Gain Insights into the Latest Cybersecurity Trends from Horizon Europe Funded Projects

A Joint White Paper from AI4CYBER, CERTIFY, CROSSCON, ENCRYPT, KINAITICS, REWIRE, TRUMPET and TRUSTEE

AI4CYBER CERTIFY CROSSCON encrypt KINAITICS REWIRE TRUMPET TRUSTEE

Funded by the European Union

Gain Insights into the Latest Cybersecurity Trends from Horizon Europe Funded Projects: A Joint White Paper from AI4CYBER, CERTIFY, CROSSCON, ENCRYPT, KINAITICS, REWIRE, TRUMPET and TRUSTEE

Executive Summary

In recent years, the significance of cybersecurity has grown exponentially in an increasingly digital world. This white paper represents a collaborative effort to consolidate insights from eight distinct European projects, all funded to address the evolving cybersecurity landscape. Within these pages, we aim to provide valuable insights into each project's objectives, use cases, high-level architecture, and the pivotal technologies that will be harnessed to safeguard our digital ecosystem. By shedding light on these initiatives, we intend to equip various stakeholders with the most current information necessary to tackle emerging cybersecurity challenges effectively.

1 Introduction

In today's interconnected world, the rapid expansion of digital data has ushered in an era of unprecedented innovation and convenience. However, it has also brought forth an array of cyber threats that jeopardize the security and privacy of sensitive information across critical domains such as healthcare, finance, and entertainment. These challenges have necessitated the development of robust solutions that not only enhance data security but also ensure compliance with stringent regulations like the General Data Protection Regulation (GDPR).

The European Union has recognized the urgency of addressing these cybersecurity challenges, leading to the initiation of eight groundbreaking projects, each committed to advancing the field of cyber security. This joint white paper aims to provide an overview of these projects and their objectives, shedding light on their significance in shaping the future of data protection and cybersecurity.

The domain of cybersecurity has evolved rapidly in response to the increasing digitization of critical sectors, exposing vulnerabilities that necessitate innovative solutions. With digital data becoming the lifeblood of industries, the need for privacy-preserving technologies has become paramount. These technologies include Fully Homomorphic Encryption (FHE), Secure Multi-Party Computation (SMPC), and Differential Privacy (DP), which form the backbone of efforts to safeguard sensitive information.

The challenges in the realm of cybersecurity are multifaceted. First and foremost, the exponential growth of digital data has placed immense pressure on existing privacy-preserving technologies, often rendering them inefficient and non-scalable. Moreover, the diverse spectrum of cybersecurity threats demands a comprehensive approach, involving the integration of various privacy-preserving methods.

The limitations of single-key FHE schemes have spurred research into multi-key and threshold FHE, coupled with hardware acceleration, to improve computation times. Traditional security mechanisms also require seamless integration with advanced privacy-preserving technologies, necessitating methods like transciphering to address scalability issues.

To address challenges and limitations related to cybersecurity, the projects discussed in this white paper are poised to embark on several basic research directions. These include:

- Increasingly sophisticated cyber attacks by hackers and cybercriminals.
- Rapidly evolving malware and ransomware threats targeting both individuals and organizations.
- Shortage of skilled cybersecurity professionals and experts to address growing security needs.
- Difficulty in keeping up with constantly changing cybersecurity regulations and compliance requirements.
- Lack of comprehensive cybersecurity awareness and training programs for employees.
- Vulnerabilities in Internet of Things (IoT) devices leading to potential security breaches.
- Insider threats posed by disgruntled employees or careless handling of sensitive data.
- Complexity of managing and securing cloud-based services and data storage.
- Limited resources and budgets for implementing robust cybersecurity measures.
- Persistent challenges in securing critical infrastructure systems against cyber attacks.

The eight European projects highlighted in this white paper represent a collective effort to address the pressing challenges posed by the digital data revolution and the escalating cybersecurity threats. These initiatives seek to redefine the landscape of cybersecurity by advancing privacy-preserving technologies, enhancing data security, and ensuring regulatory compliance. As we delve into each project's specifics, we will uncover the innovative approaches and technologies that hold the potential to reshape the future of cybersecurity in Europe and beyond.

2 Background

The motivation behind this joint paper is rooted in the pressing need to confront the dynamic and evolving challenges of cybersecurity in Europe. The proliferation of digitalization across crucial sectors has ushered in a new era of opportunities and convenience, but it has also ushered in a parallel era of heightened risks. The exponential growth of digital data, particularly in domains like healthcare, finance, and entertainment, has led to an abundance of sensitive information, making data security and privacy preservation paramount concerns.

The digital data revolution has exposed vulnerabilities that malicious actors are quick to exploit, leading to an ever-increasing array of cyber threats. These threats pose significant risks not only to individual privacy but also to the stability and security of organizations, institutions, and nations. The motivation behind this collaborative effort is to harness the collective knowledge and expertise of eight prominent European projects. By working together and sharing insights, these projects seek to form a united front

against the multifaceted challenges of data security and privacy, ultimately strengthening the cybersecurity landscape in Europe.

In addition to the eight projects featured in this joint paper, the European Union has been actively promoting research and development initiatives aimed at bolstering cybersecurity on a continental scale. A multitude of EU-wide research initiatives has been launched, encompassing a wide spectrum of activities within the cybersecurity domain. These initiatives include the development of cutting-edge cybersecurity technologies, the establishment of industry best practices, and the creation of comprehensive frameworks to facilitate regulatory compliance.

While these broader initiatives play a vital role in advancing cybersecurity awareness and capabilities across Europe, this joint paper focuses on the eight projects that represent the pinnacle of innovation in privacy-preserving technologies. These projects delve deeply into the technical nuances of cybersecurity, striving to create scalable, efficient, and user-friendly solutions capable of countering the most sophisticated cyber threats while ensuring strict adherence to regulatory requirements.

2.1 Presentation of Regulatory Bodies' Efforts

Regulatory bodies at the European Union level have taken proactive steps to address the critical challenges posed by cybersecurity in the digital age. One of the most significant regulatory milestones is the implementation of the GDPR. GDPR has set rigorous standards for the collection, processing, and protection of personal data, imposing substantial penalties for data breaches. It has become a cornerstone in data protection and privacy regulation, both within the EU and beyond.

Furthermore, the European Union has been actively engaged in shaping policies and regulations that govern data security and privacy. The EU Data Strategy, for instance, outlines a comprehensive approach to data governance, emphasizing the need for secure and trustworthy data management practices. Regulatory bodies are committed to creating an environment where individuals and organizations can trust that their data is handled with the highest standards of care and compliance.

The joint paper is designed to complement and reinforce the efforts of regulatory bodies by showcasing research initiatives that contribute to the development of privacy-preserving technologies and robust cybersecurity solutions. In doing so, the paper bridges the gap between cutting-edge research and regulatory compliance, serving as a catalyst for a more secure and privacy-conscious digital ecosystem across Europe.

3 Key Research Directions in the Projects

3.1 ENCRYPT

The ENCRYPT project aims to tackle privacy and security challenges in critical sectors such as healthcare, finance, and entertainment, driven by the expansion in digital data. It focuses on making privacy-preserving technologies such as Fully Homomorphic Encryption (FHE), Secure Multi-Party Computation (SMPC), and Differential Privacy (DP) more scalable and efficient to meet GDPR regulations. The project explores advanced FHE schemes, hardware acceleration, and integrates various cybersecurity methods to enhance data protection. It emphasizes user-friendliness with tools for privacy risk assessment and AI-based recommendation systems for selecting PP technologies. ENCRYPT strives for a configurable

framework that secures data and complies with laws, enhancing performance in sensitive data handling, with plans for real-world validation in cross-border federated data processing.

