mobile and wireless networks, and understand how to identify and mitigate security threats and attacks. 5. Understanding legal and ethical issues in mobile and wireless network security: Students should be able to demonstrate an understanding of the legal and ethical issues related to mobile and wireless network security, such as privacy, data protection, and intellectual property rights.

Learning and Teaching Strategies	
Strategies	1- Lectures: Lectures are a common teaching strategy for introducing students to the concepts, threats, and security mechanisms related to mobile and wireless networks. Lectures may be delivered in person or online, and may include multimedia such asslides and videos. 2- Laboratory sessions: Laboratory sessions provide students with hands-on experience in designing and implementing secure mobile and wireless networks. These sessions may be conducted in a physical laboratory or through online simulation tools. 3- Online resources: Online resources such as interactive simulations, virtual labs, and video tutorials can be used to supplement lectures and laboratory sessions, and to provide students with additional opportunities to practice and apply their knowledge. 4- Assignments and assessments: Assignments and assessments such as quizzes, exams, and project reports can be used to evaluate students' understanding of the course material and their ability to apply their knowledge and skills to practical problems. 5- Guest lectures: Inviting guest lecturers who are experts in mobile and wireless network security can provide students with real-world examples and insights into the field.

Student Workload (SWL)			
Structured SWL (h/sem)	64	**Structured SWL (h/w)**	4
Unstructured SWL (h/sem)	61	**Unstructured SWL (h/w)**	4
Total SWL (h/sem)	**125**		

Module Evaluation

As		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	2	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #6
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	**Introduction to Wireless Networks** • Overview of wireless networks • Wireless network architecture • Wireless network protocols • Wireless network security threats
2	**Introduction to Wireless and Mobile Networks** • Overview of wireless and mobile networks • Security challenges in wireless and mobile networks • Security goals and requirements for wireless and mobile networks
3	**Wireless Network Security Mechanisms** • Security mechanisms in wireless networks • Cryptography in wireless networks • Authentication and access control in wireless networks • Security protocols in wireless networks
4	**Wireless Network Security Protocols** • Wi-Fi security protocols (WEP, WPA, WPA2) • Security mechanisms for wireless ad hoc networks
5	**Mobile Network Security** • Mobile network architecture • Mobile network protocols • Mobile network security threats • Mobile network security mechanisms
6	**Mobile Network Security Protocols** • GSM security protocols. • GSM security threats
7	**Mobile Network Security Protocols** • 3G and 4G security protocols • 3G and 4G security threats
8	**Midterm Exam**
9	**Mobile Network Security Protocols** • LTE security protocols. • LTE security threats. • LTE Security tools.
10	**Mobile Device Security** • Mobile device security threats • Mobile device management (MDM) • Mobile application security
11	**Bluetooth Security**

	• Bluetooth security protocols • Bluetooth security threats.
12	**Bluetooth Security** **• Bluetooth security mechanisms** • Bluetooth security tools
13	**WiMAX Security** • WiMAX security mechanisms • WiMAX security tools
14	**RFID Security** • RFID security protocols. • RFID security threats. • RFID security mechanisms. • RFID security tools
15	Review and Student presentation
16	**Final Exam**

	Delivery Plan (Weekly Lab. Syllabus)
WEEK	**Material Covered**
1	Lab 1: Getting started
2	Lab 2: Wi-Fi security protocols (WEP)
3	Lab 3: Wi-Fi security protocols (WPA).
4	Lab 4: Wi-Fi security protocols (WPA2) - Case 1
5	Lab 5: Wi-Fi security protocols (WPA2) - Case 2
6	Lab 6: GSM.
7	Lab 7: 3G
8	Lab 8: 4G
9	Lab 9 : 5 G
10	Lab 10: WiMAX.
11	Lab 11: Bluetooth
12	Lab 12: RFID.
13	Lab 13: LTE.
14	Lab 14: Review and Student presentation1.
15	Lab 14: Review and Student presentation2.
16	Final Exam

Learning and Teaching Resource		
	Text	**Available in the Library?**

Required Texts	" Wireless Network Security: A Beginner's Guide" by Tyler Wrightson.	Yes
Recommended Texts	"Computer Networking: A Top-Down Approach" by James F. Kurose and Keith W. Ross.	Yes
Websites		

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 -69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Electrical Circuits

Module Information				
Module Title	**Electrical Circuits**			**Module Delivery**
Module Type	**Core**			☐ **Theory**
Module Code	**BCYSCE301-S2**			☒ **Lecture**
ECTS Credits	**8**			☒ **Lab**
SWL (hr/sem)	**175**			☐ **Tutorial**
				☐ **Practical**
				☒ **Seminar**
Module Level	UGx11 3	**Semester of Delivery**	6	
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul	

Module Leader	Dr. Razan Abdulhammed	**e-mail**	rabdulhammed@ntu.edu.iq
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	Ph.D.
Module Tutor	Dr. Razan Abdulhammed	**e-mail**	rabdulhammed@ntu.edu.iq
Peer Reviewer Name	Name	**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	50. Cloud Security: Understand the importance of security in cloud computing and learn about various security measures and best practices for protecting cloud-based systems and data. 51. Cloud Storage and Networking: Explore cloud storage solutions and networking concepts relevant to cloud computing. Learn about data management, data backup, and network connectivity in the cloud. 52. Cloud Migration and Integration: Gain knowledge of strategies and techniques for migrating existing systems and applications to the cloud. Understand how to integrate cloud-based services with on-premises infrastructure. 53. Cloud Management and Monitoring: Learn about cloud management tools and techniques for provisioning, monitoring, and optimizing cloud resources. Understand how to manage performance, scalability, and cost in the cloud. 54. Cloud Service Providers: Familiarize yourself with major cloud service providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Understand their offerings, features, and pricing models. 55. Emerging Trends and Future Directions: Stay up to date with the latest trends and advancements in cloud computing. Explore emerging technologies and concepts shaping the future of cloud computing.
Module Learning Outcomes	41. Understand the identity and access management practices of both cloud providers and consumers.

	42. Understand how to protect data-at-rest, data-in-transit, and data-in-use within a cloud environment. 43. Understand standard cloud security network designs and architecture models. 44. Identify different cloud delivery models. 45. Evaluate security features offered by public cloud providers. 46. Build cloud infrastructure with security in mind. 47. Understand cloud computing models, security, and privacy. 48. Make sense of different cloud-based services 49. Understand and analyze risk in the cloud. 50. Interact with Azure and AWS environments using a secure approach
Indicative Contents	Introduction to Cloud Computing Foundations of Cloud Security Cloud Computing Security Fundamentals Cloud Infrastructure Security Cloud Data Security Cloud Security Operations and Management Cloud Secure server configuration and integrated access management Advanced Cloud Security

Learning and Teaching Strategies	
Strategies	1. Lectures: In-depth presentations by instructors covering theoretical concepts and practical examples. 2. Tutorials: Interactive sessions to reinforce understanding through problem-solving and discussions. 3. Practical Exercises: Hands-on activities and lab sessions to gain practical experience in using cloud computing technologies. 4. Case Studies: Analysis of real-world cloud computing implementations and scenarios. 5. Group Projects: Collaborative projects to design and develop cloud-based solutions.

Student Workload (SWL)			
Structured SWL (h/sem)	109	**Structured SWL (h/w)**	7
Unstructured SWL (h/sem)	91	**Unstructured SWL (h/w)**	6
Total SWL (h/sem)	**200**		

Module Evaluation				
As	**Time/Number**	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**

Formative assessment	**Quizzes**	2	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)	
Week	**Material Covered**
Week 1	Introduction to Cloud Computing Overview of Cloud Computing Cloud Computing Architecture Cloud Service Models.
Week 2	Foundations of Cloud Security Introduction to Cloud Security Cloud Security Architecture Cloud Security Controls Cloud Security Compliance and Regulations Cloud Security Risk Management
Week 3	Cloud Computing Security Fundamentals Cloud Computing Security Threats and Attacks Cloud Computing Security Controls
Week 4	Cloud Computing Security Fundamentals Cloud Computing Security Standards and Regulations Cloud Computing Security Best Practices
Week 5	Cloud Infrastructure Security Cloud Infrastructure Security Architecture Cloud Infrastructure Security Controls
Week 6	Cloud Infrastructure Security Cloud Infrastructure Security Best Practices Cloud Infrastructure Security Management
Week 7	Cloud Data Security Cloud Data Security Architecture Cloud Data Security Controls
Week 8	Cloud Data Security Cloud Data Security Best Practices Cloud Data Security Management
Week 9	Cloud Application Security Cloud Application Security Best Practices Cloud Application Security Management
Week 10	Cloud Application Security Cloud Application Security Best Practices Cloud Application Security Management
Week 11	Cloud Security Operations and Management Cloud Security Operations Cloud Security Management
Week 12	Cloud Security Operations and Management Cloud Security Incident Response Cloud Security Auditing and Compliance
Week 13	Cloud Secure server configuration and integrated access management

Week 14	Cloud Security Operations Cloud Security Incident Response Cloud Security Monitoring and Logging Cloud Security Automation Cloud Security Assessment and Auditing Cloud Security Governance
Week 15	Advanced Cloud Security Cloud Security Threats and Vulnerabilities Cloud Security Best Practices Cloud Security Strategy and Planning Cloud Security Tools and Technologies Cloud Security Case Studies
Week 16	**Preparatory week before the final Exam**

