Huimin ZENG

+1 217-721 8064 | huiminz3@illinois.edu

Education

University of Illinois at Urbana-Champaign Champaign, U.S.A
Graduate Research Assistant *Aug. 2021 - Present*

- **Advisor**: Prof. Dr. Dong Wang
- **Relevant Courses**: Social Sensing; Data Mining; Advanced Topics in NLP

Technical University of Munich Munich, Germany
Master of Science in Computer Science; GPA: 1.3/1.0; Ranking: Top 3% *Sep. 2018 - Jul. 2021*

- **Relevant Courses**: Machine Learning (Top 5%); Introduction to Deep Learning (Top 10%)
- **Master Thesis**: Floating Point Soundness in Neural Network Verification **SRILab @ ETH**

University of California, San Diego La Jolla, U.S.A
Master's Exchange Program in Computer Science and Engineering; GPA 4.0/4.0 *Jan. 2020 - Sep. 2020*

- **Relevant Courses**: Pattern Recognition (Top 10%); Learning Algorithms; Convex Optimization; Data Modeling

Tongji University Shanghai, China
Bachelor of Engineering in Robotics and Mechatronics; GPA: 4.52/5.0 (90.24/100.0); Ranking: Top 10% *Sep. 2014 - Aug. 2018*

- **Relevant Courses**: Linear Algebra(Top 5%); Probabilistic Theory (Top 10%)); Robotics (Top 3%)
- **Bachelor Thesis**: Development for a Concept of a Real-time Communication System with Chatbot-Integration **@ BMW**

Selected Publications

- **Federated Recommendation via Hybrid Retrieval Augmented Generation**
  Huimin Zeng, *Zhenrui Yue, Qian Jiang, Dong Wang*
  Accepted by the IEEE International Conference on Big Data (BigData) 2024
- **Fair Federated Learning Models via Biased Vision-Language Models**
  Huimin Zeng, *Zhenrui Yue, Yang Zhang, Lanyu Shang, Dong Wang*
  Accepted by the Findings of the 62nd Annual Meeting of the Association for Computational Linguistics (ACL Findings) 2024
- **Fair Sequential Recommendation without User Demographics**
  Huimin Zeng, *Zhankui He, Zhenrui Yue, Julian McAuley, Dong Wang*
  Accepted by the 47th International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR) 2024
- **Mitigating Demographic Bias of Federated Learning Models via Robust-Fair Domain Smoothing**
  Huimin Zeng, *Zhenrui Yue, Qian Jiang, Yang Zhang, Lanyu Shang, Ruohan Zong, Dong Wang*
  Accepted by the 44th IEEE International Conference on Distributed Computing Systems (ICDCS) 2024
- **Open-Vocabulary Federated Learning via Multimodal Prototyping**
  Huimin Zeng, *Zhenrui Yue, Dong Wang*
  Accepted by the Annual Conference of the North American Chapter of the Association for Computational Linguistics (NAACL) 2024
- **Manipulating Out-Domain Uncertainty Estimation in Deep Neural Networks via Targeted Clean-Label Poisoning**
  Huimin Zeng, *Zhenrui Yue, Yang Zhang, Lanyu Shang, Dong Wang*
  Accepted by the 32nd ACM International Conference on Information and Knowledge Management (CIKM) 2023
- **On Adversarial Robustness of Demographic Fairness in Face Attribute Recognition**
  Huimin Zeng, *Zhenrui Yue, Lanyu Shang, Yang Zhang, Dong Wang*
  Accepted by the International Joint Conference on Artificial Intelligence (IJCAI) 2023
- **Zero- and Few-Shot Event Detection via Prompt-Based Meta Learning**
  Zhenrui Yue, ***Huimin Zeng***, *Mengfei Lan, Heng Ji, Dong Wang*
  Accepted by the the 61st Annual Meeting of the Association for Computational Linguistics (ACL) 2023
- **MetaAdapt: Domain Adaptive Few-Shot Misinformation Detection via Meta Learning**
  Zhenrui Yue, ***Huimin Zeng***, *Yang Zhang, Lanyu Shang, Dong Wang*
  Accepted by the the 61st Annual Meeting of the Association for Computational Linguistics (ACL) 2023
- **Fairness-aware Training of Face Attribute Classifiers via Adversarial Robustness**
  Huimin Zeng, *Zhenrui Yue, Ziyi Kou, Yang Zhang, Lanyu Shang, Dong Wang*
  Accepted by Elsevier Knowledge-Based Systems (KBS), 2023
- **On Attacking Out-Domain Uncertainty Estimation in Deep Neural Networks**
  Huimin Zeng, *Zhenrui Yue, Yang Zhang, Ziyi Kou, Lanyu Shang, Dong Wang*
  Accepted by the International Joint Conference on Artificial Intelligence (IJCAI) 2022
- **Boosting Demographic Fairness of Face Attribute Classifiers via Latent Adversarial Representations**
  Huimin Zeng, *Zhenrui Yue, Lanyu Shang, Yang Zhang, Dong Wang*
  Accepted by the IEEE International Conference on Big Data (BigData) 2022

