Dr. Yanzhao Wu

Assistant Professor at Florida International University
11200 SW 8TH ST, CASE 212D, Miami, FL 33199, USA
yawu@fiu.edu +1 404-279-2853 yanzhaowu.me

Education

Georgia Institute of Technology **Aug. 2017 – May 2022**
Ph.D. in Computer Science *Atlanta, GA, USA*

University of Science and Technology of China (USTC) **Sep. 2013 – Jul. 2017**
B.E. in Computer Science and Technology *Hefei, Anhui, China*

Research Interests

- Machine Learning Systems
- Large Language Models
- Edge AI Systems
- Deep Learning

Experience

Florida International University **Dec. 2022 – Present**
Assistant Professor in the Knight Foundation School of Computing and Information Sciences *Miami, FL*

Meta Platforms, Inc. **May 2022 – Dec. 2022**
Research Scientist in Ads Core ML *Menlo Park, CA*

- **Model and Feature Exploration:** Explore and advance machine learning techniques and applications to improve the overall efficiency and performance of large-scale Ads recommendation systems.

Georgia Institute of Technology **Aug. 2017 – May 2022**
Graduate Research/Teaching Assistant *Atlanta, GA*

- **High-performance Object Detection on Edge Devices:** Build an efficient framework for supporting various object detection/tracking models and achieving high performance on multiple edge devices.
- **High Accuracy and Robust Ensemble of Deep Neural Networks:** Design and implement an ensemble framework to improve deep neural network accuracy and optimize inference robustness on GPUs and edge devices.
- **Semi-automatic Hyperparameter Tuning for Deep Neural Networks:** Accelerate deep learning training and improve the training efficiency via semi-automatic hyper-parameter tuning.
- **Experimental Analysis and Optimization of Deep Learning Frameworks:** Analyze the hyper-parameters and core components of Deep Learning (DL) and optimize DL frameworks by tuning data and hardware related parameters.

Facebook, Inc. **Summer 2020, Summer 2021**
Software Engineer Intern *Menlo Park, CA*

- **Data-efficient Learning with DNN Ensembles:** Study the data efficiency of DNN ensemble models and design effective subsampling strategies to improve data efficiency for training ML models. (Summer 2021)
- **Pipeline Parallelism for Deep Learning Recommendation Models:** Apply pipeline parallelism into Facebook deep learning recommendation models to accelerate distributed recommendation model training. (Summer 2020)

IBM Research **Summer 2018, Summer 2019**
Research Intern *San Jose, CA*

- **A Performance Study of Deep Learning with the IBM High-performance Storage System:** Conduct a comprehensive performance analysis of the IBM Comanche storage system with different storage devices, such as persistent memory and SSD, on popular deep learning workloads. (Summer 2019)
- **Accelerating Deep Learning with Direct-to-GPU Storage:** Integrate the IBM Direct-to-GPU storage system into Caffe to obtain over 2× performance improvement by reducing the overhead of data transmission. (Summer 2018)

Publications

[1] *Security and Privacy Challenges of Large Language Models: A Survey*
Badhan Chandra Das*, M Hadi Amini, and **Yanzhao Wu**
ACM Computing Surveys

[2] *Effective Diversity Optimizations for High Accuracy Deep Ensembles*
Hongpeng Jin*, Maryam Akhavan Aghdam*, Sai Nath Chowdary Medikonduru*, Wenqi Wei, Xuyu Wang, Wenbin Zhang, and **Yanzhao Wu**
2024 IEEE International Conference on Cognitive Machine Intelligence (CogMI 2024)

[3] *Boosting Imperceptibility of Stable Diffusion-based Adversarial Examples Generation with Momentum*
Nashrah Haque, Xiang Li, Zhehui Chen, **Yanzhao Wu**, Lei Yu, Arun Iyengar, and Wenqi Wei
2024 IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS 2024)

[4] *Individual Fairness with Group Awareness Under Uncertainty*
Zichong Wang, Jocelyn Dzuong, Xiaoyong Yuan, Zhong Chen, **Yanzhao Wu**, Xin Yao, and Wenbin Zhang
2024 European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD 2024)

[5] *On the Efficiency of Privacy Attacks in Federated Learning*
Nawrin Tabassum*, Ka-Ho Chow, Xuyu Wang, Wenbin Zhang, and **Yanzhao Wu**
2024 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops - FedVision

[6] *Backdoor Attacks Against Low-Earth Orbit Satellite Fingerprinting*
Tianya Zhao, Ningning Wang, **Yanzhao Wu**, Wenbin Zhang, Xuyu Wang
2024 IEEE International Conference on Computer Communications Workshops - DeepWireless

