COMP8325

Applications of Artificial Intelligence for Cyber Security

Session 1, In person-scheduled-weekday, North Ryde 2024

School of Computing

Contents

General Information

Unit convenor and teaching staff
Muhammad Ikram
muhammad.ikram@mq.edu.au

Hassan Asghar
hassan.asghar@mq.edu.au

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

Online quizzes, in-class activities, or scheduled tests and exams must be undertaken at the time indicated in the unit guide. Should these activities be missed due to illness or misadventure,

students may apply for Special Consideration.

All other assessments must be submitted by 11:55 pm on their due date.

Late Assessment Submission Penalty

Unless a Special Consideration request has been submitted and approved, a 5% penalty (of the total possible mark of the task) will be applied for each day a written report or presentation assessment is not submitted, up until the 7th day (including weekends). After the 7th day, a grade of '0' will be awarded even if the assessment is submitted. The submission time for all uploaded assessments is **11:55 pm**. A 1-hour grace period will be provided to students who experience a technical concern.

For any late submission of time-sensitive tasks, such as scheduled tests/exams, performance assessments/presentations, and/or scheduled practical assessments/labs, please apply for Special Consideration.

Assessments where Late Submissions will be accepted

Class participation -- YES, Standard Late Penalty applies

Assignment, Group project and presentation, and Final examination -- NO, unless special consideration is Granted

Special Consideration

The Special Consideration Policy aims to support students who have been impacted by short-term circumstances or events that are serious, unavoidable, and significantly disruptive, and which may affect their performance in assessment. If you experience circumstances or events that affect your ability to complete the assessments in this unit on time, please inform the convenor and submit a Special Consideration request through ask.mq.edu.au.

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.

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.

Assignment

Assessment Type [1]: Project Indicative Time on Task [2]: 30 hours Due: **Week 7** 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. This task aims 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.

[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

Requirements to Pass this Unit

To pass this unit you must:

- Achieve a total mark equal to or greater than 50%, and
- Achieve at least 50% in the final examination

Assessment Tasks

Name	Weighting	Hurdle	Due
Class participation	10%	No	23:55 Wednesdays (week 2--13)
Final examination	45%	No	Exam Week
Assignment	25%	No	23:55 Friday, Week 7
Group project and presentation	20%	No	23:55 Friday, Week 12

Class participation

Assessment Type [1]: Participatory task
Indicative Time on Task [2]: 0 hours
Due: **23:55 Wednesdays (week 2--13)**
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.

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.

Assignment

Assessment Type [1]: Project
Indicative Time on Task [2]: 30 hours
Due: **23:55 Friday, Week 7**
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: **23:55 Friday, 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.

---

[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

There will be one two-hour lecture each week and one one-hour workshop (starting from Week 1), 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.

Methods of Communication

We will communicate with you via your university email or through announcements on iLearn. Queries to convenors can either be placed on the iLearn discussion board or sent to their email address from your **university email** address.

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 a 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.

COVID Information

For the latest information on the University's response to COVID-19, please refer to the Coronavirus infection page on the Macquarie website: https://www.mq.edu.au/about/coronavirus-faqs. Remember to check this page regularly in case the information and requirements change during semester. If there are any changes to this unit about COVID-19, these will be communicated via iLearn.

Unit Schedule

Week	Topic
1	Course overview; Python basics
2	Overview of ML application in cyber security
3	Regression and classification
4	Anomaly detection I
5	Anomaly detection II
6	Private and secure machine learning
7	Behaviour metrics attacks (recorded due to public holiday)
8	Vulnerability and malware analysis (recorded due to public holiday)
9	Botnets, DDoS attacks, and network traffic analysis
10	Spam emails and phishing URLs
11	Digital forensics and incident response
12	Guest lecture
13	Revision

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
- Assessment Procedure
- Complaints Resolution 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

Academic Integrity

At Macquarie, we believe academic integrity – honesty, respect, trust, responsibility, fairness and courage – is at the core of learning, teaching and research. We recognise that meeting the expectations required to complete your assessments can be challenging. So, we offer you a range of resources and services to help you reach your potential, including free online writing and maths support, academic skills development and wellbeing consultations.

Student Support

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

The Writing Centre

The Writing Centre provides resources to develop your English language proficiency, academic writing, and communication skills.

- Workshops
- Chat with a WriteWISE peer writing leader
- Access StudyWISE
- Upload an assignment to Studiosity

- Complete the 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

Macquarie University offers a range of Student Support Services including:

- IT Support
- Accessibility and disability support with study
- Mental health support
- Safety support to respond to bullying, harassment, sexual harassment and sexual assault
- Social support including information about finances, tenancy and legal issues
- Student Advocacy provides independent advice on MQ policies, procedures, and processes

Student Enquiries

Got a question? Ask us via AskMQ, or contact Service Connect.

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.

Changes from Previous Offering

Student feedback from the previous offering of this unit was very positive overall, with students pleased with the clarity around assessment requirements and the level of support from teaching staff. As such, no change to the delivery of the unit is planned, however we will continue to strive to improve the level of support and the level of student engagement.

Unit information based on version 2024.01R of the Handbook