

PRATIK VAISHNAVI

pvaishnavi@cs.stonybrook.edu | Stony Brook, NY
pratik18v.github.io | linkedin.com/in/pratik-vaishnavi-aa2585b3

PROFESSIONAL SUMMARY

8+ years of research experience in Machine Learning, Deep Learning and Computer Vision, covering the following **topics**: adversarial robustness, transfer learning, knowledge distillation, self-supervised learning, domain generalization, and video understanding; and the following **models**: classifiers, detectors, generative AI models, transformers, and segmentation models.

EDUCATION

PhD, Computer Science, Stony Brook University **08/2018 – 05/2024 (Expected)**

Thesis: Improving the Usability of Methods for Training and Evaluating Secure ML Models

Topics: Adversarial Machine Learning, Knowledge Transfer, Self-supervised Learning, Vision Foundation Models, LLM Pre-training

MS, Computer Science, Stony Brook University **08/2016 – 05/2018**

Thesis: Generating Temporal Action Proposals in Long Untrimmed Videos

Topics: Video Understanding, Action Detection, Sequential Modelling (LSTMs, GRUs)

BTech, Electronics, Sardar Vallabhbhai National Institute of Technology **07/2012 – 05/2016**

Thesis: Developing Software for Drone-Based Precision Farming

EXPERIENCE

Sony AI, Security & Privacy Research Intern, Tokyo, Japan **05/2023 – 09/2023**

Developed an efficient method to train secure object detectors (Faster-RCNN, YOLO, SSD) using dataset distillation. Reduced training time by 50% while preserving performance and robustness, in turn reducing monetary costs and environmental impact associated with GPU usage.

Amazon, Applied Scientist Intern, Seattle, WA **06/2021 – 09/2021**

Developed a video-based camera obstruction detector using 3D-CNNs to improve the reliability of Amazon One devices in unrestricted deployment settings. Curated a camera obstruction dataset from scratch, containing over 3000 videos collected using 19 unique obstructions. Work was published at Amazon Machine Learning Conference and spawned a dedicated project for a new full-time employee.

Amazon, Applied Scientist Intern, Remote **05/2020 – 08/2020**

Developed a novel spoof image generation method using Generative Adversarial Networks (GANs). Effectively integrated synthetic data into the training process of the spoof detector of the Amazon One device, reducing ACER by 14% on average across 13 unseen spoof categories. Work was published at Amazon Computer Vision Conference.

SKILLS

- **Coding** | Python (NumPy, Pandas, Scikit-learn, OpenCV), Bash, HTML, CSS, JavaScript
- **Deep Learning Frameworks** | PyTorch, TensorFlow, Keras
- **Miscellaneous** | LaTeX, Markdown, Linux, MATLAB, Git, AWS, Docker

SELECTED PUBLICATIONS

- [Accelerating Certified Robustness Training via Knowledge Transfer](#)
NeurIPS 2022 | [P. Vaishnavi](#), K. Eykholt, and A. Rahmati
- [On the Feasibility of Compressing Certifiably Robust Neural Networks](#)
TSRML Workshop @ NeurIPS 2022 | [P. Vaishnavi](#), V. Krish, F. Ahmed, K. Eykholt, and A. Rahmati
- [Transferring Adversarial Robustness Through Robust Representation Matching](#)
USENIX Security Symposium 2022 | [P. Vaishnavi](#), K. Eykholt, and A. Rahmati
- [Ares: A System-Oriented Wargame Framework for Adversarial ML](#)
IEEE Security and Privacy Workshops 2022 | F. Ahmed, [P. Vaishnavi](#), K. Eykholt, and A. Rahmati
- [Can Attention Masks Improve Adversarial Robustness?](#)
EDSMLS Workshop @ AAAI 2020 | [P. Vaishnavi](#), T. Cong, K. Eykholt, A. Prakash, and A. Rahmati
- [Complete List on Google Scholar](#)

OTHER PROJECTS

- Multi-layer Neural Composer for Personalized Product Descriptions (*Fall 2017 and Spring 2018*)
Investigated attention-based sequence-to-sequence language generation methods as a scalable approach for delivering personalized e-commerce product descriptions. Specifically, developed a multimodal learning method to refine product embeddings by collectively using image and text data.
- Large-scale Video Understanding (*Spring 2017*)
Developed a classifier to assign video-level labels for the YouTube-8M dataset containing 8 million videos. Used a combination of pre-trained feature encoders and Mixture of Experts to improve the Average Precision@k by 7% over the available baseline.

REVIEWER DUTIES

- **Conferences:** CVPR, ICCV, ECCV, ACCV, NeurIPS, ICLR, ICML, USENIX Security, IEEE S&P
- **Journals:** IEEE Transactions on Image Proc., IEEE Transactions on Info. Forensics & Security
- **Workshops:** TSRML @ NeurIPS 2022, EDSMLS @ AAAI 2020

TEACHING ASSISTANTSHIPS (STONY BROOK UNIVERSITY)

- CSE 508: Network Security (*Fall 2019 & Spring 2021*)
- CSE 527: Introduction to Computer Vision (*Spring 2019*)
- CSE 512: Machine Learning (*Fall 2018*)

AWARDS AND EXTRACURRICULARS

- Best Poster Award Recipient, Graduate Research Day, 2023
- Organizer, Adversarial Machine Learning Reading Group, 2022
- Invited Speaker, IBM Security Group Seminar, 2021
- Mentor, Women in Science and Engineering Lab Rotations, 2021
- Organizing Committee, Graduate Research Day, 2021
- Vice President, Computer Science Graduate Student Organization, 2020-2021
- Editor, College Newsletter, 2015
- Executive Board Member, Literary Affairs Committee, 2013-2015