Department of Computer and Information Sciences
Towson University

CyberAI

COSC 670 Fall 2024

Course Instructor:

Dr. Wassila Lalouani
Office: **YR443**
E-mail: wlalouani@towson.edu

Class Schedule: Tuesday 4:30-7:10pm
Office hours: Tuesday 12:30 PM - 3:30 PM (In person/Online)
Credits: 3 credits

Research interest:
Machine learning, networking security, Wireless Sensor Networks, Fault tolerant computing and communication, Cyber-physical systems, Telehealth systems.

TA: **Abdullahi, Abdullahi**
E-mail: aabdull2@students.towson.edu

Course Syllabus:

Objective: This course provides students an opportunity to delve into the forefront of cybersecurity by exploring emerging topics that are shaping the field today. Through a combination of lectures, hands-on labs, and projects, students will be introduced to state-of-the-art artificial intelligence (AI) techniques, learning how these advanced methods are being applied to solve real-world security challenges. The course will cover the practical application of AI in identifying, analyzing, and mitigating cybersecurity threats, offering students a comprehensive understanding of how AI can enhance security measures across various domains. The course will also provide an in-depth exploration of the unique challenges posed by emerging AI systems, including vulnerabilities, adversarial attacks, and the ethical implications of AI in security. By the end of the course, students will have developed the capability to apply AI-driven solutions to a wide range of security issues, making them adept at navigating the evolving landscape of cybersecurity. In summary, this course aims to (1) investigate emerging cybersecurity topics, (2) present cutting-edge artificial intelligence (AI) techniques, (3) utilize and enhance AI capabilities to address real-world security challenges, and (4) examine and resolve cybersecurity issues within AI systems.

Learning Objectives:

By the completion of the course, you should be able to:

- Understand concepts, principles, and methodologies of cybersecurity solutions.
- Explore a range of current open problems in cybersecurity.
- Describe the key components of the Cyber Physical Systems.
- Understand how to engage in cybersecurity research, and to investigate novel ideas.
- Understand and implement typical AI tools to resolve real-world cybersecurity problems.
- Comprehend the fundamental theories of machine learning, and data analytics.
- Conduct exploratory analysis on real-world datasets, such as those from CPS and IoT, using deep learning and other data mining techniques.
- Formulate security challenges in IoT or AI systems and select appropriate algorithms and evaluation methods for solutions.
- Demonstrate knowledge understanding through a real-world project.
- Gain hands-on experience with deep learning tools like TensorFlow, Keras, Numpy, and others.

Prerequisites: Programming skills are required, and knowledge of AI, machine learning, and cybersecurity will be helpful.

Reference Books:
A textbook is not required. Instead, references can be selected from technical books, magazines, journals, and relevant conferences.

Course Outline

Part I: Cybersecurity

- Introduction to cybersecurity
- Emerging topics in cybersecurity
- Opportunities, challenges and methodologies

Part II: Background on AI Techniques

- Introduction to data mining and machine learning
- Classification and ensemble learning
- Clustering
- Deep learning techniques
- Modern learning algorithms

Part III: AI applications in cybersecurity

- Application i: smart and robust system in Internet of Things (IoT).
- Application ii: smart and robust system in cyber physical systems (CPS).
- Application iii: develop AI based decentralized applications, e.g., smart transportation, smart health, etc.

Part IV: Cybersecurity in AI

- Adversarial machine learning

- Distributed AI system – federated learning
- Exploring system attacks and defense in emerging decentralized AI systems

Grade Structure and Policy

The course will be a combination of Lecture, classroom discussions, and a Labs.

Course Grading Scale for graduate Students:

Course work	Grade distribution
Homework Assignments	20%
Reading Assignments	20%
literature survey	20%
Project	40%

Final grade will be computed as follow:

Course grade	Range	Course grade	Range
A	≥93% - < 100%	C+	≥ 77% - < 80%
A-	≥90% - < 92%	C	≥ 70% - < 77%
B+	≥87% - < 90%	D+	≥ 67% - < 70%
B	≥83% - < 87%	D	≥ 60% - < 67%
B-	≥ 80% - <83%	F	< 60%

Assignments:

