Shuli Jiang

shulij@andrew.cmu.edu @11hifish Google Scholar
https://11hifish.github.io/

Research Interests

I am a fifth-year Ph.D. student at the School of Computer Science, Carnegie Mellon University, advised by Prof. Gauri Joshi. My research spans the theory and applications of machine learning optimization, differential privacy, distributed learning, communication efficiency, and the security of large language models (LLMs).

Education

August 2020 – present
Carnegie Mellon University, Pittsburgh, PA, USA
Ph.D. student at the Robotics Institute, School of Computer Science
Advisor: Prof. Gauri Joshi
Expected Graduation Date: June 2025

May 2019 – May 2020
Carnegie Mellon University, Pittsburgh, PA, USA
M.S. in Computer Science
Thesis title: *Deep Multi-view Clustering Using Local Similarity Graphs*
Advisor: Prof. Artur Dubrawski

August 2015 – May 2019
Carnegie Mellon University, Pittsburgh, PA, USA
B.S. in Computer Science, University Honor
Minor: Electrical and Computer Engineering

Research Publications

($\alpha\beta$: alphabetical order, $**$: contribution order)

In Submission

1. (**) Shuli Jiang, Pranay Sharma, Zhiwei Steven Wu, Gauri Joshi
   The Cost of Shuffling in Private Gradient Based Optimization
   In Submission to ICML 2025 Link

Preprints

1. (**) Shuli Jiang, Swanand Ravindra Kadhe, Yi Zhou, Farhan Ahmed, Ling Cai, Nathalie Baracaldo
   Turning Generative Models Degenerate: The Power of Data Poisoning Attacks
   arXiv 2024 Link

Conference / Journal Proceedings

1. ($**$) Shuli Jiang, Qiuyi Richard Zhang, Gauri Joshi
   Optimized Tradeoffs for Private Prediction with Majority Ensembling
   Transaction on Machine Learning Research (TMLR November 2024) Link
2. ($**$) Shuli Jiang, Pranay Sharma, Gauri Joshi
   Correlation Aware Sparsified Mean Estimation Using Random Projection Link Code
   The Thirty-seventh Conference on Neural Information Processing Systems (NeurIPS 2023)
3. ($**$) Shuli Jiang, Robson Leonardo Ferreira Cordeiro, Leman Akoglu

D.MCA: Outlier Detection with Explicit Micro-Cluster Assignments Link Code

The Twenty-second IEEE International Conference on Data Mining (ICDM 2022)

4. ($\alpha\beta$) Shuli Jiang, Hai Thanh Pham, David P. Woodruff, Qiuyi Richard Zhang

   Optimal Sketching for Trace Estimation Link Code

   The Thirty-fifth Conference on Neural Information Processing Systems (NeurIPS 2021 Spotlight)

5. ($\alpha\beta$) Shuli Jiang, Dongyu Li, Irene Mengze Li, Arvind V. Mahankali, David P. Woodruff

   Streaming and Distributed Algorithms for Robust Column Subset Selection Link Code

   The Thirty-eighth International Conference on Machine Learning (ICML 2021)

6. (**) Bohan Zhang, Dana Van Aken, Justin Wang, Tao Dai, Shuli Jiang, Jacky Lao, Siyuan Sheng, Andrew Pavlo, Geoffrey J. Gordon

   A Demonstration of the OtterTune Automatic Database Management System Tuning Service Link Code

   The VLDB Endowment, Vol. 11, No. 12 (VLDB 2018)

Workshop Proceedings

1. (**) Shuli Jiang, Swanand Kadhe, Yi Zhou, Ling Cai, Nathalie Baracaldo

   Forcing Generative Models to Degenerate Ones: The Power of Data Poisoning Attacks Link

   NeurIPS 2023 Workshop on Backdoors in Deep Learning - The Good, the Bad, and the Ugly (Best Poster Award)

Technical Reports

1. ($\alpha\beta$) Theresa Gebert, Shuli Jiang, Jiaxian Sheng

   Characterizing Allegheny County Opioid Overdoses with an Interactive Data Explorer and Synthetic Prediction Tool Link Code

   HackAuton Best Show Prize, 2018

2. Shuli Jiang

   Deep Multi-view Clustering Using Local Similarity Graphs Link

   Master's Thesis, 2020, Advisor: Prof. Artur Dubrawski

Patent

April 2024

Inventors: Shuli Jiang, Swanand Kadhe, Yi Zhou, Ling Cai, Nathalie Baracaldo
Title: **A System and Method to Defend Against Data Poisoning Attacks Targeting Generative LLMs**
Reference number: P202303734US01
Filed by IBM Research

Work Experience

January 2025 - April 2025

Google Research, Remote in Pittsburgh, PA, USA
Student Researcher (Part-Time)
Manager: Nicolas Mayoraz
Focus: Differential Privacy, Recommender Systems
Continue working on private learning for recommender systems.

