

# Arezoo Rajabi

Senior Quantitative Analytic Specialist & Adjunct faculty at University of Washington

Email: [rajabia@uw.edu](mailto:rajabia@uw.edu)

Linkedin: [www.linkedin.com/in/arezoo-rajabi](https://www.linkedin.com/in/arezoo-rajabi)

Homepage: <http://rajabia.github.io>

Wells Fargo Bank

333 Market ST

San Francisco, CA

EDUCATION	<b>Ph.D. in Computer Science</b>	Sep. 2014 – June 2021
	<i>Oregon State University, Corvallis, Oregon, USA</i>	
	<i>Thesis: Two Sides of a Coin: Adversarial-Based Image Privacy and Defending Against Adversarial Perturbations for Robust CNNs</i>	
	<b>M.Sc. in Computer Engineering (Software Engineering)</b>	Sep. 2011 – Sep. 2013
	<i>Sharif University of Technology, Tehran, Iran</i>	
	<i>Thesis: Local Community Detection in Social Networks</i>	
	<b>B.Sc. in Computer Science</b>	Sep. 2005 – Jan. 2011
	<i>Sharif University of Technology, Tehran, Iran</i>	
	<i>Thesis: Community Detection in Complex Networks</i>	
RESEARCH AREAS	Differential Privacy, Attacks and Defenses in Deep Learning, Trustworthy AI, Large Language Models	
WORK& RESEARCH EXPERIENCE	<b>Senior Quantitative Analytic Specialist,</b>	Dec. 2022 – Present
	<i>Wells Fargo Bank, CA, USA</i>	
	<ul style="list-style-type: none"><li><i>Machine Learning Model Development:</i> Developing and deploying machine learning models for privacy-sensitive and large datasets.</li><li><i>Performance Monitoring:</i> Designing comprehensive monitoring plans to assess the performance of deployed models.</li><li><i>Model Lifecycle Management:</i> Documenting the complete model lifecycle, including design solutions and key performance indicators (KPIs).</li></ul>	
	<b>Postdoctoral Scholar,</b>	March 2021 – Dec. 2022
	<i>NSL Lab, University of Washington, Seattle, WA, USA</i>	
	<ul style="list-style-type: none"><li><i>Privacy-Preserving RL Algorithm:</i> Developing a differential privacy method for RL algorithms with a risk-neutral decision-making approach and creating a defense mechanism against membership inference attacks for pre-trained deep neural networks.</li><li><i>Multi-Domain Trojan Detection:</i> Proposing a multi-domain Trojan sample detection system during the inference phase. Achieving a minimum success rate of 85</li><li><i>Federated Learning for Trojan Prevention:</i> Implementing a federated learning approach to counteract Trojan samples during the training phase.</li></ul>	
	<b>Graduate Research Assistant,</b>	Sep. 2014 – Sep. 2020
	<i>Oregon State University, Corvallis, Oregon, USA</i>	
	<ul style="list-style-type: none"><li>Developing image privacy methods based on adversarial learning methods against automated face detection methods</li><li>Developing two fault tolerance approaches for outliers in distributed smart grid power systems</li></ul>	

