Kaustubh Sridhar

4258 Chestnut Street, Unit 308
Philadelphia, PA, 19104
☎ *+1 267-290-7947*
✉ *ksridhar@seas.upenn.edu*

Education

2019 - Present **University of Pennsylvania**, *PA, USA.*
PhD Student, Electrical and Systems Engineering, *GPA: 3.86/4.*
Advised by Prof. Insup Lee[†,¶], Prof. Oleg Sokolsky[†] and Prof. James Weimer[†],
[†]*PRECISE Center, Computer and Information Science*, [¶]*Electrical and Systems Engineering*

2015 - 19 **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.

Achievements and Awards

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)

Research Interests

Autonomous Vehicle Safety and Security, Robust deep learning, Cyber-physical systems

Publications

1 **Sridhar, K.**, Ivanov, R.[†], Juliato, M.[‡], Sastry, M.[‡], Lesi, V.[‡], Yang, L.[‡], Weimer, J.[†], Sokolsky, O.[†], Lee, I.[†], "A Framework for Checkpointing and Recovery of Hierarchical Cyber-Physical Systems", Work In Progress ([‡] *Intel Labs*, [†] *PRECISE Center*) (↗)

2 Kantaros, Y.[†], Carpenter, T.[†], **Sridhar, K.**[†], Yang, Y.[†], Lee, I.[†], Weimer, J.[†], "Real-Time Detectors for Digital and Physical Adversarial Inputs to Perception Systems", Accepted at ICCPS '21 (↗)

3 **Sridhar, K.**, Sukumar, S., "Finite-time, Event-triggered Tracking Control of Quadrotors", Proceedings of the 5th CEAS Conference on Guidance, Navigation and Control (EuroGNC), Italy, 2019 (↗)

4 Das, H.[↑], **Sridhar, K.**[↑], Padhi, R., "Bio-inspired Landing of Quadrotor using Improved State Estimation", Proceedings of the 5th IFAC Conference on Advances in Control and Optimization Of Dynamical Systems, 2018 ([↑] *equal contribution*) (↗)

Doctoral Research

Title **Adversarially Robust Deep Learning**

Description - Tackling vulnerability of deep neural networks to adversarial samples via a novel control-theoretic approach of monitoring persistent excitation of neurons, adapting activation functions.
- Demonstrating SOTA robustness of persistently excited networks with Projected Gradient Descent, Carlini-Wagner adversaries on MNIST, CIFAR and Imagenet datasets.
- Invented real-time detectors for both digital and physical adversarial images based on label-invariant, feature smoothing transformations and KL divergence.

Title **Safety for Autonomous Vehicles with Sensor Anomalies** (In collaboration with **Intel Labs**)

Description - Designed framework for sensor-anomaly resilient control of cyber-physical systems (autonomous vehicles, medical devices, *etc.*) via checkpointing and roll-forward recovery of state-estimates.
- Proved better performance than EKF on numerical simulated autonomous ground robots. (↗)

Title **Scalable and Informed Data Programming**

Description - Improved scalability of Snorkel (tool for data programming,*i.e.* automatic labelling of unlabelled training data) with recursive clustering of dependent weak labellers.

Technical skills

Languages	C, C++, Python
Machine Learning	Pytorch, PySyft, Pandas, Tensorflow, Tensorflow-Federated, Sklearn, CUDA
Robotics	OpenCV, ROS, Gazebo, MATLAB, SolidWorks

Projects

Oct 2020 - Present **University of Pennsylvania,** Guided by Prof. Pratik Chaudhary in "Prin. of Deep Learning"
Batch Normalization's Effects on Transfer, Meta and Adversarially Robust Learning.
- Analyzing performance of DNNs trained with and without batch normalization layers on image classification tasks in transfer, meta and adversarially robust learning. (↗)

Mar - May 2020 **University of Pennsylvania** Guided by Prof. Rajeev Alur in "Computer Aided Verification"
Safety verification of self-driving robot with bounded reachability solver.
- Applied dReal (SMT solver) and dReach (symbolic reachability analyzer) tools in verifying safety requirements on simulation of an autonomous vehicle at an intersection.

Mar - May 2020 **University of Pennsylvania,** Guided by Prof. Insup Lee in "Data-driven IoT/Edge Comp."
Federated Learning for Internet of Medical Things.
- Developed patient-specific DNN models for predicting vital signs via asynchronous federated learning on simulated smart bed and vital signs monitors. (↗)

Nov - Dec 2019 **University of Pennsylvania,** Guided by Prof. Lyle Ungar in "Machine Learning"
Predicting Vehicle Pose with Deep Neural Networks.
- Constructed an ensemble CNN of EfficientNet, ResNet & DenseNet architectures for predicting pose of cars in images; ranked in top 10% in Baidu's Kaggle Challenge (↗)

Previous Research Experience

May - Jul 2018 **Duke University** Guided by Prof. Miroslav Pajic
Developed a Self-Driving Platform for Intrusion Detection testing.
- Created image processing & control algorithms for lane-keeping with GPU-enabled robot. (↗)
- Proposed novel IDS for camera misinformation attacks & transferred code to *Intel, Hillsboro*.

2018 **Indian Institute of Technology Bombay** Guided by Prof. Srikant Sukumar
Event Triggered Control for Quadrotors.
- Formulated a novel finite-time, event-triggered control strategy for quadrotor attitude and position tracking and validated via numerical simulations. (↗)

Backstepping Control of a Parrot AR Drone.
- Implemented a novel backstepping control strategy for automatically tracking a given trajectory with a Parrot AR Drone aided by a VICON Motion Capture system (↗)

May - Jul 2017 **Indian Institute of Science Bangalore** Guided by Prof. Radhakant Padhi
Navigation for Bio-inspired Autonomous Landing of Quadrotors.
- Estimated position (accurate to 5cm), orientation of Parrot AR Drone using Extended Kalman Filter fusion of monocular SLAM & IMU; Designed PID controller for autonomous landing (↗)

Coursework

Graduate	Principles of Deep Learning, Machine Learning, Convex Optimization, Data-driven IoT/Edge Computing, Linear Systems Theory, Elements of Probability, Computer Aided Verification
Undergraduate	Data Structures and Algorithms, Linear and Nonlinear Control Theory, Adaptive Control, Optimal Control, State Estimation, Modelling and Simulation, Navigation and Guidance

Positions of Responsibility

Jan - May 2021 Teaching Assistant, CIT 595: Computer Systems Programming
- Responsible for lectures on C/C++ and weekly recitations to class of 80 students.

2018 - 2019 Head, Department Academic Mentorship Program, IIT Bombay
- Led a team of 22 senior mentors to counsel 89 sophomores, 29 under-performing students