Fujiao Ji

Ph.D. Candidate in Computer Science
University of Tennessee, Knoxville
Expected start date: Apr. 22
(865)-824-7093

fji1@utk.edu
https://fujiaoji.github.io
Expected graduation date: 2027 summer

RESEARCH INTERESTS

LLM Security; LLM Distillation; Adversarial Attacks & Defenses; Web Security & Phishing Detection

EDUCATION

University of Tennessee, Knoxville Aug. 2022 – Present
Ph.D. in Computer Science TN, USA
Advisor: Dr. Doowon Kim

Shandong University of Science and Technology Aug. 2018 – Jun. 2021
M.S. in Computer Software and Engineering Qingdao, China
Advisor: Prof. Zhongying Zhao

EXPERIENCE

University of Tennessee, Knoxville Aug. 2022 - Present
Graduate Research Assistant, Graduate Teaching Assistant TN, USA
Phishing website investigation.

Shandong University of Science and Technology Aug. 2018 - Jun. 2021
Graduate Research Assistant, Graduate Teaching Assistant Qingdao, China
Heterogeneous graph representation learning.

Baidu Map Jun. 2021 - Jan. 2022
Research Internship, directed by Dr.Yibo Sun and Dr. Lei Shao Beijing, China
Named entity recognition for Chinese address data.

PROJECTS

Measurement Study of Visual-based Anti-Phishing Models Aug. 2022 - Dec. 2024

- Evaluated the effectiveness of visual-based anti-phishing models using the collected 451k real-world phishing websites sourced from the APWG.
- Identified and analyzed three strategies used by attackers to evade detection mechanisms.
- Assessed model robustness under coarse-grained and fine-grained settings using various manipulations identified in the collected data, revealing critical limitations in current visual-based detection approaches.

Measurement Study of LLM-based Anti-Phishing Models Jan. 2025 - Present

- Evaluated the inherent knowledge and reasoning capabilities of commercial and open-source LLMs in detecting phishing websites against deep learning-based detectors, showing that commercial LLMs achieve lower false positive rates.
- Investigated the impact of input components, HTML pre-processing techniques, and prompt engineering strategies on detection performance, identifying optimal configurations for reliability and effectiveness.
- Conducted failure analysis revealing that false positives are often associated with brand reputation; proposed incorporating screenshot-based inputs to improve detection accuracy for LLMs.

Understanding and Characterizing LLM-Generated Phishing Websites Jun. 2025 - Present

- Designed and implemented a systematic evaluation framework incorporating diverse prompt generation, LLM-driven website synthesis, and multi-dimensional analysis to assess the quality of phishing websites generated by commercial, open-source, and uncensored LLMs.

- Conducted in-depth analysis of generated websites across visual fidelity and functional realism, identifying key differences across LLMs and targeted brands and highlighting emerging real-world security risks.
- Developed actionable insights and recommendations to guide future detection, mitigation, and defense strategies against LLM-generated phishing attacks.

Chinese Address Parsing Project Jun. 2021 - Jan. 2022

- Extracted and structured address data in the format of province, city, district, town, and point of interest.
- Recognized named entities through a biaffine attention mechanism based on the pre-trained model ERNIE 1.0 under the framework of PaddlePaddle and improved performance via post-processing.
- Evaluated the performance of point of interest chunks, where the F1 score is 81.25% for 1,000 real-world data from Baidu Map and 80.41% for 2,985 public data from Chinese Address Corpus.

Heterogeneous Networks Analysis Sept. 2018 - Jun. 2019

- Conducted literature reviews on the work related to heterogeneous networks.
- Made a comparative study on heterogeneous networks and classified them into four categories according to topological and attribute information.

PUBLICATIONS

- **Ji, Fujiao**, Yerim Kim, Hyoungshick Kim, and Doowon Kim. Under Revision.
- **Ji, Fujiao**, and Doowon Kim. 'How Can We Effectively Use LLMs for Phishing Detection?: Evaluating the Effectiveness of Large Language Model-based Phishing Detection Models.' arXiv preprint arXiv:2511.09606 (2025).
- **Ji, Fujiao**, Kiho Lee, Hyungjoon Koo, Wenhao You, Euijin Choo, Hyoungshick Kim, and Doowon Kim. 'Evaluating the effectiveness and robustness of visual similarity-based phishing detection models.' In 34th USENIX Security Symposium (USENIX Security 25), pp. 3201-3220. 2025.
- Lim, Kyungchan, Kiho Lee, **Fujiao Ji**, Yonghwi Kwon, Hyoungshick Kim, and Doowon Kim. 'What's in Phishers: A Longitudinal Study of Security Configurations in Phishing Websites and Kits.' In Proceedings of the ACM on Web Conference 2025, pp. 957-968. 2025.
- Elgedawy, Ran, Porter Dosch, John Sadik, Senjuti Dutta, Anuj Gautam, Konstantinos Georgiou, Farzin Gholamrezae, **Ji, Fujiao**, et al. 'Occasionally secure: A comparative analysis of code generation assistants.' arXiv preprint arXiv:2402.00689 (2024).
- **Ji, Fujiao**, Zhongying Zhao, Hui Zhou, Heng Chi, and Chao Li. 'A comparative study on heterogeneous information network embeddings.' Journal of Intelligent & Fuzzy Systems 39, no. 3 (2020): 3463-3473.
- Zhao, Zhongying, Hui Zhou, Bijun Zhang, **Ji, Fujiao**, and Chao Li. 'Identifying high influential users in social media by analyzing users' behaviors.' Journal of Intelligent & Fuzzy Systems 36, no. 6 (2019): 6207-6218.

SKILLS

Languages & Framework: Python, Pytorch, Tensorflow, PaddlePaddle

Tools: Tmux, Visual Studio Code, Jupyter, Notion, vLLM, Hugging Face, LaTex

PROFESSIONAL ACTIVITIES

USENIX Artifact Evaluation Committee, 2026

IEEE S&P Artifact Evaluation Committee, 2026