Juyang Bai

(773) 754-6670 — jbai23@jh.edu
https://juyangbai.github.io/
Baltimore, MD

EDUCATION

Johns Hopkins University, Baltimore, MD *Aug 2023 - Present*
Ph.D. in Electrical and Computer Engineering
Northwestern University, Evanston, IL *Sep 2021 - May 2023*
M.S. in Electrical and Computer Engineering, GPA: 4.0/4.0
Zhejiang Sci-Tech University, Hangzhou, Zhejiang *Sep 2017 - Jun 2021*
B.S. in Electrical Information Engineering, Rank: 1/129, GPA: 3.55/5.0 (86/100)

EXPERIENCE

Efficient, Secure and Intelligent Computing Laboratory, Baltimore, MD *Aug 2023 - Aug 2024*
Research Assistant
Supervisor: Deliang Fan
Research focus:

- Propose a novel privacy-preserving DNN model obfuscation framework to obfuscate both model architecture and weights through a reinforcement learning (RL) based searching algorithm.
- Deploy the obfuscated DNN model in real TEE/GPU systems, where only the authorized user with keys could achieve full model functionality and accuracy.
- Explored one-bit flip attacks on soft-IP (AMD-Xilinx DPU) to reveal how malicious tenants can expose soft-IP instructions and mechanisms in both multi-tenant and single-tenant FPGA environments.
- Developed two defense mechanisms against one-bit flip attacks on soft-IP: a rule-based invalid instruction scanning method and a time series-based machine learning approach.

Design Automation of Intelligent Systems Lab, Evanston, IL *May 2022 - May 2023*
Research Assistant
Supervisor: Qi Zhu
Research focus:

- Designed supervised contrastive learning and unsupervised semantics-guided reconstruction methods for vehicle trajectory anomaly detection, demonstrating their effectiveness across various settings.
- Explored and compared various representations and architectures for anomalous trajectory detection in supervised and unsupervised settings, demonstrating the algorithms' ability to generalize to unseen anomaly patterns and analyzing the effectiveness of different modules in the proposed methods.

Ka Moamoa Lab, Evanston, IL *May 2022 - May 2023*
Research Assistant
Supervisor: Josiah Hester
Research focus:

- Develop an external wearable hub that collects and processes data from multiple sensors (IMU, PPG, and ECG) to analyze human activities.
- Implemented a Pulse Transit Time (PTT) algorithm to extract heart rate measurements from combined PPG and ECG signals.

Image and Video Processing Lab, Evanston, IL *Sep 2022 - May 2023*
Research Assistant
Supervisor: Aggelos Katsaggelos
Research focus:

- Develop a preprocessing algorithm to create a matched dataset of cell images from partial-wave spectroscopic (PWS) and confocal microscopy, aligning shape and rotation.
- Develop a UNeXt-based model to translate PWS cell images to their confocal microscopy equivalents, enabling cross-modality image synthesis.

Meng's Lab, Hangzhou, Zhejiang *Mar 2019 - Jun 2021*
Research Assistant
Supervisor: Meng Li

Research focus:

- Developed a line-following Unmanned Ground Vehicle (UGV) for indoor inspections, integrating custom-designed driver boards, infrared tracking modules, PID control for navigation, and Tiny-YOLOv3 for real-time environmental monitoring.
- Proposed and implemented a DCNN-based fish classification system for challenging underwater environments, utilizing transfer learning and image augmentation to achieve 89% accuracy with limited data and computational resources.
- Developed a line patrol drone for electrical transmission inspection, incorporating Mahony complementary filtering for attitude adjustment, Kalman filtering for multi-sensor data fusion, and cascade PID control for precise navigation.

PUBLICATIONS

Phantom: Privacy-Preserving Deep Neural Network Model Obfuscation in Heterogeneous TEE and GPU Systems
USENIX Security 2025 (Under Review)
Juyang Bai, Md Hafizul Islam Chowdhuryy, Jingtao Li, Fan Yao, Chaitali Chakrabarti, Deliang Fan
From Threat to Defense: Cross-Tenant Denial of Service Attack in Multi-tenant FPGA System and the Evolution of Hypervisor
(On Manuscript)
Yukui Luo*, **Juyang Bai***, Sabbir Ahmed, Adnan Siraj Rakin, Deliang Fan, Xiaolin Xu
Learning Representation for Anomaly Detection of Vehicle Trajectories
IROS 2023
Ruochen Jiao, **Juyang Bai**, Xiangguo Liu, Takami Sato, Xiaowei Yuan, Qi Alfred Chen, Qi Zhu
Towards a Toolkit for Free Living Wearable Development
HASCA, 2022
Blaine Rothrock, Alexander Curtiss, **Juyang Bai**, Josiah Hester
Fish Image Classification Using Deep Convolutional Neural Network
CIPAE 2020
Xiaojuan Lan, **Juyang Bai**, Meng Li, Jiajun Li.

HONORS And AWARDS

Government Scholarship in Zhejiang Province	*Nov 2020*
First-class Scholarship	*Oct 2020*
3rd Place China Collegiate Computing Contest-Network Technology Challenge	*Oct 2020*
Second-class Scholarship & Merit Student	*Nov 2019*
1st Place Softbank Robot Cup Wheeled Robot Sprint Group	*Nov 2019*
3rd Place Softbank Robot Cup Biped Robot Dance Group	*Nov 2019*
First-class Scholarship for Freshman	*Sep 2017*

TEACHING EXPERIENCE

EN.520.231 - Mastering Electronics Lab *Fall 2024*
Role: Teaching Assistant
Instructor: Sathappan Ramesh

SERVICE

Reviewer
IROS, DATE

TECHNICAL SKILLS

Programming Skills: Python, C/C++, CUDA, Matlab, LaTeX
Deep Learning Tools: Pytorch, Tensorflow
Tools: Git, Blender, SolidWorks
GRE: 166(Verbal) + 170(Math) + 4.5(Writing)