Engineering Educators Bringing the World Together
2025 ASEE Annual Conference & Exposition
Palais des congrès de Montréal, Montréal, QC • June 22–25, 2025
Paper ID #45546

The Weaving of Machine Learning and Artificial Intelligence into the Fabric of Cybersecurity Curriculum: From Degree Plan to Capstone Projects

Dr. Mahmoud K Quweider, The University of Texas Rio Grande Valley

M K Quweider is a Computer and Cybersecurity Sciences Professor at the U. of Texas at UTRGV. He received his Ph.D. in Engineering Science (Multimedia and Imaging Specialty) and B.S. In Electrical Engineering, M.S. in Applied Mathematics, M.S. in Engineering Science, and M.S. in Biomedical Engineering, all from the University of Toledo, Ohio. He also holds a Bachelor/Master of English and a Master of Business Administration from the University of Texas at Brownsville. He recently obtained a master's in digital forensics from Champlain College, after which he founded the B.Sc. in Cyber Security. After graduation, he was employed at several corporations, including Pixera, a digital multimedia processing company in Cupertino, CA; 3COM, a networking and communication company in Schaumberg, IL; and Mercantec, an E-Commerce company in Naperville, IL. He has more than 50 publications in the field and has served as a reviewer and moderator for several scientific and educational journals and conferences. He joined UTB (UTRGV) in the Spring of 2000. His areas of interest include AI/Machine Learning, Networking and Cyber Security, and Digital Imaging.

Dr. Liyu Zhang, University of Texas Rio Grande Valley
Dr. Jorge Castillo, The University of Texas Rio Grande Valley

Jorge Castillo, Ph.D., is an Assistant Professor at the University of Texas Rio Grande Valley, specializing in Cybersecurity and Electrical Engineering. He earned his Ph.D. in Electrical Engineering from the University of Texas at San Antonio, with a focus on blockchain technology for secure applications. His research interests include blockchain systems, machine learning and privacy-preserving methodologies.

Dr. Ala Qubbaj, The University of Texas Rio Grande Valley

Dr. Ala Qubbaj is the Dean for the College of Engineering and Computer Science at the University of Texas Rio Grande Valley (UTRGV)

The Weaving of Machine Learning and Artificial Intelligence into the Fabric of Cybersecurity Curriculum: From Degree Plans to Capstone Projects

Abstract

As our newly designed degree in Cybersecurity enters its fourth year, students in the program are starting to take courses beyond the basic ones, including senior courses, technical electives, and capstone projects. While Cybersecurity is at the heart of our degree that addresses the national need for cybersecurity specialists, how we approach the education and pedagogy of cybersecurity in the era of ***Big Data*** and ***AI/ML*** (Artificial Intelligence/Machine Learning) is a question that we are addressing in real-time as techniques and measures and countermeasures of cybersecurity attacks keep evolving and taking advantages of the rapid advancements in computing, memory, storage, networking, and virtualization technologies.

Educational modules with hands-on labs are available at different junctions to give students in the program multiple chances to incorporate the latest techniques in AI/ML into their degree. Whether it is advising and orientation sessions, faculty-led seminars, student-club workshops, technical electives, or capstone projects, custom-tailored material has been created specifically for our cybersecurity students. This paper presents our systematic efforts to pervade the curriculum with a hands-on, immersive approach to integrating AI/ML. We will present the following modules that were developed or are currently being developed.

- Early Workshops/Seminars/Sessions
    - Advising.
    - Degree Plans.
    - Departmental.
    - Student Clubs.
- The AI/ML teachings in a cybersecurity-focused technical elective (Course was named CYBI-4336: Cybersecurity Engineering with ML/AI):
    - Description of each module.
    - The list of objectives and sub-objectives for each module.
    - Case studies in Cybersecurity.
    - The list of AI/ML hands-on labs using public resources:
        - Taxonomy of each technique in the lab.
        - Delivery method of each lab.
- Research opportunities for cybersecurity students in ML/AI:
    - Capstone Projects.
    - AI/ML public cloud platforms.
    - Public tools for collaboration.
- Grant proposals with AI/ML emphasis
    - AI/ML Infrastructure
    - Labs

By presenting our efforts, we hope to benefit from other efforts and that other instructors facing the same issues can benefit from our experience by adopting best practices while avoiding pitfalls.

Keywords: Machine Learning, Artificial Intelligence, Cyber Security, AI/ML Curriculum Development, Project-based Learning.

Introduction and Motivation

In 2020, a new ***Cybersecurity*** bachelor's degree was created at UTRGV College of Engineering and Computer Science. The degree was motivated by the shortage of personnel and a high expected growth rate. According to the U.S. Bureau of Labor Statistics, employment in cybersecurity fields is projected to grow by 33% from 2023 to 2033, much faster than the average for all occupations. This rapid growth highlights the urgent need for skilled cybersecurity professionals to address the ever-evolving landscape of cyber threats and protect our digital world. The degree is structured around a blend of theory and practice. It is a collaborative interdisciplinary degree that follows a holistic approach integrating technical, legal, business, and policy skills using computer science courses with support courses from Business, Information Systems, and Criminal Justice [1-4].

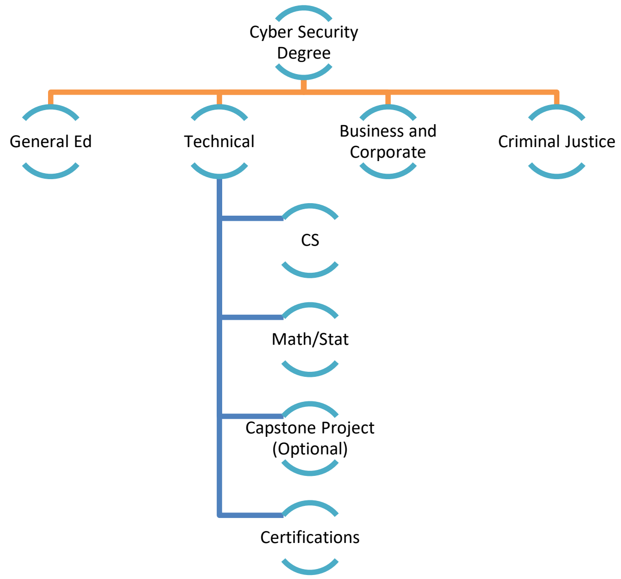


Figure 1. Cyber Security Degree Architecture [1-4]

