CURRICULUM VITAE (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 30303

EDUCATION BACKGROUND

- **Ph.D.**, Georgia State University, 2019 - expected May 2024

  Major: Computer Science; Supervisor: Dr. Zhipeng Cai; Co-Supervisor: Dr. Wei Li

- **B.S.**, University of Electronic Science and Technology of China, 2015 - 2019

  Major: Computer Science & Technology

PROFESSIONAL CREDENTIAL

- **Research Assistant**, Department of Computer Science, Georgia State University, 2019 - Present
- **Teaching Assistant**, Department of Computer Science, Georgia State University, 2019 - Present

RESEARCH INTERESTS

- **Data Security and Privacy**
- **Trustworthy Artificial Intelligence**
- **Deep Learning**
- **Internet of Things**

TEACHING EXPERIENCES

Teaching Assistant, Georgia State University

- **CSc 8222** Network Security: Summer 23
- **CSc 8230** Secure and Private AI: Spring 23
- **CSc 3210** Computer Organization and Programming: Summer 22, Fall 22
- **CSc 1302** Principle Of Programming For Data Science II: Spring 22, Fall 21, Spring 21, Fall 20

HONORS AND AWARDS

- **Outstanding Research Award (The Solo One):** 500$, offered by Department of Computer Science at GSU, Spring 2022.
- **Brains & Behavior Fellowship**: 22,000$/yr, offered by Neuroscience Institute at GSU, 2021, 2022, and 2023.
- **Best Paper Award (The Solo One)**: "A Self-Supervised Purification Mechanism for Adversarial Samples", by B. Xie, **H. Xu**, Z. Xiong, Y. Li and Z. Cai, *2022 IEEE Smart Data (SmartData)*, August, 2022.

PUBLICATIONS

Ongoing Research Papers:

1. **H. Xu**, W. Li, D. Takebi, and Z. Cai, Privacy-Preserving Multimodal Sentiment Analysis[J]. *ACM Transactions on Privacy and Security (TOPS)*, 2023. (Under Review)
2. **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)(**IF: 3.515**)
2. **H. Xu**, Z. Cai and W. Li, Privacy-Preserving Mechanisms for Multi-Label Image Recognition. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 2022, 16(4): 1-21.(**IF: 4.54**)
3. **H. Xu**, Z. Cai, R. Li and W. Li, Efficient CityCam-to-Edge Cooperative Learning for Vehicle Counting in ITS. *IEEE Transaction on Intelligent Transportation Systems (TITS)*, 2022, 23(9), 16600-16611.(**IF: 2.534**)
4. **H. Xu**, Z. Cai, D. Takabi and W. Li, Audio-Visual Autoencoding for Privacy-Preserving Video Streaming. *IEEE Internet of Things Journal (IoTJ)*, 2021, 9(3): 1749-1761.(**IF: 9.936**)
5. **H. Xu**, W. Li, and Z. Cai, Analysis on Methods to Effectively Improve Transfer Learning Performance. *Theoretical Computer Science (TCS)*, 2022, 940: 90-107.(**IF: 1.002**)
6. Z. Xiong, **H. Xu**, W. Li and Z. Cai, Multi-Source Adversarial Sample Attack on Autonomous Vehicles. *IEEE Transactions on Vehicular Technology (TVT)*, 2021, 70(3): 2822-2835.(**IF: 5.978**)
7. S. De, **H. Xu**, M. Bermudez-Edo, Z. Cai, Deep Generative Models in the Industrial Internet of Things: A Survey. *IEEE Transaction on Industrial Informatics (TII)*, 2022, 18(9): 5728-5737.(**IF: 10.215**)
8. 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)*, 2021, 54(6): 1-38.(**IF: 10.282**) (**Cites: 217**)
9. Z. Kang, **H. Xu**, B. Wang, H. Zhu and Z. Xu, Clustering with Similarity Preserving. *Neurocomputing*, 2019, 365(6): 211-218.(**IF: 5.719**) (**Cites: 57**)
10. M. Li, **H. Xu** and Y. Deng, Evidential Decision Tree based on Belief Entropy. *Entropy*, 2019, 21(9): 897.(**IF: 2.738**) (**Cites: 85**)
11. **H. Xu** and Y. Deng, Dependent Evidence Combination based on Decision-Making Trial and Evaluation Laboratory Method. *International Journal of Intelligent Systems*, 2019, 34(7): 1555-1571.(**IF: 8.993**) (**Cites: 61**)
12. **H. Xu** and Y. Deng, Dependent Evidence Combination based on Shearman Coefficient and Pearson Coefficient. *IEEE ACCESS*, 2018, 6: 11634-11640.(**IF: 3.476**) (**Cites: 197**)

Published Conference Papers:

1. **H. Xu**, Z. Cai, Z. Xiong and W. Li, Backdoor Attack on 3D Grey Image Segmentation. *IEEE International Conference on Data Mining (ICDM)*, 2023. (Acceptance Ratio: 9.37%)
2. **H. Xu**, Z. Cai and W. Li, Which Option Is a Better Way to Improve Transfer Learning Performance?. *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. *2022 IEEE Smart Data (SmartData)*, 2022: 501-509. **(Best Paper Award)**

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.

PROFESSIONAL ACTIVITIES

- Brain & Behavior Fellow in Neuroscience Institute at GSU
- Reviewer of the conferences: NIPS 2023, ICML 2023, KDD 2023, AAAI 2023, IJCAI 2023, ICCC 2023
- Reviewer of the journals: IEEE TII, IEEE TVT, IEEE TCSS, IEEE IoTJ, IEEE TWC
- Mentor of the capstone projects: "Privacy-Preserving Multimodal Sentiment Analysis", and "Efficient CityCam-to-Edge Cooperative Learning for Vehicle Counting in ITS", cooperated with Hanyang University