Joshua C. Zhao

zhao1207@purdue.edu - LinkedIn

EDUCATION

***Purdue University**, West Lafayette IN*

Elmore Family School of Electrical and Computer Engineering

Ph.D. in Electrical and Computer Engineering — Aug 2021 – May 2026 (Anticipated)

- Purdue Andrews Fellowship

***Northwestern University**, Evanston IL*

Robert R. McCormick School of Engineering and Applied Science

BS in Computer Engineering, MS in Computer Science — Sept 2017 – March 2021

- *Eta Kappa Nu, Beta Tau Chapter (Electrical Engineering Honor Society)* — Dec 2019 – Present
- *Tau Beta Pi (Engineering Honor Society)* — Oct 2020 – Present

Research focus: I am broadly interested in deep learning and machine learning with a primary focus on machine learning security and privacy. My main research publications have been in federated learning privacy and distributed learning robustness.

PUBLICATIONS

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%)

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%)

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%)

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).

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%)

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).

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).

ENGINEERING EXPERIENCE

***Prof. Saurabh Bagchi's Lab**, Dept. of Electrical and Computer Engineering, Purdue University*

Graduate Research

- Developed an attack against secure aggregation FL that arbitrarily scales towards **FedAVG** aggregation. The attack **leaks roughly 85% of total user data** while prior work leaks less than 1% of user data. Furthermore, identified that FedAVG (a typically more challenging scenario to attack) is more susceptible to attacks than FedSGD. Work accepted to **IEEE S&P 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.
- 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.
- 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**.

April 2021 - Present

Prof. Seda Memik's Lab*, Dept. of Electrical Computer Engineering, Northwestern University*
Undergraduate Research

- Currently investigating 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

June 2019 - March 2021

Prof. Oliver Cossairt's Lab, *Dept. of Computer Science, Northwestern University*
Undergraduate Research

- Developing a convolutional neural network in PyTorch to generate 3D face structure from single in-the-wild images. Training data will be 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.

Oct 2019 - March 2021

Prof. Chris Chu's Lab*, Dept. of Electrical and Computer Engineering, Iowa State University*
Undergraduate Research

- Programmed a machine-learning artificial neural net in python using only the standard libraries and NumPy and trained the model using the MNIST data set to recognize handwritten numbers

June 2018 – Sept 2018

Design Thinking and Communication Courses 1&2*, Northwestern University*
Student

- Developed and produced a portable device to assist people with arthritis in opening sealed bottlers
- 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

Sept 2017 – June 2018

NU Solar Car Electrical Team*, Northwestern University*
Team Member

- *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

Oct 2017 – Oct 2018