CSCI 459, AI Enhanced Security

COURSE SYLLABUS: Spring 2024

INSTRUCTOR INFORMATION

Instructor	Dr. Srujan Kotikela
Office Location	RELLIS ACB2-210
Office Hours	Tu/Thu 9:30 AM -11:30 AM or by appointment
Email	srujan.kotikela **at** tamuc **dot** edu (1-2 business days) Email subject MUST contain CSCI 459 – Spring2024
Communication Response Time	Within 24 hours on weekdays, but any communication after Friday 5pm will be responded to by the following Monday

COURSE INFORMATION

Lectures (Time/Location):

- Monday / Wednesday, 1:25 – 2:40 PM. In-person (room TBD).

Textbook(s) Required:

- None

Recommended Textbook(s), References & Resources:

Generally, we will utilize resources from the internet including but not limited to open-source projects, GitHub repositories, and research papers.

Course Description

This course will provide key terminology and techniques to understand AI and cybersecurity. It emphasizes on how to adopt AI techniques, such as machine learning algorithms and big data techniques to enhance the security and privacy for various computing systems. The course will illustrate cutting-edge techniques and provide hands-on experiences on combining AI with cybersecurity to enhance various secure systems.

Student Learning Outcomes

Upon completing this course students should be able to:

- Understand the fundamental concepts of Machine Learning and Artificial Intelligence in the context of cybersecurity.
- Understand, develop and apply AI/ML tools and algorithms for different cybersecurity applications.
- Understand and implement the AI/ML lifecycle including performance assessment.
- Understand the capabilities and limitations/risks of AI applications in cybersecurity.

COURSE REQUIREMENTS

The *syllabus/schedule are subject to change.*

Minimal Technical Skills Needed

Prerequisites: CSCI 310, MATH 2414, and MATH 403.

Instructional Methods

During this course, we will be using traditional and active learning methods, and work together using:

- Lectures: using slides, supplementary materials, and hands-on exercises.
- Assignments/labs: that will be released via the Learning Management Systems (D2L).
- Individual projects: details of the project will be released during weeks 3.

Student Responsibilities and Tips for Success in the Course

You own your success in this course, including ensuring you understand the expectations, timelines, policies and learning objectives.

Baseline expectations:

a. Check LMS frequently and remain current with the course content and assignments
b. Start your homework assignments early so that you can ask for help if needed.
c. Check the feedback on homework assignments.
d. Do your own work: you are encouraged to collaborate and consult with classmates to improve your understanding and to develop problem-solving strategies. However, cheating and plagiarism will not be tolerated, i.e. do not copy other people's work.
e. Communicate with the instructor when you are confused or having difficulties with the course material / assignment / project.
f. Get help (sooner than later) if you have challenges or problems:
    - Start or join a study group with classmate(s) from the course to compare notes and discuss class content.

GRADING & ASSESSMENTS

Final grades in this course will be based on the following scale: A = 90%-100%, B = 80%-89%, C = 70%-79%, D = 60%-69%, F = 59% or below.

Assessments

Assessment Type	Weight of Final Grade	Learning Objectives
Assignments, labs, quizzes and participation	35 %	Critical understanding and problem solving using course concepts
Midterm Exam	20 %	
Final Exam	20 %	
Project	25 %	

Project Information: A significant component of the course consists of selecting a semester project. Each student is to work on their project individually. Students are expected to share regular updates on their project progress. More details on the project will be shared during week 2/3 of the course.

COURSE OUTLINE / CALENDAR

- **Tentative calendar**

Week	Course Subject
Week 1	Introduction and System Setup
Weeks 2, 3	Background Review
Week 3	**Projects Assigned**
Week 4, 5	AI for Cybersecurity Application 1
Week 6, 7	AI for Cybersecurity Application 2
Week 8	Review, **Midterm Exam**
Week 9	**Spring Break**
Week 10, 11	AI for Cybersecurity Application 3
Week 12, 13	AI for Cybersecurity Application 4
Week 14	Assessing AI for Cybersecurity: Challenges and Opportunities
Week 15	Ethics and security of Artificial Intelligence for Cybersecurity
Week 16	**Project Presentations, Final Exam**

*The schedule is **tentative** and may be adjusted to fit the actual class progress.