Delivery Plan (Weekly Lab. Syllabus)	
Week	**Material Covered**
Week 1	**Lab 1: Introduction to Cloud Platforms** • **Setting up accounts on major cloud platforms (e.g., AWS, Azure, GCP)** • **Navigating the cloud platform interfaces** Deploying a basic virtual machine instance
Week 2	**Lab 2:** Virtualization and Containerization • Creating and managing virtual machines using hypervisors (e.g., VirtualBox) • Exploring containerization with Docker **Building and running containers locally**
Week 3	**Lab 3:** Cloud Storage • Setting up and configuring cloud storage services (e.g., Amazon S3, Azure Blob Storage) • Uploading and downloading files from cloud storage **Implementing data replication and backup strategies**
Week 4	**Lab 4:** Networking in the Cloud • Configuring virtual networks and subnets • Creating security groups and access control rules **Establishing VPN connections between on-premises and cloud environments**
Week 5	**Lab 5:** Serverless Computing • Deploying serverless functions using AWS Lambda or Azure Functions • Integrating serverless functions with other cloud services (e.g., S3, API Gateway) **Monitoring and troubleshooting serverless applications.**
Week 6	**Lab 6:** Cloud Database Management • Creating and managing relational databases (e.g., Amazon RDS, Azure SQL Database) • Exploring NoSQL databases (e.g., DynamoDB, Cosmos DB) **Performing data backups and restores**
Week 7	**Lab 7:** Infrastructure as Code • Introduction to Infrastructure as Code (IaC) tools like Terraform or AWS CloudFormation • Writing IaC templates to provision cloud resources.
Week 8	**Lab 8**Infrastructure as Code • Automating resource deployment and updates
Week 9	**Lab 9:** Cloud Security and Identity Management • Configuring identity and access management (IAM) policies • Implementing multi-factor authentication (MFA) for cloud accounts **Enforcing security best practices and monitoring for security breaches**
Week 10	**Lab 10**: Load Balancing and Auto Scaling • Configuring load balancers for distributing traffic (e.g., AWS ELB, Azure Load Balancer) • Setting up auto scaling to dynamically adjust resources based on demand **Testing load balancing and auto scaling scenarios**
Week 11	**Lab 11**: Continuous Integration and Deployment (CI/CD) Implementing a CI/CD pipeline using tools like Jenkins or AWS CodePipeline Automating the build, test, and deployment of cloud-based applications

	Integrating version control systems (e.g., Git) with CI/CD processes
Week 12	**Lab 12**: Cloud Monitoring and Logging • Implementing monitoring and logging services (e.g., AWS CloudWatch, Azure Monitor) • Configuring alerts and notifications for resource monitoring **Analyzing logs and performance metrics for troubleshooting**
Week 13	**Lab 13**: Cloud Cost Optimization • Monitoring and analyzing cloud costs using cost management tools (e.g., AWS Cost Explorer, Azure Cost Management) • Implementing cost optimization techniques (e.g., rightsizing, scheduling) **Estimating and optimizing cloud resource usage for cost-efficiency**
Week 14	Cloud Cost Optimization • Estimating and optimizing cloud resource usage for cost-efficiency
Week 15	**Review and Student presentation**
Week 16	Final Exam

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Fundamentals of Electric Circuits, C.K. Alexander and M.N.O Sadiku, McGraw-Hill Education	Yes
Recommended Texts	DC Electrical Circuit Analysis: A Practical Approach Copyright Year: 2020, dissidents.	No
Websites	https://www.coursera.org/browse/physical-science-and-engineering/electrical-engineering	

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Operating Systems Security

Module Information					
Module Title	**Operating Systems Security**			**Module Delivery**	
Module Type	**Core**			**Theory** **☒ Lecture** **☒ Lab** **Tutorial** **Practical** **☒ Seminar**	
Module Code	**BCYSCE302-S2**				
ECTS Credits	**5**				
SWL (hr/sem)	**150**				
Module Level	UGx11 3		**Semester of Delivery**	6	
Administering Department	Cyber Security and Cloud Computing Techniques Engineering		**College**	Technical Engineering College for computer and AI / Mosul	
Module Leader	Dr. Razan Abdulhammed		**e-mail**	rabdulhammed@ntu.edu.iq	
Module Leader's Acad. Title	Lecture		**Module Leader's Qualification**	Ph.D.	
Module Tutor	Dr. Zakaria Noor Aldeen Mahmood		**e-mail**	E-mail	
Peer Reviewer Name	Name		**e-mail**	E-mail	
Scientific Committee Approval Date	25/10/2024		**Version Number**	1.0	

Relation with other Modules العلاقة مع المواد الدراسية الأخرى			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	56. To introduce students to a broad range of operating system security topics including system security plans, security design, security threats and risks, system and application security tools, implementation of security plan, system monitoring and audit logs and resolution of any security breach.
Module Learning Outcomes	51. Understand the main concepts of advanced operating systems, including parallel processing systems. 52. Acquire a basic understanding of operating systems, including their role, types, and batch systems.

	53. Describe the services an operating system provides to users, processes, and other systems, and discuss the various ways of structuring an operating system. 54. Acquire the basic operating system concepts such as processes and threads. 55. Understand the fundamental concepts of operating systems, including OS structures, processes/threads, memory management, and file systems. 56. Gain a general understanding of the structure of modern computers, the purpose, structure, and functions of operating systems, and illustrate key OS concepts.
Indicative Contents	Indicative content includes the following. Protection system. (15hrs) system security principles. (10hrs) Classical and Modern approaches to system security. (10hrs) Access control. (6hrs) System vulnerabilities. (15hrs) System Memory protection. (6hrs) System Auditing. (10hrs) system security plans. (8hrs)

Learning and Teaching Strategies	
Strategies	The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials.

Student Workload (SWL)			
Structured SWL (h/sem)	64	**Structured SWL (h/w)**	4
Unstructured SWL (h/sem)	61	**Unstructured SWL (h/w)**	4
Total SWL (h/sem)	**200**		

Module Evaluation				
As	**Time/Number**	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**

Formative assessment	**Assignments**	4	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Seminar	3	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)	
Week	**Material Covered**
Week 1	Protection systems
Week 2	Foundational system security principles
Week 3	Classic approaches to system security
Week 4	System vulnerabilities, Real-world vulnerabilities (buffer overflow), Threats and exploits (gaining remote shell)
Week 5	Access control overview, Mandatory access control in common OS , in research and commercial operating systems
Week 6	Address space randomization
Week 7	Memory protection and Virtual machine introspection (VMI)
Week 8	system security plans, Backup and restore
Week 9	Auditing and Protection systems
Week 10	Malware overview, detection and analysis, and malware immunization
Week 11	File system management and utilities
Week 12	Mail facility, Pipes, redirection, and filters
Week 13	Hardware and software constructs that protect modern operating systems
Week 14	Personal and public privacy and security, Technologies for privacy and security in operating systems
Week 15	Review and Student presentation
Week 16	Final Exam

Delivery Plan (Weekly Lab. Syllabus)	
Week	**Material Covered**
Week 1	Lab1: Getting Started.
Week 2	Lab2: secure Process Scheduling
Week 3	Lab 3: secure Building of a Simple Operating System - bootstrapping
Week 4	Lab 4: secure Building of a Simple Operating System - memory management
Week 5	Lab5: Building a Simple Operating System - process management
Week 6	Lab 6: Virtualization (run an operating system as a guest on another operating system).

Week 7	Lab 7: Resource exhaustion (How an operating system behaves under resource exhaustion).
Week 8	Lab 8: System vulnerabilities-buffer overflow
Week 9	Lab 9: System vulnerabilities- Threats and exploits (gaining remote shell)
Week 10	Lab 10: system security plans, Backup and restore
Week 11	Lab 11: Auditing and Protection systems, and Log files
Week 12	Lab 12: Rootkit Detection - detecting and removing a rootkit from a system
Week 13	Lab 13: Exploring Firewall Configuration.
Week 14	Lab 14: configuring a firewall to block unauthorized access to a system
Week 15	Review and Student presentation
Week 16	Final Exam

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	1. Operating System Concepts by Abraham Silber Schatz, Greg Gagne, and Peter B. Galvin 2. Guide to Operating Systems by Greg Tomsho.	No
Recommended Texts	1. Linux for Beginners: An Introduction to the Linux Operating System and Command Line by Jason Cannon. 2. The Art of UNIX Programming by Eric S. Raymond. Linux Bible by Christopher Negus	No
Websites		

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Secure Software development

Module Information				
Module Title	**Secure Software development**		**Module Delivery**	
Module Type	**Core**		☐ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**BCYSCE305-S2**			
ECTS Credits	**5**			
SWL (hr/sem)	**125**			
Module Level	UGx11 4	**Semester of Delivery**	8	
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul	
Module Leader	Name	**e-mail**	rabdulhammed@ntu.edu.iq	
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	Ph.D.	
Module Tutor	Dr. Razan Abdulhammed	**e-mail**	rabdulhammed@ntu.edu.iq	
Peer Reviewer Name	Name	**e-mail**	E-mail	
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0	

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	1. To teach students how to develop software that is secure and resistant to cyber-attacks. 2. To provide students with an understanding of the legal and regulatory requirements for secure software development
Module Learning Outcomes	1. Identifying security risks: Students will learn how to identify, categorize, and prioritize the information and other resources used by software systems and to develop security requirements for the processes that access the data 2. Performing software security evaluations: Students will learn to perform software security evaluations, establish security requirements, and develop guidelines for security that are applied during the software design, operations, and maintenance processes. 3. Creating secure software: Students will learn design and development techniques used to avoid the most common software errors by using defensive coding techniques, managing resources securely, and creating secure interaction between components. 4. Preventing vulnerabilities: The emphasis in the course is the design and development of software that prevents many vulnerabilities from occurring in the first place. 5. Understanding security principles: Students will learn the principles of secure software development, including specifying program behavior, the classes of well-known defects, how they manifest themselves, and how to avoid them. 6. Applying security early in the software lifecycle: Students will recognize the benefits of designing security early in software and learn how to create security early in the software's lifecycle. 7. Writing secure code: Students will apply what they learn in the course by writing secure code. 8. Fluency in programming languages: Students should have fluency, not just familiarity, in at least one high-level programming language C++ or Java
Indicative Contents	Indicative content includes the following. 1. Secure coding principles 2. Software vulnerabilities 3. Software security requirements 4. secure coding standards security testing of software
Learning and Teaching Strategies	
Strategies	• Promote student involvement through encouraging students to be active participants in the project design process. • Create interdependence: Structure the project so that students are dependent on one another. For example, ensure that projects are sufficiently complex that students must draw on one another's knowledge and skills. • Assign projects that are relevant and meaningful to students. • Project-based learning is a teaching method in which students learn by actively engaging in real-world, meaningful, and personal projects. With this teaching strategy, students gain knowledge and skills over an extended period.