September 2024 - November 2024

Google Research, Remote in Pittsburgh, PA, USA
Student Researcher (Part-Time)
Manager: Walid Krichene, Nicolas Mayoraz
Focus: Differential Privacy, Recommender Systems
Continue working on private learning for recommender systems.

May 2024 - August 2024

Google Research, Mountain View, CA, USA
Student Researcher
Manager: Walid Krichene, Nicolas Mayoraz
Focus: Differential Privacy, Recommender Systems
Design differentially private learning algorithms for training models, such as Factorization Machines, for ads prediction and recommender systems. Our focus is on scenarios where datasets contain both private and public features, exploring how to leverage public features to improve the privacy-utility trade-off.

May 2023 - August 2023

IBM Research (Almaden), San Jose, CA, USA
Research Summer Intern (AI Security and Privacy Solutions)
Advisor: Swanand Kadhe, Manager: Nathalie Baracaldo
Focus: Large Language Model (LLM) Security
Investigate security vulnerabilities of large language models (LLMs) in terms of data poisoning attacks targeting natural language generation (NLG) tasks, including text summarization, text completion, table-to-text generation, etc. Design and develop defense strategies to counter-attack those types of security threats to LLMs.

June 2018 - August 2018

Morgan Stanley, New York City, NY, USA
Technology Analyst (Application Development)
Focus: Outlier Detection
Develop a data quality management system which collects real-time trading data from multiple source databases, detects potential anomalies to ensure data quality and visualizes anomalous data.

June 2017 - August 2017

PreSenso Ltd., Haifa, Israel
Software Engineer Intern
Focus: Outlier Detection
Develope an anomaly detection benchmark for evaluating and comparing the performances of different anomaly detection algorithms on various patterns of anomalies.

Public Talks

September 2024

CMU CyLab Security & Privacy Institute Partners Conference
Topic: Differentially Private Incremental Gradient (IG) Methods with Public Data

Public Talks (continued)

- February 2024 — NSF CPS Frontier Annual Review Lightening Talk (3-min)
  Topic: Distributed Vector Mean Estimation
- September 2023 — AI-EDGE Students and Postdocs gathering for AI Research and Knowledge Sharing (AI-EDGE SPARKS)
  Topic: Federated Learning and Distributed Vector Mean Estimation
- May 2023 — CMU Robotics Institute Ph.D. Speaking Qualifier Public Talk
  Topic: Differential Privacy and Private Majority Ensembling

Service

- Conference/Workshop Reviewer — SODA 2022, SIGKDD 2023, NeurIPS 2023, ICLR 2024, AISTATS 2024, SDM 2024, ISIT 2024, NeurIPS 2024, ICLR 2025, AISTATS 2025, MLSys 2025, ICML 2025
- Workshop Reviewer — AAAI The First Workshop on DL-Hardware Co-Design for AI Acceleration 2023, ICLR Workshop R2-FM 2024, ICML Workshop FM-Wild 2024, 2025, AutoML Workshop 2024
- Journal Reviewer — IEEE/ACM Transactions on Networking 2023, Data-centric Machine Learning Research (DMLR) 2024
- Department Service — CMU Robotics Institute Ph.D. Admission Committee 2023, 2024

Teaching Assistantship

- Fall 2022 — **16-831 Statistical Techniques in Robotics**, @ Carnegie Mellon University
- Fall 2020 — **10-725 Convex Optimization**, @ Carnegie Mellon University
- Fall 2017 — **17-214 Principles of Software Construction**, @ Carnegie Mellon University

Technical Skills

- Programming — Python, Java, Matlab (Basic), C (Basic)
- Tools — Python: {Tensorflow, PyTorch, Pandas}, LaTeX

Awards

- 2023 — NeurIPS 2023 Scholar Award
- 2022 — IEEE ICDM 2022 Student Travel Award ($ 700)
- Graduate Student Assembly/Provost Conference Travel Grant ($ 750)
- 2019 — Carnegie Mellon University Undergraduate University Honor
- 2015 – 2019 — Carnegie Mellon University Undergraduate Dean's List
- 2018 — HackAuton Best Show Prize
- 2017 – 2019 — Carnegie Mellon University Innovation Scholar
- 2017 — Buncher Entrepreneurship Award ($ 10, 000)