



Sina Sajadmanesh

 [linkedin.com/in/sajadmanesh](https://www.linkedin.com/in/sajadmanesh)
 sina.sajadmanesh@gmail.com

 (+41) 787812478
 Zurich, Switzerland

EDUCATION

Ph.D. in Electrical Engineering (GPA: 5.75 / 6)
Swiss Federal Institute of Technology (EPFL), Lausanne, Switzerland May 2019 – Aug 2023

M.Sc. in Information Technology Engineering (GPA: 18.1 / 20)
Sharif University of Technology, Tehran, Iran Sep 2014 – Sep 2016

B.Sc. in Computer Software Engineering (GPA: 16.19 / 20)
University of Isfahan, Esfahan, Iran Sep 2009 – Feb 2014

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.

Research Assistant
Idiap Research Institute, Martigny, Switzerland, May 2019 – August 2023
*Recruited as a doctoral researcher to contribute to **AI4Media**, a European research project focusing on ethical and trustworthy AI to serve media and society. Developed privacy-preserving graph neural network (GNN) models using differential privacy to reduce privacy risks in real applications, such as recommendation systems and knowledge graphs.*

- Conducted high-quality and impactful research: **published two papers** in top conferences, namely, **ACM CCS** and **USENIX Security**, and one under review, **received over 60 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 a differentially private GNN model** using **PyTorch-Geometric**, **Opacus**, and **Auto-DP** that enables privacy-preserving training and inference of GNNs. **Received over 20 stars and 1 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 to contribute to their ongoing research on trustworthy AI.*

- **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.*

- **Hand-picked to work on a project** about federated reinforcement learning for privacy-preserving recommendation.
- **Developed an experimental framework** to evaluate the performance of 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 for the center.

- **Conducted a comprehensive study on massively scalable graph databases**, such as [Neo4j](#), [OrientDB](#), and [Janus-Graph](#), 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

Joined the Data Science and Machine Learning Lab as a master's student and continued as a research assistant after graduation. Worked on a range of research projects in the areas of privacy-preserving machine learning, web data science, and social and information network analysis.

- Conducted high-quality and impactful research: **published four papers** in top-tier venues, including [IEEE IoTJ](#), [ACM TKDD](#), and [TheWebConf](#), **with over 350 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 **research assistantship** from [IBM-ILLINOIS Center for Cognitive Computing Systems Research](#) (declined due to visa issues).

TEACHING EXPERIENCE

Lecturer

International AI Doctoral Academy (AIDA), Online,

Nov 2022

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,

Fall 2017

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 Member

Privacy and Fairness in AI for Health Workshop (2023)

Program Committee Member

ACM Workshop on Wireless Security and Machine Learning (WiseML) (2023), ICLR PAIR2Struct Workshop (2022)

Scientific Peer Reviewer

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 (Expert), Java (Moderate), C++ (Moderate), Shell Scripting (Moderate), SQL (Moderate), LaTeX (Moderate)

Machine Learning & Data Analysis:

PyTorch, PyTorch-Geometric, Tensorflow, Tensorflow-Lite, Scikit-Learn, Pandas, Numpy, Jupyter, Matplotlib

MLOps & Related Technologies:

Weights & Biases, PyTorch-Lightning, Dask, Git, Linux, Docker

Privacy-Enhancing Technologies:

Flower (Federated Learning), Opacus (Differentially Private ML), Auto-DP (Privacy Accounting)

PUBLICATIONS

- [1] Sina Sajadmanesh and Daniel Gatica-Perez
[ProGAP: Progressive Graph Neural Networks with Differential Privacy Guarantees](#)
Technical Report, ArXiv e-prints, Apr 2023
- [2] 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 23), Aug 2023
- [3] Sina Sajadmanesh and Daniel Gatica-Perez
[Locally Private Graph Neural Networks](#)
ACM Conference on Computer and Communications Security (CCS 2021), Nov 2021
- [4] Sina Sajadmanesh and Daniel Gatica-Perez
[When Differential Privacy Meets Graph Neural Networks](#)
Technical Report, ArXiv e-prints, Jun 2020
- [5] 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, May 2020
- [6] 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, Aug 2019
- [7] Sina Sajadmanesh, Jiawei Zhang, and Hamid R. Rabiee
[NPGLM: A Non-Parametric Method for Temporal Link Prediction](#)
Technical Report, ArXiv e-prints, Jun 2017
- [8] Sina Sajadmanesh, Sina Jafarzadeh, Seyed Ali Ossia, *et al.*
[Kissing Cuisines: Exploring Worldwide Culinary Habits on the Web](#)
International World Wide Web Conference (WWW 2017) Companion, Apr 2017
- [9] Sina Sajadmanesh, Hamid R. Rabiee and Ali Khodadadi
[Predicting Anchor Links between Heterogeneous Social Networks](#)
IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Aug 2016