HAMIDREZA TAJALLI

◇ Contact: hamidreza.tajalli@ru.nl, behrad.tajali@gmail.com
◇ LinkedIn: https://www.linkedin.com/in/behrad-tajalli/

EDUCATION

Radboud University *Nov. 2021 – Nov. 2025*
Ph.D. in Computer Science (Specialized in Robust Machine Learning)

Sharif University of Technology *Oct. 2017 – Jan. 2020*
M.Sc. in Computer Science (Safety and Security of AI)

K. N. Toosi University of Technology *Oct. 2012 – Oct. 2016*
B.Sc. in Computer Science

WORKING EXPERIENCE AND PROJECTS

AISY Lab (Nijmegen) November 2021 - Present
ML Researcher

- Developed and deployed collaborative learning frameworks (Federated Learning and Split Learning), with a focus on evaluating and improving their robustness against model poisoning attacks.

- Implemented Extreme Learning Machines (ELMs), U-Net architectures, and vision transformers for image-based tasks, enhancing resilience against data poisoning through targeted robustness techniques.

· - Designed and applied novel universal perturbation strategies to improve ML model performance on tabular datasets, achieving up to a 20% accuracy increase on Google AutoML and XGBoost.

· - Investigated vulnerabilities in large language models (LLMs) during multi-stage training pipelines and developing defensive techniques to mitigate risks from model manipulation attacks.

IntelliSEC (Karlsruhe) May 2021 - October 2021
ML developer

Developed deep learning models resilient to data inference attacks by integrating differential privacy mechanisms, enhancing model robustness without significant performance trade-offs.

DNS Lab (Tehran) November 2017 - November 2020
ML Researcher

Implemented innovative adversarial defense techniques by transferring adversarial ML methods from image classification to encrypted network traffic analysis. Demonstrated effectiveness by neutralizing WFP models of over 90%.

Amnafzar Co. (Tehran) March 2019 - March 2020
Java Developer

Member of SIEM group in developing PARHAM, An application for management & analyzing enterprise systems logs.

Shatel Co.(Tehran) Summer 2016

Internship

Member of SOC(Security Operation Center)Performing real-time status monitoring of network systems along with getting involved in multiple aspects of preventing, detecting and responding to internal and external threats.

TECHNICAL SKILLS

Programming Languages	Python, Java, C/C++, JavaScript, HTML, CSS
Frameworks & Libraries	Pytorch, Tensorflow, Keras, Scikit-learn, XGBoost, LightGBM, CatBoost, Pandas, Numpy
LLM Toolkits	Hugging Face, LangChain, RAG, NLTK, Faiss
MLOps	DVC, Docker, MLflow, FastAPI, Gradio
Cloud Services	Azure ML, VertexAI (GCP), SageMaker (AWS)
Databases	RDBMS, NoSQL
Language	English (Full working proficiency), Dutch (B1)
Licenses & certifications	IBM Generative AI Engineering with LLMs, Microsoft AI & ML Engineering