3.1.1 ENCRYPT Objectives

The ENCRYPT project vision is realized around the following list of project-wide objectives:

- To improve the applicability and performance of privacy-preserving (PP) technologies towards GDPR compliant, cross-border federated processing of personal and other sensitive data, developing a toolset of scalable, practical, and reliable privacy-preserving technologies.
- To improve the user-friendliness of PP technologies facilitating the identification, understanding, selection, and adoption of PP technologies by all actors involved in the personal data collection and processing.
- To foster, and inherently support interoperability for privacy-preserving processing of similar data types across organizations, and across sectors.
- To promote GDPR-compliant common European Data Spaces and facilitate the exchange of cyber threat intelligence, liaising with relevant initiatives and projects with a focus on standardization.
- To ensure the applicability of the developed solutions, co-designing them with end-users, and validating them in realistic use cases including federated data infrastructures with personal data.
- To strengthen the ecosystem of open-source developers and researchers of privacy-preserving solutions disseminating, and exploiting open-source project results, as well as upskilling researchers.

3.1.2 ENCRYPT main architecture

ENCRYPT proposes an intelligent and user-centric framework (Fig. 1) for the confidential processing of privacy-sensitive data via configurable, optimizable, and verifiable privacy-preserving techniques and its overall architecture is given in the figure below.

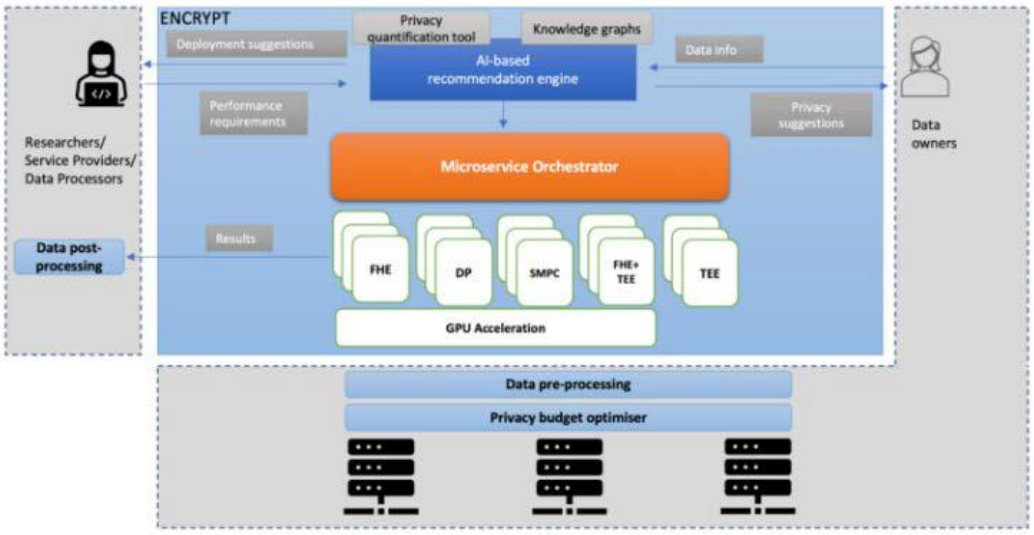

Figure 1 The ENCRYPT framework architecture

ENCRYPT harnesses state-of-the-art privacy-preserving technologies like FHE, SMPC, DP, and TEE. These technologies are configurable for enhanced security and performance. ENCRYPT intelligently combines

their unique features to overcome limitations while capitalizing on their individual advantages. To address performance concerns, the platform provides Graphics Processing Unit (GPU)-based acceleration services, optimizing the processing of confidential data.

Furthermore, ENCRYPT includes intelligent components that adapt to user and data requirements. An AI-based recommendation system offers insights on necessary privacy levels and the deployment/configuration of privacy-preserving technologies, ensuring personalized recommendations for various user profiles. The platform supports GDPR compliance through knowledge graph tools that standardize datasets. Privacy quantification helps users assess and match privacy needs for specific data. Data pre-processing streamlines the execution of selected privacy-preserving technologies, reducing computational overhead. Additionally, post-processing aids in easily retrieving and interpreting results. ENCRYPT's flexibility and adaptability make it a comprehensive solution for secure data processing.

3.1.3 ENCRYPT main technologies

The main technologies in the ENCRYPT project are the following:

- **Homomorphic Encryption**: Homomorphic encryption (HE) allows encrypted data computations. Fully Homomorphic Encryption (FHE) handles additions and multiplications but has noise issues. Various HE schemes exist, each with unique features. The ENCRYPT project uses OpenFHE for its robustness and supports multi-user engagement. It aims to scale HE by integrating it with Trusted Execution Environments (TEE) and transciphering, blending homomorphic with symmetric encryption. Research focuses on advancing non-linear operations via functional bootstrapping from TFHE, targeting practical HE applications.
- **Virtual Secure Enclave:** Privacy-preserving technologies such as Homomorphic Encryption (HE) and Trusted Execution Environments (TEE) face challenges like delays, Ciphertext Expansion (CTE), and limited memory (e.g., Intel SGX's 128MB). The ENCRYPT project introduces a Virtual Secure Enclave that combines TEE and HE, offloading HE tasks to cloud-based TEEs to overcome CTE and memory issues. It also refreshes ciphertext noise within TEEs, improving security and efficiency by addressing both noise accumulation and memory limitations.
- **Differential Privacy:** Differential Privacy (DP)[1] is a mathematical framework used in ENCRYPT to ensure data analysis privacy, valued for its composability, group privacy, and resilience against external information. Composability allows for secure modular designs, group privacy manages correlated data effectively, and robustness defends against external data knowledge. ENCRYPT applies DP to mask input data for AI integration and allows users to manage the privacy-utility trade-off with a "privacy budget." It enhances Deep Learning libraries to optimize this budget, balancing privacy with data usefulness, in line with ENCRYPT's objectives.
- **Data preprocessing tool services:** The ENCRYPT data preprocessing tool optimizes privacy technologies by preparing datasets for better performance. It selectively encrypts key data for Homomorphic Encryption (HE) to boost privacy and scalability and minimizes risks in Differential Privacy (DP) by reducing feature correlations. It also improves data quality by eliminating duplicates and managing missing values and identifies Private Identifiable Information (PII) across

[1] Dwork, C., "Differential privacy" in Automata, Languages and Programming, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, Springer Berlin Heidelberg, 2006, pp. 1–12.

formats, supporting the Recommendation Engine (RE) in choosing appropriate privacy methods. This tool significantly enhances data privacy and the efficiency of ENCRYPT's privacy technologies.

