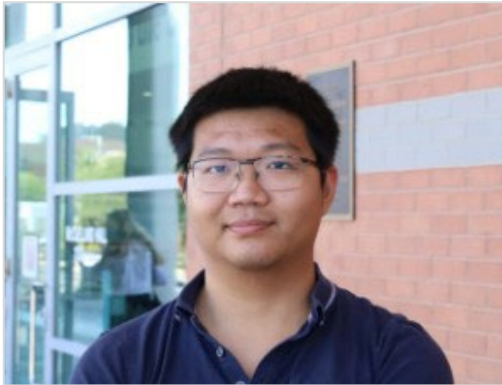


Instructor Contact Information



Instructor: James Hu, PHD Candidate
Office Hours: By appointment. Send email *at least one day* in advance to schedule.
Email: jameshu@arizona.edu
Webpage: <https://eller.arizona.edu/people/james-hu>

Course Overview

This graduate level course is designed to provide students with a hands-on introduction to the fundamental concepts and tools of Artificial Intelligence (AI) and its application in cybersecurity. Students will become familiar with the fundamentals of AI, Deep Learning, Transformers, Large Language Models. Students will learn how to apply these AI techniques under a framework based on Data Analytics and Adversarial AI. In addition to AI research knowledge, this course will deliver cutting edge research examples of how adversaries are leveraging AI to threaten cybersecurity and how cybersecurity analysts can leverage AI to counteract these AI-enabled threats. These domains include Phishing Detection and AI Model Security. Students will gain significant experience in implementing and evaluating AI by creating a novel AI4Cyber research project and paper utilizing the aforementioned AI techniques.

Prerequisite Requirements

No formal prerequisites are required; however, the following background knowledge is recommended:

- Proficiency in programming languages such as Python, R, Java, or C/C++ (Python preferred).
- Familiarity with mathematics and basic statistical concepts.

Course Learning Outcomes

Upon successful completion of this course, students will be able to:

- Collect and preprocess data
- Implement ML & AI systems
- Implement GenAI systems
- Attack and Improve AI systems

Course Readings and Materials

Required Readings

All required course readings and materials will be available on Brightspace/D2L.

Course Workload Expectations

This course is structured around **7** weeks. Given this condensed timeframe, you should expect a heavier than normal workload. The course workload is estimated below.

Course Item	Estimated Hours
Watch and study course lectures	30 hours
Reading materials and practicing tools	20 hours
Preparing for exams	15 hours
Project Milestone 1	10 hours
Project Milestone 2	20 hours
Project Milestone 3	20 hours
Final Project	20 hours

This averages out to be approximately **19** hours/week for the course. These estimates will vary depending upon the student's knowledge level and/or time commitment.

Course Schedule

The expected weekly progress and deliverables are outlined in the course schedule. Please see the course schedule as posted in the course space.

There is a considerable amount of material covered in this class. It is essential that you stay current with all reading and homework assignments. Note **DUE Dates** on course deliverables.

Working Ahead of Schedule

To maintain the integrity of the group learning environment, this course is not structured to allow students to work ahead.

Course Time Zone

All dates and times mentioned in this course represent Mountain Standard Time (Arizona), which are UTC-7 hours. Arizona does not observe Daylight Savings Time. You can use the following link to get the current local time in Tucson, Arizona: <http://www.timeanddate.com/worldclock/city.html?n=393>

Office Hours and Communications

Please use the **Ask the Instructor** discussion forum in the course space to contact the instructor for content related questions. All students can then benefit from the response. Under normal circumstances, the instructor will respond within 24 hours of your post Monday through Friday and 48 hours on Saturday and Sunday. If you have a question regarding your personal performance in the course, please email the instructor directly using the address above. When appropriate, the instructor will provide feedback on course work that needs to be manually graded (e.g., essay papers, projects) within 3-5 days of submission. You will be able to see results for automatically graded course work (online quizzes) after the specified deadline.

Office Hours

The instructor will host virtual office hours in the Zoom tool located in the course space on the left of the screen under **Table of Contents -> Office Hours** by appointment. Please email the instructor **at least one day** in advance to set up a time to meet. Please start the email subject with **MIS 555** and include your **available days and times** in the email.

Brightspace (D2L) Learning Management System

This course uses the UA Brightspace/D2L learning management system. You are **required** to use Brightspace with this class and are encouraged to check our class course space daily.

You are also encouraged to have Brightspace email forwarded to your primary email account. The instructor will use Brightspace for course assignments, quizzes, exams, content distribution, and important announcements. The UA Brightspace system is available at: <https://d2l.arizona.edu/>.

