HONGHUI XU

Personal Website: https://honghuixuhenry.github.io
https://github.com/honghuixuhenry ✉hxu16@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:** 3.89/4.00

RESEARCH INTERESTS

- **Secure and Private AI**
- **Deep Learning Applications**

TEACHING EXPERIENCES

Teaching Assistant, Georgia State University — **June 2023 - August 2023**

- **CSc 8222:** Network Security (Class Size: 20)

  I conduct labs on network security, design assignments and projects, grade assignments, projects and exams.

Teaching Assistant, Georgia State University — **January 2023 - May 2023**

- **CSc 8230:** Secure and Private AI (Class Size: 25)

  I design hands-on labs to familiarize students with private and secure AI-related tools and packages, demonstrate hands-on labs and mini projects, and grade labs and projects.

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

- **CSc 3210:** Computer Organization and Programming (Class Size: 50)

  I conduct weekly labs on Assembly language programming for x86 architecture and grade labs and exams.

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

- **CSc 1301:** Principle Of Programming For Data Science I (Class Size: 50)
- **CSc 1302:** Principle Of Programming For Data Science II (Class Size: 50)

  I conduct weekly labs in JAVA and grade labs and assignments.

PUBLICATIONS

Ongoing Research Papers:

1. **H. Xu**, W. Li, and Z. Cai, Privacy Enhanced Online Multi-Sensor Data Prediction with Certified Performance Influence, 2023. (Expected Submission to IEEE ICDE).
2. J. Qian, **H. Xu**, Z. Chen, H. Li, Q. Gao, and Y. Huo, Computation Offloading of Multiple DAG Tasks in Mobile Edge Computing, *Sensors*, 2023. (Under Review)

3. **H. Xu**, W. Li, D. Takebi, and Z. Cai, Privacy-Preserving Multimodal Sentiment Analysis[J]. *IEEE Transaction on Information Forensics and Security (TIFS)*, 2023. (Major Revision)

4. **H. Xu**, Z. Cai and W. Li, Overheard: Audio-based Integral Event Inference[C]. *ACM International Conference on Web Search and Data Mining (WSDM)*, 2023. (Under Review)

Published Journal Papers:

1. B. Xie, **H. Xu**, Y. Joe, D. Seo, and Z. Cai, Lightweight Super-Resolution Model for Complete Model Copyright Protection. *Tsinghua Science and Technology (TST)*, 2023. (Accepted)

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 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**)

4. **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**)

5. **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**)

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**) (**Total Cites: 200**)

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**) (**Total Cites: 55**)

10. M. Li, **H. Xu** and Y. Deng, Evidential Decision Tree based on Belief Entropy[J]. *Entropy*, 21(9), 897. (**Impact Factor: 2.738**) (**Total Cites: 82**)

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. (**Impact Factor: 8.993**) (**Total Cites: 59**)

12. **H. Xu** and Y. Deng, Dependent Evidence Combination based on Shearman Coefficient and Pearson Coefficient[J]. *IEEE ACCESS*, 6, 2018. (**Impact Factor: 3.476**) (**Total Cites: 193**)

Published Conference Papers:

1. **H. Xu**, Z. Cai, Z. Xiong and W. Li, Backdoor Attack on 3D Medical Image Segmentation[C]. *IEEE International Conference on Data Mining (ICDM)*, 2023. (Accept) (**9.77%**)

2. **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.

3. B. Xie, **H. Xu**, Z. Xiong, Y. Li and Z. Cai, A Self-Supervised Purification Mechanism for Adversarial Samples[C]. *2022 IEEE Smart Data (SmartData)*, 2022.

PROFESSIONAL ACTIVITIES

Reviewer of the following **Conferences:**

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

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)

Mentor of the following **Capstone Projects:**

- “Privacy-Preserving Multimodal Sentiment Analysis”, Hanyang University, South Korea. (August 2022 – May 2023)
- “Efficient CityCam-to-Edge Cooperative Learning for Vehicle Counting in ITS”, Hanyang University, South Korea. (August 2021 – May 2022)

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, 2022, and 2023.