Position Offered: UNIVERSITY GRADUATE

Project: *SECURIA. SECURe artificIAl intelligence*

Technological and scientific fields: Artificial Intelligence and Cybersecurity

Location: Madrid, Comunidad de Madrid, ICMAT, https://www.icmat.es

Research Group/PI: DataLab, IP: David Ríos Insua. https://datalab.icmat.es

PROJECT SUMMARY

Besides the benefits brought by artificial intelligence, a series of associated risks have been identified, focusing mainly on attacks against machine learning algorithms due to their potentially very negative impacts. Such threats are exacerbated by the massive adoption of these technologies, particularly since the rise of LLMs. From a regulatory and public policy perspective, the importance of this problem is well reflected in the EU AI Act. From a technical perspective, the growing importance of the field of adversarial machine learning is highlighted, primarily based on game theory methods under unrealistic common knowledge assumptions in the realm of security and cybersecurity.

Within the SECURIA project, this position will develop more rigorous methods and algorithms to strengthen machine learning algorithms against targeted attacks, which will converge into operational pipelines for their implementation in real-world AI-based systems. The methodology and software produced will be made available to the community to promote a more responsible and secure development of AI.

PROFESSIONAL PROFILE

Minimum requirements:

- Graduate or Bachelor's degree in Mathematics or Physics.
- Master in Statistics and Data Analysis.
- Knowledge of English and Spanish.

Merits to be considered:

- Proficiency in Python programming language.
- Training in Bayesian analysis and machine learning techniques.
- Proven experience with research contracts.

WHAT IS OFFERED

Cutting-edge training is offered in such current topics as Artificial Intelligence and Cybersecurity, as the central objective of SECURIA is to enable the development of a rigorous framework for risk management in AI that will converge into operational pipelines for their implementation in real-world AI-based systems, as well as strategic methodologies for developing responsible policies for scaling AI systems. From the second year onwards, the candidate will have research support responsibilities while continuing their training, with a total of 185 credits, which includes two stays at prestigious institutions such as George Washington University and the Air Force Institute of Technology, not to mention a whole plan for scientific dissemination and transfer, of which they will be a part along with the DataLab research group

Contract conditions:

Indefinite contract for a University Graduate associated with the Momentum Project of 4 years' duration according to Spanish science law. Gross annual salary (37.000 € - 41.000 €).

Start of contract: before 31 December 2024

PRINCIPAL INVESTIGATOR CONTACT

Email: marta.sanz@icmat.es

Phone: +34 91 29 99 743 / +34 607 40 77 00

momentum@csic.es | https://momentum.csic.es/

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
CSIC red.es
MOMENTUM CSIC
Plan de Recuperación, Transformación y Resiliencia
GENERACIÓN D