The degree includes technical electives such as ***Data Mining*** and ***Artificial Intelligence/Machine Learning (AI/ML)*** that students can take as seniors. AI and ML are proving to be transformative technologies, reshaping how current fields are fundamentally approached, including our own cybersecurity. To that effect, AI/ML inclusion in the university curriculum is essential. Their early Integration would help students develop critical cybersecurity operational skills in high demand across various sectors such as IT, e-commerce, healthcare, finance, marketing, and technology. For example, understanding AI/ML-driven threat detection and response systems can significantly enhance the ability to protect vulnerable digital infrastructures in any corporation. As AI/ML is a double-edged sword, it is used by cyber-criminals and rogue actors for malicious purposes, including data theft, ransomware attacks, service disruption, espionage, social engineering, and malware distribution. On the other hand, good actors use it for real-time threat detection and responses, vulnerability assessments, phishing and malware detection, user behavior analytics, automated incident response, predictive analytics, network security, and fraud detection to ensure personal and organizational data privacy and security.

The importance of ML and AI in cybersecurity cannot be overstated, as these technologies enable faster, more accurate, and efficient solutions to combat evolving cyber threats. Incorporating

AI/ML early and systematically into the university curriculum of public institutions can provide accessible, cutting-edge education that prepares students for the rapidly evolving job market. Moreover, educating students on AI's ethical implications and societal impacts ensures they are prepared to develop responsible and sustainable solutions. With the increasing reliance on technology and the internet, protecting sensitive information from cyber threats has become a top priority for individuals, businesses, and governments alike, and incorporating AI/ML into the program empowers students to become future leaders who drive progress in an increasingly digital world, with a strong emphasis on the critical field of cybersecurity. Approaching this need to fuse AI/ML in our cybersecurity curriculum starts by identifying the key applications of AI/ML in cybersecurity. Once these are identified, we can determine the freshman, sophomore, and junior courses that can prepare the students for technical elective AI/ML courses taken during the senior year.

Related Work

There have been different attempts at incorporating the machine learning curriculum in college-level courses or degrees. Various papers highlight the integration of AI, ML, and cybersecurity into educational curriculums, reflecting the increasing importance of these fields. The following is a representative set of related work.

- Machine Learning: An Undergraduate Engineering Course by S. Khorbotly [5]. This paper discusses the development of an undergraduate machine learning course, including the challenges faced and the balance between breadth and depth of topics.
- Infusing Data Science into Mechanical Engineering Curriculum with Course-Specific Machine Learning Modules [6]. This paper explores how machine learning modules can be integrated into mechanical engineering core courses rather than having dedicated data science courses.
- A Cloud-Based Approach to Introducing Machine Learning in Project-Based Learning Environments [7]. This paper details the material, technical efforts, and student learning outcomes from a renovated machine-learning curriculum.
- Learning from Machine Learning and Teaching with Machine Teaching [8]. This paper identifies how innovations in AI can enhance the quality of collegiate classroom experiences and improve student performance.
- A Survey on Curriculum Learning by Xin Wang et al [9]. This paper comprehensively reviews curriculum learning, discussing motivations, definitions, theories, and applications.
- Cybersecurity Education in Universities: A Comprehensive Guide to Curriculum Development by Ramezanian and Niemi [10]. This paper offers a detailed guideline for developing cybersecurity curriculums at the university level.
- Cybersecurity Education and Assessment in EDURange [11]. This paper discusses the use of EDURange for cybersecurity education and assessment.
- What Are Cybersecurity Education Papers About? A Systematic Literature Review [12]. This paper systematically reviews cybersecurity education papers, covering topics, teaching contexts, evaluation methods, and impacts.

Our paper is more of an intra-departmental framework combining many of the abovementioned techniques and tailoring them to our cybersecurity major early in the student educational pipeline.

Driven by the importance of incorporating AI in education due to its crucial role in cybersecurity, where it streamlines mundane tasks and enhances threat detection, risk management, and system resilience. The framework presents our efforts to seamlessly fuse AI/ML into the cybersecurity curriculum from the early stages. From admission/advising to graduation, we show our developed educational framework integrating cybersecurity applications of AI/ML into the curriculum.

UTRGV Cybersecurity AI/ML Holistic Framework

Fig. 2 illustrates the framework, which consists of three areas: 1. administrative, Curriculum, Research, and Extra Activities. We discuss each area in the following.

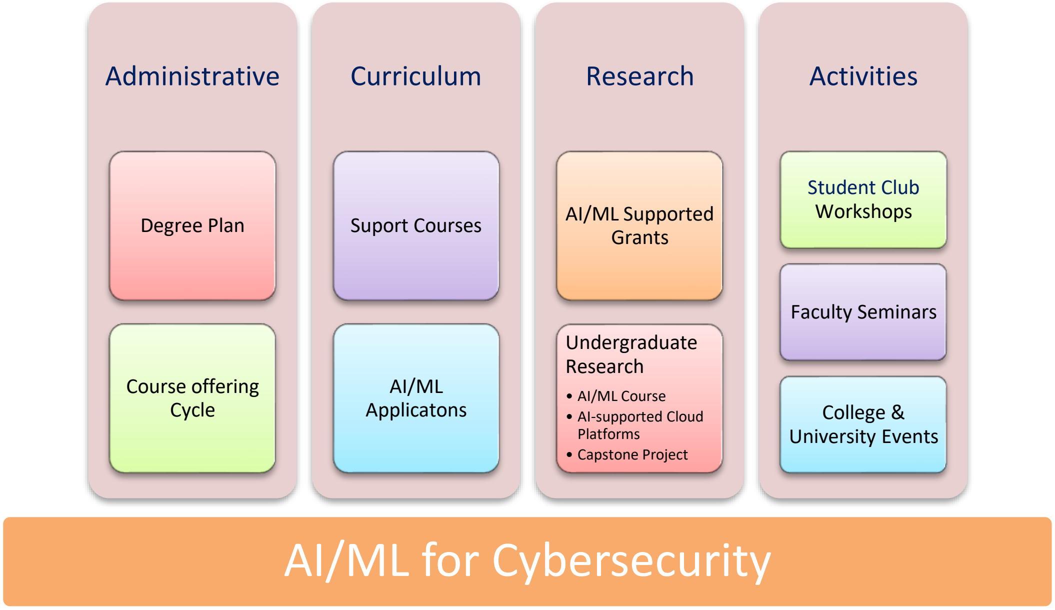


Figure 2. AI/ML Framework

Administrative

The Cybersecurity program offers a senior-level elective course focusing on Artificial Intelligence (AI) and Machine Learning (ML), specifically emphasizing cybersecurity applications. Although the course is a technical elective, we started offering it once the student pipeline was filled up and they could take it (The degree is less than 4 years old). We also plan to provide the course non-stop every fall semester. The course is highlighted in advising sessions and recommended in the degree plan. We recently received an NSF grant that provided computing infrastructure to data-intensive classes in the college, including the AI/ML course.

