ALI ANSARI

Tehran, Iran

Education

Sharif University of Technology

Tehran, Iran

 $B.Sc.\ in\ Computer\ Engineering\ -\ Fully\ funded$

Oct. 2020 - present

• Overall GPA: 19.26/20 (3.985/4.0) - GPA in Major: 19.50/20 (3.97/4.0)

• Thesis: A data-driven approach for robust detection of out-of-distribution data (Advised by Prof. M.H. Rohban) - Grade: 20/20

Hasheminejad 1 High School

Mashhad, Iran

Diploma in Mathematics and Physics

Sept. 2017 - June 2020

Publications

RODEO: Robust Outlier Detection via Exposing Adaptive Out-of-Distribution Samples

ICML 2024

Hossein Mirzaei, Mohammad Jafari, Hamid Reza Dehbashi, <u>Ali Ansari</u>, Sepehr Ghobadi, Masoud Hadi, Arshia Soltani Moakhar, Mohammad Azizmalayeri, Mahdieh Soleymani Baghshah, Mohammad Hossein Rohban

Scanning Trojaned Models Using Out-of-Distribution Samples

NeurIPS 2024

Hossein Mirzaei, <u>Ali Ansari</u>*, Bahar Dibaei Nia*, Mojtaba Nafez, Moein Madadi, Sepehr Rezaee, Zeinab Sadat Taghavi, Arad Maleki, Kian Shamsaie, Mahdi Hajialilue, Jafar Habibi, Mohammad Sabokrou, Mohammad Hossein Rohban

A Contrastive Teacher-Student Framework for Novelty Detection under Style Shifts

Submitted to ICLR 2025

Hossein Mirzaei, Mojtaba Nafez, Moein Madadi, Arad Maleki, Mahdi Hajialilue, Zeinab Sadat Taghavi, Sepehr Rezaee, <u>Ali Ansari</u>, Bahar Dibaei Nia, Kian Shamsaie, Mohammadreza Salehi, Jafar Habibi, Mahdieh Soleymani Baghshah, Mohammad Sabokrou, Mohammad Hossein Rohban

Research Interests

- Trustworthy & Safe AI
- Generative AI

- Large Language Models
- Computer Vision
- Representation Learning
- Algorithms

Honors and Awards

 ${\bf Ranked}\ {\bf 1^{st}}$ as a team in a nation-wide competition on developing Persian LLM

2024

• Worked on the problem of efficient inference of Falcon model on CPU.

Bronze Medal in Regional ICPC Contest

2022

Ranked 3rd among more than 150,000 students, National University Entrance Exam of Iran (Konkur)

2020

Received silver medal among over 10000 students, Iran National Olympiad in Informatics

2019

Research Experiences

Sharif University of Technology

Aug 2022 – present

Research Assistant, supervised by Prof. M.H. Rohban

Tehran, Iran

• Research areas: Computer Vision, Trustworthy AI (Adversarial Robustness, Backdoor Attacks, Out-of-Distribution Detection)

Projects

- RODEO: Robust Outlier Detection via Exposing Adaptive Out-of-Distribution Samples (ICML 2024)
- TRODO: Scanning Trojaned Models Using Out-of-Distribution Samples (NeurIPS 2024)
- A Contrastive Teacher-Student Framework for Novelty Detection under Style Shifts (submitted to ICLR 2025)

Chinese University of Hong Kong

July 2024 - present

Research Assistant, co-supervised by Prof. Tsung-Yi. Ho and Dr. Pin-Yu

Hong Kong

- Chen
 - Conducted a literature review on transformers architecture and LLMs security
 - Develop a method to detect jailbreaks in LLMs both effectively and efficiently

Hong Kong University of Science And Technology

July 2023 - Sep 2023

Research Assistant, supervised by Prof. A. Goharshady

Hong Kong

- Designing parameterized algorithms that leverage tree-width and related parameters to identify the hierarchical structure of data locality in a sequence of memory accesses, with the aim of minimizing cache misses
- Became familiar with various topics in theoretical computer science including cryptography, program analysis and game theory

Teaching Experiences

Teaching Assistant

- Machine Learning Sharif University of Technology Spring 2024
- Computer Networks Sharif University of Technology Spring 2024
- Probability and Statistics Sharif University of Technology Spring 2022
- Design & Analysis of Algorithms Sharif University of Technology (Fall 2022, Spring 2023, Fall 2023)
- Data Structures and Algorithms Sharif University of Technology (Spring 2022)
- Theory of Languages and Automata Sharif University of Technology (Spring 2023)

Instructor

• Algorithms and data structures to volunteers of Informatics Olympiad - 2021

Coursework

- Optimization for Machine Learning (Online, EPFL)
- Deep Learning for Computer Vision (Online, cs231n, Stanford University)
- Convex Optimization (Sharif University of Technology, 17.8 / 20)
- Fundamentals of 3D Computer Vision (Sharif University of Technology, 20/20)
- Machine Learning (Sharif University of Technology, 20/20)
- Design & Analysis of Algorithms (Sharif University of Technology, 20/20)
- Computer Networks (Sharif University of Technology, 20/20)
- Artificial Intelligence (Sharif University of Technology, 19.8/20)
- Linear Algebra (Sharif University of Technology, 20/20)

Technical Skills

Languages: Python, C++, C, HTML/CSS, Java, SQL, Go, R

Technologies: Git, Docker, Bash

Frameworks: PyTorch, TensorFlow, Wandb

Other Projects

TinyNeRF | Python, Pytorch | Github

Winter 2024

- A simplified version of NeRF, implemented using PyTorch
- There is also an implementation of it in NeRF repository using TensorFlow
- This was the final project of Fundamentals of 3D Computer Vision course

C-Minus Compiler | Python | Github

Fall 2023

- As a team, implemented a Complier for C-Minus (A simplified version of C)
- This was the final project of Compilers Design course

YuGiOh | Java | 👩 Github

January 2021, June 2021

- Implemented YuGiOh game in Java
- Used LibGDX as the main library for the game

Work Experiences

Software Engineer at Divar

Tehran, Iran

Aug. 2021 - May 2022

- Worked with Django to develop the performance evaluation system for employees of the organization
- Tools & Frameworks: Django | Python | Kubernetes | Docker | GitLab

Languages

English | Professional Proficiency

IELTS Overall Band score: 8.0

Persian | Native proficiency

Hobbies

Hiking, Electronic Music, Movies, Podcasts

References

Mohammad Hossein Rohban

- Associate Professor Sharif University of Technology
- rohban@sharif.edu

Pin-Yu Chen

- Principal Research Staff Member- IBM Research AI
- pin-yu.chen@ibm.com

Mahdieh Soleymani Baghshah

- Associate Professor Sharif University of Technology
- soleymani@sharif.edu

Mohammad Sabokrou

- Staff Research Scientist Okinawa Institute of Science and Technology
- mohammad.sabokrou@oist.jp

Amir Kafshdar Goharshady

- Assistant Professor Hong Kong University of Science and Technology
- $\bullet \ goharshady@cse.ust.hk\\$