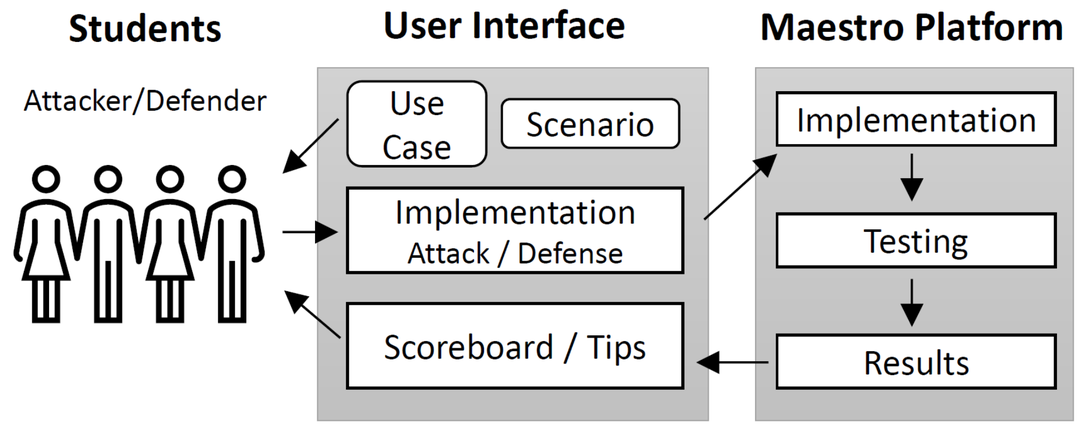
# Multi-Level Attack and Defense Simulation Environment for Artificial Intelligence Education and Research

Zhou Li, Sergio Gago Masague, Sameer Singh (University of California, Irvine)

https://maestro-ai.github.io/

## Objectives

- Design a platform that simulates adversarial machine learning tasks of existing research
- Give students hands-on experiences with building robust AI systems
- Enable comprehensive comparison of different attacks and defenses of robust AI

