Yaxin Li (Gloria Li)

CONTACT INFORMATION

428 S Shaw Ln Rm 3115
East Lansing, MI 48824
Personal Webpage: https://yaxinli.netlify.app/

E-mail: liyaxin1@msu.edu
Phone: (+1)5175056654
GitHub: https://github.com/I-am-Bot

EDUCATION

M.S. in Michigan State University, Computer Science and Engineering — Sep 2019 – Present

- Advisor: Dr. Jiliang Tang

B.S. in Tsinghua University, Information Science and Technology — Aug 2015 – Jul 2019

SKILLS

Languages: Python, C, C++, MATLAB, Latex, Markdown, C#, Java, JavaScript, HTML5, SQL
Framework/Tools: Pytorch, Tensorflow, Sckit-learn, SpringBoot, React, AWS, Spark, MongoDB, sanity

PROJECT EXPERIENCE

Opensource ToolBoxs

- **DeepRobust: Representative Pytorch Attacks and Defenses Toolbox on image and graph domains** (500+ stars on Github, first author paper published in AAAI) - Lead the development of all popular machine learning security algorithms, include 20 attacks and defenses for image classification and 20+ target on graph neural network. (Python)

Projects

- **Android mobile application for SIEMENS product anti-counterfeiting via NFC tag. (Undergraduate Research Project)** - Design and implement the front-end of the Android application with Java. This application read the NFC tag and distinguish fake identification code. (Java)
- **Online Chatroom. (Network and Communication Course Project)** - Independently implement a chat application with functions including: login, connecting to server and music player. Implemented by JavaScript with Node.js and Express framework, building connections between server and client via socket.io. (JavaScript)
- **Personal Webpage.** - Build my portfolio with React, Sanity.io and Tailwind from scratch. (JavaScript)

MACHINE LEARNING RESEARCH EXPERIENCE

Selected Research Projects and Publications (Full Publication List)

- **Enhancing Adversarial Training with Feature Separability** - Improve deep learning model robustness through regularizing intra-class and inner-class feature distance. Achieve the state of the art performance on MNIST and CIFAR10 datasets under evaluation of different attacks using Pytorch framework. (Python)
- **Yet Meta Learning Can Adapt Fast, It Can Also Break Easily (Second author paper published in SDM-21)** - Evaluate the robustness of popular meta learning frameworks with designed gradient-based attacking methods. Successfully degrade the meta learning performance by more than 40%. (Python)
- **Graphical Evolutionary Game Theoretic Analysis of Super Users in Information Diffusion. (Second author paper published in ICASSP-20)** - Model and simulate the fake information diffusion process in social network using evolutionary game theory. (MATLAB)

Surveys

- **Adversarial Attacks and Defenses on Graphs (SIGKDD Explorations-22)** -Introduce robustness related algorithms in graph classification and launch comprehensive experiments based on DeepRobust.

WORK EXPERIENCE

Research Assistant at DSE lab, Michigan State University — Sep 2019 – Jul 2021

- Focus on Adversarial Robustness; security and privacy issue in machine learning

Teaching Assistant at Michigan State University — Sep 2021 – Present

- CSE232 Introduction to Programming II (Language: C++)
- CSE480 Database System (Language: python, MySQL)

Research Intern at TAL Education Group — Jun 2020 – Sep 2020

HONORS & AWARDS

- KDD CUP 2020: Regular Machine Learning Competition Track: Adversarial Attacks and Defense on Academic Graph, **Top 10 Winner**.
- NOIP 2012, 2013: National Olympiad in Informatics in Provinces, Beijing, China. **First Prize**.

[*CV compiled on 2022-03-08*]