- **Acceleration Service:** GPUs, known for parallel processing capabilities, are crucial in speeding up tasks requiring extensive computations, like graphics rendering and scientific simulations. Within the "ENCRYPT" project, leveraging GPU acceleration is targeted at boosting data processing speeds using privacy-preserving technologies like FHE, enhancing overall efficiency.
- **Knowledge Graphs:** Knowledge Graphs (KGs) support data interoperability, sharing, and understanding, ensuring integration across fields. ENCRYPT uses ontologies for accurate modeling and structuring of information and relationships, allowing scalable integration by merging existing components. It follows W3C standards such as RDF and OWL, incorporating key ontologies like FIBO, SNOMED CT, DICOM, UCO, and DPV for specific applications.
- **Risk Assessment Framework:** A methodology and framework, alongside a prototype, are created for evaluating privacy and cybersecurity risks, featuring an ongoing assessment process supported by a tool. The aims are to pinpoint and mitigate high-risk privacy threats and adapt the methodology for various use cases. Initial steps require choosing a privacy-sensitive business process, engaging stakeholders (DPO, CISO, Process Owner), and documenting the process, data processing, and IT assets. Feedback is expected after using the methodology and tool.
- **AI-Recommendation Engine:** The ENCRYPT project introduces an AI-based recommendation engine (RE) to help choose appropriate privacy-preserving technology (PPT) based on data sensitivity, usage, computational resources, and performance needs. Utilizing Fuzzy Logic, it simulates human decision-making, showcasing AI capabilities. The RE also incorporates insights from other privacy-enhancing technologies (PETs) in ENCRYPT, such as Knowledge Graphs and data preprocessing, for thorough data protection.

3.1.4 ENCRYPT use cases

The ENCRYPT project explores use cases into the following areas:

- **Medical Use Case – Cooperative Oncology**: Cooperative oncology, involving a multidisciplinary team, presents data-sharing and privacy challenges. The ENCRYPT platform addresses these by securing data communication, ensuring integrity, and preserving patient privacy. It supports secure data processing and sharing among healthcare professionals, aiding in diagnostics and treatment while complying with GDPR and safeguarding against patient identification.

- **Cyber Security Use Case:** The CTI use case in ENCRYPT addresses privacy concerns in cyber threat intelligence (CTI) by using privacy-preserving methods like data minimization, anonymization, and pseudonymization to safeguard data during collection and sharing from sources like social media and vulnerability databases. This approach aims to encourage data sharing among organizations to combat sophisticated cyber threats.

- **Fintech Use Case**: ENCRYPT's Fintech use case tackles security and privacy in small-scale banks to protect client anonymity and risk assessment, alongside training AI models with data shared by financial institutions for client analysis and behavior prediction. Privacy-preserving techniques are used to keep sensitive data anonymous while facilitating AI model development for effective data analysis.

3.2 AI4CYBER

AI4CYBER stands for Trustworthy Artificial Intelligence for Cybersecurity Reinforcement and System Resilience and the project aims at fighting advanced cyberattacks and AI-powered cyberattacks with new AI technologies. Along its three years of duration, the project will research and develop services offering smart cybersecurity capabilities to fight such threats. By leveraging data analytics and Artificial Intelligence (AI), the project will advance the state-of-the-art in diverse functions in cybersecurity to improve their efficiency and automation. Such smart cybersecurity functions or services are seamlessly coupled in the AI4CYBER framework. Furthermore, the project researches on the Trustworthiness of the AI, and the results are adopted in the AI4CYBER framework components themselves. The AI4CYBER framework is modular, and its components can be adopted in conjunction or separately, as required.

3.2.1 AI4CYBER objectives

The main objective of AI4CYBER is to establish an Ecosystem Framework, the AI4CYBER framework that provides next generation AI-based cyber security services supporting critical system developers and operators to efficiently manage system robustness, resilience, and appropriate response in the face of advanced and AI-powered cyberattacks. The project will thus deliver a collection of innovative resilience and autonomous response services that leverage data analytics, AI models and Big Data, aimed to be encapsulated in cybersecurity tools to ensure a continuum of system protection.

At the technical level, the main objective can be branched in five objectives as follows:

- Objective 1: Provide an Ecosystem Framework of next-generation trustworthy cybersecurity services that leverage AI and Big Data technologies to support system developers and operators in effectively managing robustness, resilience, and dynamic response against advanced and AI-powered cyberattacks.
- Objective 2: Deliver a new breed of AI-driven software robustness and security testing services that significantly facilitates the testing experts' work, through smarter flaw identification and code fixing automation.
- Objective 3: Provide cybersecurity services for comprehension, detection, and analysis of AI-powered attacks to prepare the critical systems to be resilient against them.
- Objective 4: Offload security operators from complex and tedious tasks offering them mechanisms to optimize the orchestration of the most appropriate combination of security protections, and continuously learn from system status and defense's' efficiency.
- Objective 5: Ensure European fundamental rights and values-based AI technology for the AI4CYBER framework through the integration of demonstrable explainability, fairness and technology robustness (security) capabilities in the AI4CYBER components.

3.2.2 AI4CYBER main architecture

The description of the AI4CYBER framework approach can be found here.[2]

[2] Iturbe, E., Rios, E., Rego, A., & Toledo, N. (2023, August). Artificial Intelligence for next generation cybersecurity: The AI4CYBER framework. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-8).

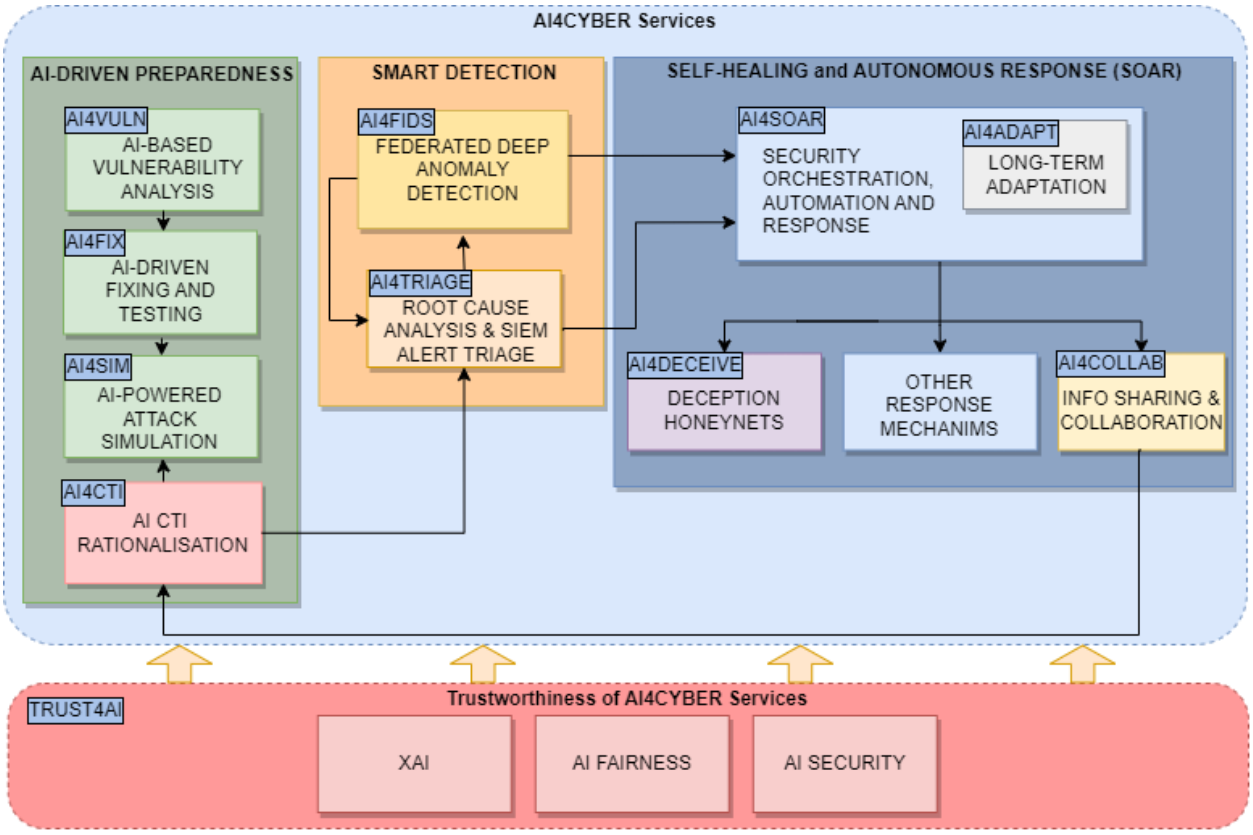

Figure 2: AI4ACYBER framework components.

