جامعة الخليج العربي
Arabian Gulf University

MASTER OF SCIENCE IN NEXT-GENERATION COMPUTING

College of Education, Administrative & Technical Studies | Department Name

An interdisciplinary program focusing on environmental management, water, and agriculture across the GCC region through scientific integration.

1. Track Overview

Track	Focus	Starting Page
AI and Formal Methods for Cybersecurity	This specialization aims to meet the needs of the GCC society for skilled human resources capable of dealing with the challenges of sound environmental management and actively contributing to sustainable development.	Page 2
Track 2	-	
Track 3	-	

جامعة الخليج العربي
Arabian Gulf University

MASTER OF SCIENCE IN NEXT-GENERATION COMPUTING

AI and Formal Methods for Cybersecurity

Total Credit Hours: 36

1. Program Track Overview

With the increase in the scale and sophistication of cyberattacks, new methods need to be employed to maintain the same level of security. One of these methods is the use of artificial intelligence to provide security operations analysts with early detection of security threats and vulnerabilities. Another is the use of formal methods techniques to verify the absence of security vulnerabilities at the design stage, allowing for the construction of highly secure protocols and critical systems. This program combines AI and formal methods to develop the next generation of cybersecurity, leading to significant innovations and providing real opportunities for research and development.

To obtain a master's degree, students must complete 36 credits as follows:

2. Study Plan

Course Code	Course Title	Credit Hours
Semester 1		
NGCM601	Logic & Discrete Mathematics	2
NGCM602	Foundations of Computer Science	2
NGCM603	Artificial Intelligence Fundamentals	2
NGCM604	Object Oriented Programming and Data Analysis	2
NGCM605	Scientific Writing	1
Total Credit Hours		**9**
Semester 2		
NGCM611	Cybersecurity Fundamentals	2
NGCM612	Artificial Intelligence for Information Security	2
NGCM613	Formal Methods for Information Security	2
NGCM614	Quantum Computing and Cybersecurity	2
NGCM615	Research Methodology	1
Total Credit Hours		**9**

Course Code	Course Title	Credit Hours
Semester 3		
See the list of Elective Courses	2 Elective Courses	4
NGCM697	Advanced Special Topics in Cybersecurity	1
NGCM698	Applied Project	4
Total Credit Hours		**9**
Semesters 4		
NGCM699	Master's Thesis	9
Total Credit Hours		**9**
Total Programme Credit Hours		**36**

Elective Courses:

Course Code	Course Title	Credit Hours
NGCM 641	Ethical Hacking and Systems Defense	2
NGCM 642	Network and Application Security	2
NGCM 643	Emerging Technology Security	2
NGCM 644	Cyber Risk Management	2
NGCM 645	Digital Forensics	2
NGCM 646	Big Data and Advanced AI	2

3. Course Descriptions

Logic & Discrete Mathematics (NGCM601)

In this course we will introduce the basic notions of logic and discuss what makes some arguments valid or invalid. This leads to a definition of a mathematical proof and in particular mathematical induction. This course focuses on the advanced concepts of propositional logic, predicate logic, higher-order logic, type theory and graph theory.

Foundations of Computer Science (NGCM602)

In this course, the students become familiar with computer architecture (processor, memory hierarchy, input, and output) and system software (compilers, assemblers, loaders, operating systems). Both fundamental concepts and practical examples are discussed. Then, we will give an introduction to algorithms and data structures. It aims to provide students with a toolbox of standard algorithms and data structures, as well as the skills to analyze the complexity and prove the correctness of an algorithm.

Artificial Intelligence Fundamentals (NGCM603)

In this course, we will present the guiding principles of AI, its applications and use cases, and how it is transforming our lives. We will present classic AI topics like problem-solving, knowledge representation and reasoning, and decision-making with uncertainty. Then, we will explore the basics of Machine Learning, Deep Learning, and the most popular learning algorithms, including supervised, unsupervised, semi-supervised, and reinforcement Machine Learning techniques.

Object Oriented Programming and Data Analysis (NGCM604)

Object-oriented programming offers numerous benefits, including faster development, reusability, and reduced maintenance costs. This course is designed to strengthen students' programming skills through extensive and engaging projects. It covers core object-oriented principles and provides a broad exposure to programming areas such as multi-threaded applications, inter-process communication, and database interactions. Additionally, we will focus on data visualization tools and teach students how to extract insights from data. Students will learn to create visualizations, analyze data trends, and build interactive dashboards.

Scientific Writing (NGCM 605)

This course introduces the essential components of effective scientific writing, focusing on crafting research papers for publication. Through interactive lessons and practical exercises, participants will learn how to structure a research manuscript, apply scientific writing principles, and navigate the publication process.

