Dario Gosmar

+39 345 580 1853 | dario.gosmar@gmail.com | github.com/d4darius | dario-gosmar

EXPERTISE

Agentic AI & LLM Reliability. My research focuses on enhancing the trustworthiness of Large Language Models through agentic iterative workflows and structured knowledge retrieval. I develop frameworks that combine human-like reasoning patterns with rigorous verification to mitigate hallucinations and adversarial vulnerabilities.

EXPERIENCE

Politecnico di Torino 2024 – Present
Student Researcher, Computational Electromagnetism Research Lab (CERL) Torino, Italy

- Participating in the Early Research Honor School program.
- I investigated the application of Neural Networks to preconditioning problems in computational electromagnetism and verified correlations between object's geometry and the conditioning power of the Calderon-Yukawa operator.

Politecnico di Torino 2023 – 2024
Part-time LAIB Technician Torino, Italy

- Oversaw the correct usage of laboratory equipment and resources.
- Provided general technical assistance and performed routine maintenance on lab systems.

PUBLICATIONS

[1] Diego Gosmar, Deborah A. Dahl, **Dario Gosmar**. *Prompt Injection Detection and Mitigation via AI Multi-Agent NLP Frameworks*. arXiv pre-print, 2025.

- Developed a multi-agent NLP framework designed to mitigate prompt injection vulnerabilities, achieving a **45.7% reduction** in successful attacks.
- Formalized injection patterns to construct a comprehensive benchmarking dataset for evaluating detection systems.

PROJECTS

MCP Servers for Agentic Retrieval over Knowledge Graphs

- Engineered a Model Context Protocol (MCP) server to interface LLMs with RDF Knowledge Graphs via SPARQL, achieving **53% accuracy** on state-of-the-art models.
- Constructed a specialized dataset of competency questions based on the **DOREMUS ontology** to evaluate agentic knowledge retrieval capabilities.
- Benchmarked system performance across multiple agentic clients using a multi-metric evaluation framework to validate retrieval effectiveness.

GIN-Fusion: Graph Isomorphism Networks for 6D Pose Estimation

- Augmented the DenseFusion architecture by integrating Graph Isomorphism Network (GIN) layers to refine per-pixel feature extraction.
- Achieved a **10% increase in accuracy** over the baseline model by enhancing geometric feature representation.

Callimachus: Ambient Agent Learning Assistant

- Designed an ambient agent using LangChain to assist in note-taking by synthesizing multiple data sources.
- Implemented Human-In-The-Loop (HITL) and memory features, allowing users to iteratively improve assistant performance.

Energetic Modeling Platform

- Developed an interactive **Streamlit** dashboard to facilitate the techno-economic sizing of hybrid power plants.
- Enabled a multidisciplinary team to model and optimize off-grid energy scenarios for the islands of Ponza and Belep.

EDUCATION

Politecnico di Torino — Torino, Italy
M.S. Data Science for Engineering — 2024 – Present (Exp. 2026)

Institut EURECOM — Biot, France
Diplôme d'Ingénieur - Science des données — 2025 – Present (Exp. 2027)

Politecnico di Torino — Torino, Italy
B.S. Computer Engineering — 2021 – 2024
Grade: 110/110 cum laude (110L)

SKILLS

Languages: Python, C++, SQL
Frameworks & Libraries: PyTorch, NumPy, Pandas, LangChain
Spoken Languages: Italian (Native), English (C1), French (A2), German (A1)

Interests

Mountaineering (Hiking, Skiing), Video Editing (Adobe Premiere, DaVinci Resolve), Cooking.