	• Backward course design is essential for project-based learning because it provides a planning framework that works back from the module's overall objectives, course, or project and creates a series of lessons built to help achieve these goals. • cooperative learning: Cooperative learning is a teaching strategy in which students work together in small groups to achieve a common goal. This strategy can help students develop teamwork and communication skills. • Provide continual feedback: Provide feedback to students throughout the project to help them improve their understanding and performance. • experiential learning

Student Workload (SWL)			
Structured SWL (h/sem)	63	**Structured SWL (h/w)**	4
Unstructured SWL (h/sem)	62	**Unstructured SWL (h/w)**	4
Total SWL (h/sem)	**125**		

Module Evaluation

63 As		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	1	10% (10)	10	LO #5, #7
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #11
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

Week	Material Covered
Week 1	Introduction وSoftware assurance definition وProperties of secure software, Abstraction: comparison of languages and approaches (object oriented, dynamic, functional, logical)
Week 2	Issues and challenges in the Software Development Life Cycle (SDLC); Secure languages & design; Modern development models
Week 3	Secure coding principles & practices and the API generation, Code reviews , Static analysis , Defensive coding , Secure coding standards
Week 4	Static & dynamic code checking
Week 5	properties of secure software
Week 6	Causes of vulnerabilities, Root causes of software vulnerabilities, Software vulnerabilities: Zero days, Design, Implementation, and Environment vulnerabilities, CVE, CVSS, NVD
Week 7	Seven pernicious kingdoms, compare severity of software vulnerabilities based on CVSS score,
Week 8	software vulnerability as design, implementation, or environmental
Week 9	Software security requirements, SQUARE model, prioritize software security requirements.
Week 10	Security in the software lifecycle, SDLC models, Maturity models, BSIMM , Open SAMM , NIST SSDF different phases of security enhanced software lifecycle models
Week 11	gap analysis using BSIMM and Open SAMM models
Week 12	relevant secure coding standards
Week 13	static analysis tools for application security testing
Week 14	Software security testing, different types of fuzzing techniques for black box security testing of software

Week 15	**Review and Student presentation.**
Week 16	**Preparatory week before the final Exam**

Delivery Plan (Weekly Lab. Syllabus)	
Week	**Material Covered**
Week 1	Lab 1: Getting Started
Week 2	Lab 2: Introduction to **SeCodEd**.
Week 3	Lab 3: Configuration and setting up of SeCodED framework.
Week 4	Lab 4: platform exploration
Week 5	Lab 5: Vulnerabilities Database
Week 6	Lab 6: Concept of Static Analysis
Week 7	Lab 7: Concept of Dynamic Analysis
Week 8	Lab 8: static analysis tools
Week 9	Lab 9: Dynamic vulnerability scanning tools
Week 10	Lab 10: Concept of Code Review
Week 11	Lab 11: Manual Code Review
Week 12	Lab 12: Automatic Code Review
Week 13	Lab 13: other open-source tools and platforms OWASP Labware
Week 14	Lab 14: other open-source tools and platforms SMSD Labware
Week 15	Lab 15: Project and Presentation
Week 15	**Final Exam**

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Secure Software Development: A Security Programmer's Guide by Grembi Jason.	Yes
Recommended Texts		No
Websites		

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Intrusions detection

Module Information

Module Title	**Intrusions detection**	**Module Delivery**	
Module Type	**Core**	☒ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**BCYSCE400-S1**		
ECTS Credits	**7**		
SWL (hr/sem)	**175**		
Module Level	4	**Semester of Delivery**	7
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Zakaria Noor Aldeen Mahmood	**e-mail**	E-mail
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	Ph.D.
Module Tutor		**e-mail**	zakaria@ntu.edu.iq
Peer Reviewer Name		**e-mail**	
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules

Prerequisite module		**Semester**	
Co-requisites module	1. Practicing Cybersecurity: Ethical Hacking and Vulnerability Lab (BCYSCE404-S1)	**Semester**	7

	2. AI for Cybersecurity Engineering (BCYSCE402-S1)		

Module Aims, Learning Outcomes and Indicative Contents

Module Objectives	3- To learn the basic understanding of network Intrusion detection systems concepts, principles, and practices. 4- To learn the basic techniques and methodologies for designing and analyzing Intrusions detection system. 5- To learn different types of intrusion detection systems. 6- To learn hands-on experience with both Snort and Suricata intrusion detection and prevention 7- To learn how to protect sensitive data from unauthorized access and outside intruders. 8- To learn Intrusions detection implementation techniques for secure systems. The students should be able to understand the uses and purpose of using Intrusions detection systems. 9- Help the students perform the needed cyber security works as well as qualifying him to use the different kinds of Intrusions detection tools and instructions to build & execute the projects of cyber security engineering.
Module Learning Outcomes	10- Understanding the fundamentals of Intrusions detection systems. Mastering of Snort and Suricata intrusion detection and prevention. Becoming familiar with protecting sensitive data. Being competent in common users authorized accessing and prevent data. Being able to perform defensive techniques and security tools and settings to provide data protection.

Learning and Teaching Strategies

Strategies	11- The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)

Structured SWL (h/sem)	78	**Structured SWL (h/w)**	4

Unstructured SWL (h/sem)	72	**Unstructured SWL (h/w)**	6
Total SWL (h/sem)	**150**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due
Formative assessment	**Quizzes**	٤	10% (10)	2,6,10,١٤
	Assignments	5	10% (10)	2 ,6,8,10,١٢
	Projects / Lab.	1٤	10% (10)	Continuous
	Report	1	10% (10)	10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7
	Final Exam	3hr	50% (50)	15
Total assessment			100% (100 Marks)	

INTRUSIONS DETECTION - PROGRAMME COURSE DESCRIPTION

Code BCYSCE400-S1	Name of the Course Unit	Semester	In-Class Hours (T+P)	Credit	ECTS Credit
	Intrusions detection	**1**	**2+3**		**6**

GENERAL INFORMATION	
Language of Instruction :	**English**
Level of the Course Unit :	**BACHELOR'S DEGREE**
Type of the Course :	**Compulsory**
Mode of Delivery of the Course Unit	**Face to Face**
Coordinator of the Course Unit	**Dr. Zakaria Noor Aldeen Mahmood**
Instructor(s) of the Course Unit	**Dr. Zakaria Noor Aldeen Mahmood**

OBJECTIVES AND CONTENTS	
Objectives of the Course Unit:	To learn the basic techniques and methodologies for designing and analyzing Intrusions detection system and provide hands-on experience with both Snort and Suricata intrusion detection and prevention.
Contents of the Course Unit:	• Introduction to Network Intrusion Detection System. • Snort Intrusion detection system. • Suricata Intrusion detection system. • Differences between Snort and Suricata • Defensive Techniques and Tools

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	Introduction to Network Intrusion Detection System: Overview of network intrusion detection systems, Types of intrusion detection systems. Network traffic analysis
2	Snort Intrusion detection system: Introduction to Snort, Installation and configuration of Snort, Snort Rulesets, and signatures, Understanding the rules and rule management
3	Snort Intrusion detection system: Creating custom rules for Snort, Packet analysis using Snort, Analysis of alerts generated by Snort, Threat hunting with Snort.
4	Suricata Intrusion detection system: Introduction to Suricata, Installation and configuration of Suricata, Rulesets, and signatures, Understanding the rules and rule management
5	Suricata Intrusion detection system: Creating custom rules for Suricata, Packet analysis using Suricata, Analysis of alerts generated by Suricata, Threat hunting with Suricata.
6	Differences between Snort and Suricata: Architecture, Protocol detection, performance, Customization options.
7	Differences between Snort and Suricata: Compatibility, User-friendliness, features, Third-party integrations.
8	Defensive Techniques and Tools: Firewall technologies, Virtual Private Networks (VPNs)
9	Defensive Techniques and Tools: Intrusion Prevention Systems (IPS)
10	Offensive Techniques and Tools: Port Scanning, vulnerability scanning, Exploitation technique.
11	Network Traffic Analysis Packet capture analysis, Protocol analysis
12	Automated and manual response to attacks.
13	Incident handling and Legal and organizational issues of intrusion detection
14	Incident handling of incident response system
15	Review
16	Final Exam

Delivery Plan (Weekly Lab. Syllabus)

	Material Covered
Week 1	Lab 1: Getting started with Snort
Week 2	Lab 2: Installation and Configuration of SNORT according to different organization requirements
Week 3	Lab 3: Exploring Snort Rulesets and Manageing Snort Rulesets
Week 4	Lab 4: Creating new rulesets and Packet Analysis using Snort
Week 5	Lab 5: Generated Alerts and analysis.
Week 6	Lab 6: Local and Global threat hunting with snort
Week 7	Lab 7: Getting started with Suricata Installation and configuration
Week 8	Lab 8: Exploring and Manage Suricata Rulesets
Week 9	Lab 9: Creating new rulesets
Week 10	Lab 10: Local and Global threat hunting with Suricata
Week 11	Lab 11: Snort and Suricata as Intrusion prevention system
Week 12	Lab 12: offensive and Defensive in Network
Week 13	Lab 13: Incident handling of intrusion detection
Week 14	Lab 14: Incident handling of incident response system
Week 15	Review
Week 16	**Final Exam**

Learning and Teaching Resources

	Text	Available in the Library?
Required Texts	**3.** Intrusion Detection with SNORT Book by Jack Koziol (2003)	no
Recommended Texts	4. Network Intrusion Detection, book, by Stephen Northcutt, Judy Novak (2002)	no
Websites		

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group	**FX –** Fail	(45-49)	More work required but credit awarded

(0 – 49)	**F –** Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Artificial Intelligence for Cybersecurity

Module Information					
Module Title	**Artificial Intelligence for Cybersecurity**			**Module Delivery**	
Module Type	**Core**			☒ **Theory**	
Module Code	**BCYSCE402-S1**			☒ **Lecture**	
ECTS Credits	٦			☒ **Lab**	
SWL (hr/sem)	١٥٠			☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Level		UGx11 4	**Semester of Delivery**		7
Administering Department		Cyber Security and Cloud Computing Techniques Engineering	**College**		Technical Engineering College for computer and AI / Mosul
Module Leader	Dr. Zakaria Noor Aldeen Mahmood		**e-mail**		E-mail
Module Leader's Acad. Title		Lecturer	**Module Leader's Qualification**		Ph.D.
Module Tutor			**e-mail**		zakaria@ntu.edu.iq
Peer Reviewer Name			**e-mail**		
Scientific Committee Approval Date		25/10/2024	**Version Number**		1.0

Relation with other Modules			
Prerequisite module		**Semester**	
Co-requisites module	1. Practicing Cybersecurity: Ethical Hacking and Vulnerability Lab (BCYSCE404-S1) 2. Intrusions detection (BCYSCE400-S1)	**Semester**	7

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	1. To learn the basic understanding of AI systems concepts, principles, and practices. 2. To learn the basic techniques and methodologies for designing and analyzing AI systems for cyber security. 3. To learn different types of AI application on cyber security. 4. To learn hands-on experience machine learning and prediction. 5. To learn how to use AI system to protect sensitive data from unauthorized access and outside intruders. 6. To learn cyber security problems and how to solve them using AI implementation techniques. 7. The students should be able to understand the uses and purpose of data collection and preprocessing. 8. Help the students perform feature selection and data reduction using classification and clustering techniques.
Module Learning Outcomes	31. Understanding the fundamentals of AI systems. 32. Mastering of machine learning application such as classification, clustering and prediction. 33. Becoming familiar with Weka software to implement machine learning algorithms and prediction.

