4505 S. Maryland Pkwy
Las Vegas, Nevada
United States
☎ *+1 702-774-3407*
✉ *zuobin.xiong@unlv.edu*
🌐 *zuobinxiong.github.io*
in *zuobin-xiong*

Zuobin Xiong

Assistant Professor, Computer Science

> *May the Force be with you.*
> Star Wars 1977

Experience

2023 **Assistant Professor**, *Department of Computer Science*.
University of Nevada, Las Vegas, Las Vegas, NV

2025.08 **Visiting Scholar**, *Department of Computer Science*.
University of Southern California, Los Angeles, CA

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

Education

2023 **Ph.D.**, *Georgia State University*, Atlanta, Georgia.
Computer Science
- Advisors: Dr. Wei Li & Dr. Zhipeng Cai
- Dissertation: Towards Privacy Preservation of Federated Learning in Artificial Intelligence of Things

2019 **M.E.**, *Harbin Engineering University*, Harbin, China.
Computer Science & Technology

2016 **B.S.**, *Northeast Forestry University*, Harbin, China.
Mathematics & Applied Mathematics

Research Area

AI/ML
- Distributed Machine Learning
- Generative AI
- Machine Unlearning
- AI4Science

Data Privacy
- Differential Privacy
- Private/Adversarial Machine Learning

the Internet of Things
- Edge Computing
- Artificial Intelligence of Things (AIoT)
- Social Internet of Things (SIoT)

Data Mining – Trajectory Data Mining
– Graph Mining

Honors & Awards

2024
UNLV University Faculty Travel Grant, *Las Vegas*, NV.
November. Awarded by University Faculty Travel Committee (UFTC)

2024
NSF SaTC Aspiring PI Workshop Travel Grant, *Chicago*, Illinois.
April. Awarded by NSF 2024 SaTC Aspiring PI Workshop

2023
Outstanding Graduate Student Award, *Atlanta*, Georgia.
April. Awarded by the College of Arts & Sciences, Georgia State University

2023
AAAI Student Travel Scholarship, *D.C.*, USA.
February. Awarded by AAAI -23 and the Association for the Advancement of Artificial Intelligence

2022
Best Paper Award, *Espoo*, Finland.
August. Awarded by the 8th IEEE International Conference on Smart Data (SmartData 2022)

2021
Outstanding Graduate Research Award, *Atlanta*, Georgia.
April. Awarded by the Department of Computer Science, Georgia State University

Fundings

2025
2027
A Guided Pathway to Enhancing HSI Student Experience and Success in Generative AI with the Planting of Education Oriented GPU Cluster, *National Science Foundation*.
PI, $199,413

2025
2025
Harnessing Data Revolution for Fire Science (HDRFS) Data Analytics Mentor, *NSF RII HDRFS*.
PI, $4,750

2025
2027
An Explainable AI-Supported Performance Monitoring System in Distributed Sustainable Energy Networks, *National Science Foundation*.
Single PI, $286,889

2024
2026
Are You Ready for College? An Explainable AI-Supported Efficient Solution for College Students Mental Health Condition Detection and Beyond, *University of Nevada, Las Vegas*.
PI, $35,000

2024
2026
Intelligent IoT Security: Next-Generation Cyber Defense Mechanisms and Vulnerability Exploration Using Language Models, *South Korea*.
Co-PI, $357,739

2023
2025
NSF RII Track-2 FEC: AI SUSTEIN Seed Grant, *NSF RII Track-2 Seed Grant Program*.
PI, $30,000

Journal Papers

[1] Z. Xiong, W. Li, Y. Li, and Z. Cai, "Distributed generative model: A data synthesizing framework for multi-source heterogeneous data", *IEEE Transactions on Artificial Intelligence*, pp. 1–1, 2025. DOI: 10.1109/TAI.2025.3575548.

[2] A. Huang*, Z. Cai, and Z. Xiong, "A survey of machine unlearning in generative ai models: Methods, applications, security, and challenges", *IEEE Internet of Things Journal*, pp. 1–1, 2025. DOI: 10.1109/JIOT.2025.3570989.

[3] J. Choi, Z. Xiong, and K. Kang, "Long short-term memory-based computerized numerical control machining center failure prediction model", *Mathematics*, vol. 13, no. 7, p. 1093, 2025.

[4] L. Zhang, S. Park, Z. Xiong, J. Son, and Y. Lee, "Understanding illicit promotional contents on short video platforms", *Tsinghua Science and Technology*, 2024.

[5] G. Lu, Z. Xiong, R. Li, N. Mohammad, Y. Li, and W. Li, "Defeat: A decentralized federated learning against gradient attacks", *High-Confidence Computing*, vol. 3, no. 3, p. 100 128, 2023.

