YUN-YUN (ALICE) TSAI

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

SUMMARY

Applying for CS Ph.D. program in the regimes of Security and Artificial Intelligence, I am interested in **robust machine learning**, (ICML'20), **DNN model reverse extraction** (NDSS'20), and **design automation on autonomous vehicle system** (DATE'19). I received M.S. and B.S. in computer science from National Tsing Hua University with industrial experience in Microsoft Azure.

EDUCATION

National Tsing Hua University (NTHU) Hsinchu, Taiwan

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

- Overall GPA: 3.9/4.0, Advisor: Prof. Tsung-Yi Ho
- Visiting Scholar at the Security in Silicon Lab (SSL) at University of Florida (UF) *Mar., 2019 – Aug., 2019*

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

- Overall GPA: 3.5/4.0, Last 60 GPA: 3.8/4.0

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.

RESEARCH AND WORKING EXPERIENCE

Graduate Research Assistant Tsing Hua Emerging Technology Automation Lab, Hsinchu, Taiwan

Advisor: Prof. Tsung-Yi Ho *Sept., 2018 – present*

Co-Advisor: Dr. Pin-Yu Chen, IBM Research Trusted AI group, Yorktown, NY, USA

- **Model robustness against composite adversarial examples**
  - Searching the worst-case combinations (i.e., ordering and bias offset) of pixel-/semantic-based adversaries and spatial transformations using reinforcement learning, which are used for adversarial training to enhance model robustness beyond low-level perturbations in the ℓ_p space.
- **Limited-data transfer learning on black-box ML models**
  - Utilizing adversarial reprogramming techniques and zeroth-order gradient estimation algorithms to transfer model functionality from general ImageNet classifier to specific medical imaging classifiers with limited training data, and the results outperform both traditional and SOTA transfer learning methodologies.
- **Autonomous vehicle sequence optimization for Cooperative Adaptive Cruise Control**

– Reducing 1.3∼2.2x total operation times and the platoon length by 20% by proposing a clique-based partition-and-merge algorithm to optimally reorder vehicle sequence given a pre-defined platoon length determined by braking factors.

Visiting Scholar **SSL at UF**, Gainesville, FL, USA
Advisor: Prof. Yier Jin *Mar., 2019 – Aug., 2019*

- **Large-scale DNN model extraction from Machine Learning as a Services.**

– Reducing 30x queries for copying a given black-box ML model using adversarial active learning and local approximation of decision boundary with different model architectures while remaining same performance.

Research Intern **Microsoft Cloud and AI Team**, Taipei, Taiwan
Mentors: Cheryl Hsu *July, 2017 – June, 2018*

– Prototyping IoT solutions to 20+ business partners (e.g., NEC, Nexcom) by leveraging Azure IoT Cloud and Edge computing in a wide range of scenarios including Smart City, Retail, Home and Manufacturing.

Highlighted Courseworks

Analysis: Linear Algebra, Calculus(II), Computer Architecture, Introduction to Data Science*, Cryptography and Network Security, Computational Methods for Biomedical Image Analysis*, Introduction to Artificial Intelligence and Music*, Analysis and synthesis of digital audio signals, Introduction to Embedded Systems
Engineering: Computer Vision*, Computer Graphics*, Deep learning for Autonomous Driving*, Design Automation of Emerging Technologies*, Fintech Innovation and Applications*, System Integration Implementation(I)(II)
(obtained A or A+ in all, *: graduate-level)

Professional Service and Skills

Teaching Assistant	Fundamental of Formal Language, Very-Large-Scale Integration (VLSI)
Paper Review	IEEE Access, ICLR 2021, AAAI 2021, ICPAI 2020
Invited Talk	CYBERSEC 2020 – Blackhat Awarded Forum,TAAI keynote 2020
Programming Languages	Python, R, C/C++, Verilog
Packages	Tensorflow, Pytorch, Sci-kit Learn, Keras, Caffe
Languages	English (fluent), Chinese (native)
TOEFL iBT	102/120 (Reading 28, Listening 25, Writing 26, Speaking 23)

Extracurricular Activities

Musical Performance

– First stand of Viola, NTHU Symphony Orchestra *Sept., 2014 – June, 2021*
– Piano concerto soloist, Annual summer concert of NTHU orchestra *May 30, 2017*
– Music competitions (piano): Winner of NTHU concerto competition *2017*
– 1st prize of both viola solo and piano quintet in the National High School Student's Music Contest Final *2011*

Student Volunteer, NTHU musical charity camp *Jun, 2017*

– Coordinated a musical charity camp for underprivileged children from elementary schools in remote areas and taught them to play string instruments.

Technical Teaching Leader, Microsoft Coding Angel bootcamp *Dec, 2017*

– Designed hands-on implementations with Microsoft Data Scientists on basic ML algorithms, R/Python tutorials on Azure Machine Learning Studio for building predictive models and trained other SDE interns to conduct a workshop for 100+ female college students in STEM.

Director of Team Mentor, NTHU CS camp *2016 – 2017*

– Led 20 mentors from college to train 100 participants from senior high schools for coding skills on Python and Unity to design games.

Team Manager, NTHU Table Tennis Team *2016 – 2017*

– Responsible for managerial duties for the team.