Tiago Barbosa

Informatics and Computing Engineering
tiago.filipe.barbosa@gmail.com | August 5th 2002
Porto, Portugal

Linktree

Engineer with a strong academic background in artificial intelligence, applied machine learning and computer vision. Independently designed and developed a modular framework for adversarial robustness in deep learning, now under submission to IEEE Access. Familiar with modern AI techniques, including retrieval-augmented generation (RAG) and agentic workflows. Comfortable navigating end-to-end ML pipelines, including model deployment and emerging cloud tools. Known for autonomy, problem-solving and leading multidisciplinary teams in fast-paced academic and international environments. Passionate about building trustworthy, scalable AI systems with real-world impact.

Education

Faculty of Engineering of University of Porto — Porto, Portugal
Master's Degree in Informatics and Computing Engineering — *Sep 2023 - Jul 2025*

- Graduated with **18.1/20**
- **Key Areas**: Artificial Intelligence, Deep Learning, AI Security / Adversarial ML, MLOps, Software Development (Large Scale), Distributed Systems (Large Scale), Enterprise Management and Project Management

Vienna University of Technology (TU Wien) — Vienna, Austria
Erasmus+ Exchange Programme — *Sep 2024 - Feb 2025*

- **Key Areas**: Generative AI, Quantum Computing, Cryptocurrencies and Ubiquitous Computing (IoT)

Faculty of Engineering of University of Porto — Porto, Portugal
Bachelor's Degree in Informatics and Computing Engineering — *Sep 2020 - Jul 2023*

- Graduated with **18/20**
- **Key Areas**: Artificial Intelligence, Parallel and Distributed Computing, Web Technologies, Computer Networks, Computer Security, Programming, Algorithms and Data Structures, Databases, Operating Systems, Algorithm Design and Compilers

Other:

Denmark TU (BEST Summer Course) about Computer Vision — Copenhagen, Denmark — *Jul 2025*

Boğaziçi University (BEST Summer Course) about Brand Management — Istanbul, Turkey — *Jul 2024*

Projects

Safe-DL: A Modular Framework for Secure Deep Learning (Master's dissertation) — @FEUP
Feb 2025 - Jul 2025

- Conceived and developed an original framework for evaluating and mitigating adversarial threats in deep learning systems. The solution integrates threat modelling, attack simulation, risk scoring, automated defence selection and audit-ready reporting. Currently under submission to IEEE Access, the project bridges deep learning with AI security and regulatory compliance (e.g., AI Act), enabling robust and transparent AI deployments.
- Graded **19/20**
- **Skills:** Python, PyTorch, Deep Learning, Adversarial Machine Learning, Cybersecurity, Risk Analysis, Framework Design, Autonomy, Research and Critical Thinking

Notifications Micro Service (Bachelor's Capstone Project) — @Altice Labs and FEUP *Feb 2023 - Jun 2023*

- This project proposes a new microservice for network alerts. It goes beyond traditional methods by sending real-time notifications directly to Altice and users' preferred platforms (WhatsApp, Teams, etc.). This ensures faster response times and a more informed user experience, ultimately improving telecommunication service reliability.
- **Skills:** Java, Quarkus, Kubernetes, Leadership, Teamwork and Logical Thinking

Certifications

AWS Certified Cloud Practitioner (CLF-C02) – Amazon Web Services, 2025

- Cloud computing concepts (IaaS, PaaS, SaaS, Serverless)
- Core AWS services: EC2, S3, RDS, Lambda, VPC, CloudFront
- Security, compliance, and the Shared Responsibility Model
- AWS pricing models and cost optimization strategies

AWS Certified AI Practitioner (AIF-C01) – Amazon Web Services, 2025

- Fundamentals of Artificial Intelligence and Machine Learning
- AWS AI/ML services: SageMaker, Bedrock, Comprehend, Rekognition, Transcribe, Polly
- Generative AI concepts, prompt engineering, and model evaluation
- Responsible AI principles and ethical considerations

Skills

Programming Languages: Python, Java, C, C++, JavaScript, TypeScript

AI & ML Frameworks: PyTorch, TensorFlow, OpenCV, LangChain, LangGraph, LlamaIndex, Hugging Face Transformers, Ollama, scikit-learn, Keras, spaCy

Programming Paradigms & Concepts: Object-Oriented Programming (OOP), Functional Programming (FP), Concurrency, Parallelism, Multithreading, Multiprocessing

Cloud & DevOps Tools: AWS (SageMaker, Bedrock, Comprehend, Rekognition, Lambda, S3, EC2, IAM), Google Cloud Platform (Vertex AI, BigQuery, AI Platform, Cloud Functions), Microsoft Azure (Machine Learning, Cognitive Services, Functions, Blob Storage), Docker, Kubernetes, Git, GitHub Actions, CI/CD, Terraform, FastAPI

Databases & Search: SQL, NoSQL, Vector Databases

Key Topics & Interests: Artificial Intelligence, Deep Learning, Computer Vision, Generative AI, Large Language Models (LLM) Integration and Fine-Tuning, Retrieval-Augmented Generation (RAG), Agentic AI Systems, AI Security, Adversarial Machine Learning, Prompt Engineering, MLOps, MLflow, Model Deployment, API Integration, Data Engineering Pipelines

Soft skills: Autonomy, Problem-Solving, Critical Thinking, Teamwork, Leadership, Communication, Adaptability, Time Management, Project Management, Creativity, Cross-Cultural Collaboration

Languages: Portuguese – Native, English – Fluent (C1)