

Arad Maleki Toolabi

aradmalekitoolabi@gmail.com | aradmaleki02.github.io | linkedin.com/in/aradmaleki | github.com/aradmaleki02

EDUCATION

Sharif University of Technology

- B.Sc. in Computer Engineering | Current GPA: 19.06/20

Sep 2020 – Present

Tehran, Iran

PUBLISHED PAPERS

Scanning Trojaned Models Using Out-of-Distribution Samples

Accepted at NeurIPS 2024

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

PAPERS SUBMITTED FOR PUBLICATION

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

Submitted to ICLR 2025

3rd Author, Authors anonymized due to double-blind review

A Survey on Multi-GPU systems

Submitted to ACM Computing Surveys

Atiyeh Gheibi, **Arad Maleki**, Amirsaeed Ahmadi, Masoud Mohammadi, Sahand Zoufan, Mahdi Alinejad, Mohammad Alizadeh, Komeil Yahyazadeh, Negar Akbarzadeh, Sina Darabi-Moghadam, Shaahin Hessabi, Hamid Sarbazi-Azad

PatchGuard: Adversarially Robust Anomaly Detection and Localization

Submitted to CVPR 2025

2nd Author, Authors anonymized due to double-blind review

PAPERS IN PROGRESS

Mitigating Hallucinations in LVLMs Open Text Generation

Planned for submission at TACL journal

Arad Maleki

Learning-Based Cache Bypassing in Multi-GPU Architectures

Planned for submission at MICRO 2025

Arad Maleki, Atiyeh Gheibi, Hamid Sarbazi-Azad

RESEARCH EXPERIENCE

My research interests lie at the intersection of enhancing **Efficiency** and **Trustworthiness** in ML systems.

Research Assistant

Mar 2024 – Present

Sharif University of Technology - Prof. Sarbazi-Azad's HPCAN lab

Tehran, Iran

- Participated in research regarding Multi-GPU systems, resulting in a comprehensive survey.

Research Assistant

Sep 2023 – Mar 2024

Sharif University of Technology - Prof. Rohban's Robust and Interpretable ML lab

Tehran, Iran

- Participated in multiple research projects, resulting in a publication and two preprints submitted to top venues.

Research Intern

Jun 2023 – Sep 2023

Ruhr University Bochum

Bochum, Germany

- Remote internship under Prof. Setareh Maghsudi researching robustness in Inverse RL systems.

Research Intern

Feb 2023 – Jun 2023

Sharif University of Technology - Prof. Heydarnoori's Intelligent Software Engineering lab

Tehran, Iran

- Worked on offline large-scale workload sharing across multiple GPUs.

TEACHING ASSISTANCE EXPERIENCE

Machine Learning: Fall 2024, Spring 2024, Fall 2023 | **Intro Bioinformatics:** Fall 2024 | **Mobile:** Spring 2024

Fundamentals of Programming: Spring 2022, Fall 2021 | **Advanced Programming:** Spring 2022, Fall 2021

WORKING EXPERIENCE

ML Engineering Intern | *Danesh Solutions*

Sep 2024 – Present

- Working on efficiently fine-tuning LLMs to assist Persian users seeking banking transactions, focusing on optimizing data pipelines and designing scalable model architectures tailored for production deployment.

VOLUNTARY EXPERIENCE

Educational Content Curator | *National AI Olympiad for high schoolers*

Nov 2024 – Present

- Designing educational material on multiple topics, including Probability & Statistics, Linear Algebra, and Deep Learning, for high schoolers participating in Iran's 1st National AI Olympiad.

Scientific Staff | *Rayan AI Contest – Organized by Prof. Rohban*

Jul 2024 – Nov 2024

- Collaborated on the design and implementation of Phase 2 of the challenge.

HONORS AND AWARDS

Iran's Nationwide Universities Exam | *Ranked 105th amongst more than 155,000 Students*

2020

Iran's National Mathematics Olympiad | *Certificate of Honorable Mention*

2019

Iran's National Informatics Olympiad | *Reached 3rd stage (Top 1%) in consecutive years*

2018 & 2019

SELECTED COURSEWORK

AI & Learning: Reinforcement Learning (Graduate, 18.2/20), Machine Learning (19.1/20), Artificial Intelligence (20/20), Linear Algebra (18.8/20), Intro to BioInformatics (20/20), Signals & Systems (18/20)

Algorithmic: Data Structures & Algorithms (20/20), Game Theory (20/20), Design of Algorithms (19.5/20), Theory of Machines & Languages (20/20), Discrete Structures (20/20)

Architecture: Computer Structure & Lang (19.1/20), Computer Architecture (18.4/20), Compiler (20/20)

SKILLS

Programming Languages: Java, Python, C/C++, C#, SQL, Golang, Unity

Languages: Persian (Native), English (Full Professional proficiency), Arabic (Elementary Proficiency)

NOTABLE PROJECTS

BioInformatics Project | *Python, R, BioConda, PCA*

- Completed multiple BioInformatics-related tasks such as Analyzing the impact of Social Behaviour in the context of Neurobiology
- Used several BioInformatics tools and concepts including BLAST, DGE, RNA-Seq, and Genome Alignment

Face Recognition | *Python, Numpy, Matplotlib*

- Developed a notebook which inputs the image of some human faces and is expected to tell which faces are novel when prompted with the face of the same humans but in a different state (smiling)
- Used Linear Algebra & ML concepts such as PCA, Image mean, Eigenvectors, etc.
- Improved my theoretical knowledge of Linear Algebra as this project required some problem analysis skills

Mini Kafka | *Python, Docker, Go, CI/CD, Docker Compose*

- Created a small queue architecture inspired by Kafka, with features like fault tolerance and scalability
- Used popular software engineering tools such as Docker, Docker Compose, GitHub Actions, etc.

YoGiOh! | *Java, LibGDX, Gradle, GSON*

- Implemented our version of the popular game Yu-Gi-Oh! with Java and the graphics library LibGDX
- Worked in a team of 3 to contribute over 20,000 lines of code
- Implemented OOP concepts and computer network concepts, resulting in a multiplayer game with the option to play on a connected network

Micromaster | *Android Studio, Java, Gradle, JUnit, Room database, GSON*

- Implemented a mobile app to help users take university courses, submit homework, and download course material
- Implemented three entities: Lecturer, Student, and Teaching Assistant. Each entity has its own accesses and restrictions, and users interact with each other accordingly (Student submits homework, TA corrects it, etc.)