The course revisits many junior-level concepts and recasts them to benefit from AI/ML. Students are advised to take the course if they want to be up to date with the latest advancements in AI/ML. Enrolling in this course will help students gain a competitive edge and contribute to shaping the future of AI and ML. The course is scheduled to be offered every fall for three years.

AI/ML-focused Curriculum

We start by identifying the key AI/ML application areas in Cybersecurity to build a practical framework. The following areas were identified:

- **Threat Detection and Response**: AI and ML algorithms can analyze vast amounts of data to detect anomalies and potential threats in real time, enabling faster and more accurate responses.
- **Vulnerability Assessment**: Automated systems can scan for vulnerabilities in software and hardware, continuously improving their detection capabilities based on historical data.
- **Phishing Detection**: AI can analyze email content and patterns to identify phishing attempts, reducing the risk of successful attacks.
- **Malware Detection**: Machine learning models can identify and classify malware, including polymorphic malware that changes its code to evade detection.
- **Incident Response**: AI-driven systems can automatically respond to detected threats, mitigating damage and reducing response times.
- **Predictive Analytics**: By analyzing historical data, AI can predict potential threats and vulnerabilities, allowing organizations to proactively strengthen their defenses.
- **Network Security**: AI can monitor network traffic to detect suspicious activities and potential intrusions, enhancing overall network security.
- **Security Information and Event Management (SIEM)**: AI can enhance SIEM systems by more efficiently correlating and analyzing security events.
- **Fraud Detection**: AI can identify patterns indicative of fraudulent activities, helping financial institutions and other organizations prevent fraud.

These areas demonstrate how AI/ML is revolutionizing cybersecurity, making it more efficient and effective in protecting against ever-evolving threats. The need for AI/ML in these areas cannot be overstated, as these technologies enable faster, more accurate, and efficient solutions to combat evolving cyber threats. By incorporating these technologies into the curriculums of public and two-year colleges, institutions can provide accessible, cutting-edge education that prepares students for the rapidly evolving job market. Moreover, educating students on AI's ethical implications and societal impacts ensures they are prepared to develop responsible and sustainable solutions. In today's digital age, the importance of cybersecurity cannot be overstated. With the increasing reliance on technology and the internet, protecting sensitive information from cyber threats has become a top priority for individuals, businesses, and governments. Our AI/ML framework is designed to allow the lower-level courses to build toward the effective use of AI/ML in cybersecurity. This complementary approach ensures that students gain a robust understanding of core AI/ML principles while developing expertise in critical areas such as data science, cloud computing, and advanced cybersecurity techniques. By integrating these diverse subjects, the framework provides students with the necessary skills to develop innovative solutions and effectively tackle complex cybersecurity challenges using AI/ML technologies. This holistic educational strategy aims to prepare students for the ever-evolving landscape of cybersecurity.
To that end, The framework can be divided into the following modules to support AI/ML applications in cybersecurity effectively:

