Jingtao Li

Objective: To embrace cutting-edge machine learning research & products

1249 E SPENCE
Tempe, AZ 85281
(480) 738-3855
jingtao1@asu.edu

EDUCATION

Arizona State University, Tempe — *P.h.D.* **(Aug. 2018 - Now)**

Expected Graduation: 2023 Summer

GPA:4.0/4.0

Research Interests: reliable/secure/private machine learning systems.

UESTC, Chengdu, China — *B.Eng.* **(Aug. 2014 - June 2018)**

Major: Electrical Engineering

GPA: 3.88/4.0 (Outstanding Student Award, 10 recipients annually)

PROJECTS

Reliable/Secure/Private DNN Research **(Aug. 2018 - Now)**

- Proposed a two-step resistance transfer framework called ResSFL to protect split federated learning schemes against model inversion attacks. (CVPR‘ 22)
- Proposed a full-stack obfuscation framework to prevent neural architecture stealing of DNN systems running on GPUs. (Host’ 21)
- Reduction of communication/computation overhead of split learning - a new private distributed DNN training scheme. (SIPS’ 21)
- Proposed a lightweight integrity checking method to detect and recover DNN weight corruption. (DATE’ 21)
- Proposed a weight-reconstruction-based DNN training scheme to mitigate fault injection attacks (DAC’ 20).

Parallel Algorithm Mapping **(Aug. 2019 - Now)**

- Full implementation of parallel versions of graph algorithms (BFS, CF, PageRank, SSSP and GCN) on a gem5-based super-scalar processor protocol.
- Optimize the speedup, energy efficiency with cache reconfigurability, synchronize-free implementation, graph partition and prefetcher techniques.

Split Federated Learning for Edge Devices **(Jan. 2022- May. 2022)**

- Implemented SFL framework on Arduino Nano BLE 33 and achieve >10% better accuracy on keyword spotting tasks compared to FL.

SKILLS

Python/C++

Pytorch/Tensorflow/TVM

Android Studio

Nvidia CUDA

Embedded Hardware

COURSES

Machine Learning	Deep Learning
Computer Vision	Reinforcement Learning
Algorithm	Mobile System Architecture
Embedded ML system	Computer Architecture

PUBLICATIONS

CVPR’ 22 [1st author]

HOST’ 21 [1st author]

SIPS’ 21 [2nd author]

DATE’ 21 [1st author]

DAC’ 20 [1st author]

SIPS’ 19 [1st author]

More on Google Scholar