Yimo (Harry) Deng

+86 18161800875 | yimodeng@hkust-gz.edu.cn | Harry-Deng | www.dengemo.com
Northeastern University, Hunnan District 110169, Shenyang, China

Targeting a Ph.D. position starting in Fall 2024

EDUCATION

Northeastern University (985 & 211) ***B.E.*** ***Sept 2020 - June 2024 (Expected)***
Information Security ***Shenyang, China***
Average Score: ***90.1/100;*** *GPA:* ***3.9/4.0;***
Major Courses: Advanced Mathematics (Calculus), Linear Algebra, Probability Theory and Mathematical Statistics, Discrete Mathematics, Mathematics for Information Security (Number Theory), Game Theory, Computer Networks, Principles of Computer Organization, The Principle and Security of Operating system, Data Structures and Algorithm Analysis, Machine Learning and Big Data Mining, Fundamentals of Cryptography, Linux Programming, etc.

PUBLICATION

1. **Y. Deng**, & C. Huang, "Divide-and-Conquer Attack: Harnessing the Power of LLM to Bypass the Censorship of Text-to-Image Generation Model," *arXiv preprint arXiv:2312.07130, 2023*.

RESEARCH EXPERIENCE

Harnessing the Power of LLM to Bypass the Censorship of Text-to-Image Generation Engine
Nov 2023- Dec 2023
Supervised by Prof. Huangxun Chen ***HKUST(GZ), China***
- Discovered an attack scheme that bypasses the censorship of Text-to-Image generation engines.
- Built a system that harnesses LLM-generated adversarial prompts to against LLM-assisted safety filter.
- Effectiveness: The average success rate of bypassing DALL·E 3's safety filters is over 92.9%, and the average rate of generating harmful images across different categories is over 47.4%.
- Results: Completed a research paper (Submitted).

Security and Privacy in Distributed Machine Learning for Vehicular Ad hoc Networks | Mitacs Globalink
May 2023- Sept 2023
Supervised by Prof. Jianping Pan(FIEEE) ***UVic, Canada***
- Design a secure and privacy-focused distributed machine learning framework for VANETs.
- Protect the location privacy of smart device holders in VANETs, and manage malicious nodes within the system.
- Results: Completed the internship remotely across a 13-hour time difference and proposed a valuable solution.

An Economic Study of Cooperative Resource Provision in JointCloud Computing
Mar 2023 - May 2023
Supervised by Prof. Rongfei Zeng ***NEU, China***
- Analyzed Alibaba PAI cluster data to determine how various cloud users impact CSPs' decision-making.
- Utilized an evolutionary game model for economic analysis of JCC, uncovering stable dynamics between CSPs and users.
- Results: Completed a research paper (Ready for submission).

Intrusion Detection System Based on Voltage Fingerprint in In-Vehicle Network CAN Bus Network
Jun 2022 - Oct 2022
Supervised by Prof. Jian Xu ***NEU, China***
- Designed an IDS by identifying differences in voltage sample features collected from the CAN bus.
- Effectiveness: Addressed the issue of traditional CAN-based message rule and anomaly behavior learning IDS being unable to locate the source of attacks. Reduced the voltage sampling rate of the IDS to 50K samples per second.
- Results: Built a fully functional detection system and won a national competition award.

Diagnosis of Fundus Diseases Based on Convolutional Neural Network
Aug 2021 - Jan 2022 ***XDU, China***
- Performed experiments on several retinal image recognition algorithms.
- Assessed the efficacy of each method in accurately detecting various eye diseases.
- Effectiveness: The classification accuracy of retinal diseases was improved by 5.67%.
- Results: Developed a fundus image-assisted diagnostic system employing a sophisticated machine learning algorithm, subsequently securing an accolade in a national competition.

WORK & TEACH EXPERIENCE

Research Assistant | *Information Hub, HKUST(GZ)* ***Sept 2023 - Present***
Supervised by Prof. Huangxun Chen ***HKUST(GZ), China***
- Exploring security issues in the application of LLMs in specialized domains.
- Exploring backdoor attacks in large language models integrated with robot computer vision.

Guest Speaker | *Software College, NEU* ***Mar 2023***
- Game Theory, Evolutionary Game Theory, Spring 2023

Java Development Engineer (Intern) | *NEUTech, NEUSoft* ***May 2021 - Aug 2021***
- Developed an information management system with a GUI for a senior care center independently.

PROJECT EXPERIENCE

Yawn Suite | *Cyber Attack* ***Mar 2023 - Apr 2023***
- Developed a cyber attack software similar to Burp Suite, enabling ARP and DDoS attacks on hosts within LAN.

Crypto En & Decryptor | *Cryptography* ***Jun 2022 - Sept 2022***
- Developed a sophisticated encryption and decryption communication desktop software, which supports various cryptographic techniques, including traditional ciphers, RC4, RSA, DH, MD5, AES, and DES.

NEU Hermit | *Schedule Management* ***Mar 2022 - Jun 2022***
- Conceived and developed a multifaceted schedule management app, encompassing features such as a calendar, daily agenda, course timetable, and Moments. This app has a registered software copyright.

COMPETITION AWARDS

International Meritorious Winner | Mathematical Contest in Modeling ***May 2023***
International Honorable Mention | Interdisciplinary Contest in Modeling ***May 2022***
National Third Prize | National College Student Information Security Competition ***Sept 2022***
National Third Prize | National E-commerce Innovation Competition for College Students ***Jun 2022***
International Third Prize | Asia-pacific Mathematical Contest in Modeling for College Students ***Jan 2022***
Regional third prize | C4-Network Technology Challenge ***Aug 2022***
Provincial Second Prize | China International Internet+ Innovation and Entrepreneurship Competition ***Jul 2022***

CERTIFICATES AND HONORS

Huawei Scholarship (Only three winners in NEU) ***2021-2022***
Northeastern University Scholarship ***2021-2022***
Outstanding Student ***2021-2022***
Yipu Science and Technology Scholarship (Only one winner in NEU) ***2020-2021***
Northeastern University Scholarship ***2020-2021***
Outstanding Student Leader Model ***2020-2021***

OTHER EXPERIENCE

President of the **Student Union**, College of Software, Northeastern University
The Best College Host in Northeastern University at the academic year 2020-2021
Leader of 2021 Summer Vacation Research Team on Rural Vitalization