Joshua C. Zhao

Purdue University zhao1207@purdue.edu joshuaczhao.github.io joshua-c-zhao

Research Summary

My research focuses on machine learning with an emphasis on building scalable, reliable, and robust systems. As a machine learning security researcher, I am particularly passionate when learning about new systems and improving the safety (reliability of the models and the ethical uses) of real world deep learning applications.

My work has been published in top computer vision, security, and systems conferences (CVPR, IEEE S&P, AsiaCCS, DSN-S), ranging from data privacy and model reliability under data heterogeneity (key problems in real-world deployments of large-scale settings in federated learning) to model robustness (reliability, adversarial machine learning, and efficient robust transfer learning). One of my recent works also explores using foundation models to improve weakly supervised point cloud semantic segmentation.

During my time at Woven by Toyota, I have also worked in autonomous driving / ADAS, where my work in perception focused on training models for both occupancy prediction as well as occupancy flow.

Computer skills: Deep Learning (PyTorch, Tensorflow, Keras), Machine Learning (Scikit-learn, XGBoost, etc.), Python (NumPy, Pandas, etc.), MATLAB, C/C++, LaTeX, Microsoft Office (Excel, Powerpoint)

Education

Purdue University, West Lafayette, IN — Aug 2021 - May 2026 (Anticipated)
Ph.D. in Electrical and Computer Engineering

Northwestern University, Evanston, IL — Sept 2020 – March 2021
BS/MS in Computer Engineering and Computer Science

Publications

C = Conference, W = Workshop, J = Journal, S = Under Submission

[C.1] **Joshua C. Zhao**, Atul Sharma, Ahmed Roushdy Elkordy, Yahya H. Ezzeldin, Salman Avestimehr, Saurabh Bagchi, "*LOKI: Large-scale Data Reconstruction Attack against Federated Learning through Model Manipulation.*" IEEE Symposium on Security & Privacy, 2024 (pp. 1287-1305). (Acceptance rate: 261/1463 = 17.8%)

[C.2] **Joshua C. Zhao**, Ahaan Dabholkar, Atul Sharma, Saurabh Bagchi. "*Leak and Learn: An Attacker's Cookbook to Train Using Leaked Data from Federated Learning.*" IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2024 (pp. 12247-12256). (Acceptance rate: 2719/11532 = 23.6%)

[C.3] **Joshua C. Zhao**, Ahmed Roushdy Elkordy, Atul Sharma, Yahya H. Ezzeldin, Salman Avestimehr, Saurabh Bagchi, "*The Resource Problem of Using Linear Layer Leakage Attack in Federated Learning.*" IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2023 (pp. 3974-3983). (Acceptance rate: 2360/9155 = 25.8%)

[C.4] Atul Sharma, Wei Chen, **Joshua C. Zhao**, Qiang Qiu, Saurabh Bagchi, and Somali Chaterji. "*FLAIR: Defense against Model Poisoning Attack in Federated Learning.*" ACM ASIA Conference on Computer and Communications Security, 2023 (pp. 553-566). (Acceptance rate: 32/200 = 16.0%)

[W.1] Atul Sharma, **Joshua C. Zhao**, Wei Chen, Qiang Qiu, Saurabh Bagchi, and Somali Chaterji. "*How to Learn Collaboratively – Federated Learning to Peer-to-Peer Learning and What's at Stake.*" DSN Disrupt (DSN-S), 2023 (pp. 122-126). (Acceptance rate: 17/36 = 47.2%)

[J.1] **Joshua C. Zhao**, S. Bagchi, S. Avestimehr, K. Chan, S. Chaterji, D. Dimitriadis, J. Li, N. Li, A. Nourian, H. Roth, "*The Federation Strikes Back: A Survey of Federated Learning Privacy Attacks, Defenses, Applications, and Policy Landscape.*" ACM Computing Surveys (CSUR), 2025 (pp. 1-37).

