COMP8325

Applications of Artificial Intelligence for Cyber Security

Session 1, Special circumstances 2021

School of Computing

Contents

Notice

As part of Phase 3 of our return to campus plan, most units will now run tutorials, seminars and other small group activities on campus, and most will keep an online version available to those students unable to return or those who choose to continue their studies online.

To check the availability of face-to-face activities for your unit, please go to timetable viewer. To check detailed information on unit assessments visit your unit's iLearn space or consult your unit convenor.

General Information

Unit convenor and teaching staff
Convenor, Lecturer
Muhammad Ikram
muhammad.ikram@mq.edu.au
Contact via +61 02 9850 8439
Room 286 BD Building, 4 Research Park Drive, Macquarie Park, NSW 2109

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

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.

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.

Assessment Tasks

Name	Weighting	Hurdle	Due
Class participation	10%	No	Weekly
Assignment	25%	No	Week7
Group project and presentation	20%	No	Week 12
Final examination	45%	No	Exam Week

Class participation

Assessment Type [1]: Participatory task
Indicative Time on Task [2]: 0 hours
Due: **Weekly**
Weighting: **10%**

Each week, a mark will be awarded based on the level of participation shown by students in the discussion during the lectures.

On successful completion you will be able to:

- Explain the basic concepts and the limitations of Artificial Intelligence.
- Detect intrusion in networks and systems by applying tools and techniques revealing abnormal patterns in datasets.
- Communicate professionally in written and oral form to a range of audiences.
- Analyse the trends of applications of Artificial Intelligence in cyber security.

Assignment

Assessment Type [1]: Project
Indicative Time on Task [2]: 30 hours
Due: **Week7**
Weighting: **25%**

In this assignment, the student will be given a series of datasets and will be asked to develop an analysis of this data and provide a report. The aim of this task is to be able to identify unusual patterns and abnormal activity using data.

On successful completion you will be able to:

- Detect intrusion in networks and systems by applying tools and techniques revealing abnormal patterns in datasets.
- Communicate professionally in written and oral form to a range of audiences.

Group project and presentation

Assessment Type [1]: Project
Indicative Time on Task [2]: 30 hours
Due: **Week 12**
Weighting: **20%**

In this assessment task, students as a group will be required to research and evaluate a tool leveraging AI for cyber security purposes. The task also involves a presentation of the findings.

On successful completion you will be able to:

- Detect intrusion in networks and systems by applying tools and techniques revealing abnormal patterns in datasets.
- Communicate professionally in written and oral form to a range of audiences.

- Analyse the trends of applications of Artificial Intelligence in cyber security.

Final examination

Assessment Type [1]: Examination
Indicative Time on Task [2]: 15 hours
Due: **Exam Week**
Weighting: **45%**

A three hour examination in the exam period.

On successful completion you will be able to:

- Explain the basic concepts and the limitations of Artificial Intelligence.
- Communicate professionally in written and oral form to a range of audiences.
- Analyse the trends of applications of Artificial Intelligence in cyber security.

---

[1] If you need help with your assignment, please contact:

- the academic teaching staff in your unit for guidance in understanding or completing this type of assessment
- the Writing Centre for academic skills support.

[2] Indicative time-on-task is an estimate of the time required for completion of the assessment task and is subject to individual variation

Delivery and Resources

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

Unit Schedule

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

Week	Topic	Lecturer
1	Course overview; Python basics	MI + XZ
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	TBD
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	Revision	MI + XZ

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://policies.mq.edu.au). 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

Students seeking more policy resources can visit Student Policies (https://students.mq.edu.au/support/study/policies). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

To find other policies relating to Teaching and Learning, visit Policy Central (https://policies.mq.edu.au) and use the search tool.

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/admin/other-resources/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.