University *of* New Haven

TAGLIATELA COLLEGE OF ENGINEERING

Electrical and Computer Engineering and Computer Science

DSCI 6015
AI & Cybersecurity
Fall 2021
Meeting Times and Location(s): MW 3:55pm – 5:10pm ET @ Buckman 233C
Credit Hours: 3
Vahid Behzadan, Ph.D.
Faculty Contact Information:
Office Location: Maxy120A or Zoom
Phone: 203-479-4723 Email: vbehzadan@newhaven.edu
Office Hours: MW 12pm-1pm or by request
Department Chair: Dr. Ali Golbazi agolbazi@newhaven.edu

COURSE SYLLABUS

This syllabus is informational in nature and is not an express or implied contract. It is subject to change due to unforeseen circumstances, as a result of any circumstance outside the University's control, or as other needs arise. If, in the University's sole discretion, public health conditions or any other matter affecting the health, safety, upkeep or wellbeing of our campus community or operations requires the University to make any syllabus or course changes or move to remote teaching, alternative assignments may be provided so that the learning objectives for the course, as determined by the University, can still be met. The University does not guarantee that this syllabus will not change, nor does it guarantee specific in-person, on-campus classes, activities, opportunities, or services or any other particular format, timing, or location of education, classes, activities, or services.

The Accessibility Resource Center can be reached at (203) 932-7332 or by email at AccessibilityResCtr@newhaven.edu. For additional information, please refer to the Accessibility Resource Center (ARC) website at www.newhaven.edu/campusaccess. For additional assistance from the Dean of Students Office, please contact: deanofstudents@newhaven.edu. If you require assistance with the technology requirement, please visit the Student Technical Support page.

Course Description:

Prerequisite: CSCI 6602 or equivalent course in Python.

Hands-on introduction to the applications of machine learning and cybersecurity in cybersecurity, and the security issues in AI systems. Topics covered include supervised and unsupervised machine learning for intrusion detection, malware detection, spam classification, and vulnerability discovery; as well as adversarial attacks on machine learning such as poisoning, adversarial examples, and model reversal. 3 credits.

Required Text(s):

None – external resources such as reading material, slides, code, and video lectures will be provided.

Course Structure/Course Format/Course Objectives:

This class is offered as an on-ground course, with lectures, in-class exercises, take-home programming assignments, reading assignments, and projects. Active learning will constitue as much as 50% of the class. Participation will be recorded based on engagement in discussions (online/in-person), as well as submitted assignments.

Student Learning Outcomes:

Upon completion of this course students will be able to:

1. Practice the tools and techniques for data collection, cleaning, modeling, and visualization for cybersecurity applications
2. Develop machine learning applications for malware detection, intrusion detection, fraud prevention, and threat intelligence analysis for cybersecurity
3. Identify the security vulnerabilities and challenges in AI-driven applications.

Course Requirements & Assessment:

Please see official University of New Haven Academic Policies located in the links below:
Graduate Grading System

Assignments/Projects:

- All submissions are online, either via Canvas or Gradescope (as instructed in the assignment details). Please turn in whatever you have for participation credit, event if incomplete.
- Homework assignments can be completed via pen and paper, but the final submission must be scanned/photographed copies of the work. If handwriting is deemed illegible there may be a penalty, or the attempt may be completely reject.

Examinations:

- No official exam! Assessment will be based on assignments, projects, presentations, and participation.

Participation:

Active learning will constitue as much as 50% of the class. Participation will be recorded based on engagement in discussions (online/in-person), as well as submitted assignments.

Grading

Grades earned are based on your performance on homework, quizzes, exams and the final exam.

Class Projects	25%
Quizzes/Participation	10%
Paper Presentations	15%
Midterm Project	25%
Final Project	25%
Total**	100%

**Final Grades are assigned with the following scale:

Typical Undergraduate Scale

Grades Scored Between			Letter Equivalent
97	to	100	A+
94	to	Less than 97	A
90	to	Less than 94	A-
87	to	Less than 90	B+
84	to	Less than 87	B
80	to	Less than 84	B-
77	to	Less than 80	C+
74	to	Less than 77	C
70	to	Less than 74	C-
67	to	Less than 70	D+
63	to	Less than 67	D
60	to	Less than 63	D-
		Less than 60	F

Typical Graduate Scale

Grades Scored Between			Letter Equivalent
97	to	100	A+
94	to	Less than 97	A
90	to	Less than 94	A-
87	to	Less than 90	B+
84	to	Less than 87	B
80	to	Less than 84	B-
77	to	Less than 80	C+
74	to	Less than 77	C
70	to	Less than 74	C-
		Less than 70	F

The calculation of final grades is determined by the faculty member. The calculated grade in the total column in Canvas may or may not be reflective of your final grade.

