Masih Eskandar

masih.eskandar@gmail.com | meskandars.github.io

 /in/meskandars | Github | Google Scholar

SUMMARY

I am a Ph.D. candidate in Electrical Engineering at Northeastern University, specializing in Continual Learning and the application of machine learning to medical imaging and genomics, with additional expertise in Adversarial Robustness. I am passionate about advancing research in Large Language Models (LLMs), Transformers, and State Space Models (SSMs), with hands-on experience developing LLM-based dialogue agents and activation engineering techniques.

EDUCATION

- **Northeastern University** │ Advisor: Prof. Jennifer Dy   *09/2022 - 09/2026 (In Progress)*
  Ph.D. in Electrical Engineering   Boston, MA
  ◦ **Courses**: Big Data Sparsity and Control - Advanced Computer Vision - Advanced Deep Learning - Verifiable Machine Learning - Advanced Machine Learning - Statistical Inference - Linear Systems Analysis
  ◦ GPA: 3.86/4.00

- **Sharif University of Tech.** │ Advisor: Prof. M.H. Rohban   *09/2018 - 06/2022*
  B.Sc. in Computer Engineering   Tehran, Iran
  ◦ **Courses:** Linear Algebra - Probability and Statistics - Advanced Information Retrieval - Natural Language Processing (NLP) - Signal Processing
  ◦ GPA: 3.96/4.00

EXPERIENCE

- **Northeastern Univerisity** │ Machine Learning Lab @ SPIRAL   *09/2022 - Curr.*
  Research Assistant   Boston, MA
  ◦ Created a novel regularization-based approach to mitigating forgetting using weight perturbations (STAR, ICLR 2025) Currently developing continual learning algorithms with theoretical guarantees on forgetting/generalization
  ◦ Working on developing Transformer-based models for tissue-specific and patient-specific splice site predictions of RNA-seq data
  ◦ Investigated the adversarial robustness of parameter-efficient prompt-tuning and proposed a novel solution by using adaptive attacks (ADAPT, TMLR 2025)
  ◦ Implemented deep learning methodologies for dermatology, including image generation using stable diffusion, multi-modal LLMs, and feature matching

- **Technical University of Munich** │ CAMP   *06/2021 - 11/2021*
  Research Intern   Munich, Germany
  ◦ Developed a novel method for explaining model predictions for individual samples or classes using various input augmentations in conjunction with information bottleneck methods

- **Sharif University of Tech.** │ Robust/Interpretable ML lab   *06/2020 - 06/2021*
  Research Intern   Tehran, Iran
  ◦ Proposed an efficient signle-step adversarial attack generation method for performing adversarial training while avoiding overfitting (ZeroGrad, ISWA 2023)

PUBLICATIONS

- STAR: Stability-Inducing Weight Perturbation for Continual Learning   **ICLR 2025**
  M. Eskandar, T. Imtiaz, D. Hill, Z. Wang, J. Dy

- ADAPT to Robustify Prompt Tuning Vision Transformers   **TMLR 2025**
  M. Eskandar, T. Imtiaz, Z. Wang, J. Dy

- ZeroGrad: Costless conscious remedies for catastrophic overfitting in the FGSM adversarial training   **ISWA 2023**
  Z. Golgooni, M. Saberi*, **M. Eskandar***, M.H. Rohban

SKILLS

- **Programming Languages:** Python, C++/C, R, Java, Golang, Verilog, SQL, Assembly (MIPS)
- **Data Science & Machine Learning:** PyTorch, Tensorflow, JAX, Numpy, Pandas

ADDITIONAL WORK EXPERIENCE

• **Setak (Messaging App)** *02/2022 - 06/2022*
Backend Software Developer Intern Tehran, Iran
  ◦ Database Management - API Development
  ◦ Relevant experiences: SQL, Spring, Kafka, Docker

HONORS AND AWARDS

• **Undergraduate Excellence Award** *2021*
Technical University of Munich
• **2nd place @ Webelopers Website Development Competition** *2019*
Sharif University of Tech.
• **Rank 30th Nationwide** *2018*
University Entrance Exam ∼ Among 150K Participants