In the following we summarize the main functionality supported by the components (see fig. 2).

3.2.3 AI4CYBER main technologies

The main technologies adopted in AI4CYBER are data analytics, Big Data and Artificial Intelligence which are employed in the project to improve the efficiency, efficacy, and automation of cybersecurity capabilities in the system lifecycle, from code development, through the system, design and deployment to the operation.

The AI4CYBER framework solution combines the following services:

- AI4VULN – Code testing: An open-source solution to perform automatic identification and verification of vulnerabilities and weaknesses in the code with much higher accuracy rate than existing vulnerability analysis solutions thanks to the application of symbolic execution and the use of AI to support scalability.
- AI4FIX – Vulnerability fixing: A fully open-source end-to-end vulnerability fixing solution supporting Java, bringing automatic unit testing of proposed fixes, which enables to shift the fixing of the vulnerability much earlier in the software development flow, which in turn saves development time and reworks.
- AI4AICTI - Cyber Threat Intelligence improvement: An advanced solution that offers latest AI-powered Cyber Threat Intelligence (CTI) to detection and threat simulation tools for raising their efficiency, including data of both Adversarial Machine Learning (AML) attacks and AI-boosted attacks.

- AI4FIDS – Federated Detection of threats: A high-performance and accuracy detection solution for Advanced and AI-powered attacks detection in distributed environments where privacy of data processed by detection agents need to be kept.
- AI4SIM - Threat Simulation: An Advanced cyberattacks simulation solution capable to simulate advanced and AI-powered attacks against Information Technology (IT), Operational Technology (OT) and IoT systems depending on the customer needs.
- AI4TRIAGE – Incident triage: AI-based root cause analysis and alert triage to prioritize events to focus on the response.
- AI4SOAR – Security Orchestration, Automation and Response: AI-powered Security Orchestration, Automation and Response solution capable to deploy multiple security controls at different layers of the system for better react against cyber incidents and attacks.
- AI4ADAPT – Long term adaptation: The service that will enrich the AI4SOAR with long-term response based on self-learning the system status and the efficiency of the security controls deployed.
- AI4DECEIVE – Deception and honeypots: The intelligent deception mechanisms that will enrich the response of the AI4SOAR.
- AI4COLLAB –Information sharing and collaboration: The service for automatic anonymous sharing of incident information.
- TRUST4AI - Trustworthiness of AI: A set of highly innovative methods and models ensuring trustworthiness of AI systems. The services include AI explainability methods, AI fairness evaluation and security testing against Adversarial Machine Learning threats.

3.2.4 AI4CYBER use cases

There are three validation use cases in AI4CYBER, which propose scenarios of representative critical systems in Europe, as follows:

- **Electricity Smart grids:** AI4CYBER will simulate advanced, AI-powered, and adversarial attacks on Energy sector assets, including Wide Area Measurement Systems (WAMS), Building Automation Systems, and Electric Vehicle (EV) Charging infrastructure, across various application domains.
- **Banking applications and services:** AI4CYBER will enhance banking applications' security, complementing existing tools to improve both static and dynamic defenses. It will be tested in scenarios aimed at bolstering banking infrastructure cybersecurity against advanced network attacks and leaks, and streamlining vulnerability detection, fixing, and management in banking applications, reducing human involvement and increasing efficiency.
- **Hospital services:** AI4CYBER will be evaluated in hospital settings, focusing on the security of health data and EHR systems against cyber-physical attacks targeting services like user authentication, patient check-ins, and laboratory and radiology requests and results.

3.3 CERTIFY

The CERTIFY vision is to provide IoT stakeholders with tools and mechanisms necessary to achieve a guaranteed level of security, by empowering them to detect, evaluate and respond to virtually any possible attack in a collaborative and decentralized way throughout the entire lifecycle of IoT-enabled systems. The CERTIFY mission is to define a sound methodological (aligned with international frameworks and standards), technological (encompassing cybersecurity enablers) and organizational (considering skill development and stakeholders needs) approach towards IoT security lifecycle management. The CERTIFY

approach will enable: i) security by design support; ii), continuous security assessment and monitoring; iii) timely detection, mitigation, and reconfiguration; iv) secure device update; and v) continuous security information sharing. The CERTIFY project aims at designing and implementing a novel framework (Figure 3) for managing the cybersecurity of network-connected IoT devices throughout their whole lifecycle. Indeed, we advocate that only a holistic way of managing device security can strengthen cybersecurity resilience while providing an opportunity for cost reduction.

3.3.1 CERTIFY objectives

To achieve its mission, CERTIFY defined a set of specific objectives:

- Cybersecurity situational awareness for IoT-enabled environments through a multi-stakeholder sharing of threats and mitigations.
- Secure reconfiguration and maintenance of customizable embedded devices by means of open hardware primitives and services.
- Perform security operational management based on bootstrapping and monitoring of attacks and malicious behaviors.
- Runtime security compliance and continuous certification methodology via empirical and objective metrics.
- Foster knowledge delivery via wide dissemination, capacity building and supporting standardization activities.
- Industrial validation of the CERTIFY framework in IoT ecosystems.

