Posición Ofertada: PREDOCTORAL
Proyecto: *SECURIA. Inteligencia artificial segura*

Ámbitos tecnológicos o científicos: Inteligencia Artificial y Ciberseguridad

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

Grupo de Investigación / IP: DataLab, IP: David Ríos Insua. https://datalab.icmat.es

RESUMEN DEL PROYECTO

Además de los beneficios que trae la inteligencia artificial, se han identificado una serie de riesgos asociados de los que nos centraremos principalmente en los ataques a algoritmos de aprendizaje automático debido a sus potenciales impactos muy negativos. Tales amenazas se exacerban por la adopción masiva de estas tecnologías, desde el auge de los LLMs. Desde un punto de vista normativo y de política pública, la importancia del problema queda bien reflejado en la EU AI Act. Desde una perspectiva técnica, se destaca la creciente importancia del campo del aprendizaje automático adversario, basado principalmente en métodos de teoría de juegos bajo hipótesis de conocimiento común poco realistas en el ámbito de la seguridad y la ciberseguridad.

Dentro del proyecto SECURIA, en esta posición se desarrollarán métodos más rigurosos y algoritmos más rigurosos para robustecer algoritmos de aprendizaje automático frente a ataques dirigidos, que convergerán en pipelines operativos para su implementación en entornos reales de sistemas basados en IA. La metodología y el software producidos se pondrán a disposición de la comunidad para promover un desarrollo más responsable y seguro de la IA.

PERFIL PROFESIONAL

Requisitos mínimos:

- Graduado/a o Licenciado/a en Matemáticas o en Ingeniería Matemática
- Máster en alguna rama de Aprendizaje Automático.
- Conocimiento de Inglés y Español.

Méritos valorables:

- Dominio del lenguaje de programación Python.
- Formación en métodos de análisis bayesiano y aprendizaje automático.
- Experiencia contrastada con contratos en investigación.

QUÉ SE OFRECE

Se ofrece una formación puntera en temas de tanta actualidad como Inteligencia Artificial y Ciberseguridad, orientados a realizar una tesis doctoral en el área de Aprendizaje Automático Adversario (AAA), pilar fundamental para el desarrollo de un marco riguroso para la gestión de riesgos en IA. Dentro del programa formativo se incluyen estancias en laboratorios principales en AAA como Cagliari y Urbana Champaign, formación en competencias digitales asociada a las actividades del DataLab, así como formación en transferencia a mercado y difusión de la investigación dentro de las actividades del precitado grupo integrado en el ICMAT, centro de referencia en investigación matemática en España.

Condiciones de contrato:

Contrato Predoctoral de 4 años de duración. Salario anual bruto de 23.871,33 €.

Inicio del contrato: antes del 31 de diciembre de 2024

CONTACTO DEL INVESTIGADOR PRINCIPAL

E-mail: marta.sanz@icmat.es

Teléfono: +34 91 29 99 743

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