

# Joshua C. Zhao

📍 Purdue University    ✉ zhaol207@purdue.edu    🌐 joshuaczhao.github.io    in joshua-c-zhao

## Research focus

I am interested in deep learning and machine learning with a primary focus on security and privacy. My previous research publications have been in federated learning privacy and distributed learning robustness. I am currently working on projects improving the robustness and generalization trade-off in adversarial machine learning.

## Education

**Purdue University**, West Lafayette, IN Aug 2021 - May 2026  
(Anticipated)  
*Elmore Family School of Electrical and Computer Engineering*  
*Ph.D. in Electrical and Computer Engineering*

- Purdue Andrews Fellowship

**Northwestern University**, Evanston, IL Sept 2017 – March 2021  
*Robert R. McCormick School of Engineering and Applied Science*  
*BS in Computer Engineering, MS in Computer Science*

- Eta Kappa Nu, Beta Tau Chapter (Electrical Engineering Honor Society)
- Tau Beta Pi (Engineering Honor Society)

## 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. 30-30). (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.*” Accepted to IEEE/CVF CVPR, 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 CVPR, 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 AsiaCCS, 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] Yingyi Luo, **Joshua C. Zhao**, Arnav Aggarwal, Seda Ogreni-Memik, and Kazutomo Yoshii. “*Thermal Management for FPGA Nodes in HPC Systems.*” ACM TODAES, 2020 (26, pp.1-17).
- [S.1] **JC. Zhao**, S. Bagchi, S. Avestimehr, K. Chan, S. Chaterji, D. Dimitriadis, J. Li, N. Li, A. Nourian, H. Roth, “*Federated Learning Privacy: Attacks, Defenses, Applications, and Policy Landscape - A Survey.*” Under submission to ACM Computing Surveys (CSUR).

## Research Experience

**Graduate Research** Purdue University  
*Prof. Saurabh Bagchi’s Lab, Dependable Computing Systems Laboratory (DCSL)* April 2021 - Present

- Developed an attack against secure aggregation **federated learning** that arbitrarily scales towards FedAVG aggregation. The attack **leaks 85% of total user data** while prior work leaks less than 1% of user data. Furthermore, identified that FedAVG (a typically more challenging scenario) is more susceptible to attacks than FedSGD. Work accepted to **IEEE S&P 2024** as first author.
- Explored the reconstruction quality of various methods of data reconstruction attacks for downstream tasks. Models trained centrally on the leaked data **perform up to 20.4% better than federated learning** even with an

extremely limited amount of data or low quality images. Accepted for publication at **CVPR 2024** as first author.

- Discovered the resource problems of privacy attacks on large scale federated learning with linear layer leakage. Using a sparse attack method we **decrease model size overhead by over 327x and computation time by 3.34x compared to SOTA** while maintaining an equivalent leakage rate. Work is accepted at **CVPR 2023** as first author.
- Evaluated the robustness of aggregation techniques in federated learning against malicious clients and developed a new aggregation design that provides **robustness with up to 45% malicious clients**. Work published in **AsiaCCS 2023**.

#### **Undergraduate Research**

*Prof. Seda Memik's Lab, Dept. of Electrical Computer Engineering*

*Northwestern University*

*June 2019 - March 2021*

- Investigated deep learning on chips with hardware-induced weight loss (coming from loss of power).
- Training DS-CNN networks for keyword spotting tasks and testing accuracy with different dropout rates being applied during the testing phase. Also testing model accuracy when random weight decay is applied on model parameters.
- Developed machine learning models using python 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.

#### **Undergraduate Research**

*Prof. Oliver Cossairt's Lab, Dept. of Computer Science*

*Northwestern University*

*Oct 2019 - March 2021*

- Developed a convolutional neural network in PyTorch to generate 3D face structure from single in-the-wild images. Training data generated through a 3D morphable head model.
- Designed and trained an encoder deep learning network to generate 3D face information using inputs of rendered images through PyTorch3D. In addition, applied the rendering process into the training as a custom regularization term in order to improve the actual rendering quality.
- Implemented a rendering process in PyTorch3D that takes in 2.5D (color and depth) information and renders multiple new images using light sources at different locations.
- Created an optimization framework to iteratively estimate surface normals of a scene using images under different lighting.
- Investigated image registration for 3D surface measurements of specular objects using feature-based alignment algorithms.

## **Other**

#### **Peer Mentor – CS 349 Machine Learning**

*Undergraduate TA*

*Northwestern University*

*Mar 2020 – June 2020*

- Peer mentor for Spring 2020, CS 349 Machine Learning.
- Graded student homework and held weekly office hours to explain difficult concepts in the course and also assist students in homework issues.

#### **Kellogg School of Management, Career Management Center**

*Work Study Student*

*Northwestern University*

*Mar 2020 – June 2020*

- Worked on data entry, summarization, and presentation for CMC career advising workshops and student advising.
- Directing students to the appropriate advisers from the front desk and answered phone calls relating to the Career Management Center.

#### **Design Thinking and Communication Courses 1&2**

*Design project*

*Northwestern University*

*Sept 2017 – June 2018*

- Developed and produced a portable device to assist people with arthritis in opening sealed bottles.
- Designed a cooking measuring set for three-year olds to use safely and effectively in the kitchen.
- Worked as a group of four to design and prototype the above products and present it at the design fair and to our client.

#### **NU Solar Car Electrical Team**

*Team Member*

*Northwestern University*

*Oct 2017 – Oct 2018*

- *Goal:* Develop a solar car as a team to compete in the annual Formula Sun Grand Prix.
- Programming an Arduino-based touch screen LED to display key information during driving.
- Performed heat shrinking, wire crimping, soldering, and other electrical tasks.