Sina Sajadmanesh

linkedin.com/in/sajadmanesh
sina.sajadmanesh@gmail.com
(+41) 787812478
Zurich, Switzerland

Education

- Ph.D. in Electrical Engineering (GPA: 5.75 / 6) — May 2019 – Aug 2023
  Swiss Federal Institute of Technology (EPFL), Lausanne, Switzerland
- M.Sc. in Information Technology Engineering (GPA: 18.1 / 20) — Sep 2014 – Sep 2016
  Sharif University of Technology, Tehran, Iran
- B.Sc. in Computer Software Engineering (GPA: 16.19 / 20) — Sep 2009 – Feb 2014
  University of Isfahan, Esfahan, Iran

Professional Experience

- AI Engineer
  Sony AI, Zurich, Switzerland — October 2023 – Present

  Working as a member of the Privacy-Preserving Machine Learning team to contribute to the development of secure and trustworthy AI solutions.

  - **Developed an end-to-end classification pipeline** using OpenMMLab frameworks and HuggingFace to train and test privacy-preserving **vision foundation models** for Sony's next-generation AI products.
  - **Improved the speed of training and inference** of models by optimizing the code and leveraging distributed computing.

- Research Assistant
  Idiap Research Institute, Martigny, Switzerland — May 2019 – August 2023

  Worked as a doctoral researcher on privacy-preserving graph neural network (GNN) models using differential privacy to reduce privacy risks in real applications, such as recommendation systems and knowledge graphs.

  - **published three papers** in top conferences: CCS, USENIX, and WSDM, **received over 120 citations** since 2021 and delivered **more than 6 invited talks** at top institutions and companies, such as Imperial College London, University of Illinois, and Twitter.
  - **Implemented locally private GNN models** using PyTorch-Geometric that enables online social networks to learn from their users' data without compromising their privacy. **Received over 38 stars and 13 forks** on GitHub.
  - **Developed differentially private GNN solutions** using PyTorch-Geometric, Opacus, and Auto-DP that enables privacy-preserving training and inference of GNNs. **Received over 40 stars and 12 fork** on GitHub.
  - **Finalist** in CSAW Applied Research Competition for the best paper award in computer security in Europe.
  - **Offered a travel grant** to attend CISPA Summer School 2022 on Trustworthy Artificial Intelligence in Germany.

- Visiting Collaborator
  The Alan Turing Institute, London, UK — March 2023

  Joined the Safe and Ethical AI group as a visiting PhD student.

  - **Co-organized a workshop** on Privacy and Fairness in AI for Health with **11 invited speakers** from top research institutes and companies, such as Oxford, Microsoft, and DeepMind, and **over 60 attendees**.

- Research Intern
  Brave Software, San Francisco, CA, USA (Remote) — Mar 2022 – May 2022

  Recruited as a member of the research team to contribute to privacy-preserving machine learning research, aiming to improve Brave Browser's ads and news recommendation systems.

  - **Developed an experimental framework** to train and evaluate federated neural bandits under client heterogeneity using PyTorch and Flower for server-side simulation and Tensorflow-Lite for mobile clients.

- Data Engineer
  Sharif ICT Innovation Center, Tehran, Iran Sep 2018 – May 2019

  Served in a part-time role as a member of an R&D team to develop a native big-data processing platform.

  - **Conducted a comprehensive study on massively scalable graph databases**, such as Neo4j, OrientDB, and JanusGraph, by setting up, configuring, and benchmarking them on a computing cluster.
  - **Developed a dashboard** to discover key insights from customers' data using Kibana, Elasticsearch, and Cassandra.

- Research Assistant
  Sharif University of Technology, Tehran, Iran Nov 2014 – May 2019

  Worked in the Data Science and Machine Learning Lab on a range of research projects in the areas of privacy-preserving machine learning, web data science, and social and information network analysis.

  - **published four papers** in top-tier venues, including IEEE IoTJ, ACM TKDD, and TheWebConf, **with over 410 citations** since 2016.
  - Worked on a hybrid mobile-server learning architecture based on Siamese fine-tuning and split learning to make non-private pre-trained deep learning models privacy-preserving at the inference stage.
  - **Conducted large-scale data analysis** using a collection of recipes published on the web and their content, aiming to understand cuisines and culinary habits around the world. **Received media coverage** from prominent news outlets, such as MIT Technology Review, The Independent, and France 24.
  - **Developed time-aware link prediction algorithms** over heterogeneous social networks using recurrent neural networks and non-parametric machine learning.
  - Received **full PhD studentship** from IBM-ILLINOIS Center for Cognitive Computing Systems Research and The Hong Kong University of Science and Technology.

