Yimo (Harry) Deng

+86 18161800875 | yimodeng@hkust-gz.edu.cn | Harry-Deng | www.dengemo.com
HKUST(GZ), No.1 Du Xue Rd, Nansha District, Guangzhou, China

EDUCATION

Northeastern University ***B.E.*** ***Sept 2020 - July 2024 (Expected)***
Information Security ***Shenyang, China***
Average Score: ***90.1/100;*** *GPA:* ***3.9/4.0;***
Major Courses: 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.

University of Victoria ***Visiting Student*** ***May 2023 - August 2023***
Mitacs Globalink Research Internship Program ***BC, Canada***
Visit Lab: The Protocols for Advanced Networking Laboratory (PANLab).

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

Adversarial Attack on Multimodal Large Language Models from the Physical Domain
Feb 2024 - Present
Supervised by Prof. Huangxun Chen ***HKUST(GZ), China***
- Design a method for applying adversarial perturbations to MMLLMs via optical components.
- **Expected Results:** Implementing an attack scheme from the physical domain on MMLLMs and completing a research paper.

Harnessing the Power of LLM to Bypass the Censorship of Text-to-Image Generation Engine
Nov 2023 - Jan 2024
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.

Security and Privacy in Distributed Machine Learning for Vehicular Ad hoc Networks
May 2023 - Sept 2023
Supervised by Prof. Jianping Pan ***UVic, Canada***
- Designed 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 a technical report and received a return offer.

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.

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.

WORK & TEACH EXPERIENCE

Research Assistant | *Information Hub, HKUST(GZ)* ***Sept 2023 - Present***
Supervised by Prof. Huangxun Chen
- Exploring security issues in the application of LLMs in specialized domains.
Guest Speaker | *Software College, NEU* ***Mar 2023***
- Game Theory, Evolutionary Game Theory, Spring 2023
Java Development Engineer (Intern) | *NEUTech, NEUSoft* ***May 2021 - July 2021***
- Developed an info-management system with a GUI for a senior care center.

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**, Software College, Northeastern University
The Best College Host in Northeastern University at the academic year 2020-2021