

Cristian Cosci

📍 Italy

LinkedIn 
GitHub 
Google Scholar 
cosci.cristian@gmail.com 

Work and Research Experience

Machine Learning Reply December 2024 – Present
Senior Machine Learning Engineer (October 2026 – Present) Turin, Italy
Machine Learning Engineer (December 2024 – October 2026)

- **Main Topics:** LLMs, Fine-Tuning, CPT, Computer Vision, Operations Research, Optimization Algorithms
- **Generative AI:** Adaptation of open-source LLMs to enterprise domains through Continual Pre-Training and Fine-Tuning (LoRA), covering data preprocessing and analysis, synthetic data generation and evaluation; technical guidance and definition of guidelines for effective LLM adaptation
- **Computer Vision:** Design and development of Computer Vision solutions for enterprise use cases
- **Logistics & Optimization:** Machine Learning and optimization algorithms for intermodal rail and road transport planning and for the scheduling of container terminal operations
- **Talks:** Speaker at several events on AI and AI applied to logistics

University of Bologna and University of Pisa November 2023 – November 2024
Researcher in Artificial Intelligence Bologna and Pisa, Italy
Research Topic: *Generative AI and Trustworthiness*

Internship September 2022 – January 2023
University of Perugia, Mathematics and Computer Science Department

- Analysis and Implementation of Adversarial Attacks on Image Classification models that exploit the knowledge provided by Explainability methods based on Activation Maps

Education

University of Perugia November 2021 – September 2023
Master's Degree in Computer Science: Artificial Intelligence Curriculum Perugia, Italy
Final Grade: *110/110 with Honors*
Thesis Title: *"Adversarial Attacks on Explainability Methods for Image Classification Models"*

University of Perugia October 2018 – November 2021
Bachelor's Degree in Computer Science Perugia, Italy
Final Grade: *110/110 with Honors*
Thesis Title: *"Bitcoin price-trend prediction using Machine Learning"*

Publications

Pirates of the RAG: Adaptively Attacking LLMs to Leak Knowledge Bases 2025

- C. Di Maio, C. Cosci, M. Maggini, V. Poggioni, S. Melacci
- *Proceedings of the 28th European Conference on Artificial Intelligence (ECAI 2025) – top-tier conference, CORE rank A*
- *Frontiers in Artificial Intelligence and Applications*, vol. 413, pp. 4041–4048, doi:10.3233/FAIA251293

Other Experience

Program Committee Member 2024

Second AEQUITAS Workshop on Fairness and Bias in AI | co-located with ECAI 2024

Participation in the "2nd European Summer School on Artificial Intelligence" July 2024

ESSAI & ACAI 2024, Athens, Greece

- Two weeks of lectures and seminars by researchers in the field of Artificial Intelligence
- Main topics covered: Deep Learning, Computer Vision and Natural Language Processing

Participation in the "AI & Society 2024 Summer School" June 2024

University of Pisa, Tropea, Italy

- One week of lectures and seminars by researchers in the field of Ethics and AI
- Won the "Best Project Award" in a competition among other Ph.D. students.

Teaching assistant February 2024 – June 2024

University of Perugia, Department of Mathematics and Computer Science

- Teaching assistant for the Master's Degree course: Machine Learning with Laboratory

Teaching assistant November 2022 – February 2023

University of Perugia, Department of Mathematics and Computer Science

- Teaching assistant for the Bachelor's Degree course: Procedural Programming with Laboratory

Participation in the 2022 Summer School: "School in AI" September 2022

University of Modena and Reggio Emilia, Department of Computer Engineering

- Two weeks of lectures and seminars by researchers in the field of Artificial Intelligence
- Main topics covered: Deep Learning, Computer Vision and Natural Language Processing

Participation in the 2020 CyberChallenge edition January 2020 – June 2020

University of Perugia, CINI National Cybersecurity Laboratory

- Course focused on technical, scientific and ethical introduction to issues related to cybersecurity
- Main topics covered: cryptography, malware analysis and web security.

Skills

Computer Skills

- **Programming Languages:** *Python, C, Java, MATLAB*
- **Frameworks & libraries for AI:** *PyTorch, TensorFlow, Keras, OpenCV, NumPy, SciPy, NetworkX, Pandas, Matplotlib, scikit-learn*
- **Generative AI & LLMs:** *Continual Pre-Training, Fine-Tuning (LoRA), RAG, Synthetic Data Generation*
- **Cloud Platforms:** *AWS, GCP, Azure*
- **Operating Systems:** *Advanced knowledge of Linux and Windows*
- **Other tools:** *Docker, L^AT_EX*

Languages

- **Italian:** Native
- **English:** C1