Old Dominion University

CYSE 635: AI Security and Privacy

Fall 2024

Final Project

Description

Our objective is to implement AI-powered Cybersecurity projects to defend cyber-physical systems and secure the relevant AI algorithms. There are two possible tracks:

- **Track 1: AI in Cyber-Physical Systems**
- **Track 2: Security of AI Algorithms**

Your job is to perform the following tasks:

- choose a track for the project,
- develop a project proposal,
- identify the necessary datasets, algorithms, and tools,
- implement the projects in Python-based platforms, and
- create a project report discussing the implementation and findings

This is a group-based project, and you should do the following things:

- Create or join a group where the maximum number of group members is five or less.
- Give a unique name to your group.
- Collaborate with the group members to brainstorm ideas, learn technologies, develop project proposals, and implement the final project.

Note: You can use any open-source cyber threat or attack dataset for the project. However, it is advised to avoid the datasets that are used in course assignments and class sessions. You can reuse the codes shown in the class sessions, but I suggest you explore open-source repositories, including GitHub, for the codes.

Project Topics

- You have the freedom to choose your own project topic, but it must be approved by the instructor.

- If you are unsure about the project topics, you can choose one from the following topics:

    - AI-based Anomaly Detection for Smart Home Devices (Track 1)
    - AI-powered Cyber Defense for Smart Home (Track 1)
    - AI-driven Vulnerability Scanning and Attack Discovery (Track 1)
    - AI-based Real-Time Fault Detection for Autonomous Drones (Track 1)
    - AI-based Cyber Defense for Healthcare (Track 1)
    - AI-based Malware Analysis (Track 1)
    - AI-assisted Social Engineering Simulation (Track 1)
    - AI-powered Traffic Signal Control System for Smart Cities (Track 1)
    - AI-based Cyber Attack Detection in Autonomous Vehicles (Track 1)
    - Data Poisoning Attack on AI (Track 2)
    - Evasion Attack on AI (Track 2)
    - Membership Inference Attack on AI (Track 2)
    - Generative Adversarial Network Implementation (Track 2)

Deliverables

There will be 4 deliverables for this project:

- **Deliverable 1**: Project Proposal Submission and Presentation (Due Date: 10/30/2024)
- **Deliverable 2**: Project Progress and To-do List (Due Date: 11/13/2024)
- **Deliverable 3**: Final project Presentation (Due Date: 11/24/2024, 12/04/2024)
- **Deliverable 4**: Final Project Report (Due Date: 12/04/2024)

Deliverable 1: Project Proposal Submission and Presentation

Task 1: Project Proposal Submission (in Canvas) [30 points]

- **Problem statement**: briefly describe what security problem you want to solve

5 points

- **Proposed solution**: what AI and/or security methods you plan to utilize to solve the problem **10 points**

- **Dataset description**: talk about the dataset size, features, labels and any relevant information **5 points**

- **Tools and technologies**: talk about the libraries and platforms you plan to use to complete this project **4 points**

- **Expected output**: outline your expectation about the project output **6 points**

Task 2: Proposal Presentation [20 points]

- Give a 10 minutes PowerPoint presentation during the class
- Details about the presentation will be shared later.

Deliverable 2: Project Progress and To-do List [20 points]

- Submit a detailed report in Canvas discussing the progress of the project, the outputs you already have, and the outstanding tasks you need to finish before the final presentation.

- This report must reflect the project proposal and should contain the similar structure (i.e., *problem statement*, *proposed solution* etc.) to discuss the project.

Deliverable 3: Final project Presentation [50 points]

- Prepare a 20 minutes PowerPoint presentation detailing out the problem, proposed solution, dataset details, tools and technologies, project tasks, project results, and limitations of the project.

- Present your completed project in front of the whole class. We will also share more information about the presentation later.

Deliverable 4: Final Project Report [50 points]

- Prepare a 3–5 pages report explaining everything about the project. A template will be shared before the due date of this deliverable with you so that you can prepare your report following the template.