Parham Gohari

PHD GRADUATE STUDENT

Profile

Experienced researcher with background in data privacy in the cyber domain. Adept in analyzing algorithms that process sensitive information to identify privacy vulnerabilities. Seeking to use my research experience in an internship position to gain hands-on experience with real-world systems.

Education

Ph.D., University of Texas at Austin, Austin, TX

2018 — PRESENT

Cockrell School of Engineering - Decision, Information, and Communications Engineering Track.

- Current GPA: 3.91

B. S., Sharif University of Technology, Tehran, Iran

2013 — 2018

Electrical Engineering Department - Controls and Systems Track - Minor in Economics.

- GPA: 3.88
- Recipient of Iran's National Elites Foundation Award

Work Experience

Graduate Research Assistant, Prof. Ufuk Topcu's Autonomous Systems Group, Austin, TX

AUGUST 2018 — PRESENT

- Researched enhancing automated decision-making systems' privacy.
- Published 2 conference papers, 1 journal paper, and 3 preprints on arXiv.
- Cited by 14 subsequent research papers.

Vounteer Mentor, Oden Institute for Computational Engineering & Sciences, Austin, TX

JUNE 2021 — SEPTEMBER 2021

- Mentored a summer intern for 4 months.
- Trained the intern on designing membership attacks on neural networks.
- Held daily meetings to track progress.
- Submitted a conference paper to ICLR 2022 at the end of the internship.

Ongoing Projects

Consensual Advertising

JUNE 2021 — PRESENT

- Designed a privacy-preserving advertisement scheme for web users with extreme privacy preferences, e.g., regular users of Tor browsers.
- The algorithm both delivers ads and performs user analyses, while enforcing differential privacy.

Kickstarting Deep Reinforcement Learning under Privacy Constraints

JANUARY 2021 — PRESENT

- Designed a privacy-preserving algorithm for reinforcement learning agents to share hints with one another.
- Designed an algorithm enabling the agents to benefit from the shared hints.
- Empirically showed that the resulting scheme speeds up the training process.

Details

Austin, TX
pgohari@utexas.edu

Links

parhamgohari.com

LinkedIn

Google Scholar

Soft Skills

Research

Communication and Presentation

Problem Solving

Teamwork

Programming Skills

Python

Stable Baselines

OpenAI Gym

Mosek

Gurobi

Hobbies

Piano, CrossFit, Travel

Past Projects

Membership Inference Attacks on Recurrent Neural Networks

2021

- Studied the privacy implications of deploying recurrent neural networks.
- Implemented a successful membership attack against recurrent networks.
- Provided empirical evidence that recurrent neural networks are more vulnerable to membership attacks than their feed-forward counterparts.
- Proposed a defense mechanism and empirically showed its success.

Privacy-Preserving Policy Synthesis in Markov Decision Processes

2020

- Designed a privacy-preserving decision-making algorithm for systems whose model holds confidential information about the environment dynamics.
- Theoretically studied the algorithm's trade-off between privacy and utility.
- Empirically validated the theoretical developments.
- Paper published in IEEE Conference of Decision and Control.

Differential Privacy on the Unit Simplex via the Dirichlet Mechanism

2019

- Theoretical contribution to differential privacy.
- Mathematically proved that perturbing probability values using the Dirichlet distribution satisfies differential privacy.
- Paper published in Transactions of Information Forensics and Security.
- Subsequent studies used the paper to design decentralized trading systems, power systems, etc.

Activities

Invited Speaker at University of Florida, 2021

- Presented my work 'Consensual Advertising' to Prof. Matthew Hale's group.

Invited Speaker at UC Berkeley, 2020

2020

- Presented my work 'Privacy-Preserving Policy Synthesis' at the Semi-Autonomous Seminar hosted by Prof. Shankar Sastry.

Courses

Cybersecurity Law/Policy, Law Department

Statistical Machine Learning, ECE Department

Large Scale Optimization, ECE Department

Reinforcement Learning, CS Department

Online Learning, ECE Department

Optimization Under Uncertainty, ORI Department

References

References available upon request