[6] L. Jiang, Y. Yan, Z. Tian, Z. Xiong, and Q. Han, "Personalized sampling graph collection with local differential privacy for link prediction", *World wide web*, vol. 26, no. 5, pp. 2669–2689, 2023.

[7] Z. Xiong, "Towards privacy preservation of federated learning in artificial intelligence of things", 2023.

[8] Z. Xiong, Z. Cai, C. Hu, D. Takabi, and W. Li, "Towards neural network-based communication system: Attack and defense", *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 4, pp. 3238–3250, 2022.

[9] J. Wang, Z. Xiong, Q. Han, X. Han, and D. Yang, "Top-k socially constrained spatial keyword search in large siot networks", *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9280–9289, 2021.

[10] G. Li, G. Yin, Z. Xiong, and F. Chen, "Cgpp-poi: A recommendation model based on privacy protection", *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, p. 4 873 574, 2021.

[11] Z. Xiong, Z. Cai, D. Takabi, and W. Li, "Privacy threat and defense for federated learning with non-iid data in aiot", *IEEE Transactions on Industrial Informatics*, vol. 18, no. 2, pp. 1310–1321, 2021.

[12] Z. Cai, Z. Xiong, H. Xu, P. Wang, W. Li, and Y. Pan, "Generative adversarial networks: A survey toward private and secure applications", *ACM Computing Surveys (CSUR)*, vol. 54, no. 6, pp. 1–38, 2021.

[13] X. Tao, Y. Peng, F. Zhao, *et al.*, "Gated recurrent unit-based parallel network traffic anomaly detection using subagging ensembles", *Ad Hoc Networks*, vol. 116, p. 102 465, 2021.

[14] Z. Xiong, H. Xu, W. Li, and Z. Cai, "Multi-source adversarial sample attack on autonomous vehicles", *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2822–2835, 2021.

[15] Z. Xiong, Z. Cai, Q. Han, A. Alrawais, and W. Li, "Adgan: Protect your location privacy in camera data of auto-driving vehicles", *IEEE Transactions on Industrial Informatics*, vol. 17, no. 9, pp. 6200–6210, 2020.

[16] Q. Han, Z. Xiong, and K. Zhang, "Research on trajectory data releasing method via differential privacy based on spatial partition", *Security and Communication Networks*, vol. 2018, no. 1, p. 4 248 092, 2018.

Conference Papers

[17] A. Huang*, Z. Xiong, M. Ye, and J. Son, "It is hard to unlearn dogged backdoor samples in diffusion models", in *NeurIPS 2025 Workshop: Reliable ML from Unreliable Data*.

[18] C. Dahal* and Z. Xiong, "How well do llms unlearn facts?-a knowledge graph perspective", in *Women in Machine Learning Workshop@ NeurIPS 2025*.

[19] G. C. Amaizu, A. M. Sai, Y. Li, and Z. Xiong, "Trusted medical ai: Blockchain-backed device authentication with digital twin-enhanced xai for lung cancer detection", in *Proceedings of the IEEE International Performance Computing and Communications Conference (IPCCC)*, November 21–23, 2025, Austin, TX, USA, Nov. 2025.

[20] J. Ahn*, Z. Xiong, H. Cho, K. Kang, and J. Son, "Efficient phishing website detection via html tag sequence analysis using encoder models", in *International Conference on Computer Communications and Networks*, IEEE, 2025.

[21] A. Huang*, J. Son, and Z. Xiong, "Ddsnet: A lightweight dense depthwise separable network for tumor classification", in *ACM/SIGAPP Symposium on Applied Computing*, ACM, 2025.

[22] L. Wang*, Z. Xiong, G. Luo, W. Li, and A. Chen, "Fcfl: A fairness compensation-based federated learning scheme with accumulated queues", in *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*, Springer, 2024, pp. 386–402.

[23] Z. Xiong, W. Li, and Z. Cai, "Appro-fun: Approximate machine unlearning in federated setting", in *2024 33rd International Conference on Computer Communications and Networks (ICCCN)*, IEEE, 2024, pp. 1–9.

[24] Z. Xiong, W. Li, Y. Li, and Z. Cai, "Exact-fun: An exact and efficient federated unlearning approach", in *2023 IEEE International Conference on Data Mining (ICDM)*, IEEE, 2023, pp. 1439–1444.

[25] H. Xu, Z. Cai, Z. Xiong, and W. Li, "Backdoor attack on 3d grey image segmentation", in *2023 IEEE International Conference on Data Mining (ICDM)*, IEEE, 2023, pp. 708–717.

[26] L. Li, W. Liu, Z. Xiong, and Y. Wang, "Sequence-based modeling for temporal knowledge graph link prediction", in *International Conference on Artificial Neural Networks*, Springer, 2023, pp. 550–562.

[27] Z. Xiong, W. Li, and Z. Cai, "Federated generative model on multi-source heterogeneous data in iot", in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 37, 2023, pp. 10 537–10 545.

