COURSE CONTENT

Academic Year	2022/2023	**Semester**	1 or 2
School/Programme	EEE/CME		
Course Code	EE6102		
Course Title	Cyber Security and Blockchain Technology 网络安全和区块链技术		
Pre-requisites	Nil		
No of AUs	3		
Contact Hours	Lecture 39 hours (13 weeks)		
Expected Implementation date of new/revised course	AY2022-2023, Semester 2		

Any cross-listing?
Is course opened to all Postgraduate students (including IGP) or specific program (please indicate)?

Within EEE							Outside EEE (Please specify)
MSc Programmes*					MEng	PhD	
CME	CCA	ET	PE	SP			
GE	GE	GE	GE	GE			

* List of MSc programmes

- MSc Communication Engineering (CME) Programme
- MSc Computer Control & Automation (CCA) Programme
- MSc Electronics (ET) Programme
- MSc Power Engineering (PE) Programme
- MSc Signal Processing (SP) Programme

Course Aims 课程的目标是

The industry 4.0 offers massive benefits to society but also provides opportunities to cyber attackers. Thus, the purpose of the first part of the course is to provide MSc students with the basic concepts of cyber security, and the necessary skills so that they can design cyber security policies and deploy appropriate technology to protect cyber space. Blockchain allows transactions of any kind to be simultaneously anonymous and secure. Thus, the aim of the second part of the course is to explain the basic concepts of Blockchain, its development, the potential business applications and how it can transform the world during Industry 4.0 revolution. This course is suitable for students studying MSc degree. Due to industry 4.0 and digital transformation, currently there is huge demands for jobs in this area and this demand will continue to increase as most industries will have to adopt industry 4.0 in order to remain competitive.

工业4.0为社会带来了巨大的利益，但也为网络攻击者提供了机会。
因此，课程第一部分的目的是为硕士学生提供网络安全的基本概念，以及必要的技能，以便他们能够设计网络安全策略并部署适当的技术来保护网络空间。
区块链允许任何类型的交易同时匿名和安全。
因此，课程第二部分的目的是解释区块链的基本概念，它的发展，潜在的商业应用以及它如何在工业4.0革命期间改变世界。
本课程适合攻读硕士学位的学生。
由于工业4.0和数字化转型，目前这一领域的就业需求巨大，而且这种需求将继续增加，因为大多数行业将不得不采用工业4.0以保持竞争力。

Intended Learning Outcomes (ILO)

By the end of this course, students should be able to:

预期学习成果（ILO）在本课程结束时，学生应该能够：

1) Identify and explain modern cyber security threats landscape
2) Design robust cyber security policies and learn modern cyber security technologies
3) Learn skills and strategies to implement, manage, control, and govern cyber security at corporate and national level
4) Understand basic concepts and types of Blockchain Technology

1)识别和解释现代网络安全威胁形势
2)设计强大的网络安全政策并学习现代网络安全技术
3)学习在企业和国家层面实施，管理，控制和治理网络安全的技能和策略
4)了解区块链技术的基本概念和类型
5)通过用例和案例研究，了解和学习不同行业中可能的应用。

网络安全威胁形势、工业4.0和网络安全、网络安全教育、意识和合规性、网络安全规划、政策和合规性、网络安全风险评估和基于生物识别的安全方法、公钥基础设施（PKI）、网络安全以及防火墙和入侵检测的作用、在线支付和加密货币。
区块链技术的基础知识，区块链技术的类型，区块链技术在工业4.0中的应用，用例和实际案例研究

5) Appreciate and learn possible applications in several industries with use cases and case studies.

Course Content

Cyber Security Threat Landscape, Industry 4.0 and Cyber Security, Cyber Security Education, Awareness and Compliance, Cyber Security Planning, Policies and Compliance, Cyber Security Risk Assessments and Biometric-based Security approaches, Public key Infrastructure (PKI), Web Security and role of firewalls and Intrusion Detection, Online Payment, and Cryptocurrencies. Basics of Blockchain technology, Types of blockchain Technology, Blockchain Technology Applications for Industry 4.0, use cases and real-world case studies

Assessment (includes both continuous and summative assessment) 评估（包括持续评估和总结性评估）

Note: It is advised that Group component and class participation should not be more than 40% and 20% respectively, unless with good justification.

注意：除非有充分的理由，否则建议小组组成和课堂参与分别不应超过40%和20%。

Component	ILO Tested	Weighting	Team/Individual	Assessment Rubrics
1. Final Examination	1, 2, 3, 4,5	50%	Individual	Complete assessment of the course
2. Continuous Assessment 1 (CA1): Quiz	1,2,4,5	30%	Individual	Test on comprehensive skills and understanding of the course
3. CA2: Assignment	1,2, 4	20%	Individual	
Total		100%		

Description of Assessment Components: 评估内容描述：

1. CA1: The quiz will include standard and challenging questions related to various topics covered in the course.
2. CA2: For this assignment, you will be required to do research, collect statistics related to cyber-attacks and blockchain technology, suggest suitable technology and procedures to enhance cyber security and submit a proper written report.

