Yanzhao Wu

266 Ferst Drive, Room 3337, Atlanta, Georgia, 30332, USA
yanzhaowu@gatech.edu • +1 (404) 279-2853 • http://yanzhaowu.me/

EDUCATION

Georgia Institute of Technology, Atlanta, Georgia, USA

- Ph.D. student in Computer Science — Aug 2017 – May 2022 (expected)
  - Area: **Systems** & **Machine Learning**
  - Focus: Big Data, Deep Learning, Systems
  - Cumulative GPA: 3.92 / 4.00

University of Science and Technology of China (USTC), Hefei, Anhui, China

- Bachelor of Computer Science and Technology — Sep 2013 – Jul 2017
  - Graduated with **Honors**.
  - Cumulative GPA: 3.80 / 4.30

RESEARCH EXPERIENCE

Data-efficient Learning with DNN Ensembles

- Smart Decisions Team, Facebook — May 2021 – Aug 2021
  - Mentor: Dr. Yin Huang
  - Focus: **Data Efficiency**, Ensemble Learning
  - Goal: Study the data efficiency of DNN ensemble models and design effective subsampling strategies to improve data efficiency for training ML models.

High-performance Object Detection on Edge Devices

- Distributed Data Intensive Systems Lab, Georgia Tech — Aug 2020 – May 2021
  - Supervisor: Prof. Ling Liu
  - Focus: Deep Learning, **Edge AI**
  - Goal: Design and implement an efficient framework for supporting various object detection models and achieving high performance on multiple edge devices.

Pipeline Parallelism for Deep Learning Recommendation Models

- AI System SW/HW Co-Design Team, **Facebook** — May 2020 – Aug 2020
  - Mentor: Dheevatsa Mudigere
  - Focus: Deep Learning, **Pipeline Parallelism**
  - Goal: Apply pipeline parallelism into Facebook deep learning recommendation models to accelerate distributed recommendation model training.
  - Achievement: **PipeDLRM** – an open-sourced software package built on top of DLRM and PyTorch.

High Accuracy and Robust Ensemble of Deep Neural Networks

- Distributed Data Intensive Systems Lab, Georgia Tech — Aug 2019 – May 2020
  - Supervisor: Prof. Ling Liu
  - Focus: Deep Learning, Ensemble Learning
  - Goal: Design and implement an ensemble framework for improving deep neural network accuracy and optimizing inference robustness.
  - Achievement: **EnsembleBench** – a holistic framework for promoting high diversity ensemble learning.

A Performance Study of Deep Learning with the High-performance Storage System

- Storage Systems Research Group, **IBM Research** — May 2019 – Jul 2019
  - Mentors: Dr. Daniel Waddington, Dr. Luna Xu
  - Focus: Storage Systems, Deep Learning Frameworks
  - Achievement: Conducting a comprehensive performance analysis of the high-performance storage system with different storage backends, such as **persistent memory** and SSD, with popular deep learning workloads.

Semi-automatic Hyper-parameter Tuning for Training Deep Neural Networks

- Distributed Data Intensive Systems Lab, Georgia Tech — Aug 2018 – May 2019
  - Supervisor: Prof. Ling Liu
  - Focus: Deep Learning, Hyper-parameter Tuning
  - Goal: Accelerate deep learning training and improve the training efficiency via semi-automatic hyper-parameter tuning.
  - Achievement: **LRBench** – a semi-automatic learning rate tuning tool to enhance the deep neural network training efficiency and accuracy.

Accelerating Deep Learning with Direct-to-GPU Storage

- Storage Systems Research Group, **IBM Research** — May 2018 – Aug 2018
  - Mentors: Amit Warke, Dr. Daniel Waddington
  - Focus: Storage Systems, Deep Learning Frameworks
  - Achievement: Integrating the Direct-to-GPU storage system into Caffe to obtain **over 2**× performance improvement by reducing the overhead of data transmission.

Experimental Analysis and Optimization of Deep Learning Frameworks

- Distributed Data Intensive Systems Lab, Georgia Tech — Aug 2017 – May 2018
  - Supervisor: Prof. Ling Liu
  - Focus: Deep Learning Frameworks, Performance Analysis
  - Goal: Analyze the hyper-parameters and basic components of Deep Learning and optimize Deep Learning Frameworks by tuning data-related and hardware-related parameters.
  - Achievement: **GTDLBench** – a performance benchmark of deep learning frameworks to measure and optimize mainstream deep learning frameworks.

