Subject Description Form

Subject Code	EIE4121
Subject Title	Machine Learning in Cyber-security
Credit Value	3
Level	4
Pre-requisite	Nil
Co-requisite/ Exclusion	Nil
Objectives	1. To introduce concepts about machine learning techniques in cyber-security 2. To develop skills of using recent techniques for solving practical problems in cyber-security
Intended Learning Outcomes	**Upon completion of the subject, students will be able to:** Category A: Professional/academic knowledge and skills 1. Understand different machine learning techniques 2. Use different techniques for solving problems in cyber security Category B: Attributes for all-roundedness 3. Present ideas and findings effectively
Subject Synopsis/ Indicative Syllabus	**Syllabus:** 1. Machine learning techniques Introduction to machine learning; Basic concepts and classification; Supervised learning and unsupervised learning; classification; clustering; Neural Networks; Support vector machines; Dimensionality reduction; Deep learning 2. Machine learning development environments Software tools for implementing machine learning techniques; Generalization performance; Issues of over-fitting. 3. Malware Analysis Introduction to malware analysis; Types of malware analysis; static analysis, dynamic analysis; Behavioral vs code analysis; Use of machine learning techniques for malware detection such as K-Means, support vector machines, convolutional neural networks. 4. Phishing detection Introduction to phishing detection; Analysis of email/websites/message features for phishing characterization; Use of techniques such as logistic regression and decision tree for phishing detection. 5. Anomaly Detection Introduction to the anomaly definition; overview of anomaly detection techniques; static rules technique; use of machine learning techniques such as autoencoder for anomaly detection. **Laboratory Experiments:** Practical Works: 1. Introduction to machine learning framework 2. Evaluation of machine learning techniques in malware detection 3. Evaluation of machine learning techniques in phishing detection

Teaching/Learning Methodology

Teaching and Learning Method	Intended Subject Learning Outcome	Remarks
Lectures	1, 2	Fundamental principles and key concepts of the subject are delivered to students.
Tutorials	1, 2	Supplementary to lectures; Students will be able to clarify concepts and to have a deeper understanding of the lecture material; Problems and application examples are given and discussed.
Laboratory sessions	2, 3	Students will evaluate different kinds of machine learning techniques.
Mini-project	1, 2, 3	Students are required to study the use of machine learning techniques in cyber-security application. Students will need to submit a written report and make a presentation.

Assessment Methods in Alignment with Intended Learning Outcomes

Specific Assessment Methods/Tasks	% Weighting	Intended Subject Learning Outcomes to be Assessed (Please tick as appropriate)		
		1	2	3
1. Continuous Assessment (total 50%)				
• Tests	18%	√	√	
• Laboratory sessions	13%		√	√
• Mini-project	19%		√	√
2. Examination	50%	√	√	
Total	100%			

The continuous assessment consists of tests, laboratory exercises and a mini-project.

Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:

Specific Assessment Methods/Tasks	Remark
Tests	These can measure students' understanding of the theories and concepts as well as their comprehension of subject materials.
Examination	end-of chapter type problems used to evaluate students' ability in applying concepts and skills learnt in the classroom; students need to think critically in order to come with a solution for a problem.
Laboratory sessions,	oral examination will be conducted to evaluate

<table>
<tr><td></td><td colspan="2"><table><tr><td>mini-project</td><td>student's technical knowledge and communication skills.</td></tr></table></td></tr>
<tr><td rowspan="7">Student Study Effort Expected</td><td colspan="2">Class contact (time-tabled):</td></tr>
<tr><td>• Lecture</td><td>24 Hours</td></tr>
<tr><td>• Tutorial/Laboratory/Practice Classes</td><td>15 Hours</td></tr>
<tr><td colspan="2">Other student study effort:</td></tr>
<tr><td>• Lecture: preview/review of notes; homework/assignment; preparation for test/quizzes/examination</td><td>26 Hours</td></tr>
<tr><td>• Tutorial/Laboratory/Practice Classes: preview of materials, revision and/or reports writing</td><td>40 Hours</td></tr>
<tr><td colspan="2">Total student study effort:</td><td>105 Hours</td></tr>
<tr><td>Reading List and References</td><td colspan="2">1. Thomas Tony, Athira P. Vijayaraghavan, Sabu Emmanuel, "Machine learning approaches in cyber security analytics", Springer, 2020.
2. Padmavathi Ganapathi and D. Shanmugapriya, "Handbook of Research on Machine and Deep Learning Application for Cyber security", IGI Global, 2020.
3. Mark Stamp, Introduction to Machine Learning with Applications in Information Security, Chapman and Hall/CRC, 2017.
4. Chiheb Chebbi, Mastering Machine Learning for Penetration Testing, Packt Publishing Ltd, 2018.
5. Monnappa K A, Learning Malware Analysis, Packt Publishing Ltd, 2018.
6. Dipanjan Sarkar, Raghav Bali and Tushar Sharma, Practical Machine Learning with Python, Apress, 2018.</td></tr>
<tr><td>Last Updated</td><td colspan="2">June 2021</td></tr>
<tr><td>Prepared by</td><td colspan="2">Bonnie Law</td></tr>
</table>