Bharathwaj Krishnaswami Sreedhar

ksbharathwaj17@gmail.com | ksb1712 | ksb1712.github.io | ksbharathwaj17

Education

MSc (Double-Degree) specializing in AI & Robotics — *Oct 2018 - Nov 2020*
KTH Royal Institute of Technology | Technische Universität Berlin — *Sweden & Germany*

B.Tech in Electrical and Electronics Engineering — *Aug 2014 - May 2018*
National Institute of Technology, Tiruchirappalli — *Trichy, India*

Skills

Programming Languages:	C, C++, Python, Java, Matlab
Frameworks and Tools:	TensorFlow, PyTorch, OpenCV, Scikit-learn, Dask, CUDA, DVC
Areas of Interest:	Deep learning, Reinforcement Learning, AI Safety, SLAM, Path Planning

Experience

neurocat GmbH — *Berlin, Germany*
Research Engineer - Robustness — *Feb,2021 - Present*

- Worked on analyzing robustness of perception models for railway systems as part of the Berlin digital rail operations project.
- Collaborated on a project with Fraunhofer AISEC and BSI Germany, focusing on state-of-art adversarial attacks and defences for medical data.
- Part of the core development team of *aidkit*, a ML quality assessment platform.
- Implemented various adversarial, corruption attacks and associated metrics in *aidkit*.
- Worked on developing a framework agnostic system for executing ML models.

Sony R&D | SL1 — *Stuttgart, Germany*
Master Thesis | AI Speech and Sound Group — *Feb,2020 - July,2020*

- Worked on Bayesian optimization for Neural Architecture Search (NAS)
- Implemented specialized graph kernels to identify optimal architecture using Gaussian modeling.
- Adapted Graph convolutional network as an embedding layer for best architecture search.
- Obtained results comparable to state-of-the-art on NASBench101 under hardware constraints via parallelization.
- Achieved over 100x improvement compared to random Search on NASBench-101.

National University of Singapore — *Singapore*
Summer Research Intern | OEIL - Medical Imaging — *May,2017 - Aug,2017*

- Worked under the supervision of Dr. Michael Girard and Dr. Alexandre Thiéry.
- Developed a custom CNN architecture for semantic segmentation.
- Separated seven layers of RNFL from monochrome OCT scans.
- Implemented an algorithm to detect and trace the contour of Bruch's membrane in a 3D volume scan.

Publications

Chapter 3 - "Security of AI-Systems: Fundamentals - Adversarial Deep Learning"
2022 Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany.

Deep Learning for Hardware-Constrained Driverless Cars
2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 2020

DRUNET: A Dilated-Residual U-Net Deep Learning Network To Segment ...
Biomedical Optics Express –Vol 9, Issue 7 (2018)