[7] *ZipZap: Efficient Training of Language Models for Large-Scale Fraud Detection on Blockchain*
Sihao Hu, Tiansheng Huang, Ka-Ho Chow, Wenqi Wei, **Yanzhao Wu**, and Ling Liu
ACM Web Conference 2024

[8] *Adaptive Deep Neural Network Inference Optimization with EENet*
Fatih Ilhan, Ka-Ho Chow, Tiansheng Huang, Selim Tekin, Wenqi Wei, **Yanzhao Wu**, Myungjin Lee, Ramana Kompella, Hugo Latapie, Gaowen Liu, and Ling Liu
2024 IEEE/CVF Winter Conference on Applications of Computer Vision 2024 (WACV 2024)

[9] *Hierarchical Pruning of Deep Ensembles with Focal Diversity*
Yanzhao Wu, Ka-Ho Chow, Wenqi Wei, and Ling Liu
ACM Transactions on Intelligent Systems and Technology (TIST)

[10] *Demystifying Data Poisoning Attacks in Distributed Learning as a Service*
Wenqi Wei, Ka-Ho Chow, **Yanzhao Wu**, and Ling Liu
IEEE Transactions on Services Computing (TSC)

[11] *Privacy Risks Analysis and Mitigation in Federated Learning for Medical Images*
Badhan Chandra Das*, M. Hadi Amini, and **Yanzhao Wu**
2023 International Conference on Bioinformatics and Biomedicine (IEEE BIBM 2023)

[12] *Exploring Model Learning Heterogeneity for Boosting Ensemble Robustness*
Yanzhao Wu, Ka-Ho Chow, Wenqi Wei, and Ling Liu
23rd IEEE International Conference on Data Mining (IEEE ICDM 2023)

[13] *Model Cloaking against Gradient Leakage*
Wenqi Wei, Ka-Ho Chow, Fatih Ilhan, **Yanzhao Wu**, and Ling Liu
23rd IEEE International Conference on Data Mining (IEEE ICDM 2023)

[14] *Rethinking Learning Rate Tuning in the Era of Large Language Models*
Hongpeng Jin*, Wenqi Wei, Xuyu Wang, Wenbin Zhang, and **Yanzhao Wu**
2023 IEEE International Conference on Cognitive Machine Intelligence (CogMI 2023)

[15] *Amplifying Object Tracking Performance on Edge Devices*
Sanjana Vijay Ganesh, **Yanzhao Wu**, Gaowen Liu, Ramana Kompella, and Ling Liu
2023 IEEE International Conference on Cognitive Machine Intelligence (CogMI 2023)

[16] *Invisible Watermarking for Audio Generation Diffusion Models*
Xirong Cao, Xiang Li, Divyesh Jadav, **Yanzhao Wu**, Zhehui Chen, Chen Zeng, and Wenqi Wei
2023 IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS 2023)

[17] *STDLens: Model Hijacking-Resilient Federated Learning for Object Detection*
Ka-Ho Chow, Ling Liu, Wenqi Wei, Fatih Ilhan, and **Yanzhao Wu**
2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2023)

[18] *Securing Distributed SGD against Gradient Leakage Threats*
Wenqi Wei, Ling Liu, Jingya Zhou, Ka-Ho Chow, and **Yanzhao Wu**
IEEE Transactions on Parallel and Distributed Systems (TPDS)

[19] *Selecting and Composing Learning Rate Policies for Deep Neural Networks*
Yanzhao Wu and Ling Liu
ACM Transactions on Intelligent Systems and Technology (TIST)

[20] *Boosting Deep Ensemble Performance with Hierarchical Pruning*
Yanzhao Wu and Ling Liu
21st IEEE International Conference on Data Mining (ICDM 2021)

[21] *Transparent Network Memory Storage for Efficient Container Execution in Big Data Clouds*
Juhyun Bae, Ling Liu, Ka-Ho Chow, **Yanzhao Wu**, Gong Su, and Arun Iyengar
2021 IEEE International Conference on Big Data (IEEE BigData 2021)

[22] *Learning Text-Image Joint Embedding for Efficient Cross-Modal Retrieval with Deep Feature Engineering*
Zhongwei Xie, Ling Liu, **Yanzhao Wu**, Lin Li, and Luo Zhong
ACM Transactions on Information Systems (TOIS)

[23] *Parallel Detection for Efficient Video Analytics at the Edge*
Yanzhao Wu, Ling Liu, and Ramana Kompella
2021 IEEE International Conference on Cognitive Machine Intelligence (CogMI 2021)

[24] *RDMAbox: Optimizing RDMA for Memory Intensive Workload*
Juhyun Bae, Ling Liu, **Yanzhao Wu**, Gong Su, and Arun Iyengar
2021 International Conference on Collaborative Computing: Networking, Applications and Worksharing (CIC 2021)

