

# Kaustubh Sridhar

4258 Chestnut Street, Unit 308  
Philadelphia, PA, 19104  
☎ +1 267-290-7947  
✉ [ksridhar@seas.upenn.edu](mailto:ksridhar@seas.upenn.edu)

## Education

- 2019 - Present **University of Pennsylvania**, Philadelphia, PA.  
**PhD Candidate, Electrical and Systems Engineering**, GPA: 3.93/4.  
Advised by [Prof. Insup Lee](#), [Prof. Oleg Sokolsky](#), and [Prof. James Weimer](#), [PRECISE Center](#).
- 2015 - 2019 **Indian Institute of Technology Bombay**, Mumbai, India.  
Bachelor Of Technology (with Honors) In Aerospace Engineering, GPA: 9.07/10.  
**Minor in Systems and Control Engineering**, Class Rank 2.

## Research Interests

Sample-Efficient Deep Reinforcement Learning (RL), RL for Combinatorial Optimization, Adversarial Robustness of Neural Networks (NN), Out-of-Distribution (OOD) Detection, Safety and Security of Autonomous Vehicles and Cyber-Physical Systems.

## Research Experience

- Aug 2019 - Present **PRECISE Center, University of Pennsylvania**, PhD Researcher, Philadelphia, PA.  
Advised by [Prof. Insup Lee](#), [Prof. Oleg Sokolsky](#), [Prof. James Weimer](#).  
Collaborated with [Prof. Osbert Bastani](#), [Prof. Edgar Dobriban](#), [Prof. Fanxin Kong](#).  
Highlights:
  - Improved deep RL sample-efficiency by two-orders-of-magnitude with option templates [2022A, videos].
  - Enhanced adversarial robustness of NN's via persistent excitation [2022C], overdesigning [2022E].
  - Developed conformal time-series OOD detectors [2022D] and real-time adversarial detectors [2021].
  - Composed sensor attacks and recovery algorithms for cyber-physical systems [2022F, 2022G, 2020].
- May - Aug 2022 **Amazon Web Services (AWS) AI Labs**, Applied Scientist Intern, Santa Clara, CA.  
Collaborated with [Dr. Murali Narayanaswamy](#), [Dr. Abishek Sankararaman](#), [Vikramank Singh](#)  
Highlight: Model-free RL augmentations for model-based virtual machine packing in datacenters [2022B].
- May - Aug 2021 **Argo AI (Ford & VW's Self-Driving Partner)**, Systems Engineer Intern, Dearborn, MI.  
Product Security and Sensor Functional Safety Team  
Highlight: Threat models for object detection and tracking algorithms for Argo's self-driving cars.
- May - Aug 2018 **Cyber-Physical Systems Lab, Duke University**, Summer Research Fellow, Durham, NC.  
Advised by [Prof. Miroslav Pajic](#),  
Highlight: Built a self-driving platform for intrusion detection testing [videos].
- Jan - Dec 2018 **Indian Institute of Technology Bombay**, Undergraduate Research Assistant, India.  
Advised by [Prof. Srikant Sukumar](#),  
Highlight: Bachelor's thesis on real-time quadrotor control [2019, videos].

## Publications and Preprints

### Deep Reinforcement Learning

- 2022A Souradeep Dutta, **Kaustubh Sridhar**, Osbert Bastani, Edgar Dobriban, James Weimer, Insup Lee, Julia Parish-Morris, "[Exploring with Sticky Mittens: Reinforcement Learning with Expert Interventions via Option Templates](#)", Conference on Robot Learning (**CoRL**) 2022.
- 2022B **Kaustubh Sridhar**, Vikramank Singh\*, Murali Narayanaswamy\*, Abishek Sankararaman\*, "[Predict-and-Critic for Cloud Resource Allocation](#)", Under review at **AAAI 2023**. (\* AWS AI Labs)

### Robust Deep Learning

- 2022C **Kaustubh Sridhar**, Oleg Sokolsky, Insup Lee, James Weimer, "[Improving Neural Network Robustness via Persistency of Excitation](#)", American Control Conference (**ACC**) 2022.
- 2022D Ramneet Kaur, **Kaustubh Sridhar**, Sangdon Park, Susmit Jha\*, Anirban Roy\*, Oleg Sokolsky, Insup Lee, "[CODiT: Conformal Out-of-distribution Detection in Time-series Data](#)", Principles of Distribution Shift (PODS) Workshop at the International Conference of Machine Learning (**ICML**) 2022.

