Yue Zhao

CONTACT Information	yue.z@usc.edu pithub.com/yzhao062	213-821-2369 CS Department, GCS Hall		
	in linkedin.com/in/yzhao062 thttps://viterbi-web.usc.edu/~yzhao010/ IN USC Faculty Directory	Los Angeles, CA United States, 90089 Department of Computer Science		
	G Google Scholar	University of Southern California		
RESEARCH SUMMARY	My research builds reliable , robust , and scalable AI that advances science and benefits society. I focus on rigorous algorithmic foundations, safety for large models and agents, high-impact applications, and open, reproducible systems.			
	1. Reliable AI Foundations: Detecting the Unexpected I develop fundamental algorithms and benchmarks for detecting rare, unseen, or abnormal patterns across modalities. This line unifies anomaly detection, out-of-distribution (OOD) detection, and automated model selection to ensure that AI systems remain predictable under uncertainty.			
	□ Anomaly & OOD Detection□ Automated Model Selection□ Robust Learning	□ Benchmarks & Evaluation□ Multimodal & Graph Settings□ Data Efficiency		
	2. Trust & Safety in Large Language Models and Agents I study how to make large models and agentic systems reliable under real-world conditions, focusing on hallucination mitigation, privacy and security safeguards, jailbreak prevention, model-extraction defenses, and dynamic evaluation of reasoning.			
	□ LLM Safety & Reliability□ Hallucination Mitigation□ Jailbreak Detection	□ Privacy & Model Extraction□ Trust/Stress Evaluation□ Routing & Online Control		
	3. Foundation Models for Science & Society I apply foundation models and generative AI to high-stakes domains, combining domain knowledge with reliable modeling to support scientific discovery and decision-making.			
	□ AI for Science□ Generative/Foundational Models□ Decision Modeling	□ Climate/Weather & Extreme Events□ Healthcare & Biomedicine□ Political & Social Systems		
	4. Scalable, Automated & Open AI Systems I create efficient, reproducible ML systems that operationalize the above ideas at scale. Open-source tools include PyOD (30M+ downloads) and related libraries with 20K+ GitHub stars. My work emphasizes distributed inference, automated workflows, and user-centric design to democratize reliable AI.			
	□ ML Systems & Tooling□ Automated ML & Workflows□ Open-source AI	 □ Distributed/Agentic Inference □ Reproducibility & Evaluation □ Accessibility & Adoption 		
FULL-TIME PROFESSIONAL EXPERIENCE	University of Southern California Thomas Lord Department of Computer Science Assistant Professor (Tenure-Track) • Foundations Of Robust Trustworthy Intelligent	Aug. 2023 - Present Systems (FORTIS) Lab: Link		
	• USC Machine Learning Center (MaSCle): Link			
	PwC Canada Consulting & Deals Senior Consultant (Data Scientist)	Aug. 2017 - Jun. 2019		

EDUCATION

Carnegie Mellon University

Pittsburgh, PA

Ph.D. in Information Systems and Management

Sep. 2019 - May. 2023

- Affiliation: CMU automated learning systems group (Catalyst) and Data Analytics Techniques Algorithms (DATA) Lab
- Advisors and Mentors: CMU: Prof. Leman Akoglu, Prof. Zhihao Jia, and Prof. George Chen. I collaborate with Prof. Jure Leskovec at Stanford, and Prof. Philip S. Yu at UIC.

University of Toronto

Toronto, ON

Master of Science in Computer Science

Sep. 2015 - Dec. 2016

University of Cincinnati

Cincinnati, OH

Bachelor of Science in Computer Engineering

Sep. 2010 - May. 2015

Minor: Computer Science and Mathematics

Awards,

As Principal Investigator (August 2023 onwards)

Grants, and Funding

NSF POSE I	Funding	Aug. 2025
Capital One Research Awards	Grant	Oct. 2024
Amazon Research Awards	Gift	Aug. 2024
Best Paper Award @ KDD Resource-Efficient Learning Workshop	Recognition	Aug. 2024
NSF ATD	Funding	Aug. 2024
NSF POSE II	Funding	Jun. 2024
Google Cloud Research Innovators	Recognition	Mar. 2024
AAAI New Faculty Highlights	Recognition	Feb. 2024

Note: Monetary values represent my portion of the funding. Total project budgets may be larger.

Prior to Principal Investigator Role (Before August 2023)

Meta 2022 AI4AI Research Award (student co-PI)	Recognition	Oct. 2022
The Norton Labs Graduate Fellowship	Fellowship	Mar. 2022
CMU Presidential Fellowship	Fellowship	2019
Mitacs-Accelerate Research and Development Funding	Funding	2016-2017
University Global Award and Scholarship	Scholarship	2010 - 2015
Mantei/Mae Award & Scholar	Award	2012 - 2015
Engineer of the Month	Recognition	Jun. 2014

Note: Monetary values are omitted for awards and recognitions received prior to PI role.

PUBLICATIONS

Preprints & Under Submission



Note: *first authors and †corresponding authors if more than one.

