Mengdie Huang (Maggie)

Postdoctoral Research Associate, Purdue University

mengdiehuang.github.io | huan1932@purdue.edu | maggiehuang2310@gmail.com

RESEARCH AREAS

My research focuses on the security and robustness of ML models in critical domains. My overarching goal is to build resilient, trustworthy AI architectures by advancing core research thrusts:

- **Certified Robustness and Vulnerability Assessment:** Scalable certification for provable adversarial robustness guarantees, and realizable evasion attacks to expose vulnerabilities across network and image domains.
- **Robust Transfer Learning and Downstream Adaptation:** Parameter-efficient training and representation distillation for robust downstream adaptation of foundation models against cross-domain threats.
- **Security of Multimodal Foundation Models:** Hardening vision-language models against adversarial attacks and data extraction, with a focus on membership inference and robust VLM adaptation.
- **Adversarial Robustness in Distributed AI:** Securing federated and decentralized learning against evasion attacks and developing self-evolving defense mechanisms for distributed architectures.

EDUCATION

Purdue University, West Lafayette, IN — Sep 2022 – Jun 2025
Visiting Ph.D. in Computer Science (Advisor: Dr. Elisa Bertino)

Xidian University, Xi'an, China — Sep 2019 – Jun 2025
Ph.D. in Cyberspace Security (Advisor: Dr. Xiaofeng Chen)

Communication University of China, Beijing, China — Sep 2017 – Jun 2019
Master in Electronics and Communication Engineering
Bachelor in Radio and Television Editing

Huai'an University, Huai'an, China — Sep 2013 – Jun 2017
Bachelor in Communication Engineering

WORK EXPERIENCE

Postdoctoral Research Associate, Purdue University, West Lafayette, IN — Jul 2025 – Present
Advisors: Dr. Elisa Bertino and Dr. Ninghui Li
Research: Robustness of large language and vision foundation models.

Visiting Scholar (Ph.D. Student), Purdue University, West Lafayette, IN — Sep 2022 – Jun 2025
Advisor: Dr. Elisa Bertino
Research: Robustness of deep learning-based network traffic analysis systems.

Research Assistant, Xidian University — Sep 2019 – Aug 2022
Advisor: Dr. Xiaofeng Chen
Research: Robustness of deep learning-based image classification systems.

Research Intern, National Radio and Television Administration — May 2019 – Jul 2019
Research: Secure video coding standards.

PUBLICATIONS

[*] *Equal contribution* [†] *Mentored student*

Journal Papers

[1] TDSC 2026 — TriXfer: Triple-Cross Transfer Attack on Vision Transformer–Adapted Downstream Classifiers.
Mengdie Huang, Yingjun Lin[†], Ninghui Li, Xiaofeng Chen, Elisa Bertino.
In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2026.

[2] TDSC 2025 CARD: Robustness-Preserving Transfer Learning for Network Intrusion Detection via Contrastive Adversarial Representation Distillation.
Mengdie Huang, Yingjun Lin[†], Ninghui Li, Xiaofeng Chen, Elisa Bertino.
In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2025, pp. 5134-5151.

[3] TOPS 2025 Dimensional Robustness Certification for Deep Neural Networks in Network Intrusion Detection Systems.
Mengdie Huang, Yingjun Lin[†], Xiaofeng Chen, Elisa Bertino.
In *ACM Transactions on Privacy and Security (TOPS)*, 2025, pp. 1-33.

[4] TIOT 2024 ARIoTEDef: Adversarially Robust IoT Early Defense System based on Self-evolution against Multi-step Attacks.
Mengdie Huang, Hyunwoo Lee, Ashish Kundu, Xiaofeng Chen, Anand Mudgerikar, Ninghui Li, Elisa Bertino.
In *ACM Transactions on Internet of Things (TIOT)*, 2024, 5(3): 1-34.

[5] JIT 2019 Sparse Selective Encryption for HEVC 4K Video Using Spatial Error Spread.
Mengdie Huang, Cheng Yang, Hao Li, Jian Shen.
In *Journal of Internet Technology (JIT)*, 2019, 20(5): 1589-1600.

Conference Papers

[1] TrustCom 2024 **(Best Paper)** MARS: Robustness Certification for Deep Network Intrusion Detectors via Multi-Order Adaptive Randomized Smoothing.
Mengdie Huang, Yingjun Lin[†], Xiaofeng Chen, Elisa Bertino.
In *IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom)*, 2024, pp. 767-774.

[2] AsiaCCS 2023 Boost Off/On-Manifold Adversarial Robustness for Deep Learning with Latent Representation Mixup.
Mengdie Huang, Yi Xie, Xiaofeng Chen, Jin Li, Changyu Dong, Zheli Liu, Willy Susilo.
In *ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, 2023, pp. 716-730.