1. *Homework*: **(20%)** The assignments offer the opportunity to gain practical experience with the topics covered in class. Collaboration with classmates is not permitted unless the assignment explicitly said so. Students will put their gained knowledge to practice and demonstrates their skills.
2. Reading Assignments **(20%)**: The students will be assigned research papers to present in class. The objective is to familiarize students with research publications, encourage class discussion, and enhance the course content with illustrative techniques from the literature. Evaluation will be based on the clarity of the oral presentation (30%), the depth of understanding of the technical material (40%), and the quality of the slides (30%).
3. **literature survey (20%):** The primary goal of the literature survey is to help students to perform independent research. Students are expected to conduct a survey of the state-of-the-art in on one of the above covered areas and present literature survey in class and facilitate an in-depth discussion in class. Students need to work together with the instructor in selecting their papers for presentations. A survey report should be finished, which should contain at least 5 papers.
4. Project **(40%):** The project will offer students the opportunity to apply their acquired knowledge and showcase their skills. Project topics must be approved by the instructor, and students are encouraged to explore open research problems at the intersection of cybersecurity and AI. Students are expected to review relevant literature, propose effective solutions, and validate their approaches. A comprehensive paper should be prepared, detailing the identified problem, justifying the chosen solution, and discussing the results. Additionally, students should present their work in class during the final week of the course.
    a. 1 or 2 students per group and select the main idea for your project
    b. Fully motivate the problem and survey related work (10%)
    c. Project preparation (e.g., data preparation and preprocessing, project proposal) (15%)
    d. Develop your own solutions – substantial novel AI-driven algorithm development, theoretical analysis, and implementation are expected (25%)
    e. A thorough empirical evaluation and comparing with baseline methods (20%)
    f. A fully developed project report (20%): with at least 8 pages in ACM template
    g. Project presentation (10%)

Course Policies:

- Late assignments are not accepted unless an extension is preapproved by the instructor.
- All assignments, class lectures, reviews, and general course information will be managed through blackboard.
- Most grades will be available in Blackboard unless notification from the instructor. You are responsible to check your grades and request any corrections prior to the last day of classes.
- All students are expected to be on time and remain for the duration of the class. Written documentation of the reason for the absence may be requested by the instructor and must be submitted for the absence to be excused.
- Your email to the instructor should be from your university assigned student email address and make sure to include COSC 670 in the subject. Emails received from other accounts are ignored. Also, the instructor will manage to answer emails within at most two

days.

- Students should come to each class session prepared with their laptops, as this course will involve labs.

#	Date	Subject	Reading/Lab/Article Discussion
1	Week 1 Aug. 27	Course Overview/Introduction to Cybersecurity	Literature Survey Group Form Up
2	Week 2 Sep. 3	Emerging Topics in Cybersecurity	Reading Assignment Literature Scan
3	Week 3 Sep. 10	Introduction to IoT	Reading Assignment Literature Scan
4	Week 4 Sep. 17	Introduction to AI	Reading Assignment Literature Scan
5	Week 5 Sep. 24	Classification and Ensemble Learning	Reading Assignment Literature Scan
6	Week 6 Oct. 1	Clustering	Lab 1: Classification
7	Week 7 Oct. 8	Deep Learning - ANN	Lab 2: ANN
8	Week 8 Oct. 15	Deep Learning – RNN, CNN	
9	Week 9 Oct. 22	AI in Cybersecurity – Smart and Robust CPS and IoT Guest Speaker	Project Proposal Presentations
10	Week 10 Oct. 29	AI Enabled Applications Guest Speaker	Lab 3: RNN Project Proposal Report Due
11	Week 11 Nov. 5	Decentralized AI Systems Guest Speaker	Literature Survey Presentations
12	Week 12 Nov. 12	Cybersecurity in AI – Secure Distributed Learning (Federated Learning) Guest Speaker	Lab 4: CNN Literature Survey Presentations
13	Week 13 Nov. 19	Secure and Robust Learning – Adversarial Learning Guest Speaker	Reading Assignment
14	Week 14 Nov. 26	Secure and Robust Learning – Adversarial Learning Guest Speaker	Reading Assignment
15	Week 15 Dec. 3	Guest Speaker	Project Presentations

Course and University Policies

Attendance and Absence Policy

Attendance is necessary for success in this class. In case of an emergency, please notify the instructor. Repeated absences may result in course failure.

Academic Integrity Policy

By enrolling is this course, each student must honor Towson University's Academic Integrity Policy. Cheating, fabrication, plagiarism, and helping others to commit these acts are all forms of academic dishonesty. Academic misconduct could result in disciplinary action. For more information, please see: https://www.towson.edu/provost/academicresources/documents/03_01_00_student_academic_integrity_policy.pdf , Student Academic Integrity Policy FAQs for International Students, Towson University Student Code of Conduct.

Course Repeat Policy

According to the University policy, students may NOT repeat a course more than once without prior permission from the Academic Standards Committee.

Students with Disabilities Policy

If you are a student with a disability, please contact me at the beginning of the semester. A memo from Disability Support Services (DSS) authorizing your accommodations is required. For additional information, please contact Disability Support Services: https://www.towson.edu/dss/.

Additional resource:

Please check the following links.

Blackboard: All assignments, Slides and general course information will be managed through Blackboard. For additional help, please refer to the following link:
https://www.towson.edu/technology/training/blackboard/students.html.

Technical Support

Lab Information: Lab hours and policies for the CIS Dept:
http://www.towson.edu/fcsm/departments/computerinfosci/resources/labs.html
for technology questions: Student Computing Services (SCS).

Tutoring & Learning Center:
https://www.towson.edu/tutoring-learning/
https://libraries.towson.edu/

Writing Services:
https://www.towson.edu/cla/centers/writing/?utm_source=redirect&utm_content=writingcenter