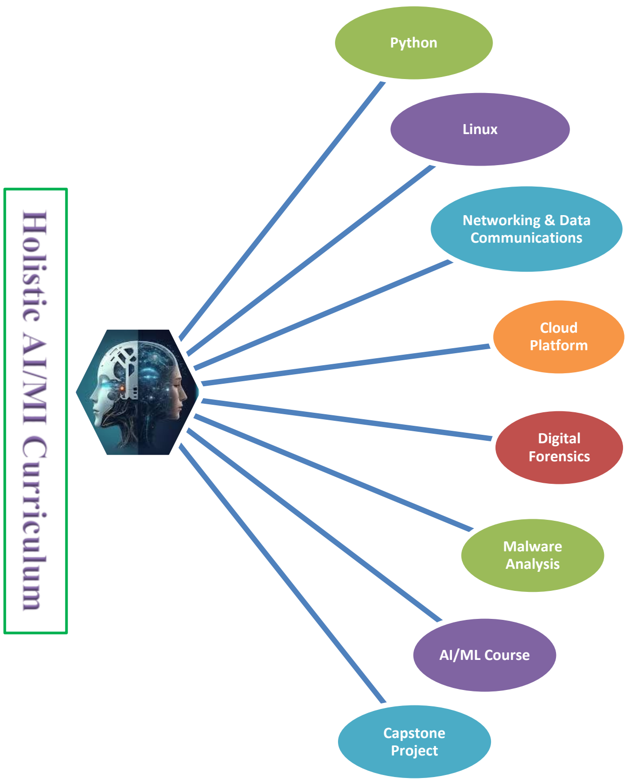


Figure 3. AI/ML Framework with Major Cybersecurity Courses

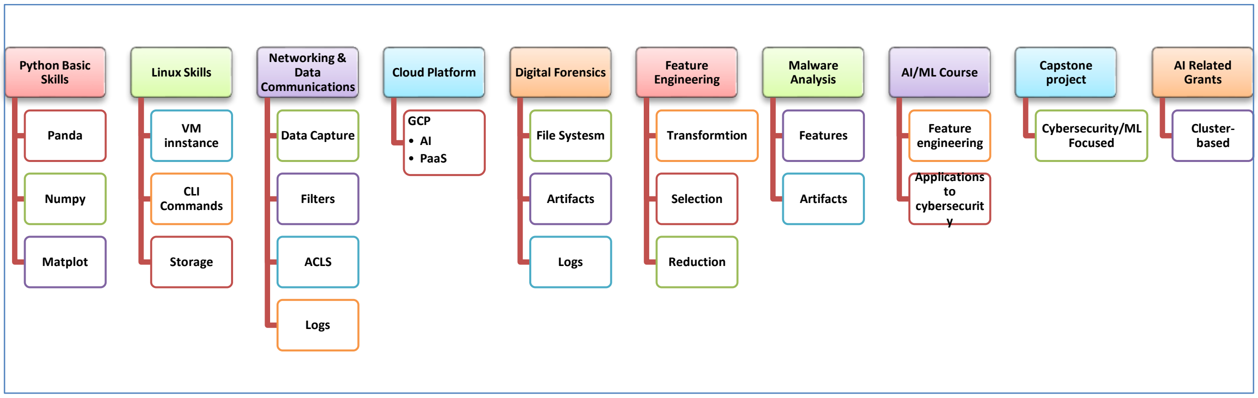


Figure 4. Cybersecurity AI/ML Support Skills

AI/ML Support Skills Details

The following details the skill set with concepts and topics covered in the courses leading to the AI/ML and Capstone Project courses. While the ideas and issues are independent of AI/ML, we emphasize their applications and roles in cybersecurity and AI/ML. CYBI-XXX designates the course number where the topics/concepts are covered.

1. Python Basic Skills (CYBI-2322: Foundations of Systems I)

- Overview of Python programming
- Pandas
    a. Data manipulation and analysis

   b. Handling data structures
- NumPy
   a. Numerical computing with arrays
   b. Mathematical functions
- Matplotlib
   a. Data visualization
   b. Plotting graphs and charts

2. **Linux Skills (CYBI-2324: Foundations of Systems II)**
   a. Basic Linux commands
   b. File system navigation
   c. VM Instance
   d. Creating and managing virtual machines
   e. CLI Commands
      a. Command Line Interface (CLI) basics
      b. Advanced CLI tools
3. **Networking & Data Communications (CYBI-3335: Networking & Data Communications)**
   - Data Capture
      a. Techniques for capturing data
      b. Real-time data collection
   - Filters
   - Access Control Lists (ACLs)
   - Logs
      a. Log management and analysis
      b. Security information and event management (SIEM)
4. **Cloud Platform (CYBI-3346: Cloud Computing & Security)**
   - Google Cloud Platform (GCP)
   - GCP services for AI/ML
   - Platform as a Service (PaaS)
   - Leveraging PaaS for AI/ML solutions
5. **Digital Forensics (CYBI-4319: Digital Forensics)**
   - Fundamentals of digital forensics
   - File Systems
      a. Analyzing file system artifacts
   - Processes and Memory
6. **Malware Analysis (4330: Malware Hacking)**
   - Introduction to malware analysis
   - Identifying malware features and artifacts
7. **AI/ML Course (CYBI-4336: Cybersecurity Engineering with AI/ML)**
   - Feature Engineering
   - AI/ML Infrastructure & Computing Tools
   - Real-world applications of AI/ML in Cybersecurity
   - Case studies and examples
8. **Capstone Project (CYBI-4340: Capstone Project)**
   - Capstone project focused on AI/ML and cybersecurity

The holistic framework ensures comprehensive learning, combining foundational skills with advanced topics to effectively support AI/ML applications in cybersecurity. These modules provide a structured approach to learning and integrating AI/ML with cybersecurity, ensuring students are well-prepared to address current and future challenges in the field. Next, we discuss the AI/ML course and the Capstone Project, the two pathways that systematically incorporate AI/ML into the Cybersecurity degree.

AI/ML Course

For cybersecurity majors, we designed a course in AI/ML as a technical elective to be taken as a senior. The following is the course catalog description.

Cybersecurity Engineering with AI & ML

Table 1. Course Description

CYBI-4336: **Cybersecurity Engineering with AI & ML**	This course integrates artificial intelligence (AI) and machine learning (ML) techniques into cybersecurity practices. This course covers advanced topics such as AI-driven threat detection, automated response systems, and the ethical implications of using AI in cybersecurity. Students will learn how to develop and implement AI-based security solutions to protect against sophisticated cyber threats. The course also emphasizes hands-on experience with real-world scenarios and projects to prepare students for the challenges they will face in the cybersecurity field.

The course was offered for the first time in 2021, and the authors were tasked with teaching it and establishing a framework for future instructors to follow. As this is a non-engineering course, and the degree under which it falls is geared toward graduating cybersecurity analysts, we decided to create a customized course for our students and our degree. What follows is the summary of each module. Appendix A has the course module's design details, the associated labs, and the resources dedicated to the course.

Table 2. AI/ML Modules Summary

Lab Module	Description
What is ML/AI, Applications in Cybersecurity (CS)	Module 1 Introduces ML/AI. It introduces AI/ML Applications in CS.
Preliminaries (Python, Pandas, NumPy, Matplot)	Module 2 Reviews Python, Pandas, NumPy, and Matplot.
The Perceptron Neural Network Model	Module 3 Introduces the Perceptron with activations function & metrics.
The Confusion Matrix	Module 4 Introduces the confusion matrix and related metrics: TP, TN, FP, FN, Recall, Precision, and Accuracy.

Feature Engineering: Part-01	Module 5 introduces feature engineering as it relates to CS.
Feature Engineering: Part-02	Module 6 introduces feature engineering as it relates to CS.
Feature Engineering: Part-03	Module 7 introduces feature engineering as it relates to CS.
Feature Engineering: Scaling	Module 8 introduces feature engineering scaling as it relates to CS (Min, Max, Robust)
Supervised Classification: RFT	Module 9 introduces Random Forest Trees with apps to CS.
Supervised Classification: KNN	Module 10 introduces KNN with apps to CS.
Supervised Classification: NBC	Module 11 introduces Naïve Bayesian Classification with apps to CS.
Supervised Classification: SVM	Module 12 introduces Support Vector Machine Classification with apps to CS.
Supervised Classification: Keras TensorFlow	Module 13 introduces TensorFlow Classification with apps to CS.

Student Evaluation & Feedback

Appendix C includes the raw, unedited course evaluation with students' feedback. The course was a great hit with the students, and the overall rating of agree and strongly agree was 99%. The overall rating of the class was 4.94/5.0. We also noticed that many students choose to do a capstone project related to AI/ML if they take the AI/ML course before their capstone project. Some of the comments ask for more AI/ML applications in the cybersecurity area, which the authors took notice of and will implement in the next tier of the class. It's worth noting that all datasets used in this class are related to Cybersecurity. Examples include data for malware detection, network intrusion, and spam email.

