Sepehr Rezaee

sepehrrezaee2002@gmail.com | github.com/SepehrRezaee | My Scholar | My LinkedIn Account

SepehrRezaee.com

Education

Shahid Beheshti University, BS in Computer Sciences *2021 – 2025*

- **GPA:** 3.2/4.0
- **Interests:** Deep Learning, Computer Vision, Generative AI, AI Safety, And AI Agents

Allameh Tabatabaei (Advanced) High School, Math Diploma *2019 – 2021*

- **GPA:** 3.87/4.0

Experience

Research Intern, Mackenzie W. Mathis Lab – EPFL, Lausanne *2025 – Present*

- *Co-authored an accepted paper at ICCV 2025, introducing DISTIL, a data-free, diffusion-driven framework for trigger inversion in Trojaned neural networks, which set new benchmarks on BackdoorBench (+7.1% accuracy) and object detection scanning (+9.4%).*
- *Developed novel generative modeling pipelines for safe and interpretable AI, leveraging latent diffusion guided by classifier feedback to reveal adversarial vulnerabilities.*
- *Collaborated with a multidisciplinary team to pioneer zero-shot, data-free defenses for backdoor attacks, advancing reliable machine learning for mission-critical applications.*
- *Contributed to empirical evaluation and benchmarking of generative defense strategies, helping to establish best practices for future research in trustworthy AI.*

AI Engineer, Agentic Systems PropTy Global *Aug 2024 – Present*

Remote

- *Architected and deployed production-ready, multi-agent LLM systems using LangChain and custom RAG pipelines, powering autonomous recommendation and business decision workflows with an 85%+ task completion rate.*
- *Designed and implemented robust agent-to-agent communication protocols and memory modules to enable context-aware, goal-driven reasoning in dynamic environments.*
- *Engineered a scalable backend leveraging FastAPI, PostgreSQL (3TB+), and MongoDB, optimizing queries and indexing for sub-100ms API response times in real-time recommendation scenarios.*
- *Integrated fine-tuned LLMs into customer-facing platforms, reducing user onboarding time by 15% and significantly improving the contextual relevance and personalization of chatbot interactions.*
- *Deployed containerized solutions via Docker and Kubernetes, accelerating deployment cycles by 40% and efficiently managing high-concurrency user traffic.*
- *Established advanced monitoring, observability, and feedback loops with Prometheus, Grafana, and the ELK stack, connecting agent actions to live business KPIs and enabling continuous agent evaluation and optimization.*
- *Collaborated on designing and iterating agent improvement pipelines, driving measurable gains in system performance and user engagement.*
- *Implemented AWS SageMaker pipelines for efficient model training and inference, reducing operational costs by 20% through the use of spot instances and automated scaling.*

Research Assistant, Robust and Interpretable Machine Learning Lab – Sharif University of Technology, Tehran *2024 – 2025*

- *Authored and co-authored 3 papers submitted to NeurIPS 2024, focusing on enhancing model reliability and security in machine learning.*
- *Developed and implemented 3 robust machine learning pipelines, increasing model reliability under adversarial conditions.*
- *Collaborated with a multidisciplinary team of 10 members to integrate machine learning solutions into real-world applications (Autonomous Driving, Face Detection, Diagnosing Disease), improving operational efficiency.*
- *Presented research findings at 2 international conferences, elevating the lab's visibility and fostering academic collaborations.*

Research Assistant, Artificial Intelligence and Scientific Computing Lab – Shahid Beheshti University, Tehran *2023 – 2025*

- *Co-authored 2 under-review & 1 published research papers, including:*
  - *Physics-Informed Lane-Emden Solvers Using Lynx-Net: Implementing Radial Basis Functions in Kolmogorov Representation*
  - *Leveraging Physics-Informed Convolutional Neural Networks (PICNNs) to Solve Linear and Non-linear Fokker-Planck Equations (FPEs)*
  - *Comparison of Pre-training and Classification Models for Early Detection of Alzheimer's Disease Using Magnetic Resonance Imaging*
- *Modeled disease progression using differential equations, enhancing the understanding of biological mechanisms.*
- *Employed Physics-Informed Neural Networks (PINNs), increasing model accuracy through the integration of physical laws.*

Deep Learning and Neuroscience Intern Researcher, Institute for Research in Fundamental Sciences (IPM) – Tehran *2023 – 2024*

- *Conducted comprehensive M/EEG data analysis utilizing advanced deep learning techniques to decode neural signals.*
- *Developed and optimized neural network architectures for improved signal processing and feature extraction.*
- *Collaborated with neuroscientists to interpret data results and contribute to the understanding of brain functionalities.*
- *Assisted in the preparation of research manuscripts and presentations for academic dissemination.*

Publications

- ***DISTIL: Data-Free Inversion of Suspicious Trojan Inputs via Latent Diffusion*** 2025
  (Accepted to ICCV)

  Authors: Hossein Mirzaei, Zeinab Sadat Taghavi, ***Sepehr Rezaee****, Masoud Hadi, Moein Madadi, Mackenzie W Mathis*