PUBLICATION

- **Yanzhao Wu**, Ling Liu, Zhongwei Xie, Ka-Ho Chow, and Wenqi Wei. "Boosting Ensemble Accuracy by Revisiting Ensemble Diversity Metrics" (CVPR 2021)
- Wenqi Wei, Ling Liu, **Yanzhao Wu**, Gong Su, and Arun Iyenger. "Gradient-Leakage Resilient Federated Learning" (ICDCS 2021)
- Zhongwei Xie, Ling Liu, **Yanzhao Wu**, Lin Li, Luo Zhong. "Learning TFIDF Enhanced Joint Embedding for Recipe-Image Cross-Modal Retrieval Service" (IEEE TSC 2021)
- **Yanzhao Wu**, Ling Liu, Zhongwei Xie, Juhyun Bae, Ka-Ho Chow, Wenqi Wei. "Promoting High Diversity Ensemble Learning with EnsembleBench" (IEEE CogMI 2020)
- Zhongwei Xie, Ling Liu, **Yanzhao Wu**, Lin Li, Luo Zhong. "Cross-Modal Joint Embedding with Diverse Semantics" (IEEE CogMI 2020)
- Semih Sahin, Ling Liu, Wenqi Cao, Qi Zhang, Juhyun Bae, **Yanzhao Wu**. "Memory Abstraction and Optimization for Distributed Executors" (IEEE CIC 2020)
- Wenqi Wei, Ling Liu, Margaret Loper, Ka-Ho Chow, Mehmet Emre Gursoy, Stacey Truex, **Yanzhao Wu**. "Adversarial Deception in Deep Learning: Analysis and Mitigation" (IEEE TPS-ISA 2020)
- Ka-Ho Chow, Ling Liu, Margaret Loper, Juhyun Bae, Mehmet Emre Gursoy, Stacey Truex, Wenqi Wei, **Yanzhao Wu**. "Adversarial Objectness Gradient Attacks in Real-time Object Detection Systems" (IEEE TPS-ISA 2020)
- Juhyun Bae, Gong Su, Arun Iyengar, **Yanzhao Wu** and Ling Liu. "Efficient Orchestration of Host and Remote Shared Memory for Memory Intensive Workloads." (MemSys 2020)
- Ka-Ho Chow, Ling Liu, Emre Gursoy, Stacey Truex, Wenqi Wei and **Yanzhao Wu**, "Understanding Object Detection Through An Adversarial Lens." (ESORICS 2020)
- Wenqi Wei, Ling Liu, Margaret Loper, Ka Ho Chow, Mehmet Emre Gursoy, Stacey Truex and **Yanzhao Wu**, "A Framework for Evaluating Client Privacy Leakages in Federated Learning." (ESORICS 2020)
- Wenqi Wei, Ling Liu, Margaret Loper, Ka Ho Chow, Emre Gursoy, Stacey Truex, **Yanzhao Wu**. "Cross-layer Strategic Ensemble Defense against Adversarial Examples." (IEEE ICNC 2020)
- **Yanzhao Wu**, Ling Liu, Juhyun Bae, Ka-Ho Chow, Arun Iyengar, Calton Pu, Wenqi Wei, Lei Yu, Qi Zhang. "Demystifying Learning Rate Polices for High Accuracy Training of Deep Neural Networks." (IEEE BigData 2019)
- Ka-Ho Chow, Wenqi Wei, **Yanzhao Wu**, Ling Liu. "Denoising and Verification Cross-Layer Ensemble Against Black-box Adversarial Attacks." (IEEE BigData 2019)
- Ling Liu, Wenqi Wei, Ka-Ho Chow, Margaret Loper, Emre Gursoy, Stacey Truex, **Yanzhao Wu**. "Deep Neural Network Ensembles against Deception: Ensemble Diversity, Accuracy and Robustness" (IEEE MASS 2019)
- **Yanzhao Wu**, Ling Liu, Calton Pu, Wenqi Cao, Semih Sahin, Wenqi Wei, Qi Zhang. "A Comparative Measurement Study of Deep Learning as a Service Framework" (IEEE TSC 2019)
- Ling Liu, Wenqi Cao, Semih Sahin, Qi Zhang, Juhyun Bae, **Yanzhao Wu**. "Memory Disaggregation: Research Problems and Opportunities" (ICDCS 2019)
- **Yanzhao Wu**, Wenqi Cao, Semih Sahin, and Ling Liu. "Experimental Characterizations and Analysis of Deep Learning Frameworks" (IEEE BigData 2018)
- Ling Liu, **Yanzhao Wu**, Wenqi Wei, Wenqi Cao, Semih Sahin, and Qi Zhang. "Benchmarking Deep Learning Frameworks: Design Considerations, Metrics and Beyond." (ICDCS 2018)
- Pengcheng Wang, Jeffrey Svajlenko, **Yanzhao Wu**, Yun Xu and Chanchal K. Roy. "CCAligner: a token based large-gap clone detector" (ICSE 2018)

PEER REVIEW

- Conference: ICDE 2018, UCC 2018, BDCAT 2018, ICDCS 2019, WWW 2021
- Journal: IEEE TKDE, ACM TOIT