- 81. Yuexing Hao, Yue Huang, Haoran Zhang, Chenyang Zhao, Zhenwen Liang, Paul Pu Liang, <u>Yue Zhao, Lichao Sun, Saleh Kalantari, Xiangliang Zhang, Marzyeh Ghassemi</u>
 - The Role of Computing Resources in Publishing Foundation Model Research

Under submission

arXiv preprint arXiv:2510.13621

80. Wang Wei, Tiankai Yang, Hongjie Chen, <u>Yue Zhao</u>, Franck Dernoncourt, Ryan A. Rossi, Hoda Eldardiry Learning to Route LLMs from Bandit Feedback: One Policy, Many Trade-offs

Under submission

- arXiv preprint arXiv:2510.07429
- 79. Langzhou He, Junyou Zhu, Fangxin Wang, Junhua Liu, Haoyan Xu, <u>Yue Zhao</u>, Philip S. Yu, Qitian Wu Can Molecular Foundation Models Know What They Don't Know? A Simple Remedy with Preference Optimization

Under submission

arXiv preprint arXiv:2509.25509

78. Yuehan Qin, Li Li, Defu Cao, Tiankai Yang, Yue Zhao

M3OOD: Automatic Selection of Multimodal OOD Detectors

Under submission

arXiv preprint arXiv:2508.11936

77. Yuangang Li, Yiqing Shen, Yi Nian, Jiechao Gao, Ziyi Wang, Chenxiao Yu, Shawn Li, Jie Wang, Xiyang Hu, Yue Zhao

Mitigating Hallucinations in Large Language Models via Causal Reasoning

Under submission

arXiv preprint arXiv:2508.12495

76. Bolin Shen, Eren Erman Ozguven, <u>Yue Zhao</u>, Guang Wang, Yiqun Xie, Yushun Dong Learning from the Storm: A Multivariate Machine Learning Approach to Predicting Hurricane-Induced Economic Losses

Under submission

arXiv preprint arXiv:2506.17964

75. Li Li, Peilin Cai, Ryan A. Rossi, Franck Dernoncourt, Branislav Kveton, Junda Wu, Tong Yu, Lixin Song, Tiankai Yang, Yuehan Qin, Nesreen K. Ahmed, Samyadeep Basu, Subhojyoti Mukherjee, Ruiyi Zhang, Yuxiao Zhou, Zichao Wang, Yue Huang, Yu Wang, Xiangliang Zhang, Philip S. Yu, Xiyang Hu, Yue Zhao

A Personalized Conversational Benchmark: Towards Simulating Personalized Conversations

Under submission

arXiv preprint arXiv:2505.14106

74. Zixiang Xu, Yanbo Wang, Yue Huang, Jiayi Ye, Haomin Zhuang, Zirui Song, Lang Gao, Chenxi Wang, Zhaorun Chen, Yujun Zhou, Sixian Li, Wang Pan, <u>Yue Zhao</u>, Jieyu Zhao, Xiangliang Zhang, Xiuying Chen

SocialMaze: A Benchmark for Evaluating Social Reasoning in Large Language Models

Under submission

arXiv preprint arXiv:2505.23713

73. Tiankai Yang, Junjun Liu, Wingchun Siu, Jiahang Wang, Zhuangzhuang Qian, Chanjuan Song, Cheng Cheng, Xiyang Hu, Yue Zhao

AD-AGENT: A Multi-agent Framework for End-to-end Anomaly Detection

Under submission

arXiv preprint arXiv:2505.12594

72. Haoyan Xu, Zhengtao Yao, Xuzhi Zhang, Ziyi Wang, Langzhou He, Yushun Dong, Philip S. Yu, Mengyuan Li, Yue Zhao

GLIP-OOD: Zero-Shot Graph OOD Detection with Foundation Model

Under submission

arXiv preprint arXiv:2504.21186

71. Haoyan Xu, Zhengtao Yao, Ziyi Wang, Zhan Cheng, Xiyang Hu, Mengyuan Li, <u>Yue Zhao</u> Graph Synthetic Out-of-Distribution Exposure with Large Language Models

Under submission

arXiv preprint arXiv:2504.21198

70. Weidi Luo, Qiming Zhang, Tianyu Lu, Xiaogeng Liu, Yue Zhao, Zhen Xiang, Chaowei Xiao Doxing via the Lens: Revealing Privacy Leakage in Image Geolocation for Agentic Multi-Modal Large Reasoning Model

Under submission

arXiv preprint arXiv:2504.19373

69. Yuehan Qin, Shawn Li, Yi Nian, Xinyan Velocity Yu, <u>Yue Zhao</u>[†], Xuezhe Ma[†] Don't Let It Hallucinate: Premise Verification via Retrieval-Augmented Logical Reasoning **Under submission**

arXiv preprint arXiv:2504.06438

68. Yiming Tang, Yi Fan, Chenxiao Yu, Tiankai Yang, <u>Yue Zhao</u>, Xiang Hu StealthRank: LLM Ranking Manipulation via Stealthy Prompt Optimization **Under submission**

arXiv preprint arXiv:2504.05804

67. Chengxuan Qian, Shuo Xing, Shawn Li, <u>Yue Zhao</u>, Zhengzhong Tu
DecAlign: Hierarchical Cross-Modal Alignment for Decoupled Multimodal Representation Learning
Under submission
arXiv preprint arXiv:2503.11892

