

# XI LI

she/her/hers | 814-777-6667 | UH4151, 1402 Tenth Avenue South, Birmingham, AL, 35294

[XiLiUAB@uab.edu](mailto:XiLiUAB@uab.edu)  $\diamond$  [lixi1994.github.io](https://github.com/lixi1994)  $\diamond$  [Google Scholar](#)

## RESEARCH INTERESTS

---

My research interests reside in **trustworthy AI**, aiming to assess and address the broader ethical concerns surrounding ML models, such as **robustness**, **privacy**, **fairness**, and **interpretability**. My research vision is to bridge AI with **interdisciplinary** research by developing trustworthy and reliable AI systems that advance technology and serve the greater social good.

## EMPLOYMENT

---

<b>Tenure-Track Assistant Professor</b> Department of Computer Science University of Alabama at Birmingham	Aug. 2024 - present
<b>Machine Learning Engineer Intern</b> Modern Recommendation System Team Meta	May 2024 - August 2024

## EDUCATION

---

<b>The Pennsylvania State University</b> Ph.D. in Computer Science and Engineering Advisor: Dr. George Kesidis and Dr. David Miller M.S. in Computer Science and Engineering	State College, PA Aug. 2018 - July 2024 Aug. 2016 - July 2018
<b>The Southeast University</b> B.E. in Electrical Engineering	Nanjing, China Aug. 2012 - June 2016

## PUBLICATIONS

---

- X. Bi, **X. Li**. *Securing Federated Learning Against Novel and Classic Backdoor Threats During Foundation Model Integration*. under review.
- **X. Li**, Y. Zhang, R. Lou, C. Wu, J. Wang. *Chain-of-Scrutiny: Detecting Backdoor Attacks for Large Language Models*. under review.
- **X. Li**, J. Wang. *Position Paper: Assessing Robustness, Privacy, and Fairness in Federated Learning Integrated with Foundation Models*. under review.
- G. Yang, **X. Li**, H. Wang, D. J. Miller, G. Kesidis. *CEPA: Consensus Embedded Perturbation for Agnostic Detection and Inversion of Backdoors*. under review.
- **X. Li**, C. Wu, J. Wang. *Vulnerabilities of Foundation Model Integrated Federated Learning Systems Under Adversarial Threats*. under review.
- **X. Li**, Z. Xiang, D. J. Miller, G. Kesidis. *Backdoor Mitigation by Correcting Distribution of Neural Activation*. Neurocomputing, 2024.
- **X. Li**, D. J. Miller, Z. Xiang, G. Kesidis. *BIC-based Mixture Model Defense against Data Poisoning Attacks on Classifiers: A Comprehensive Study*. IEEE Transactions on Knowledge and Data Engineering (TKDE), 2024.
- **X. Li**, C. Wu, J. Wang. *Unveiling Backdoor Risks Brought by Foundation Models in Heterogeneous Federated Learning*. The Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD), 2024.
- **X. Li**, S. Wang, R. Huang, M. Gowda, G. Kesidis. *Temporal-Distributed Backdoor Attack Against Video Based Action Recognition*. AAAI, 2024.
- **X. Li**, S. Wang, C. Wu, H. Zhou, J. Wang. *Backdoor Threats from Compromised Foundation Models to Federated Learning*. FL@FM-NeurIPS'23.
- **X. Li**, D. J. Miller, Z. Xiang, G. Kesidis. *A BIC-based Mixture Model Defense against Data Poisoning Attacks on Classifiers*. IEEE International Workshop on Machine Learning for Signal Processing (MLSP), 2023.

- **X. Li**, D. J. Miller, Z. Xiang, G. Kesidis. *Test-Time Detection of Backdoor Triggers of Poisoned Deep Neural Networks*. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2022.
- Z. Xiang, D. J. Miller, S. Chen, **X. Li**, G. Kesidis. *Detecting Backdoor Attacks Against Point Cloud Classifiers*. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2022.
- Z. Xiang, D. J. Miller, S. Chen, **X. Li**, G. Kesidis. *A Backdoor Attack against 3D Point Cloud Classifiers*. ICCV, 2021.

## TEACHING EXPERIENCE

---

- **Instructor** UAB  
 CS652/752 Advanced Algorithms and Applications 2025 Spring  
 CS685/785 Foundation of Data Science 2024 Fall
- **Teaching Assistant** PSU  
 CMPSC465 Data Structures and Algorithms 2021 Spring  
 CMPSC/MATH 451 Numerical Computations 2019 Fall - 2024 Spring  
 CMPEN/EE 455 Digital Image Processing I 2018 Fall

## PROFESSIONAL SERVICE

---

### Conference Program Committee:

- Association for the Advancement of Artificial Intelligence (AAAI), 2025
- SIAM International Conference on Data Mining (SDM), 2024

### Conference Reviewer:

- Artificial Intelligence and Statistics (AISTATS), 2025
- Association for the Advancement of Artificial Intelligence (AAAI), 2025
- International Conference on Learning Representations (ICLR), 2025
- IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2022-2025
- SIGKDD Conference on Knowledge Discovery and Data Mining (KDD), 2023, 2024
- IEEE/CVF Computer Vision and Pattern Recognition Conference (CVPR), 2024, 2025
- Conference on Neural Information Processing Systems (NeurIPS), 2024
- Conference on Language Modeling (COLM), 2024

### Journal Reviewer:

- Computers and Security (C&S), 2024
- IEEE Transactions on Circuits and Systems for Video Technology (TCSVT), 2024

### Student Volunteer:

- Conference on Neural Information Processing Systems (NeurIPS), 2023