YUN-YUN (ALICE) TSAI

(+886) 973-798-908 • alice103000004@gmail.com • https://yunyuntsai.github.io

RESEARCH INTERESTS

I have been working on artificial intelligence in security and the robustness in deep learning, including adversarial attack, defense and robust evaluation.

EDUCATION

National Tsing Hua University (NTHU) Hsinchu, Taiwan

Master of Science in Computer Science *Sept., 2018 – June, 2020*

- Overall GPA: $4.18/4.30$, Advisor: Prof. Tsung-Yi Ho
- Visiting Scholar at the HSL at University of Florida (UF) *Mar., 2019 – Aug., 2019*

Bachelor of Science in Computer Science *Sept., 2014 – June, 2018*

- Overall GPA: $3.50/4.30$, Last 60 GPA: $3.89/4.30$

PUBLICATIONS

Conference and Workshop Papers

[C1] **Yun-Yun Tsai**, Pin-Yu Chen, and Tsung-Yi Ho, "Transfer Learning without Knowing, Reprogramming black box machine learning model with scarce data and limited resources," in Proceeding of International Conference on Machine Learning (**ICML**), 2020.

[C2] Honggang Yu, Kaichen Yang, Teng Zhang, **Yun-Yun Tsai**, Tsung-Yi Ho, Yier Jin, "CloudLeak: Large-Scale Deep Learning Models Stealing Through Adversarial Examples," in Proceeding of Network and Distributed System Security Symposium (**NDSS**), 2020.

[C3] **Yun-Yun Tsai**, Pin-Yu Chen, Tsung-Yi Ho, "Adversarial Machine Learning for Social Good: Reprogramming black box machine learning model with scarce data and limited resources," Advances in Neural Information Processing Systems (**NeurIPS**) NewInML Workshop, Poster, 2019.

[C4] Ta-Wei Huang, **Yun-Yun Tsai**, Chung-Wei Lin, Tsung-Yi Ho, "Vehicle Sequence Reordering with Cooperative Adaptive Cruise Control," in Proceeding of Design, Automation and Test in Europe Conference and Exhibition (**DATE**), 2019.

Patents

[P1] Pin-Yu Chen, **Yun-Yun Tsai**, Sijia Liu, Chia-Yu Chen, I-Hsin Chung, Tsung-Yi Ho. "Transfer Learning With Machine Learning Systems", U.S. Patent Application No: 17/029506, Application Date: September 23, 2020.

WORKING AND RESEARCH EXPERIENCE

Graduate Research Assistant *July., 2020 – present*

Advisor: *Prof. Tsung-Yi Ho* *THETA Lab, NTHU, Hsinchu, Taiwan*

- Focus on federated learning systems and sophisticated adversarial attack.

Visiting Scholar *Mar., 2019 – Aug., 2019*

Advisor: *Prof. Yier Jin* *Hardware Security Lab at UF, Gainesville, FL, USA*

- Model retrieving attack on large-scale deep learning models.

Software Engineer Intern *July, 2017 – June, 2018*

Mentors: *XXX* *Microsoft Azure IoT Team, Taipei, Taiwan*

- Built POC (covers Smart City/Retail/Home/Manufacturing) leveraging Azure IoT Cloud services to demonstrate IoT solutions to 10+ technical business partners.
- Designed/Created Azure Machine Learning hands-on materials with Microsoft MVPs and delivered the workshop in coding angel event to 100+ college STEM female students.

PROFESSTIONAL SERVICE AND SKILLS

Paper Review	IEEE Access
Teaching Assistant	Fundamental of Formal Language
Invited Talk	CYBERSEC 2020
Programming Languages	Python, R, C/C++, Verilog
Packages	Tensorflow, Pytorch, Sci-kit Learn, Keras
Certification	Microsoft Professional Program Certificate in Data Science

Activities

Musical Performance

- First stand of Viola, NTHU Orchestra *Sept., 2014 – June, 2018*
- Piano concerto soloist, Annual summer concert of NTHU orchestra *May 30, 2017*
- 1^{st} prize of viola solo and piano quintet in The National High School Student's Music Contest Finals in Taiwan

Student Association Committee *2016 – 2017*

- Director of Team Mentors: Led 20 mentors (college students) to train 100 participated senior high school students on basic computer science