- 2021 Yiannis Kantaros, Taylor Carpenter, **Kaustubh Sridhar**, Yahan Yang, Insup Lee, James Weimer, "[Real-Time Detectors for Digital and Physical Adversarial Inputs to Perception Systems](#)", ACM/IEEE 12th International Conference on Cyber-Physical Systems (**ICCPS**) **2021**.
- 2022E **Kaustubh Sridhar**, Souradeep Dutta, Ramneet Kaur, Oleg Sokolsky, Insup Lee, "[Towards Alternative Techniques for Improving Adversarial Robustness: Analysis of Adversarial Training at a Spectrum of Perturbations](#)", arXiv:2206.06496.

#### Safety and Security of Autonomous Vehicles and Cyber-Physical Systems

- 2022F Mengyu Liu<sup>†</sup>, Lin Zhang<sup>†</sup>, Pengyuan Lu, **Kaustubh Sridhar**, Fanxin Kong<sup>†</sup>, Oleg Sokolsky, Insup Lee, "[Fail-Safe: Securing Cyber-Physical Systems against Hidden Sensor Attacks](#)", IEEE Real-Time Systems Symposium (**RTSS**) **2022**. (<sup>†</sup> Syracuse University)
- 2022G Pengyuan Lu, Mengyu Liu<sup>†</sup>, Lin Zhang<sup>†</sup>, **Kaustubh Sridhar**, Oleg Sokolsky, Fanxin Kong<sup>†</sup>, Insup Lee, "[Recovery from Adversarial Attacks in Cyber-physical Systems: Shallow, Deep and Exploratory Research](#)", Under Review at **ACM Computing Surveys**. (<sup>†</sup> Syracuse University)
- 2020 **Kaustubh Sridhar**, Radoslav Ivanov, Marcio Juliato<sup>†</sup>, Manoj Sastry<sup>†</sup>, Vuk Lesi<sup>†</sup>, Lily Yang<sup>†</sup>, James Weimer, Oleg Sokolsky, Insup Lee, "[A Framework for Checkpointing and Recovery of Hierarchical Cyber-Physical Systems](#)", arXiv:2205.08650 2020. (<sup>†</sup> Intel Labs)

#### Earlier Work in Quadrotor Control

- 2019 **Kaustubh Sridhar**, Srikant Sukumar, "[Finite-time, Event-triggered Tracking Control of Quadrotors](#)", Proceedings of the 5th CEAS Conference on Guidance, Navigation and Control (**EuroGNC**) **2019**.
- 2018 Hemjyoti Das, **Kaustubh Sridhar**, Radhakant Padhi, "[Bio-inspired Landing of Quadrotor using Improved State Estimation](#)", Proceedings of the 5th IFAC Conference on Advances in Control and Optimization Of Dynamical Systems (**ACODS**) **2018**.

### Awards

- 2022 **Outstanding Reviewer (top 10%)**, ICML 2022
- 2019 **The Dean's Fellowship and The Howard Bradwell Fellowship**, University of Pennsylvania
- 2018 **SN Bose Scholarship**, Govt. of India and the Indo-U.S. Science and Technology Forum
- 2015 **KVPY Fellowship**, Govt. of India

### Technical skills

Languages	Python, C, C++	Robotics	OpenCV, ROS, Gazebo, MATLAB
Machine Learning	Pytorch, Tensorflow, CUDA, Gym, Sklearn, Pandas		

### Key Coursework

Graduate	Principles of Deep Learning, Reinforcement Learning, Machine Learning, Convex Optimization, Data-driven IoT/Edge Computing, Linear Systems Theory, Advanced Probability, Computer Aided Verification
Undergraduate	Data Structures and Algorithms, Linear and Nonlinear Control Theory, Adaptive and Optimal Control

### Positions of Responsibility

- 2022 **Reviewer**, [NeurIPS](#), [ICML](#), [ICCPS](#)
- 2021, 2022 **Teaching Assistant**, University of Pennsylvania  
 Spring 2022: CIS 441/541: Embedded Software for Life-Critical Systems  
 Spring 2021: CIT 595: Computer Systems Programming.
- 2018 - 2019 **Head**, *Department Academic Mentorship Program*, IIT Bombay  
 - Led a team of 22 senior mentors to counsel 89 sophomores, 29 under-performing students.