6 Vingging Vy Hagran Wang Vugging Liang Philip

66. Xiongxiao Xu, Haoran Wang, Yueqing Liang, Philip S. Yu, <u>Yue Zhao</u>, Kai Shu Can Multimodal LLMs Perform Time Series Anomaly Detection? **Under submission**

arXiv preprint arXiv:2502.17812

65. Kaixiang Zhao, Lincan Li, Kaize Ding, Neil Zhenqiang Gong, <u>Yue Zhao</u>, Yushun Dong A Survey of Model Extraction Attacks and Defenses in Distributed Computing Environments **Under submission**arXiv preprint arXiv:2502.16065

64. Yue Huang, Chujie Gao, Siyuan Wu, Haoran Wang, Xiangqi Wang, Yujun Zhou, Yanbo Wang, Jiayi Ye, Jiawen Shi, Qihui Zhang, Yuan Li, Han Bao, Zhaoyi Liu, Tianrui Guan, Dongping Chen, Ruoxi Chen, other authors, <u>Yue Zhao</u>, other authors, Xiangliang Zhang

On the Trustworthiness of Generative Foundation Models: Guideline, Assessment, and Perspective Under submission

arXiv preprint arXiv:2502.14296

https://trustgen.github.io/

63. Shixuan Li, Wei Yang, Peiyu Zhang, Xiongye Xiao, Defu Cao, Yuehan Qin, Xiaole Zhang, <u>Yue Zhao,</u> Paul Bogdan

Climate LLM: Efficient Weather Forecasting via Frequency-Aware Large Language Models ${\bf Under\ submission}$

arXiv preprint arXiv:2502.11059

62. Lincan Li, Jiaqi Li, Catherine Chen[†], Fred Gui[†], other collaborators, <u>Yue Zhao</u>[†], Yushun Dong[†] Political-LLM: Large Language Models in Political Science

Under submission

arXiv preprint arXiv:2412.06864

61. Chenxiao Yu, Jinyi Ye, Yuangang Li, Zhaotian Weng, Zheng Li, Emilio Ferrara, Xiyang Hu[†], <u>Yue Zhao</u>[†] A Large-Scale Simulation on Large Language Models for Decision-Making in Political Science Under submission

arXiv preprint arXiv:2412.15291

60. Junda Wu, Hanjia Lyu, Yu Xia, Zhehao Zhang, Joe Barrow, Ishita Kumar, Mehnoosh Mirtahebi, Hongjie Chen, Ryan A. Rossi, Franck Dernoncourt, Tong Yu, Ruiyi Zhang, Jiuxiang Gu, Nesreen K. Ahmed, Yu Wang, Xiang Chen, Hanieh Deilamsalehy, Namyong Park, Sungchul Kim, Huanrui Yang, Subrata Mitra, Zhengmian Hu, Nedim Lipka, Yue Zhao, Jiebo Luo, Julian McAuley Personalized Multimodal Large Language Models: A Survey

Under submission

arXiv preprint arXiv:2412.02142

59. Han Bao, Yue Huang, Yanbo Wang, Jiayi Ye, Xiangqi Wang, Xiuying Chen, <u>Yue Zhao</u>, Tianyi Zhou, Mohamed Elhoseiny, Xiangliang Zhang

AutoDavis: Automatic and Dynamic Evaluation Protocol of Large Vision-Language Models on Visual Question-Answering?

ICML 2025 DataWorld Workshop arXiv preprint arXiv:2410.21259

Peer-reviewed Journal Papers

- 58. Haoyan Xu, Kay Liu, Zhengtao Yao, Philip S. Yu, Kaize Ding[†], <u>Yue Zhao</u>[†] LEGO-Learn: Label-Efficient Graph Open-Set Learning *Transactions on Machine Learning Research (TMLR)*, 2025
- 57. Hao Dong, Gaetan Frusque, <u>Yue Zhao</u>, Eleni Chatzi, Olga Fink NNG-Mix: Improving Semi-supervised Anomaly Detection with Pseudo-anomaly Generation *IEEE Transactions on Neural Networks and Learning Systems (TNNLS)*, 2024
- 56. Ling Yang*, Zhilong Zhang*, Yang Song, Shenda Hong, Runsheng Xu, <u>Yue Zhao</u>, Wentao Zhang, Bin Cui, Ming-Hsuan Yang

Diffusion Models: A Comprehensive Survey of Methods and Applications ACM Computing Surveys (CSUR), 2023 (*equal contribution)

55. <u>Yue Zhao*</u>, Martin Q. Ma*, Xiaorong Zhang, Leman Akoglu
The Need for Unsupervised Outlier Model Selection: A Review and Evaluation of Internal Evaluation
Strategies

ACM SIGKDD Explorations Newsletter (SIGKDD Explor.), 2023 (*equal contribution)