[3] CIC 2023 A Pro-Active Defense Framework for IoT Systems.
Elisa Bertino, Hyunwoo Lee, **Mengdie Huang**, Charalampos Katsis, Zilin Shen, Bruno Ribeiro, Daniel De Mello, Ashish Kundu.
In *IEEE International Conference on Collaboration and Internet Computing (CIC)*, 2023, pp. 125-132.

[4] ESORICS 2022 GAME: Generative-based Adaptive Model Extraction Attack.
Yi Xie, **Mengdie Huang**, Xiaoyu Zhang, Changyu Dong, Willy Susilo, Xiaofeng Chen.
In *European Symposium on Research in Computer Security (ESORICS)*, 2022, pp. 570-588.

[5] ICCT 2018 Selective Encryption of H.264/AVC based on Block Weight Model.
Mengdie Huang, Cheng Yang, Yuan Zhang.
In *IEEE International Conference on Communication Technology (ICCT)*, 2018, pp. 1368-1373.

[6] ICCA 2016 An Effective Scheme for Provable Data Possession.
Shanyue Bu, **Mengdie Huang**, Kun Yu.
In *International Conference on Intelligent Control and Computer Application (ICCA)*, 2016, pp. 344-348.

Papers Under Submission

[1] 2027 Local Knowledge for Global Impact: Evasion Attack Against Vertical Federated Learning.
Chen Peng[*†], **Mengdie Huang**[*], Ninghui Li, Elisa Bertino. (joint first authors)

[2] 2027 GRAFT: Adversarially Robust Transfer Learning for Graphs Under Structural Data Scarcity.
Mir Imtiaz Mostafiz[*†], **Mengdie Huang**[*], Imtiaz Karim, Elisa Bertino. (joint first authors)

[3] 2027 Local Nonlinear Substitution for Bounding Activation Functions.
Zhongkui Ma, **Mengdie Huang**, Guangdong Bai, Elisa Bertino, Zihan Wang.

[4] 2027 CARE: Robust Transformer-based Network Intrusion Detection via Consistency-aware Attention-Representation Enhancement.
MD Shamsul Kaonain*†, **Mengdie Huang***, Imtiaz Karim, Elisa Bertino. (joint first authors)

[5] 2027 EntroDelta: An Error-Bounded, Data-Free Compression Framework for Model Storage.
Yani Liu†, Feng Zhang, Yu Zhang, **Mengdie Huang**, Elisa Bertino, Xiaoyong Du.

Books

[1] Book 2024 Searchable Encryption.
Xiaofeng Chen, **Mengdie Huang**, etc.
In *Science Press, China Science Publishing & Media Co., Ltd.*, 2024.

[2] Book 2023 Cloud Computing Security (2nd Edition).
Xiaofeng Chen, **Mengdie Huang**, etc.
In *Science Press, China Science Publishing & Media Co., Ltd.*, 2023.

GRANT WRITING EXPERIENCE

Core Author of the NSF proposal, Purdue – West Lafayette, IN — Aug 2026
Model Robustness, Ownership, and Privacy Preserving in Transfer learning

Author of the Amazon research proposal, Purdue – West Lafayette, IN — May 2026
Formal and Drift-Aware Containment of Agents in Regulated Systems

Core Author of the Cisco research proposal, Purdue – West Lafayette, IN — Mar 2023
Detection of GenAI Generated Malware Variants and Sandbox Evasion using GenAI
Awarded $\$150,000$ by Cisco Research

INVITED TALKS

CS 59200-AAS, Department of Computer Science, Purdue University — Feb 2026
Robustness in Machine Learning – From Adversarial Robustness to LLM Safety

CS 59200-AAS, Department of Computer Science, Purdue University — Feb 2026
Robustness in Machine Learning – From Adversarial Robustness to Certified Robustness

SPARKS Seminar, NSF AI-EDGE Institute — Dec 2025
Robustness Certification for Deep Neural Networks in Network Intrusion Detection Systems

School of AI and Computer Science, Shaanxi Normal University — Oct 2025
AI Security: Adversarial Attacks and Robustness in Deep Learning

TEACHING

Teaching Assistant, Xidian University — Jul 2021 – Jul 2022
Course: Distributed Computing
Instructor: Dr. Miroslaw Kutylowski, School of Cyber Engineering

Teaching Assistant, Xidian University — Sep 2020 – Jan 2021
Course: Probability Theory and Mathematical Statistics
Instructor: Dr. Jianfeng Wang, School of Cyber Engineering

Reading Group Instructor, Communication University of China — Sep 2017 – Jun 2019
Topic: Principles and Practices of H.264/H.265 Secure Video Coding
Format: Organized and led a reading group for undergraduate students

MENTORING

Chen Peng, Ph.D. Student, Purdue University — Feb 2026 – Present
Research: Adversarial machine learning in multimodal domain.