	34. Being competent in common data analyzing and preprocessing using SPSS software. 35. Being able to perform AI techniques and Neural Networks application for data security and protection.

Learning and Teaching Strategies	
Strategies	The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)			
Structured SWL (h/sem)	79	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	71	**Unstructured SWL (h/w)**	4
Total SWL (h/sem)	**150**		

Module Evaluation				
As		**Time/Number**	**Weight (Marks)**	**Week Due**
Formative assessment	**Quizzes**	٤	10% (10)	2,6,10,١٤
	Assignments	5	10% (10)	2 ,6,8,10, ١٢
	Projects / Lab.	1٤	10% (10)	Continuous
	Seminar	1	10% (10)	10

Summative assessment	**Midterm Exam**	2hr	10% (10)	7
	Final Exam	3hr	50% (50)	15
Total assessment			100% (100 Marks)	

Code BCYSCE402-S1	Name of the Course Unit	Semester	In-Class Hours (T+P)	Credit	ECTS Credit
	Artificial Intelligence for Cybersecurity	**1**	**2+3**		**6**

ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY - PROGRAMME COURSE DESCRIPTION

GENERAL INFORMATION	
Language of Instruction :	**English**
Level of the Course Unit :	**BACHELOR'S DEGREE**
Type of the Course :	**Compulsory**
Mode of Delivery of the Course Unit	**Face to Face**
Coordinator of the Course Unit	**Dr. Zakaria Noor Aldeen Mahmood**
Instructor(s) of the Course Unit	**Dr. Zakaria Noor Aldeen Mahmood**

OBJECTIVES AND CONTENTS	
Objectives of the Course Unit:	**Introduce the student to understand AI and their applications in Cybersecurity**.
Contents of the Course Unit:	• Introduction to Machine learning. • Data: collection, processing, and features. • Introducing Cyber Security problems. • Regression

OBJECTIVES AND CONTENTS	
	• Classification • Clustering • Ensemble learning • Neural Networks

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	Introduction: What is Machine Learning? Difference between: Inference vs. Prediction, Supervised vs. Unsupervised Learning Problems, Regression vs. Classification
2	Data: Types, Data processing, cleaning, visualization, and exploratory analysis
3	Data set collection and feature extraction
4	Cyber Security problems that can be solved using Machine learning: Malware Analysis, Intrusion Detection, Spam detection, Phishing detection, Financial Fraud detection, Denial of Service Detection
5	Estimation Theory, Hypothesis testing
6	Linear Regression (uni- and multi-variate) and Logistic Regression
7	Basic Classification Techniques
8	Spectral Embedding, Manifold detection, and Anomaly Detection
9	Decision Trees and Random Forest
10	Ensemble learning: Bagging and Boosting Ensemble Classifiers i.e. Using Multiple Classifications to Improve Prediction Accuracy The Bootstrap Method Using the Bootstrap to Produce a Bagged Classifier An Alternative Ensemble Classifier AdaBoost and Other Boosting Methods
11	Support Vector Machines (SVM) The Support Vector Classifier Computing the SVM for Classification The SVM as a Penalization Method
12	Clustering Methods K-means Clustering Hierarchical Clustering

13	Neural Networks
14	Neural Networks
15	Review/preparation for final exam
16	Final Exam

Delivery Plan (Weekly Lab. Syllabus)	
Week	**Material Covered**
Week 1	Lab 1: Getting started with Weka
Week 2	Lab 2: Data preprocessing
Week 3	Lab 3: Features extractions
Week 4	Lab 4: Regression -1 (Linear)
Week 5	Lab 5: Regression -2. (Logistic)
Week 6	Lab 6: Classifications -1 (ZeroR and OneR)
Week 7	Lab 7: Classifications -2 (Naive Bayes)
Week 8	Lab 8: Classifications-3 (Decision Trees and Random Forest)
Week 9	Lab 9: Ensembles learning (Bagging)
Week 10	Lab 10: Ensembles learning (Boosting)
Week 11	Lab 11: Clustering -1 (K-mean)
Week 12	Lab 12: Clustering -2 (Hierarchical)
Week 13	Lab 13: Neural Networks -1
Week 14	Lab 14: Neural Networks -2
Week 15	Lab 15: Review/preparation for final exam
Week 16	Final Project Exam

WORKLOAD & ECTS CREDITS OF THE COURSE UNIT

Artificial Intelligence for Cybersecurity

Workload for Learning & Teaching Activities

Type of the Learning Activates	Learning Activities (# of week)	Duration (hours, h)	Workload (h)
Lecture & In-Class Activities	15	2	30
Preliminary & Further Study	NA	NA	NA
Land Surveying	NA	NA	NA
Group Work	NA	NA	NA
Laboratory	15	3	45
Reading	6	1	6
Assignment (Homework)	5	2	10
Project Work	NA	NA	NA
Seminar	1	1	1
Internship	NA	NA	NA
Technical Visit	NA	NA	NA
Web Based Learning	5	2	10
Implementation/Application/Practice	NA	NA	NA
Practice at a workplace	NA	NA	NA
Occupational Activity	NA	NA	NA
Social Activity	NA	NA	NA

Thesis Work	NA	NA	NA
Field Study	NA	NA	NA
Report Writing	1	٢	٢
Final Exam -Theory	1	3	3
Final Exam - Practical	1	1	1
Preparation for the Final Exam- Theory	1	20	20
Preparation for the Final Exam -Practical	1	10	٥
Mid-Term Exam - Theory	1	2	2
Mid-Term Exam - Practical	1	1	1
Preparation for the Mid-Term Exam	1	١٠	10
Short Exam (Quizzes)	٤	0.5	٢
Preparation for the Short Exam (Quizzes)	٤	2	8
Total Workload of the Course Unit			150

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	**4.** Data Mining and Machine Learning in Cybersecurity, April 2011 by Sumeet Dua, Xian Du	no
Recommended Texts	5. Mastering Machine Learning for Penetration Testing, (2018) By Chiheb Chebbi	no
Websites	https://www.youtube.com/watch?v=oGInXoYnjNQ https://www.youtube.com/watch?v=HkpxBy2dIMM	

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Graduate project Design

Module Information			
Module Title	**Graduate project Design**	**Module Delivery**	
Module Type	**Core**	☐ **Theory** ☒ **Lecture** ☐ **Lab** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**BCYSCE403-S2**		
ECTS Credits	**3**		
SWL (hr/sem)	**1**		
Module Level	UGx11 4	**Semester of Delivery**	7
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Name	**e-mail**	rabdulhammed@ntu.edu.iq
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	Ph.D.

Module Tutor	Dr. Razan Abdulhammed	**e-mail**	rabdulhammed@ntu.edu.iq
Peer Reviewer Name	Name	**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	Students of the Cybersecurity and Cloud Computing Engineering gain experience in basic design in their last year of study through the graduation project. Students can work anywhere in teams ranging in number from three to five students, with an average of three students per team. In addition, students are allowed to form their teams and select their graduation projects, which must be approved by the academic staff member who delivers the course. The main purpose of the project graduation course is to encourage the students to apply the knowledge they have acquired during their study. The projects need to integrate engineering criteria and realistic constraints, such as economic, environmental, moral, security, social, political, and sustainability-related considerations.
Module Learning Outcomes	36. Protect and defend computer systems and networks from cybersecurity attacks: This includes characterizing privacy, legal, and ethical issues of information security, identifying vulnerabilities critical to the information assets of an organization, and defining the security controls sufficient to provide a required level of confidentiality, integrity, and availability in an organization's computer systems and networks. 37. Diagnose and investigate cybersecurity events or crimes related to computer systems and digital evidence: This involves diagnosing attacks on an organization's computer systems and networks, proposing solutions including development, modification, and execution of incident response plans, and applying critical thinking and problem-solving skills to detect current and future attacks on an organization's computer systems and networks. 38. Effectively communicate in a professional setting to address information security issues: This includes communication orally and in writing, proposed information. 39. Secure a computer-based system, process, component, or program to meet business needs: This involves analyzing a problem and identifying and defining the security risks and requirements appropriate to its solution, applying mathematical foundations, algorithmic principles, cryptography, and computing theory in the modeling and design of security solutions for software or system architecture, and applying design and development principles in the construction of secure software systems of varying complexity. 40. Analyze, categorize, and assess the threats, vulnerabilities, and risks of an enterprise network and endpoints, as well as design and implement security solutions: This involves understanding the threats, vulnerabilities, and risks of an enterprise network and endpoints, and designing and implementing security solutions to mitigate them. 41. Engage in a highly collaborative process of idea generation, information sharing, and feedback that replicates key aspects of cybersecurity work: This includes engaging in a collaborative process of idea generation,

	information sharing, and feedback that replicates key aspects of cybersecurity work, and applying cybersecurity principles to real-world problems.
Indicative Contents	Indicative content includes the following. Filed survey for certain problems associated with Iraqi cybersecurity space. (8hrs) Project Selection and Proposal as a result from Identifying problems need solve through the filed study survey. (2hrs) Literature Review and Background Research(6hrs) Searching for suitable solution(s) (2hrs) Project Planning and Design (8hrs) Final design proposal defense(2hrs)
Learning and Teaching Strategies	
Strategies	• Promote student involvement through encourage students to be active participants in the project design process. • Create interdependence: Structure the project so that students are dependent on one another. For example, ensure that projects are sufficiently complex that students must draw on one another's knowledge and skills. • Assign projects that are relevant and meaningful to students. • Project-based learning is a teaching method in which students learn by actively engaging in real-world, meaningful, and personal projects. With this teaching strategy, students gain knowledge and skills over an extended period. • Backward course design is essential for project-based learning because it provides a planning framework that works back from the module's overall objectives, course, or project and creates a series of lessons built to help achieve these goals. • cooperative learning: Cooperative learning is a teaching strategy in which students work together in small groups to achieve a common goal. This strategy can help students develop teamwork and communication skills. • Provide continual feedback: Provide feedback to students throughout the project to help them improve their understanding and performance. • experiential learning

Student Workload (SWL)			
Structured SWL (h/sem)	34	**Structured SWL (h/w)**	2
Unstructured SWL (h/sem)	41	**Unstructured SWL (h/w)**	2
Total SWL (h/sem)	**75**		