Expectations:

Students should expect to spend at least 3 hours on academic studies outside, and in addition to, each hour of class time. There will be readings, homework questions/problems, and programming projects.

Late Work: Assignments turned in late may be accepted with a grade penalty, if the solutions are not distributed yet. This is completely at the discretion of the instructor, as the goal is to balance learning and fairness.

Missed Work: Exams may be made up in only the most unavoidable situations (at the discretion of the instructor). A formal excused absence (such as a note from Health Services or a healthcare provider) will be required before you can make up a missed exam.

Individual Work: Students must work individually on assignments and projects unless specifically allowed to work in groups by the instructor. Any work taken from the internet must be cited properly (acceptance of code taken from elsewhere is at the discretion of the instructor) or will be considered plagiarism. Failure to adhere to this policy will result in penalties ranging from a zero on the assignment to a zero in the final grade. Students may also be subject to disciplinary action by the University of New Haven (see University Policies).

Course Outline/Schedule:

Week 1: Intro to AI for Cybersecurity
Week 2: Landscape of cybersecurity - sources of data
Week 3: Introduction to machine learning - linear classifiers
Week 4: SVM and Logistic Regression - Spam and Phishing Classification
Week 5: Clustering techniques for network anomaly detection
Week 6: Machine learning for malware detection I - Intro to malware analysis
Week 7: Midterm Project
Week 8: Machine learning for malware detection II
Week 9: Deep learning I - CNNs and RNNs

Week 10: Deep learning II - GANs and deepfakes
Week 11: Paper Presentations - Final Project Proposal
Week 12: Paper Presentations
Week 13: Adversarial Machine Learning - Paper Presentations
Week 14: AI Safety, Security, and Ethics - Paper Presentations
Week 15: Final Project Presentations

Diversity Statement

The University of New Haven embraces diversity and recognizes our responsibility to foster a diverse, inclusive, and welcoming environment in which all members of the Charger community of all backgrounds and identities can learn, work, and live together. We benefit from the academic, social, and cultural developments that arise from a diverse campus that is committed to equity, inclusion, belonging, and accountability.

We have a responsibility as a community and as individuals to address and remove barriers, achieve success, and sustain a culture of inclusivity, empathy, kindness, and compassion. We encourage, welcome, and embrace participation in ongoing dialogue, engagement, and education to critically examine and thoughtfully respond to the changing realities of our community. Diversity, equity, inclusion, acceptance, and belonging enrich the Charger community and are instrumental to institutional success and fulfillment of the University mission.

Reporting Bias Incidents

At the University of New Haven, there is an expectation that all community members are committed to creating and supporting a climate which promotes civility, mutual respect, and open-mindedness. There also exists an understanding that with the freedom of expression comes the responsibility to support community members' right to live and work in an environment free from harassment and fear. It is expected that all members of the University community will engage in anti-bias behavior and refrain from actions that intimidate, humiliate, or demean persons or groups or that undermine their security or self-esteem.

If you have an immediate safety concern for yourself or others, and/or believe someone poses an immediate threat to themselves or others, please contact University Police at 203-932-7070 or call 911. Community members can report bias-motivated incidents by completing the form at **www.newhaven.edu/biasreporting**. Community members are encouraged to complete this form if they are the target of bias or harassing behaviors, witness such behaviors, or gain knowledge of these behaviors occurring within the University community. All matters concerning bias and harassment will be handled by the Dean of Students Office and Human Resources Office.

University-wide Academic Policies

A continually-updated list of University-wide academic policies and descriptions of key university student resources, can be found on Canvas. You can access them by simply clicking on the (?) help button.

The University-wide academic policies include (but are not limited to) the University's attendance policy, procedures for both adding / dropping a course and course withdrawals, an explanation for the sorts of circumstances where incomplete (INC) grades could be considered by the faculty, and the academic integrity policy (among others). Also in this location you will

find information regarding the process for reporting bias and topics related to our maintaining a positive learning environment (including, but not limited to, discrimination and sexual misconduct).

