

# Shuo Han

Email: shuohan2024.1@u.northwestern.edu | Address: Evanston, IL

## Education Background

<b>Northwestern University</b>	<b>2022.09 – 2024.08</b>
<ul style="list-style-type: none"><li>Master of Science in Statistics and Data Science</li></ul>	
<b>Boston University</b>	<b>2019.09 – 2022.08</b>
<ul style="list-style-type: none"><li>Bachelor of Arts in Computer Science and Statistics</li><li>Awards: Dean's List</li></ul>	

## Research Interests

*Trustworthy Large Language Models(LLMs), AI for Security, and Data Mining.*

## Publication

- Zelei Cheng, Xian Wu, Jihao Yu, Xin-Qiang Cai, **Shuo Han**, Xinyu Xing., "Soft-Label Integration for Robust Toxicity Classification", submitted to NeurIPS, 2024
- Shuo Han.**, "Hydro-GRNNI: Hydrological Graph Recurrent Neural Network for Imputation", Northwestern University, 2024
- Chenli Wang, Juyang Wu, Xing Yang, Junfei Wang, Jian Shu, Jiazhong Lu, Yuanyuan Huang, **Shuo Han.**, "MC-GAN: an Adversarial Sample Defense Algorithm", ICCWAMTIP, 2024
- Jian Shu, Bo Xian, Chenli Wang, Peter Zhizhin, Yuanyuan Huang, **Shuo Han.**, "A Botnet Data Collection Method For Industrial Internet", ICCWAMTIP, 2024

## Research Experiences

### Research Assistant in LLM for Security

University of New South Wales **2024.05 – Present**

*Research Advisor:* Prof. Nan Sun & Prof. Xiao Wang

- Design experiments to test the robustness and uncertainty of LLM responses for cybersecurity tasks.
- Develop an automated evaluation framework to assess LLMs' reliability in identifying and reasoning about security-related bugs.

### Research in AI for Security

Northwestern University **2023.12 – 2024.05**

*Research Advisor:* Prof. Xinyu Xing

Project Background: Toxicity detection in human-LLM interactions often relies on single-annotator labels that can be biased, so we aim to use crowdsourced labels for more balanced and accurate assessments.

- Crafted toxic prompts using prompt engineering techniques and annotated them through third-party companies and LLMs. Integrate these crowdsourced annotations using a soft-labeling technique.
- Incorporated a bi-level optimization algorithm and GroupDRO loss based on topics to compute out-of-distribution loss, addressing distribution shifts caused by variations in annotators and topic difficulties.

### Research Assistant in Data Mining

Northwestern University **2023.07-2024.08**

*Research Advisor:* Prof. Kaize Ding

Project Background: The sparsity of U.S. hydrological data impedes effective assessment. To overcome this challenge, we explored using graph neural networks to impute missing data through spatiotemporal dependencies.

- Designed the model to capture upstream-downstream information among all monitoring stations, rather than relying solely on general latitude and longitude data, to better suit hydrological data.
- Use Graph Recurrent Neural Networks to capture spatial and temporal information, leveraging the recurrent structure for temporal data and the graph structure for spatial dependencies.

### Research Assistant in AI Security

Advanced Cryptography and System Security Key Laboratory, Northwestern University **2023.05-2023.08**

*Research Advisor:* Prof. Yuanyuan Huang

- Explored applying model compression techniques to enhance the model structure, achieving lower computational costs and improved accuracy for Generative Adversarial Networks.
- Proposed a data collection method for the industrial internet that includes network traffic and industrial control features, enhancing the accuracy of botnet detection.
- Applied a Logistic Regression approach for botnet detection on the collected dataset, addressing both binary classification and multiclassification tasks.

## **Teaching and Volunteer**

---

### **Graduate Teaching Assistant**

Northwestern University

Primary responsibilities: Host office hours, grade assignments, and lead project presentation sessions.

- STAT 332-0/IBIS 432, Spring 2023, Class size:30
- STAT 303-2, Winter 2023, Class size: 100

### **Volunteer**

- The Seventeenth International Conference on Web Search and Data Mining, 2024

## **Skills**

---

- Languages: Mandarin (native), English, Korean Beginner, Japanese Beginner
- Software: Adobe Illustrator, MS OFFICE
- Programming language: Python, Java, C, R, SQL, CSS, HTML, Java Script, OCaml
- Framework/Technology: Pytorch, Tensorflow, Git, HuggingFace