Masoud Poorghaffar Aghdam

Lojman 33. No. 1 Bilkent University, Ankara, Turkey Masoud.live
m.poorghaffar@bilkent.edu.tr linkedin.com/in/MasoudAghdam github.com/MPCL5

Education

Bilkent University September 2023 - July 2025 (Expected)
M.Sc. of Computer Engineering (GPA: 3.75 / 4.00) *Ankara, Turkey*

- **Relevant Coursework:** Deep Learning, Machine Learning, Bioinformatics
- **Advisor:** Dr. Ercument Cicek

University of Tabriz September 2018 - July 2022
B.Sc. of Computer Engineering (GPA: 3.33 / 4.00) *Tabriz, Iran*

- **Relevant Coursework:** Data Structures and Algorithms (C++), Data Mining, Fundamentals & Applications of Artificial Intelligence
- **Advisor:** Dr. Jafar Tanha

National Organization for Development of Exceptional Talents (Sampad) July 2018
Post Graduate Diploma (PGD) in Mathematics & Physics (GPA: 3.77 / 4.00) *Bonab, Iran*

Publications

Generated Data with Fake Privacy: Hidden Dangers of Fine-tuning Large Language Models on Generated Data
Akkus A, Poorghaffar Aghdam M, *Li M*, *Chu J*, *Backes M*, *Zhang Y*, *Sav S.*
arXiv · https://doi.org/10.48550/arXiv.2409.11423
Fine-tuning large language models (LLMs) with generated data is often considered a privacy-preserving alternative to real data, but our study reveals significant privacy risks. We evaluate Personal Information Identifier (PII) leakage and Membership Inference Attacks (MIAs) on the Pythia Model Suite and Open Pre-trained Transformer (OPT), finding that fine-tuning with generated data can increase privacy vulnerabilities. Notably, PII extractions for Pythia rose by over 20% and MIAs' ROC-AUC score for Pythia-6.9B increased by more than 40%, emphasizing the need for stronger privacy safeguards in LLM fine-tuning.

A Reinforcement Learning-based Approach for Dynamic Privacy Protection in Genomic Data Sharing Beacons
Poorghaffar Aghdam M, *Shukueian Tabrizi S*, *Ayoz K*, *Ayday E*, *Sav S*, *Cicek AE.*
bioRxiv · https://doi.org/10.1101/2024.10.28.620587
A reinforcement learning-based approach to enhance privacy in the Beacon Project, protecting genomic data from membership inference attacks. Designed a dynamic defense mechanism that adapts in real-time to evolving threats, distinguishing between legitimate users and attackers.

Research Projects

Main Contributor - Deep Clustering Variational Mixtures of ODEs for Inferring Cellular Gene Expression Dynamics

- Introduced a new model capable of clustering cells among different cohorts based on their RNA velocity by adapting Variational Deep Embedding (VaDE) in VeloVAE model.
- Stabilized training process.

Main Contributor - Enhancing details of images generated from VAE based clustering methods using Diffusional Models

- Used Variational Deep Embedding model for clustering.
- Utilized a Diffusional Model to capture and add random details to the generated images.

Teaching Experience

Bilkent University
*Teaching Assistant - **CS201** Algorithms and Programming I* *Fall 2024*
*Teaching Assistant - **CS201** Fundamental Structures of Computer Science I* *Fall 2023, Spring 2024*
*Teaching Assistant - **CS464** Introduction to Machine Learning* *Spring 2024*
*Teaching Assistant - **CS102** Algorithms and Programming II* *Fall 2023*

University of Tabriz
Teaching Assistant - Theory of Languages and Automata *Spring 2022*
Teaching Assistant - Algorithms *Spring 2021*
Teaching Assistant - Data Structures *Fall 2020*

Academic Service

Intelligent Systems for Molecular Biology (***ISMB***) Conference — *Reviewer, 2025*

Research in Computational Molecular Biology (***RECOMB***) Conference — *Reviewer, 2024*

Intelligent Systems for Molecular Biology (***ISMB***) Conference — *Reviewer, 2024*

Research in Computational Molecular Biology (***RECOMB***) Conference — *Reviewer, 2023*

Technical Skills

Languages: C++, C#, Java, Python, Java Script, R

Frameworks: PyTorch, TensorFlow, Theano (Familiar), ASP Dot net core, Nest JS, Next JS, React JS

Tools: Git, Docker, Linux (Mostly Debian base), Trello, Microsoft Azure, WSL

Concepts: Operating System, Caching, Machine Learning, Neural Networks, Database Normalization, Agile Methodology, Cloud Computing

Main Models: Convolutional Networks, Variational Auto Encoders, Generative Adversarial Networks, Diffusion Models, Transformers (No practical Experience)

Databases: MySQL, Microsoft SQL Server, Mongo DB, PostgreSQL

Work Experience

Raychat — May 2022 - March 2023

Software Engineer — *Tabriz, Iran*

Raychat is a customer service chat product. I was responsible for optimizing the performance of the back-end software, ensuring efficiency and scalability. In addition, was responsible for training and supervising the interns, providing them technical guidance.
Website: Raychat.io

Landin — July 2021 - November 2021

Front-End Developer — *Tehran, Iran*

Landin is a digital marketing solution that provides landing pages after clicking on ads. I worked on front-end development, implementing methods to enhance the loading time of their generated landing pages. In addition, I was responsible for developing a landing page editor.
Website: Landin.ir

Arkatech — April 2020 - July 2021

Full Stack Developer — *Tabriz, Iran*

ArkaTech was a start-up that helped other businesses establish their own e-commerce company. I was responsible for the development of the front-end software. I used various front-end development libraries including React Js and Next Js. I addition, I passed my internship in ArkaTech.

Social Engagements

Vice-President: Computer Engineering Association of Tabriz University

Volunteer: Radio Geek - A university radio talking about hot technology topics.