Md Shamsul Kaonain, Ph.D. Student, Purdue University — Jun 2025 – Present
Research: Network Traffic Analysis with deep learning.

Yani Liu, Visiting Ph.D. Student, Purdue University — Mar 2025 – Mar 2026
Research: Data compression in machine learning.

Mir Imtiaz Mostafiz, Ph.D. Student, Purdue University — Jan 2025 – Present
Research: Robustness of graph neural networks.

Yuchen Jason Hu, Undergraduate Student, Purdue University — Feb 2024 – Present
Research: Robust Transfer Learning.

Yingjun Link Lin, Undergraduate Student, Purdue University — Nov 2022 – Dec 2023
Research: Adversarial attack and robustness in deep learning.

Yundong Liu, PhD student, Xidian University — Sep 2022 - Jun 2025
Research: Network Traffic Analysis.

Wei Li, Undergraduate student, Xidian University — Dec 2019 - Jun 2020
Research: Adversarial attack with Fast Gradient Sign Method.

Fengdong Li, Undergraduate student, Communication University of China — Sep 2018 - Jun 2019
Research: Selective Encryption for HEVC Video.

Yujie Wang, Undergraduate student, Communication University of China — Sep 2018 - Jun 2019
Research: Selective Encryption for HEVC Video.

PROFESSIONAL SERVICE

Journal Services

Reviewer, IEEE Transactions on Dependable and Secure Computing (TDSC) — 2025 – Present
Reviewer, IEEE Transactions on Networking (TNET) — 2025 – Present
Reviewer, IEEE Transactions on Parallel and Distributed Systems (TPDS) — 2025 – Present
Reviewer, IEEE Transactions on Information Forensics & Security (TIFS) — 2024 – Present
Reviewer, IEEE Transactions on Neural Networks and Learning Systems (TNNLS) — 2024 – Present
Reviewer, ACM Transactions on Multimedia Computing, Communications, Applications (TOMM) — 2024 – Present
Reviewer, Computers and Electrical Engineering (CEE) — 2024 – Present
Reviewer, Computing and Informatics (CAI) — 2024 – Present
Reviewer, American Journal of Artificial Intelligence (AJAI) — 2024 – Present
Reviewer, ACM Computing Surveys — 2023 – Present
Reviewer, IEEE Transactions on Knowledge and Data Engineering (TKDE) — 2022 – Present
Reviewer, Telecommunication Systems (TELS) — 2021 – Present
Reviewer, Computer Standards & Interfaces (CSI) — 2021 – Present
Reviewer, Connection Science — 2020 – Present
Reviewer, IEEE Transactions on Circuits and Systems for Video Technology (TCSVT) — 2019 – Present

Conference Services

PC Member, IEEE International Conference on Parallel and Distributed Systems (ICPADS) — 2026
Artifact Evaluation Committee, ACM Conference on Computer and Communications Security (CCS) — 2025, 2026
Artifact Evaluation Committee, Network and Distributed System Security Symposium (NDSS) — 2026
Reviewer, International Conference on Data Security and Privacy Protection (DSPP) — 2024, 2025
Reviewer, Annual Computer Security Applications Conference (ACSAC) — 2024
Reviewer, European Symposium on Research in Computer Security (ESORICS) — 2021, 2024, 2025

Reviewer, ACM Conference on Data and Application Security and Privacy (CODASPY)	2023, 2024, 2025
Reviewer, International Conference on Machine Learning for Cyber Security (ML4CS)	2022
Reviewer, Information Security Conference (ISC)	2022
Reviewer, International Conference on Information and Communications Security (ICICS)	2021
Sub-Reviewer, IEEE Symposium on Security and Privacy (S&P)	2025, 2026
Sub-Reviewer, ACM Conference on Computer and Communications Security (CCS)	2025
Sub-Reviewer, USENIX Security Symposium (USENIX Security)	2026

HONORS & AWARDS

Awarded Peer Reviewer, IEEE Transactions on Dependable and Secure Computing (TDSC)	2025
Awarded Peer Reviewer, IEEE Transactions on Knowledge and Data Engineering (TKDE)	2025
Best Paper Award, IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom)	2024
Doctoral Academic Scholarship, Xidian University	2019 – 2022
Graduate Academic Scholarship, Communication University of China	2017 – 2019
Undergraduate Academic Scholarship, Huai'an University	2013 – 2017

REFERENCES

Dr. Elisa Bertino, Department of Computer Science, West Lafayette, IN	Purdue University
Dr. Ninghui Li, Department of Computer Science, West Lafayette, IN	Purdue University