[25] *Gradient-Leakage Resilient Federated Learning*
Wenqi Wei, Ling Liu, **Yanzhao Wu**, Gong Su, and Arun Iyenger
41st IEEE International Conference on Distributed Computing Systems (ICDCS 2021)

[26] *Boosting Ensemble Accuracy by Revisiting Ensemble Diversity Metrics*
Yanzhao Wu, Ling Liu, Zhongwei Xie, Ka-Ho Chow, and Wenqi Wei
2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2021)

[27] *Learning TFIDF Enhanced Joint Embedding for Recipe-Image Cross-Modal Retrieval Service*
Zhongwei Xie, Ling Liu, **Yanzhao Wu**, Lin Li, and Luo Zhong
IEEE Transactions on Services Computing (TSC)

[28] *Promoting High Diversity Ensemble Learning with EnsembleBench*
Yanzhao Wu, Ling Liu, Zhongwei Xie, Juhyun Bae, Ka-Ho Chow, and Wenqi Wei
2020 IEEE International Conference on Cognitive Machine Intelligence (CogMI 2020)

[29] *Cross-Modal Joint Embedding with Diverse Semantics*
Zhongwei Xie, Ling Liu, **Yanzhao Wu**, Lin Li, and Luo Zhong
2020 IEEE International Conference on Cognitive Machine Intelligence (CogMI 2020)

[30] *Memory Abstraction and Optimization for Distributed Executors*
Semih Sahin, Ling Liu, Wenqi Cao, Qi Zhang, Juhyun Bae, and **Yanzhao Wu**
2020 International Conference on Collaborative Computing: Networking, Applications and Worksharing (CIC 2020)

[31] *Adversarial Deception in Deep Learning: Analysis and Mitigation*
Wenqi Wei, Ling Liu, Margaret Loper, Ka-Ho Chow, Mehmet Emre Gursoy, Stacey Truex, and **Yanzhao Wu**
2020 IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS 2020)

[32] *Adversarial Objectness Gradient Attacks in Real-time Object Detection Systems*
Ka-Ho Chow, Ling Liu, Margaret Loper, Juhyun Bae, Mehmet Emre Gursoy, Stacey Truex, Wenqi Wei, and **Yanzhao Wu**
2020 IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS 2020)

[33] *Efficient Orchestration of Host and Remote Shared Memory for Memory Intensive Workloads*
Juhyun Bae, Gong Su, Arun Iyengar, **Yanzhao Wu**, and Ling Liu
2020 International Symposium on Memory Systems (MEMSYS 2020)

[34] *Understanding Object Detection Through An Adversarial Lens*
Ka-Ho Chow, Ling Liu, Mehmet Emre Gursoy, Stacey Truex, Wenqi Wei, and **Yanzhao Wu**
2020 European Symposium on Research in Computer Security (ESORICS 2020)

[35] *A Framework for Evaluating Client Privacy Leakages in Federated Learning*
Wenqi Wei, Ling Liu, Margaret Loper, Ka-Ho Chow, Mehmet Emre Gursoy, Stacey Truex, and **Yanzhao Wu**
2020 European Symposium on Research in Computer Security (ESORICS 2020)

[36] *Cross-layer Strategic Ensemble Defense against Adversarial Examples*
Wenqi Wei, Ling Liu, Margaret Loper, Ka Ho Chow, Emre Gursoy, Stacey Truex, and **Yanzhao Wu**
2020 International Conference on Computing, Networking and Communications (ICNC 2020)

[37] *Demystifying Learning Rate Policies for High Accuracy Training of Deep Neural Networks*
Yanzhao Wu, Ling Liu, Juhyun Bae, Ka-Ho Chow, Arun Iyengar, Calton Pu, Wenqi Wei, Lei Yu, and Qi Zhang
2019 IEEE International Conference on Big Data (IEEE BigData 2019)

[38] *Denoising and Verification Cross-Layer Ensemble Against Black-box Adversarial Attacks*
Ka-Ho Chow, Wenqi Wei, **Yanzhao Wu**, and Ling Liu
2019 IEEE International Conference on Big Data (IEEE BigData 2019)

[39] *Deep Neural Network Ensembles against Deception: Ensemble Diversity, Accuracy and Robustness*
Ling Liu, Wenqi Wei, Ka-Ho Chow, Margaret Loper, Emre Gursoy, Stacey Truex, and **Yanzhao Wu**
16th IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS 2019)

[40] *Memory Disaggregation: Research Problems and Opportunities*
Ling Liu, Wenqi Cao, Semih Sahin, Qi Zhang, Juhyun Bae, and **Yanzhao Wu**
39th IEEE International Conference on Distributed Computing Systems (ICDCS 2019)

