Zih-Dwo Yeh (Doyle)

☎ (+1) 814-862-8109 ✉ doyleyeh.job@gmail.com linkedin.com/in/doyle980216 github.com/doyleyeh

Machine Learning Engineer | Software Developer | Cybersecurity Specialist

Education

The Pennsylvania State University University Park, PA, USA
Master of Science in Informatics August 2023 – May 2025

- Coursework: Computer Security, Software Security, Cybersecurity Analytics, Network Management, Cloud Security, Data Mining, Machine Learning

National Taipei University of Technology Taipei, Taiwan
Master of Science in Computer Science September 2021 – July 2023

- Coursework: Pattern-oriented Software Design, Design and Analysis of Algorithms, Cloud Computing, Data Science, Operating Systems, Network Security and Penetration Testing

National Taipei University of Technology Taipei, Taiwan
Bachelor of Science in Electrical Engineering September 2016 – July 2020

- Coursework: Object-Oriented Programming, Computer Networks, Image Processing, Python Programming

Skills

Programming Languages: C++, Python, MATLAB, SQL, JavaScript (or TypeScript)
Development: Node.js, Next.js, Express.js, Tailwind CSS
Machine Learning/AI: PyTorch, TensorFlow, Scikit-Learn, Hugging Face Transformers
Packages and Tools: Git/GitHub, Docker, Conda, VSCode, Shell/Bash, Linux, Wireshark

Experience

SYSTEX Corporation Taipei, Taiwan
IT Intern September 2018 – June 2019

- Maintained over 100 company workstations and laptops, troubleshooting hardware and software issues to ensure system stability and smooth operation.
- Configured and managed network settings, servers, and edge devices, ensuring compliance with security policies and company standards.
- Performed virus updates using FortiClient, safeguarding company systems from malware threats and optimizing network security.
- Conducted packet analysis with Wireshark to diagnose and resolve network issues related to Ethernet switching and IP routing.

Projects

Active Retrieval-Augmented Generation (RAG) by Small Language Models (SLMs) 2024 – 2025

- Built a confidence-based active retrieval system enhancing accuracy in multi-hop QA tasks for SLMs.
- Dynamically integrated external knowledge based on real-time model confidence, reducing retrieval overhead.
- Improved Exact Match accuracy by 15–20% on 2WikiMultihopQA dataset across multiple small-scale models (Llama, Gemma, Qwen).
- Achieved near-commercial LLM performance with cost-effective, locally-deployable SLMs.

Large Language Models (LLMs) Attribution Classifier 2023 – 2024

- Constructed a dataset of 25,000 prompt-completion pairs from five LLMs through an automated pipeline for text extraction, truncation, and labeling.
- Fine-tuned ALBERT, DistilBERT, and RoBERTa (with LoRA adaptation), achieving 67.6% accuracy and a 0.68 macro-F1 score.
- Conducted comprehensive ROC-AUC evaluation and detailed error analysis to identify model-specific confusion patterns, guiding future data augmentation strategies.

Defense Technique Against Inference Attacks (MIAs) in Federated Learning (FL) 2022 – 2023

- Developed a defense mechanism adding noise to reduce MIAs in FL.
- Used gradient-based optimization to minimize confidence score distortion while defending against MIAs.
- Reduced MIA accuracy to near random guessing levels across training epochs.
- Implemented and evaluated the defense with AlexNet, enhancing data privacy in decentralized systems.