Module Evaluation					
As		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	Quizzes				
	Assignments	2	10% (10)	1, 2,3,4	LO # 1, 2, 3 and 4
	Projects / Lab.	14	15% (10)	Continuous	All
	Report	2	10% (10)	2,4	LO # 2 and 4
Summative assessment	Midterm Exam	2 hr	20% (20)	7	LO # 1 - 6
	Final Exam	3 hr	50% (50)	15	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)	
Week	Material Covered
Week 1,2,3,4	Filed survey for certain problems associated with Iraqi cybersecurity space. (8hrs)
Week 5	Project Selection and Proposal as a result from Identifying problems need solve through the filed study survey. (2hrs)
Week 6,7,8,9	Literature Review and Background Research(8hrs)
Week 10,11	Searching for suitable solution(s) (2hrs)
Week 12,13,14,15	Project Planning and Design (8hrs)
Week 16	**Preparatory week before the final design proposal defense(2hrs)**

Learning and Teaching Resources		
	Text	Available in the Library?
Required Texts	By Subject	Yes
Recommended Texts		No
Websites		

Grading Scheme مخطط الدرجات			
Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors

	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Cloud Application

Module Information					
Module Title	**Cloud Application**			**Module Delivery**	
Module Type	**Core**			☐ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**BCYSCE 403-S2**				
ECTS Credits	**5**				
SWL (hr/sem)	**125**				
Module Level	UGx11 1		**Semester of Delivery**	1	
Administering Department	Cyber Security and Cloud Computing Techniques Engineering		**College**	Technical Engineering College for computer and AI / Mosul	
Module Leader	Name		**e-mail**	E-mail	
Module Leader's Acad. Title	Professor		**Module Leader's Qualification**	Ph.D.	
Module Tutor	Name (if available)		**e-mail**	E-mail	
Peer Reviewer Name	Name		**e-mail**	E-mail	
Scientific Committee Approval Date	25/10/2024		**Version Number**	1.0	

Relation with other Modules			
Prerequisite module	**Cloud computing security BCYSCCET301-S2**e	**Semester**	

Co-requisites module		**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	1. Understanding the fundamentals of cloud computing: This includes the basic concepts, principles, and components of cloud computing such as virtualization, service models, deployment models, and cloud security. 2. Designing and developing cloud applications: This involves learning how to design and implement cloud applications using various programming languages, tools, and frameworks. 3. Deploying and managing cloud applications: This includes understanding how to deploy cloud applications to various cloud platforms, such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP), and how to manage them using various cloud management tools. 4. Ensuring cloud application security: This involves understanding the security risks associated with cloud computing and how to implement security measures to protect cloud applications and data. 5. Integrating cloud applications with other systems: This includes learning how to integrate cloud applications with other systems such as databases, APIs, and messaging systems. 6. Monitoring and optimizing cloud application performance: This involves understanding how to monitor and optimize the performance of cloud applications using various performance monitoring and optimization tools.
Module Learning Outcomes	1. Understand the fundamentals of cloud computing and the benefits of using cloud applications. 2. Learn how to design, deploy, and manage cloud applications using various cloud platforms. 3. Gain knowledge of cloud application development frameworks and tools such as AWS, Azure, or Google Cloud Platform. 4. Learn how to create and configure cloud-based databases and data storage solutions. 5. Understand how to implement security and compliance measures for cloud applications. 6. Learn how to troubleshoot and optimize cloud applications for performance and scalability. 7. Understand how to integrate cloud applications with other cloud services and on-premise systems.

	8. Gain knowledge of cloud application architecture patterns and best practices. 9. Understand how to monitor and analyze cloud application usage and performance metrics.

Learning and Teaching Strategies	
Strategies	1. Start with the basics: Before diving into complex cloud applications, ensure that you have a solid understanding of the basics of cloud computing and the cloud service you want to learn. 2. Use online learning resources: There are numerous online resources available for learning cloud applications, including tutorials, videos, and documentation. Utilize them to gain a better understanding of the technology. 3. Practice with hands-on experience: The best way to learn cloud applications is by practicing with hands-on experience. Sign up for a cloud service provider's free tier, create your own projects, and experiment with different features to gain practical experience. 4. Join online communities: Join online communities such as forums, social media groups, and online learning communities to connect with other learners and experts in the field. You can ask questions, share your experiences, and learn from others. 1. 5-Stay up-to-date: Cloud technology is constantly evolving, so it's essential to stay up-to-date with the latest trends, updates, and best practices. Follow industry experts, read blogs, attend webinars, and participate in online communities to stay informed.

Student Workload (SWL)			
Structured SWL (h/sem)	79	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	46	**Unstructured SWL (h/w)**	3
Total SWL (h/sem)	**125**		

Module Evaluation					
As		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	Quizzes	4	10% (10)	2,5,8,10	Cloud service,cloud native,sevice offerd,types of cloud database
	Assignments	5	10% (10)	3,6,9,11,13	Cloud addaption,microsevice, data manager,service manager
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	14	10% (10)	Continuous	All
Summative assessment	Midterm Exam	2hr	10% (10)	7	Week1 to week8
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)	
Week	Material Covered
Week 1	Cloud basics: Understanding what the cloud is and why it's important. Principles for Cloud Application Development, Cloud Application Design Scalability Reliability, and availability
Week 2	Cloud service providers: Learning about prominent cloud service providers like AWS, Google, IBM, and Microsoft, and the services they offer.
Week 3	Cloud adoption: Understanding cloud trends and practices, including Hybrid Multiclouds, Microservices, Serverless, DevOps, Cloud Native, and Application Modernization.
Week 4	The basics of developing cloud applications.
Week 5	cloud-native application development
Week 6	microservices, and containerization.
Week 7	Cloud application deployment and management, Cloud application software, upgrades, resiliency, and evolution
Week 8	Cloud service providers: AWS, Google, IBM, and Microsoft, and the services offered.
Week 9	Cloud data management, data storage, data processing, and data analytics. Cloud Resource Management and Scheduling: Policies and mechanisms for resource management, resource bundling, combinatorial, fair queuing, start time fair queuing, borrowed virtual time, cloud scheduling subject to deadlines, scheduling map reduce applications subject to deadlines, resource management and application scaling
Week 10	different types of cloud databases, such as relational, NoSQL, and NewSQL databases
Week 11	Cloud Service Management, the basics of cloud service management, service-level agreements (SLAs), service management frameworks, and service monitoring and reporting

Week 12	Cloud Case Studies and Real-world Applications: real-world examples of cloud applications and their implementation. The challenges faced during the implementation of cloud applications and the strategies used to overcome them.
Week 13	Applications of cloud computing: Healthcare, energy systems, transportation, manufacturing
Week 14	Applications of cloud computing: education, government, mobile communication, application development
Week 15	review
Week 16	Final Exam

Delivery Plan (Weekly Lab. Syllabus)	
Week	**Material Covered**
Week 1	**Lab 1: Getting Started**
Week 2	**Lab 2: Cloud Computing Basics Lab**
Week 3	**Lab 3: Cloud Infrastructure Lab**
Week 4	**Lab 4: Cloud Security Lab.**
Week 5	**Lab 5: Cloud Storage Lab**
Week 6	**Lab 6: Cloud Networking Lab**
Week 7	**Lab 7: Cloud Application Development Lab**
Week 8	**Lab 8: Cloud Deployment Lab**
Week 9	**Lab 9: Cloud Migration Lab**
Week 10	**Lab 10: Cloud Monitoring and Management Lab**
Week 11	**Lab 11: Exploring Cloud Cost Optimization Lab**
Week 12	**Lab 12: Cloud Cost Optimization Lab case study 1.**
Week 13	**Lab 13: Cloud Cost Optimization Lab case study 2.**
Week 14	**Lab 14: Project and Presentation**
Week 15	**review**
Week 16	**Final Exam**

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Cloud Computing: Concepts, Technology & Architecture, by Thomas Erl, Ricardo Puttini, and Zaigham Mahmood	Yes
Recommended Texts	Building Applications and Infrastructure in the Cloud, by George Reese	No
Websites		

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Practicing cybersecurity: Ethical Hacking and Vulnerability Lab

Module Information			
Module Title	**Practicing cybersecurity: Ethical Hacking and Vulnerability Lab**	**Module Delivery**	
Module Type	**Core**	☐ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**BCYSCE404-S1**		
ECTS Credits	**7**		
SWL (hr/sem)	**175**		
Module Level	UGx11 4	**Semester of Delivery**	8
Administering Department	Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul
Module Leader	Name	**e-mail**	rabdulhammed@ntu.edu.iq

Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	Ph.D.
Module Tutor	Dr. Razan Abdulhammed	**e-mail**	rabdulhammed@ntu.edu.iq
Peer Reviewer Name	Name	**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules			
Prerequisite module	BCYSCE200-S2, BCYSCE203-S2 BCYSCE300-S1 BCYSCE300-S2 BCYSCE304-S1	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	14. To learn the principles and techniques associated with the cybersecurity practice known as penetration testing or ethical hacking. 15. To learn Planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting. 16. To learn system vulnerabilities and How system vulnerabilities can be exploited and learns to avoid such problems.
Module Learning Outcomes	42. Understand the attack phases, threats, and attack vectors. 43. Learn how to use penetration testing tools. 44. Evaluate and discuss the standards and ethical issues pertaining to performing security testing. 45. Understand the basics of using the Cyber Range 46. Discuss known attacks, malware, and vulnerabilities. 47. Identify and evaluate system security. 48. Learn basic digital forensics techniques. 49. Articulate the required planning and preparation for a penetration test. 50. Understand the fundamentals of information security and ethical hacking. 51. Identify information security threats and vulnerabilities, types of malwares, and vulnerability assessments. 52. Learn network-level attacks including sniffing, denial-of-service, and session hijacking, and their countermeasures. 53. Understand web application attacks and countermeasures. 54. Learn wireless attacks and countermeasures
Indicative Contents	Introduction to Ethical Hacking. Ethical requirements. Penetration test report. Vulnerability Analysis Methods. Scanning and Sniffing Networks. System Hacking. Session Hijacking Hacking Web Servers Hacking Web Applications Hacking Wireless Networks. Hacking Mobile Platforms. Metasploit exploitation. Cryptography weaknesses. Evading IDS, Firewalls, and Honeypots
Learning and Teaching Strategies	
Strategies	The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes,

	interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)			
Structured SWL (h/sem)	63	**Structured SWL (h/w)**	4
Unstructured SWL (h/sem)	112	**Unstructured SWL (h/w)**	7
Total SWL (h/sem)	**175**		