[J.2] Yingyi Luo, **Joshua C. Zhao**, Arnav Aggarwal, Seda Ogrenci-Memik, and Kazutomo Yoshii. "*Thermal Management for FPGA Nodes in HPC Systems.*" ACM TODAES, 2020 (26, pp.1-17).

[S.1] **Joshua C. Zhao**, Ahaan Dabholkar, Saurabh Bagchi, "*Separate Classes, Separate Features? Separate Class Adversarial Training Reconciles Robust and Non-robust Features.*" (pp. 1-18).

[**S.2**] **Joshua C. Zhao**, Saurabh Bagchi, "*Are Fast Methods Stable in Adversarially Robust Transfer Learning?*" (pp. 1-13).

[**S.3**] Kasra Derakhshandeh, **Joshua C. Zhao**, Somali Chaterji, "*SEEMSeg: Calibration of SEEM for Weakly Supervised Point Cloud Semantic Segmentation.*" (pp. 1-16).

Research and Professional Experience

Autolabeling for Autonomous Driving / ADAS | Woven by Toyota Palo Alto, CA
Internship | Mentor: Chris Ochoa June 2025 - Sept 2025

- Developed an occupancy flow prediction head for the AD/ADAS autolabeling model, including the ground truth generation, model design, and performance evaluation.

Distributed Learning and Adversarial Machine Learning | Purdue University West Lafayette, IN
Research | Mentor: Prof. Saurabh Bagchi | CVPR, IEEE S&P, AsiaCCS, DSN-S, CSUR April 2021 - Present

- Demonstrated that federated learning with secure aggregation (and FedAvg) is still susceptible to large-scale data reconstruction (privacy) attacks.
- Evaluated robust aggregation techniques in distributed/federated learning and developed a new aggregation design that provides robustness with up to 45% byzantine clients (security and reliability).
- Demonstrated that FGSM is an effective alternative to PGD when fine-tuning in robust transfer learning, losing as 0.35% robustness on average while using 4× less training time.
- Explored natural accuracy and robustness in adversarial machine learning, showing that achieving high robustness with very little sacrifice in natural accuracy is possible.

Machine Learning FPGA Temperature Prediction | Northwestern University Evanston, IL
Research | Mentor: Prof. Seda Memik | ACM TODAES June 2019 - March 2021

- Developed machine learning models to predict the temperature of FPGAs and applied them in task placement, decreasing the peak temperature in a system of FPGAs by up to 26.4°C.
- Performed feature selection, model selection, and parameter tuning to minimize the prediction error of a machine learning model to below 1.3 °C on average when predicting FPGA peak temperature.

PyTorch3D and Computational Imaging | Undergraduate Research Evanston, IL
Research | Mentor: Prof. Oliver Cossairt Oct 2019 - March 2021

- Implemented a rendering pipeline using PyTorch3D that renders multiple new images using 2.5D (color and depth) information and light sources at different locations.
- Designed and trained an encoder deep learning network to generate 3D face information using inputs of rendered images through PyTorch3D. Applied the rendering process into the training as a custom regularization term in order to improve the actual rendering quality.

Awards, Services, and Teaching

- **Guest lecturer at Purdue University** for ECE 60872 (Fault-Tolerant Computer System Design). I gave the two following lectures on ML security:
  - How reliable is your model? (adversarial machine learning)
  - Distributed machine learning, a secure and private alternative?

- **Reviewer:** ICCV, CVPR, CVPR FedVision, NeurIPS, AAAI

- **Head of NSF Center CHORUS Student Committee.** Organize virtual seminars/panels across 4 universities and industry partners. Per-semester newsletters summarizing the happenings in the CHORUS center.

Awards:

- Bilsland Dissertation Fellowship
- Purdue Andrews Fellowship
- DCSL Best Fresher Award, Group Champion Award
- Eta Kappa Nu, Beta Tau Chapter (Electrical Engineering Honor Society)
- Tau Beta Pi (Engineering Honor Society)
- Northwestern University Summer Undergraduate Research Fellowship