

# Kaustubh Sridhar

4233 Chestnut Street, Unit 444  
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.  
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

Deep Reinforcement Learning, Robust Deep Learning, Learning for Dynamics and Control, 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. 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 [3, videos].
  - Enhanced adversarial robustness of NN's via persistent excitation [4], overdesigning [12].
  - Developed conformal time-series OOD detectors [5] and real-time adversarial detectors [6].
  - Composed sensor attacks and recovery algorithms for cyber-physical systems [7, 8, 9].
- May - Aug 2022 **Amazon Web Services (AWS) AI Labs**, Applied Scientist Intern, Santa Clara, CA.  
Collaborated with [Dr. Murali Narayanaswamy](#), [Dr. Abishek Sankararaman](#)  
Highlight: Model-free RL augmentations for model-based resource allocation in datacenters [2].
- 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 [10].
- May - Aug 2017 **Indian Institute of Science Bangalore**, Summer Research Fellow, India.  
Advised by Prof. Radhakant Padhi,  
Highlight: Bio-inspired autonomous quadrotor landing algorithms [11].

## 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 Under Review

### Learning for Dynamics and Control

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

### Deep Reinforcement Learning

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

### Robust Deep Learning

- 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<sup>†</sup>, Anirban Roy<sup>†</sup>, Oleg Sokolsky, Insup Lee, "[CODiT: Conformal Out-of-distribution Detection in Time-series Data](#)", *International Conference of Machine Learning (ICML) Workshops* **2022**. Also, ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS) 2023 (<sup>†</sup>SRI International).
- 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

- 7 Lin Zhang<sup>†</sup>, **Kaustubh Sridhar**, Mengyu Liu<sup>†</sup>, Pengyuan Lu, Fanxin Kong<sup>†</sup>, 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**. (<sup>†</sup>Syracuse University)
- 8 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)
- 9 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)

### Earlier Work in Quadrotor Control

- 10 **Kaustubh Sridhar**, Srikanth Sukumar, "[Finite-time, Event-triggered Tracking Control of Quadrotors](#)", Proceedings of the 5th CEAS Conference on Guidance, Navigation and Control (**EuroGNC**) **2019**.
- 11 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**.

---

## 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**, [NeurIPS](#), [ICML](#), [L4DC](#), [ICCPS](#)
- 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