JAECHUL (Harry) ROH

Final Year Student in Computer Engineering, HKUST

jcroh980508@gmail.com | https://www.jrohs.com | https://github.com/jcroh0508

EDUCATION

Hong Kong University of Science and Technology **September 2017 – Present**

B.Eng. in Computer Engineering, School of Engineering Clear Water Bay, Hong Kong

PUBLICATIONS

[1] Impact of Adversarial Training on the Robustness of Deep Neural Networks (Paper ID: MSCS-704)

ROH, Jaechul, the first author

- **Accepted** by the *2022 International Conference on Modeling, Simulation and Computing Science (MSCS 2022)* on April 15th, 2022
- Will be published by IEEE Conference Publishing Services, and will be submitted to EI Compendex, Thomson ISTP and CNKI databases for indexing

[2] MSDT: Masked Language Model Scoring Defense in Text Domain

ROH, Jaechul, Minhao Cheng, Yajun Fang

- **Submitted** to the *IEEE International Conference on Universal Village (IEEE UV2022)* on July 9th, 2022, for reviewing

[3] Evaluating the Robustness of Federated Learning in Smart Home Face Recognition System

ROH, Jaechul, Yajun Fang

- **Submitted** to the *IEEE International Conference on Universal Village (IEEE UV2022)* on September 15th, 2022, for reviewing

RESEARCH / WORK EXPERIENCE

IEEE International Conference on Universal Village 2022 **May 2022 – Present**

Student Research Program, Supervisor: Dr. Yajun Fang (CSAIL, MIT) Cambridge, Massachusetts

- Experimented the robustness of federated learning in smart home face recognition system in respect to MIT Universal Village concept.

MSDT: Masked Language Model Scoring Defense in Text Domain **January 2022 – May 2022**

Independent Work Research, Supervisor: Prof. Minhao CHENG Clear Water Bay, Hong Kong

- Proposed a novel improved textual defense method against backdoor attack on pre-trained language models.

Personal Research Project **January 2022 – March 2022**

Topic: "Impact of Adversarial Training on the Robustness of Deep Neural Networks"

- Experimented the effectiveness of various methods of adversarial training on improving the robustness of neural networks against classifying perturbed histopathological images.

Super Chain AI (Conard International) **June 2021 – August 2021**

NLP Engineer Intern in the Artificial Intelligence Team Kowloon Bay, Hong Kong

- In charge of topic modeling and semantic analysis based on customer reviews and assigning specific semantics to the topics extracted.
- Competitors' analysis through web-scrapping customer reviews from other drop-shipping websites.

Military Service at Head Quarter of 12th Infantry Division **July 2018 – March 2020**

Sergeant of Republic of Korea Army Injae, Kang Won Do, Republic of Korea

- Officer Administrative Clerk Specialist
- Squad Leader of the Head Quarter

PROJECTS

Histopathological Scan Cancer Detection **December 2021 - January 2022**

2022 Personal Winter Project, Supervisor: Prof. Mark Vogelsberger (MIT)

- Demonstrated a user-friendly application that aids to classify whether a histopathologic scan contains metastatic cancer using modified Convolutional Neural Network and modified Resnet-18.
- In charge of implementing the neural networks for the classification task.

Presentation Project on "Adversarial Attack" **September 2021 – November 2021**

Machine Learning course Final Project, Instructor: Prof. Dit-Yan YEUNG Clear Water Bay, Hong Kong

- 30-minute video presentation on the topic of "Adversarial Attack"
- Papers reviewed: *"Explaining and Harnessing Adversarial Examples" & "Is Bert Really Robust? A Strong Baseline for Natural Language Attack on Text Classification and Entailment"*
- Video Link: https://www.youtube.com/watch?v=maMC93Lf-mY

SKILLS / LANGUAGES

Programing Languages: Python, C, C++
Frameworks/Libraries: PyTorch, Hugging Face, NLTK, spaCY, MongoDB, Selenium, Beautifulsoup
Languages: Korean (Native), English (Native), Chinese (Fluent)