Pratik Vaishnavi

Personal Data

Address: Room 334, NCS, Stony Brook University - 11794
email: pvaishnavi@cs.stonybrook.edu
Website: https://pratik18v.github.io

Education

Present Aug 2018	PhD in Computer Science Stony Brook University, NY
May 2018 Aug 2016	MS in Computer Science Stony Brook University, NY
May 2016 Aug 2012	Bachelors of Technology in Electronics Engineering Sardar Vallabhbhai National Institute of Technology, India

Work Experience

Sep 2023 May 2023	Research Intern at Privacy Preserving Machine Learning Team Manager: Lingjuan Lyu *SonyAI, Tokyo, Japan*
Sep 2021 Jun 2021	Applied Scientist Intern at Amazon One Team Manager: Manoj Aggarwal *Amazon, Seattle, Washington*
Aug 2020 May 2020	Applied Scientist Intern at Amazon One Team Manager: Manoj Aggarwal *Amazon, Remote*
May 2018 Jun 2017	Research Assistant at Data Science Lab Advisor: Steven Skiena *Stony Brook University, New York*
Jul 2015 May 2015	Research Intern at Electrical Engineering Department Advisor: Rajeev Ranjan Sahay *Indian Institute of Technology, Kharagpur, India*

Publications

1. On the Feasibility of Compressing Certifiably Robust Neural Networks

   Pratik Vaishnavi, Veena Krish, Farhan Ahmed, Kevin Eykholt, Amir Rahmati

   Workshop on Trustworthy and Socially Responsible Machine Learning, NeurIPS, 2022

2. Accelerating Certified Robustness Training via Knowledge Transfer

   Pratik Vaishnavi, Kevin Eykholt, Amir Rahmati

   Advances in Neural Information Processing Systems (NeurIPS), 2022

3. Transferring Adversarial Robustness Through Robust Representation Matching

   Pratik Vaishnavi, Kevin Eykholt, Amir Rahmati

   USENIX Security Symposium, 2022

4. Ares: A System-Oriented Wargame Framework for Adversarial ML

   Farhan Ahmed, *Pratik Vaishnavi*, Kevin Eykholt, Amir Rahmati

   Deep Learning and Security Workshop, IEEE Symposium on Security and Privacy, 2022

5. Can attention masks improve adversarial robustness?

   Pratik Vaishnavi, Tianji Cong, Kevin Eykholt, Atul Prakash, Amir Rahmati

   International Workshop on Engineering Dependable and Secure Machine Learning Systems, AAAI, 2020

6. Robust Pose Detection using Deep Learning

   International Conference on Computer Vision and Image Processing, 2017

7. Nrityabodha: Towards understanding Indian classical dance using deep learning

   Signal Processing: Image Communication, Elsevier, 2016

8. 2 papers internally published at Amazon.

Pre-prints

1. Towards Model-Agnostic Adversarial Defenses using Adversarially Trained Autoencoders

   Pratik Vaishnavi, Kevin Eykholt, Atul Prakash, Amir Rahmati

   arXiv:1909.05921, 2019

2. Robust classification using robust feature augmentation

   Kevin Eykholt, Swati Gupta, Atul Prakash, Amir Rahmati, *Pratik Vaishnavi*, Haizhong Zheng

   arXiv:1905.10904, 2019

Invited Talks

- "Transferring Adversarial Robustness using Robust Representation Matching"

  IBM Security Group Seminar

Academic Services

- Reviewer
  - **Conferences:** ICCV, ICML, CVPR, NeurIPS, ECCV, USENIX Security, TheWebConf
  - **Journals:** IEEE Transactions on Information Forensics & Security, IEEE Transactions on Image Processing
  - **Workshops:** Trustworthy and Socially Responsible Machine Learning (NeurIPS '22), Engineering Dependable and Secure Machine Learning Systems (AAAI '20)
- Teaching Assistant - Computer Science Deptartment, Stony Brook University
  - CSE 508: Network Security *(Fall'19 & Spring'21)*

- CSE 527: Introduction to Computer Vision *(Spring'19)*
- CSE 512: Machine Learning *(Fall'18)*

Major Projects

August 2018 – Present
Improving the usability of model re-training based adversarial defenses
PhD Dissertation, Advisor: Prof. Amir Rahmati
Developing techniques to improve the usability of methods for training (empirically/provably) robust deep neural networks to be deployed in commercial applications.

June 2017 – May 2018
Temporal action proposals in long untrimmed videos
MS Thesis, Advisor: Prof. Minh Hoai Nguyen
Developed a unified deep neural network based model for temporal localization and detection of human actions in long untrimmed video sequences.

Feb 2017 – Dec 2017
Multi-layer Neural Composer for Personalized Product Descriptions
Advisor: Prof. Niranjan Balasubramanian
Investigated neural language generation methods as a scalable approach for delivering personalized descriptions. Specifically, explored using images to refine product descriptions generated by sequence-to-sequence language generators.

Jan 2017 – May 2017
Large scale video understanding
Advisor: Prof. Minh Hoai Nguyen
Investigated the effectiveness of ensemble of deep learning models for labelling videos based on their content.

Skill Set

- **Languages:** Python; **DL Frameworks:** PyTorch, Tesnorflow, Keras; **Version Control:** Git; **Documentation:** LaTeX, Markdown

Extracurriculars

- Stony Brook University
  - Organizer: Adversarial Machine Learning Reading Group (Spring'22)
  - Mentor: Women in Science and Engineering Lab Rotations (Spring'21 & Fall'21)
  - Vice President: Computer Science Graduate Student Organization (Fall'20 & Spring'21)
  - Organizer: Graduate Research Day '21
  - Best Poster Award Recipient: Graduate Research Day '23
- Sardar Vallabhbhai National Institute of Technology
  - Executive Board Member: Literary Affairs Committee
  - Editor: College Newsletter (Renesa)