Submitting Assignments:

- There will be several assignments, labs, and/or quizzes that are tightly related to the class materials and topics. Submissions are expected to be completed in good quality and by the deadlines.
- Your completed work must be placed in the appropriate dropbox in D2L Online**. DO NOT EMAIL ME ANY ASSIGNMENTS AS THEY WILL BE DELETED.** If you have challenges in accessing D2L temporarily, you can email me your assignment as a proof of on-time submission. **However**, you still need to upload it to the assignment folder as soon the issue is resolved to receive credit.
- You MUST check your files before and after uploading them to D2L to ensure they can be open appropriately. In the case that the instructor is not able to open your submission file(s) your submission will not be graded.
- Unless special instructions are provided**, assignments are NOT to be posted on ANY discussion board, online websites or file-sharing platforms**. Please follow the rules for naming and posting assignments.
- All assignments must be submitted using D2L if applicable. Students must adhere to the following rules when submitting assignments. Failure to do so will affect their grades.
    - **File Name:** Should be named according to the following pattern: <LastName>_<FirstName>_AX.pdf, where LastName is the student's last name, FirstName is the

student's first name, and X is the assignment number

- For example, my assignment3, file submission will be named Kotikela_Srujan_A3.pdf.

TECHNOLOGY REQUIREMENTS

LMS

All course sections offered by Texas A&M University-Commerce have a corresponding course shell in the myLeoOnline Learning Management System (LMS). Below are technical requirements

LMS Requirements: https://community.brightspace.com/s/article/Brightspace-Platform-Requirements
LMS Browser Support: https://documentation.brightspace.com/EN/brightspace/requirements/all/browser_support.htm

ACCESS AND NAVIGATION

You will need your campus-wide ID (CWID) and password to log into the course. If you do not know your CWID or have forgotten your password, contact the Center for IT Excellence (CITE) at 903.468.6000 or helpdesk@tamuc.edu.

Note: Personal computer and internet connection problems do not excuse the requirement to complete all coursework in a timely and satisfactory manner. Each student is expected to have a backup method to deal with these inevitable problems. In case of extreme technology related circumstances, please communicate directly with the instructor to best manage your success in this course.

COMMUNICATION AND SUPPORT

Technical Support

If you are having technical difficulty with any part of Brightspace, please contact Brightspace Technical Support at 1-877-325-7778. Other support options can be found here: https://community.brightspace.com/support/s/contactsupport

Interaction with Instructor Statement

To communicate with me about this course, kindly use the email address included in this syllabus. During the week, you can generally expect a response to your emails within 1-2 business days. *If you do not receive my response in 2 business days, please send a second email to me*.

To ensure I get your email and respond within indicated timelines above, please make sure that:

- Your email message is sent from your Texas A&M Commerce student account.
  - Your email message includes a descriptive subject with the indicated prefix:

CSCI 459 – Spring 2024: <descriptive subject>

COURSE AND UNIVERSITY PROCEDURES/POLICIES

Course Specific Procedures/Policies

Attendance is required but not graded. Students are expected to do the readings, attend class, and participate inclass discussions. Each student is responsible for managing their own time and work-load. Emergency / extreme circumstances causing a student to miss deadlines/exams will need to be supported by official and university approved documentation.

The *syllabus/schedule are subject to change.*

Positive Learning Environment

Your commitment as a student to learning is evidenced by your enrollment at Texas A &M University-Commerce."All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment." (See Student's Guide Handbook, Policies and Procedure, Conduct).

Sharing Your Work

All work produced by students may be shared by the instructor with the class for purposes of example and training. Such work will be as anonymous as possible. Finally, the instructor may share your work anonymously with future classes or in her own writing and research.

Late Work Policy

All assignments are due at the date and time specified.

Please keep in mind that NO late work will be accepted without penalty. If an assignment is turned in after the due date, **20% of the grade will be forfeited**. An assignment must be submitted within 24 hours of thedue date if you want it graded.

