COMP8325

Applications of Artificial Intelligence for Cyber Security

Session 1, Weekday attendance, North Ryde 2020

Department of Computing

Contents

General Information 2

Learning Outcomes 2

General Assessment Information 3

Assessment Tasks 3

Delivery and Resources 3

Unit Schedule 4

Policies and Procedures 5

Disclaimer

Macquarie University has taken all reasonable measures to ensure the information in this publication is accurate and up-to-date. However, the information may change or become out-dated as a result of change in University policies, procedures or rules. The University reserves the right to make changes to any information in this publication without notice. Users of this publication are advised to check the website version of this publication [or the relevant faculty or department] before acting on any information in this publication.

General Information

Unit convenor and teaching staff Convenor, Lecturer Xuyun Zhang xuyun.zhang@mq.edu.au Contact via +61 02 9850 8229 Room 287 BD Building, 4 Research Park Drive, Macquarie Park, NSW 2109 Lecturer Muhammad Ikram muhammad.ikram@mq.edu.au Contact via 0450607476 Room 286 BD Building, 4 Research Park Drive, Macquarie Park, NSW 2109
Credit points 10
Prerequisites (COMP6320 or ITEC653) or admission to MInfoTechCyberSec
Corequisites
Co-badged status
Unit description This unit deals with the applications of Artificial Intelligence in the field of Cyber Security. Topics covered include machine learning-based intrusion detection systems, malware detection, AI as a service, digital forensics, incident response leveraging SIEM data. Special attention will be given to the concept of adversarial machine learning.

Important Academic Dates

Information about important academic dates including deadlines for withdrawing from units are available at https://www.mq.edu.au/study/calendar-of-dates

Learning Outcomes

On successful completion of this unit, you will be able to:

ULO1: Explain the basic concepts and the limitations of Artificial Intelligence.

ULO2: Detect intrusion in networks and systems by applying tools and techniques revealing abnormal patterns in datasets.

ULO3: Communicate professionally in written and oral form to a range of audiences.

ULO4: Analyse the trends of applications of Artificial Intelligence in cyber security.

Assessment Tasks

Coronavirus (COVID-19) Update

Assessment details are no longer provided here as a result of changes due to the Coronavirus (COVID-19) pandemic.

Students should consult iLearn for revised unit information.

Find out more about the Coronavirus (COVID-19) and potential impacts on staff and students

General Assessment Information

Late Submission

No extensions will be granted without an approved application for Special Consideration. There will be a deduction of 10% of the total available marks made from the total awarded mark for each 24 hour period or part thereof that the submission is late. For example, 25 hours late in submission for an assignment worth 10 marks – 20% penalty or 2 marks deducted from the total. No submission will be accepted after solutions have been posted.

Supplementary Exam

If you receive special consideration for the final exam, a supplementary exam will be scheduled after the normal exam period, following the release of marks. By making a special consideration application for the final exam you are declaring yourself available for a resit during the supplementary examination period and will not be eligible for a second special consideration approval based on pre-existing commitments. Please ensure you are familiar with the policy prior to submitting an application. Approved applicants will receive an individual notification one week prior to the exam with the exact date and time of their supplementary examination.

Delivery and Resources

Coronavirus (COVID-19) Update

Any references to on-campus delivery below may no longer be relevant due to COVID-19.

Please check here for updated delivery information: https://ask.mq.edu.au/account/pub/display/unit_status

Classes

There will be one two-hour lecture each week and one one-hour workshop, you can find the time and location information can be found via MQ Timetables. You are expected to attend both classes as they provide complimentary learning activities each week. In practical classes you will write code and do experiments, and in lectures we will mainly discuss the theories, principles

and methods.

Textbooks

We do not have a single specific textbook, but will refer to the following texts for your reference during the semester:

David Freeman, Clarence Chio, "Machine Learning and Security", O'Reilly Media, Inc., 2018. (electronic edition available via MQ Library)

Sumeet Dua, Xian Du, "Data Mining and Machine Learning in Cybersecurity", Auerbach Publications, 2011.

Dhruba Kumar Bhattacharyya, Jugal Kumar Kalita, "Network Anomaly Detection: A Machine Learning Perspective", Chapman and Hall/CRC, 2013.

You will be given readings from these and other sources each week.

Technology Used and Required

We will make use of Python 3 for the analysis of cyber security related datasets, including a range of modules such as *scikit-learn, pandas, numpy, tensorflow, etc.* that provide additional features. These can all be installed via the Anaconda Python distribution. We will discuss this environment and the installation process in the first week of classes.

Project Work

A major part of the assessment in this unit is based on a project that you will complete in group. This will allow you to explore the techniques you are learning from classes in a real-world exercise of applying machine learning in cybersecurity.

Unit Schedule

Coronavirus (COVID-19) Update

The unit schedule/topics and any references to on-campus delivery below may no longer be relevant due to COVID-19. Please consult iLearn for latest details, and check here for updated delivery information: https://ask.mq.edu.au/account/pub/display/unit_status

Unit Schedule

The indicative list of topics is shown here, this is subject to change based on feedback from the class.

Week	Topics	Lecturer
1	Course overview; Python basics	ALL
2	Machine learning basics	XZ

3	Overview of ML application in cyber security	XZ
4	Anomaly detection	XZ
5	Data privacy issues	XZ
6	Adversary machine learning	XZ
7	Guest lecture	
8	Behaviour metrics attacks	MI
9	Vulnerability and malware analysis	MI
10	Botnets, DDoS attacks, and network traffic analysis	MI
11	Spam emails and phishing URLs	MI
12	Digital forensics and incident response	MI
13	Summary	ALL

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central). Students should be aware of the following policies in particular with regard to Learning and Teaching:

- Academic Appeals Policy
- Academic Integrity Policy
- Academic Progression Policy
- Assessment Policy
- Fitness to Practice Procedure
- Grade Appeal Policy
- Complaint Management Procedure for Students and Members of the Public
- Special Consideration Policy (***Note:*** *The Special Consideration Policy is effective from 4 December 2017 and replaces the Disruption to Studies Policy.)*

Students seeking more policy resources can visit the Student Policy Gateway (https://students.m

q.edu.au/support/study/student-policy-gateway). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

If you would like to see all the policies relevant to Learning and Teaching visit Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central).

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/study/getting-started/student-conduct

Results

Results published on platform other than eStudent, (eg. iLearn, Coursera etc.) or released directly by your Unit Convenor, are not confirmed as they are subject to final approval by the University. Once approved, final results will be sent to your student email address and will be made available in eStudent. For more information visit ask.mq.edu.au or if you are a Global MBA student contact globalmba.support@mq.edu.au

Student Support

Macquarie University provides a range of support services for students. For details, visit http://students.mq.edu.au/support/

Learning Skills

Learning Skills (mq.edu.au/learningskills) provides academic writing resources and study strategies to help you improve your marks and take control of your study.

- Getting help with your assignment
- Workshops
- StudyWise
- Academic Integrity Module

The Library provides online and face to face support to help you find and use relevant information resources.

- Subject and Research Guides
- Ask a Librarian

Student Services and Support

Students with a disability are encouraged to contact the Disability Service who can provide appropriate help with any issues that arise during their studies.

Student Enquiries

For all student enquiries, visit Student Connect at ask.mq.edu.au

If you are a Global MBA student contact globalmba.support@mq.edu.au

IT Help

For help with University computer systems and technology, visit http://www.mq.edu.au/about_us/offices_and_units/information_technology/help/.

When using the University's IT, you must adhere to the Acceptable Use of IT Resources Policy. The policy applies to all who connect to the MQ network including students.