Last Updated on 2nd April 2023

Sanjay Kariyappa

https://sanjaykariyappa.github.io
sanjaykariyappa@gmail.com | 678.650.5017 | Mountain View, CA

SUMMARY

Sr. AI Research Associate at JP Morgan Chase, working on secure, privacy-preserving and explainable AI

EDUCATION

GEORGIA TECH

PHD IN ECE
Dec 2022 | Atlanta, GA
GPA: 4.0 / 4.0

GEORGIA TECH

MS IN ECE
Dec 2014 | Atlanta, GA
GPA: 4.0 / 4.0

SRI JAYACHAMARAJENDRA COLLEGE OF ENGINEERING

BS IN ECE
June 2013 | Mysore, India
GPA: 3.78 / 4.0

LINKS

Github:// **sanjaykariyappa**
LinkedIn:// **sanjay-kariyappa**
Twitter:// **@sanjayatwork**

RESEARCH INTERESTS

Machine learning, deep learning, privacy, security, federated learning, uncertainty estimation, semi-supervised learning, computer architecture, ML accelerators

COURSEWORK

Statistical Machine Learning
Digital Image Processing
Advanced Computer Architecture
ML Hardware Acceleration
Advanced Memory Systems

SKILLS

Programming Languages:
• Python • C • C++
• Matlab • Latex
Software Libraries:
Pytorch • Tensorflow • Keras
• Pandas • Numpy

PUBLICATIONS

MAZE: Data-Free Model Stealing Attack Using Zeroth-Order Gradient Estimation
[CVPR 2021] Sanjay Kariyappa, Atul Prakash, Moinuddin K Qureshi

Protecting DNNs from Theft using an Ensemble of Diverse Models
[ICLR 2021] Sanjay Kariyappa, Atul Prakash, Moinuddin K Qureshi

Defending Against Model Stealing Attacks with Adaptive Misinformation
[CVPR 2020] Sanjay Kariyappa, Moinuddin K Qureshi

ExPLoit: Extracting Private Labels in Split Learning
[SaTML 2023] Sanjay Kariyappa, Moinuddin K Qureshi

Measuring and Controlling Split Layer Privacy Leakage Using Fisher Information
[FL-NeurIPS 2022] Kiwan Maeng, Chuan Guo, Sanjay Kariyappa, Ed Suh

Cocktail Party Attack: Breaking Aggregation-Based Privacy in Federated Learning using Independent Component Analysis
[Under Submission] Sanjay Kariyappa, Chuan Guo, Kiwan Maeng, Wenjie Xiong, Ed Suh, Moinuddin K Qureshi, Hsien-Hsin S. Lee

Enabling Inference Privacy with Adaptive Noise Injection
[Under Submission] Sanjay Kariyappa, Ousmane Dia, Moinuddin K Qureshi

Semantics Preserving Adversarial Examples
[AML-CV workshop] Sanjay Kariyappa, Ousmane Dia

Improving Adversarial Robustness of Ensembles with Diversity Training
[Arxiv] Sanjay Kariyappa, Moinuddin K Qureshi

Tolerating Noise in PCM-Based AI Accelerators via Noise-Aware Training
[IEEE Transactions on Electron Devices 2021] S Kariyappa, H Tsai, K Spoon, S Ambrogio, P Narayanan, C Mackin, A Chen, MK Qureshi, GW Burr,

WORK EXPERIENCE

JP MORGAN CHASE | SR. AI RESEARCH ASSOCIATE

Feb 2023 – present | Palo Alto, CA

META | AI RESEARCH INTERN (FAIR)

May 2022 - Aug 2022 | Boston, MA

- Developed a novel attack on federated learning to break aggregation based privacy using independent component analysis. **(paper)**

FACEBOOK | SOFTWARE ENGINEERING INTERN

May 2021 - Aug 2021, May 2020 - Aug 2020 | Menlo Park, CA

- Explored the use of semi-supervised learning techniques to improve conversion prediction models for online advertising.

IBM | RESEARCH INTERN

May 2019 – Aug 2019 | San Jose, CA

- Developed Noise-Resilient DNNs that are robust against hardware noise for PCM-based analog AI hardware. **(paper)**

ORACLE | HARDWARE DEVELOPER

Jan 2015 – Aug 2017 | Santa Clara, CA