<b>SELECTED PUBLICATIONS</b>	1. <b>A. Rajabi</b> , S. Asokraj, F. Jiang, L. Niu, B. Ramasubramanian, J. Ritcey, R. Poovendran, MDTD: A Multi-Domain Trojan Detector for Deep Neural Networks, ACM Conference on Computer and Communications Security (ACM CCS), Sep. 2023.		
	2. J. Jia, Z. Yuan, D. Sahabandu, L. Niu, <b>A. Rajabi</b> , B. Ramasubramanian, B. Li, R. Poovendran, FLGAME: A Game-theoretic Defense against Backdoor Attacks In Federated Learning, Thirty-seventh Conference on Neural Information Processing Systems (NeurIPS), Sep 2023 ( <a href="https://neurips.cc/virtual/2023/poster/70499">https://neurips.cc/virtual/2023/poster/70499</a> ).		
	3. <b>A. Rajabi</b> , D. Sahabandu, L. Niu, B. Ramasubramanian, R. Poovendran, LDL: A Defense for Label-Based Membership Inference Attacks, ACM Asia Conference on Computer and Communications Security (AsiaCCS), July 2023 ( <b>7% acceptance rate</b> ).		
	4. <b>A. Rajabi</b> , B. Ramasubramanian, A. Marruf, R. Poovendran, Privacy Preserving Reinforcement Learning Beyond Expectation, Accepted in 61st IEEE Conference on Decision and Control, 2022.( <a href="https://arxiv.org/pdf/2203.10165.pdf">https://arxiv.org/pdf/2203.10165.pdf</a> ).		
	5. <b>A. Rajabi</b> , M. Abbasi, R. B. Bobba, K. Tajik, Adversarial Images Against Super-Resolution Convolutional Neural Networks for Free, Privacy Enhancing Technology Symposium (PETS), 2022.		
	6. <b>A. Rajabi</b> , R. B. Bobba, M. Rosulek, C. Wright, W. Feng, On the (Im)Practicality of Adversarial Perturbation for Image Privacy, Privacy Enhancing Technology Symposium (PETS), 2021.		
	7. M. Abbasi, <b>A. Rajabi</b> , C. Shui, C. Gagné, R. B. Bobba, Toward Adversarial Robustness by Diversity in an Ensemble of Specialized Deep Neural Networks, Canadian Conference on Artificial Intelligence (Canadian AI), 2020. (Best Paper Award)		
<b>PATENTS</b>	Arezoo Rajabi, Dinuka Sahabandu, Luyao Niu, Bhaskar Ramasubramanian, Radha Poovendran, <i>LDL: A Defense for Label-Based Membership Inference Attacks</i> , Record of Innovation filed with CoMotion At University of Washington, Seattle Dec. 2022.		
<b>PROFESSIONAL SERVICES</b>	Adjunct Faculty at University of Washington 2022- present Organizer at The Trojan Detection Challenge (LLM Edition), NeurIPS 2023 2023		
	Organizer at Trojan Detection Challenge, NeurIPS 2022 2022		
	Diversity co-chair at Security and Privacy Symposium 2023		
<b>PRESENTATIONS</b>	Paper Presentation at DSN workshop on Dependable and Secure Machine Learning Workshop for " <i>Adversarial Profile: Detecting Out-distribution Samples and Adversarial Examples for Pre-trained CNNs</i> " 2019		
	Paper and Poster Presentation at 2nd Annual Industrial Control System Security Workshop (ICSS) for " <i>A Resilient Algorithm for Power System Mode Estimation using Synchrophasors</i> " 2016		
	Poster Presentation at Graduate Research Showcase, School of Engineering, Oregon State University for " <i>Towards Dependable Deep Convolutional Neural Networks (CNNs) with Out-distribution Learning</i> " 2018		
<b>TEACHING EXPERIENCE</b>	<b>Teaching Assistant</b> Sep. 2014 – Sep. 2020		
	<i>Oregon State University, Corvallis, Oregon, USA</i> Courses: Network Security, Advanced System Security, Operating Systems (I), Analysis of Algorithms, Distributed Systems, Computer Applications		

**Teaching Assistant**  
*Sharif University of Technology, Tehran, Iran*  
Courses: Multi-media Networks, Complex Networks

Sep. 2011 – Sep. 2012

**AWARDS**

**First Place Winner** at Graduate Research Showcase for Poster Presentation 2018  
Cyber Resilient Energy Delivery Consortium (CREDC) Summer School Student  
Scholarship 2017  
Student Travel Awards from Top Security Conferences (S&P, CCS, GREPSEC, and  
ACSAC)

**SKILLS**

**Domain Specific Skill:** Image Classification, Reinforcement Learning, Large Language  
Models, Statistical Analysis and Testing, Clustering and Outlier Detection, Graph  
Convolutional Networks

**Programming Languages:** Python, Java, R, Matlab, C#

**Machine/Deep Learning Tools:** PyTorch, Opacus, Keras, Tensorflow, MatConvNet,  
Scikit-Learn, ggplot, SciPy, Robustness, Hugging Face

**Other Tools:** SQL, Hadoop, Amazon Web, H2O Services