

# Xiaoting Li

+1(814)6990779  
✉ [xiaotili0123@gmail.com](mailto:xiaotili0123@gmail.com)  
📄 [xiaoting.me](http://xiaoting.me)

## Education

- Aug 2017-Feb 2022 **Pennsylvania State University**, *United States*,  
*College of Information Sciences and Technology*,  
Ph.D. degree advised by Dr. Dinghao Wu.
- Feb 2019-Jul 2019 **Ecole Polytechnique Fédérale de Lausanne (EPFL)**, *Switzerland*,  
*School of Computer and Communication Sciences*,  
Visiting PhD student at [Very Large Scale Computing Lab](#).
- Sep 2016-Feb 2017 **University of Strathclyde**, *United Kingdom*,  
*Department of Computer Science*,  
Visiting student advised by Dr. John Levine.
- Sep 2013-Jun 2017 **B.E. University of Electronic Science & Technology of China**,  
*Dept. of Computer Science and Technology, major in Information Security*,  
Advised by Dr. Hong Qu. Thesis: Robustness Improvement on Spiking Neural Network,  
GPA: 3.88/4.0.

## Work Experience

- Mar 2022-Present **Visa Research**, *Staff Research Scientist*.
  - *Fundamental Research*
    - Graph Learning; Generative AI; Deep Tabular Learning; Recommendation Systems;
    - Published **9** papers, filed **15+** provisional and non-provisional patents;
  - *Selected Applied Projects (leading role)*
    - **Large Transaction Modeling**  
Developing the Gen-AI framework to meet foundational payment modeling goals involves building a unified transformer model. This model mirrors the architecture of open-source GPT-based models to understand user transaction behaviors. Additionally, we are developing a future transaction generation prototype using pre-trained models to support various business use cases.
    - **Payment Orchestration**  
Building data-centered fraud detection and model decision explanation solutions on tabular transaction data; leveraging counterfactual learning in tree-based/deep learning models to recommend transaction retries to improve the approval rate of false declined payments.
- May 2021-Aug 2021 **Visa Research**, *Research Intern*, Active Graph Learning.  
Published paper "SmartQuery: An Active Learning Framework for Graph Neural Networks through Hybrid Uncertainty Reduction".
- Jun 2020-Aug 2020 **ByteDance Inc.**, *Research Intern*, Statically Analyzing critical C++ projects.  
Investigating a couple of static analysis tools including CppCheck, Flawfinder, etc., on C++ projects. We use **Clang Static Analyzer** to adapt to company's unique compile framework and develop customized checkers to meet specific detection requirements and to reduce false positives in code testing.

## Publication

- ICML 2024 Weijie Ren, **Xiaoting Li**, Huiyuan Chen, Vineeth Mohan, Zhuoyi Wang, Mahashweta Das, Vasant Honavar, TagLog: Test-Time Adaptation for Tabular Data Using Logic Rules. *In Proceedings of the Forty-first International Conference on Machine Learning*.
- ICML 2024 Zhuomin Chen, Jiaxing Zhang, Jingchao Ni, **Xiaoting Li**, Yuchen Bian, Md Mezbahul Isam, Ananda Mondal, Hua Wei, Dongsheng Luo, Generating In-Distribution Proxy Graphs for Explainable Graph Neural Networks. *In Proceedings of the Forty-first International Conference on Machine Learning*.
- TKDD 2023 **Xiaoting Li**, Lingwei Chen, Dinghao Wu, Adversary for Social Good: Leveraging Adversarial Attacks to Protect Personal Attribute Privacy. *In Proceedings of the ACM Transactions on Knowledge Discovery from Data*.

IJCAI 2023 Huiyuan Chen, **Xiaoting Li**, Menghai Pan, Chin-Chia Michael Yeh, Yan Zheng, Kaixiong Zhou, Probabilistic Masked Attention Networks for Explainable Sequential Recommendation. *In Proceedings of 32nd International Joint Conference on Artificial Intelligence*.

RecSys 2023 Huiyuan Chen, **Xiaoting Li**, Vivian Lai, Chin-Chia Michael Yeh, Yujie Fan, Yan Zheng, Simple yet effective adversarial training for recommendation. *In Proceedings of 17th ACM Conference on Recommender Systems*.

CIKM 2022 **Xiaoting Li**, Yuhang Wu, Vineeth Rakesh, Yusan Lin, Hao Yang, Fei Wang, SMARTQUERY: An Active Learning Framework for Graph Neural Networks through Hybrid Uncertainty Reduction. *In Proceedings of 31th ACM International Conference on Information and Knowledge Management*.

RecSys 2022 Huiyuan Chen, **Xiaoting Li**, Kaixiong Zhou, Xia Hu, Chin-Chia Michael Yeh, Yan Zheng, Hao Yang, TinyKG: Memory-Efficient Training Framework for Knowledge Graph Neural Recommender Systems. *In Proceedings of 16th ACM Conference on Recommender Systems*.

RecSys 2022 Huiyuan Chen, Yusan Lin, Menghai Pan, Lan Wang, Chin-Chia Michael Yeh, **Xiaoting Li**, Yan Zheng, Fei Wang, Hao Yang, Denoising Self-Attentive Sequential Recommendation. *In Proceedings of 16th ACM Conference on Recommender Systems [Best Paper]*.

SecureComm 2022 **Xiaoting Li**, Lingwei Chen, Dinghao Wu, Adversary for Social Good: Leveraging Attribute-Obfuscating Attack to Protect User Privacy on Social Networks. *In Proceedings of 18th EAI International Conference on Security and Privacy in Communication Networks*.