54. Kexin Huang*, Tianfan Fu*, Wenhao Gao*, <u>Yue Zhao</u>, Yusuf Roohani, Jure Leskovec, Connor W. Coley, Cao Xiao, Jimeng Sun, Marinka Zitnik Artificial Intelligence Foundation for Therapeutic Science Nature Chemical Biology (NCHEMB), 2022 (*equal contribution)

53. <u>Yue Zhao*</u>, Zheng Li*, Xiyang Hu, Nicola Botta, Cezar Ionescu, George H. Chen ECOD: Unsupervised Outlier Detection Using Empirical Cumulative Distribution Functions *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 2022. (*equal contribution)

 Yue Zhao, Zain Nasrullah, Zheng Li PyOD: A Python Toolbox for Scalable Outlier Detection Journal of Machine Learning Research (JMLR), 2019.

Conference & Workshop Papers

- 51. Yanbo Wang, Zixiang Xu, Yue Huang, Xiangqi Wang, Zirui Song, Lang Gao, Chenxi Wang, Xiangru Tang, Yue Zhao, Arman Cohan, Xiangliang Zhang, Xiuying Chen DyFlow: Dynamic Workflow Framework for Agentic Reasoning Advances in Neural Information Processing Systems (NeurIPS), 2025
- 50. Shawn Li, Jiashu Qu, Yuxiao Zhou, Yuehan Qin, Tiankai Yang, <u>Yue Zhao</u> Treble Counterfactual VLMs: A Causal Approach to Hallucination *Findings of the Association for Computational Linguistics: EMNLP*, 2025.
- Yuangang Li, Jiaqi Li, Zhuo Xiao, Tiankai Yang, Yi Nian, Xiyang Hu, <u>Yue Zhao</u> NLP-ADBench: NLP Anomaly Detection Benchmark *Findings* of the Association for Computational Linguistics: *EMNLP*, 2025.
- 48. Lincan Li, Eren Erman Ozguven, <u>Yue Zhao</u>, Guang Wang, Yiqun Xie, Yushun Dong TyphoFormer: Language-Augmented Transformer for Accurate Typhoon Track Forecasting *ACM International Conference on Advances in Geographic Information Systems (SIGSPATIAL*), 2025.
- 47. Yi Nian*, Shenzhe Zhu*, Yuehan Qin, Shawn Li, Ziyi Wang, Chaowei Xiao, <u>Yue Zhao</u> JailDAM: Jailbreak Detection with Adaptive Memory for Vision-Language Model Conference on Language Modeling (COLM), 2025.
- 46. Shawn Li, Peilin Cai, Yuxiao Zhou, Zhiyu Ni, Renjie Liang, You Qin, Yi Nian, Zhengzhong Tu, Xiyang Hu, Yue Zhao Secure On-Device Video OOD Detection Without Backpropagation International Conference on Computer Vision (ICCV), 2025.
- 45. Zerui Xu, Fang Wu, Yue Zhao Retrieval-Reasoning Large Language Model-based Synthetic Clinical Trial Generation ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD Workshop on AI Agent for Information Retrieval), 2025. ACM Conference on Bioinformatics, Computational Biology, and Health Informatics (ACM BCB, 2025.
- 44. Haoyan Xu*, Zhengtao Yao*, Yushun Dong, Ziyi Wang, Ryan A. Rossi, Mengyuan Li, <u>Yue Zhao</u> Few-Shot Graph Out-of-Distribution Detection with LLMs

 European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD), 2025.