One issue with AI/ML is the need for a higher-level mathematics background that includes Calculus, linear algebra, and Optimization. However, the degree requires only up to Precalculus. To solve this problem, the class instructor opted to use ready-made tools that don’t require a deep understanding of the mathematics behind the algorithms. Such tools include Scikit Learn and TensorFlow.

Research Oriented Course

In addition to industry certification, students in the program must complete a research-oriented project. The course perfectly complements the AI/ML course in that it allows the students to continue their research and dive deeper into modern applications of AI/ML in cybersecurity. The following is the course catalog description.

Capstone Project

Table 3. Course Description	
CYBI-4340: **Capstone Project**	Students will complete a well-defined research-oriented project in a team setting with the guidance of departmental faculty. Course Prerequisites: CYBI 3335, Senior Standing, six additional credits in 3XXX level CYBI courses, and departmental approval. Course Modality: As stated in the previous section, this course will be delivered synchronously online.

The course was offered for the first time in fall 2023, spring 2024, and fall 2024. Appendix B shows the list of projects in the course's last offering. As we can see, many students are choosing AI/ML for their capstone project. We expect this number to grow as students take the AI/ML technical course.

AI/ML Infrastructure, Research & Grants

AI/ML is notorious for needing computational power (GPUs/TPUs), reliable data storage, and seamless connectivity to enable efficient and scalable data handling and model training. We have approached this need in two ways: using public tools and infrastructure and applying for on-premises infrastructure through grants.

Regarding the first way, we have leveraged public cloud infrastructure built explicitly for AI/ML pipelines. Examples include the following top three:

- Amazon Web Services (AWS): Popular for its AI services like SageMaker for building, training, and deploying machine learning models.
- Microsoft Azure: Known for its Azure Machine Learning and integration with OpenAI, allowing the development and operationalization of AI models.
- Google Cloud Platform (GCP): This platform offers AI and ML services like AutoML and Vertex AI, facilitating the creation and deployment of models at scale.

For students with a limited budget, **Google Collaboratory** has proven to be a fantastic, budget-friendly platform that provides free access to cloud-based Jupiter notebooks and GPUs, perfect for AI and ML projects.

The second way to overcome the need for computational resources was to apply for external funding. We were lucky to secure NSF funding for AI/ML and other intensive courses at the engineering college. The acquired infrastructure includes a high-performance GPU server with eight NVIDIA A100 GPUs, enabling efficient handling of complex AI computations. Managed using Slurm scheduling software, this server optimizes resource allocation for AI-driven tasks. The grant is part of enhancing undergraduate STEM courses within multiple departments in the College of Engineering and Computer Science, particularly those emphasizing computational aspects, including Computational Fluid Dynamics (CFD), ***Blockchain (BC), Cybersecurity Machine Learning (CML)***, Finite Element Analysis (FEA), Senior Design (SD), and Undergraduate Research (UR). The first use of the equipment for the CML will commence in the fall of 2025. We are currently in the process of preparing hands-on labs for the students to access the server remotely.

Extracurricular Activities Support

While teaching and research are the heart of our mission to integrate AI/ML, group activities outside the classroom can also be crucial. Student clubs can engage in various activities such as organizing workshops, hackathons, and coding sessions, securing industry experts and academics to speak at events, promoting these events through social media and other channels, creating engaging content related to AI and ML, recruiting and managing volunteers, conducting hands-on tutorials and sessions on AI/ML concepts, assisting members with technical issues, mentoring students on AI/ML projects, connecting with local schools to foster interest in AI/ML, collaborating with companies for internships and projects, and engaging alumni in the AI/ML field for mentorship and support. Cybersecurity majors can be part of the Cybersecurity Club, which was created simultaneously with the degree. With mentorship from faculty, the club has and continues to conduct workshops and activities that include AI/ML.

College events are another avenue where students can be aware of AI/ML's current state of the art. The Engineering college supports many activities during the e-week (Engineering week), including research poster day. We have encouraged students in the cybersecurity program to participate in this event to showcase their research in AI/ML. One of the authors has participated annually in those events by advising students who have already taken the AI/ML course and/or the capstone project. We are glad to report that at least one of the mentored teams was among the top three in the best poster sessions.

Discussion

While teaching AI/ML seems straightforward, establishing a framework provides a holistic approach to this new exciting field and its applications in cybersecurity. The framework helps build a foundation for AI and ML in cybersecurity, where students understand early in their education the prerequisites for applying AI/ML in their field, from basic cybersecurity concepts to network security, threat detection, and incident response. The support courses clarify that Python is essential for implementing AI/ML algorithms and preparing students for AI and ML applications in cybersecurity through case studies, real-world examples, and hands-on projects.

The AI/ML-focused capstone projects are a great way to provide practical, hands-on experience with AI and ML in a more specialized way. Students can delve deeper into cybersecurity-related fields and see how AI/ML can help. For example, Network Security and Threat Detection can be significantly improved with AI-Based Threat Detection and Response Systems that use machine learning for real-time threat identification. Moreover, Application Security projects can utilize AI to find vulnerabilities and protect applications, while IoT Security projects can create AI-driven solutions for connected devices. Other interesting areas that students can explore include fraud detection systems, data privacy, incident response, domain generation algorithms (dgas), malware analysis, ransomware detection and mitigation, and reverse engineering.

We also stress the importance of extracurricular activities beyond the classroom. Student clubs such as the Cybersecurity Club and College events such as Research Day are excellent ways for students to peer connect; these play a crucial role in spreading AI and ML education by organizing diverse activities like workshops, hackathons, faculty seminars, poster sessions, and expert talks, which foster learning and collaboration among students and faculty alike. By engaging in hands-on projects and promoting community partnerships, these clubs create an impactful environment that encourages practical application and growth in AI/ML.