The list of key university student resources to enable learning include (but are not limited to) the University's Center for Student Success, Writing Center, Center for Learning Resources, and the Accessibility Resource Center.

Course Delivery Options

On-Ground: Fully on-ground course with every student meeting in-person.

For courses with a location of ONLI that also list time and day information, students should plan to be available during that time for synchronous online learning. Classes with no time listed are asynchronous, fully online, and coded ONLI. Due to social distancing requirements, some courses will be offered in Hybrid or Flex formats. ***Online learning may occur at any time, depending on how the University may determine classes are best taught under any circumstance.*** *All courses, including selected labs, practicums, project-based, and clinical courses may require limited, additional meeting times to accommodate accreditation, regulatory, and similar requirements and students will be advised about this at the beginning of those classes.*

University of New Haven

UNIVERSITY STUDENT SUPPORT SERVICES

The University recognizes that students can often use some help outside of class and offers academic assistance through several offices.

Accessibility Resources Center

Students with disabilities, chronic health-related conditions, or military service-connected disorders are encouraged to share, in confidence, information about course specific approved reasonable accommodations. The Accessibility Resources Center, located in Sheffield Hall, is responsible for and committed to providing supports and resources that serve to promote educational equity and ensure that students are able to participate in the opportunities available at the University of New Haven. Reasonable accommodations are not made without written documentation from the Accessibility Resources Center.

Center for Learning Resources (CLR)

The Center for Learning Resources (CLR), located in the Peterson Library, provides academic content support to the students of the University of New Haven using metacognitive strategies that help students become aware of and learn to apply optimal learning processes in the pursuit of creating independent learners. CLR tutors focus sessions on discussions of

concepts and processes and typically use external examples to help students grasp and apply the material.

Center for Student Success (CSS)

The Center for Student Success provides students with a multitude of resources available on campus and assists students in fulfilling their educational, social and personal goals.

Counseling & Psychological Services (CAPS)

CAPS offers confidential, free services in order to support student mental health and wellbeing. The services include individual and group therapy, support groups, consultations, and 24/7 crisis support. We are available in person and remotely, and are in the office M-F, 8:30-4:30. Please call us to schedule an appointment or with any questions at 203-932-7333; you can also schedule online. If you experience a mental health crisis after hours, you can call our main number for support.

Myatt Center

The Myatt Center for Diversity and Inclusion is committed to creating a multicultural environment through intentional education, campus community engagement, and valuing the unique identities of each member of the Charger Community. Our commitment to diversity is driven by the core values of connection, belonging, inclusivity, equity, acceptance, and accountability. The Myatt Center's focus is to create a respectful and inclusive environment based our awareness and ability to engage with others who are different on many levels including ethnicity, race, sexual orientation, gender, military, religious belief, and life experiences.

Marvin K. Peterson Library

The Library provides access to online databases, e-books, e-journals, electronic U.S. Government Documents, print books, educational games, and audiovisual materials. A search can be conductedthrough all these resources at once by using the search box "Articles, Books, & More."

The Library provides three floors with individual quiet study space, collaborative group study space, study rooms with technology, whiteboards, Dell desktops, iMacs, scanners, and printers. The entire library is a wireless zone.

Librarians assist in locating relevant sources of information for research papers, thesis, honors thesis, and other projects. Librarians answer general reference questions and help with effectively evaluating sources of information. Help is available through a Chat Service, 24/7 Ask a Librarian Service, a Zoom Reference Service, and by E-Mail. Complete the Research Consultation Form to arrange a time convenient for you.

LibGuides are created to assist students with research. They contain an overview of resources available through the library, as well as tutorials, subject guides, and course specific guides.

University Writing Center

The mission of the Writing Center is to provide high-quality tutoring to undergraduate and graduate students as they write for a wide range of purposes and audiences. Tutors are undergraduate and graduate students who are majoring in a variety of fields across the

University. We are here to work with you at any stage in the writing process; just bring in your assignment, your ideas, and any writing you've done so far. To make an appointment, you can register for an account with our scheduling site https://newhaven.mywconline.com or visit us in person at our desk on the first floor of Peterson Library (just to the left after you enter the library).