Module Evaluation					
As		**Time/Number**	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	1	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Assignments	4	10% (10)	2 ,4,6and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

Week	Material Covered
Week 1	Introduction, software installation, Pre-engagement, scoping.
Week 2	Ethical requirements and legal issues.
Week 3	Penetration test report structure and components.
Week 4	Vulnerability Analysis Methods, Foot printing and Reconnaissance
Week 5	Scanning and Sniffing Networks, Scanning using Nmap
Week 6	System Hacking: NetBIOS and NFS, Windows passwords, hashes, Linux passwords, hashes with salt, Searching Linux, and Windows file systems
Week 7	Session Hijacking, TCP, UDP, connections, SSL, and TLS encryption.
Week 8	Malware Threats
Week 9	Hacking Web Servers and Hacking Web Applications: File transfer protocol: ftp, http, Telnet, DNS, Web Reconnaissance.
Week 10	Hacking Wireless Networks and Hacking Mobile Platforms
Week 11	Metasploit exploitation framework
Week 12	Cryptography weaknesses
Week 13	Evading IDS, Firewalls, and Honeypots, and Use of netcat and pivoting
Week 14	Lock picking, master keys, and oracle hacks
Week 15	Review and Student Presentation
Week 16	**Preparatory week before the final Exam**

Delivery Plan (Weekly Lab. Syllabus)

Week	Material Covered
Week 1	Lab 1: Getting started lab environment
Week 2	Lab 2: System Hacking
Week 3	Lab 3: Scanning and Sniffing
Week 4	Lab 4: Session Hijacking: TCP, UDP, SSL, and TLS.
Week 5	Lab 5: Hacking Web Servers and Applications: ftp, http, Telnet, DNS.

Week 6	Lab 6: Wireless Networks Vulnerability Analysis
Week 7	Lab 7: Mobile Platforms Vulnerability Analysis - IOS
Week 8	Lab 8: Mobile Platforms Vulnerability Analysis - Android
Week 9	Lab 9: Malwares threat Vulnerability Analysis
Week 10	Lab 10: Metasploit Framework
Week 11	Lab 11: Metasploit exploitation
Week 12	Lab 12: Pent testing with Metasploit
Week 13	Lab 13: Working with Active Exploits in Metasploit
Week 14	Lab 14: Working with Passive Exploits in Metasploit
Week 15	Review and Student presentation
Week 16	Final Exam

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Ethical Hacking: A Hands-on Introduction to Breaking In by Daniel G. Graham	Yes
Recommended Texts		No
Websites		

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Research Methodology

Module Information					
Module Title	**Research Methodology**			**Module Delivery**	
Module Type	**Core**			**☒Theory** **☒Lecture** **☐Lab** **☐ Tutorial** **☐ Practical** **☒ Seminar**	
Module Code	**BCYSCE405-S1**				
ECTS Credits	**3**				
SWL (hr/sem)	**75**				
Module Level		UGx11 4	**Semester of Delivery**		1
Administering Department		Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul	
Module Leader	Dr.Razan Abdulhammed		**e-mail**	rabdulhammed@ntu.edu.iq	
Module Leader's Acad. Title		Lecturer	**Module Leader's Qualification**		PhD.
Module Tutor	None		**e-mail**	None	
Peer Reviewer Name		Name	**e-mail**	None	
Scientific Committee Approval Date		25/10/2024	**Version Number**	1.0	

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	1. Understanding the research process. 2. Learning about different research methods. 3. Developing skills in research design and planning. 4. Developing skills in data analysis. 5. Understanding ethical considerations in research.
Module Learning Outcomes	6. Understanding the research process: Students should be able to demonstrate an understanding of the research process, including the formulation of research questions, the design of research studies, data collection methods, data analysis techniques, and the interpretation of research results. 7. Designing and planning research studies: Students should be able to design and plan research studies, including developing research questions, selecting appropriate research methods, and designing data collection instruments. 8. Analyzing and interpreting data: Students should be able to analyze and interpret data using appropriate statistical and qualitative data analysis techniques, and be able to use software tools for data analysis. 9. Communicating research findings: Students should be able to communicate research findings effectively through written reports, presentations, and other forms of communication.

Learning and Teaching Strategies	
Strategies	The learning and teaching strategies for a course in research methodology will depend on a variety of factors, including the level of study, course objectives, and student needs. However, some common learning and teaching strategies for research methodology may include: 1. Lectures: Lectures are a common teaching strategy for introducing students to different research methods and the research process. Lectures may be delivered in person or online, and may include multimedia such as slides and videos. 2. Workshops: Workshops provide students with hands-on experience in designing, conducting, and analyzing research studies. Workshops may include activities such as designing research studies, collecting and analyzing data, and presenting research findings. 3. Group discussions: Group discussions provide students with the opportunity to share their experiences and perspectives on research methodology, and to learn from their peers. Group discussions may be conducted in person or online, and may be facilitated by the instructor or by students themselves. 4. Research projects: Research projects provide students with the opportunity to apply their knowledge and skills in research methodology to a

	practical problem. Research projects may involve designing and conducting a research study, analyzing data, and presenting research findings. 5. Online resources: Online resources such as interactive tutorials, videos, and case studies can be used to supplement lectures and workshops, and to provide students with additional opportunities to practice and apply their knowledge. 6. Assignments and assessments: Assignments and assessments such as quizzes, exams, and research reports can be used to evaluate students' understanding of the course material and their ability to apply their knowledge and skills to practical problems.

Student Workload (SWL)			
Structured SWL (h/sem)	49	**Structured SWL (h/w)**	3
Unstructured SWL (h/sem)	26	**Unstructured SWL (h/w)**	2
Total SWL (h/sem)	**75**		

Module Evaluation

As		**Time/Number**	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	2	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #6
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	**Introduction to Research Methodology** • Basic concepts employed in quantitative and qualitative research • Research ethics • Research design
2	**Research Methods** • Survey research • Experimental research • Action research • Case study research
3	**Data Collection and Analysis** • Data collection methods • Data analysis techniques • Statistical analysis
4	**Reporting Research Findings** • Communicating research findings to experts and the general population • Writing research reports • Presenting research findings
5	**Writing Process** • Understanding the writing process. • Analyzing the audience and purpose. • Developing a writing plan. • Drafting and revising. • Editing and proofreading.
6	**Technical Writing Style** • Writing with clarity and conciseness • Using plain language
7	**Technical Writing Style** • Writing for a global audience • Using visuals to enhance understanding.
8	**Technical Writing Genres** • Writing technical reports • Writing proposals
9	**Technical Writing Genres** • Writing instructions and manuals • Writing scientific papers • Writing for the web
10	**Midterm Exam**
11	**Technical Writing Skills**

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
	• Constructing a logical outline of a technical document • Writing with awareness of expository techniques such as definition, classification, and comparison
12	**Technical Writing Skills** • Using appropriate tone and style • Using correct grammar, punctuation, and mechanics • Citing sources and avoiding plagiarism
13	**Scientific and Technical Writing** • Introduction to the essential elements of scientific and technical writing • Practice in the forms and discourses of scientific and technical writing • Developing skills in writing technical reports, proposals, and scientific papers
14	Using appropriate tone and style, Using correct grammar, punctuation, and mechanics, Citing sources and avoiding plagiarism, Practice in the forms and discourses of scientific and technical writing,
15	Review and Student presentation
16	**Final Exam**

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Textbook: Research Methods: A Process of Inquiry by Anthony M. Graziano and Michael L. Raulin	Yes
Recommended Texts	Research articles and case studies.	Yes
Websites		

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Reverse Engineering- Malwares Analysis

Module Information					
Module Title	**Reverse Engineering- Malwares Analysis**			**Module Delivery**	
Module Type	**Core**			☐ **Theory**	
Module Code	**BCYSCE403-S2**			☒ **Lecture**	
ECTS Credits	**7**			☐ **Lab**	
SWL (hr/sem)	**175**			☐ **Tutorial**	
				☐ **Practical**	
				☐ **Seminar**	
Module Level		UGx11 4	**Semester of Delivery**		8
Administering Department		Cyber Security and Cloud Computing Techniques Engineering	**College**		Technical Engineering College for computer and AI / Mosul
Module Leader	Name		**e-mail**		rabdulhammed@ntu.edu.iq
Module Leader's Acad. Title		Lecturer	**Module Leader's Qualification**		Ph.D.

Module Tutor	Dr. Razan Abdulhammed	**e-mail**	rabdulhammed@ntu.edu.iq
Peer Reviewer Name	Name	**e-mail**	E-mail
Scientific Committee Approval Date	25/10/2024	**Version Number**	1.0

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives أ	17. Introduction to reverse engineering and its importance in cybersecurity. 18. Master Reverse Engineering tools and techniques. 19. Be familiar with the taxonomy of malware. 20. Be competent in common reverse engineering techniques. 21. Be competent in common anti-reverse engineering techniques such as obfuscation. 22. Conduct triage malware analysis by running the malware in a sandbox, extracting strings, and more. 23. Open the executables with a disassembler and try to understand what they do. 24. Understand the code, structure, and functionality of malicious software. 25. Basic concepts of assembly language and disassembly. 26. Tools and techniques for reverse engineering. 27. Learn how to provide protection against malware
Module Learning Outcomes	55. Understanding the fundamentals of reverse engineering and malware analysis, including terminology and processes. 56. Mastering reverse engineering tools and techniques, including common anti-reverse engineering techniques such as obfuscation. 57. Becoming familiar with the taxonomy of malware and recognizing known patterns. 58. Being competent in common reverse engineering techniques, such as static and dynamic analysis. 59. Being able to perform hands-on malware analysis, including triage, static, and dynamic analysis. 60. Being able to write Python automation scripts to aid in malware analysis.