- 43. Tiankai Yang*, Yi Nian*, Shawn Li, Ruiyao Xu, Yuangang Li, Jiaqi Li, Xiyang Hu, Ryan Rossi, Kaize Ding, Xia Hu, <u>Yue Zhao</u>
 - AD-LLM: Benchmarking Large Language Models for Anomaly Detection Findings of the Association for Computational Linguistics (ACL Findings), 2025.
- 42. Yu Xia, Subhojyoti Mukherjee, Zhouhang Xie, Junda Wu, Xintong Li, Ryan Aponte, Hanjia Lyu, Joe Barrow, Hongjie Chen, Franck Dernoncourt, Branislav Kveton, Tong Yu, Ruiyi Zhang, Jiuxiang Gu, Nesreen K. Ahmed, Yu Wang, Xiang Chen, Hanieh Deilamsalehy, Sungchul Kim, Zhengmian Hu, Yue Zhao, Nedim Lipka, Seunghyun Yoon, Ting-Hao Kenneth Huang, Zichao Wang, Puneet Mathur, Soumyabrata Pal, Koyel Mukherjee, Zhehao Zhang, Namyong Park, Thien Huu Nguyen, Jiebo Luo, Ryan A. Rossi, Julian McAuley
 - From Selection to Generation: A Survey of LLM-based Active Learning Annual Meeting of the Association for Computational Linguistics (ACL), 2025.
- 41. Kaixiang Zhao, Lincan Li, Kaize Ding, Neil Zhenqiang Gong, <u>Yue Zhao</u>, Yushun Dong A Survey on Model Extraction Attacks and Defenses for Large Language Models *ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD Lecture-Style Tutorial Track)*, 2025.
- 40. Shawn Li, Huixian Gong, Hao Dong, Tiankai Yang, Zhengzhong Tu, <u>Yue Zhao</u> DPU: Dynamic Prototype Updating for Multimodal Out-of-Distribution Detection Conference on Computer Vision and Pattern Recognition (CVPR), **Q** Highlight, 2025
- 39. Hanhui Wang, Yihua Zhang, Ruizheng Bai, <u>Yue Zhao</u>, Sijia Liu, Zhengzhong Tu Edit Away and My Face Will Not Stay: Personal Biometric Defense against Malicious Generative Editing
 - Conference on Computer Vision and Pattern Recognition (CVPR), 2025
- 38. Yanbo Wang, Jiayi Ye, Siyuan Wu, Chujie Gao, Yue Huang, Xiuying Chen, <u>Yue Zhao</u>, Xiangliang Zhang TRUSTEVAL: A Dynamic Evaluation Toolkit on Trustworthiness of Generative Foundation Models Annual Conference of the North American Chapter of the Association for Computational Linguistics (NAACL Demo Track), 2025.
- 36. Sihan Chen, Zhuangzhuang Qian, Wingchun Siu, Xingcan Hu, Jiaqi Li, Shawn Li, Yuehan Qin, Tiankai Yang, Zhuo Xiao, Wanghao Ye, Yichi Zhang, Yushun Dong, <u>Yue Zhao</u> PyOD 2: A Python Library for Outlier Detection with LLM-powered Model Selection International World Wide Web Conference (The Web Conference Demo Track), 2025
- 35. Sizhe Liu, Yizhou Lu, Siyu Chen, Xiyang Hu, Tianfan Fu, <u>Yue Zhao</u>
 DrugAgent: Automating AI-aided Drug Discovery Programming through LLM Multi-Agent Collaboration
 - AAAI Workshop on Foundation Models for Biological Discoveries (FMs4Bio), 2025.
- 34. Hao Dong, <u>Yue Zhao</u>, Eleni Chatzi, Olga Fink MultiOOD: Scaling Out-of-Distribution Detection for Multiple Modalities Advances in Neural Information Processing Systems (NeurIPS), ♀ Spotlight, 2024
- 33. Xueying Ding, <u>Yue Zhao</u>, Leman Akoglu
 Fast Unsupervised Deep Outlier Model Selection with Hypernetworks
 ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD), 2024
- 32. Lichao Sun, Yue Huang, Haoran Wang, Siyuan Wu, Qihui Zhang, Chujie Gao, Yixin Huang, Wenhan Lyu, Yixuan Zhang, Xiner Li, Zhengliang Liu, Yixin Liu, Yijue Wang, Zhikun Zhang, 50+ collaborative authors, Yue Zhao
 - TrustLLM: Trustworthiness in Large Language Models International Conference on Machine Learning (ICML), 2024
- Songtao Liu, Hanjun Dai, <u>Yue Zhao</u>, Peng Liu
 Preference Optimization for Molecule Synthesis with Conditional Residual Energy-based Models International Conference on Machine Learning (ICML), Oral, 2024
- Yue Zhao, Leman Akoglu
 Hyperparameter Optimization for Unsupervised Outlier Detection
 International Conference on Automated Machine Learning (AutoML), 2024

29. Yue Zhao

Towards Reproducible, Automated, and Scalable Anomaly Detection

AAAI Conference on Artificial Intelligence (AAAI), New Faculty Highlights, 2024

28. Minqi Jiang*, Chaochuan Hou*, Ao Zheng*, Songqiao Han, Hailiang Huang † , Qingsong Wen, Xiyang Hu † , Yue Zhao †

ADGym: Design Choices for Deep Anomaly Detection.

Advances in Neural Information Processing Systems (NeurIPS), 2023
(†Corresponding author)

- 27. Jaemin Yoo, <u>Yue Zhao</u>, Lingxiao Zhao, Leman Akoglu
 DSV: An Alignment Validation Loss for Self-supervised Outlier Model Selection
 European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in
 Databases (ECML/PKDD), 2023
- 26. Peng Xu, Lin Zhang, Xuanzhou Liu, Jiaqi Sun, <u>Yue Zhao</u>, Haiqin Yang, Bei Yu Do Not Train It: A Linear Neural Architecture Search of Graph Neural Networks *International Conference on Machine Learning (ICML)*, 2023
- Yue Zhao, Guoqing Zheng, Subhabrata Mukherjee, Robert McCann, Ahmed Awadallah ADMoE: Anomaly Detection with Mixture-of-Experts from Noisy Labels Thirty-Seventh AAAI Conference on Artificial Intelligence (AAAI), 2023
- Yue Zhao, George H. Chen, Zhihao Jia
 TOD: GPU-accelerated Outlier Detection via Tensor Operations International Conference on Very Large Data Bases (VLDB), 2023
- 23. Songqiao Han*, Xiyang Hu*, Hailiang Huang*, Minqi Jiang*, <u>Yue Zhao*</u> ADBench: Anomaly Detection Benchmark Advances in Neural Information Processing Systems (NeurIPS), 2022 (*equal contribution & the corresponding author)
- 22. <u>Yue Zhao*</u>, Kay Liu*, Yingtong Dou*, et al. Benchmarking Node Outlier Detection on Graphs Advances in Neural Information Processing Systems (NeurIPS), 2022 (*equal contribution)
- Yue Zhao, Xiaorong Zhang, Leman Akoglu
 ELECT: Toward Unsupervised Outlier Model Selection

