Malhar Jere

mjjere@eng.ucsd.edu | **217-530-7679 | malharj.github.io | US Citizen**

EDUCATION

University of California at San Diego **La Jolla, California**
Master of Science in Electrical and Computer Engineering December 2019
(starting employment in September 2020)

University of Illinois at Urbana-Champaign **Urbana-Champaign, Illinois**
B.S. in Electrical Engineering August 2013 – May 2017
Honors: *Dean's List (2 semesters)* | *Alumni Achievement Scholarship* | *University Achievement Scholarship*

SKILLS

Programming Languages/Software: Python, SQL, C/C++, MATLAB, x86, ARM assembly
Frameworks and Libraries: TensorFlow, Keras, PyTorch, MXNet, OpenCV, Numpy, scikit-learn, Pandas, Flask, AWS SageMaker
Concepts: Machine Learning, Deep Neural Networks, Computer Vision Systems, Embedded Systems, Deep Learning, Privacy

EXPERIENCE

Google X Development LLC **Mountain View, CA**
Incoming Machine Learning Resident Summer of 2020

Adaptive Computing and Embedded Systems Lab **La Jolla, CA**
Graduate Researcher **August 2018 - present**

- Published work on attacking GAN-based DeepFake detectors that got news coverage on TheNextWeb https://thenextweb.com/neural/2020/03/06/scientists-figured-out-how-to-fool-state-of-the-art-deepfake-detectors/
- Utilizing conditional GANs for privacy-preserving video anonymization
- Designed black-box adversarial attacks against ResNet-50, VGG-19, Inception-v3 Deep Neural Nets
- Published work at AAAI-20 on improving efficiency of detecting adversarial samples using linear transformations

Intuit **Mountain View, CA**
Data Scientist Intern | Machine Learning Privacy and Security Summer 2019

- Investigated Neural Network based techniques for privacy-preserving synthetic data generation
- Contributed to techniques for synthetic data generation using generative models
- Analysed synthetic data generation using differential privacy

The Climate Corporation **San Francisco**
Software Engineering Intern Summer 2017

- Designed, built and tested prototype from scratch for autonomous rover obstacle avoidance
- Reported on emerging trends in Agricultural Robotics for CTO at Agricultural Robotics Challenge

Motorola Solutions **Schaumburg, IL**
Software Engineering Intern Summer 2016

- Embedded RF applications in C++
- Implemented Automatic Gain Control (AGC) for Software Defined Radio platforms

PUBLICATIONS

1. P Neekhara, S Hussain, **M Jere**, F Koushanfar, J McAuley, "*Adversarial Deepfakes: Evaluating Vulnerability of Deepfake Detectors to Adversarial Examples*", ***https://arxiv.org/abs/2002.12749***
2. **M Jere**, S Herbig, C Lind, F Koushanfar, "*Principal Component Properties of Adversarial Samples*", AAAI-20 Workshop on Engineering Dependable and Secure Machine Learning Systems, New York, 2020
3. **M Jere**, B Hitaj, G Ciocarlie, F Koushanfar, "*Scratch that! An Evolution-based Adversarial Attack against Neural Networks*", ***https://arxiv.org/abs/1912.02316***