ROBERT GORDON UNIVERSITY ABERDEEN

This Module Version is not active until 01/Sep/2025

MODULE DESCRIPTOR

Module Title

Machine Learning for Cyber Security

Reference	CMM541	Version	3
Created	August 2024	SCQF Level	SCQF 11
Approved	May 2019	SCQF Points	15
Amended	November 2024	ECTS Points	7.5

Aims of Module

To provide students with the ability to evaluate and apply the methods, tools and techniques used in machine learning for cyber security.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Analyse the data science process lifecycle.
2	Evaluate the different machine learning algorithms used in cyber security.
3	Appraise the security of machine learning products.
4	Design machine learning solutions for defensive and offensive security.

Indicative Module Content

The case for Machine Learning (ML) in security. Data sets and Data types in security (e.g. structured vs unstructured, labelled vs unlabelled, overfitting vs underfitting, class imbalance, biased). ML product development lifecycle (e.g. TDSP or CRISP-DM). ML types (e.g. supervised, unsupervised, reinforcement). ML tasks (e.g. classification, clustering, regression, dimension reduction, density estimation, deep learning). Popular ML algorithms (e.g. LDA, CART, SVM, Naive bayesian, KNN, K-means, Random forests, Genetic algorithms, ANNs, Autoencoder). ML security applications: cracking CAPTCHA, detecting malicious URLs, detecting malware/ransomware, detecting phishing/spam emails, detecting network traffic anomalies and DOS attacks, detecting credit card fraud, securing autonomous systems (e.g., robotics), protecting communication channels and ensuring secure access controls. Challenges/limitations of ML in security. Guidelines for applying ML to security. Introduction to adversarial ML. Security of ML products. Programming in Python and using relevant tools and libraries.

Module Delivery

Key concepts are introduced and illustrated through lectures. The necessary practical skills are developed through a series of laboratory exercises.

Module Ref:	CMM541 v3

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	30
Non-Contact Hours	120	120
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	150
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4
Description:	Students will design and implement a Machine Learning solution to a given defensive/offensive security problem, and critically evaluate the vulnerabilities of Machine Learning (ML) algorithms.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of C1. An overall minimum grade of D is required to pass this module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in C1.
B	The student needs to achieve a B in C1.
C	The student needs to achieve a C in C1.
D	The student needs to achieve a D in C1.
E	The student needs to achieve an E in C1.
F	The student needs to achieve an F in C1.
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

Module Ref:	CMM541 v3

INDICATIVE BIBLIOGRAPHY

1	HALDER, S. and OZDEMIR, S., 2018. Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem. Birmingham, UK: Packt Publishing.
2	PALOMARES CARRASCOSA, I., Kalutarage, H.K and Huang, Y., eds., 2017. Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications. Springer.
3	STAMP, M., 2017. Introduction to machine learning with applications in information security. Chapman and Hall/CRC.
4	CHIO, C. and FREEMAN, D., 2018. Machine Learning and Security: Protecting Systems with Data and Algorithms. O'Reilly.