Mengdie Huang

Visiting Ph.D., Purdue University

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

Lawson Computer Science Building, 305 N University St, West Lafayette, IN 47907

RESEARCH INTEREST

My research interests span **machine learning security**. I have been focusing on the robustness of deep neural networks and large language models against adversarial attacks, transfer attacks, and distribution shifts, with particular emphasis on robust training and certified defenses.
I have a strong background in deep learning, including techniques like manifold learning, randomized smoothing, transfer learning, contrastive learning, knowledge distillation, parameter-efficient fine-tuning, and unlearning, applied to both image-domain, text-domain, and network traffic-domain prediction and generation tasks.

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
Thesis: *Research on Key Techniques for Adversarial Robustness of Deep Neural Networks*.
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

Huaiyin Institute of Technology, Huai'an, China — Sep 2013 – Jun 2017
Bachelor in Communication Engineering

PUBLICATIONS

Papers Published

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

[2] **Mengdie Huang**, Yingjun Lin, Xiaofeng Chen, Elisa Bertino*. Dimensional Robustness Certification for Deep Neural Networks in Network Intrusion Detection Systems[J]. *ACM Transactions on Privacy and Security (TOPS)*, 2025.

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

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

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

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

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

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

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

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

Papers Under Review

[1] **Mengdie Huang**, Yingjun Lin, Ninghui Li, Elisa Bertino. TripleCross-BTA: Black-Box Transfer Attack against Downstream Models Derived from Vision Foundation Models. *Under R2 Review of ACM Conference on Computer and Communications Security*, 2025.

[2] Yundong Liu, **Mengdie Huang**, Meixia Miao. Network traffic classification techniques based on deep learning: A Survey. *Under R2 Review of Chinese Journal of Computers*, 2025.

Book

[1] Xiaofeng Chen*, **Mengdie Huang**, etc. Cloud Computing Security (2nd Edition). *Science Press. China Science Publishing & Media Co., Ltd.* 2023. ISBN: 9787030762856.

GRANT WRITING EXPERIENCE

Author of the NSF proposal (as student), Purdue – West Lafayette, IN Feb 2025

Model Robustness, Ownership, and Privacy Preserving in Transfer learning

Author of the proposal (as student), Purdue – West Lafayette, IN Mar 2023

Detection of GenAI Generated Malware Variants and Sandbox Evasion using GenAI,
Awarded $150,000$ by Cisco Research

ACADEMIC SERVICE

Journal Reviewer

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

Conference Reviewer

- ACM Conference on Computer and Communications Security (CCS): 2025

- IEEE Symposium on Security and Privacy (SP): 2025
- International Conference on Data Security and Privacy Protection (DSPP): 2024, 2025
- Annual Computer Security Applications Conference (ACSAC): 2024
- European Symposium on Research in Computer Security (ESORICS): 2021, 2024, 2025
- ACM Conference on Data and Application Security and Privacy (CODASPY): 2023, 2024, 2025
- International Conference on Machine Learning for Cyber Security (ML4CS): 2022
- Information Security Conference (ISC): 2022
- International Conference on Information and Communications Security (ICICS): 2021

Artifact Evaluation Committee Member

- ACM Conference on Computer and Communications Security (CCS): 2025

PROJECTS

Pro-Active Attack Management for Edge Computing Security, West Lafayetter, IN — Nov 2022 - Dec 2023

Developed a robust LSTM-based network intrusion detection system to defend against cyber chain attacks.
Sponsor: Cisco Systems, Inc.

Universal and Efficient 4K Video Protection Technology Supporting Coding Standard Extension, Beijing, China — Jun 2018 - Jun 2019

Developed A Secure and Efficient 4K HEVC Video Encoding Framework.
Sponsor: National College Students Innovation and Entrepreneurship Training Program.

EMPLOYMENT

Visiting Scholar, Purdue University – West Lafayette, IN — Sep 2022 - Jun 2025

Study robust deep learning models in network traffic analysis systems.
Advisor: Dr. Elisa Bertino

Research Assistant, Xidian University – Xi'an China — Sep 2019 - Aug 2022

Study robust deep learning models in image recognition systems.
Advisor: Dr. Xiaofeng Chen

Teaching Assistant, Xidian University – Xi'an China — Jul 2021 - Jul 2022

Course: *Distributed Computing*
Instructor: Dr. Miroslaw Kutylowski

Teaching Assistant, Xidian University – Xi'an China — Sep 2020 - Jan 2021

Course: *Probability Theory and Mathematical Statistics*
Instructor: Dr. Jianfeng Wang

Research Intern, National Radio and Television Administration – Beijing, China — May 2019 - Jul 2019

Research on secure video coding standards.
Department: Academy of Broadcasting Science

MENTORING

Md Shamsul Kaonain, Ph.D. Student, Purdue University — Jun 2025 - Present

Research: Machine learning security.

Yu Zhang, Visiting Ph.D. Student, Purdue University — Mar 2025 - Present

Research: data compression in machine learning.

Yani Liu, Visiting Ph.D. Student, Purdue University — Mar 2025 - Present

Research: Data compression in machine learning.

Mirza Masfiqur Rahman, Ph.D. Student, Purdue University — Jan 2025 - Present
Research: Robustness of graph neural networks.

Jason Hu, Undergraduate Student, Purdue University — Feb 2024 - Present
Research: Adaptive transfer attacks.

Yundong Liu, Ph.D. Student, Xidian University — Sep 2023 - Present
Research: Network Traffic Analysis with deep learning.

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

Weihao Liu, Undergraduate student, Xi'an University of Posts and Telecommunications — Dec 2020 - Jun 2021
Research: Iterative adversarial attack with projected gradient descent.

Mengchen Wang, Undergraduate student, Xi'an University of Posts and Telecommunications — Dec 2020 - Jun 2021
Research: Adversarial attack with Jacobian-based Saliency Map.

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.

TECHNOLOGY CONTEST AWARDS

Blue Bridge Cup National Software Development Technology Competition — Mar 2016
Jiangsu Province Second Prize, China

National College Student Innovation and Entrepreneurship Competition — Sep 2015
Jiangsu Province Third Prize, China

Challenge Cup National College Students Extracurricular & **Academic Contest** — Jun 2015
Jiangsu Province First Prize, China

SKILLS

Programming: Python, C++, HTML, Java, SQL, MATLAB
Tools: Pytorch, Sklearn, Keras, HuggingFace, VScode, etc.
Language: English, Chinese
Certificate: National Computer Rank Examination Grade 4 (NCRE-4), Network Engineer

EXCERPT AWARDS & HONORS

- Outstanding Doctoral Student Awarded by Xidian University — Sep 2019 - Sep 2022
- Xidian University Doctoral Academic Scholarship for Four Consecutive Years — Sep 2019 - Sep 2022
- Merit Graduate Student Awarded by Communication University of China — Jun 2019
- Communication University of China Graduate Academic Scholarship — Sep 2017 - Sep 2018
- Integrated Communication Social Scholarship Supported by Ze Media — Sep 2018
- Outstanding Graduate Awarded by Huaiyin Institute of Technology — Jun 2017
- Huaiyin Institute of Technology Undergraduate Academic Scholarship — Sep 2013 - Sep 2016

** Others available upon request.*
** Last updated on June 3, 2025.*