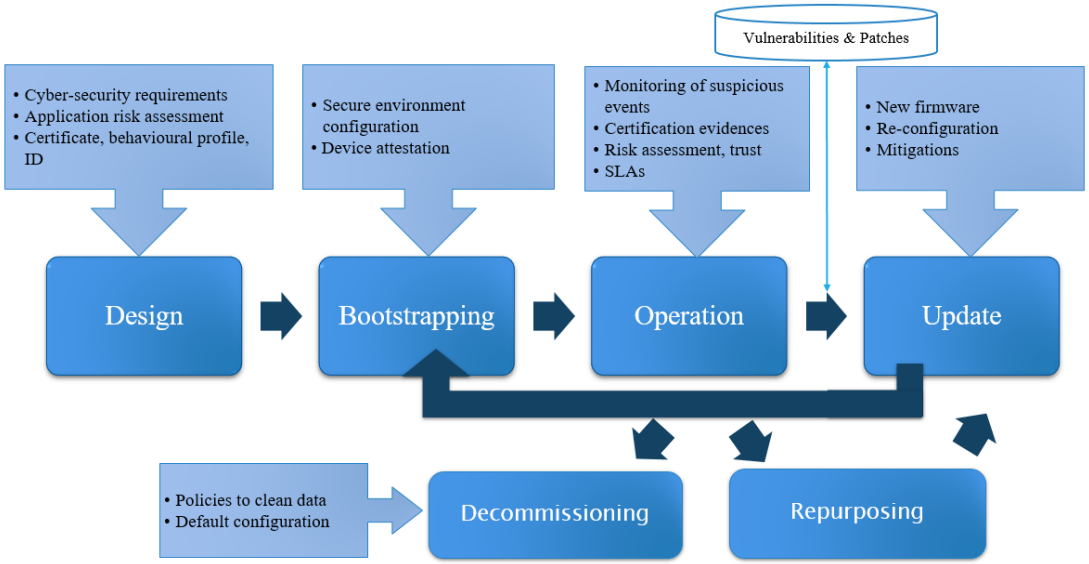

Figure 3: The enhanced cybersecurity lifecycle in CERTIFY

3.3.2 CERTIFY main architecture

The CERTIFY framework is structured into three layers for IoT security: the foundational layer focuses on security enablers for RISC-V and ARM hardware architectures; the middle layer develops software solutions and agents for device and network monitoring; the top layer involves security services for IoT environments and data sharing with external partners. To maintain device security over its lifespan, CERTIFY introduces a cybersecurity lifecycle management framework for IoT, facilitating internal and

external security information exchange, including interactions with manufacturers and ISACs. This supports security decisions, updates, and risk assessments, aiming for agile certification processes. CERTIFY's approach to IoT security management includes security by design, continuous assessment, rapid response to threats, secure OTA updates, and ongoing information sharing. Components and solutions part of the CERTIFY architecture are regrouped in a number of categories:

- CERTIFY secure node: it includes the design and low-level security enablers for the MCUs (Micro Controller Units).
- CERTIFY security services: it includes the agents running on the embedded device offering, secure bootstrapping, runtime attestation, authentication, and reconfiguration.
- CERTIFY enforcement domain: services deployed in the domain to provide a secure device update and enrolment.
- CERTIFY orchestration domain: supported by the inventorying and registry, it orchestrates the security operations performed on the device and in the domain.
- CERTIFY runtime sensors and monitoring domain: collects and processes logs and row data to protect against cyberthreats and vulnerabilities, and enforces the best security responses considering external knowledge and current configuration of the domain.
- Cyber-threat sharing domain: includes services for the secure configuration of the IoT devices according to device specifications and latest threats, and the sharing of the local knowledge.
- Manufacturer sources: CERTIFY leverages the knowledge on threats and vulnerabilities affecting the IoT devices to securely configure them and trigger the evaluation methodology once an update is required due to a changed threat landscape.

3.3.3 CERTIFY main technologies

The following technological pillars constitute the CERTIFY framework:

- The infrastructure for sharing security information leverages digital ledger technology (DLT) to provide a reliable and transparent platform for exchanging data on vulnerabilities, threats, and attacks among stakeholders, including manufacturers, consumers, certification authorities, and Information Sharing and Analysis Centers (ISACs).
- Secure bootstrapping and deployment of IoT environments enhance the MUD (Manufacturer Usage Description) file use by adding a behavioral profile that outlines configuration policies across various layers, not just the network, during the device's initial setup and enrollment.
- Secure bootstrapping and deployment of IoT environments enhance the MUD (Manufacturer Usage Description) file use by adding a behavioral profile that outlines configuration policies across various layers, not just the network, during the device's initial setup and enrollment.
- CERTIFY aligns with the Global Platform's secure ecosystem, adopting Secure Elements (SE) in hardware or software and leveraging RISC-V features to innovate a customized Trusted Execution Environment (TEE) for security functions and architecture.
- Effective maintenance and lifecycle support include a security assessment methodology that uses collected evidence for device recertification, adapting to evolving threats by using a threat MUD file for quick mitigation dissemination before patch releases.
- Runtime attestation involves integrity monitoring solutions that assess device integrity from the network bootstrapping phase, allowing for flexible attestation goal reconfiguration with minimal runtime overhead, utilizing hardware security features.

- IDS, SIEM, and SOAR represent tools for detecting network intrusions, correlating security information from sensors, and orchestrating automated responses in the deployment domain.

3.3.4 CERTIFY use cases

The CERTIFY approach will be validated with respect to a substantial set of challenging use cases contributed by project partners (and briefly mentioned in this section):

- **Secure management of devices in a connected aircraft cabin system**: IoT devices in aircraft cabins will enable intelligent cabins but managing them securely poses challenges. This involves ensuring secure deployment, continuous monitoring, and maintaining the availability, integrity, and confidentiality of software and data on these devices.
- **Smart micro-factories**: Smart production environments are blending Operational Technology (OT) and Information Technology (IT) into a pervasive computing system. Challenges arise from legacy components, retrofitting sensors, diverse communication protocols, and cloud-based management, needed to adjust to evolving product and production demands.
- **Tracking and monitoring of artworks**: Safeguarding artworks during transport and exhibition is a top priority for stakeholders like owners, couriers, insurers, and museums. This can be achieved by using lightweight embedded devices as black boxes, recording environmental events that may indicate mishandling. Challenges include securely attaching the device to the artwork, ensuring the logs' integrity and availability, and monitoring the device.

3.4 CROSSCON

IoT infrastructures are intricate, comprising hardware, firmware, OS, network, edge, and cloud layers, expanding the attack surface. IoT deployments involve diverse devices with varying security features, complicating security measures. The edge, hosting most IoT devices, presents a diverse landscape, from basic microcontrollers with limited resources to powerful APUs and adaptable hardware for ML. Ensuring a common security baseline across this diversity is challenging. Even devices of the same class may use different hardware (e.g., ARM vs. RISC-V) and proprietary security mechanisms (e.g., ARM OP-TEE, Intel SGX, Trustonic TEE, Qualcomm TEE, RISC-V Keystone), hindering interoperability and trust. To address these challenges, the Cross-platform Open Security Stack for Connected Devices (CROSSCON) project proposes an open, portable, and vendor-independent IoT security stack. CROSSCON aims to provide essential security services across various edge devices and computing architectures, including RISC-V. By offering flexibility and compatibility, CROSSCON seeks to enhance IoT security, mitigating potential vulnerabilities and fostering interoperability throughout the IoT ecosystem.

3.4.1 CROSSCON objectives

The main objectives of CROSSCON are:

- Support IoT stakeholders with the design and implementation of an innovative IoT open-source security stack.
- Strengthen memory protection and isolation in new and existing TEEs, mitigating the impact of side-channel attacks.
- Provide methodology, techniques, and related tools to formally verify "correct by design" secure open-source software and firmware for connected devices.
- Offer IoT stakeholders with a set of novel and high assurance trusted services.
- Provide a toolchain that integrates and validates lightweight techniques for security assurance.

- Provide IoT stakeholders with a validation and testing methodology, a replicable testbed, and testing and validation results for CROSSCON innovations.

3.4.2 CROSSCON main architecture

The purpose of the CROSSCON architecture is to enable the secure and isolated execution of security-sensitive tasks on a wide variety of IoT devices having very different levels of hardware (HW) support for security features. The goal of CROSSCON, therefore, is to define a flexible and adaptable set of architectural components that can provide a set of security features maximally utilizing the capabilities of the underlying HW platform to provide the best possible level of isolation for sensitive workloads. To achieve that CROSSCON aims at designing and implementing an open, highly portable, and vendor-independent IoT security stack, and offers the necessary low-layer security primitives and trusted services to enable essential services and security properties at the higher layers, to the operating systems and applications running on IoT devices. The overview of the architecture is depicted in Figure 4.

