TIANJI CONG

Phone (734)-680-3985 **Email** congtj@umich.edu

SUMMARY

Tianji Cong is a Ph.D. student in the EECS Department at the University of Michigan. His research focuses on adversarial machine learning. His work aims to demonstrate real risks of adversarial examples to deep-learning-based vision systems in the physical world and design defenses to enhance the robustness of deep neural networks against both digital and physical attacks. He is also passionate about programming that can automate the workflow.

EDUCATION

University of Michigan, Ann Arbor, MI August 2025 (Expected)
Ph.D. Precandidate in Computer Science and Engineering
Advised by Prof. Atul Prakash

University of Michigan, Ann Arbor, MI April 2020
Bachelor of Science in Computer Science Cumulative GPA: 3.82/4.00
Bachelor of Science in Honor Math

Course Highlights: Programming Language, Web Systems, Database Management Systems, Machine Learning, Computer Vision, Mobile App Development for Entrepreneurs, Computer Security, Foundations of Computer Science, Computer Organization, Numerical Linear Algebra , Coding Theory, Algebra I/II

SKILLS

Programming Languages: Python, C/C++, SQL, JavaScript
Framework: PyTorch, TensorFlow, Flask, React

PUBLICATION

Can Attention Masks Improve Adversarial Robustness? February 2020
Pratik Vaishnavi, **Tianji Cong**, Kevin Eykholt, Atul Prakash, Amir Rahmati
In AAAI-2020 Workshop on Engineering Dependable and Secure Machine Learning Systems

RESEARCH EXPERIENCE

Security Research Group, University of Michigan Ann Arbor, Michigan
Research Assistant, advised by Prof. Atul Prakash May 2019 - Present
Guaranteeing AI Robustness against Deception (GARD) Program

- Built and submitted a model that utilizes a hierarchical structure and composed transformations as defenses
- Identified and reported bugs in open source libraries including Adversarial Robustness Toolbox (IBM), ARMORY Adversarial Robustness Evaluation Test Bed (Two Six Labs) , and Foolbox (Bethge Lab)
- Reimplemented ATTA, an efficient adversarial training algorithm, and enabled it for larger datasets on a single GPU

Designing and Evaluating Digital Adversarial Attacks and Defenses for DNN Models

- Investigated the hypothesis that background elimination could make the adversarial attack harder by reducing the attack surface and empirically showed that masking the background could help defend against l_∞-bounded attack
- Developed an end-to-end pipeline that leverages attention masks to enhance the robustness of DNN models
- Benchmarked DNN models on various datasets including GTSRB, Masked MS-COCO, CIFAR-10, and MNIST
- Collected a classification dataset Masked MS-COCO from MS-COCO dataset using Mask R-CNN

Database Research Group, University of Michigan Ann Arbor, Michigan
Research Assistant, advised by Prof. Michael Cafarella May 2019 - December 2019
TAHOMA Video Analytic System

- Led the work of optimizing CNN model search space and built user classifiers for various tasks
- Implemented and debugged a hierarchical video analytic system which generates and evaluates many potential classifier cascades that jointly optimize the CNN architecture and input data representation
- Improved the data storage method that reduces preprocessing costs and query time with space tradeoff

Economic Product Price Predictor

- Preprocessed unbalanced data with various inconsistent quality and built an LSTM model that takes in machine-readable product descriptions and predicts categories for products across 113 categories

- Built a price predictor on top of the category classifier using transfer learning and evaluated model performance and reliability with statistic analysis

Database Research Group, University of Michigan Ann Arbor, Michigan
Research Assistant, advised by Dr. Yongjoo Park August 2018 - October 2018
VerdictDB

- Developed a Python interface using Plotly to visualize streaming data when users wait for the query result
- Tested the VerdictDB tutorial of MySQL/MariaDB setup using docker and provided feedback for its documentation
- Tested the VerdictDB tutorial of TPC-H data setup in MySQL and provided feedback for its documentation

TEACHING EXPERIENCE

Electrical Engineering and Computer Science Department, University of Michigan Ann Arbor, Michigan
Teaching Assistant for EECS 484 Database Management Systems September 2019 - April 2020

- Prepared and Instructed a weekly lab for about twenty students
- Facilitated both physical and virtual office hours to prepare students for homework, projects, and exams
- Developed and reviewed homework and exam questions

WORK EXPERIENCE

English Language Institute, University of Michigan Ann Arbor, Michigan
Program Assistant July 2018 - August 2018

- Facilitated a teacher preparation course for international students who speak English as an additional language
- Provided oral and written feedback for prospective graduate student instructors on the quality of their instruction

PROJECTS

Major Design Project, University of Michigan Ann Arbor, Michigan
Advised by Prof. Elliot Soloway January 2020 - April 2020
CarpoolCruise (Full-stack project using Flask and React, deployed on AWS)

- Developed a centralized open forum that enables UM students to find carpool partners to the airport
- Set up the infrastructure for teammates and iterativly implemented features like the email address confirmation

Intergalactic Mobile Learning Center, University of Michigan Ann Arbor, Michigan
Advised by Prof. Elliot Soloway July 2018 - August 2018
Google Drive Traffic Signal (Published in Chrome Web Store for K-12 education usage)

- Developed a Chrome extension that detects Google Drive connection in real time and logs anomalous activities
- Evaluated several collaborative web applications developed by previous members on various devices and platforms

AWARDS AND HONORS

Awarded Blue Ribbon in UROP's Annual Spring Symposium (2018)
University Honors (2017 Fall - 2020 Winter)