ICICS 2022 **Xiaoting Li**, Xiao Liu, Lingwei Chen, Rupesh Prajapati, Dinghao Wu, FuzzBoost: Reinforcement Compiler Fuzzing. *In Proceedings of 24th International Conference on Information and Communications Security*.

SIGIR 2022 Quan Li, **Xiaoting Li**, Lingwei Chen, Dinghao Wu, Distilling Knowledge on Text Graph for Social Media Attribute Inference. *In Proceedings of International ACM SIGIR Conference on Research and Development in Information Retrieval*.

SDM 2022 Lingwei Chen, **Xiaoting Li**, Dinghao Wu, Adversarially Reprogramming Pretrained Neural Networks for Data-limited and Cost-efficient Malware Detection. *In Proceedings of SIAM International Conference on Data Mining*.

IAAI 2022 **Xiaoting Li**, Xiao Liu, Lingwei Chen, Rupesh Prajapati, Dinghao Wu, AlphaProg: Reinforcement Generation of Valid Programs for Compiler Fuzzing. *In Proceedings of 34th Annual Conference on Innovative Applications of Artificial Intelligence*.

IJCNN 2021 **Xiaoting Li**, Lingwei Chen, Jinquan Zhang, James Larus, Dinghao Wu, Watermarking-based Defense against Adversarial Attacks on Deep Neural Networks. *In Proceedings of International Joint Conference on Neural Networks*.

ICSE 2021 Qinkun Bao, Zihao Wang, **Xiaoting Li**, James Larus, Dinghao Wu, Abacus: Precise Side-Channel Analysis. *In Proceedings of 43rd International Conference on Software Engineering*.

SDM 2020 **Xiaoting Li**, Lingwei Chen, Dinghao Wu, Turning Attacks into Protection: Social Media Privacy Protection Using Adversarial Attacks. *In Proceedings of SIAM International Conference on Data Mining*.

ECML-PKDD 2020 Lingwei Chen, **Xiaoting Li**, Dinghao Wu, Enhancing Robustness of Graph Convolutional Networks via Dropping Graph Connections. *In Proceedings of European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases*.

AAAI 2019 Xiao Liu, **Xiaoting Li**, Rupesh Prajapati, Dinghao Wu, DeepFuzz: Automatic Generation of Syntactically Correct C Programs for Fuzz Testing. *In Proceedings of 33th AAAI Conference on Artificial Intelligence*.

## Patent Applications

Apr 2023 Huiyuan Chen, **Xiaoting Li**, Vivian Lai, Michael Yeh, Huiyuan Chen, Yan Zheng, Yujie Fan, Mahashweta Das, Hao Yang, Embarrassingly Simple and Fast Adversarial Training for Collaborative Filtering.

Mar 2023 **Xiaoting Li**, Xiaodong Yang, Huiyuan Chen, Yiwei Cai, Mahashweta Das, Hao Yang, Attacking Graph Neural Networks via Adversarial Influence Maximization.

May 2022 Huiyuan Chen, **Xiaoting Li**, Menghai Pan, Hao Yang, Michael Yeh, Simplifying Transformer for Sequential Recommendation via Softmax-free Gated Attention Mechanism.

- Apr 2022 Huiyuan Chen, **Xiaoting Li**, Hao Yang, Michael Yeh, Yan Zheng, TinyKG: Memory-saving Training Framework for Knowledge Graph Neural Recommender Systems.
- Mar 2023 **Xiaoting Li**, Yuhang Wu, Yu-San Lin, Fei Wang, System, Method, and Computer Program Product for Active Learning in Graph Neural Networks Through Hybrid Uncertainty Reduction.
- Oct 2022 Zhimeng Jiang, Han Xu, Menghai Pan, Huiyuan Chen, **Xiaoting Li**, Mahashweta Das, Hao Yang, GRAPH INFLUENCE FUNCTION.

## Other Experience

Professional  
Service

### Program Committee Member.

- International Joint Conference on Artificial Intelligence (IJCAI 2024)
- Thirty-Eighth AAAI Conference on Artificial Intelligence (AAAI 2024)
- IEEE International Conference on Big Data (IEEE BigData 2022, 2023)
- Thirty-Seventh AAAI Conference on Artificial Intelligence (AAAI 2023)
- 22nd IEEE International Conference on Data Mining (ICDM 2022)
- European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD 2020, 2021, 2022)

### Program External Reviewer.

- ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD 2021)
- 21nd IEEE International Conference on Data Mining (ICDM 2021)
- 43rd International Conference on Software Engineering (ICSE 2021)
- The ACM Conference on Computer and Communications Security (CCS 2019)

### Teaching Assistant.

- PSU IST336: Cyber Security in Windows Malware analysis (2020 Spring)
- PSU IST140: Application Development in Java (2018 Fall)

## Selected Honors and Awards

- Feb 2022 AAAI Conference Student Travel Grant Award.
- Jul 2021 Grace Hopper Conference (GHC) Scholarship.
- Apr 2020 Women in Cyber Security (WiCyS) Scholarship.
- Jan 2019 AAAI Conference Student Travel Grant Award.
- Apr 2018 Women in Cyber Security (WiCyS) Scholarship.
- Sept 2016 National Scholarship for Outstanding Undergraduates.
- Apr 2016 Honorable Mention in 2016 Mathematical Contest in Modeling.
- Sept 2015 Provincial Second Prize in National Mathematical Contest in Modeling.
- May 2015 Award of Excellence in National Mathematical Modeling Contest.

## Computer Skills

- Language Python, Scala, Java, Shell, C, R, Matlab, SML
- Substantial skill Keras, Tensorflow, PyTorch, Vim, Linux