JIAYUN ZHANG

jiz069@ucsd.edu jiayunz.github.io Google Scholar github.com/jiayunz

EDUCATION

University of California, San Diego — La Jolla, CA
Ph.D. Candidate in Computer Science — Sep 2020 - June 2025 (expected)

- Advisors: Prof. Rajesh Gupta and Prof. Jingbo Shang
- Research Interests: machine learning, data mining, federated learning, internet of things

Fudan University — Shanghai, China
B.S. in Computer Science (with honors) — Sep 2015 - Jun 2020

SELECTED RESEARCH PROJECTS

Privacy-Preserving Distributed Learning in Heterogeneous Edge Computing Environments — Jan 2022 – Now

- **Federated Learning with Heterogeneous Models** (WWW'24) [code][video]
  Tech Stack: neural architecture search, knowledge distillation
  – Explored resource-skew environments where few powerful devices collaborate with many lower-capacity devices.
  – Designed a graph hypernetwork-based aggregation by modeling computational graphs, enabling reciprocal knowledge exchange for heterogeneous model architectures to fit varying device capacities.
  – Evaluated across image and language tasks with various model architectures (CNN families, Adapter Transformers fine-tuning, etc.); improved accuracy by 3.6% and 8.7% on strong and weak devices respectively.
- **Federated Learning with Non-identical Client Class Sets** (KDD'23) [paper][code][video]
  Tech Stack: language modeling, knowledge distillation
  – Studied a non-IID scenario where clients annotate local data based on their own (different or even non-overlapping) class sets and learn a global model that works for the union of the classes.
  – Proposed FedAlign, a framework that models natural language class names to anchor class representations and align client feature spaces; improved accuracy by 9.6% across six tasks (language and IoT classification).

Machine Learning with Data Scarcity — Sep 2020 – Now

- **Minimally-Supervised Contextual Inference from Human Mobility** (IJCAI'23) [paper]
  Tech Stack: semi-supervised learning, time-series
  – Studied contextual inference (e.g., demographics) when only limited labels (e.g., 10 per class) are available.
  – Proposed STColab, a collaborative distillation framework that iteratively distills knowledge between spatial and temporal information and collaboratively enhances inference performance.
- **Demographic Inference from Sparse Shopping Transactions** (MLoG Workshop at WSDM'23) [paper]
  Tech Stack: graph mining, representation learning
  – Studied demographic inference based on households' shopping transactions where each household has a limited number of transactions. Proposed a graph embedding method based on motif (i.e., subgraph) patterns.
  – Designed a context selection algorithm through propagation over 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

- **Protecting Personal Privacy against Unauthorized DL Models** (USENIX Security'22) [paper][code][website]
  Tech Stack: facial recognition, adversarial training
  – 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.

INTERNSHIP EXPERIENCE

VMware — Shanghai, China
MTS (Member of Technical Staff) Intern — Apr 2018 – Oct 2018

- Developed an LSTM-based 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 the cloud resource platform to support the use of virtual machine templates.
- Worked on Template Validation Service for security verification of virtual machine templates uploaded to database.

SELECTED PUBLICATIONS

- **J. Zhang**, S. Li, H. Huang, Z. Wang, X. Fu, D. Hong, R. K. Gupta, J. Shang. "How Few Davids Improve One Goliath: Federated Learning in Resource-Skewed Edge Computing Environments." WWW, 2024.
- **J. Zhang**, X. Zhang, X. Zhang, D. Hong, R. K. Gupta, J. Shang. "Navigating Alignment for Non-identical Client Class Sets: A Label Name-Anchored Federated Learning Framework." KDD, 2023. [pdf]
- **J. Zhang**, X. Zhang, D. Hong, R. K. Gupta, J. Shang. "Minimally Supervised Contextual Inference from Human Mobility: An Iterative Collaborative Distillation Framework." IJCAI, 2023. [pdf]
- **J. Zhang**, X. Zhang, D. Hong, R. K. Gupta, J. Shang. "DEMOMOTIF: Demographic Inference from Sparse Records of Shopping Transactions based on Motif Patterns." Workshop on Machine Learning on Graphs at WSDM 2023. [pdf]
- X. Zhang, R. R. Chowdhury, **J. Zhang**, D. Hong, R. K. Gupta, J. Shang. "Unleashing the Power of Shared Label Structures for Human Activity Recognition." CIKM, 2023. [pdf]
- X. Zhang, X. Fu, D. Teng, C. Dong, K. Vijayakumar, **J. Zhang**, R. R. Chowdhury, J. Han, D. Hong, R. Kulkarni, J. Shang, R. K. Gupta. "Physics-Informed Data Denoising for Real-Life Sensing Systems." SenSys, 2023. [pdf]
- Q. Gong, Y. Liu, **J. Zhang**, Y. Chen, Q. Li, Y. Xiao, X. Wang, P. Hui. "Detecting Malicious Accounts in Online Developer Communities Using Deep Learning." TKDE, 2023. [pdf]
- H. Li, S. Shan, E. Wenger, **J. Zhang**, H. Zheng, B.Y. Zhao. "Blacklight: Defending Black-Box Adversarial Attacks on Deep Neural Networks." USENIX Security, 2022. [pdf]
- **J. Zhang**, Y. Chen, Q. Gong, A.Y. Ding, Y. Xiao, X. Wang, P. Hui. "Understanding the Working Time of Developers in IT Companies in China and the United States." IEEE Software, 2021, 38(2):96-106. [pdf]
- **J. Zhang**, P. Byvshev, Y. Xiao. "Dataset: A video dataset of a wooden box assembly process." Workshop on Data Acquisition to Analysis with SenSys, 2020. [pdf]
- S. Shan, E. Wenger, **J. Zhang**, H. Li, H. Zheng, B.Y. Zhao. "Fawkes: Protecting Personal Privacy against Unauthorized Deep Learning Models." USENIX Security, 2020. [pdf]
- Q. Gong, **J. Zhang**, Y. Chen, Q. Li, Y. Xiao, X. Wang, P. Hui. "Detecting Malicious Accounts in Online Developer Communities Using Deep Learning." CIKM, 2019. [pdf]
- Q. Gong, **J. Zhang**, X. Wang, Y. Chen. "Identifying Structural Hole Spanners in Online Social Networks Using Machine Learning." SIGCOMM Poster, 2019. [pdf]

PROFESSIONAL SERVICES

- Program Committee Member / Reviewer: WWW'24, SDM'24, AAAI'23/24, KDD'23, UbiComp'23.
- 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
Xiyuan Scholar (Undergraduate Research Program at Fudan University)	2018
Scholarship for Outstanding Students, Fudan University	2016 & 2018 & 2019

SKILLS

Programming: Python, C/C++, C#, Matlab, Shell, HTML/CSS, Ruby...
Machine Learning: PyTorch, Keras, Tensorflow, Scikit-Learn...
Other: MySQL, PostgreSQL, Django, Bootstrap, Unity, Blender, Git, LaTex...