4233 Chestnut Street, Unit 444
Philadelphia, PA, 19104
+1 267-290-7947
ksridhar@seas.upenn.edu

# Kaustubh Sridhar

## Education

2019 - Present **University of Pennsylvania**, *Philadelphia, PA.*
**PhD Candidate**, **Electrical and Systems Engineering**, GPA: 3.93/4.
ASSET and 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

My research is at the intersection of Machine Learning and Sequential Decision Making. Currently, I am excited by Deep Reinforcement Learning, Neurosymbolic Generative Models, Robust Deep Learning, and Autonomous Vehicle Safety and Security.

## Research Experience

Aug 2019 - Present **University of Pennsylvania**, *PhD Candidate*, Philadelphia, PA.
Advised by Prof. Insup Lee (ACM/IEEE Fellow), Prof. James Weimer.
Frequently collaborated with Prof. Dinesh Jayaraman, Prof. Edgar Dobriban, Prof. Osbert Bastani, Prof. Oleg Sokolsky, Prof. Fanxin Kong.
Highlights:
- Created a tool for guaranteed conformance of deep generative models to any constraints [12, gifs].
- Improved deep hierarchical RL sample-efficiency by two-orders-of-magnitude [11, videos].
- Working towards models that can learn and adapt instantaneously in online model-based RL [10].
- Enhanced adversarial robustness of NN's with guarantees [8].
- Developed conformal time-series OOD detectors [7] and real-time adversarial attack detectors [6].
- Composed sensor attacks and recovery algorithms for cyber-physical systems [5, 4, 3].

May - Aug 2022 **Amazon Web Services (AWS) AI Labs**, *Applied Scientist Intern*, Santa Clara, CA.
Collaborated with Dr. Murali Narayanaswamy, Dr. Abishek Sankararaman
Highlight: Accelerated datacenter resource allocation by combining model-based and model-free RL [9].

May - Aug 2021 **Argo AI (Ford & Volkswagen's Self-Driving Partner)**, *Research Intern*, Dearborn, MI.
Product Security and Sensor Functional Safety Team
Highlight: Built threat models for object detection and segmentation algorithms on autonomous vehicles.

May - Aug 2018 **Duke University**, *Summer Research Fellow*, Durham, NC.
Advised by Prof. Miroslav Pajic, Cyber-Physical Systems Lab
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 [2].

## Publications

**Neurosymbolic Generative Models**

12 **Kaustubh Sridhar**, Souradeep Dutta, James Weimer, Insup Lee, "Guaranteed Conformance of Neurosymbolic Models to Natural Constraints.",
➥ **ICLR 2023** workshop on Neurosymbolic Generative Models,
➥ Conference on Learning For Dynamics and Control (**L4DC**) **2023**,
➥ Invited talk at Johns Hopkins University.

**Deep Reinforcement Learning**

11 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**.

10 **Kaustubh Sridhar**, Souradeep Dutta, Dinesh Jayaraman, James Weimer, Insup Lee, "Deep Consistent Interpolation Between Prototypes Accelerates Model-Based Reinforcement Learning",
➥ In preparation for Neural Information Processing Systems (**NeurIPS**) **2023**.

9 **Kaustubh Sridhar**, Vikramank Singh[†], Murali Narayanaswamy[†], Abishek Sankararaman[†], "Predict-and-Critic: Accelerated End-to-End Predictive Control for Cloud Computing through Reinforcement Learning.", ([†]**Amazon AWS AI Labs**)
➥ In preparation for Neural Information Processing Systems (**NeurIPS**) **2023**.

**Robust Deep Learning**

8 **Kaustubh Sridhar**, Oleg Sokolsky, Insup Lee, James Weimer, "Improving Neural Network Robustness via Persistency of Excitation",
➥ American Control Conference (**ACC**) **2022**.

