

Kaustubh Sridhar

4258 Chestnut Street, Unit 308
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: 3.86/4.
Advised by [Prof. James Weimer](#), [Prof. Oleg Sokolsky](#) and [Prof. Insup Lee](#), [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

Robust Deep Learning, Efficient Deep Reinforcement Learning, Safety and Security of Autonomous Vehicles, Cyber-Physical Systems.

Publications and Preprints

Robust Deep Learning

- 1 **Kaustubh Sridhar**, Oleg Sokolsky, Insup Lee, James Weimer, "[Improving Neural Network Robustness via Persistency of Excitation](#)", Proceedings of the American Control Conference (ACC) 2022
- 2 Yiannis Kantaros, Taylor Carpenter, **Kaustubh Sridhar**, Yahan Yang, Insup Lee, James Weimer, "[Real-Time Detectors for Digital and Physical Adversarial Inputs to Perception Systems](#)", Proceedings of the ACM/IEEE 12th International Conference on Cyber-Physical Systems (ICCPs) 2021
- 3 Ramneet Kaur, **Kaustubh Sridhar**, Sangdon Park, Susmit Jha*, Anirban Roy*, Oleg Sokolsky, Insup Lee, "[CODiT: Conformal Out-of-distribution Detection in Time-series Data](#)", Submitted to the International Joint Conference on Artificial Intelligence (IJCAI) 2022. (* SRI)

Efficient Deep Reinforcement Learning

- 4 Souradeep Dutta, **Kaustubh Sridhar**, Osbert Bastani, Edgar Dobriban, James Weimer, Insup Lee, Julia Parish-Morris, "[Reinforcement Learning with Expert Interventions via Option Templates](#)", Submitted to the International Conference on Machine Learning (ICML) 2022

Safety and Security of Autonomous Vehicles (AVs) and other Cyber-Physical Systems (CPS)

- 5 **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](#)", Preprint ([†] Intel Labs)

Earlier Work in Quadrotor Control

- 6 **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
- 7 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

Work and Research Experience

- May - Aug 2021 **Systems Engineer Intern, [Argo AI](#),** *Dearborn, MI.*
Product Security and Sensor Functional Safety Team
- Ensured continuous coverage of AVs to adversarial actors and adversarial objects in the environment by bridging Systems-Theoretic Process Analysis (STPA) from SOTIF (Safety Of The Intended Functionality, ISO 21448) with TARA (Threat Analysis and Risk Assessment, ISO 21434) procedure.
- Identified potential attack paths in each autonomy subsystem's security architecture and created threat models for object detection and tracking algorithms.
- Programmed verification and validation scripts for the onboard authentication and encryption protocols.
- Aug 2019 - **PhD Researcher, [PRECISE Center](#),** *Philadelphia, PA.*
Present Advised by [Prof. James Weimer](#), [Prof. Oleg Sokolsky](#), [Prof. Insup Lee](#).

Collaborated with [Prof. Fanxin Kong](#), [Prof. Osbert Bastani](#), [Prof. Edgar Dobriban](#), and Dr. Marcio Juliato, Dr. Manoj Sastry, Dr. Vuk Lesi, Dr. Lily Yang [[Intel Labs](#)].

- **Robust Deep Learning**

- Leveraged Persistency of Excitation from adaptive control to provably improve the adversarial robustness of state-of-the-art standard and adversarially trained deep neural networks on MNIST, CIFAR10, and CIFAR 100 datasets against projected gradient descent attack and autoattack. (Paper 1)
- Invented state-of-the-art real-time detectors for both digital and physical adversarial images based on label-invariant, feature smoothing transformations and KL divergence. (Paper 2)
- Devised out-of-distribution detectors for anomalous weather and motion events in AV video streams with temporally equivariant non-conformity measures. (Paper 3, In Progress)

- **Efficient Deep Reinforcement Learning**

- Pioneered order-of-magnitude speed improvements in long-horizon deep RL tasks like minecraft, robotic block stacking and google football with option templates, shortcuts that use expert-designed controllers to execute a potential option to understand the benefits of learning said option's policy. (Paper 4, In Progress)

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

- Designed a framework for sensor-anomaly resilient control of AVs via checkpointing and roll-forward recovery of states; proved attack-time recovery unlike an EKF on simulated ground robots. (Paper 5)
- Proposed MPC (Model-Predictive Control) based real-time recovery of nonlinear CPS facing sensor or actuator attacks within a dynamically estimated safety deadline computed with reachability techniques and aided by Taylor model flowpipe approximations. (Under Double-blind Review)

May - Aug 2018 **Summer Research Fellow**, [Cyber-Physical Systems Lab](#), Duke University, Durham NC.
Advised by [Prof. Miroslav Pajic](#), **Self-Driving Platform for Intrusion Detection testing**

- Created lane-keeping and cruise control algorithms for a 1/10th scale, Nvidia TX1 powered self-driving robot and proposed a novel intrusion detection system to tackle camera misinformation attacks.

2018 **Undergraduate Research Assistant**, Indian Institute of Technology Bombay, India.
Advised by [Prof. Srikant Sukumar](#), **Real-time Quadrotor Control**

- Formulated a novel finite-time, event-triggered control strategy for quadrotor attitude and position tracking with resource-constrained embedded hardware and validated via numerical simulations. (Paper 6)

Awards

2019 **The Dean's Fellowship and 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)

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, 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 **Reviewer**, [ICCPs](#), [ICML](#)

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.