Christiana Marchese

cemb2020@mymail.pomona.edu
LinkedIn
Personal Website
GitHub

Education

Pomona College, Claremont, CA — May 2024
Bachelor of Arts Computer Science; GPA: 3.94/4.00
Yonsei University, Seoul, South Korea — August 2022-December 2022
CIEE Arts and Sciences Program Study Abroad Program

Research Interests

I am interested in the privacy and security of machine learning (ML) systems as well as the application of ML to system security problems. Currently, I am investigating the vulnerabilities of ML systems and improving their robustness with training and test-time defenses.

Current Research Projects

Senior Thesis, Advised by Dr. Eleanor Birrell and Dr. Anthony Clark — August 2023-Present
Securing Federated Learning Against Post-Breach Evasion Attacks

- Implementing and evaluating a potential test-time defense method specific to federated learning

Research Assistant, Autonomous Robotics and Complex Systems (ARCS) Lab — January 2023-Present
Adversarial Training for Sim-to-Real Transfer

- Researching methods to overcome the sim-to-real transfer gap to develop more safe, robust mobile robots
- Implementing adversarial example generation algorithms for adversarial training of computer vision models

Published Work

Investigating Neural Network Architectures, Techniques, and Datasets for Autonomous Navigation in Simulation
Oliver Chang, Christiana Marchese, Jared Mejia, and Anthony J. Clark
2021 IEEE Symposium Series on Computational Intelligence (SSCI) Conference (PDF)

Unpublished Work

Research Poster and Presentation:
Predicting Mental Health Outcomes with Deep Learning
Christiana Marchese
2021 ACM Practice and Experience in Advanced Research Computing (PEARC) Conference (PDF)

Class Project Writeup:
Implementing and Evaluating the Probability Weighted Word Saliency Algorithm as a Method of Adversarial Example Generation for Deep Neural Networks
Christiana Marchese
2023 Natural Language Processing Final Class Project (PDF)

Past Research Projects

Cybersecurity Intern, AT&T June 2023-August 2023

ML-Driven Fraud Detection Project with the Research and Innovation in Security Engineering Team

- Developed ML model for sim swap fraud detection across customer call logs to streamline the confirmation of fraud cases (FastAI)
- Researched and implemented word-based and phrase-based sentiment identification algorithms for the text highlighting of words commonly associated with fraud cases
- Work deployed in internal fraud detection app that attempts to confirm thousands of fraud cases every day

CVE Analysis Project with the Application Vulnerability Team

- Created mechanized reports to assess the impact of CVEs across the application landscape
- Web scraped CVE data and processed internal vulnerability data (Beautifulsoup, PySpark, DataBricks)
- Collaborated with the AI Tiger group to brainstorm AI-driven solutions for vulnerability remediation efforts

Research Assistant, Autonomous Robotics and Complex Systems (ARCS) Lab May 2021-May 2022

Investigating Neural Network Architectures, Techniques, and Datasets for Autonomous Navigation

- Researched neural networks that retain different degrees of state for simulated maze navigation (GitHub)
- Built custom datasets and modified convolutional neural network (CNN) architectures to create hybrid-input CNNs and ConvLSTMs (Pytorch and FastAI)
- Wrote automation scripts to streamline the training and inference of neural network models
- Conducted literature reviews and wrote lab learning material, library documentation, and a publication

Research Apprentice, NSF XSEDE Empower Program January 2021-May 2021

Predicting Mental Health Outcomes with Deep Learning

- Researched the use of deep learning for community assessment of mental health, using US Census Bureau data, CDC data, geospatial analysis, and TACC's Stampede2 supercomputer resources
- Developed and compared a linear regression model, a multilayer perceptron, and a CNN that all predict the risk level of California counties for suicide based on community features (Sklearn, Pytorch)

High-Performance Computing Support, Pomona College August 2020-May 2021

Observing Trends in Technical Skill Demand with Topic Modeling

- Processed and visualized data (Python, R) to research market trends in technical skill demand

Teaching Experience

Computer Systems – Teaching Assistant, Pomona College August 2023-Present

English Conversation – Teacher (Volunteer), Liberty in North Korea August 2022-December 2022

Introduction to Computer Science – Teaching Assistant, Pomona College January 2021-May 2021

Honors

Academic: Marshall Scholarship Finalist (2023), Pomona College Scholar, SCIAC All-Academic Team

Athletic (Water Polo): Division 1 All CIF-SS Third Team Selection, CIF-SS Jim Staunton Champions for Character Award, All-Trinity League First Team Selection, 2019 CIF-SS Division 1 Regional State Champion

Other Industry Work Experience

Meta University Engineering Intern – Android, Meta Platforms Inc. May 2022-August 2022

- Created a fully functional Android social media app: SurfStop (Java)
- Implemented a Parse backend running on top of MongoDB, data offline persistence (Room ORM), ephemeral timelines through database auto-purging (JavaScript, Java), etc.
- Deployed custom in-app beach state image classifier with web-scraped image data (Keras) (Model's GitHub)

Skills

Technical: Proficient in Python, Java; Experienced in TensorFlow/Keras, Pytorch, Fastai, TensorFlow Federated, Android Mobile Development, Jupyter Notebook, C, Git, Linux, CAD, soldering

Language: English (native), Korean (intermediate, conversational), Spanish (elementary)

Extracurricular Activities

Surf Club, Spotlight Musical Theatre, Greenroom Theatre, Korean Student Association, Association for Computing Machinery-Women