- You have one 24-hour "late day" token that can be used on any of the assignments
- After you've used your token, assignments will still be accepted up to 24 hours late, but with a20% penalty (automatically deducted).
- Assignments turned in more than 24 hours late will NOT be reviewed and will not be graded.

Additional extensions on assignments will be granted with appropriate documentation. If you have a problem submitting an assignment on time you should contact me **BEFORE** the due date.

Makeup Policy

There will be NO makeup exams or quizzes. If you shall miss a quiz/exam because of acceptable extreme circumstances (hospitalization, serious injury, death in the family etc.), you may be offered to choose to receive agrade based on your in-class ranking in the next quiz/exam.

Collaboration Policy

Students are encouraged to consult with each other, with the instructor, or anyone else about any assignments / project. However, this must be limited to the discussion of the problem and sketching general approaches to a solution. Each student is responsible for submitting their own independent solutions to the assignment / project. **Consulting another student's or group's solution is prohibited**, and submitted solutions may not be copiedfrom any source. These and any other form of unacceptable collaboration on assignments constitute **cheating**. If you have any question or doubts about whether some activity would constitute cheating, please feel free to ask.

Academic Integrity

Instances of academic dishonesty will not be tolerated. Cheating on exams or plagiarism (presenting the work of another as your own, or the use of another person's ideas without giving proper credit) will result in a failing grade and sanctions by the University. **For this class, all assignments / quizzes / exams / project areto be**

completed by the individual student unless otherwise specified.

Any student cheating will receive a zero on the work they are doing, and subsequent cheating will result in a failinggrade and potential academic sanctions.

Basic Tenets of Common Decency

"All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment." (Student's Guide Handbook, Policies and Procedures, Conduct.). This means that rude and/or disruptive behavior will not be tolerated.

Disclaimer

This syllabus is meant to provide general guidance of what to expect from this course. The instructor reserves the right to make changes as appropriate based on the progress of the class. All changes made to this syllabus during the semester will be announced. This document has been posted electronically. If you print a copy of it, please be sure toconsult the last modified date of the online version to verify that your printed copy is current.

University Specific Procedures

Student Conduct

All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conduciveto a positive learning environment. The Code of Student Conduct is described in detail in the Student Guidebook.
http://www.tamuc.edu/Admissions/oneStopShop/undergraduateAdmissions/studentGuidebook.aspx
Students should also consult the Rules of Netiquette for more information regarding how to interact with studentsin an online forum: https://www.britannica.com/topic/netiquette

TAMUC Attendance

For more information about the attendance policy please visit the Attendance webpage and Procedure 13.99.99.R0.01. http://www.tamuc.edu/admissions/registrar/generalInformation/attendance.aspx
http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/academic/13.99.99.R0.01.pdf

Academic Integrity

Students at Texas A&M University-Commerce are expected to maintain high standards of integrity and honesty in allof their scholastic work. For more details and the definition of academic dishonesty see the following procedures:

Undergraduate Academic Dishonesty 13.99.99.R0.03
http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/undergraduates/13.99.99.R0.03UndergraduateAcademicDishonesty.pdf
Graduate Student Academic Dishonesty 13.99.99.R0.10
http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/graduate/13.99.99.R0.10GraduateStudentAcademicDishonesty.pdf

Students with Disabilities-- ADA Statement

The *syllabus/schedule are subject to change.*

The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. Ifyou have a disability requiring an accommodation, please contact:

Office of Student Disability Resources and Services

Texas A&M University-Commerce, Gee Library- Room 162, Phone (903) 886-5150 or (903) 886-5835, Fax (903) 468-8148

Email: studentdisabilityservices@tamuc.edu

Website: Office of Student Disability Resources and Services

http://www.tamuc.edu/campusLife/campusServices/studentDisabilityResourcesAndServices/

Nondiscrimination Notice

Texas A&M University-Commerce will comply in the classroom, and in online courses, with all federal and state laws prohibiting discrimination and related retaliation on the basis of race, color, religion, sex, national origin, disability, age, genetic information or veteran status. Further, an environment free from discrimination on the basis of sexual orientation, gender identity, or gender expression will be maintained.

The *syllabus/schedule are subject to change.*