 IEEE International Conference on Data Mining (ICDM), 2022.
- Zhiming Xu, Xiao Huang, <u>Yue Zhao</u>, Yushun Dong, Jundong Li Contrastive Attributed Network Anomaly Detection with Data Augmentation Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD), 2022.
- Yue Zhao, Ryan A. Rossi, Leman Akoglu
 Automatic Unsupervised Outlier Model Selection
 Advances in Neural Information Processing Systems (NeurIPS), 2021.
- 18. Kwei-Herng Lai, Daochen Zha, Junjie Xu, <u>Yue Zhao</u>, Guanchu Wang, Xia Hu Revisiting Time Series Outlier Detection: Definitions and Benchmarks *Advances in Neural Information Processing Systems* (*NeurIPS*), 2021
- 17. Kexin Huang*, Tianfan Fu*, Wenhao Gao*, <u>Yue Zhao</u>, Yusuf Roohani, Jure Leskovec, Connor W. Coley, Cao Xiao, Jimeng Sun, Marinka Zitnik

Therapeutics Data Commons: Machine Learning Datasets and Tasks for Drug Discovery and Development

Advances in Neural Information Processing Systems (NeurIPS), 2021 (*equal contribution)

- 16. Yue Zhao*, Xiyang Hu*, Cheng Cheng, Cong Wang, Changlin Wan, Wen Wang, Jianing Yang, Haoping Bai, Zheng Li, Cao Xiao, Yunlong Wang, Zhi Qiao, Jimeng Sun, Leman Akoglu SUOD: Accelerating Large-scale Unsupervised Heterogeneous Outlier Detection Conference on Machine and Learning Systems (MLSys), 2021. (*equal contribution)
- 15. Kwei-Herng Lai*, Daochen Zha*, Guanchu Wang, Junjie Xu, <u>Yue Zhao</u>, Devesh Kumar, Yile Chen, Purav Zumkhawaka, Minyang Wan, Diego Martinez and Xia Ben Hu TODS: An Automated Time Series Outlier Detection System (Demo paper) *Thirty-Fifth AAAI Conference on Artificial Intelligence (AAAI)*, 2021. (*equal contribution)

 Meng-Chieh Lee, <u>Yue Zhao</u>, Aluna Wang, Pierre Jinghong Liang, Leman Akoglu, Vincent S. Tseng, Christos Faloutsos

AutoAudit: Mining Accounting and Time-Evolving Graphs IEEE International Conference on Big Data (Big Data), 2020

- 13. Changlin Wan, Dongya Jia, <u>Yue Zhao</u>, Wennan Chang, Sha Cao, Xiao Wang, and Chi Zhang A Data Denoising Approach to Optimize Functional Clustering of Single Cell RNA-sequencing Data *IEEE International Conference on Bioinformatics and Biomedicine* (*BIBM*), 2020
- Yue Zhao, Xueying Ding, Jianing Yang, Haoping Bai.
 SUOD: Toward Scalable Unsupervised Outlier Detection
 Workshops at the Thirty-Fourth AAAI Conference on Artificial Intelligence, 2020.
 Extended version published in MLSys 2021.
- Zheng Li, <u>Yue Zhao</u>, Nicola Botta, Cezar Ionescu, Xiyang Hu COPOD: Copula-Based Outlier Detection IEEE International Conference on Data Mining (ICDM), 2020.
- Zheng Li, <u>Yue Zhao</u>, Jialin Fu SYNC: A Copula based Framework for Generating Synthetic Data from Aggregated Sources IEEE International Conference on Data Mining Workshops (ICDMW), 2020.
- 9. Yiqun Mei, <u>Yue Zhao</u>, Wei Liang DSR: An Accurate Single Image Super Resolution Approach for Various Degradations *IEEE International Conference on Multimedia and Expo (ICME)*, 2020, London, UK.
- 8. <u>Yue Zhao</u>, Xuejian Wang*, Cheng Cheng*, Xueying Ding*
 Combining Machine Learning Models and Scores using combo Library (Demo paper)
 Thirty-Fourth AAAI Conference on Artificial Intelligence (AAAI), 2020.

