BENJAMIN BROWN

(484) 788-3226 ◇ Emmaus, PA
brown.ben.2019@gmail.com ◇ github.com/bendoesai ◇ linkedin.com/in/bendoesai

OBJECTIVE

Passionate, independently motivated, consistently curious AI security researcher with experience in adversarial machine learning, high-performance computing, and systems optimization. Looking to collaborate with elite specialists on novel applications of AI that have extensive impact. **Available Immediately**

SKILLS

Software Python, PyTorch, TensorFlow, NumPy, ART, OpenCV, C++, C, Assembly, Version Control (Git)
ML/AI Adversarial ML, Computer Vision, Real-time Inference, Reinforcement Learning, Time Series Analysis

EDUCATION

BS Electrical Engineering - AI Option, Rochester Institute of Technology — Earned 2024
Applied Statistics Immersion, Rochester Institute of Technology — Earned 2024

EXPERIENCE

Research Assistant | DeFake Project — Aug 2023 - Present
Tags: AI Security, Adversarial ML, ART, Deepfake Detection, HPC, Research — *Rochester, NY (Remote)*

- Converted research requirements into Python code extending DeepfakeBench with ART for adversarial ML tasks.
- Analyzed vulnerabilities of 10+ video, spatial, and naive deepfake detectors via adversarial sample generation.
- Tuned parameters of AutoAttack, C&W, and PGD to generate 20,000+ adversarial samples with minimal delta.
- Accessed Ubuntu SSH server for development of prototype framework on CUDA-enabled multi-GPU machine.
- Packaged experimental runs for RIT's HPC cluster with SPACK, and Anaconda, reducing runtimes by days.

Team Lead | Advanced Growing Resources — August 2023 - May 2024
Tags: Project Management, Technical Communication, Embedded Systems, C++ — *Rochester, NY*

- Gathered customer requirements for the design and production of hardware and firmware for a SWIR sensor.
- Lead small, diverse team through 8 design reviews to deliver a working prototype 50% under budget.
- Wrote C++ to interface with a Teensy microcotroller and communicate with hardware via SPI and I2C.
- Produced detailed technical report detailing design process and presented at CEIS symposium and Imagine RIT.

Electrical Intern | L3Harris Technologies — Jan 2023 - Aug 2023
Tags: Systems Optimization, Python Automation, Embedded Linux — *Rochester, NY*

- Designed automated testbench for VHF radios using serial communication, increasing efficiency by 57%.
- Communicated with embedded Linux environment via serial port to log results of 20+ verification tests.
- Debugged and repaired failing units using multimeters, oscilloscopes, spectrum analyzers and function generators.

Machine Learning Intern | TIMET Morgantown — Jan 2022 - Aug 2022
Tags: Python, Time Series Analysis, Industry 4.0, OpenCV, XGBoost, YOLOv4 — *Morgantown, PA*

- Worked directly under senior technical fellow to unlock millions of data points from all steps of production.
- Deployed YOLOv4 on edge device to spot melting defects on video using Python and OpenCV.
- Estimated chemical profile of melt using historical time series data via SQL, Scikit-learn, and XGBoost.

CURRENT PROJECT - TRACKMANIA RL

Tech Stack: Windows, git, Python, PyTorch, Anaconda, Gymnasium, TMRL

- Developed real-time autonomous driving agent in Python, integrated within a simulated training environment.
- Researched split-head model to operate on three continuous controls simultaneously.
- Optimized LIDAR-based A2C agent to navigate complex control task under 50ms inference constraint.
- Compiled results in technical report about the agent's capability to handle complex control tasks.