Module Definition Form (MDF)

Module code: MOD006570	**Version:** 4 **Date Amended:** 10/Jul/2024

1. Module Title
Cyber Security and AI Case Studies

2a. Module Leader
Raj Shukla

2b. School
School of Computing and Information Sciences at Anglia Ruskin University

2c. Faculty
Faculty of Science and Engineering

3a. Level
7

3b. Module Type
Standard (fine graded)

4a. Credits
15

4b. Study Hours
150

5. Restrictions

Type	Module Code	Module Name	Condition
Pre-requisites:	None		
Co-requisites:	None		
Exclusions:	None		
Courses to which this module is restricted:	MSc Artificial Intelligence with Cybersecurity MSc Artificial Intelligence with Cybersecurity [with placement]		

LEARNING, TEACHING AND ASSESSMENT INFORMATION

6a. Module Description

During your study you will be provided with an introduction to cybersecurity concepts and approaches ranging from network/web security and intrusion detection to cybersecurity programming and Linux scripting as well as how AI and machine learning techniques/algorithms can be leveraged to implement cyber thread intelligence. You will not be expected to have previous experience with threat detection, but it is desirable to have an understanding of network protocols, the Linux operating system and scripting, together with an understanding of web development and programming. Throughout the module, in addition to AI techniques for Cyber Security, we will also discuss applications of security for AI and how secure and safe machine learning can be obtained through secure model training and detection of adversarial samples.

Classes will include lectures, practical labs and research seminars/activities/case-studies enabling you to gain a deep understanding and practical experience on the topics while being aware on the latest research outcomes, advances and progresses in the area.

Knowledge of Cybersecurity and AI Case Studies will help you to be able to provide technical security consultancy to organisations on designing, applying and using Machine Learning solutions to address a wide range of organisational cybersecurity issues. It can help to improve your skills in a range of ML and Cybersecurity relevant techniques and tools (from concepts to implementations). In addition, your study will promote your capability to work as an independent researcher while being able to proactively and constructively work as part of a research team.

6b. Outline Content

- Network Security
- Web Security
- Cybersecurity Programming
- Cyber Threat Classification
- Machine Learning Algorithms
- Secure Machine Learning

6c. Key Texts/Literature

The reading list to support this module is available at: https://readinglists.aru.ac.uk/

6d. Specialist Learning Resources

You will work with Linux OS (Kali), Machine Learning and Cybersecurity tools and techniques.

7. Learning Outcomes (threshold standards)		
No.	**Type**	**On successful completion of this module the student will be expected to be able to:**
1	Knowledge and Understanding	Demonstrate a critical awareness of the role machine learning plays in modern threat detection systems.
2	Knowledge and Understanding	Define and identify techniques for threat detection in modern networks.
3	Intellectual, practical, affective and transferrable skills	Demonstrate an in-depth understanding of cybersecurity issues and relevant machine learning techniques and tools
4	Intellectual, practical, affective and transferrable skills	Assess and appraise how penetration testing tools can be applied to machine learning in threat detection.

8a. Module Occurrence to which this MDF Refers				
Year	**Occurrence**	**Period**	**Location**	**Mode of Delivery**
2026/7	ZZF	Template For Face To Face Learning Delivery		Face to Face

8b. Learning Activities for the above Module Occurrence			
Learning Activities	**Hours**	**Learning Outcomes**	**Details of Duration, frequency and other comments**
Lectures	24	1-2	Lecture 2 hr x 12 weeks
Other teacher managed learning	12	3-4	Tutorial 1 hr x 12 weeks
Student managed learning	114	1-4	Self-study, practical activities, and research 9 hrs x 12 weeks
TOTAL:	150		

9. Assessment for the above Module Occurrence

The assessment for some modules includes a presentation (see below for details on how this particular module is assessed). We recognise that presenting, especially to a large group, can cause significant anxiety or distress for some students. If this may affect you, please contact your Module Leader or the Disability and Neurodiversity Service as early as possible. We will work with you to consider appropriate reasonable adjustments. Depending on your individual needs, these might include, for example, presenting to a smaller group or presenting only to a member of academic staff.

Assessment No.	Assessment Method	Learning Outcomes	Weighting (%)	Fine Grade or Pass/Fail	Qualifying Mark (%)
010	Coursework	1-4	100 (%)	Fine Grade	30 (%)

Coursework

Assessment components for Element 010

Component No.	Assessment Title	Submission Method	Weighting (%)	Components needed for Mark Calculation?
010/1	Project report 1500 words	Canvas	50 (%)	All
010/2	In class test 45 minutes	Scheduled Activity: Timetabled assessment task	50 (%)	

In order to pass this module, students are required to achieve an overall mark of 40% (for modules at levels 3, 4, 5 and 6) or 50% (for modules at level 7*).

In addition, students are required to:
(a) achieve the qualifying mark for each element of fine graded assessment as specified above
(b) pass any pass/fail elements

[* the pass mark of 50% applies for all module occurrences from the academic year 2024/25 – see Section 3a of this MDF to check the level of the module and Section 8a of this MDF to check the academic year]