CURRICULUM VITAE (HONGHUI XU)

Personal Website: https://honghuixuhenry.github.io

https://github.com/honghuixuhenry ✉hxu10@kennesaw.edu ☎(470)-417-6213

📍Department of Information Technology, Kennesaw State University, Marietta, GA 30060

EDUCATION BACKGROUND

- **Computer Science Ph.D., Georgia State University, 2019 - 2023**
- **Computer Science & Technology B.S., University of Electronic Science and Technology of China, 2015 - 2019**

PROFESSIONAL CREDENTIAL

- **Assistant Professor, Department of Information Technology, Kennesaw State University, 01/01/2024 - Present**
- **Research Assistant, Department of Computer Science, Georgia State University, 08/14/2019 - 12/31/2023**
- **Teaching Assistant, Department of Computer Science, Georgia State University, 08/14/2019 - 12/31/2023**

RESEARCH INTERESTS

- **Data Security and Privacy in AI**
- **Trustworthy AI**
- **Responsible AI**
- **Internet of Things**

TEACHING EXPERIENCES

Assistant Professor, Kennesaw State University

- **IT 7123 Business Intelligence: Fall 24**
- **CYBR 4423 Unix/Linux Administration: Spring 24**

Teaching Assistant, Georgia State University

- **CSc 8228 Privacy Aware Computing: Fall 23**
- **CSc 8222 Network Security: Summer 23**
- **CSc 8230 Secure and Private AI: Spring 23**

Lab Instructor, Georgia State University

- **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

- **First-Year Scholar: 1,000$, offered by KSU, Fall 2024.**
- **Summer Research Camp Fellowship: 10,000$, offered by KSU and CCSE in KSU, Summer 2024.**
- **Outstanding Research Award (Single Recipient): 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 (Single Recipient): "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)**

Published Journal Papers:

1. **H. Xu, Z. Cai, L. Ma, Y. Li, D. Seo, and W. Li, Overheard: Audio-based Integral Event Inference. *ACM Journal of Data and Information Quality (JDIQ)*, 2024. (Accept)**
2. **H.Xu, Y. Li, O. Balogun, S. Wu, Y. Wang, and Z. Cai, Security Risks Concerns of Generative AI in the IoT. *IEEE Internet of Things Magazine (IoTM)*, 7(3), 62-672024.**
3. **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. (IF: 3.515)**
4. **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)**
5. **H. Xu, Z. Cai, R. Li and W. Li, Efficient CityCam-to-Edge Cooperative Learning for Vehicle Counting in ITS. *IEEE Transactions on Intelligent Transportation Systems (TITS)*, 2022, 23(9), 16600-16611.(IF: 2.534)**
6. **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)**
7. **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)**
8. **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)**
9. **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)**
10. **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)**
11. **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)**
12. **M. Li, H. Xu and Y. Deng, Evidential Decision Tree based on Belief Entropy. *Entropy*, 2019, 21(9): 897.(IF: 2.738) (Cites: 85)**
13. **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)**
14. **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, W. Li, S. Wu, L. Zhao, and Z. Cai, APOLLO: Differential Private Online Multi-Sensor Data Prediction with Certified Performance. *IEEE International Conference on Data Mining (ICDM)*, 2024. (Acceptance Ratio: 9.37%)**
2. **D. Zheng, S. Cao, H. Xu, and X. Cao, Deploying Security-Aware Service Function Chains with Asymmetric Dedicated Protection. *IEEE International Conference on Communications (ICC)*, 2024. (Accepted)**

3. **D. Zheng, X. Liu, W. Tang, H. Xu, and X. Cao, Cost Optimization in Security-Aware Service Function Chain Deployment with Diverse Vendors. *IEEE Global Communications Conference (GLOBECOM)*, 2023. (Accepted)**

4. **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%)**

5. **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.**

6. **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

- **Guest Editor: IET Communications**
- **Guest Editor: Tsinghua Science and Technology**
- **Track Chair: MSN 2024**
- **TPC Member: WASA 2024**
- **Session Chair: SDM 2024**
- **Program Committee Member: ICML 2024, NIPS 2024, COCOON 2024, AAAI 2024, SDM 2024, ICMC 2023**
- **Reviewer of the conferences: CVPR 2024, ICLR 2024, NIPS 2023, ICML 2023, KDD 2023, AAAI 2023, IJCAI 2023**
- **Reviewer of the journals: IEEE TII, IEEE TVT, IEEE TCSS, IEEE IoTJ, IEEE TWC, IEEE TMC**