CA1：测试将包括与课程中涉及的各种主题相关的标准和具有挑战性的问题。
CA2：对于这项作业，你将被要求做研究，收集有关网络攻击和区块链技术的统计数据，建议适当的技术和程序，以加强网络安全，并提交适当的书面报告。

Formative feedback

CA1: For the quiz, you will receive feedback once you have received the results. In addition, you will have access to practice quiz questions, which will provide you useful feedback regarding your understanding of this course.

CA2: For this assignment, you will receive individual written feedback once the assignments have been marked.

CA1：对于测试，您将在收到结果后收到反馈。
此外，您还可以访问练习测验问题，这将为您提供有关您对本课程理解的有用反馈。
对于这个作业，一旦作业被标记，你将会收到个别的书面反馈。

每个模块都有基于MCQ的练习测验，不计入课程评估；
然而，即时的结果将使你发现你在这门课上做得如何。
对于错误的答案，你会收到详细的答案，这将使你正确地理解主题。
此外，YouTube和其他视频链接以及每个主题后面提供的进一步学习材料链接将加强和改善你的学习。
将会有交叉提问和互动讨论，这将加强和改善你对这门课程的理解和学习。

Learning and Teaching Approach 学习与教学方法

Note: Please include and indicate TEL component. 注：请包括并注明TEL部分。

Approach	**How does this approach support you in achieving the learning outcomes?**
Lecture	Each module will have MCQ based practice quizzes, which will not carry any marks towards the course assessment; however, the instant results will enable you to find out how you are doing in this course. For the wrong answers, you will receive detailed answers, which will enable you to understand the topics properly. In addition, YouTube and other video links and further study material links provided at the end of each topic will enhance and improve your learning. There will be cross-questions and interactive discussions, which will enhance and improve your understanding and learning about this course.
Extra Questions/Answers	Each week, standard and some challenging questions will be posted at the course site and students will be encouraged to try and solve those problems. Professor will guide you through the questions and you will have many opportunities to interact and ask questions to clarify your doubts. Also, at the end of each week, sample solutions will be uploaded at the course site, which will enable you to find out how you are doing in this course.
Online Discussion	This forum will be monitored, and your questions and doubts will be addressed regularly to help your understanding.

每周，标准问题和一些具有挑战性的问题将发布在课程网站上，学生们将被鼓励去尝试解决这些问题。
教授将指导你完成问题，你将有很多机会互动和提问，以澄清你的疑问。
此外，在每周结束时，示例解决方案将上传到课程网站，这将使您能够了解您在这门课程中的表现。

这个论坛将被监控，你的问题和疑虑将被定期解答，以帮助你理解。

Reading and References

Textbook:

(1) Stallings William, "Cryptography and Network Security: Principles and Practice", 8th Edition, Pearson/Prentice- Hall, 2020.

(1)Stallings William，“密码学与网络安全：原理与实践”，第8版，Pearson/Prentice- Hall，2020。

References:

(1) Sudeep Tanwar," Blockchain Technology: From Theory to Practice", Springer, 2022.
(2) Ralph Moseley "Advanced Cybersecurity Technologies", CRS Press, December 2021.

Course Policies and Student Responsibilities

Suggested fields for this portions include general policies with regards to students' assignment, punctuality absenteeism, etc.

课程政策和学生责任建议这部分内容包括与学生作业、准时缺勤等有关的一般政策。

(1) General

You are expected to complete all assigned pre-class readings and activities, attend all seminar classes punctually and take all scheduled assignments and tests by due dates. You are expected to

你应该完成所有指定的课前阅读和活动，按时参加所有的研讨会课程，
并在截止日期前完成所有预定的作业和测试。
你应该负责跟进他们错过的课程笔记、作业和与课程相关的研讨会通知。
你应该参加所有的研讨会讨论和活动。

take responsibility to follow up with course notes, assignments and course related announcements for seminar sessions they have missed. You are expected to participate in all seminar discussions and activities.

无正当理由缺课将影响你的整体课程成绩。
有效的理由包括生病并提供医疗证明，
参加南洋理工大学批准的活动并提供相关机构的借口信。

(2) Absenteeism

Absence from class without a valid reason will affect your overall course grade. Valid reasons include falling sick supported by a medical certificate and participation in NTU's approved activities supported by an excuse letter from the relevant bodies.

If you miss a lecture, you must inform the course instructor via email prior to the start of the class.

如果你错过了一节课，你必须在上课前通过电子邮件通知课程导师。

Academic Integrity

Good academic work depends on honesty and ethical behaviour. The quality of your work as a student relies on adhering to the principles of academic integrity and to the NTU Honour Code, a set of values shared by the whole university community. Truth, Trust and Justice are at the core of NTU's shared values.

As a student, it is important that you recognize your responsibilities in understanding and applying the principles of academic integrity in all the work you do at NTU. Not knowing what is involved in maintaining academic integrity does not excuse academic dishonesty. You need to actively equip yourself with strategies to avoid all forms of academic dishonesty, including plagiarism, academic fraud, collusion and cheating. If you are uncertain of the definitions of any of these terms, you should go to the Academic Integrity Handbook for more information. Consult your instructor(s) if you need any clarification about the requirements of academic integrity in the course.

