

JIAYUN ZHANG

✉ jiz069@ucsd.edu  [jiayunz.github.io](https://github.com/jiayunz)  [Google Scholar](https://scholar.google.com/citations?user=jiz069)  github.com/jiayunz

EDUCATION

University of California San Diego

Ph.D. Program in Computer Science and Engineering

Advisor: Prof. Rajesh K. Gupta and Prof. Jingbo Shang

Research Interests: Federated Learning, Data-Efficient ML

La Jolla, CA, U.S.A

Sep 2020 - June 2025 (expected)

Fudan University

B.S. in Computer Science (with honors)

Shanghai, China

Sep 2015 - Jun 2020

PUBLICATIONS

Conference and Journal Papers

- Xiyuan Zhang, Xiaohan Fu, Diyan Teng, Chengyu Dong, Keerthivasan Vijayakumar, **Jiayun Zhang**, Ranak Roy Chowdhury, Junsheng Han, Dezhi Hong, Rashmi Kulkarni, Jingbo Shang and Rajesh K. Gupta “Physics-Informed Data Denoising for Real-Life Sensing Systems.” *ACM Conference on Embedded Networked Sensor Systems (SenSys’23)* [pdf]
- Xiyuan Zhang, Ranak Roy Chowdhury, **Jiayun Zhang**, Dezhi Hong, Rajesh K. Gupta, Jingbo Shang “Unleashing the Power of Shared Label Structures for Human Activity Recognition.” *32nd ACM International Conference on Information and Knowledge Management (CIKM’23)* [pdf]
- **Jiayun Zhang**, Xiyuan Zhang, Xinyang Zhang, Dezhi Hong, Rajesh K. Gupta, Jingbo Shang. “Navigating Alignment for Non-identical Client Class Sets: A Label Name-Anchored Federated Learning Framework.” *29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD’23)* [pdf]
- **Jiayun Zhang**, Xinyang Zhang, Dezhi Hong, Rajesh K. Gupta, and Jingbo Shang. “Minimally Supervised Contextual Inference from Human Mobility: An Iterative Collaborative Distillation Framework.” *32nd International Joint Conferences on Artificial Intelligence. (IJCAI’23)* [pdf]
- Qingyuan Gong, Yushan Liu, **Jiayun Zhang**, Yang Chen, Qi Li, Yu Xiao, Xin Wang, Pan Hui. “Detecting Malicious Accounts in Online Developer Communities Using Deep Learning.” *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 2023. [pdf]
- Huiying Li, Shawn Shan, Emily Wenger, **Jiayun Zhang**, Haitao Zheng, Ben Y. Zhao. “Blacklight: Defending Black-Box Adversarial Attacks on Deep Neural Networks.” *31st USENIX Security Symposium (USENIX Security’22)* [pdf]
- Yihan Ma, Hua Sun, Yang Chen, **Jiayun Zhang**, Yang Xu, Xin Wang, Pan Hui. “DeepPredict: A Zone Preference Prediction System for Online Lodging Platforms.” *Journal of Social Computing*, 2021, 2(1):52-70. [pdf]
- **Jiayun Zhang**, Yang Chen, Qingyuan Gong, Aaron Yi Ding, Yu Xiao, Xin Wang, Pan Hui. “Understanding the Working Time of Developers in IT Companies in China and the United States.” *IEEE Software*, 2021, 38(2):96-106. [pdf]
- Erzheng Fu, Yingqiu Zhuang, Jianxi Zhang, **Jiayun Zhang**, Yang Chen. “Understanding the User Interactions on GitHub: A Social Network Perspective.” *24th IEEE International Conference on Computer Supported Cooperative Work in Design (CSCWD’21)* [pdf]
- Shawn Shan, Emily Wenger, **Jiayun Zhang**, Huiying Li, Haitao Zheng, Ben Y. Zhao. “Fawkes: Protecting Personal Privacy against Unauthorized Deep Learning Models.” *29th USENIX Security Symposium (USENIX Security’20)* [pdf]
- Qingyuan Gong, **Jiayun Zhang**, Yang Chen, Qi Li, Yu Xiao, Xin Wang, Pan Hui. “Detecting Malicious Accounts in Online Developer Communities Using Deep Learning.” *28th ACM International Conference on Information and Knowledge Management (CIKM’19)* [pdf]