Conclusions and Future Work

In this paper, we advocated for the early adoption of a comprehensive framework that introduces the A/ML field early in the student's education. We presented a comprehensive framework for teaching AI/ML, with cyber security emphasis, in higher education. The framework emphasizes the importance of AI/ML in the Cybersecurity program by laying the foundation for the field early in the student's journey. We have developed two pathways in which the students can gain a deep understanding of the field as well as conduct research that is closely integrated with AI/ML. The AI/ML course has a set of thirteen modules, each with hands-on lab modules using local and public resources and tools such as Anaconda and Google's Collab. The templates for each module can be adopted by any program that seeks integration of AI/ML into its Cybersecurity program. With the Capstone Project, students can delve deeper into any of the interesting applications of AI/ML in Cybersecurity, such as Phishing detection, Malware Classification, and Network instruction detection, among many others. Future work will include conducting AI/ML data ingestion, aggregation, transformation, processing, training, and classification on public cloud platforms such as Amazon, Azure, GCP, and Digital Ocean.

Acknowledgment

Special thanks to Dr. Nadim Zgeib from the Mechanical Engineering Department at UTRGV for being the PI for the NSF grant entitled "Equipping undergraduates with computational engineering skills for the challenges of tomorrow through project-based learning," that will furnish Cybersecurity students with state-of-the-art computing cluster to apply Cybersecurity Machine Learning (CML).

References

1. Quweider, MK, et al., (2022, August), *Crafting a Degree, Empowering Students, Securing a Nation: The Creation of a Modern Cyber Security Degree for the 21st Century*. Paper presented at 2022 ASEE Annual Conference & Exposition, Minneapolis, Minnesota. https://peer.asee.org/41292
2. Quweider, MK, et al., (2023, July), *Early Integrating of Industry Certification Domains and Objectives into a Modern Cybersecurity Degree Curriculum.* Paper presented at 2023 ASEE Annual Conference & Exposition, Baltimore, Maryland. https://nemo.asee.org/public/conferences/327/papers/37056/view
3. Quweider, MK, Zhang, L., and De La Cruz, A. A. (2024, June), *QCTaaS (Quality Cloud Teaching as a Service): An Immersive Framework for Teaching Cloud Computing for Cybersecurity Majors* Paper presented at 2024 ASEE Annual Conference & Exposition, Portland, Oregon.
4. https://www.utrgv.edu/cyberspace/academics/index.htm.
5. Khorbotly, S. (2022, April). Machine Learning: An Undergraduate Engineering Course. Paper presented at the 2022 ASEE Illinois-Indiana Section Conference, Anderson, Indiana.
6. Xu, Y., Zhao, B., Tung, S., & Hu, H. (2023, June). Infusing Data Science into Mechanical Engineering Curriculum with Course-Specific Machine Learning Modules. Paper presented at the ASEE Annual Conference & Exposition, Baltimore, Maryland.
7. Stone, J. E. (2022, June). A Cloud-Based Approach to Introducing Machine Learning in Project-Based Learning Environments. Paper presented at the ASEE Annual Conference & Exposition, Minneapolis, Minnesota

8. Buccafusca, L. (2023, June). Learning from Machine Learning and Teaching with Machine Teaching: Using Lessons from Data Science to Enhance Collegiate Classrooms. Paper presented at the ASEE Annual Conference & Exposition, Baltimore, Maryland
9. Wang, X., Chen, Y., & Zhu, W. (2021). A Survey on Curriculum Learning. IEEE Transactions on Pattern Analysis and Machine Intelligence, 43, 2953-2971.
10. Ramezanian, S., & Niemi, V. (2024). Cybersecurity Education in Universities: A Comprehensive Guide to Curriculum Development. IEEE Access, 12, 61741-61766.
11. Weiss, R., & Mache, J. (2017). Cybersecurity Education and Assessment in EDURange. IEEE Security & Privacy, 15(3), 90-95.
12. Švábenský, V., et al., (2020, March). What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. The 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20), Portland, OR, USA.

Appendix A: AI/MI Modules Description

Module 01 (Summary & Resources)

Cybersecurity Engineering with ML/AI	CYBI- 4336 Fall 2024
Module 1 Summary	
Summary:	*What is ML/AI, Applications in Cybersecurity (CS)* Module 1 Introduces ML/AI. It introduces AI/ML Applications in CS.
Readings/ Watching:	Module 01 Slides. Video Lecture.
Resources:	• Module 01 Notes [Power Point Slides]/Video Lecture.
Deliverables/ Assignments:	1. Description: Set up Anaconda with CPU/GPU. 2. Participate in the discussion Q/A session with your TA

Module 02 (Summary & Resources)

Cybersecurity Engineering with ML/AI	CYBI- 4336 Fall 2024
Module 2 Summary	
Summary:	*Preliminaries (Python, Pandas, NumPy, Matplot)* Module 2 Reviews Python, Pandas, NumPy, and Matplot.
Readings/ Watching:	Module 02 Slides. Video Lecture.
Resources:	• Module 02 Notes [Power Point Slides]/Video Lecture. • AI_ML Notebooks Python, NumPy, Panda, Matplot.
Deliverables/ Assignments:	1. Hw#1. 2. Participate in the discussion Q/A session with your TA

Module 03 (Summary & Resources)

Cybersecurity Engineering with ML/AI	CYBI- 4336 Fall 2024
Module 3 Summary	
Summary:	*The Perceptron Neural Network Model* Module 3 Introduces the Perceptron with activations function & metrics.
Readings/ Watching:	Module 03 Slides. Video Lecture.
Resources:	• Module 03 Notes [Power Point Slides]/Video Lecture. • AI_ML Notebook Perceptron, Phishing Detector
Deliverables/ Assignments:	1. Project-02. **2.** Participate in the discussion Q/A session with your TA

Module 04 (Summary & Resources)

Cybersecurity Engineering with ML/AI	CYBI- 4336 Fall 2024
Module 4 Summary	
Summary:	*The Confusion Matrix* Module 4 Introduces the confusion matrix and related metrics: TP, TN, FP, FN, Recall, Precision, and Accuracy.
Readings/ Watching:	Module 04 Slides. Video Lecture.
Resources:	• Module 04 Notes [Power Point Slides]/Video Lecture. • AI_ML Notebook ConfusionMatrix.
Deliverables/ Assignments:	1. Project-03. **2.** Participate in the discussion Q/A session with your TA

Module 05 (Summary & Resources)

