Arezoo Rajabi

Ph.D. Candidate in Computer Science
Oregon State University

Email: rajabia@oregonstate.edu
LinkedIn: www.Linkedin.com/in/arezoo-rajabi
Homepage: http://rajabia.github.io/
Phone: (541) 283 - 6021

A dedicated and passionate ML/Cybersecurity researcher. Eager to work on new challenges. Proposed a practical adversarial perturbation scheme for image privacy in image sharing platforms. Introduced simple and efficient approaches for adversarial and out-distribution samples detection in Deep Neural Networks. Expertise in learning deep neural networks (DNNs, GANS, AEs, etc. by using PyTorch, Keras and Tensorflow on GPUs) and machine learning toolkits (Scikit-Learn, SciPy, LIME, etc.), experience on distributed and clustered data processing tools (Spark, Hadoop), convex optimization, and statistical data analysis methods.

Education

Oregon State University, Corvallis, Oregon, USA **Sep. 2014-March 2021**
Doctor of Philosophy in Computer Science (GPA:3.68/4)
Thesis: Two Sides of a Coin: Adversarial-Based Image Privacy and Defending Against Adversarial Perturbations for Robust CNNs

Sharif University of Technology, Tehran, Tehran, Iran **Sep. 2011-Sep. 2013**
Master of Science in Computer Engineering (GPA: 16.38/20)
Thesis: Local Community Detection in Complex Networks

Sharif University of Technology, Tehran, Tehran, Iran **Sep. 2005-Sep. 2010**
Bachelor of Science in Computer Science

Professional Experience

Oregon State University, Corvallis, Oregon, USA **Sep. 2015-Present**
Graduate Research Assistant
- Proposed a practical perturbation scheme for image privacy in image sharing platforms
- Improved augmented CNNs to detect out-distributions samples using a small set of proper out-distribution samples
- Improved standard and dynamic alternative direction method of multipliers mode estimation in power systems for tolerating false data injection attack

Digital Media Lab, Sharif University of Technology, Tehran, Iran **Sep. 2011-Sep. 2013**
Graduate Research Assistant
- Introduced a local community detection method to find the community of a given node without having knowledge of the network topology
- Collaborated with a Ph.D. student on his project of sampling from complex networks with high community structure with unknown topology
- Supervised an undergrad student on her project of social networks topology inference using diffusion information

Oregon State University, Corvallis, Oregon, USA **Sep. 2014-Present**
Graduate Teaching Assistant
- Teaching assistant for several undergrad and grad courses including Network Security, Advanced System Security, Operating Systems(I), Distributed Systems

Sharif University of Technology, Tehran, Iran **Sep. 2012-Sep. 2013**
Graduate Teaching Assistant
- Teaching assistant for Multi-Media Networks and Complex Networks courses

Soft Skills:
- Critical Thinking
- Problem Solving
- Teamwork
- Communication

Hard Skills:
- Deep learning
- Machine learning
- Image privacy
- Data science
- Graph theory and complex networks
- Cybersecurity
- Convex optimization

Programming Languages:
- Python, Java, R, MATLAB, C#, C++

Machine & Deep Learning Toolkits:
- PyTorch, TensorFlow, Keras
- Scikit-Learn, SciPy, Panda, Ggplot, Matplot, LIME
- Hadoop, Spark, AWS
- RapidMiner, Weka

Software and Tools:
- CVX, Lindo, MySQL, PST, OPNET, Git

Selected Coursework:
- Machine & Deep learning, Convex optimization, Probabilistic graphical model, Distributed systems

Publications & Manuscripts

- **A. Rajab**i, R. Bobba, M. Rosulek, C. Wright, W. Feng, “On the (Im)Practicality of Adversarial Perturbation for Image Privacy", Accepted in Privacy Enhancing Technology Symposium (PETS), 2021.
- M. Abbasi, **A. Rajabi**, C. Gagné, R. Bobba, "Toward Adversarial Robustness by Diversity in an Ensemble of Specialized Deep Neural Networks", Long paper in Canadian Conference on Artificial intelligence, 2020 (Best Paper Award).
- M. Abbasi, C. Shui, **A. Rajabi**, C. Gagné, R. Bobba, "Towards Metrics for Differentiating Out-of-Distribution Sets", European Conference on Artificial Intelligent (ECAI), 2020.
- **A. Rajabi**, R. Bobba, "False Data Detection in Distributed Oscillation Mode Estimation using Hierarchical K-means", IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, 2019.
- **A. Rajabi**, R. Bobba, "Adversarial Profile: Detecting Out-distribution Samples and Adversarial Examples for Pre-trained CNNs", DSN Workshop on Dependable and Secure Machine Learning (DSML), 2019.
- M. Abbasi, **A. Rajabi**, C. Gagné, R. Bobba, "Towards Dependable Deep Convolutional Neural Networks (CNNs) with Out-distribution Learning", DSN Workshop on Dependable and Secure Machine Learning (DSML), 2018.
- M. Abbasi, **A. Rajab**i, A.S. Mozafari, R.B. Bobba, C. Gagné, " Controlling Over-generalization and its Effect on Adversarial Examples Generation and Detection", Arxiv Preprint, 2018.
- **A. Rajabi,** R. Bobba, "A Resilient Algorithm for Power System Mode Estimation using Synchrophasors", Proceedings of the 2nd Annual Industrial Control System Security Workshop (ICSS), ACM, 2016.
- M. Salehi, H. R. Rabiee and **A. Rajabi**, "Sampling from Complex Networks with High Community Structures", Chaos: An Interdisciplinary Journal of Nonlinear Science", 2012.

Selected Projects

- **Data Anonymization and Synthesis Project** *(Submitted by Desjardin and Bank of Canada in Tenth Montreal Industrial Problem Solving Workshop (IPSW), Montreal, Canada*
  - Reviewed the literature on data anonymization and synthesis using GANs, adversarial learning and AEs
- **Image Privacy using Adversarial Perturbation**
  - Investigated the practicality of traditional adversarial learning approaches for image privacy and proposed two practical adversarial perturbation schemes for image privacy

Selected Presentations

- **Paper Presentation at Dependable Machine Learning Workshop,** “Adversarial Profile: Detecting Out-distribution Samples and Adversarial Examples for Pre-trained CNNs”
- **Paper Presentation at 2nd Annual Industrial Control System Security Workshop (ICSS)**, “A Resilient Algorithm for Power System Mode Estimation using Synchrophasors “
- **Poster Presentation at Graduate Research Showcase**, **School of Engineering, Oregon State University**, “Towards Dependable Deep Convolutional Neural Networks (CNNs) with Out-distribution Learning”

Awards

- **First Place at Graduate Research Showcase**, School of Engineering, Oregon State University, 2018
- **Summer School Student Scholarship** from Cyber Resilient Energy Delivery Consortium, 2017
- **Student Travel Awards** from Top Security Conferences (S&P, ACM, ACSAC, GREPSEC)

Selected Certificates

- **Spark Fundamentals II**, Cognitive Class, (An IBM Initiative)
- **Data Science Foundation- Level 2**, Cognitive Class, (An IBM Initiative)
- **Summer School Participation**, Cyber Resilient Energy Delivery Construction (CREDC)