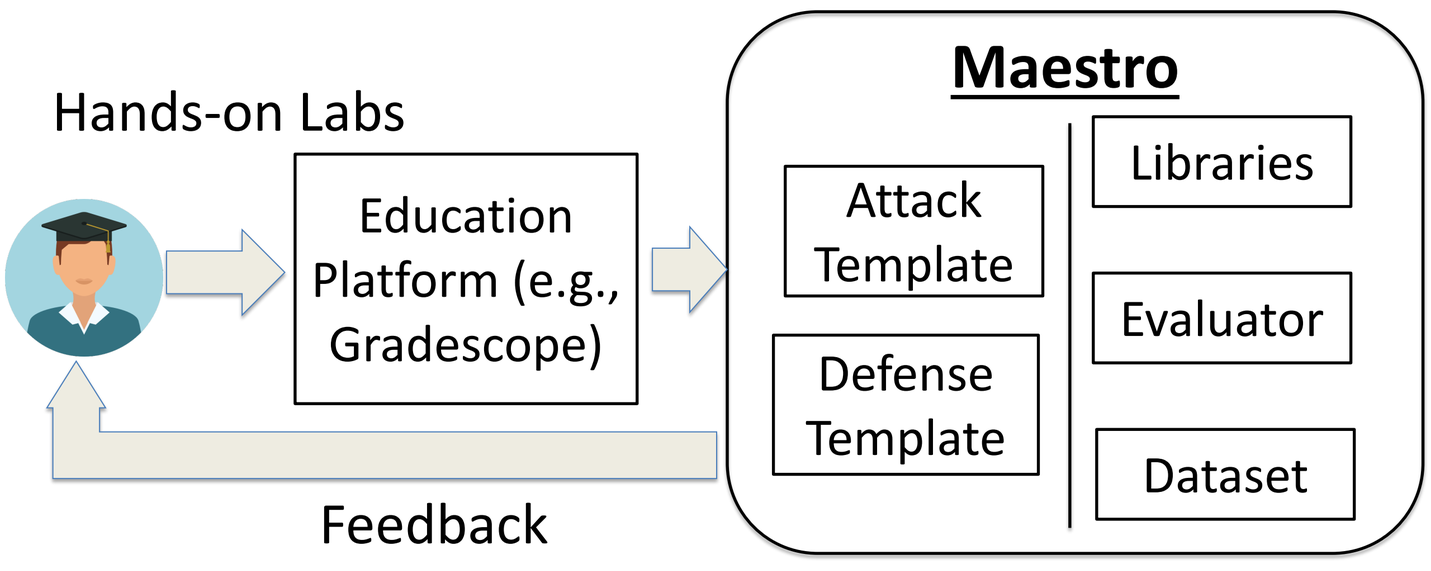



## Challenges

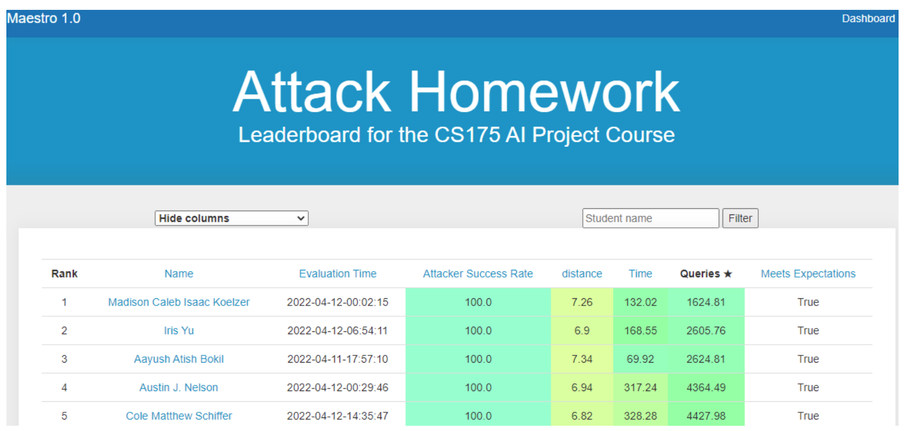
- The research efforts in robust AI are fragmented, lacking a systematic simulation and evaluation framework
- Though AI courses are broadly offered by institutions, the topic of robust AI is often overlooked
- No hands-on labs for students to learn robust AI

## Scientific Impacts

- Several papers published in top AI and cyber-security conferences and journals about robust AI (NAACL'21, TIFS, ACSAC'21)
- Platform (Maestro) implementing various attack and defense methods has been developed
- Game-based strategies are developed for the pedagogical activities of robust AI




Education Setup




| Rank | Name | Evaluation Time | Attacker Success Rate | distance | Time | Queries ★ | Meets Expectations |
|---|---|---|---|---|---|---|---|
| 1 | Madison Caleb Isaac Koelzer | 2022-04-12-00:02:15 | 100.0 | 7.26 | 132.02 | 1624.81 | True |
| 2 | Iris Yu | 2022-04-12-06:54:11 | 100.0 | 6.9 | 168.55 | 2605.76 | True |
| 3 | Aayush Atish Bokil | 2022-04-11-17:57:10 | 100.0 | 7.34 | 69.92 | 2624.81 | True |
| 4 | Austin J. Nelson | 2022-04-12-00:29:46 | 100.0 | 6.94 | 317.24 | 4364.49 | True |
| 5 | Cole Matthew Schiffer | 2022-04-12-14:35:47 | 100.0 | 6.82 | 328.28 | 4427.98 | True |

Course Leaderboard

## Societal Impact

- Raise public awareness of AI robustness
- Foster a workforce with skills of building robust AI systems

UCI University of California, Irvine

## Education and Outreach

- A project-based course has been offered at UCI (2022 Winter and Spring) to teach robust AI with the platform
- Tutorials about robust AI have been delivered at AAAI 2021 and CPAIOR 2021

## Quantify Impacts

- More than 150 UCI students enrolled in the robust AI course
- Course surveys show students benefit from the Maestro platform
- Maestro platform is open-sourced