

Marie Skłodowska-Curie Actions Staff Exchanges

1. IDENTIFICAÇÃO DO PROJETO

Nome do Projeto	AI Attack and Defense for the Smart Healthcare
Acrónimo	ANTIDOTE
Call	HORIZON-MSCA-2023-SE-01
Programa	Horizon Europe — Marie Skłodowska-Curie Actions (MSCA)
Tipo de Ação	Staff Exchange (SE)

2. Keywords

Cybersecurity • Medical Image Analysis • Artificial Intelligence • Medical IoT •
Adversarial AI • Robust AI • Cyberattack Detection

3. Abstract

The smart healthcare domain utilizing a combination of Artificial Intelligence (AI) and medical Internet of Things devices is undoubtedly transforming the healthcare industry as it can deliver new applications and solutions that benefit patients, doctors and hospitals. Improved treatment, cost reduction and faster diagnosis are some of the advantages that smart healthcare brings to healthcare stakeholders. First, AI can be utilized to efficiently process data for improved disease diagnosis in medical images including liver lesion classification and segmentation, brain tumor segmentation, breast cancer detection, etc. Besides, AI can assist in securing the healthcare system from cybersecurity attacks that target the operation of medical IoT devices or sensitive medical data. However, the common assumption with AI is that the training, testing and deployment environment is benign and trustworthy. This assumption, however, does not hold true in general. As a matter of fact, research in this area has shown that small perturbations in the important features of AI models during training or testing phase can trivially undermine their performance. This gives rise to adversarial AI, in which attackers can trick healthcare AI models to degrade their diagnostic or cybersecurity detection performance.

ANTIDOTE project objective is to create a sustainable European and inter-sectoral network of organizations working on a joint research programme in the interdisciplinary fields of Healthcare, AI and Cybersecurity. The participants will exchange skills and knowledge which will allow them to design and develop concrete mechanisms to evaluate the robustness of AI models and propose novel methods to ensure their secure, safe, resilient and robust operations in the healthcare domain. The outcomes of the ANTIDOTE project will have a significant benefit for European society, while strengthening the collaborative research between the different countries and sectors

4. CONSÓRCIO / PARCEIROS

#	Organização	País
1	University of Piraeus Research Center	Grécia
2	PDM – Projecto Desenvolvimento Manutenção	Portugal
3	Ionian University	Grécia
4	Istraživačko Razvojni Centar za Bioinženjering (BioIRS)	Sérvia
5	Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT)	Itália
6	BEIA Consult International SRL	Roménia
7	Universitet u Kragujevcu (University of Kragujevac)	Sérvia
8	INFOLYSIS P.C.	Grécia
9	Universitatea Națională de Știință și Tehnologie (NUSTPB)	Roménia

5. INFORMAÇÃO SOBRE SECONDMENT

Campo	Detalhe
Destinos Possíveis	Qualquer destino internacional, idealmente uma empresa [Depende das vagas disponíveis no momento]
Duração	1 a 12 meses
Bolsa Mensal	2.300 € (acrescidos ao salário)
Secondee — Investigadores	Qualquer investigador com experiência na área e com contrato com a COFAC
Secondee — Estudantes	Estudantes inscritos num ciclo de estudos da Universidade Lusófona



UNIVERSIDADE
LUSÓFONA