7 Ramneet Kaur, **Kaustubh Sridhar**, Sangdon Park, Susmit Jha[†], Anirban Roy[†], Oleg Sokolsky, Insup Lee, "CODiT: Conformal Out-of-distribution Detection in Time-series Data", ([†]SRI International)
➥ **ICML 2022** workshop on Principles of Distribution Shift,
➥ ACM/IEEE International Conference on Cyber-Physical Systems **(ICCPS) 2023**.
➥ Best paper award nomination at ICCPS 2023.

6 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 International Conference on Cyber-Physical Systems (**ICCPS**) **2021**.

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

5 Lin Zhang, **Kaustubh Sridhar**, Mengyu Liu, Pengyuan Lu, Fanxin Kong, Oleg Sokolsky, Insup Lee, "Real-Time Data-Predictive Attack-Recovery for Complex Cyber-Physical Systems",
➥ IEEE Real-Time and Embedded Technology and Applications Symposium (**RTAS**) **2023**.

4 Mengyu Liu, Lin Zhang, Pengyuan Lu, **Kaustubh Sridhar**, Fanxin Kong, Oleg Sokolsky, Insup Lee, "Fail-Safe: Securing Cyber-Physical Systems against Hidden Sensor Attacks",
➥ IEEE Real-Time Systems Symposium (**RTSS**) **2022**.

3 Pengyuan Lu, Mengyu Liu, Lin Zhang, **Kaustubh Sridhar**, Oleg Sokolsky, Fanxin Kong, Insup Lee, "Recovery from Adversarial Attacks in Cyber-physical Systems: Shallow, Deep and Exploratory Research",
➥ Under Review at **ACM Computing Surveys**.

**Earlier Work in Quadrotor Control**

2 **Kaustubh Sridhar**, Srikant Sukumar, "Finite-time, Event-triggered Tracking Control of Quadrotors",
➥ Conference on Guidance, Navigation and Control (**EuroGNC**) **2019**.

1 Hemjyoti Das, **Kaustubh Sridhar**, Radhakant Padhi, "Bio-inspired Landing of Quadrotor using Improved State Estimation",
➥ Conference on Advances in Control and Optimization Of Dynamical Systems (**ACODS**) **2018**.

## Awards

2023 **Best Paper Award Nomination** for CODiT [7] at ICCPS 2023

2022 **Top Reviewer (top 10%)**, NeurIPS 2022

2022 **Outstanding Reviewer (top 10%)**, ICML 2022

2023 **NSF Travel Grant**, ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS) 2023

2022 **Student Travel Grant**, American Control Conference 2022

2019 **The Dean's Fellowship**, University of Pennsylvania

2019 **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

## Other Projects

1 "Fixing Reward Hacking with Large Language Models."
- Created a framework for an RL agent in Deepmind AI Safety environments to leverage GPT4 to detect reward hacking, fix its own reward function, and learn to adapt quickly to the new reward function.

## Technical skills

Languages Python, C, C++ Robotics Mujoco, Bullet, CARLA, ROS, Gazebo

Machine Learning Pytorch, OpenAI Gym, Tensorflow, JAX, CUDA, Sklearn, Pandas

## Key Coursework

Graduate Deep Learning, Reinforcement Learning, Convex Optimization, Probability, Computer Aided Verification

Undergraduate Data Structures and Algorithms, Linear and Nonlinear Control Theory, Adaptive and Optimal Control

## Service

2022 - 2023 **Reviewer**
- Conferences: ICML 2022, 2023, NeurIPS 2022, L4DC 2023, ICCPS 2022
- Workshops: Neuro-Symbolic Generative Models (NeSy-GeMs) workshop at ICLR 2023

2018 - 2019 **Head**, *Department Academic Mentorship Program*, IIT Bombay
- Led a team of 22 senior mentors to counsel 89 sophomores, 29 under-performing students.

## Teaching Experience

Spring 2022 **Teaching Assistant**, *CIS 541: Embedded Software for Life-Critical Systems*, University of Pennsylvania

Spring 2021 **Teaching Assistant**, *CIT 595: Computer Systems Programming*, University of Pennsylvania