Indicative Contents	Indicative content includes the following. Introduction to Reverse Engineering. (3hrs) Assembly Language and Disassembly. (6hrs) Tools and Techniques for Reverse Engineering. (6hrs) Introduction to malware analysis. (12hrs) Reverse Engineering Techniques. (12hrs) Malware Analysis Tools. (3hrs) Static Analysis Techniques. (8hrs) Dynamic Analysis Techniques. (8hrs) Malware Behavior Analysis. (6hrs) Reverse Engineering Malware ode(6hrs)
Learning and Teaching Strategies	
Strategies	The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)			
Structured SWL (h/sem)	79	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	96	**Unstructured SWL (h/w)**	6
Total SWL (h/sem)	**75**		

Module Evaluation

As		**Time/Number**	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	2	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)	
Week	**Material Covered**
Week 1	**Introduction to Reverse Engineering** • Definition and importance of reverse engineering • Types of reverse engineering Legal and ethical considerations.
Week 2	**Assembly Language and Disassembly** • Introduction to assembly language • Basic instructions and syntax • Disassembly tools and techniques Hands-on exercises using IDA Pro and Binary Ninja.
Week 3	**Tools and Techniques for Reverse Engineering** • Debugging and tracing • Dynamic and static analysis • Malware analysis tools and techniques • Hands-on exercises using OllyDbg, WinDbg, and Ghidra
Week 4	**Introduction to malware analysis** • Overview of reverse engineering techniques • Overview of software security and defense practices
Week 5	**Reverse Engineering Techniques** • Static analysis • Dynamic analysis • Code obfuscation techniques • Anti-debugging techniques • Anti-disassembly techniques
Week 6	**Malware Analysis Tools** • IDA Pro • OllyDbg • WinDbg

	• Sysinternals Suite • Wireshark
Week 7	**Malware Analysis Methodology** • Malware classification • Malware behavior analysis • Malware signature creation • Malware removal and prevention
Week 8	**Introduction to Reverse Engineering and Malware Analysis** • Overview of Reverse Engineering and Malware Analysis • Types of Malware • Malware Analysis Process • Malware Analysis Tools
Week 9	**Tools and Techniques for Malware Analysis** • Debuggers • Disassemblers • Decompiles • Hex Editors • Memory Analysis Tools
Week 10	**Static Analysis Techniques** • File Analysis • Strings Analysis • PE Header Analysis • Import/Export Table Analysis
Week 11	**Dynamic Analysis Techniques** • Debugging Techniques • Memory Analysis • Network Analysis • System Call Tracing
Week 12	**Malware Behavior Analysis** • Malware Functionality • Malware Persistence • Malware Communication • Malware Evasion Techniques
Week 13	**Reverse Engineering Malware Code** • Assembly Language Basics Reverse Engineering Techniques.
Week 14	**Reverse Engineering Malware Code**

	• Code Obfuscation Techniques • Anti-Debugging Techniques
Week 15	**Final Exam**
Week 16	**Preparatory week before the final Exam**

Delivery Plan (Weekly Lab. Syllabus)	
Week	**Material Covered**
Week 1	**Lab 1: Getting Started**
Week 2	**Lab 2: Setting up a virtual machine for malware analysis**
Week 3	**Lab 3: Exploring common types of reverse engineering**
Week 4	**Lab 4: Basic Assembly commands for reverse engineering 1.**
Week 5	**Lab 5: Basic Assembly commands for reverse engineering -2.**
Week 6	**Lab 6: Debugging and tracing.**
Week 7	**Lab7: Dynamic analysis**
Week 8	**Lab 8: Static analysis**
Week 9	**Lab 9: Malwares Analysis using IDA Pro.**
Week 10	**Lab 10: Malwares Analysis using WinDbg.**
Week 11	**Lab 11: Malwares Analysis using Sysinternals Suite.**
Week 12	**Lab 12: Malwares Analysis using Wireshark.**
Week 13	**Lab 13: Code Obfuscation**
Week 14	**Lab14: Memory Analysis Tools**
Week 15	**Final Exam**

Learning and Teaching Resources			
	Text	**Available in the Library?**	
Required Texts	Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware by Abhijit Mahanta and Anoop Saldanha | Sep 23, 2020.	Yes	
Recommended Texts		No	
Websites			

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group	**A -** Excellent	90 - 100	Outstanding Performance

(50 - 100)	**B -** Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Introduction to Digital Forensics

Module Information معلومات المادة الدراسية					
Module Title	**Introduction to Digital Forensics**			**Module Delivery**	
Module Type	**Core**			☐ **Theory** ☒ **Lecture** ☒ **Lab** ☒ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**BCYSCE402-S2**				
ECTS Credits	**7**				
SWL (hr/sem)	**175**				
Module Level		UGx11 4	**Semester of Delivery**		٢
Administering Department		Cyber Security and Cloud Computing Techniques Engineering	**College**	Technical Engineering College for computer and AI / Mosul	
Module Leader	Dr. Rabei Raad Ali		**e-mail**	rabei@ntu.edu.iq	
Module Leader's Acad. Title		Professor	**Module Leader's Qualification**		Ph.D.
Module Tutor	Name (if available)		**e-mail**	E-mail	
Peer Reviewer Name		Name	**e-mail**	E-mail	
Scientific Committee Approval Date		25/10/2024	**Version Number**		1.0

Relation with other Modules			
Prerequisite module	Introduction to Cybersecurity (**BCYSCE 108-S2)**	**Semester**	\
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	1. To emphasize the fundamentals and importance of digital forensics. 2. To provide the student with the ability to carry out computer forensic investigations. 3. To appraise forensic software with a view to develop appropriate investigation strategies in the light of emerging digital technologies.
Module Learning Outcomes	4. Students will explain and properly document the process of digital forensics analysis. 5. Students will gain an understanding of the tradeoffs and differences between various forensic tools. 6. Students will be able to describe the representation and organization of data and metadata within modern computer systems. 7. Students will understand the inner workings of file systems. 8. Students will be able to create disk images, recover deleted files and extract hidden information. 9. Students will be introduced to the current research in computer forensics. This will encourage them to define research problems and develop effective solutions.

Learning and Teaching Strategies	
Strategies	In order to encourage students' participation, the classes will be designed to be dynamic and interactive. Rather than relying solely on traditional lecture-style teaching, the emphasis will be placed on promoting discussions, group activities, and collaborative problem-solving exercises. This will create an environment where students feel empowered to voice their thoughts, ask questions, and engage in meaningful dialogue with both the instructor and their peers.

Student Workload (SWL)			
Structured SWL (h/sem)	79	Structured SWL (h/w)	5
Unstructured SWL (h/sem)	96	Unstructured SWL (h/w)	٦
Total SWL (h/sem)	١٧٥		

Module Evaluation					
As		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	Quizzes	2	10% (10)	5 and 10	LO #3, #5 and #10, #14
	Assignments	4	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	Midterm Exam	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)	
Week	Material Covered
Week 1	Introduction: Understanding the Digital Forensics Profession and Investigations.
Week 2	Data acquisition: the process of collecting data from various sources such as computers, mobile devices, and cloud storage.
Week 3	Digital forensics tools: different tools and techniques used in digital forensics investigations.
Week 4	Network forensics: This involves investigating network traffic to identify potential security breaches or cyber attacks
Week 5	Mobile and wireless device forensics: how to extract data from mobile devices such as smartphones and tablets.
Week 6	Mobile and wireless device forensics: File present in SIM card. External memory dump and evidence in memory card. Mobile evidence extraction process.
Week 7	Mid-term Exam + Data Acquisition methods- physical, file system, logical and Manual Acquisition. Mobile investigation tool kit.
Week 8	Cloud forensics: investigating data stored in cloud environments such as Google Drive or Dropbox.

Week 9	Social media forensics investigates social media accounts and messages. Source for social media evidence, Types of Data Available on Social Networking sites.
Week 10	Social media forensics investigates different evidence collection methods from social networking sites, intelligence gathering from social media, Tools and techniques for intelligence gathering, indirect method, direct method with login, direct method without login.
Week 11	Cyber laws: the legal aspects of cybercrime investigations, including laws related to digital evidence and privacy.
Week 12	Digital evidence controls the importance of maintaining the integrity of digital evidence throughout an investigation.
Week 13	Recovering Graphics Files. Computer Forensics Analysis and Validation.
Week 14	Virtual Machine and Cloud Forensics.
Week 15	Email Investigations. Report Writing for Tech Investigations. Expert Testimony in Tech Investigations. Ethics for the Investigator and Expert Witness.
Week 16	**Preparatory week before the final Exam**

Delivery Plan (Weekly Lab. Syllabus)	
Week	**Material Covered**
Week 1	Lab 1: Introducing Digital Forensics tools.
Week 2	Lab 2: Network forensics.
Week 3	Lab 3: Mobile and wireless device forensics.
Week 4	Lab 4: Extracting GPS Data from Mobile Devices
Week 5	Lab 5: Recovering Deleted Data from Mobile Devices
Week 6	Lab 6: Social media forensics
Week 7	Lab 7: Intelligence gathering

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press; 3 edition. ISBN 978-0123742681.	Yes
Recommended Texts	Ho, A. T. S. and Li, S (2015). Handbook of Digital Forensics of Multimedia Data and Devices. Wiley-IEEE Press. ISBN 978-1118640500	No
Websites	https://www.guru99.com/computer-forensics-tools.html	

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A** - Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX** – Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Cybersecurity for IoTs

Module Information معلومات المادة الدراسية					
Module Title	**Cybersecurity for IoTs**			**Module Delivery**	
Module Type	**Core**			☒**Theory** ☐**Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**BCYSCE404-S2**				
ECTS Credits	**7**				
SWL (hr/sem)	**175**				
Module Level	UGx11 4		**Semester of Delivery**	2	
Administering Department	Cyber Security and Cloud Computing Techniques Engineering		**College**	Technical Engineering College for computer and AI / Mosul	
Module Leader	Dr.Razan Abdulhammed		**e-mail**	rabdulhammed@ntu.edu.iq	
Module Leader's Acad. Title	Lecturer		**Module Leader's Qualification**	PhD.	
Module Tutor	None		**e-mail**	None	
Peer Reviewer Name	Name		**e-mail**	None	
Scientific Committee Approval Date	25/10/2024		**Version Number**	1.0	

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	6. Confidentiality. 7. Authentication: Ensuring that only authorized users are able to access IoT devices and systems. 8. Availability: Ensuring that IoT devices and systems are always available and accessible to authorized users. 9. Risk management. 10. Resilience.
Module Learning Outcomes	10. Understanding the concepts and principles of cybersecurity and how they apply to IoT devices and systems. 11. Identifying and analyzing the various cyber threats and vulnerabilities that exist in the IoT ecosystem, hacking, and social engineering. 12. Understanding the legal and ethical issues related to cybersecurity in the IoT ecosystem, including privacy, data protection, and intellectual property.

