ZHUANGDI ZHU

Assistant Professor (Tenure-Track)
Department of Cyber Security Engineering
George Mason University
Fairfax, VA 22030

Phone: (517) 802-0847
Email: zzhu24@gmu.edu
Homepage: zhuangdizhu.github.io
Google Scholar Profile

EDUCATION

Michigan State University, USA
· Ph.D., Computer Science. *Jan 2017 - Aug 2022*

Australian National University, Australia
· Exchange Program, Computer Science. *July 2014 - Dec 2014*

Nanjing University of Science and Technology, China
· B.S., Computer Science. *Sept 2011 - Jun 2015*

RESEARCH INTERESTS

Zhuangdi's research interest focuses on principled *machine learning*. She aims to develop machine-learning techniques to address real-world needs. She has developed effective machine learning solutions for various applications, including wireless communication, cloud computing, algorithmic trading, human-computer interaction, internet of things, etc. Zhuangdi's strength also resides in integrated research, with her broader research intersected with *systems* and *wireless networking*.

PROFESSIONAL EXPERIENCE

Microsoft *Sep 2022 - Oct 2023*
Senior Data & Applied Scientist *Washington, United State*

· Developed end-to-end pipelines of knowledge extraction from Large Language Models; facilitate the creation of AI-powered search services;
· Built content recommendation services on Bing search for recreational segments, including movies, books, TV shows, and games.

Meta *Jun 2021 - Sep 2021*
PhD Intern, Machine Learning Track *California, United States*

· Designed and delivered production-level ads-ranking models that optimize towards long-term revenues following reinforcement learning principles;
· Online testing on Facebook's real traffic indicates that this prototype model has positive effects on users' long-term behavior.

Meta *Jun 2019 - Aug 2019*
PhD Intern, Mchine Learning Track *Washington, United States*

· Delivered online machine learning pipelines to fight against image abuse at Facebook Pages.
· Designed and built highly robust classifiers to detect unoriginal image posting in real-time.

Google *May 2018 - Aug 2018*
PhD Intern, Human Computer Interaction *California, United States*

· Designed a wearable platform to enable real-time gesture interactions;
· Implemented a multi-classification model with optical and motion sensor inputs that recognize user gestures in real-time.

PUBLICATIONS

CONFERENCE ARTICLES:

1. Zhuangdi Zhu, Junyuan Hong, Steve Drew, and Jiayu Zhou. Resilient and Communication Efficient Learning for Heterogeneous Federated Systems. *The 39th International Conference on Machine Learning* (**ICML 2022**).

2. Zhuangdi Zhu, Kaixiang Lin, Bo Dai, and Jiayu Zhou. Self Adaptive Imitation Learning: Learning Sparse Rewarded Tasks from Sub-Optimal Demonstrations. *The 36th AAAI Conference on Artificial Intelligence* (**AAAI 2022**).

3. Shuyang Yu*, Zhuangdi Zhu*[1], Boyang Liu, Anil Jain, and Jiayu Zhou. Robust Unsupervised Domain Adaptation from a Corrupted Source. *the 22nd IEEE International Conference on Data Mining* (**ICDM 2022**).

4. Zhuangdi Zhu, Junyuan Hong, and Jiayu Zhou. Data-Free Knowledge Distillation for Heterogeneous Federated Learning. *The 38th International Conference on Machine Learning* (**ICML 2021**).

5. Junyuan Hong, Zhuangdi Zhu, and Jiayu Zhou. Federated Adversarial Debiasing for Fair and Trasnferable Representations. *The 27th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (**KDD 2021**).

6. Zhuangdi Zhu, Kaixiang Lin, Bo Dai, and Jiayu Zhou. Off-Policy Imitation Learning from Observations. *The 34th Conference on Neural Information Processing Systems* (**NeurIPs 2020**).

7. Yushi Cheng, Xiaoyu Ji, Wenyuan, Hao Pan, Zhuangdi Zhu, Chuang-Wen You, Yi-Chao, and Lili Qiu. MagAttack: Guessing Application Launching and Operation via Smartphone. *The ACM Asia Conference on Computer and Communications Security* (**AsiaCCS 2019**).

8. Zhuangdi Zhu, Yi-Chao Chen, Fan Zhang, and Chuang-Wen You. MagAttack: Remote App Sensing with Your Phone. *The 18th ACM International Joint Conference on Pervasive and Ubiquitous Computing* (**UBICOMP 2016**).

JOURNAL ARTICLES:

1. Jiajun Wu, Steve Drew, Fan Dong, Zhuangdi Zhu, and Jiayu Zhou. Topology-aware federated learning in edge computing: A comprehensive survey. To appear on **ACM Computing Surveys**, 2024.