Assignments and Assessments

Generative AI Policy

Important: In this course, generative artificial intelligence/large-language-models (AI/LLM) tools, such as ChatGPT, Dall-E, and Gemini, may be used to assist with research on individual and group assignments, as long as there is proper acknowledgment and citation.

If you are in doubt as to whether you are using generative AI tools appropriately in this course, I encourage you to discuss your situation with me. Be aware that many AI companies collect information; do not enter confidential information as part of a prompt. LLMs may make up or hallucinate information. These tools may reflect misconceptions and biases of the data on which they were trained and the human-written prompts used to steer them. You are responsible for checking facts, finding reliable sources for, and making a careful, critical examination of any work that you submit.

Course Project

Many firms are actively researching how to integrate AI into their cybersecurity operations to protect their interests. For this project, students will assume the role of such a researcher and identify, explore, implement, evaluate, and present a completed AI4Cyber research project pertaining Threat Analysis. Students are required to develop and manage all aspects of the project, including data collection, model implementation, and method evaluation. Students will have three graded milestones, each containing a PowerPoint slide deck and implementation code. The PowerPoint slide deck demonstrates the current progress of their research project. The implementation code is in python and should contain the runtime results in either a Jupyter Notebook or another accessible format. In addition to the three graded milestones, students are to submit a final report written in IEEE conference format at the end of class. Full details about each milestone's submission, project report and related grading rubrics, presentation guidelines, as well as project examples will be posted in the **Table of Contents -> Project Proposal and Milestones** area of the course space.

Students are allowed to work individually, in pairs, or in groups of three. Each team share the same grade amongst each member and may submit the same files for grading. Please note that the project and its workload was designed with the intention of being completed in a group setting (2+). Students choosing to work individually must do so prepared for the increased workload.

Irrespective of group composition, students are required to manage their own technology set ups. **Please elect a leader once your team is formed. Leaders are responsible for submitting a document that includes your group details into Brightspace/D2L.** Numerous tutorials and resources will be provided on D2L to help students with

selected data collection, aggregation, and analytics tasks. However, it is each student's responsibility to manage their technical knowledge and learning. Due to the limited time in this class, it is impossible to teach all the technological variations and implementation. Thus, students are expected to have a positive attitude and demonstrate the ability to learn and self-teach any technologies they are unfamiliar with but want/are required to use for their project.

Team Collaboration Policy: To facilitate healthy and productive group collaboration, I will ask for peer evaluations on your team's collaboration throughout the semester. If there is consensus and proof that a team member is not contributing, communication between the student and me will be conducted, and his or her grades on team project assignments will also be deducted accordingly.

Final Exam

There is one online exam associated with this course. The Exam covers learning materials of weeks 1 through 6. Each exam will contain 3 – 4 essay format questions. The Exam is open book and open note. Students have one week to complete the exam from when it opens. You will have 2 hours and one attempt to complete each exam. Please consult the course schedule for exam schedules. During the exam, you are allowed to access external resources (notes, websites, and course materials). However, the use of AI tools or seeking help from others are strictly prohibited.

Turning in Assignments

All graded assignments and assessments will be submitted electronically through the course space. Specific submission instructions are provided for each assignment in the course space.

Late Assignment Policy

Late assignments will not receive points. Please allow yourself time to mitigate any computer glitches.

Course Grading

Course grades will be determined based on the items listed below.

Course Work	Points	Percentage
Final Exam	100	25%
Project Milestone 1	40	10%
Project Milestone 2	100	25%
Project Milestone 3	60	15%
Final Project	200	50%
TOTAL	500	100%

The approximate final course grade breakdown will be as shown below.

Total Points	Percentage	Letter Grade
450 – 500	90%-100%	A
400 – 449	80%-89%	B
350 – 399	70%-79%	C
300 – 349	60% -69%	D
0 – 299	0%-59%	E

Incomplete Policy

If you experience extraordinary circumstances beyond your control, which prevent you from completing the course within the scheduled 7-week timeframe, you must request an incomplete by emailing the Instructor **before the end of the course**. Please clearly explain the reasons for the request and provide relevant documentation. Please be aware that you must be receiving a passing grade at the time of the request. If granted an incomplete, you should review the related policy stipulations at <https://www.registrar.arizona.edu/grades/incomplete-i-grade>

Academic Policies and Institutional Resources

Academic Policies and Procedures

As a University of Arizona student, you are expected to become familiar with and abide by the university-wide policies and procedures. You can find complete, up-to-date information at <https://academicaffairs.arizona.edu/syllabus-policies>

Academic Integrity

Upon accepting admission to the University of Arizona (UA), you immediately assumed a commitment to uphold the Code of Academic Integrity. Complete copies of the UA and Eller policies can be found online at:

- The University of Arizona: <https://deanofstudents.arizona.edu/policies/code-academic-integrity>
- Eller College of Management: <https://eller.arizona.edu/programs/undergraduate/advising/policies-expectations/integrity-guide>

Any instances of academic dishonesty will result in a grade of E for the course.

