SPATIAL

IOTWeek | Dublin
June 20-23, 2022

IoT Week 2022

Security and Privacy Accountable Technology Innovations, Algorithms, and Machine Learning

Jose Gonzalez

jose@australo.org

SPATIAL project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement N° 101021808.

THE CHALLENGE.

Artificial Intelligence is dominated by the United States and China

- The 2 biggest economic poles
- USA: Audio & Natural Language Processing; Autonomous Robotics; Connected & Automated Vehicles
- China: New patents

How to position Europe as a frontrunner in AI.

A strategy centred around two pillars

EXCELLENCE

TRUST

Address specific features of AI technologies that make the application and enforcement of legislation challenging and generate high risks

SPATIAL

RESEARCH GAPS.

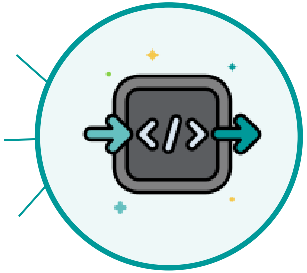
DATA MODEL TRAINING

How data is influencing the behaviour of the AI systems

- BIAS
- PRIVACY
- DATA POISONING

BLACK-BOX AI

Understanding how the systems are making safe decisions

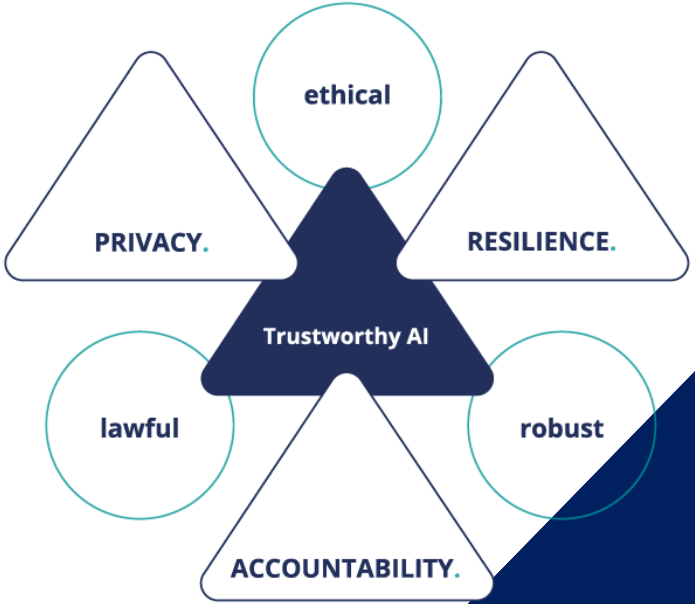


- EXPLAINABILITY
- RISK LEVELS
- TRANSPARENCY

OUR MISSION.

Achieve
Trustworthy AI
in cybersecurity
solutions.

Delivering building blocks to enforce **data privacy**, **resilience engineering**, and **legal-ethical accountability**



OUR GOALS.

Transparency and Explainability

Verification and validation SW + HW mechanisms for security solution development

Explainability Metrics |

Accountability Algorithms |

Distillation for pre-trained Models |

Resilience and Privacy

Enhance resilience in the training and deployment of AI in decentralized, uncontrolled environments

Homomorphic Encryption |

Privacy-preserving Computing |

Risk Assessment |

SPATIAL

OUR GOALS.

Societal Impact for Uptake

Provide adoption and adaptation specifications to reduce complexity of integration

Requirements and KPIs |

Guidelines |

Validation in use cases |

Education and Skills Building

An educational module to raise awareness and provide technical, ethical and legal skills

MOOC |

Knowledge fast-track |

Based on ‘Elements of AI’ |

USE CASE 1 - Privacy-preserving AI on the Edge

- **CHALLENGE:** Assess the performance of privacy-preserving ML deployed on edge computing nodes (telco environment)

- **IMPACT:** Protect user’s sensitive data from devices. Enable 3rd party AI solutions to run securely and accountable in Network Virtualized infrastructure

Telefónica

SPATIAL

USE CASE 2 - Cybersecurity Analysis of 5G/4G/IoT Networks

- **CHALLENGE:** Improve current network security techniques in data infrastructure to become more resilient to attacks

- **IMPACT:** Validate the explainability and resiliency of SPATIAL security analysis in real-world 4G/5G/IoT framework

montimage

SPATIAL

USE CASE 3 – Emergency eCall System

- **CHALLENGE:** Accountable and transparent algorithms for smart data (eHealth) analysis and actuation in critical services

- **IMPACT:** Validation in a eCall communications demonstrator, automatically triggering Next Generation emergency calls

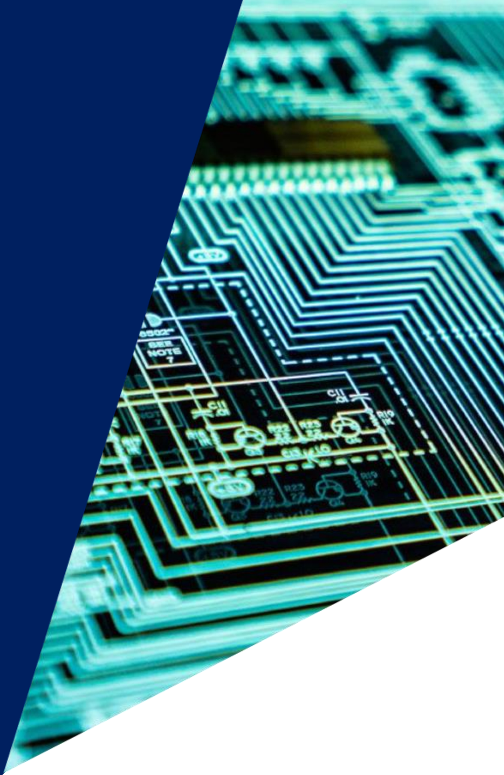
Fraunhofer FOKUS

SPATIAL

USE CASE 4 – Resilient Cybersecurity Analytics

- **CHALLENGE:** Evasion and poisoning attacks against and defences for ML models used in cybersecurity

- **IMPACT:** Implementing prototypes of dynamic attack detection systems and experiment with attack tactics to study their extent and key risks



WITH secure

SPATIAL

OUR TEAM.

TU Delft

WITH secure

montimage

MAINFLUX LABS

Telefónica

Fraunhofer FOKUS

UCD DUBLIN

TARTU ÜLIKOOL · UNIVERSITAS TARTUENSIS · 1632

Orchestrating a brighter world NEC

Erasmus University Rotterdam

AUS TRA LO

Reaktor

StandICT.eu

ARCADIAN-IoT

ERATOSTHENES

IDUNN INDUSTRIAL CYBERSECURITY

IRIS

SECANT

SPATIAL

Thank You

@SPATIAL_H2020

/spatial_h2020

info@spatial-h2020.eu

spatial-h2020.eu

SPATIAL project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement N° 101021808.