Teaching Experience

- Lecturer
  International AI Doctoral Academy (AIDA), Online

  Course: An Introduction to Trustworthy Machine Learning, November 2022

  Website: https://www.i-aida.org/course/an-introduction-to-trustworthy-machine-learning/

- Lecturer
  Sharif University of Technology, Tehran, Iran

  Course: Fundamentals of Programming (Python), Fall 2017

  Website: http://ce.sharif.edu/courses/96-97/1/ce153-12/

- Teaching Assistant
  Swiss Federal Institute of Technology (EPFL), Lausanne, Switzerland

  Courses: Computational Social Media (Spring 2021, 2022, and 2023)

- Teaching Assistant
  Sharif University of Technology, Tehran, Iran

  Courses: Artificial Intelligence (Spring 2017), Advanced Topics in Artificial Intelligence - Statistical Learning Theory (Spring 2016), Engineering Probability and Statistics (Spring 2016)

- Teaching Assistant
  University of Isfahan, Esfahan, Iran

  Courses: Artificial Intelligence (Fall 2013), Advanced Computer Programming 2 - JavaFx and Android (Fall 2012), Computer Programming - Java (Fall 2011), Computer Programming - C++ (Fall 2010)

Community and Professional Services

- **Invited Speaker:** Imperial College London (2023, 2020), University of Illinois at Chicago (2022), L3S Research Center (2022), Graph Neural Networks User Group Meetup (2021), Twitter Machine Learning Seminar (2021)

- **Organizing Committee:** Privacy and Fairness in AI for Health (2023)
- **Program Committee:** AAAI Privacy-Preserving AI (2024), Wireless Security and Machine Learning (WiseML) (2023), ICLR PAIR2Struct (2022)
- **Reviewer:** IEEE Transactions on Dependable and Secure Computing (2023), Learning on Graphs Conference (2023, 2022), International Conference on Artificial Intelligence and Statistics (AISTATS) (2023), Artificial Intelligence Journal (2022), IEEE Transactions on Big Data (2021), ICLR Workshop on Distributed and Private Machine Learning (2021), ACM Transactions on Intelligent Systems and Technology (2020), Social Network Analysis and Mining Journal (2020), World Wide Web Journal (2018)

Skills and Expertise

- **Programming and Scripting Languages:** Python, Java, C++, Shell Scripting, SQL, LaTeX
- **Machine Learning & Data Analysis:** PyTorch, PyTorch-Geometric, Tensorflow, Tensorflow-Lite, OpenMMLab, HuggingFace, Scikit-Learn, Pandas, Numpy
- **MLOps & Related Technologies:** Weights & Biases, PyTorch-Lightning, Dask, Git, GitHub, Linux, Docker
- **Privacy-Enhancing Technologies:** Flower, Opacus, Auto-DP

Publications

- Sina Sajadmanesh and Daniel Gatica-Perez
  ProGAP: Progressive Graph Neural Networks with Differential Privacy Guarantees
  ACM International Conference on Web Search and Data Mining **(WSDM)**, March 2024
- Sina Sajadmanesh and Daniel Gatica-Perez
  Privacy-Preserving Machine Learning on Graphs
  Ecole Polytechnique Fédérale de Lausanne **(PhD Thesis)**, 2023
- Sina Sajadmanesh, Ali Shahin Shamsabadi, Aurélien Bellet, and Daniel Gatica-Perez
  GAP: Differentially Private Graph Neural Networks with Aggregation Perturbation
  USENIX Security Symposium **(USENIX Security)**, Aug 2023
- Sina Sajadmanesh and Daniel Gatica-Perez
  Locally Private Graph Neural Networks
  ACM Conference on Computer and Communications Security **(CCS)**, Nov 2021
- Sina Sajadmanesh and Daniel Gatica-Perez
  When Differential Privacy Meets Graph Neural Networks
  Technical Report, ArXiv e-prints, Jun 2020
- Seyed Ali Osia, Ali Shahin Shamsabadi, Sina Sajadmanesh, *et al.*
  A Hybrid Deep Learning Architecture for Privacy-Preserving Mobile Analytics
  IEEE Internet of Things Journal **(IoTJ)**, May 2020
- Sina Sajadmanesh, Sogol Bazargani, Jiawei Zhang, and Hamid R. Rabiee
  Continuous-Time Relationship Prediction in Dynamic Heterogeneous Information Networks
  ACM Transactions on Knowledge Discovery from Data **(TKDD)**, Aug 2019
- Sina Sajadmanesh, Jiawei Zhang, and Hamid R. Rabiee
  NPGLM: A Non-Parametric Method for Temporal Link Prediction
  Technical Report, ArXiv e-prints, Jun 2017
- Sina Sajadmanesh, Sina Jafarzadeh, Seyed Ali Ossia, *et al.*
  Kissing Cuisines: Exploring Worldwide Culinary Habits on the Web
  International World Wide Web Conference Companion **(WWW)**, Apr 2017
- Sina Sajadmanesh, Hamid R. Rabiee and Ali Khodadadi
  Predicting Anchor Links between Heterogeneous Social Networks
  International Conference on Advances in Social Networks Analysis and Mining **(ASONAM)**, Aug 2016