While it is our sincere hope that you will not engage in academic misconduct, it seems prudent to clarify in advance the policy on dishonest behavior.

Reminder: this course has a zero-tolerance policy on cheating, including undeclared or deceptive use of artificial intelligence systems for document and content production.

Online Collaboration/Netiquette

In MISONline courses, you will primarily communicate with instructors and peers virtually through a variety of tools such as discussion forums, email, and web conferencing. The following guidelines will enable everyone in the course to participate and collaborate in a productive, safe environment.

- Be professional, courteous, and respectful as you would in a physical classroom.
- Online communication lacks the nonverbal cues that provide much of the meaning and nuances in face-to-face conversations. Choose your words carefully, phrase your sentences clearly, and stay on topic.
- It is expected that students may disagree with the research presented or the opinions of their fellow classmates. To disagree is fine but to disparage others' views is unacceptable. All comments should be kept civil and thoughtful. Remember that this course abides by university policies regarding disruptive behavior.
- Compose your messages and posts in a word processing tool, and check your spelling and grammar before submitting your post / email.

UA MISONline Student Support

The instructor is available to assist with content-related issues. You may, at any time, email the instructor. This course also provides an Ask the Instructor discussion forum. You are encouraged to post content-related questions to this forum at any time. The instructor monitors this forum on a regular basis and will respond in a timely fashion. It is common for other students to participate in answering questions posted in the Ask the

Instructor forum. You should feel free to contribute to the solution if you can provide knowledge or guidance related to the question.

The following are guidelines for requesting support:

- **General Course Questions:** Use the **Ask the Instructor** discussion forum for questions regarding course materials or policy.
- **Personal Course Questions:** Email the instructor to discuss grades or personal concerns.
- **Course Registration & Curriculum Questions:** Email misonline@eller.arizona.edu.
- **Brightspace Support Questions:** Click on <https://studenthelp.intech.arizona.edu/article/261-contact-us> to submit your tech support request.

Statement of copyrighted materials

All course materials (for example, lecture notes, lectures, and study guides) disseminated by the Instructor to the students, whether in class or online, are original materials and reflect the intellectual property of the instructor or author of those works as well as the Arizona Board of Regents (ABOR). All course materials are intended for individual use by students. You may not distribute or reproduce these materials for commercial purposes without the express written consent of the Instructor. Students who sell or distribute these materials for any use other than their own are in violation of the University's Intellectual Property Policy (available at <http://policy.arizona.edu/research/intellectual-property-policy>). Violations of the Instructor's and ABOR's copyright may violate the Code of Academic Integrity and result in course sanctions.

Disability Accommodations

At the University of Arizona, we strive to make learning experiences as accessible as possible. If you anticipate or experience barriers based on disability or pregnancy, please contact the Disability Resource Center (520-621-3268, <https://drc.arizona.edu/>) to establish reasonable accommodations.

Library Support

The University of Arizona Libraries is dedicated to providing the research tools you need at any time. For an abbreviated list of resources directly related to a specific course, select the **Library** link (located in the *Table of Contents* on the left of the screen). If you need any assistance, please contact the library using the **Chat** or **Ask Us** tools on the <https://lib.arizona.edu/> website.

Course Surveys and Evaluations

There are two online surveys associated with this course:

- **MIS course specific survey** – assists course designers with refining elements of the course. This survey is conducted by the MISonline team prior to the end of the course.
- **UA Student Course Survey** – standard course evaluation conducted by the University of Arizona. This will be made available through <https://login.watermarkinsights.com/connect/universityofarizona> at the appropriate time during the course. **Important:** if this link does not work, please look for an email from Watermark or go to the Brightspace homepage to access the survey.

Please participate in these online surveys! I use the comments to make changes to the course to meet student needs.

Subject to Change Statement

Information contained in the course syllabus, other than the grade and absence policy, may be subject to change with advance notice, as deemed appropriate by the instructor.