HONGHUI XU

Personal Website: https://honghuixu.netlify.app
https://github.com/ahahnut ✉hxu16@student.gsu.edu ☎(470)-417-6213
📍Department of Computer Science, Georgia State University, Atlanta, GA 30302

EDUCATION BACKGROUND

Georgia State University, Altanta, GA **September 2019 - Present**

- **Major:** Computer Science; **Degree:** Doctor of Philosophy; **GPA:** 3.90/4.00
- **Supervisor:** Prof. Zhipeng Cai

University of Electronic Science and Technology of China, Chengdu, Sichuan **September 2015 - June 2019**

- **Major:** Computer Science; **Degree:** Bachelor of Engineering; **GPA:** 3.90/4.00

RESEARCH INTERESTS

- **Fundamental Theory of Machine Learning**
- **Applications of Deep Learning**
- **Privacy-Preserving Deep Learning**

TEACHING EXPERIENCES

Lab Instructor, Georgia State University **January 2023 - Present**

- **CSc 8230:** Secure and Private AI

Lab Instructor, Georgia State University **June 2022 - December 2022**

- **CSc 3210:** Computer Organization and Programming

Lab Instructor, Georgia State University **September 2020 - May 2022**

- **CSc 1301:** Principle Of Programming For Data Science I
- **CSc 1302:** Principle Of Programming For Data Science II

PUBLICATIONS

Journal Publications:

1. **H. Xu**, W. Li, D. Takebi, and Z. Cai, Privacy-Preserving Multimodal Sentiment Analysis[J]. *IEEE Transaction on Information Forensics and Security*, 2023. (Under Review)
2. **H. Xu**, W. Li, and Z. Cai, Analysis on methods to effectively improve transfer learning performance[J]. *Theoretical Computer Science (TCS)*, 2022.
3. **H. Xu**, Z. Cai, D. Takabi and W. Li, Audio-visual autoencoding for privacy-preserving video streaming[J]. *IEEE Internet of Things Journal (IoTJ)*, 2021, 9(3): 1749-1761. (Impact Factor: 9.936)
4. **H. Xu**, Z. Cai and W. Li, Privacy-Preserving Mechanisms for Multi-Label Image Recognition[J]. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 2022, 16(4): 1-21. (Impact Factor: 4.54)
5. **H. Xu**, Z. Cai, R. Li and W. Li, Efficient CityCam-to-Edge Cooperative Learning for Vehicle Counting in ITS[J]. *IEEE Transaction on Intelligent Transportation Systems (TITS)*, 2022, 23(9), 16600-16611. (Impact Factor: 2.534)
6. Z. Xiong, **H. Xu**, W. Li and Z. Cai, Multi-source adversarial sample attack on autonomous vehicles[J]. *IEEE Transactions on Vehicular Technology (TVT)*, 2021, 70(3): 2822-2835. (Impact Factor: 5.978)
7. Z. Cai, Z. Xiong, **H. Xu**, P. Wang, W. Li and Y. Pan, Generative adversarial networks: A survey toward private and secure applications[J]. *ACM Computing Surveys (CSUR)*, 2021, 54(6): 1-38. (Impact Factor: 10.282)

8. S. De, **H. Xu**, M. Bermudez-Edo, Z. Cai, Deep Generative Models in the Industrial Internet of Things: A Survey[J]. *IEEE Transaction on Industrial Informatics (TII)*, 2022, 18(9): 5728-5737. (Impact Factor: 10.215)
9. Z. Kang, **H. Xu**, B. Wang, H. Zhu and Z. Xu, Clustering with Similarity Preserving[J]. *Neurocomputing*, 2019, 365(6), 211-218. (Impact Factor: 5.719)
10. M. Li, **H. Xu** and Y. Deng, Evidential Decision Tree based on Belief Entropy[J]. *Entropy*, 21(9), 897.
11. **H. Xu** and Y. Deng, Dependent Evidence Combination based on Decision-Making Trial and Evaluation Laboratory Method[J]. *International Journal of Intelligent Systems (IJIS)*, 34(7), 1555-1571.
12. **H. Xu** and Y. Deng, Dependent Evidence Combination based on Shearman Coefficient and Pearson Coefficient[J]. *IEEE ACCESS*, 6, 2018.

Conference Publications:

1. **H. Xu**, Z. Cai and W. Li, Backdoor Attack on 3D Medical Image Segmentation[C]. *Information Processing in Medical Imaging (IPMI)*, 2023. (Under Review)
2. **H. Xu**, Z. Cai and W. Li, Overheard: Audio-based Integral Event Inference[C]. *International Joint Conference on Artificial Intelligence (IJCAI)*, 2023. (Under Review)
3. **H. Xu**, Z. Cai and W. Li, Which Option Is a Better Way to Improve Transfer Learning Performance?[C]. *International Conference on Combinatorial Optimization and Applications (COCOA)*, Springer, Cham, 2021: 61-74.
4. B. Xie, **H. Xu**, Z. Xiong, Y. Li and Z. Cai, A Self-Supervised Purification Mechanism for Adversarial Samples[C]. *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)*, 2022.

SERVICES

Reviewer of the following **Conferences:**

- 2021 IEEE Global Communcations Conference (GLOBECOM 2021)
- 2022 EAI International Conference on Wireless Internet Conference (EAI WiCON 2022)
- 32nd International Joint Conference on Artificial Intelligence (IJCAI 2023)
- 29th ACM SIGKDD Conference on Knowledge Discovery & Data Mining (KDD 2023)
- 2023 IEEE/CIC International Conference on Communications in China (ICCC 2023)
- ICML 2023 Workshop AdvML-Frontiers

Reviewer of the following **Journals:**

- IEEE Transaction on Industrial Informatics (TII) (Impact Factor: 10.215)
- IEEE Transaction on Vehicle Technology (TVT) (Impact Factor: 5.978)
- IEEE Transaction on Computational Social Systems (TCSS) (Impact Factor: 5.14)
- IEEE Internet of Things Journal (IoTJ) (Impact Factor: 9.936)
- IEEE Transactions on Wireless Communication (TWC) (Impact Factor: 7.016)
- International Journal of Computer Vision (Impact Factor: 7.41)
- Neurocomputing (Impact Factor: 5.719)
- Scientific Reports (Impact Factor: 4.996)
- Computational Intelligence and Neuroscience (Impact Factor: 3.633)
- Computer Communications (ComCom) (Impact Factor: 3.167)

INVITED TALKS

- “Privacy-Preserving Multimodal Sentiment Analysis”, UESTC, September 15, 2022, online.
- “Privacy-Preserving Mechanisms on Data-Driven Deep Learning Applications”, VCU, Feburary 3, 2023, online.

HONORS AND FELLOWSHIPS

- Outstanding Research Award, Department of Computer Science, GSU, Spring 2022.
- Brains & Behavior Fellowship, Neuroscience Institute, GSU, 2021 and 2022.