

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,
ASSET and **PRECISE** Center. GPA: 3.94/4.
- 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 and Imitation Learning, Neurosymbolic Generative Models, Robust Deep Learning

Awards

- 2023 **Best Paper Award Nomination** for CODiT [2022B] 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

Selected Preprints and Publications

Deep Reinforcement and Imitation Learning

- [2023C] **Kaustubh Sridhar,** Souradeep Dutta, Dinesh Jayaraman, Insup Lee, "Retrieval-Augmented Decision Transformer",
➡ In preparation for International Conference on Learning Representations (**ICLR**) 2024.
- [2023B] **Kaustubh Sridhar,** Souradeep Dutta, Dinesh Jayaraman, James Weimer, Insup Lee, "**Memory-Consistent Neural Networks for Imitation Learning**",
➡ Under review at Neural Information Processing Systems (**NeurIPS**) 2023.
- [2022D] **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**)
➡ Under review.
- [2022C] 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.

Neurosymbolic Generative Models

- [2023A] **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,

Robust Deep Learning

- [2022B] 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.

- [2022A] **Kaustubh Sridhar**, Oleg Sokolsky, Insup Lee, James Weimer, "[Improving Neural Network Robustness via Persistency of Excitation](#)",
 ➔ American Control Conference (**ACC**) 2022.
- [2021A] 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.

Research Experience

- Aug 2019 - Present **University of Pennsylvania**, *PhD Candidate*, Philadelphia, PA.
 Advised by [Prof. Insup Lee](#).
 Frequent collaborators: [Prof. Dinesh Jayaraman](#), [Prof. James Weimer](#), [Prof. Oleg Sokolsky](#)
- Improving generalization and transfer of decision transformers with retrieval [2023C].
 - Improved generalization in imitation learning with a novel semi-parametric model class [2023B].
 - Created a tool for guaranteed conformance of deep generative models to any constraints [2023A, [gifs](#)].
 - Boosted deep hierarchical RL sample-efficiency by two-orders-of-magnitude [2022C, [videos](#)].
 - Enhanced adversarial robustness of NN's with guarantees [2022A].
 - Developed conformal time-series OOD detectors [2022B], real-time adversarial attack detectors [2021A]
- May - Aug 2023 **Amazon Web Services (AWS) AI Labs**, *Applied Scientist Intern*, Santa Clara, CA.
 Collaborated with [Dr. Abishek Sankararaman](#), [Dr. Vikram Nathan](#), [Dr. Murali Narayanaswamy](#)
- Improved generalization in input-driven offline RL by incorporating transformer based forecasts in conservative Q learning.
- May - Aug 2022 **Amazon Web Services (AWS) AI Labs**, *Applied Scientist Intern*, Santa Clara, CA.
 Collaborated with [Dr. Abishek Sankararaman](#), [Dr. Murali Narayanaswamy](#)
- Accelerated datacenter resource allocation by combining model-free RL with mixed integer linear programs [2022D].
- May - Aug 2021 **Argo AI (Ford & Volkswagen's Self-Driving Partner)**, *Research Intern*, Dearborn, MI.
 Product Security and Sensor Functional Safety Team
- Built threat models for object detection and segmentation algorithms on autonomous vehicles.
- May - Aug 2018 **Duke University**, *Undergraduate Summer Research Fellow*, Durham, NC.
 Advised by [Prof. Miroslav Pajic](#), Cyber-Physical Systems Lab
- Developed 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](#),
- Bachelor's thesis on real-time quadrotor control.

Invited Talks

- 2023 **Guaranteed Conformance of Neurosymbolic Generative (Dynamics) Models to Physics and Medical Constraints**
- Johns Hopkins University (CISS Session on Learning for Optimization and Control)
 - Amazon Science (Deep Earth Reading Group)
 - University of Pennsylvania (Formal Methods and Machine Learning Reading Group)

Other Projects

- Apr - May 2023 "[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.

Service and Mentorship

- 2022 - Present **Reviewer**
- [ICML](#) 2023, 2022, [NeurIPS](#) 2023, 2022, [L4DC](#) 2023, [ICCPS](#) 2022
- 2020 - 2021 **Organizer**, *Reading Group in Robust Deep Learning*, University of Pennsylvania
- 2018 - 2019 **Team Lead**, *Department Academic Mentorship Program*, IIT Bombay
- Led a team of 22 senior mentors to counsel 89 sophomores, 29 under-performing students.

Technical skills

- Languages Python, C, C++
- Machine Learning Pytorch, OpenAI Gym, Tensorflow, JAX, CUDA, Sklearn, Pandas

Robotics Mujoco, Bullet, CARLA, ROS, Gazebo

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

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