Syllabus: CS 442. Trustworthy Machine Learning

Instructor: Bo Li (lbo@illinois.com)
TA: Zijian Huang (zijianh4@illinois.edu)

1 Objectives

After this course, students will be able to understand security and privacy vulnerabilities of machine learning models, as well as how to make the learning systems robust from various perspectives.

2 Grading

Criteria	Percent of Grade
Final exam	35%
Midterm exam	25%
Homework 1	10%
Homework 2	10%
Homework 3	10%
Class participation (QA)	10%

3 Prerequisites

1. All enrolled students should have taken basic machine learning classes.
2. Homeworks will require training neural networks with standard automatic differentiation packages (TensorFlow, Pytorch).

4 Reading Materials

Checkout: `https://aisecure.github.io/TEACHING/CS442/CS442.html`