Cybersecurity Fundamentals (NGCM611)

Some of today’s most damaging attacks on computer systems involve the exploitation of network infrastructure, either as the target of attack or as a vehicle to attack end systems. This course focuses on the fundamentals of network security. The course provides an in-depth study of network attack techniques and methods to defend against them. Then, this course presents the security requirements and capabilities expected from modern hardware, operating systems, and other software environments. We will introduce topics such as a hardware refresher, hardware security, x86 security, side channels, OS

security, Linux and Windows security, SELinux, Android security, trusted execution environments, hypervisors and virtualization, system hardening, and system-stack attestation. Finally, we will present both the foundations and applications of cryptography. We will focus on the main tools of Modern Cryptography: symmetric encryption and authentication, public-key encryption, key agreement, digital signature schemes, and selected cryptanalytic techniques.

Artificial Intelligence for Information Security (NGCM612)

The goal of this course is to explain how machine learning is being applied to modern cybersecurity and threat detection. We will introduce the tools and techniques in network and software application threat mitigation and explain how artificial intelligence is used to support security analysts in their jobs.

Formal Methods for Information Security (NGCM613)

This course aims to explain how logic can be used to model problems of a computational or mathematical nature and how computers can be used to achieve this. In particular, we will present proof assistants, which allow one to formalize human reasoning by interactively constructing proofs and explain their use to certify the absence of bugs in programs. Then, we will focus on the modeling and analysis of security protocols for critical systems using formal methods, ranging from authentication protocols for network security to electronic voting protocols and online banking. We will introduce the key ideas and theoretical foundations of formal modeling and analysis of security protocols by using state-of-the-art tools.

Quantum Computing and Cybersecurity (NGCM614)

This course introduces the fundamentals of quantum computing (qubits, quantum circuits, and entanglement) and analyzes its impact on cybersecurity. Students study quantum algorithms like Shor's and Grover's that threaten current cryptographic systems, and explore quantum-resistant solutions, including post-quantum cryptography (e.g., Kyber, Dilithium) and Quantum Key Distribution (QKD). The course prepares students for the transition to the quantum era.

Research Methodology (NGCM615)

This course investigates research activities including project management, research project design and analyses, ethical considerations, proper literature review, scientific best practice (code of conduct) and dissertation preparation.

Advanced Special Topics in Cybersecurity (NGCM697)

This course covers topics of temporal or special interest which will not be made a regular on-going part of the curriculum. An experimental course may also be offered as a special topic course.

Applied Project (NGCM698)

This small group project gives students practical, hands-on experience to build their skills and confidence by working on real-world tasks in a collaborative setting.

Master's Thesis (NGCM699)

The master's thesis demonstrates a student's ability to apply the advanced knowledge and skills acquired in Artificial Intelligence and Formal Methods for Cybersecurity to address a complex problem in cybersecurity.

4. Elective Courses:

Ethical Hacking and Systems Defense (NGCM641)

This course is designed to introduce students to the fundamentals of hacking and becoming an ethical hacker. The course focuses on the code of conduct and ethics of attacking systems. The course also teaches the mindset of the criminal hacker and evolution of the hacker. Students also gain fundamental understanding and education on the elements of compromising computer systems for the explicit purposes of securing them from criminals. The course makes a very clear distinction between criminal hacking and ethical hacking, and only teaches the latter. The course then focuses on some fundamentals of system defense, including configurations and software to prevent unauthorized system access.

Network and Application Security (NGCM642)

This course provides a comprehensive foundation in securing modern networked environments. Students learn to defend against attacks on wired networks, wireless networks and web applications. Topics include Network protocols and exploits, common web vulnerabilities, and techniques for risk evaluation and mitigation. By the end of the course, students will be able to critically analyze and enhance the security of complex network and application infrastructures.

Emerging Technology Security (NGCM643)

This course examines security challenges and defense strategies for emerging technologies such as cloud computing, IoT, and blockchain. It covers cloud computing security models, IoT vulnerabilities and protection mechanisms, and blockchain security principles, including consensus, smart contracts, and decentralized trust. Students learn to evaluate and implement practical security controls for distributed and rapidly evolving systems.

Cyber Risk Management (NGCM644)

This course provides a comprehensive foundation in cyber risk management within modern organizations. Students learn to apply both qualitative and quantitative risk assessment methodologies. The course emphasizes identifying, analyzing, and prioritizing cybersecurity risks, developing risk treatment plans, and integrating cyber risk into organizational governance and strategic decision-making. By the end of the course, learners will be able to assess cyber risks, evaluate controls, and design risk-informed policies that strengthen the security posture of enterprises and critical sectors.

Digital Forensics (NGCM645)

This course provides a focused introduction to digital forensics, covering evidence identification, acquisition, preservation, and analysis across systems, networks, memory, and cloud environments. Students learn forensic standards, investigative methods, artifact interpretation, and reporting techniques. Basic incident response concepts are included to support forensic analysis, enabling learners

to reconstruct attacks and produce legally defensible forensic reports through hands-on labs and case studies.

Big Data and Advanced AI (NGCM646)

This course explores large-scale data processing and advanced AI methodologies. It covers database technologies and design principles underpinning the Big Data universe, as well as deep learning, generative models (VAEs, GANs), and reinforcement learning. Students gain skills to process complex datasets and leverage AI to extract insights and develop intelligent security solutions.