Workshop Papers and Posters

- **Jiayun Zhang**, Xinyang Zhang, Dezhi Hong, Rajesh K. Gupta, and Jingbo Shang. “DEMOMOTIF: Demographic Inference from Sparse Records of Shopping Transactions based on Motif Patterns.” *3rd International Workshop on Machine Learning on Graphs (MLOG with WSDM’23)* [pdf]

- **Jiayun Zhang**, Petr Byvshev, Yu Xiao. “Dataset: A video dataset of a wooden box assembly process.” *3rd Workshop on Data Acquisition to Analysis (DATA with SenSys’20)* [pdf]
- Qingyuan Gong, **Jiayun Zhang**, Xin Wang, Yang Chen. “Identifying Structural Hole Spanners in Online Social Networks Using Machine Learning.” *ACM SIGCOMM 2019, Poster Session (SIGCOMM’19)* [pdf]

SELECTED RESEARCH PROJECTS

Federated Learning with Statistical and System Heterogeneity

Jan 2022 – Now

co-advised by Prof. Rajesh K. Gupta and Prof. Jingbo Shang, UC San Diego

- **FL with Non-identical Client Class Sets (KDD’23)**
 - Identified a new non-IID scenario where clients annotate local data based on their own class sets and learn a global model that works for the union of the classes.
 - Designed FedAlign, a framework that leverages natural language class names to align clients’ feature spaces.
- **FL with Heterogeneous Model Architectures (In submission)**
 - Designed an FL framework based on graph hypernetwork that works for heterogeneous network architectures to fit in different running capacities and supports personalization.

Data-Efficient Machine Learning

Sep 2020 – Now

co-advised by Prof. Rajesh K. Gupta and Prof. Jingbo Shang, UC San Diego

- **Minimally-Supervised Contextual Inference from Human Mobility (IJCAI’23)**
 - Designed STColab, a collaborative distillation framework that iteratively distills knowledge between spatial and temporal information and enhances contextual inference when only limited labels are available.
- **Demographic Inference from Sparse Shopping Transactions (MLoG Workshop@WSDM’23)**
 - Proposed a network embedding method based on motif (i.e., subgraph) patterns.
 - Designed a motif context selection algorithm based on graph propagation on a user-motif bipartite graph for selecting label-indicative transaction contexts for representation learning.

Security and Privacy on Deep Neural Networks

Jan 2020 – Mar 2020

co-advised by Prof. Ben Y. Zhao and Prof. Haitao Zheng, University of Chicago

- **Protecting Personal Privacy against Unauthorized DL Models (USENIX Security’20)**
 - Collaborated in building Fawkes, a system that allows individuals to inoculate themselves against unauthorized facial recognition models by adding imperceptible pixel-level changes to their photos.

INDUSTRIAL EXPERIENCE

VMware

Shanghai, China

MTS (Member of Technical Staff) Intern

Apr 2018 – Oct 2018

- Developed a log analysis system for automatically detecting the causes of program failures. 67 types of error causes were detected with an accuracy of 0.936 on real-time data from an internal bug reporting platform.
- Developed web APIs for an internal cloud resource platform to support the use of virtual machine templates.

PROFESSIONAL SERVICES

- Program Committee Member / Reviewer: WWW, SDM, AAAI, KDD, UbiComp.
- Journal Reviewer: Computer Communications.

SELECTED AWARDS

KDD Student Travel Award	2023
Chun-Tsung Scholar (Research Program Funded by Nobel Laureate Dr. Tsung-Dao Lee)	2020
Outstanding Graduate of Fudan University	2020
1st Prize of Shanghai Open Data Innovation Research Competition (top 1 among 65 teams)	2019
Best Student Award, Mobile Systems and Networking Group at Fudan University (1 out of 32)	2019

Last Update on November 20, 2023