2. Zhuangdi Zhu, Kaixiang Lin, Anil K. Jain, and Jiayu Zhou. Transfer Learning in Deep Reinforcement Learning: A Survey. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, 2023.

3. Zhuangdi Zhu, Alex X. Liu, Fan Zhang, and Fei Chen. FPGA Resource Pooling in Cloud Computing. **IEEE Transactions on Cloud Computing**, 2019.

4. Zhangjie, Fu, Jiashuang Xu, Zhuangdi Zhu, Alex X. Liu, and Xingming Sun. Writing in the Air with WiFi Signals for Virtual Reality Devices. **IEEE Transactions on Mobile Computing**, 2019.

5. Zhao, Yangming, Chen Tian, Zhuangdi Zhu, Jie Cheng, Chunming Qiao, and Alex X. Liu Minimize the Make-span of Batched Requests for FPGA Pooling in Cloud Computing. **IEEE Transactions on Parallel and Distributed Systems**, 2018.

6. Xiaoyu J, Yushi C, Wenyuan X, Yuehan C, Hao P, Zhuangdi Zhu, Chuang-Wen You, Yi-Chao, and Lili Qiu. No Seeing is Also Believing: Electromagnetic-emission-based Application Guessing Attacks via Smartphones. **IEEE Transactions on Mobile Computing**, 2021.

[1] * Equal contribution.

PATENT:

- Philip Quinn and Zhuangdi Zhu. Sensing Hand Gestures Using Optical Sensors. US Patent App (16/243,767), 2020.

TEACHING

GMU CYSE 650: Introduction to Federated Learning *Spring 2024*

· Instructor for a graduate-level class about decentralized Artificial Intelligence.
· Designed lecture materials interplay between machine learning, IoT, and cyber security.

MSU CSE 847: Machine Learning *Spring 2020, Spring 2021*

· Volunteer teaching assistant for graduate-level machine learning class.
· Instructor for pre-exam Q & A lab sessions.
· Proposed lecture materials for CSE 847 advanced topics including *reinforcement learning* and *federated learning*.

MSU CSE 231: Introduction to Programming *Spring 2017, Spring 2018, Fall 2018*

· Instructor for weekly lab sessions to teach Python programming techniques.
· Tutor for weekly in-person Q & A sessions for hundreds of students.
· Designed take-home projects about Python data structures, including *Class* and *String*.

MSU CSE 260: Discrete Structures in Computer Science *Fall 2017*

· Teaching assistant for undergraduate-level classes; Served for grading, office-hours, and Q & A sessions.

TALKS & PRESENTATIONS

1. **SAIR 2023** Invited Talk: *Knowledge Distillation for Efficient Learning in Heterogeneous Federated Systems.*
2. **ICML 2022** Spotlight Presentation: *Resilient and Communication Efficient Learning for Heterogeneous Federated Systems.*
3. **AAAI 2022** Short Presentation: *Self Adaptive Imitation Learning: Learning Sparse Rewarded Tasks from Sub-Optimal Demonstrations.*
4. **ICML 2021** Poster Presentation: *Data-free knowledge Distillation for Heterogeneous Federated Learning.*
5. **NeurIPS 2020** Poster Presentation: *Off-Policy Imitation Learning from Observations.*

SERVICES

Organizer:

- International Joint Workshop on Federated Learning for Data Mining and Graph Analytics (**FedKDD**) Co-located with the 30th ACM SIGKDD Conference 2024
- International Workshop on Federated Learning for Distributed Data Mining (**FL4DataMining**) Co-located with the 29th ACM SIGKDD Conference 2023

Conference Reviewer:

- Conference on Neural Information Processing Systems (**NeurIPS**) 2021 - 2022

- International Conference on Machine Learning (**ICML**) 2021 - 2024
- AAAI Conference on Artificial Intelligence (**AAAI**) 2020 - 2023
- International Conference on Learning Representations (**ICLR**) 2022 - 2024
- ACM SIGKDD Conference on Knowledge Discovery and Data Mining (**KDD**) 2021 - 2022
- IEEE International Conference on Robotics and Automation (**ICRA**) 2022
- IEEE/RSJ International Conference on Intelligent Robots and Systems (**IROS**) 2022

Program Committee Member:

- AAAI Conference on Artificial Intelligence (**AAAI**) 2021 - 2023
- ACM SIGKDD Conference on Knowledge Discovery and Data Mining (**KDD**) 2022

Journal Reviewer:

- NeuroComputing 2020 - 2022
- Information Sciences 2021 - 2022
- Neural Networks 2021 - 2022
- Patterns 2022
- IEEE Network Magazine 2021 - 2022
- IEEE Journal of Automatica Sinica 2022
- IEEE Robotics and Automation Letters 2021 -2022