 (*equal contribution)
- Colin Wan, Zheng Li, Alicia Guo, Yue Zhao
 SynC: A Unified Framework for Generating Synthetic Population with Gaussian Copula
 Workshops at the Thirty-Fourth AAAI Conference on Artificial Intelligence, 2020.
 Extended version published in ICDMW 2020.
- Zain Nasrullah, <u>Yue Zhao</u>
 Music Artist Classification with Convolutional Recurrent Neural Networks
 IEEE International Joint Conference on Neural Networks (IJCNN), 2019, Hungary.
- Yue Zhao, Zain Nasrullah, Maciej K. Hryniewicki, Zheng Li LSCP: Locally Selective Combination in Parallel Outlier Ensembles SIAM International Conference on Data Mining (SDM), 2019, Calgary, Canada.
- 4. <u>Yue Zhao</u>, Maciej K. Hryniewicki DCSO: Dynamic Combination of Detector Scores for Outlier Ensembles ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD Workshop on Outlier Detection De-constructed), 2018, London, UK. Extended version published in SDM 2019, renamed to LSCP.
- 3. <u>Yue Zhao</u>, Maciej K. Hryniewicki XGBOD: Improving Supervised Outlier Detection with Unsupervised Representation Learning *IEEE International Joint Conference on Neural Networks (IJCNN*), 2018, Rio, Brazil.
- 2. <u>Yue Zhao</u>, Maciej K. Hryniewicki, Francesca Cheng, Boyang Fu, Xiaoyu Zhu Employee Turnover Prediction with Machine Learning: A Reliable Approach *Intelligent System Conference* (*Intellisys*), 2018, London, UK.
- Yue Zhao*, Zhongtian Qiu*, Yiqing Yang*, Weiwei Li*, Mingming Fan
 An Empirical Study of Touch-based Authentication Methods on Smartwatches
 ACM International Symposium on Wearable Computers (ISWC), 2017, Maui, USA. (*equal contribution)

INTERNSHIP NortonLifeLock Research Group EXPERIENCE Machine Learning Research Intern

2022

Microsoft Research

Machine Learning Research Intern

2022

Stanford University, Computer Science Department

Visiting Student Researcher (Prof. Jure Leskovec)

2021

IQVIA, Analytics Center of Excellence

Machine Learning Research Intern

2020

Siemens PLM Software USA

Software Engineer (Intern & Contract)

Mar. 2012 - Dec. 2014

Fall 2026 (scheduled)

Spring 2026 (scheduled)

Los Angeles, CA

Spring 2025

Spring 2024

Fall 2022

Fall 2021

Cincinnati, OH

Fall 2014

Pittsburgh, PA

TEACHING EXPERIENCE University of Southern California

Instructor

CSCI 566 Deep Learning and Its Applications

Instructor

CSCI 699 Adversarial and Trustworthy Foundation Models

Instructor

CSCI 566 Deep Learning and Its Applications

Instructor

CSCI 566 Deep Learning and Its Applications

 $Carnegie\ Mellon\ University$

Teaching Assistant

Managing Digital Business (Prof. David Riel)

Teaching Assistant & co-Instructor (lectures on AutoML and MLSys) Spring 2022 – Fall 2020

Intro to Artificial Intelligence (Prof. David Steier)

Teaching Assistant Spring 2022

Digital Transformation (Prof. David Riel)

Teaching Assistant (helping on course topics)

Statistics for IT Managers (Prof. Daniel Nagin)

University of Toronto Toronto, ON
Teaching Assistant & Lab Session Instructor Fall 2015

Embedded Systems (Prof. Philip Anderson)

University of Cincinnati

Teaching Assistant & Lab Session Instructor

Intro to Programming (Prof. George Purdy)

Ph.D. Students

• Haoyan Xu (USC, ECE Ph.D., 2024 Spring-), co-advised by Mengyuan Li, 🙎 Capital One Fellowship

• Yuehan Qin (USC, CS Ph.D., 2024 Fall-)

• Tiankai Yang (USC, CS Ph.D., 2024 Fall-)

• Shawn Li (USC, CS Ph.D., 2024 Fall-), Capital One Fellowship, Amazon ML Fellowship

• Jiate Li (USC, CS Ph.D., 2025 Fall-)

Services Conference/Workshop Organizing Committee

• Workflow Co-Chair for KDD 2023

• Co-organizer, AI for Financial Fraud Detection & Prevention Workshop @ 6th ACM International Conference on AI in Finance

External Reviewer for Funding Proposals

• Dutch Research Council (NWO)

Journal Editor

- Associate Editor, ACM Transactions on AI for Science (TAIS), 2025–present
- Associate Editor, IEEE Transactions on Neural Networks and Learning Systems (TNNLS), 2024–present
- Action Editor, Journal of Data-centric Machine Learning Research (DMLR), 2024-present

Program Committee (PC) or Area Chair (AC) for Conferences and Workshops

- ICLR 2025 (AC), ICLR 2026 (AC)
- AAAI 2021, 2022, 2023, 2025 (Senior PC), 2026 (Senior PC)
- ICML 2024, 2025 (AC)
- NeurIPS 2021, 2022, 2023, 2025 (AC)
- AISTATS 2024, 2025 (AC)
- MLSys 2024, 2026
- KDD 2020, 2021, 2022, 2023
- IJCAI 2022, 2023
- AAAI Demonstrations 2021, 2022
- MICCAI 2020, 2021, 2022
- ICDM 2020
- KDD Workshop on Outlier Detection and Description (ODD), 2021
- KDD Workshop on Anomaly and Novelty Detection (ANDEA), 2021, 2022
- IJCAI Workshop on Artificial Intelligence for Anomalies and Novelties (AI4AN), 2020, 2021
- INFORMS Workshop on Data Science 2021