[41] *Experimental Characterizations and Analysis of Deep Learning Frameworks*
Yanzhao Wu, Wenqi Cao, Semih Sahin, and Ling Liu
2018 IEEE International Conference on Big Data (IEEE BigData 2018)

[42] *Benchmarking Deep Learning Frameworks: Design Considerations, Metrics and Beyond*
Ling Liu, **Yanzhao Wu**, Wenqi Wei, Wenqi Cao, Semih Sahin, and Qi Zhang
38th IEEE International Conference on Distributed Computing Systems (ICDCS 2018)

[43] *A Comparative Measurement Study of Deep Learning as a Service Framework*
Yanzhao Wu, Ling Liu, Calton Pu, Wenqi Cao, Semih Sahin, Wenqi Wei, and Qi Zhang
IEEE Transactions on Services Computing (TSC)

[44] *CCAligner: A Token Based Large-Gap Clone Detector*
Pengcheng Wang, Jeffrey Svajlenko, **Yanzhao Wu**, Yun Xu, and Chanchal K. Roy
40th International Conference on Software Engineering (ICSE 2018)

* Students under my supervision.

Students

PhD Students

- Badhan Chandra Das (Co-advised with Prof. M. Hadi Amini, Spring 2023 - Present)
- Hongpeng Jin (Fall 2023 - Present)
- Maryam Akhavan Aghdam (Summer 2024 - Present)

Teaching

Florida International University

Assistant Professor

- CAP4630/CAP5602: Artificial Intelligence (Intro to AI) (Spring 2023)
- CAP5602: Introduction to Artificial Intelligence (Fall 2023)
- CAP4630: Artificial Intelligence (Spring 2024)
- CAP6619: Advanced Topics in Machine Learning (Fall 2024)
- CAP4630: Artificial Intelligence (Spring 2025)

Georgia Institute of Technology

Graduate Teaching Assistant

- CS6220 Big Data Systems and Analytics (Fall 2021)
- CS6675/CS4675 Advanced Internet Computing Systems and Application Development (Spring 2018, Spring 2019, Spring 2020, Spring 2021, Spring 2022)
- CS6235/CS4220 Embedded Systems and Real-Time Systems (Fall 2018)

Guest Lectures

- Deep Learning Hyperparameter Optimization with GTDLBench and LRBench (CS6220 in Fall 2019)
- Introduction to Emulab, Hadoop and Spark (CS6675/4675 in Spring 2019 and Spring 2020, CS6220 in Fall 2020)
- Introduction to Amazon AWS and Google Colab (CS6675/4675 in Spring 2021, CS6220 in Fall 2021)

University of Science and Technology of China

Undergraduate Teaching Assistant

- CS1001A Computer Programming A (Fall 2015)

Professional Activities

- Associate Editor: IEEE Transactions on Big Data
- Publicity Chair: IEEE CIC/CogMI/TPS 2024
- Program Committee: AAAI 2023, ICDCS 2023, IJCAI 2023, IEEE ISI 2023, AAAI 2024, SDM 2024, CCGRID 2024, IJCAI 2024, IJCAI 2025
- Conference Reviwer: ICDE 2018, UCC 2018, BDCAT 2018, ICDCS 2019, WWW 2021, CVPR 2022, ECCV 2022, CVPR 2023, KDD 2023, ICCV 2023, WACV 2024, WWW 2024, CVPR 2024, ECCV 2024
- Journal Reviwer: IEEE TKDE, IEEE TPAMI, IEEE TIFS, IEEE TSC, ACM TOIT, Journal of Information Security and Applications, Digital Communications and Networks, Computers & Security, Information Sciences, Knowledge-Based Systems, The Journal of Supercomputing, Neural Networks, Frontiers of Computer Science, Image and Vision Computing, e-Prime, Expert Systems with Applications, Future Generation Computer Systems, Journal of Network and Computer Applications, Image and Vision Computing, Computer Vision and Image Understanding, SoftwareX, Computers and Electrical Engineering, Journal of Industrial Information Integration, Artificial Intelligence in Medicine, Neurocomputing
- NSF Panelist

Awards

- FIU STEM Transformation Institute Faculty Fellow, 2023-2024
- IEEE CIC Best Paper Award, December 2021
- ICDM 2021 Student Attendance Award, December 2021
- College of Computing Student Travel Award, December 2020
- Qualified for Men's Singles in 2020 NCTTA South Regional Championships
- Outstanding Graduate Award (USTC), April 2017
- Fourth Place for 2016 ISC Student Cluster Competition, June 2016
- Excellent Student Scholarship (Top 3%, USTC), 2015-2016
- Leadership Scholarship, 2014-2015
- The Third Prize for Electromagnetism Paper Competition, June 2014