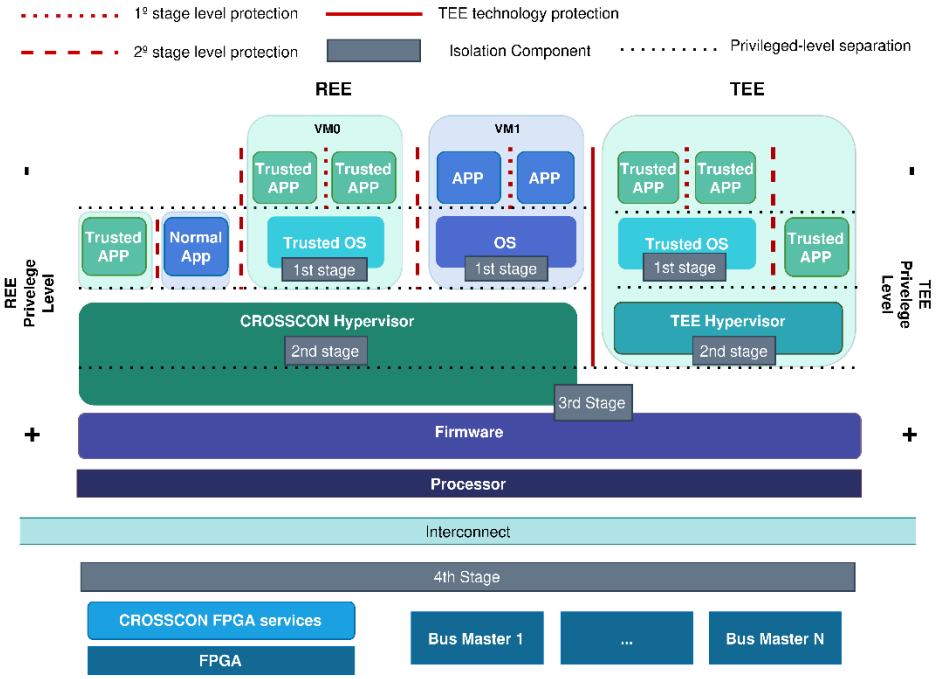

Figure 4: CROSSCON architecture

3.4.3 CROSSCON main technologies

The CROSSCON secure stack includes several components embedding novel technologies developed and/or extended during the project. In particular, an essential component of the stack is the **CROSSCON Hypervisor.** The hypervisor's ultimate objective is to create and support distinct and isolated VMs, ensuring they run as if they were operating independently on separate hardware. The hypervisor operates within a dedicated layer, with higher privileges than the OS, safeguarding hardware resources and leveraging various isolation mechanisms. CROSSCON intends to provide a hypervisor that allows hardware resources to not be shared across VMs and provide a set of built-in mechanisms (e.g., cache coloring) to guarantee strong isolation not only at the architectural but also micro-architectural level. The idea is to complement a TEE architecture with a thin static partitioning hypervisor layer to achieve enhanced isolation and security guarantees through a micro-kernel-like design. The hypervisor will ensure the

correct enforcement of the access control policies to guarantee that VMs can securely execute security-sensitive workloads, for example, running a Trusted OS and Trusted Applications.

3.4.4 CROSSCON use cases

CROSSOCON will demonstrate its results by means of the following uses cases. In particular, the uses cases will stress the interoperability characteristic of the CROSSCON secure stack, as well as the ability to implement the services of the use cases on a wider range of devices compared to the state of the art.

- **Device Multifactor Authentication**: IoT revolutionizes our lives by connecting and enabling device communication, but this connectivity poses security challenges. A key concern is authorizing only legitimate devices to access networks and specific resources. However, implementing Physical Unclonable Function (PUF)-based authentication practically has proven challenging and susceptible to various attacks. To enhance security and defend against Man-in-the-Middle (MITM) attacks, we propose a multi-factor approach that overcomes PUF-based limitations.
- **Firmware Updates of IoT Devices:** Firmware updates are crucial for IoT security, but inability to update is a common vulnerability. Insecure updates enable attackers to inject malicious code. Updates are typically delivered Over-The-Air (OTA) with digital signatures for integrity and authenticity. However, challenges remain because updates may comprise various libraries from different sources, signatures may lack mutual trust, and they don't ensure the update's logic integrity. This use case, considers two types of updates:
  - Full update: the package contains the full replacement of the old package to be installed regardless of what the previous firmware installed was.
  - Partial update: the package contains just the binary difference between the new firmware version and the old firmware version. In this case, the device has to reassemble the firmware package using the binary difference (diff) and the old package.
- **Commissioning and Decommissioning of IoT Devices:** IoT Device Commissioning is vital for devices to obtain necessary information and settings, like security certificates, credentials, and application configurations, before they operate as intended. This process is a critical step in the IoT device lifecycle, preceding regular operation.

3.5 KINAITICS

KINAITICS aims to bring robustness, resilience and responsiveness capabilities to systems involving cyberspace exposure, connections with the physical world through sensors or actuators, and in which Artificial Intelligence (AI) is used to sense, process, or control. AI is profoundly modifying products and systems in various sectors. On the one hand, its adoption creates new risks for systems, such that 60% of companies adopting AI acknowledge that the cybersecurity risks generated by AI are among the most critical. On the other hand, AI has an impact on cyber-physical security practices, both on the attack and defense sides. As a new paradigm emerges from the ubiquitous use of AI in cyber-physical systems, threat and risk assessments on systems need to be redefined to take into account the interconnection of the cyber and physical worlds and the dual use of AI. KINAITICS addresses this challenge by undertaking in-depth technical research to understand the emerging risks, and by adopting innovative defense approaches to protect systems from attack and ensure their robustness and resilience. The ambition of the KINAITICS project is to develop tools adapted to these requirements while taking into account the highest ethical standards.

3.5.1 KINAITICS objectives

The primary goals of KINAITICS include:

- Designing an Integrated Framework: this involves creating a framework that consolidates legal, ethical, and technical requirements to ensure human-aware cyber-physical security.
- Evaluating Risks and Potential Attacks Involving AI: The project aims to go beyond the current state-of-the-art in assessing risks associated with cyber-physical attacks, particularly those that leverage AI technologies.
- Innovating Defense Strategies: KINAITICS seeks to develop defense strategies that are more advanced than the current practices in cyber-physical systems security.

Interleaved with its technical objectives, the KINAITICS project has several objectives concerning the legal aspects:

- Mapping Technical, Legal, and Ethical Requirements: We're conducting research to identify and understand the technical, legal, and ethical requirements related to the project. This involves studying applicable laws and their connections to AI-driven cyber-attacks and defense.
- Ensuring Compliance with Legal and Ethical Standards: The project strives for legal and ethical compliance to promote Trustworthy AI. KINAITICS combines technical and legal requirements to facilitate comprehensive understanding and management of these aspects.
- Focus on AI Safety and Cybersecurity Regulations: The project focuses on AI safety and cybersecurity regulations like GDPR, NIS Directive, and the AI Act Proposal. It seeks to pinpoint best practices and guidelines for ethical research and legal compliance, particularly concerning data protection and security principles.
- Proposing Updates to Legal Frameworks: KINAITICS proposes updates to align the legal framework with IT and OT convergence. It offers guidance and feedback on evolving regulations, including the AI Act in development.

