Zuobin Xiong

Assistant Professor · Department of Computer Science

University of Nevada-Las Vegas, 4505 S. Maryland Pkwy. Las Vegas, NV 89154

(702)-774-3407 | zuobin.xiong@unlv.edu | https://zuobinxiong.github.io

Work Experiences

2023 - Now	**Assistant Professor** Department of Computer Science, University of Nevada-Las Vegas, Las Vegas, NV
2019 - 2023	**Graduate Teaching Assistant** Department of Computer Science, Georgia State University, Atlanta, GA
2018 - 2023	**Graduate Research Assistant** Department of Computer Science, Georgia State University, Atlanta, GA
2016 - 2017	**Software Development Engineer** Heilongjiang Huamiao Trading Ltd., Harbin, China

Research Interests

AI/ML	**Distributed Machine Learning, Federated Learning** **Machine Unlearning, Generative AI, AI4Healthcare**
Data Privacy	**Differential Privacy** **Private Machine Learning, Privacy in IoT**
Data Mining	**Data Publishing** **Graph Mining**

Awards & Honors

Apr. 2024	**NSF SaTC Aspiring PI Workshop Travel Grant** Awarded by NSF 2024 SaTC Aspiring PI Workshop
Apr. 2023	**Outstanding Graduate Student Award** Awarded by the College of Arts & Sciences, Georgia State University
Feb. 2023	**Student Travel Scholarship** Awarded by AAAI -23 and the Association for the Advancement of Artificial Intelligence
Aug. 2022	**Best Paper Award** Awarded by the 8th IEEE International Conference on Smart Data (SmartData 2022)
Apr. 2021	**Outstanding Graduate Research Award** Awarded by the Department of Computer Science, Georgia State University

Education

Georgia State University — Atlanta, USA

Ph.D., Computer Science — 2018 - 2023

- Dissertation Advisor: Dr. Wei Li & Dr. Zhipeng Cai

Harbin Engineering University — Harbin, China
M.E., Computer Science & Technology — 2016 - 2019
- Advisor: Dr. Qilong Han

Northeast Forestry University — Harbin, China
B.S., Mathematics & Applied Mathematics — 2012 - 2016
- Thesis mentor: Dr. Chunrui Zhang

Teaching Experiences

Teaching at University of Nevada, Las Vegas

Spring 2024	**CS 302, Data Structures, SEI (TBD)** Instructor, Undergraduate Level Course, Class Enrollment 40
Fall 2023	**CS 789, Advanced Network Security, SEI (4.72/5.0)** Instructor, Graduate Level Course, Class Enrollment 10

Teaching at Georgia State University

Spring 2021	**CSC 4222/6222, Intro to Cyber Security, SEI (4.5/5.0)** Instructor, Undergraduate Level Course, Class Enrollment 55
Fall 2019	**CSC 4520/6520, Design and Analysis of Algorithms, SEI (4.7/5.0)** Instructor, Undergraduate Level Course, Class Enrollment 57
Fall 2022	**CSC 4221/6221, Mobile Computing & Wireless Networks** Teaching Assistant
Spring 2022	**CSC 8920, Private and Secure AI (Online)** Teaching Assistant
Fall 2021	**CSC 4520/6520, Design and Analysis of Algorithms** Teaching Assistant
Fall 2020	**CSC 4222/6222, Cyber Security** Teaching Assistant
Spring 2020	**CSC 4740/6740, Data Mining** Teaching Assistant
Spring 2019	**CSC 4740/6740, Data Mining** Teaching Assistant

Research Grants

2024 - 2026	**Are You Ready for College? An Explainable AI-Supported Efficient Solution for College Students Mental Health Condition Detection and Beyond** PI, University of Nevada-Las Vegas, *$35,000*
2024 - 2026	**Intelligent IoT Security: Next-Generation Cyber Defense Mechanisms and Vulnerability Exploration Using Language Models** Co-PI, South Korea, *$357,739*
2023 - 2024	**RII Track-2 FEC: AI SUSTEIN Seed Funding** Single PI, NSF EPSCoR, *$29,000*
2021 - 2024	**EDU: Collaborative: Advancing Cybersecurity Learning Through Inquiry-based Laboratories on a Container-based Virtualization Platform** NSF SaTC, Writing thrusts for my advisor

Publications

Under Peer-reviewed Papers

1. RAID 2024 — HTML Tag Sequence-Based Phishing Website Detection Using Transformer Encoder
Jemin Ahn, **Zuobin Xiong**, Kyungtae Kang, and Junggab Son. *RAID 2024*.
2. ECAI 2024 — Overcoming Limited Labeled Data via Image Generation in Fine-Grained Fashion Image Classification
Hongbi Jeong, **Zuobin Xiong**, and Junggab Son. *ECAI 2024*.
3. ECAI 2024 — DDSNet: A Lightweight Dense Depthwise Separable Network for Tumor Classification
An Huang, **Zuobin Xiong**, and Junggab Son. *ECAI 2024*.
4. PKDD 2024 — FCFL: A Fairness Compensation-based Federated Learning Scheme with Accumulated Queues
Lingfu Wang, **Zuobin Xiong**, and Aiguo Chen. *PKDD 2024*.