[28] G. Lu, Z. Xiong, R. Li, and W. Li, "Decentralized federated learning: A defense against gradient inversion attack", in *International Wireless Internet Conference*, Springer, 2022, pp. 44–56.

[29] G. Lu, Z. Xiong, J. Meng, and W. Li, "Pairwise gaussian graph convolutional networks: Defense against graph adversarial attack", in *GLOBECOM 2022-2022 IEEE Global Communications Conference*, IEEE, 2022, pp. 4371–4376.

[30] B. Xie, H. Xu, Z. Xiong, Y. Li, and Z. Cai, "A self-supervised purification mechanism for adversarial samples", in *2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, IEEE, 2022, pp. 501–509.

[31] L. Li, S. Hu, J. Chen, Y. Wang, and Z. Xiong, "Exp-softlexicon lattice model integrating radical-level features for chinese ner.", in *The 34th International Conference on Software Engineering & Knowledge Engineering*, 20122, pp. 329–334.

[32] Z. Xiong, W. Li, Q. Han, and Z. Cai, "Privacy-preserving auto-driving: A gan-based approach to protect vehicular camera data", in *2019 IEEE International Conference on Data Mining (ICDM)*, IEEE, 2019, pp. 668–677.

Presentations

Conference Presentations

2024 **Appro-fun: Approximate Machine Unlearning in Federated Setting**, *Big Island*, Hawaii.
July. International Conference on Computer Communications and Networks

2023 **Exact-Fun: An Exact and Efficient Federated Unlearning Approach**, *Beijing*, China.
December. IEEE International Conference on Data Mining

2019 **Privacy-Preserving Auto-Driving: a GAN-based Approach to Protect Vehicular Camera Data**, *Beijing*, China.
June. IEEE International Conference on Data Mining

Invited Talks

2022 **Towards Privacy Preservation of Federated Learning in Artificial Intelligence of Things**, *Online*.
September. Department of Electrical and Computer Engineering, Virginia Commonwealth University

2022 **Privacy Threats and Defense in Federated Learning**, *Online*.
August. University of Electronic Science and Technology of China

Teaching

Teaching at UNLV

2025 **Fall: CS422/622 Intro to Machine Learning**, *Enrollment 24*, SEI, TBD.
Instructor. Under/Graduate Level

2025 **Spring: CS302 Data Structures**, *Enrollment 22*, SEI, TBD.
Instructor. Undergraduate Level

2024 **Fall: CS789 Advanced Topics in Computer Science**, *Enrollment 10*, SEI, 4.58/5.0.
Instructor. Graduate Level

2024 **Spring: CS302 Data Structures**, *Enrollment 40*, SEI, 4.06/5.0.
Instructor. Undergraduate Level

2023 **Fall: CS789 Advanced Topics in Computer Science**, *Enrollment 10*, SEI, 4.72/5.0.
Instructor. Graduate Level

Teaching at GSU

2021 **Spring: CSC4222/6222 Intro to Cybersecurity**, *Enrollment 55*, SEI, 4.5/5.0.
Instructor. Under/Graduate Level

2019 **Fall: CSC4520/6520 Design and Analysis of Algorithms**, *Enrollment 57*, SEI, 4.7/5.0.
Instructor. Under/Graduate Level

Student Advising

Current Graduate Students

2025 **Suprim Nakarmi**, *Ph.D. Student*, Advising.
University of Nevada, Las Vegas

2025 **Chahana Dahal**, *Ph.D. Student*, Advising.
University of Nevada, Las Vegas

2024 **An Huang**, *Ph.D. Student*, Advising.
University of Nevada, Las Vegas

2023 **Hongbi Jeong**, *Ph.D. Student*, Co-advising with Dr. Junggab Son.
University of Nevada, Las Vegas

Graduated Students

2024
2025 **Eunyoung Jang**, *M.S.*, Computer Science.
University of Nevada, Las Vegas

2023
2024 **Syed Shariq Ahmed**, *M.S.*, Computer Science.
University of Nevada, Las Vegas

Dissertation Committee

2024
2025 **Chol Park**, *Ph.D.*, Computer Science.
University of Nevada, Las Vegas

2023
2024 **Austin Janushan**, *M.S.*, Computer Science.
University of Nevada, Las Vegas

Professional Services

Editorship

Associate Editor	IEEE Networking Letters, 2024 - Present
Associate Editor	High-Confidence Computing, 2025 - Present
Associate Editor	IEEE Transactions on Neural Networks and Learning Systems (TNNLS), 2026 - Present
Guest Editor	MDPI Electronics

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 on Meta Computing (ICMC)

Reviewer

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

Academic Membership

Member	IEEE
	AAAI

Languages

Chinese	Native	*Mother Tongue*
English	Proficient	*Presentations and Lectures given in English*
Cantonese	Fluent	*Occasional practice with TVB*