3.5.2 KINAITICS main architecture

In the KINAITICS project, the defense framework is closely integrated with the cyber range and attack framework for a comprehensive security system. Defense strategies incorporate AI tools and user awareness to detect threats, including phishing attacks, through AI-based systems and employee training. The project also focuses on creating frameworks to counter attacks exploiting both physical interfaces of Cyber-Physical Systems (CPS) and their AI components. This versatile framework allows rapid testing of countermeasures in simulated and real-world settings. The attack framework is a crucial part of KINAITICS' cyber-defense platform, covering digital and physical vulnerabilities. The KINAITICS cyber range serves as a dynamic testbed, equipped with controllers, activity generators, and monitoring systems for real-time security assessments. This setup optimizes attack and defense strategies within an information system simulator, ensuring effective addressing of complex challenges in securing AI-integrated cyber-physical

systems. All these components operate within the project's legal framework, providing foundations for legal, ethical, and privacy considerations.

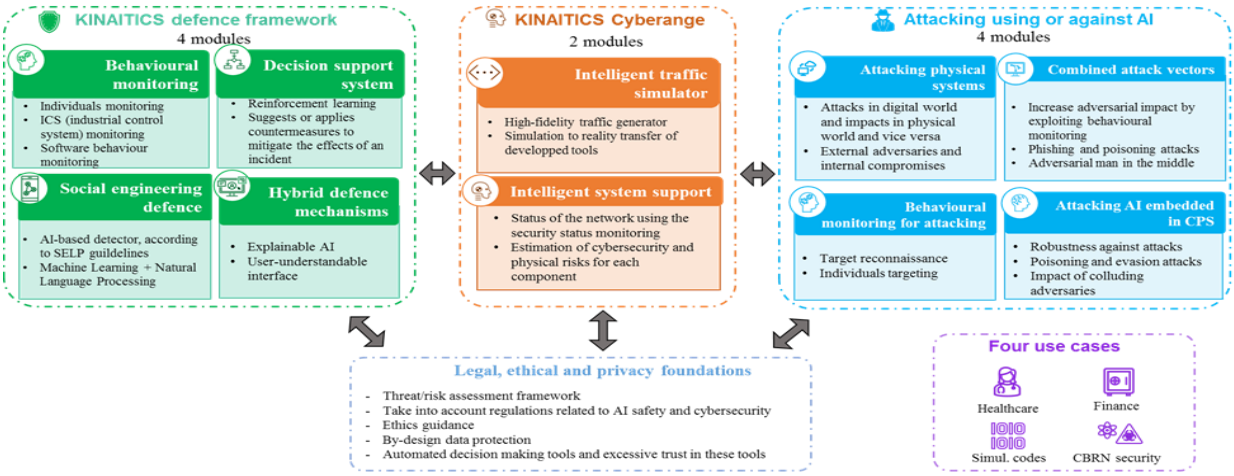

Figure 5: overall KINAITICS architecture

3.5.3 KINAITICS main technologies

Machine Learning (ML) and Artificial Intelligence (AI) enhance performance but also bring substantial cybersecurity challenges. Adversaries target AI systems for unauthorized access and customized attacks due to their complexity and data reliance. Data poisoning during training can lead to incorrect AI decisions. Adversarial attacks deceive AI models with carefully crafted inputs, causing incorrect predictions. Securing ML systems is complex, requiring understanding of adversaries' tactics. Effective countermeasures and defenses can raise security standards. Considering the adversary model, including knowledge and capabilities, is crucial for robust defenses against AI threats.

The KINAITICS project directly confronts AI-enabled threats. However, existing threat taxonomies and matrices often fall short in addressing specialized threat categories or aligning with the specific use cases and security/privacy concerns of the project. To bridge these gaps and establish targeted defenses, the KINAITICS project adopts a data-driven approach, conducting a comprehensive state-of-the-art analysis and examining existing domain-specific threat taxonomies to identify areas for improvement and consolidate effective strategies. The project utilizes frameworks like the MITRE ATT&CK and ATLAS, focusing on adversary techniques targeting AI and ML systems, and explores the ENISA Threat Landscape (ETL) Report for a deeper understanding of the evolving threat landscape.

3.5.4 KINAITICS use cases

The KINAITICS project explores several use cases, two of which are detailed below:

- **Attacks on Simulation Codes for Nuclear Facility Design**: This use case involves using simulation algorithms and the URANIE framework for designing nuclear devices and quantifying uncertainties (UQ). UQ evaluates how system inputs affect outcomes. URANIE determines sensitivity indices through Monte Carlo simulations for UQ. A key vulnerability exists at the interface between URANIE and simulation code, where tampering can lead to incorrect indices and significant risks. Additionally, adversaries might exploit input/output data to launch parameter inference attacks.
- **Phishing Email to Steal Electronic Health Record (EHR) Data**: This use case focuses on the Hospital Information System (HIS), managing sensitive patient data and being vulnerable to cyber threats like

ransomware and data harvesting. The vulnerability varies based on services, security practices, and user knowledge, assuming a standard IT setup. It targets the EHR system among others, with an average cybersecurity approach possibly missing advanced features like digital certificates or two-factor authentication. Selected HIS components are tested against various user behaviors and expertise levels.

3.6 TRUMPET

To address federated learning privacy vulnerabilities, the TRUMPET project[3,4] will conduct research to identify them and develop novel privacy enhancement technologies that will contribute to their mitigation. The project also aims to create a scalable Federated Learning (FL) platform that will improve overall data privacy and enable researchers to run AI-powered studies on European data sets with improved privacy. To demonstrate the security of the new method, experts and third-party organizations will be engaged to test and improve the platform in two eHealth federated learning use cases.

3.5.1 TRUMPET objectives

The primary goal of TRUMPET project is to research and develop novel privacy enhancement methods for Federated Learning, and to deliver a highly scalable Federated AI service platform for researchers, that will enable AI-powered studies of siloed, multi-site, cross-domain, cross-border European datasets with privacy guarantees that exceed the requirements of GDPR[5]. A secondary goal of the project is to research, develop and promote with EU data protection authorities a novel metric and tool for the certification of GDPR compliance of Federated Learning implementations.

