Philadelphia, PA
+1 267-290-7947
ksridhar@seas.upenn.edu
kaustubhsridhar.github.io

Kaustubh Sridhar

Education

2019 - Present **University of Pennsylvania**, *Philadelphia, PA.*
PhD Candidate, **Electrical and Systems Engineering**, GPA: 3.94/4.
Thesis Committee: Prof Dinesh Jayaraman, Prof Insup Lee, Prof George Pappas, Prof Nikolai Matni | 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

I am interested in creating generalist agents that are highly adaptive and efficient, for both the digital and physical world. Towards this goal, I have worked on generative models, in-context learning, deep reinforcement and imitation learning, and robust deep learning. My recent work on a retrieval-augmented generalist agent directly aims for this goal.

Selected Publications and Preprints

[Preprint 2024B] REGENT: A Retrieval-Augmented Generalist Agent That Can Act In-Context In New Environments
Kaustubh Sridhar, Souradeep Dutta, Dinesh Jayaraman, Insup Lee
➥ Under review at the International Conference on Learning Representations (**ICLR**) **2025**
➥ **NeurIPS 2024** workshops on Adaptive Foundation Models and Open World Agents.

[Preprint 2024A] A Retrieval-Enhanced Mixed-Modal Foundation Model for Ophthalmology
Kaustubh Sridhar, Aditya Rangamani, Kuk Jang, Insup Lee
➥ In Preparation.

[2023B] Memory-Consistent Neural Networks for Imitation Learning
Kaustubh Sridhar, Souradeep Dutta, Dinesh Jayaraman, James Weimer, Insup Lee
➥ International Conference on Learning Representations (**ICLR**) **2024** (Acceptance rate: 31%).

[2023A] Guaranteed Conformance of Neurosymbolic (World) Models to Natural Constraints
Kaustubh Sridhar, Souradeep Dutta, James Weimer, Insup Lee
➥ **ICLR 2023** workshop on Neurosymbolic Generative Models,
➥ Conference on Learning For Dynamics and Control (**L4DC**) **2023**.

[2022D] Exploring with Sticky Mittens: Reinforcement Learning with Expert Interventions via Option Templates
S. Dutta*, **K. Sridhar***, O. Bastani, E. Dobriban, J. Weimer, I. Lee, J. Parish-Morris
➥ Conference on Robot Learning (**CoRL**) **2022** (Acceptance rate: 39%).

[Preprint 2022C] Predict-and-Critic: Accelerated End-to-End Predictive Control for Cloud Computing through Reinforcement Learning
Kaustubh Sridhar, Vikramank Singh†, Murali Narayanaswamy†, Abishek Sankararaman†
➥ Under review (†**Amazon AWS AI Labs**).

[2022B] CODiT: Conformal Out-of-distribution Detection in Time-series Data
Ramneet Kaur, **Kaustubh Sridhar**, Sangdon Park, Susmit Jha†, Anirban Roy†, Oleg Sokolsky, Insup Lee (†SRI International)
➥ **ICML 2022** workshop on Principles of Distribution Shift,
➥ International Conference on Cyber-Physical Systems **(ICCPS) 2023** (Acceptance: 25.6%).
➥ Best paper award nomination at ICCPS 2023.

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

[2021B] Real-Time Detectors for Digital and Physical Adversarial Inputs to Perception Systems
Yiannis Kantaros, Taylor Carpenter, **Kaustubh Sridhar**, Yahan Yang, Insup Lee, James Weimer
➥ International Conference on Cyber-Physical Systems (**ICCPS**) **2021** (Acceptance rate: 26%).

[2021A] Real-Time Data-Predictive Attack-Recovery for Complex Cyber-Physical Systems
Lin Zhang, **Kaustubh Sridhar**, Mengyu Liu, Pengyuan Lu, F. Kong, Oleg Sokolsky, Insup Lee
➥ IEEE Real-Time and Embedded Technology and Applications Symposium (**RTAS**).

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

Experience

Aug 2019 - Present **University of Pennsylvania**, *PhD Candidate*, Philadelphia, PA.
Advised by Prof Insup Lee.
Closely collaborated with Prof Dinesh Jayaraman, Prof James Weimer, Prof Oleg Sokolsky.

- Developed a generalist agent, without large models and vast datasets, that can generalize to new environments via retrieval-augmentation & in-context learning [Preprint 2024B, videos].
- Building a foundation model for ophthalmology trained on a synthetic mixed-modal dataset created from uni-modal vision-language datasets with retrieval [Preprint 2024A].
- Strengthened imitation learning with any neural network – diffusion models, transformers, or MLPs, via a novel semi-parametric model class called the MCNN [2023B, videos].
- Created a tool for guaranteed conformance of generative models to constraints [2023A, gifs].
- Boosted deep hierarchical RL sample-efficiency by two-orders-of-magnitude [2022D, videos].
- Enhanced adversarial robustness of NN's with guarantees [2022A].
- Developed out-of-distribution detectors with guarantees [2022B] that run in real-time [2021B].

May - Aug 2023 **Amazon Web Services (AWS) AI Labs**, *Applied Scientist Intern*, Santa Clara, CA.
Hosts: Dr. Abishek Sankararaman, Dr. Vikram Nathan, Dr. Murali Narayanaswamy

- Improved generalization in offline RL by incorporating transformer model based forecasts in conservative Q learning; applied to cloud resource allocation problems.

May - Aug 2022 **Amazon Web Services (AWS) AI Labs**, *Applied Scientist Intern*, Santa Clara, CA.
Hosts: Dr. Abishek Sankararaman, Dr. Murali Narayanaswamy

- Accelerated datacenter resource allocation by combining model-free RL with mixed integer linear programs [Preprint 2022C].

May - Aug 2021 **Argo AI (Ford & VW's Self-Driving Partner)**, *Systems 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 [2019].

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**, 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

Invited Talks

2023 **Learning Better Policies and Dynamics Models with Memory-Consistent and Memory-Constrained Neural Networks.**
- University of Pennsylvania (GRASP Lab) [video]

2023 **Memory-Consistent Neural Networks Boost Your Diffusion Policies, Behavior Transformers, and Behavior Cloning Agents.**
- University of Pennsylvania (Perception Action Learning Group)

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)

Press Coverage

2023 Making Better Decisions with AI, Penn Engineering Today (USA).

Service and Mentorship

2022 - Present **Reviewer**
ICLR 2025, 2024, ICML 2024, 2023, 2022, NeurIPS 2024, 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

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 adapt quickly to the new reward.

Teaching

Spring 22, Fall 24 **Teaching Assistant**, *CIS 541: Embedded Software for Life-Critical Systems*, UPenn

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