- **Unsupervised Domain Adaptation for COVID-19 Information Service with Contrastive Adversarial Domain Mixup**
  ***Huimin Zeng**, Zhenrui Yue, Ziyi Kou, Lanyu Shang, Yang Zhang, Dong Wang*
  Accepted by the IEEE/ACM International Conference on Advances in Social Network Analysis and Mining (ASONAM) 2022
- **QA Domain Adaptation using Hidden Space Augmentation and Self-Supervised Contrastive Adaptation**
  Zhenrui Yue, **Huimin Zeng***, Ziyi Kou, Lanyu Shang, Dong Wang
  Accepted by the Conference on Empirical Methods in Natural Language Processing (EMNLP) 2022
- **Domain Adaptation for Question Answering via Question Classification**
  *Zhenrui Yue, **Huimin Zeng**, Ziyi Kou, Lanyu Shang, Dong Wang*
  Accepted by the International Conference on Computational Linguistics (COLING) 2022
- **Contrastive Domain Adaptation for Early Misinformation Detection: A Case Study on COVID-19**
  *Zhenrui Yue, **Huimin Zeng**, Ziyi Kou, Lanyu Shang, Dong Wang*
  Accepted by the ACM International Conference on Information and Knowledge Management (CIKM) 2022
- **Defending Substitution-Based Profile Pollution Attacks on Sequential Recommenders**
  *Zhenrui Yue, **Huimin Zeng**, Ziyi Kou, Lanyu Shang, Dong Wang*
  Accepted by the ACM Conference on Recommender Systems (RecSys) 2022
- **Certified Defense via Latent Space Randomized Smoothing with Orthogonal Encoders**
  ***Huimin Zeng**, Jiahao Su, Furong Huang*
  https://arxiv.org/abs/2108.00491
- **Adversarial Examples Created Equal? A Learnable Weighted Minimax Risk for Robustness under Non-uniform Attacks**
  Huimin Zeng*, Chen Zhu*, Tom Goldstein, Furong Huang
  Accepted by the Association for the Advancement of Artificial Intelligence (AAAI) 2021
- **Black-Box Adversarial Attacks on Sequential Recommender Systems via Data-Free Model Extraction**
  Zhenrui Yue*, Zhankui He*, **Huimin Zeng**, Julian McAuley
  Accepted by the ACM Conference on Recommender Systems (RecSys) 2021

Work Experience

Software Development Intern BMW AG, Germany
Project: A real-time communication software with Chatbot integration *Feb. 2018 - Sep. 2018*

Machine Learning Research Intern Robert Bosch LLC., U.S.A
Project: Domain-generalized machine learning framework for semantic segmentation *May. 2023 - Aug. 20023*

Teaching Experience

Teaching Assistant University of Illinois at Urbana-Champaign, U.S.A
Lecture: Introduction to Database *Aug. 2022 - Present*

Teaching Assistant Technical University of Munich, Germany
Lecture: Introduction to Deep Learning *Apr. 2019 - Aug. 2019*

Awards

2022: **UIUC Conference Travel and Presentation Award**
2021: **Bosch AIoT Scholarship, Robert Bosch GmbH**
2018: **Scholarship of German National Academic Foundation**
2017: **Tongji Scholarship of Excellence**
2017: **Tongji Scholarship for Social Practice**
2016: **Tongji Scholarship of Excellence**
2015: **Tongji Scholarship of Excellence**

Miscellaneous

- **Programming Languages**: Python, C++
- **Libraries**: PyTorch, Scikit-Learn, Numpy
- **Languages**: English, German
- **Service**: ICLR 2023, ASONAM 2023, AAAI 2024