## kvgarimella@gmail.com www.kvgarimella.github.io Google Scholar GitHub

## Karthik Garimella

	Education
2020–Present	<ul> <li>PhD, New York University</li> <li>Electrical and Computer Engineering.</li> <li>GPA: 3.84/4</li> <li>Advisor: Brandon Reagen</li> <li>Multi-Party computation and homomorphic encryption for secure neural network inference</li> <li>Security and privacy of machine learning models</li> </ul>
2018–2020	<ul> <li>MSc, Washington University in St. Louis</li> <li>Computer Engineering.</li> <li>GPA: 3.78/4</li> <li>Advisor: Xuan Silvia Zhang</li> <li>Adversarial machine learning in autonomous vehicles</li> </ul>
2013–2017	<ul> <li>BA, Hendrix College</li> <li>Major Physics, Minor Computer Science.</li> <li>O GPA: 3.97/4</li> </ul>
	Experience
Summer 2019	<b>NASA Jet Propulsion Laboratory</b> . Software Intern with the Physical Oceanography Distributed Active Archive Center (DAAC)
- Fall 2017 Summer 2018	<b>Oak Ridge National Laboratory</b> . Scientific Software Developer for the Climate Change Science Institute and the ORNL DAAC
Summer 2017	<b>NASA Goddard Space Flight Center</b> . Data Science Intern with the Goddard Earth Sciences Data and Information Services Center
	Publications
	For a full list of publications, please refer to my Google Scholar Profile.
2023	Characterizing and Optimizing End-to-End Systems for Private Inference Architectural Support for Programming Languages and Operating Systems (ASPLOS) Karthik Garimella, Zahra Ghodsi, Nandan Kumar Jha, Siddharth Garg, Brandon Reagen (arxiv) (code)
2021	Cryptonite: Revealing the Pitfalls of End-to-End Private Inferece at Scale arXiv preprint Karthik Garimella, Nandan Kumar Jha, Zahra Ghodsi, Siddharth Garg, Brandon Reagen (arxiv)
2021	A Cautionary Tale of Using Low-Degree Polynomial Activations in Privacy-Preserving Deep Learning <i>ACM Conference on Computer and Communications Security (ACM CCS) PPML Workshop</i> <b>Karthik Garimella</b> , Nandan Kumar Jha, Brandon Reagen (arxiv) (code)
2021	F-LEMMA: Fast Learning-based Energy Management for Multi-/Many-core Processors IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD) An Zou, Yehan Ma, Karthik Garimella, Benjamin Lee, Christopher D. Gill, Xuan Zhang (ieeexplore)

2020	Attacking Vision-Based Perception in End-to-End Autonomous Driving Models Journal of Systems Architecture (JSA) Adith Boloor, <b>Karthik Garimella</b> , Xin He, Christopher Gill, Yevgeniy Vorobeychik, Xuan Zhang (arxiv) (code)
	Teaching
Fall 2023	<b>New York University</b> Head Teaching Assistant for Computing Systems Architecture (ECE-GY 6913).
Spring 2023	<b>New York University</b> , Head Teaching Assistant for Deep Learning (CS-GY 6953 / ECE-GY 7123).
Spring 2019	Washington University in St. Louis Tutor for Introduction to Machine Learning (CSE 417T).
2015 - 2016	Hendrix College Lead Teaching Assistant for General Physics I and II (PHYS 235/245).
	Talks
2023	MIT CSAIL Security Seminar Characterizing and Optimizing End-to-End Private Inference.
2023	<b>UC Berkeley</b> - <b>Raluca Ada Popa's Group</b> Characterizing and Optimizing End-to-End Private Inference.
2022	Applications Driving Architecture Characterizing and Optimizing End-to-End Private Inference.
2022	<b>TechCon</b> Characterization of End-to-End Private Inference at Scale.
2021	ACM CCS Privacy-Preserving Machine Learning Workshop A Cautionary Tale of Using Low-Degree Polynomial Activations in Privacy-Preserving Deep Learning.
2019	<b>Conference on Computer Vision and Pattern Recognition (CVPR) (invited)</b> CARLA Autonomous Driving Challenge - Third Place Presentation.
	Honors and Awards
2022	GAANN PhD Fellow – New York University, Department of Education
2020	Dean's PhD Fellowship – New York University
2019	Third Place at the CVPR 2019 Autonomous Driving Challenge
2013-2017	All-Tournament, All-Sportsmanship Team Honors, ITA Scholar, Captain - Hendrix College Varsity Tennis
	Skills
Languages	Python, C/C++, Rust, Go
Tools	PyTorch, Numpy, Matplotlib, LATEX, git, shell
Relevant	Probability, Machine Learning, Deep Learning, Bayesian Machine Learning, Computer Vision,

Coursework Algorithms, Programming Languages, Computer Architecture, OS, Cryptography