cPAID is an EU project running from October 2024 to 2027

cPAID

Cloud-based Platform-agnostic Adversarial aI Defence framework– CPAID

Project Overview

The innovative EU-funded project Cloud-based Platform-agnostic Adversarial AI Defence framework (cPAID) has officially launched. Over the next 36 months, this initiative will design and develop a holistic defence framework to secure Artificial Intelligence (AI) applications against malicious actions and adversarial attacks.
As AI systems become more integrated into critical sectors, the risks posed by adversarial attacks (such as data poisoning and evasion) are growing. cPAID seeks to address these challenges by leveraging AI-based defence methods (e.g., anomaly detection, machine learning-based intrusion detection systems, adversarial training), security- and privacy-by-design principles, explainable AI (XAI), Generative AI, and context-aware risk assessments.

Project Objectives

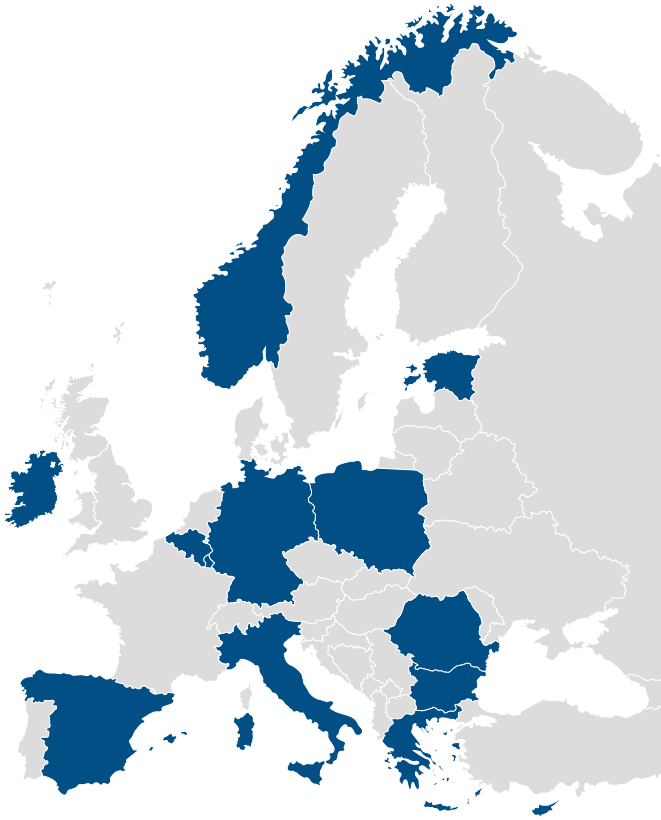
- Design and Development of the cPAID Platform: Create a robust framework for the holistic protection and enhancement of AI systems' resilience against adversarial attacks.
- MLPrivSecOps Methodology: Define and implement a novel methodology that enhances traditional MLOps by integrating Generative Adversarial AI operations and context-aware methods to self-improve system robustness.
- ML-Driven Risk Management Ontology: Research and develop a tailored ontology for AI systems to ensure comprehensive security and robustness assurances.
- AI-Assisted Intrusion Detection and Prevention: Design and develop an advanced system to detect and prevent adversarial intrusions while improving the collection, sharing, and management of information regarding such attacks.
- Cyber Ranges for Adversarial Attacks: Investigate and create simulated environments to raise awareness, improve AI professionals' knowledge, and foster capacity building within the EU.
- Real-Life Use-Case Deployment: Deploy, validate, and evaluate the cPAID components in practical, real-world scenarios.
- Results Dissemination and Impact Maximization: Effectively communicate and disseminate the project's results to ensure widespread impact and knowledge transfer.

For more information about cPAID, its objectives, and its anticipated outcomes, stay tuned for updates on our website and social media channels.

Funded by
the European Union

cPAID

The Consortium



The project unites 17 partners from 11 countries:
Luxembourg, Greece, Romania, Poland, Cyprus, Spain, Estonia, Germany, Belgium, Ireland, Norway, Italy, Bulgaria

uni.systems

InQbit Innovations

orange™

Suite5 We Deliver Intelligence

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

CAFA

Telefónica

HELLENIC MEDITERRANEAN UNIVERSITY

ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΗΡΑΚΛΕΙΟΥ

AEGIS IT RESEARCH

VUB VRIJE UNIVERSITEIT BRUSSEL

UBITECH ubiquitous solutions

konnektable TECHNOLOGIES

NTNU Norwegian University of Science and Technology

cnit consorzio nazionale interuniversitario per le telecomunicazioni

K3Y R&D AND CYBER SECURITY

Follow Us

www.cpaid.eu

/company/cpaid-project

/CpaidEUProject

/@cPAIDproject

Scan for more

Funded by the European Union under grant agreement No 101168407. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or ECCC. Neither the European Union nor the granting authority can be held responsible for them.