- ***Scanning Trojaned Models Using Out-of-Distribution Samples*** (Accepted to NeurIPS) 2024

  Authors: Hossein Mirzaei, Ali Ansari, 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*

- ***Comparison of Pre-Training and Classification Models for Early Detection of Alzheimer's Disease Using Magnetic Resonance Imaging*** (Accepted in I4C 2023) 2023

  Authors: AH Karami, ***S Rezaee****, E Mirzabeigi, K Parand*

- ***Hierarchical Clustering Algorithms, Chapter of Unsupervised Algorithms: Clustering (with Implementation)*** Aarvan Publications 2022

  Authors: Kourosh Parand, ***Sepehr Rezaee****, et al.*

- ***Physics-Informed Lane-Emden Solvers Using Lynx-Net: Implementing Radial Basis Functions in Kolmogorov Representation*** (Under review) 2025

  Authors: Elmira Mirzabeigi, Maryam Babaei, Amir Hossein Karami*,* ***Sepehr Rezaee****, Rezvan Salehi, Kourosh Parand*

Selected Projects

AI Model Security: Enhancing Robustness Against Backdoors and Trojans *2024*

- Developed methods to detect and mitigate backdoors in machine learning models, enhancing AI deployment security.
- Engineered algorithms using statistical analysis and pattern recognition, improving trojan detection rates.
- Contributed to NeurIPS 2024 publications, advancing the field of AI model security.
- **Tools Used:** Python, PyTorch, Scikit-learn, LaTeX

AI-Based Application for Early Detection of Alzheimer's Disease *2023 – 2024*

- Designed and implemented a customized multi-modal model integrating biomedical and MRI datasets.
- Enhanced diagnostic accuracy through advanced machine learning techniques with Vision Language Models (VLMs).
- **Tools Used:** PyTorch, Hugging Face, OpenCV

Physics-Informed Neural Networks for Disease Progression Modeling *2023*

- Created a Physics-Informed Neural Network integrating differential equations to predict disease progression accurately.
- Utilized clinical datasets and validated models with patient data, achieving higher accuracy than traditional methods.
- Published findings in peer-reviewed journals, contributing to AI-based healthcare innovations.
- **Tools Used:** PyTorch, NumPy, SciPy, Pandas

AI-Driven M/EEG Data Analysis for Neuroscience Research *2018*

- Applied deep learning techniques to decode M/EEG signals, uncovering neural mechanisms.
- Streamlined data workflows by automating preprocessing and artifact removal, enhancing analysis efficiency.
- Facilitated insights into brain connectivity, supporting high-impact neuroscience research publications.
- **Tools Used:** MNE-Python, PyTorch, NumPy, Pandas

Awards & Honors

Winner of the Best Ideator Award (The 7th National Young Scientists Festival) 2023
For designing an AI-based assistant for the early detection of Alzheimer's disease.

Placed 352nd out of approximately 150,000 students in the national entrance exam 2020

Teaching Assistant

Advanced Programming Head Teaching Assistant, Shahid Beheshti University, Tehran 2024 – Present

Data Mining and Analysis Head Teaching Assistant, Shahid Beheshti University, Tehran 2023

Basic Programming Teaching Assistant, Shahid Beheshti University, Tehran 2022

Assistant Teacher and Mentor 2022 – 2023

- Applications of Data Science and Artificial Intelligence in the Petrochemical Industry, the Water Industry & the Electricity Industry

Selected Courses

Courses: Foundations of Data Science (A^+, 1st), Data Mining (A^+, 1st), Advanced Data Mining (A^+, 1st), Foundation of Numerical Analysis (A^+, 1st), Non-Linear Optimization (A^+, 1st), Partial Differential Equations (A^+, 1st), Electromagnetics (A^+, 1st), Neural Network (A^+, 3rd), Foundation of Logic and Set Theory (A^+, 3rd), Principles of Operating Systems (A^+, 2nd), Foundations of Machine Learning (A^+, 2nd), Elements of Probability (A, 4th), Data Structures & Algorithms (A, 5th)

Skills

Programming Languages: Python, C++, C, MATLAB, C# & Java

Python Frameworks & Libraries: PyTorch, TensorFlow, OpenCV, MNE-Python, NumPy, SciPy, Matplotlib, Scikit-Learn, NiPype, FastAPI, Django, Django REST Framework, Selenium

Other Tools and Technologies: JAX, PostgreSQL, NoSQL, MongoDB, Kotlin, , Git, Docker, Linux, Bootstrap

Interpersonal Skills: Problem Solving, Team Working

Languages: Fluent in Persian (speaking, reading, and writing), English (Professional working proficiency)

Reference Contacts

Prof. Mohammad Hossein Rohban - rohban@sharif.edu
Prof. Mathis Mackenzie mackenzie.mathis@epfl.ch
Prof. Mohammad Sabokrou - mohammad.sabokrou@oist.jp
Prof. Kourosh Parand - k_parand@sbu.ac.ir