

WM9PH-15 Artificial Intelligence for Cyber Security

26/27

Department

WMG

Level

Taught Postgraduate Level

Module leader

Christo Panchev

Credit value

15

Module duration

4 weeks

Assessment

Multiple

Study location

University of Warwick main campus, Coventry

Description

Introductory description

AI-based solutions are having a significant impact in a number of areas, including cyber security. This module will provide students with an in-depth understanding of the main machine learning models, and their practical application in both offensive and defensive cyber operations. Furthermore, with the increasing ubiquity of AI in society and industry, the security of AI itself is becoming a critical factor. The module aims to cover this issue as part of the development and deployment of AI-based solutions.

Module aims

The module aim to develop student's knowledge of the development and application of the most common machine learning models, and in particular a critical understanding of the applicability of each machine learning algorithms in the solution of a particular problem (class of problems). It will cover the best practice and main steps of developing AI-based solution, including data collection/engineering and pre-processing, model design, training and evaluation, and deployment.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

Some of the main topics covered in the module include:

Methodology of developing an AI-based solution

Data collection, engineering and pre-processing

Unsupervised learning (clustering) models, such as k-means, nearest neighbour

Supervised learning models, such as linear/logistic regression, decision trees, random forest, SVM

Neural Networks (Deep learning) models, such as NLP, CNN, LSTM

Auto encoders

Generative AI

Security of AI

Learning outcomes

By the end of the module, students should be able to:

- Critically analyse an application domain and applicability of machine learning models in solving a specific problem.
- Collect, engineer and pre-process real-world data suitable for building machine learning models
- Develop, secure and optimise the performance a machine learning model
- Evaluate and interpret the results of a machine learning model.

Indicative reading list

[Reading lists can be found in Talis](#)

Subject specific skills

Data analysis

Decision support automation

Application of AI in offensive and defensive cyber operations

Security of AI

Transferable skills

Critical thinking

Analytical thinking

Study

Study time

Type	Required
Supervised practical classes	30 sessions of 1 hour (33%)
Private study	60 hours (67%)
Total	90 hours

Private study description

Further practical lab work and research.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A1

	Weighting	Study time	Eligible for self-certification
Machine learning project	100%	60 hours	Yes (extension)
Students will be provided with a data set and set a particular problem to solve. They will be expected to decide and justify a choice of a machine learning model, develop and evaluate a solution.			

Assessment group R1

	Weighting	Study time	Eligible for self-certification
Machine learning project	100%		No
Students will be provided with a data set and set a particular problem to solve. They will be expected to decide and justify a choice of a machine learning model, develop and evaluate a solution.			

Feedback on assessment

In a feedback form

Availability

Courses

This module is Core optional for:

- Year 1 of TWMS-H1S1 Postgraduate Taught Cyber Security Engineering (Full-time)
- Year 1 of TWMS-H1SH Postgraduate Taught Cyber Security Management (Full-time)