Industry Participation

Company Name	Description of involvement (e.g., co-curation of course, speaker or instructor), include no. of course hours if known.	Contact Person	Email
NA			

Planned Weekly Schedule

Week	Topic	Course LO	Readings/ Activities
1	Cyber Security Threat Landscape Introduction to cyber security, threats and services, Security threat and responses. Attack and attackers 网络安全威胁概况介绍 网络安全、威胁与服务、安全威胁与应对。 攻击和攻击者	1, 2	Lectures week 1
2	Cyber Security Threat Landscape Deliberate software cyber-attacks (viruses, worms, Ransomware, Trojan, Bots, etc.), Social Engineering attacks, Human break-ins (hackers), Cybercrime and Cyber warfare. 网络安全威胁概况蓄意的软件网络攻击（病毒、蠕虫、勒索软件、特洛伊木马、机器人等）、社会工程攻击、人为入侵（黑客）、网络犯罪和网络战。	1,2	Lectures week 2
3	Industry 4.0 and Cyber Security 工业4.0与网络安全	1,2,3,4	Lectures week 3

	Trends and driving forces (cloud computing, IIoT, Big Data, virtualization, Cyber-Physical systems), Industry 4.0 opportunities and cyber security challenges, Smart manufacturing, Smart city, and cyber security.	趋势与驱动力（云计算、物联网、大数据、虚拟化、网络物理系统）、工业4.0机遇与网络安全挑战、智能制造、智慧城市、网络安全。	
4	Cyber security Education, Awareness and Compliance Frameworks and model for cyber security education and awareness, Cybersecurity compliance and challenges, Cybersecurity & HR issues.	1,2,3,4 网络安全教育、意识和合规性网络安全教育和意识的框架和模型、网络安全合规性和挑战、网络安全和人力资源问题。	Lectures week 4
5	Cyber Security Planning Cyber security planning principles, Technical and non-technical aspects of cyber security, Policy based cyber security approaches, Cyber security planning methodologies, Cyber security policy Enforcement, Accountability and Senior Leadership Oversight	1,2,3,4 网络安全规划：网络安全规划原则、网络安全的技术和非技术方面、基于政策的网络安全方法、网络安全规划方法、网络安全政策执行、问责制和高层领导监督	Lectures week 5
6	Cyber security risk assessments and Biometric bases security approaches Types of cyber risks, Software, and hardware cyber risks, Biometric-based cyber security protection (Fingerprint, face, iris, hand geometry, retina, DNA etc.).	1,2,3,4 网络安全风险评估和基于生物识别的安全方法网络风险类型，软件和硬件网络风险，基于生物识别的网络安全保护（指纹，面部，虹膜，手部几何，视网膜，DNA等）。	Lectures week 6
7	Public key Infrastructure (PKI) Cryptography (symmetric and asymmetric cryptography), Data Encryption Standard and Advanced Encryption Standard,	1,2,3,4 公钥基础设施（PKI）密码学（对称和非对称密码学），数据加密标准和高级加密标准	Lectures week 7
8	Public key Infrastructure (PKI) Overview of Public key systems (Diffie-Hellman, RSA, ECC, ElGamal) , Digital signature, digital certificates, and Hashing.	1,2,3,4 PKI （Public key Infrastructure）概述公钥系统（Diffie-Hellman、RSA、ECC、ElGamal）、数字签名、数字证书和哈希。	Lectures week 8
9	Web Security and role of firewalls and Intrusion Detection Web Security (SSL), Overview of Firewall, Intrusion Detection, and prevention system, Role of firewall and intrusion detection system in distributed denial of service (DDOS) attacks.	1,2 Web安全及防火墙与入侵检测Web安全（SSL）、防火墙概述、入侵检测与防御系统、防火墙与入侵检测系统在DDOS攻击中的作用。	Lectures week 9
10	Online Payment and Cryptocurrencies Digital cash, Mobile payment, Digital wallets, Development of Cryptocurrencies (Bitcoin, Ethereum, etc.), Future of Cryptocurrencies.	1,2,3,4 在线支付和加密货币数字现金，移动支付，数字钱包，加密货币的发展（比特币，以太坊等），加密货币的未来。	Lectures week 10
11	Blockchain Technology 区块链技术	1,2,3,4	Lectures week 11

	Introduction to Blockchain technology, Distributed Ledger Technologies, Types of Blockchain technology, various development stages of blockchain technology.	介绍区块链技术、分布式账本技术、区块链技术的类型、区块链技术的各个发展阶段。	
12	Blockchain Technology Blockchain technology for business applications, Blockchain Technology Applications for Industry 4.0, use cases and real-world case studies,	1,2,3,4,5	Lectures week 12 区块链技术面向商业应用的区块链技术，区块链面向工业4.0的技术应用，用例和现实案例研究，
13	Blockchain Technology How Blockchain can disturb the current status quo and brings new benefits to the whole society during Industry 4.0 period.	1,2,3,4,5	Lectures week 13 b区块链如何在工业4.0时期打破现状，为整个社会带来新的效益。

Other information(s)

NA