Master Course Description for EE-467 (ABET sheet)

Title: Machine Learning for Cyber Security

Credits: 4

Coordinator: Radha Poovendran, Professor, Electrical and Computer Engineering

Goals: This course will study the use of machine learning for cybersecurity applications. There are many security applications which have large amounts of data related to the system as well as adversarial actions. Our ability to identify the type of machine learning algorithms that are useful for specific security applications can help us to improve the defense against attacks and also anticipate the potential attack variants that may arise in the future. Even in the case when one does not know the type of attack, if the machine learning algorithms can identify any anomaly, then the next level of security checks can be performed by other means or experts.

But nothing comes in life for free and this holds for machine learning in the context of cyber too! Another point to remember is "Beware of what you add to your tool bag! You may have an adversary manipulating your machine learning itself." This leads to adversarial machine learning where the machine learning could be tricked to fail the detection! Attacks on Google Video, Toxic Comments, and Google Vision are some of the fun examples where simple modifications make the machine learning algorithms fail!

We will start with setups where the machine learning will be useful for the cybersecurity. As indicated in the title of the course, it will be hands-on course on applying machine learning for cybersecurity applications. Machine learning algorithms will be introduced as needed.

Learning Objectives: At the end of this course, students will be able to:

1. Use machine learning algorithms to implement cybersecurity concepts
2. Implement machine learning algorithms such as clustering, k-means, regression and ensemble methods for anomaly/intrusion detection
3. Use Python libraries - NumPy, and Scikit-learn to build and evaluate AI models
4. Understand how to combat malware, detect spam, and cyber anomalies
5. Use the state-of-the-art python libraries e.g. TensorFlow to develop complex models in the cybersecurity domain and implement real-world examples

Textbook: Hands-On Machine Learning for Cybersecurity by Soma Halder and Sinan Ozdemir; Packt Publisher.

Reference Texts:

1. AI for CyberSecurity by Alessandro Parisi; Packt Publishers
2. Machine Learning for Cybersecurity by Chiheb Chebbi; Packt Publishers
3. Machine Learning for Penetration Testing by Emmanuel Tsukerman; Packt Publishers
4. Adversarial Machine Learning by Vorobeychik and Kantarcioglu; Morgan and Claypool Publishers

Prerequisites:

either CSE 163, or E E 241; either AMATH 352, MATH 208, MATH 308, or MATH 136,; and either IND E 315 , MATH/STAT 394, or STAT 390

Topics:

1. Introduction to Machine Learning for Cyber Security and Python Basics Review [Week 1]

2. Supervised Learning Techniques for Detecting Spam Emails [Week 2]

3. Machine Learning for Solving Automated Public Turing test to tell Computers and Humans Apart (CAPTCHAs) [Week 3]

4. Data Dimensionality Reduction in Cyber Attack Data [Week 4]

5. Network Anomaly Detection Using Clustering Techniques [Week 5]

6. Credit Card Fraud and Malicious Event Detection Using Decision Trees [Week 6]

7. Ensemble Learning for Online Ad blocking, Program Binary Analysis, and Credit Card Fraud Detection [Week 7]

8. Natural Language Processing Techniques for Instruction Set Architecture Identification of Program Binaries [Week 8]

9. Introduction to Adversarial Machine Learning and Backdoor Attacks (Trojan Horses) in Deep Learning [Week 9]

Course Structure: The class meets for two lectures a week, each consisting of 2 hours. There is (bi-)weekly homework due that includes small computer projects in Python. One team-oriented project is planned in this course with Python. Course includes one midterm and one final exam. In-class activities include daily quizzes.

Computer Resources: The course uses Python for homework exercises and course projects. Students are expected to use their personal laptops, but they may use the ECE department computers if available.

Grading: 45% Homework, 50% Project, 5% in-class quiz participation activity.

Religious Accommodation Policy "Washington state law requires that UW develop a policy for accommodation of student absences or significant hardship due to reasons of faith or conscience, or for organized religious activities. The UW's policy, including more information about how to request an accommodation, is available at Religious Accommodations Policy (https://registrar.washington.edu/staffandfaculty/religious-accommodations-policy/). Accommodations must be requested within the first two weeks of this course using the Religious Accommodations Request form (https://registrar.washington.edu/students/religious-accommodations-request/)."

ABET Student Outcome Coverage: This course addresses the following outcomes:

H = high relevance, M = medium relevance, L = low relevance to course.

(1) *An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics.* **(H)** The course uses mathematical tools. Students must identify and design suitable machine learning algorithms. Engineering judgment is developed through the understanding the limitations and advantages of a given data pre-processing techniques and/or machine learning algorithms. Throughout the course we emphasize the need to use sound design principles instead of relying on ad-hoc heuristics only. Towards this direction, machine learning algorithms that were mathematically correct but had design flaws are discussed. Assignments require students to analyze other machine learning algorithms with weaknesses. The homework involves solving engineering problems identified by the assignments and exemplified by class discussion. The homework and project challenge the students to identify the issues and formulate their individual solutions.

(2) *An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors.* **(M)** The project challenges the students to develop, design and implement different machine learning algorithms. In most cases, this is implemented in Python.

(3) *An ability to communicate effectively with a range of audiences.* **(M)** Students are required to write up their simulations in an engineering format. The ability to

communicate effectively in writing is a portion of the grade received on homework and projects. Students are required to give a short presentation on a selected security topic to the class (depending on the instructor).

(4) *An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts.* **(H)** The course covers security vulnerabilities in systems and their societal implications, enabling the students to recognize the ethical dilemmas that they may face in their professions. Impact of good network security protocols is emphasized. We discuss the impact of design and implementation of insecure machine learning algorithms and the way they can be exploited. Focus here will be to show how to design machine learning algorithms that are resilient to common security threats such as spams, toxic comments, and malicious URLs.

(5) *An ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives.* **(H)** The course project is conducted in teams of up to three to four members and constitute 45% of their grade.

(7) *An ability to acquire and apply new knowledge as needed, using appropriate learning strategies.* **(H)** The course emphasizes the need for evolving current secure system designs as new threats emerge and security assumptions are weakened. Further, pointers to security websites and articles are provided in order to enhance personal knowledge in this developing area.

Prepared By: Radha Poovendran

Last revised: 04/20/2022