Allen H. Yan

(503) 200-8107 · allenyan999@gmail.com

Executive Summary

I am a fourth-year Ph.D. student at Oregon State University specializing in adversarial machine learning (AML). My research focuses on developing defense and forensic techniques to protect machine learning systems from adversarial attacks. Experienced in deep learning, large language models, and reinforcement learning, with a diverse skill set in both software and hardware. Seeking an internship in the artificial intelligence domain.

Skills

Topics: Adversarial Machine Learning, Artificial Intelligence, Deep Learning, Convex & Nonlinear Optimization, Reinforcement Learning, Computer Vision, Retrieval-Augmented Generation, Large Language Models, Algorithms, Data Structures, Parallel Programming, Embedded Systems, Microprocessors, Computer Architecture, Information Theory, Circuit Theory

Software: Python, PyTorch, TensorFlow, C++, Boost C++, C, Java, JavaScript, UNIX/Linux, Assembly, Hugging Face, Git, Perforce, MATLAB, OpenCV, OpenMP, OpenVINO, Microsoft Office, LaTeX, SQL, Docker, Verilog

Language: English – Native Speaker, Chinese – Native Speaker

Education

Oregon State University – Corvallis, OR — September 2021 – June 2026 (Anticipated)
Ph.D. in Computer Science & Artificial Intelligence (Double Major) — GPA 3.97

- Academic Advisors: Dr. Jinsub Kim & Dr. Raviv Raich
- Research Focus: Adversarial Machine Learning

Baylor University – Waco, TX — August 2017 – May 2021
B.S. in Electrical and Computer Engineering: — Cumulative GPA 3.89, Major GPA 3.98

- Minor: Computer Science, Mathematics

Experience

Intel Corporation – Hillsboro, OR
AI Software Development Engineer Intern – Intel Flex — Summer 2024

- Conducted literature review of 15 recent papers on **Retrieval-Augmented Generation (RAG)** technologies and presented key findings to a forum of over 30 senior technical leaders.
- Streamlined profiling workload of 3 high-impact **RAG** systems on Lunar Lake systems.
- Improved detection rate of counterfeit image by 14.98% using **CNN**-based classification models with **TensorFlow**.
- Accelerated neural network inferencing speed by 10% using novel weight approximation technique with **PyTorch**; this innovation was submitted for patent application.
- Derisked 5 technical challenges of porting **PyTorch**-Triton AI demo workload to Intel hardware system.

Power & Performance Software Engineer Intern – CCG PEG — Summer 2020

- Developed automated workload to measure performance of Microsoft 365 on Intel hardware.
- Analyzed performance logs and browser traces of Microsoft 365 to identify areas for hardware optimization.

Oregon State University – Corvallis, OR
Graduate Research & Teaching Assistant — Fall 2021 – Present

- Devised approach to approximate attack trajectory from aftermath of test-time attacks using **generative autoencoders**, achieving 97.14% pixel similarity.
- Integrated human intervention mechanism into defensive countermeasures against ongoing **adversarial attacks** using **Python** and **PyTorch**, reducing attack effectiveness by 9.71%.
- Taught 6 graduate and undergraduate courses featuring **C**, **Python**, **Assembly**, Elm, and Prolog.

Synopsys – Pasadena, CA
Software Engineer Intern – Optical Solutions Group — Summer 2021

- Renovated data conversion framework between LightTools and CODE V using **Boost C++** and Fortran, enabling stable precision preservation beyond 3 decimal places.
- Implemented new raytracing function for fictitious materials in LightTools, adapting methods from key literature.

Baylor University – Waco, TX

Master Tutor of Computer Science & Student Success Center Website Manager Fall 2019 – Summer 2021

- Led weekly computer science lectures in **C++** and **Python** for up to 30 students and developed study materials.
- Maintained more than 10 Success Center web pages.

Undergraduate Research Assistant Fall 2018

- Redesigned Quantum-dot Cellular Automata computing software using **MATLAB** for 200% faster UI response.

Projects

Human-in-the-Loop Defense Against Test-Time Attacks on Sensor-to-Decision System Fall 2021 – Fall 2022

- Devised interactive defense and forensic countermeasures for machine learning systems against adversarial data attacks using **Python** and **PyTorch**. Project was sponsored by Naval Engineering Education Consortium (NEEC).

Approximating Inverse Attack Functions of Adversarial Examples Spring 2022

- Led a team of three to design an inverse adversarial attack function approximator using **Variational Autoencoders**.

Security Brands Keypad Testing Machine Spring 2021

- Collaborated with a team of six to design an automated security keypad stress-test fixture controlled by Arduino microcontroller and **Java** program. Project was commissioned by Security Brands Inc.

Rock, Paper, Scissors AI Spring 2021

- Trained a **LSTM** model using **TensorFlow** to predict human behavioral patterns in rock, paper.

Deep Learning Agent in Real Time Strategy (RTS) Games Fall 2020 – Spring 2021

- Implemented deep learning AI agent using **TensorFlow** to play StarCraft II.

Automatic Garden Watering System Fall 2020

- Directed a team of four to develop a webserver-controlled embedded system using BeagleBone Black microcontroller and **JavaScript**, automating soil moisture measurement and maintenance.

Publications

- **Yan, A.**, Kim, J., & Raich, R. (2023). Forensics for Adversarial Machine Learning through Attack Mapping Identification. *IEEE International Conference on Acoustics, Speech and Signal Processing*.
- Yi, Z., **Yan A.** (2024). Fake Image and Video Detection Method Based on Camera Noise Pattern. *Intel Software Professionals Conference.*
- Hollis, J., **Yan A.**, Millsap, S., Vogt, A. Rosenthal, S., Kim, J. Raich, R. (2022). Cost-Aware Defense of Sensors-to-Decisions System against Malicious Data Attacks. *Naval Engineering Education Consortium Fest.*

Leadership

2024 IEEE Sensor Array and Multichannel Signal Processing Workshop – Corvallis, OR Summer 2024

Registration Coordinator

- Communicated with conference attendees on behalf of organizing committee and conference services.
- Tracked and logged registration status of paper submissions.

Baylor Unicycle Academy – Waco, TX Fall 2018 – Spring 2020

Co-founder & Coach

- Provided instruction to club members on unicycle riding techniques.
- Advertised club publicity by performing in university and city events.

Honors & Awards

William Mearse Scholarship – 2018

- Scholarship endowed by Mearse family for qualified engineering students at Baylor University.

Regent's Gold Scholarship – 2017

- Full tuition scholarship by Baylor University in recognition of outstanding incoming students.

National Merit College Sponsored Scholarship – 2017

- Scholarship issued by College Board to National Merit Finalists.