Pablo García Arce

PhD Student in Computer Science   ✉ *pablo.garcia@icmat.es*

Professional Objective

My professional goal is to apply the knowledge I am gaining during my PhD in Adversarial Machine Learning, with a focus on Bayesian perspectives, while also developing new skills and competencies. I am committed to continuous learning and I want to explore specialized areas such as AI robustness, neural network security and advanced adversarial techniques.

Academic Background

2015–2017 **High School**, *IES José Mª Pereda*, Spain
Final grade of honors.

2017–2022 **Double Degree in Physics and Mathematics**, *University of Cantabria*, Spain
16 honors and an average mark of 9.

2019 **Introduction to Global Studies**, *University of Cantabria*, Spain

2022 **Collaboration Grant**, *University of Cantabria, Dept. of Mathematics, Statistics and Computing*, Spain
Project: Logarithmic energy of the sphere of dimension 3, an analytical and numerical approach.

2022–2023 **Master in Statistical and Computational Data Processing**, *Complutense University of Madrid*, Spain
Project: Statistical techniques for early detection of ransomware threats.

2022–2024 **Master in AI Research**, *National University of Distance Education*, Spain
Project: Some methodological insights to build intelligent psychomotor systems for enhancing skill acquisition in free-throw shooting through personalized feedback in basketball.

Work Experience

2024–Ongoing **PhD in Computer Science**, *Institute of Mathematical Sciences (ICMAT)*, Spanish National Research Council
Project: Adversarial Machine Learning.

2022–2023 **Internship (8 months)**, *Institute of Physics Technologies (Spanish National Research Council)*, Spain
Project: Statistical techniques for early detection of ransomware threats.

2021–2022 **Internship (6 months)**, *Predictia Intelligent Data Solutions*, Spain
Project: Correction of rainfall prediction for the Iberian Peninsula using Machine Learning techniques and prediction by ingredients.

2021 **Internship (3 months)**, *LIS Data Solutions*, Spain
Performed tasks typical of a data scientist, including time series prediction, dashboard deployment, and computer vision.

Publications

2024   G. Arce, P. and Ríos Insua, D. (2024). *Adversarial Machine Learning.* Wiley StatsRef: Statistics Reference Online.

Conferences

2024   **International Workshop on Bayesian Statistics**, *Contributed Talk*, Bayesian perspectives of launching a software product

2024   **4th Spanish Young Statisticians and Operational Researchers Meeting**, *Contributed Talk*, A general framework for adversarial machine learning

2024   **ISBA World Meeting**, *Invited Talk*, Das, S., G. Arce, P. and Ríos Insua, D. (2024). Product launching through adversarial risk analysis

2024   **3rd INFORMS Security Conference**, *Contributed Talk*, Security of ML systems in the regression setting in the presence of adversaries

2024   **Mathematical Aspects of Learning Theory – 20 Years Later**, *Poster*, Robustness of ML systems against adversarial attacks from a Bayesian perspective

Further Education

2008–2017   **Professional degree in Music**, *Jesús de Monasterio Music School*, Spain
Guitar specialty, average mark of 8.1.

2019–2020   **Erasmus Scholarship**, *Queen's University of Belfast*, United Kingdom
Year abroad, average mark of 9.4.

2020   **Artificial Intelligence with Python**, *Udemy (Online Course)*

Skills

Languages   Fluent in English, both written and spoken.

Programming   Python (Pytorch, numpy, pandas, xarray, scipy, sklearn, tensorflow, keras), R, Matlab.

Hobbies

A sports fan, I have played basketball for the past few years. I also practice climbing and skiing. I enjoy music, photography, and nature.