Journal Reviewer

- Journal of Machine Learning Research (JMLR)
- PNAS Nexus
- Machine Learning
- IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)
- IEEE Transactions on Knowledge and Data Engineering (TKDE)
- IEEE Internet of Things Journal (IoT-J)
- IEEE Intelligent Systems
- IEEE Journal on Selected Areas in Communications (J-SAC)
- Data Mining and Knowledge Discovery (DMAI)
- ACM Transactions on Management Information Systems (TMIS)
- Knowledge and Information Systems (KAIS)
- INFORMS Journal on Computing (IJOC)
- Big Data
- Artificial Intelligence Review (AIRE)
- Neurocomputing
- IEEE Transactions on Systems, Man, and Cybernetics: Systems
- IEEE/ACM Transactions on Computational Biology and Bioinformatics (TCBB)
- IEEE Network Magazine
- IEEE Computational Intelligence Magazine (CIM)
- BioData Mining
- European Journal of Management and Business Economics (EJMBE)
- The Journal of Open Source Software (JOSS)

Talks and Lectures	USC symposium on Frontiers of ML/AI	Towards Robust Al: Advances in Outlier and OOD Detection	Mar. 2025
	NUS Tea Talk	Towards Robust Al: Advances in Outlier and OOD Detection	Jan. 2025
	SFU@NeurIPS'24	Towards Robust Al: Advances in Outlier and OOD Detection	Dec. 2024
	KAIST	Unsupervised Model Selection: Automation with Meta-learning and LLMs	Nov. 2024
	Kennesaw State University	$\label{lem:unsupervised} Unsupervised\ Model\ Selection:\ Automation\ with\ Meta-learning \\ and\ LLMs$	Oct. 2024
	LinkedIn Anti-Abuse AI	Outlier Detection: Automation, Systems, and GenAI	Aug. 2024
	Amazon Security AI	Outlier Detection: Automation, Systems, and GenAI	Aug. 2024
	New York University	Outlier Detection: Automation, Systems, and GenAI	Aug. 2024
	University of Washington	Outlier Detection: Automation, Systems, and GenAI	Jun. 2024
	Microsoft	Outlier Detection: Automation, Systems, and GenAI	Jun. 2024
	USC Retreat on AI and Engineering Safety	Safety Measures for LLMs	Apr. 2024
	Visa Research	Towards Reproducible, Automated, and Scalable AD	Apr. 2024
	USC Symposium on Frontiers of Generative AI	Generative AI for Anomaly Detection	Mar. 2024
	AAAI New Faculty High- lights (invited)	Towards Reproducible, Automated, and Scalable AD	Feb. 2024
	U of Nevada, Las Vegas	Automated and Scalable ML Algorithms and Systems	Oct. 2023
	Samsung Seminar	Automated and Scalable Anomaly Detection Systems	Aug. 2023
	KDD SoCal Day	Enable Applications by ML with Noisy Inputs	Aug. 2023
	CMU Catalyst	How (Not) to Fail Your Academic Job Search	May. 2023
	KAUST	Automated and Scalable ML Algorithms and Systems	Apr. 2023
	Emory University	Automated and Scalable ML Algorithms and Systems	Apr. 2023
	USC	Automated and Scalable ML Algorithms and Systems	Mar. 2023
	UC Davis	Automated and Scalable ML Algorithms and Systems	Mar. 2023
	Stony Brook University	Automated and Scalable ML Algorithms and Systems	Feb. 2023
	University of Chicago	Automated and Scalable ML Algorithms and Systems	Feb. 2023
	UC Merced	Automated and Scalable ML Algorithms and Systems	Feb. 2023
	CMU PDL Meeting	Automated and Scalable ML Algorithms and Systems	Jan. 2023
	CMU Data Science Seminar	Guest Lecture Automated Anomaly Detection	Nov. 2022
	LoG Seminar	Large-scale Graph Anomaly Detection	Oct. 2022
	Intuit	Anomaly Detection for Financial Risk Modeling	Aug. 2022
	Rice University	Large-scale Anomaly Detection with Automation	Sep. 2022
	Microsoft Research	Weakly-supervised Anomaly Detection	Sep. 2022
	Wells Fargo	Anomaly Detection for Financial Risk Modeling	Aug. 2022
	Columbia University	Guest Lecture Anomaly Detection	Jul. 2022
	Morgan Stanley	Automated Outlier Detection	Jun. 2022
	Microsoft Research	Automated Outlier Detection	Jun. 2022
	Morgan Stanley	Large-scale Anomaly Detection Systems	Mar. 2022
	Rutgers Business School	Outlier Model Selection	Mar. 2022
	Tesla	Large-scale Anomaly Detection Systems	Feb. 2022
	Catalyst, CMU	Systems for Data Mining Algorithms	Dec. 2021
	E&Y Canada	ML applications in Data Analytics	Oct. 2021
	University of Nottingham	General Machine Learning Applications	Jan. 2021