Selected Journal Articles

1. HCC 2023 — DEFEAT: A decentralized federated learning against gradient attacks
Guangxi Lu, **Zuobin Xiong**, Ruinian Li, Nael Mohammad, Yingshu Li, and Wei Li. *High-Confidence Computing, Volume 3, Issue 3, September 2023.* **(IF: 5.42)**
2. WWW 2023 — Personalized Sampling Graph Collection with Local Differential Privacy for Link Prediction
Linyu Jiang, Yukun Yan, Zhihong Tian, **Zuobin Xiong** and Qilong Han. *World Wide Web*. **(IF: 3.000)**
3. TDSC 2022 — Towards Neural Network-based Communication System: Attack and Defense
Zuobin Xiong, Zhipeng Cai, Chunqiang Hu, Daniel Takabi, and Wei Li. *IEEE Transactions on Dependable and Secure Computing*. **(IF: 6.791)**
4. CSUR 2022 — Generative Adversarial Networks: A Survey Toward Private and Secure Applications
Zhipeng Cai, **Zuobin Xiong**, Honghui Xu, Peng Wang, Wei Li, and Yi Pan. *ACM Computing Surveys, Vol. 54, No. 6, Jul. 2022*. **(IF: 10.238)**
5. TII 2022 — Privacy Threat and Defense for Federated Learning with Non-iid Data in AIoT
Zuobin Xiong, Zhipeng Cai, Daniel Takabi, and Wei Li. *IEEE Transactions on Industrial Informatics, Vol. 18, No. 2, Feb. 2022*. **(IF: 11.648)**
6. IoT-J 2022 — Top-k Socially Constrained Spatial Keyword Search in Large SIoT Networks
Jinbao Wang, **Zuobin Xiong**, Qilong Han, Xixian Han, and Donghua Yang. *IEEE Internet of Things Journal, Vol. 9, No. 12, Jun. 2022*. **(IF: 10.238)**
7. AdHoc 2021 — Gated Recurrent Unit-based Parallel Network Traffic Anomaly Detection using Subagging Ensembles
Xiaoling Tao, Yang Peng, Feng Zhao, Changsong Yang, Baohua Qiang, Yufeng Wang, and **Zuobin Xiong**. *Ad Hoc Networks, Vol. 116, 2021*. **(IF: 4.816)**
8. TVT 2021 — Multi-Source Adversarial Sample Attack on Autonomous Vehicles
Zuobin Xiong, Honghui Xu, Wei Li, and Zhipeng Cai. *IEEE Transactions on Vehicular Technology, Vol. 70, No. 3, Mar. 2021*. **(IF: 6.239)**
9. TII 2021 — ADGAN: Protect Your Location Privacy in Camera Data of Auto-Driving Vehicles
Zuobin Xiong, Zhipeng Cai, Qilong Han, Arwa Alrawais, and Wei Li. *IEEE Transactions on Industrial Informatics, Vol. 17, No. 9, Sept. 2021*. **(IF: 11.648)**
10. WCMC 2021 — CGPP-POI: A Recommendation Model Based on Privacy Protection
Gesu Li, Guisheng Yin, **Zuobin Xiong**, and Fukun Chen. *Wireless Communications and Mobile Computing, Vol. 2021, Aug. 2021*. **(IF: 2.146)**
11. SCN 2021 — Research on Trajectory Data Releasing Method via Differential Privacy Based on Spatial Partition
Qilong Han, **Zuobin Xiong**, and Kejia Zhang. *Security and Communication Networks, Vol. 2018, Nov. 2018*. **(IF: 1.968)**

Selected Conference Papers

1. ICCCN 2024 — Appro-Fun: Approximate Machine Unlearning in Federated Setting
Zuobin Xiong, Wei Li, and Zhipeng Cai. *The 33rd International Conference on Computer Communications and Networks, Big Island, Hawaii, Jul. 2024*.

