Kaustubh Sridhar

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

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

Reinforcement Learning (RL), Learning for Dynamics and Control (L4DC), and Robust Deep Learning.

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. Oleg Sokolsky, Prof. Osbert Bastani, Prof. Edgar Dobriban, Prof. Fanxin Kong, Prof. Mayur Naik.
Highlights:
- Created ENFORCER, a tool for guaranteed conformance of deep NN's to constraints [1, gifs]
- Improved deep RL sample-efficiency by two-orders-of-magnitude with option templates [2, videos].
- Enhanced adversarial robustness of NN's via persistent excitation [4], overdesigning [11].
- Developed conformal time-series OOD detectors [5] and real-time adversarial detectors [7].
- Composed sensor attacks and recovery algorithms for cyber-physical systems [6, 8, 12].

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 resource allocation in datacenters [3].

May - Aug 2021 **Argo AI (Ford & Volkswagen's Self-Driving Partner)**, *Research Intern*, Dearborn, MI.
Product Security and Sensor Functional Safety Team
Highlight: Threat models for object detection and tracking algorithms for Argo's 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 [9].

May - Aug 2017 **Indian Institute of Science Bangalore**, *Summer Research Fellow*, India.
Advised by Prof. Radhakant Padhi,
Highlight: Bio-inspired autonomous quadrotor landing algorithms [10].

Awards

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

Publications and Preprints

1 **Kaustubh Sridhar**, Souradeep Dutta, James Weimer, Insup Lee, "Guaranteed Conformance of Neurosymbolic Models to Natural Constraints.", Under Review at the Learning For Dynamics and Control (**L4DC**) Conference 2023.

2 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**.

3 **Kaustubh Sridhar**, Vikramank Singh†, Murali Narayanaswamy†, Abishek Sankararaman†, "Predict-and-Critic: Accelerated End-to-End Predictive Control for Cloud Computing through Reinforcement Learning.", Under review at the Learning For Dynamics and Control (L4DC) Conference 2023. (†AWS AI Labs)

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

5 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, International Conference of Machine Learning (**ICML**) **2022** (†SRI International).

7 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**.

6 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**. (↑Syracuse University)

8 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**. (↑Syracuse University)

9 **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**.

10 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**.

11 **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, 2022.

12 **Kaustubh Sridhar**, Radoslav Ivanov, Marcio Juliato†, Manoj Sastry†, Vuk Lesi†, Lily Yang†, James Weimer, Oleg Sokolsky, Insup Lee, "A Framework for Checkpointing and Recovery of Hierarchical Cyber-Physical Systems", arXiv:2205.08650, 2020. (†*Intel Labs*)

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, 2023 **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.