Cybersecurity Engineering with ML/AI	CYBI- 4336 Fall 2024
Module 5 Summary	
Summary:	*Feature Engineering: Part-01* Module 5 introduces feature engineering as it relates to CS.
Readings/ Watching:	Module 05 Slides. Video Lecture.
Resources:	• Module 05 Notes [Power Point Slides]/Video Lecture. • AI_ML Notebook feture_engineerng: date/time
Deliverables/ Assignments:	1. Project-04. **2.** Participate in the discussion Q/A session with your TA

Module 06 (Summary & Resources)

Cybersecurity Engineering with ML/AI	CYBI- 4336 Fall 2024
Module 6 Summary	
Summary:	*Feature Engineering: Part-02* Module 6 introduces feature engineering as it relates to CS.
Readings/ Watching:	Module 06 Slides. Video Lecture.
Resources:	• Module 06 Notes [Power Point Slides]/Video Lecture. • AI_ML Notebook feture_engineerng: networking, textual
Deliverables/ Assignments:	1. Project-05. **2.** Participate in the discussion Q/A session with your TA

Module 07 (Summary & Resources)

Cybersecurity Engineering with ML/AI	CYBI- 4336 Fall 2024
Module 7 Summary	
Summary:	*Feature Engineering: Part-03* Module 7 introduces feature engineering as it relates to CS.
Readings/ Watching:	Module 07 Slides. Video Lecture.
Resources:	• Module 07 Notes [Power Point Slides]/Video Lecture. • AI_ML Notebook feture_engineerng: malware
Deliverables/ Assignments:	1. Project-06. **2.** Participate in the discussion Q/A session with your TA

Module 08 (Summary & Resources)

Cybersecurity Engineering with ML/AI	CYBI- 4336 Fall 2024
Module 8 Summary	
Summary:	*Feature Engineering: Scaling* Module 8 introduces feature engineering scaling as it relates to CS (Min, Max, Robust)
Readings/ Watching:	Module 08 Slides. Video Lecture.
Resources:	• Module 08 Notes [Power Point Slides]/Video Lecture. • AI_ML Notebook feture_engineerng-scaling
Deliverables/ Assignments:	1. Project-07. **2.** Participate in the discussion Q/A session with your TA

Module 09 (Summary & Resources)

Cybersecurity Engineering with ML/AI	CYBI- 4336 Fall 2024
Module 9 Summary	
Summary:	*Supervised Classification: RFT* Module 9 introduces Random Forest Trees with apps to CS.
Readings/ Watching:	Module 09 Slides. Video Lecture.
Resources:	• Module 09 Notes [Power Point Slides]/Video Lecture. • AI_ML Notebook Classification-RFT
Deliverables/ Assignments:	1. Project-08. **2.** Participate in the discussion Q/A session with your TA

Module 10 (Summary & Resources)

Cybersecurity Engineering with ML/AI	CYBI- 4336 Fall 2024
Module 10 Summary	
Summary:	*Supervised Classification: KNN* Module 10 introduces KNN with apps to CS.
Readings/ Watching:	Module 10 Slides. Video Lecture.
Resources:	• Module 10 Notes [Power Point Slides]/Video Lecture. • AI_ML Notebook Classification-KNN
Deliverables/ Assignments:	1. Project-09. **2.** Participate in the discussion Q/A session with your TA

Module 11 (Summary & Resources)

Cybersecurity Engineering with ML/AI	CYBI- 4336 Fall 2024
Module 11 Summary	
Summary:	*Supervised Classification: NBC* Module 11 introduces Naïve Bayesian Classification with apps to CS.
Readings/ Watching:	Module 11 Slides. Video Lecture.
Resources:	• Module 11 Notes [Power Point Slides]/Video Lecture. • AI_ML Notebook Classification-NBC
Deliverables/ Assignments:	1. Project-10. **2.** Participate in the discussion Q/A session with your TA

Module 12 (Summary & Resources)

Cybersecurity Engineering with ML/AI	CYBI- 4336 Fall 2024
Module 12 Summary	
Summary:	*Supervised Classification: SVM* Module 12 introduces Support Vector Machine Classification with apps to CS.
Readings/ Watching:	Module 12 Slides. Video Lecture.
Resources:	• Module 12 Notes [Power Point Slides]/Video Lecture. • AI_ML Notebook Classification-SVM
Deliverables/ Assignments:	1. Project-11. **2.** Participate in the discussion Q/A session with your TA

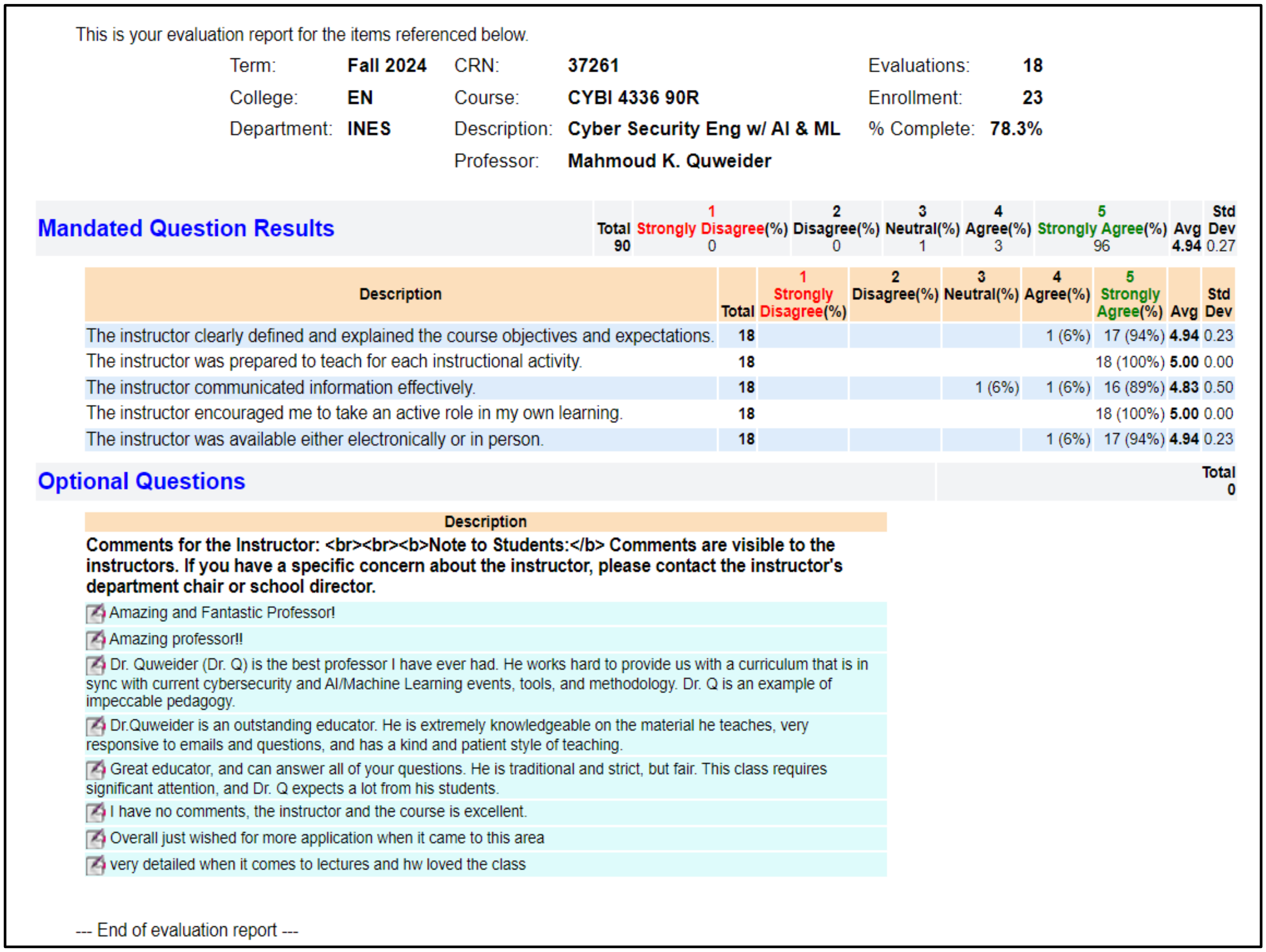
Module 13 (Summary & Resources)