Learning and Teaching Strategies	
Strategies	Learning and teaching strategies for cyber security for IoT typically involve a combination of theoretical and practical approaches. Some common strategies include: 7. Lectures and presentations: Lectures and presentations can be used to introduce students to the fundamental concepts and principles of IoT security. This can include topics such as IoT architecture, security risks, and security protocols. 8. 2. Case studies and scenarios: Case studies and scenarios can be used to help students understand the real-world implications of IoT security. This can include analyzing recent IoT security breaches, identifying security vulnerabilities in IoT systems, and developing strategies for mitigating security risks. 9. 3. Hands-on exercises and labs: Hands-on exercises and labs can provide students with practical experience in securing and managing IoT systems. This can include tasks such as configuring secure communication protocols,

	implementing access control measures, and conducting security testing and evaluation. 10. 4. Group projects and discussions: Group projects and discussions can be used to encourage collaboration and critical thinking among students. This can include tasks such as designing and implementing secure IoT systems, analyzing security risks and developing mitigation strategies, and evaluating the effectiveness of different security protocols and technologies. 5. Guest speakers and industry experts: Guest speakers and industry experts can provide students with valuable insights into current trends and best practices in IoT security. This can include topics such as emerging threats and vulnerabilities, industry standards and regulations, and career opportunities in the field.

Student Workload (SWL)			
Structured SWL (h/sem)	79	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	96	**Unstructured SWL (h/w)**	6
Total SWL (h/sem)	**175**		

Module Evaluation

As		**Time/Number**	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	2	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #6
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

	Delivery Plan (Weekly Syllabus)
WEEK	**KEY LEARNING OUTCOMES OF THE COURSE UNIT (On successful completion of this course unit, students/learners will or will be able to)**
1	**Introduction to IoTs** • Definition and characteristics of IoTs • what is the IoT and why is it important? • Elements of an IoT ecosystem. • Technology drivers, Business drivers. • Trends and implications. • Overview of Governance.
2	**IoT architecture and protocols** • Protocol Standardization for IoT – Efforts – M2M. • WSN Protocols
3	**IoT architecture and protocols** • SCADA. • RFID Protocols
4	**IoT architecture and protocols** • Issues with IoT Standardization • Unified Data Standards • Protocols • IEEE802.15.4 • BACNet Protocol • Modbus • KNX • Zigbee • Network layer • APS layer
5	**IOT ARCHITECTURE** • IoT Open-source architecture (OIC)- OIC Architecture & Design principles • IoT Devices and deployment models • IoTivity: An Open source IoT stack • Overview • IoTivity stack architecture • Resource model and Abstraction
6	**WEB OF THINGS** • Web of Things versus Internet of Things • Two Pillars of the Web • Architecture Standardization for WoT • Platform Middleware for WoT • Unified Multitier WoT Architecture • WoT Portals and Business Intelligence

7	**IOT APPLICATIONS** • IoT applications for industry: Future Factory Concepts, Brownfield IoT, Smart Objects, Smart Applications. • Study of existing IoT platforms /middleware,
8	**Midterm Exam**
9	**Security Risks in IoTs** • Threats and vulnerabilities in IoTs. • Attack vectors and techniques
10	**Security Mechanisms for IoTs** • Authentication and authorization. • Encryption and decryption. • Access control and firewalls.
11	**IoT Security Standards and Regulations** • IoT security standards and best practices. • Legal and ethical issues in IoT security
12	**IoT Security Implementation** • Designing and implementing secure IoT systems
13	**IoT Security Implementation** • Testing and evaluating IoT security
14	**Case Studies and Projects** • Real-world examples of IoT security breaches
15	**Group projects to design and implement secure IoT systems**
16	**Final Exam**

	Delivery Plan (Weekly Lab. Syllabus)
WWEEK	**Material Covered**
1	Lab1: Connecting Devices to Build IoT and Simulating IoT Devices.
2	Lab 2: Identify Pillars of the IoT System.
3	Lab ٣ : Securing Cloud Services in the IoT and Working with IFTTT and Google Accounts.
4	Lab 4: Threat Modeling: - at the IoT Device Layer, at the IoT Communication Layer, at the IoT Application Layer.
5	Lab 5: Threat Modeling to Assess Risk in an IoT System.
6	Lab 6: Evaluate Recent IoT Attacks.
7	Lab 7: Evaluate the IoT Security Risk in various sectors: Industry, healthcare, ecosystem.
8	Lab 8: Investigate Vulnerability Assessment Tools.
9	Lab ٩: Web of Things Application Vulnerability and UPnP Vulnerabilities.
10	Lab ١٠: Hacking MQTT.

11	Lab ١١: Sniffing Bluetooth with the Raspberry Pi.
12	Lab ١٢: Port Scanning an IoT Device.
13	Lab 1٣: Challenge Passwords with Kali Tools.
14	Lab 14: Compromise IoT Device Hardware, Compromise IoT Device Firmware.
15	Review and Student presentation
16	Final Exam

Learning and Teaching Resources		
	Text	**Available in the Library?**
Required Texts	Internet of Things: A Hands-On Approach" by Arshdeep Bahga and Vijay Madisetti	Yes
Recommended Texts	"Practical Internet of Things Security" by Brian Russell, Drew Van Duren, and John R. Vacca	Yes
Websites		

Grading Scheme			
Group	**Grade**	**Marks %**	**Definition**
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

Graduate project Implementation

Module Information					
Module Title	**Graduate project Implementation**			**Module Delivery**	
Module Type	**Core**			☐ **Theory** ☒ **Lecture** ☐ **Lab** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**BCYSCE405-S2**				
ECTS Credits	**4**				
SWL (hr/sem)	**100**				
Module Level	UGx11 4		**Semester of Delivery**	8	
Administering Department	Cyber Security and Cloud Computing Techniques Engineering		**C ollege**	Technical Engineering College for computer and AI / Mosul	
Module Leader	Name		**e-mail**	rabdulhammed@ntu.edu.iq	
Module Leader's Acad. Title	Lecturer		**Module Leader's Qualification**	Ph.D.	
Module Tutor	Dr. Razan Abdulhammed		**e-mail**	rabdulhammed@ntu.edu.iq	
Peer Reviewer Name	Name		**e-mail**	E-mail	
Scientific Committee Approval Date	25/10/2024		**Version Number**	1.0	

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives أ	Students of the Cybersecurity and Cloud Computing Engineering gain experience in basic design in their last year of study through the graduation project. Students can work anywhere in teams ranging in number from three to five students, with an average of three students per team. In addition, students are allowed to form their teams and select their graduation projects, which must be approved by the academic staff member who delivers the course. The main purpose of the project graduation course is to encourage the students to apply the knowledge they have acquired during their study. The projects need to

	integrate engineering criteria and realistic constraints, such as economic, environmental, moral, security, social, political, and sustainability-related considerations.
Module Learning Outcomes	61. Protect and defend computer systems and networks from cybersecurity attacks: This includes characterizing privacy, legal, and ethical issues of information security, identifying vulnerabilities critical to the information assets of an organization, and defining the security controls sufficient to provide a required level of confidentiality, integrity, and availability in an organization's computer systems and networks. 62. Diagnose and investigate cybersecurity events or crimes related to computer systems and digital evidence: This involves diagnosing attacks on an organization's computer systems and networks, proposing solutions including development, modification, and execution of incident response plans, and applying critical thinking and problem-solving skills to detect current and future attacks on an organization's computer systems and networks. 63. Effectively communicate in a professional setting to address information security issues: This includes communication orally and in writing, proposed information. 64. Secure a computer-based system, process, component, or program to meet business needs: This involves analyzing a problem and identifying and defining the security risks and requirements appropriate to its solution, applying mathematical foundations, algorithmic principles, cryptography, and computing theory in the modeling and design of security solutions for software or system architecture, and applying design and development principles in the construction of secure software systems of varying complexity. 65. Analyze, categorize, and assess the threats, vulnerabilities, and risks of an enterprise network and endpoints, as well as design and implement security solutions: This involves understanding the threats, vulnerabilities, and risks of an enterprise network and endpoints, and designing and implementing security solutions to mitigate them. 66. Engage in a highly collaborative process of idea generation, information sharing, and feedback that replicates key aspects of cybersecurity work: This includes engaging in a collaborative process of idea generation, information sharing, and feedback that replicates key aspects of cybersecurity work, and applying cybersecurity principles to real-world problems.
Indicative Contents	Indicative content includes the following. 1. Experimental Work (8hrs) 2. Data Analysis and Interpretation (8hrs) 3. Documentation and Reporting(6hrs) 4. Presentation and Demonstration(6hrs)

	5. Project Evaluation and Reflection(6hrs)
Learning and Teaching Strategies	
Strategies	• Promote student involvement through encourage students to be active participants in the project design process. • Create interdependence: Structure the project so that students are dependent on one another. For example, ensure that projects are sufficiently complex that students must draw on one another's knowledge and skills. • Assign projects that are relevant and meaningful to students. • Project-based learning is a teaching method in which students learn by actively engaging in real-world, meaningful, and personal projects. With this teaching strategy, students gain knowledge and skills over an extended period. • Backward course design is essential for project-based learning because it provides a planning framework that works back from the module's overall objectives, course, or project and creates a series of lessons built to help achieve these goals. • cooperative learning: Cooperative learning is a teaching strategy in which students work together in small groups to achieve a common goal. This strategy can help students develop teamwork and communication skills. • Provide continual feedback: Provide feedback to students throughout the project to help them improve their understanding and performance. • experiential learning

Student Workload (SWL)			
Structured SWL (h/sem)	34	**Structured SWL (h/w)**	2
Unstructured SWL (h/sem)	66	**Unstructured SWL (h/w)**	2
Total SWL (h/sem)	**100**		

Module Evaluation
تقييم المادة الدراسية

As		**Time/Number**	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**				
	Assignments	2	10% (10)	1, 2,3,4	LO # 1, 2, 3 and 4
	Projects / Lab.	14	15% (10)	Continuous	All
	Report	2	10% (10)	2,4	LO # 2 and 4
	Midterm Exam	2 hr	20% (20)	7	LO # 1 - 6

Summative assessment	**Final Exam**	3 hr	50% (50)	15	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

Week	Material Covered
Week 1,2,3,4	Experimental Work
Week 5	Data Analysis and Interpretation
Week 6,7,8,9	Documentation and Reporting
Week 10,11	Presentation and Demonstration
Week 12,13,14,15	Project Evaluation and Reflection
Week 16	Preparatory week before the final design proposal defense

Learning and Teaching Resources

	Text	Available in the Library?
Required Texts	By Subject	Yes
Recommended Texts		No
Websites		

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.