Bolin Shen

1017 Academic Way, Tallahassee, FL 32304, USA
blshen@fsu.edu • +1 (850) 322-0439 • https://blshen.org

RESEARCH INTERESTS

My research mainly focus on strengthening **Small Language Models (SLMs)**, especially by improving their memory mechanisms and reasoning abilities to achieve efficient yet powerful intelligence. In parallel, I investigate **Graph Neural Networks (GNNs)** with an emphasis on model extraction attacks and defenses mechanisms. Ultimately, my goal is to build secure, robust, and trustworthy machine learning systems that contribute to the broader vision of Responsible AI.

EDUCATION

Florida State University, Tallahassee, Florida, USA

- Ph.D. in Computer Science — Jan 2025 – Jul 2028
  - Adviser: Prof. Yushun Dong
  - Focus: Small Language Model, Graph Representation Learning

University of Michigan, Ann Arbor, Michigan, USA

- M.Eng. in Data Science and Machine Learning — Aug 2022 – May 2024
  - Teaching Assistant for EECS553 Machine Learning
  - Focus: Graph Neural Networks

RESEARCH EXPERIENCE

Singapore Management University, Singapore

- Research Engineer, Computer Science — Aug 2024 – Dec 2024
  - Project: Neural Combinatorial Optimization
  - Supervisor: Prof. Zhiguang Cao
  - Focus: Combinatorial Optimization, Traveling Salseman Problem

PUBLICATIONS

CONFERENCES

[6] **Query-Efficient Domain Knowledge Stealing Against Large Language Models**
Z Li, X Yuan, B Shen, K Le, H Wang, X Zhou, S Gao, Y Dong
The 40th AAAI Conference on Artificial Intelligence (*AAAI'2026*), Nov 2025

[5] **CEGA: A Cost-Effective Approach for Graph-Based Model Extraction and Acquisition**
Z Wang, M Lin, B Shen, K Anderson, M Liu, T Cai, Y Dong
In Proceedings of the 42nd International Conference on Machine Learning (*ICML'2025*), Jun 2025

[4] **ATOM: A Framework of Detecting Query-Based Model Extraction Attacks for Graph Neural Networks**
Z Cheng, B Shen, T Sha, Y Gao, S Li, Y Dong
In Proceedings of the 31st ACM SIGKDD Conference on Knowledge Discovery and Data Mining (*KDD'2025*), Aug 2025

[3] **LLM-Empowered Patient-Provider Communication: A Data-Centric Survey from a Clinical Perspective**
R Shao, MS Seraj, L Li, B Shen, A Bates, Y Zhao, C Pan, L Hightow-Weidman, S Chakraborty, Y Dong
In Findings of the International Joint Conference on Natural Language Processing & Asia-Pacific Chapter of the Association for Computational Linguistics (*JCNLP-AACL'2025*), Oct 2025

[2] **Learning from the Storm: A Multivariate Machine Learning Approach to Predicting Hurricane-Induced Economic Losses**
B Shen, EE Ozguven, Y Zhao, G Wang, Y Xie, Y Dong
In Proceedings of the 33nd ACM International Conference on Advances in Geographic Information Systems (*SigSpatial'2025 SpatialConnect Workshop*), Aug 2025

[1] **Federated Multi-view Spectral Clustering**
H Wang, A Li, B Shen, Y Sun, H Wang
IEEE Access (*IEEE Access*), Nov 2020

PRE-PRINTS

[5] **CREDIT: Certified Defense of Deep Neural Networks against Model Extraction Attacks**
B Shen, Z Cheng, NZ Gong, F Yao, Y Dong
arXiv preprint (*In Submission*), Sep 2025

[4] **CITED: A Decision Boundary-Aware Signature for GNNs Towards Model Extraction Defense**
B Shen, MS Seraj, Z Cheng, S Chakraborty, Y Dong
arXiv preprint (*In Submission*), May 2025

[3] **AGDN: Learning to Solve Traveling Salesman Problem with Anisotropic Graph Diffusion Network**
B Shen, Z Huang, Z Cao, Y Dong
arXiv preprint (*In Submission*), Feb 2025

[2] **Intellectual Property in Graph-Based Machine Learning as a Service: Attacks and Defenses**
L Li, B Shen, C Zhao, Y Sun, K Zhao, S Pan, Y Dong
arXiv preprint (*arXiv:2508.19641*), Aug 2025

[1] **Political-LLM: Large Language Models in Political Science**
L Li, J Li, C Chen, F Gui, H Yang, C Yu, Z Wang, J Cai, JA Zhou, B Shen, ..., Y Dong
arXiv preprint (*arXiv:2412.06864*), Dec 2024

SELECTED PROJECT

PyGIP, Open Source Python Library

- Project Leader
  - Developed a comprehensive open-source framework for Graph Neural Network (GNN) **model extraction attacks and defenses**, integrating research-level implementations with practical usability.
  - Designed modules for **attack and defense simulation**, enabling reproducible evaluation of GNN security.
  - Built on **PyTorch**, **PyTorch Geometric**, and **DGL**, providing unified APIs for attack and defense benchmarking with configurable experimental pipelines.
  - Supervised a team of researchers and contributors; Coordinated open-source release and documentation on GitHub and PyPI. We have over 160 times download per month.

Computational Neuroscience, Florida State University

- Computer Science Lead
  - Led the computer science component of a cross-disciplinary project with the Department of Psychology to study the link between **visual stimuli** and **mouse neuronal activity**.
  - Developed computational pipelines that map image features from pre-trained **vision transformers** to **neural population responses**.
  - Implemented **information bottleneck** modules to simulate hierarchical information flow across cortical nodes.
  - Analyzed alignment between artificial representations and biological neurons, providing insights into visual encoding and cortical processing.

STUDENT MENTORED

- **Iris Hong** (Washington University in St. Louis)
  Topic: Human Alignment in LLM
- **Serina Charis Madhura** (Florida State University)
  Topic: MetaFinger-LLM: Cross-Modal Ownership Verification
- **Md Nyem Hasan Bhuiyan**
  Topic: Adversarial-Guided Fingerprint Construction for Robust GNN Ownership Verification

TECHNICAL SKILLS

- Programming Language: Python, Java, C/C++, JavaScript, Lua
- ML Framework: PyTorch, Torch Geometric, DGL, Keras
- Miscellaneous: LaTeX, Git, Vim, Tmux

LANGUAGES

- Chinese: Native language.
- English: Fluent (speaking, reading, writing).

INVITED PRESENTATION

Student Seminar, Florida State University

- *AGDN: Learning to Solve Traveling Salesman Problem with Anisotropic Graph Diffusion Network*
  Invited talk at the **Student Seminar Series**, presenting novel anisotropic graph diffusion methods for combinatorial optimization problems.

Student Seminar, Florida State University

- *CREDIT: Certified Defense of Deep Neural Networks against Model Extraction Attacks* Oct 2025
  Invited presentation at the **Student Seminar Series**, highlighting theoretical and empirical advances in certified robustness for neural network intellectual property protection.

[*CV compiled on 2025-12-28*]