Cybersecurity Engineering with ML/AI		CYBI- 4336 Fall 2024
Module 13 Summary		
Summary:	*Supervised Classification: Keras Tensorflow* Module 13 introduces Tensorflow Classification with apps to CS.	
Readings/ Watching:	Module 13 Slides. Video Lecture.	
Resources:	• Module 13 Notes [Power Point Slides]/Video Lecture. • AI_ML Notebook Classification-TensorFlow	
Deliverables/ Assignments:	1. Project-12. **2.** Participate in the discussion Q/A session with your TA	

Appendix B: Sample Capstone (in Green) Project with AI/MI Emphasis

Group	Team	Title	Advisor
Group 1	Armando Garcia, Citlalli Torres, Luis Martinez, Valeria Alvarez	Security Monitoring Systems	Dr. Jose Poveda
Group 2	Elena V Sanchez, Kiran Bista, Itzel Juarez, Mac Franklin	A Hybrid Multi-layer, Multi-Factor Authentication	Dr. Jorge Castillo
Group 3	Victor Hernandez, Jeremy Soto, Steven Perez, Eduardo Flores	Phishing Campaigns for the Spread of Awareness of the Dangers of Malware	Dr. Liyu Zhang
Group 4	Jorge Rodriguez, Jesus Sanchez, Wilfredo De Leon	Self-Learning Domain Generation Algorithm Detection System On Google Cloud Platform: A Machine Learning And Cloud-Based Solution	Dr. MK Quweider
Group 5	Precious Ramos, Mia Garcia, Kayla Jimenez, Agustin Lara, Ajad Yazji	Cyber defenders: Rise Through the ranks	Dr. MK Quweider
Group 6	Matthew Stelling, Jorge Gomez, Rolando Martinez, and Ricardo Olguin	AI-based Firewall System using TensorFlow	Dr. MK Quweider
Group 7	Luisa Tovar, Mark Aguilar, Nelson Monroy, Micajah Martinez, Amadeus Dutremaine	Deep Dive into Phishing: Targeting, Payload, and Targets	Dr. MK Quweider

Appendix C: AI/ML-Class Evaluation with Unedited Comments



This is your evaluation report for the items referenced below.

Term:	**Fall 2024**	CRN:	**37261**	Evaluations:	**18**
College:	**EN**	Course:	**CYBI 4336 90R**	Enrollment:	**23**
Department:	**INES**	Description:	**Cyber Security Eng w/ AI & ML**	% Complete:	**78.3%**
		Professor:	**Mahmoud K. Quweider**		

Mandated Question Results

Total	1 Strongly Disagree(%)	2 Disagree(%)	3 Neutral(%)	4 Agree(%)	5 Strongly Agree(%)	Avg	Std Dev
90	0	0	1	3	96	**4.94**	0.27

Description	Total	1 Strongly Disagree(%)	2 Disagree(%)	3 Neutral(%)	4 Agree(%)	5 Strongly Agree(%)	Avg	Std Dev
The instructor clearly defined and explained the course objectives and expectations.	**18**				1 (6%)	17 (94%)	**4.94**	0.23
The instructor was prepared to teach for each instructional activity.	**18**					18 (100%)	**5.00**	0.00
The instructor communicated information effectively.	**18**			1 (6%)	1 (6%)	16 (89%)	**4.83**	0.50
The instructor encouraged me to take an active role in my own learning.	**18**					18 (100%)	**5.00**	0.00
The instructor was available either electronically or in person.	**18**				1 (6%)	17 (94%)	**4.94**	0.23

Optional Questions

Total
0

Description

**Comments for the Instructor:

<b>Note to Students:</b> Comments are visible to the instructors. If you have a specific concern about the instructor, please contact the instructor's department chair or school director.**

- Amazing and Fantastic Professor!
- Amazing professor!!
- Dr. Quweider (Dr. Q) is the best professor I have ever had. He works hard to provide us with a curriculum that is in sync with current cybersecurity and AI/Machine Learning events, tools, and methodology. Dr. Q is an example of impeccable pedagogy.
- Dr.Quweider is an outstanding educator. He is extremely knowledgeable on the material he teaches, very responsive to emails and questions, and has a kind and patient style of teaching.
- Great educator, and can answer all of your questions. He is traditional and strict, but fair. This class requires significant attention, and Dr. Q expects a lot from his students.
- I have no comments, the instructor and the course is excellent.
- Overall just wished for more application when it came to this area
- very detailed when it comes to lectures and hw loved the class

--- End of evaluation report ---