SAE FURUKAWA

furukawa.s[at]northeastern.edu GitHub LinkedIn

EDUCATION

Northeastern University, Boston, Massachusetts September 2025 ~ present
Ph.D. in Computer Science; Advisor: Alina Oprea

Pomona College, Claremont, CA May 2025
Bachelor of Arts Computer Science (GPA: 3.96); Cum Laude

RESEARCH INTEREST

My research focuses on privacy-preserving machine learning, differential privacy, adversarial machine learning, and machine learning applied to security.

PREPRINTS

Ashley Song, **Sae Furukawa**, Zhian Zhou, Bryce Tu, Chi David Nembhard, Machine-Learning Enhanced Human-Error Detection in Drone-Assisted Bridge Inspections, Preprint (under review at IEEE Transactions on Human-Machine Systems), 2025.

OTHER RESEARCH WORKS

Differentially Private Federated Fine-tuning of Foundation Models for Hate Speech Detection

- 2025 Pomona College Senior Thesis, Advised by Dr. David Kauchak and Dr. Eleanor Birrell

Towards the Development of a Real-Time Deepfake Audio Detection System in Communication Platforms

- Peer reviewed and accepted to the 2024 New York Annual Conference hosted by America Academic. (PDF)

INDUSTRY EXPERIENCE

Information Security Intern | Apple Information Security (AIS), Apple, Inc May ~ August 2024

- Processed over 1 million command line data using Sentence Transformer Models (SBERT) to compute word embedding.
- Developed generative models for anomaly detection in command line execution, such as Deep Autoencoding Gaussian Mixture Model (DAGMM) and Variational Autoencoder (VAE), successfully classifying all malicious commands in the top 1 % of the most anomalous.
- Researched the feasibility of implementing anomaly detection through differentially private federated learning, marking AIS's first theoretical exploration of detection systems on-device.
- Employed the Moment Accountant Gaussian Mechanism to ensure privacy guarantees for federated learning models, minimizing the privacy-utility trade-off through hyperparameter tuning and maintaining model accuracy above 90 %.
- Drafted a paper for publication documenting experimental results and findings to support AIS's ongoing research in privacy-preserving, on-device detection systems.

Software Development Intern | SMBC Nikko Securities, Tokyo, Japan December 2023 ~ January 2024

- Developed and implemented a robust testing framework for the platform's user interface, specifically designed to support rule injections in the SNET algorithm trade system, utilizing Selenium Webdriver for automation.
- Significantly improved testing efficiency by reducing the cycle duration by 75 % while expanding coverage by 400 %.
- Enhanced platform UI for improved usability and user-computer interaction performance, using Groovy, CSS, and HTML.

Cybersecurity AI Enabler Intern | RediMinds, Inc September ~ December 2023

- Built system executables aimed at recognizing and countering deep fakes and AI voice clones in real-time.
- Leveraged audio processing and feature engineering techniques, including MFCC, Mel Spectrograms, and data augmentation, to preprocess 10,000+ audio datasets and extract pertinent features.
- Designed and optimized the CNN models through hyperparameter tuning and preprocessing methods, such as normalization and learning rate scheduling, achieving a 10+ % improvement in validation accuracy.

- Developed a ResNet-based model to counter voice-based logical access attacks, outperforming baseline models from the ASVspoof 2019 challenge by reducing the Equal Error Rate (EER).

Cybersecurity Research Intern | Foundation for Defense of Democracies June ~ August 2023

- Spearheaded in-depth research into the threat landscape and security directives of the U.S. railroad industry by focusing on cyber risks specific to operational technology and industrial control systems and identifying policy gaps.
- Investigated attack vectors and exploited vulnerabilities in the Iran-Israel cyberattacks using web-scrapping and API.
- Authored policy brief analyzing the South Korea National Security Strategy and op-ed focusing on U.S.-Japan cooperation in East Asia's cyber-defense.

TEACHING EXPERIENCE

Teaching Assistant | Department of Computer Science, Pomona College September 2023 ~ May 2025

- Neural Networks (CS152), Prof. Anthony Clark, Spring 2025
- Algorithms (CS140), Prof. Kauchak, Fall 2024
- Data Structures (CS62), Prof. Papoutsaki, Fall 2023

HONORS

Pomona College Scholar, Grace Hopper Celebration Scholar (2023), Blackhat USA Student Scholar (2023)
Math Canada National Team Candidate (2020)

SKILLS

Machine Learning: PyTorch, TensorFlow, Scikit-Learn, NumPy, Pandas, Keras, Ramsay (Apple PFL), Huggingface
Programming languages: Python, C, Scala, MySQL, Java/Groovy, JavaScript, CSS/HTML, Standard ML
Languages: English (native), Japanese (native), French (fluent), Arabic (elementary)