H9AIMLC: AI/ML in Cybersecurity

Module Code:	H9AIMLC
Long Title	AI/ML in Cybersecurity APPROVED
Title	AI/ML in Cybersecurity
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle
Credits:	5
Module Coordinator:	Arghir Moldovan
Module Author:	Arghir Moldovan
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	PhD/Master's degree in a computing or cognate discipline. May have industry experience also.

Learning Outcomes	
On successful completion of this module the learner will be able to:	
#	**Learning Outcome Description**
LO1	Critically analyse AI and machine learning techniques to assess best practice guidance and ethical implications when applied to specific cybersecurity problems.
LO2	Extract, clean and transform datasets in preparation for machine learning, and build evaluate machine learning models to extract knowledge from various cybersecurity datasets.
LO3	Critically review current AI and machine learning research and assess ethical considerations and research methods applied in the field.
LO4	Evaluate and utilise AI and machine learning technologies when designing and implementing cybersecurity solutions.

Dependencies
Module Recommendations
No recommendations listed
Co-requisite Modules
No Co-requisite modules listed

Entry requirements	Programme entry requirements must be satisfied.

H9AIMLC: AI/ML in Cybersecurity

Module Content & Assessment

Indicative Content
Introduction and Background • Module overview • Core terminology (e.g., types of AI, AI vs. ML, DL vs. ML, etc.). • High level overview or AI and ML applications in cybersecurity. • Benefits and limitations of AI/ML in cybersecurity. • How attackers are trying to reduce the effectiveness of AI/ML cybersecurity solutions. • Ethical implications of AI and ML.
AI/ML and Cybersecurity • Taxonomy and classification of AI and ML techniques used in the field. • Sources of data (e.g., network, device, applications, people) • Application requirements and complexity (e.g., real-time detection, signatures vs. anomaly models, data size, computational complexity) • Integrating ML models into production
Data Extraction and Preparation • Intro to prediction. • Extracting data from network, devices, and applications (e.g., packet capture, flow data, logs) • Exploring, cleaning, pre-processing, and visualising the data • Data transformation techniques (e.g., scaling, handling imbalance, feature selection, dimensionality reduction)
Prediction Models Evaluation • Data splitting and sampling methods (e.g., holdout, cross-fold validation, stratification, etc.). • Model tuning and overfitting • Determining the best model
Regression • Regression overview • Quantitative methods of performance. • The Bias-Variances trade-off • Regression methods and algorithms (e.g., Linear Regression, Multiple Linear Regression, PLS and PCR, etc.).
Classification • Classification overview • Classification methods and algorithms (e.g., Logistic Regression, K-Nearest Neighbours, Naïve Bayes)
Decision Trees • Decision Trees • Bagging • Random Forest • Boosting
Clustering • Notions of distance and similarity • Clustering algorithms (e.g., k-means, k-medoids) • Hierarchical clustering • Density based clustering • Plotting and understanding clusters • Cluster evaluation measures
Support Vector Machines • Support Vector Machines • Kernel methods • Hyperparameter optimization techniques
Neural Networks • Activation functions • Forward and back-propagation • Optimisation algorithms: gradient descent and stochastic gradient descent • Key parameters for neural networks
Deep Learning • A brief introduction to deep learning applied to different cybersecurity problems. • Deep learning concepts and topologies. • Ethical issues, explainability and visualisation of DL networks.
Revision • Revision and catch-up

Assessment Breakdown	%
Coursework	100.00%

Assessments

Full Time

Coursework

Assessment Type:	Formative Assessment	**% of total:**	Non-Marked
Assessment Date:	n/a	**Outcome addressed:**	1,2,3,4
Non-Marked:	Yes		

Assessment Description:
Formative assessment will be provided on the in-class individual or group activities. Feedback will be provided in written or oral format, or on-line through Moodle. In addition, in class discussions will be undertaken as part of the practical approach to learning.

Assessment Type:	Project	**% of total:**	100
Assessment Date:	n/a	**Outcome addressed:**	1,2,3,4
Non-Marked:	No		

Assessment Description:
The assessment will consist of a project that will evaluate all learning outcomes. Learners will have to identify a cybersecurity problem, review state-of-the-art research and industry solutions, assess the ethical implications, and apply suitable AI/ML algorithms, techniques, and tools. The project will consist of two stages. The initial submission will be a proposal report for formative feedback. The final submission will consist of a written report and the implemented solution artefact.

No End of Module Assessment

No Workplace Assessment

Reassessment Requirement

Coursework Only
This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Reassessment Description
The reassessment strategy for this module will consist of a project that will assess all learning outcomes.

H9AIMLC: AI/ML in Cybersecurity

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	24	Per Semester	2.00
Independent Learning	Independent learning	77	Per Semester	6.42
			Total Weekly Contact Hours	4.00

Workload: Blended

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	12	Per Semester	1.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Directed Learning	Directed e-learning	24	Per Semester	2.00
Independent Learning	Independent learning	77	Per Semester	6.42
			Total Weekly Contact Hours	4.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	24	Per Semester	2.00
Independent Learning	Independent learning	77	Per Semester	6.42
			Total Weekly Contact Hours	4.00

Module Resources

Recommended Book Resources

Emmanuel Tsukerman. Machine Learning for Cybersecurity Cookbook: Over 80 recipes on how to implement machine learning algorithms for building security systems using Python, 1st Ed. Packt Publishing, [ISBN: 9781789614671].

Alessandro Parisi. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies., Packt Publishing, [ISBN: 9781789804027].

Clarence Chio,David Freeman. Machine Learning and Security: Protecting Systems with Data and Algorithms., O'Reilly Media, Inc., [ISBN: 978-1491979907].

Supplementary Book Resources

Gareth James,Daniela Witten,Trevor Hastie,Robert Tibshirani. (2021), An Introduction to Statistical Learning: With Applications in R., 2nd Edition. Springer, p.603, [ISBN: 978-1071614174].

Ian Goodfellow,Yoshua Bengio,Aaron Courville. (2016), Deep Learning, MIT Press, p.801, [ISBN: 978-0262035613].

Soma Halder,Sinan Ozdemir. Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem, 1st Ed. Packt Publishing, [ISBN: 9781788992282].

Leslie F. Sikos. (2018), AI in Cybersecurity (Intelligent Systems Reference Library Book 151), Springer, p.205, [ISBN: 9783319988429].

This module does not have any article/paper resources

Other Resources

[Article], Demertzis, K., Iliadis, L.. (2015), A Bio-Inspired Hybrid Artificial Intelligence Framework for Cyber Security. In: Daras, N., Rassias, M. (eds) Computation, Cryptography, and Network Security, Springer, https://doi.org/10.1007/978-3-319-18275- 9_7

[Article], Calix, R. A., Singh, S. B., Chen, T., Zhang, D., & Tu, M.. (2020), Cyber Security Tool Kit (CyberSecTK): A Python Library for Machine Learning and Cyber Security. Information, 11(2), 100. MDPI AG., http://dx.doi.org/10.3390/info11020100

[Website], Stanford ML Course, https://www.coursera.org/specializations /machine-learning-introduction

[Website], DataCamp, http://www.datacamp.com

Discussion Note:	