2.	ICDM 2023	Exact-Fun: An Exact and Efficient Federated Unlearning Approach **Zuobin Xiong**, Wei Li, Yingshu Li, and Zhipeng Cai. *IEEE International Conference on Data Mining*. **(AR: 19.3%)**
3.	ICDM 2023	Backdoor Attack on 3D Grey Image Segmentation Honghui Xu, Zhipeng Cai, **Zuobin Xiong**, and Wei Li. *IEEE International Conference on Data Mining*. **(AR: 19.3%)**
4.	ICANN 2023	Sequence-based Modeling for Temporal Knowledge Graph Link Prediction Wenqiang Liu, Lijie Li, **Zuobin Xiong**, and Ye Wang. *32nd International Conference on Artificial Neural Networks*.
5.	AAAI 2023	Federated Generative Model on Multi-Source Heterogeneous Data in IoT **Zuobin Xiong**, Wei Li, and Zhipeng Cai. *AAAI Conference on Artificial Intelligence, Washington, DC, USA, Feb. 2023.* **(AR: 19.6%)**
6.	Globecom 2022	Pairwise Gaussian Graph Convolutional Networks: Defense Against Graph Adversarial Attack Guangxi Lu, **Zuobin Xiong**, Jing Meng, and Wei Li. *IEEE Global Communications Conference, Rio de Janeiro, Brazil, Dec. 2022*.
7.	WiCON 2022	Decentralized Federated Learning: A Defense against Gradient Inversion Attack Guangxi Lu, **Zuobin Xiong**, and Wei Li. *EAI International Conference on Wireless Internet, Dallas, USA, Nov. 2022*.
8.	SmartData 2022	A Self-Supervised Purification Mechanism for Adversarial Samples Bingyi Xie, Honghui Xu, **Zuobin Xiong**, Yingshu Li, and Zhipeng Cai. *IEEE International Conference on Smart Data, Espoo, Finland, Aug. 2022. (Best Paper Award)*.
9.	SEKE 2022	Exp-SoftLexicon Lattice Model Integrating Radical-Level Features for Chinese NER Lijie Li, Shuangyang Hu, Junhao Chen, YeWang, and **Zuobin Xiong**. *International Conference on Software Engineering & Knowledge Engineering, Pittsburgh, USA, Jul. 2022*.
10.	ICDM 2019	Privacy-Preserving Auto-Driving: a GAN-based Approach to Protect Vehicular Camera Data **Zuobin Xiong**, Wei Li, Qilong Han, and Zhipeng Cai. *IEEE International Conference on Data Mining (ICDM), Beijing, China, Nov. 2019.* **(AR: 9.08%)**

Presentations

Invited Talks

Spet. 2022	**Towards Privacy Preservation of Federated Learning in Artificial Intelligence of Things** Department of Electrical and Computer Engineering, Virginia Commonwealth University
Aug. 2022	**Privacy Threats and Defense in Federated Learning** Department of Computer Science, University of Electronic Science and Technology of China

Conference Presentations

Dec. 2023	**Exact-Fun: An Exact and Efficient Federated Unlearning Approach** IEEE International Conference on Data Mining, Beijing, China, 2023
Jun. 2019	**Privacy-Preserving Auto-Driving: a GAN-based Approach to Protect Vehicular Camera Data** IEEE International Conference on Data Mining, Beijing, China, 2019

Student Mentoring

Current Students

2024 - now	**An Huang, Ph.D. student** Advising, *University of Nevada-Las Vegas*
2023 - now	**Lingfu Wang, Ph.D. student** Co-advising, *University of Electronic Science and Technology of China*
2023 - now	**Hongbi Jeong, Ph.D. student** Co-advising, *University of Nevada-Las Vegas*

Graduated Students

2022 - 2024 **Syed Shariq Ahmed, M.S. student**
Advising, *University of Nevada-Las Vegas*

Professional Services

Academic Membership

- Member of IEEE
- Member of AAAI

PC Member

- 18th International Conference on Wireless Artificial Intelligent Computing Systems and Applications (WASA)
- 32nd International Conference on Artificial Neural Networks (ICANN)
- 1st International Conference onMeta Computing (ICMC)

Editorship

- Guest Editor – MDPI Electronics

Conference Reviewer

- IEEE Global Communications Conference (GLOBECOM)
- IEEE Cyber Science and Technology Congress
- ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)

Journal Reviewer

- ACM Transactions on Sensor Networks (TOSN)
- Discrete Mathematics, Algorithms and Applications (DMAA)
- Elsevier Neurocomputing
- Elsevier Computer & Security
- Elsevier Computer Communications
- Elsevier High-Confidence Computing
- IEEE Transactions on Industrial Informatics (TII)
- IEEE Transactions on Vehicular Technology (TVT)
- IEEE Internet of Things Journal (IoT-J)
- IEEE Transactions on Wireless Communications (TWC)
- IEEE Transactions on Knowledge and Data Engineering (TKDE)
- IEEE Transactions on Network Science and Engineering (TNSE)
- IEEE Transactions on Computational Social Systems (TCSS)
- IEEE Networking Letters
- Security and Communication Networks
- Springer Scientific Reports - Nature
- Springer Artificial Intelligence Review
- Springer Journal of Big Data