3.5.2 TRUMPET main architecture

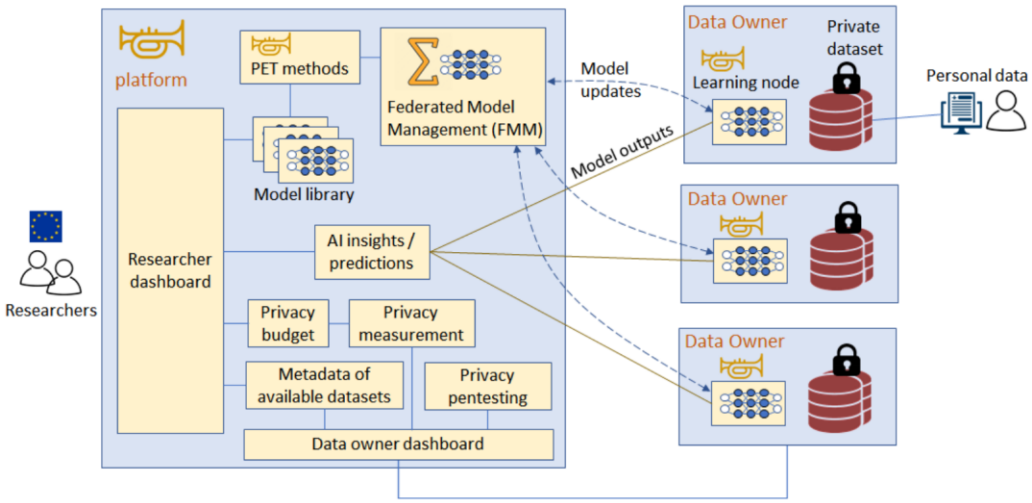

Figure 6: TRUMPET architecture

The TRUMPET high level architecture is shown in Figure 1. The TRUMPET platform facilitates a privacy-focused value chain from data subjects to researchers, acting as an intermediary. Data Owners (hospitals) keep datasets private, only allowing access via a TRUMPET learning node installed on their premises for AI

[3] https://trumpetproject.eu/

[4] https://cordis.europa.eu/project/id/101070038

[5] https://eur-lex.europa.eu/eli/reg/2016/679/oj

model training. This involves a Federated Learning (FL) process where local models are periodically integrated into a global one by the Federated Model Management (FMM), enhancing privacy without moving data. TRUMPET also addresses residual privacy risks in FL with privacy-enhancing technologies (PETs) like differential privacy and encryption, integrated into AI models and aggregation algorithms. Additionally, TRUMPET incorporates adaptive privacy risk management, assessing risks with a novel metric and setting privacy budgets for researcher access, aligning with Data Owners' privacy needs.

3.5.2 TRUMPET main technologies

FL-tailored PET methods. TRUMPET will study how the performance tradeoffs of baseline PETs improve when tailoring them to the FL setting. The following provides a short description of the most relevant PETs in the context of the TRUMPET project:

- Homomorphic Encryption (HE): It allows computation on encrypted data. HE provides a very high level of privacy because the data remain secret. Although theoretically HE could be performed without loss of accuracy, high accuracy will negatively impact computational cost. The TRUMPET FMM will use HE schemes with multiple keys to aggregate AI model updates without decrypting them, and send the resulting encrypted global model back to the learning nodes, where it will be decrypted and used to continue the training on the local dataset until the next model update cycle.
- Secure Multi-Party Computation (SMPC): It allows a group of parties to jointly compute a function while keeping the parties' inputs secret. In general, many SMPC solutions, like for example those based on the use of Secret Sharing, present a lower computational cost than HE, but usually require a higher number of communication rounds.
- Differential Privacy (DP): It offers statistical privacy guarantees by adding noise to attributes of individual data records before sharing them. While it provides the lowest computational overhead among all the PETs mentioned here, DP entails a tradeoff between privacy level and utility.
- Coded Distributed Computing (CDC): It is a combination of distributed computing and coding theoretic techniques that enables the distributed computation of a function in the coded domain while keeping the inputs private.

TRUMPET will use a combination of HE, SMPC and DP, applied to the FL model updates. By combining the PET method, we will strive to remove the residual FL privacy leakage while achieving an optimal tradeoff between computational efficiency, communication cost, reliability and utility, given the network and computation resources and infrastructures available in specific use cases.

A FL-privacy metric. In the TRUMPET project, new statistical privacy metrics are being developed to suit its specific setting, where a small, accountable group collaborates on training a statistical model with federated data. These metrics aim to measure potential knowledge gains by adversaries during data exchanges, aligning with concepts like distributional and Pufferfish privacy. Their advantage lies in their practical applicability, simulating real-world attacks by considering an adversary's uncertainty and using datasets statistically similar to the target for assessment.

A tool for the validation of FL Privacy. Having a definition of a privacy metric does not lead easily to being able to actually measure privacy according to that metric. TRUMPET will develop a tool that keeps track of the privacy budget a researcher has used so far. By doing so, we aim at not only using the classic composition rules, which have been studied for differential privacy, but also to let the tool look more intelligently at the queries, searching for tighter upper bounds of the actual privacy budget consumed.

3.5.3 TRUMPET use cases

The generic TRUMPET platform will be piloted, demonstrated and validated in three use cases of European cancer hospitals:

- **Non-small Cell Lung Cancer (NSCLC) Use Case**. It is the leading cause of cancer deaths globally. Advanced non-oncogene addicted patients often see benefits from immune checkpoint inhibitors (ICIs) that boost the immune response against tumors. Yet only some patients experience long-term benefits from such treatments. *TRUMPET will integrate clinical, biological and radiological data of NSCLC patients treated with immunotherapy to find an algorithm predictive of patients' prognosis.*
- **Stereotactic Body Radiation Therapy (SBRT) Use Case**: Surgery is key for treating solitary metastases in some cancers, but for inoperable metastasis, SBRT is becoming a preferred ablative option. Despite ongoing studies on SBRT's effectiveness for metastatic disease, there are few guidelines on selecting patients who would benefit most from it. *TRUMPET will pilot a privacy preserving classifier predicting the survival probability over 6 months, hence obtaining one criteria for the eligibility to SBRT treatment. Specifically, the model should answer the two following questions: What is the probability for a patient X to survive more than 4 or 6 months? What is the estimated survival period of patient X?*
- **Head and Neck Cancer (HNC) Use Case**: Radiation Therapy (RT) for Head and Neck Cancer (HNC) aims to be curative but often leads to toxicity, causing early and long-term side effects. It is suggested that evaluating late side effects alongside planned dose-volume histograms and RT regimens could improve treatment planning in HNC. *TRUMPET will identify causality relationships between the radiotherapy treatment plan and its delivery towards late side effects in Head and Neck cancer.*

3.6 TRUSTEE

The informatics field currently sees diverse scientific domains converging, such as Health, Space, Automotive, Education, Cross-border, and Environment, creating opportunities for innovative methodologies and knowledge generation. This convergence addresses future accidents, security threats, and complex scientific challenges arising from social conditions and innovation. ICT innovations offer both challenges and opportunities, necessitating evaluation for enhancing multidisciplinary big-data sources with trust, fairness, responsibility, and sustainability. Data space technologies play a pivotal role in integrating these requirements.

The TRUSTEE initiative merges technological and social innovations to ensure secure, sustainable data operations, focusing on optimizing, minimizing, and decentralizing data processing, transfer, and storage. TRUSTEE emphasizes ethical data collection and processing, aligning with responsible AI principles through a co-development approach. A secure-by-design Federated Platform, aligned with EU data strategy and reference architectures (GAIA-X, EOSC, EGI), forms the core, ensuring interoperability, cross-border scenarios, and scalable AI-based applications with the goal of establishing the EU as a secure and trustworthy data hub. TRUSTEE's innovative homomorphic approach guarantees user-friendly, secure, and accountable data handling.

3.6.1 TRUSTEE objectives

The TRUSTEE project combines serverless computing, edge computing, and secure clouds. It aims to provide an open-source, scalable, efficient, and trusted solution for core and edge cloud infrastructures. This solution targets time-critical, self-hosted applications while prioritizing European, privacy-preserving,

green, and responsible data practices. TRUSTEE introduces a methodology to accelerate high-quality data solutions and datasets, emphasizing both speed and data quality as it is depicted in the following figure (see figure 7).

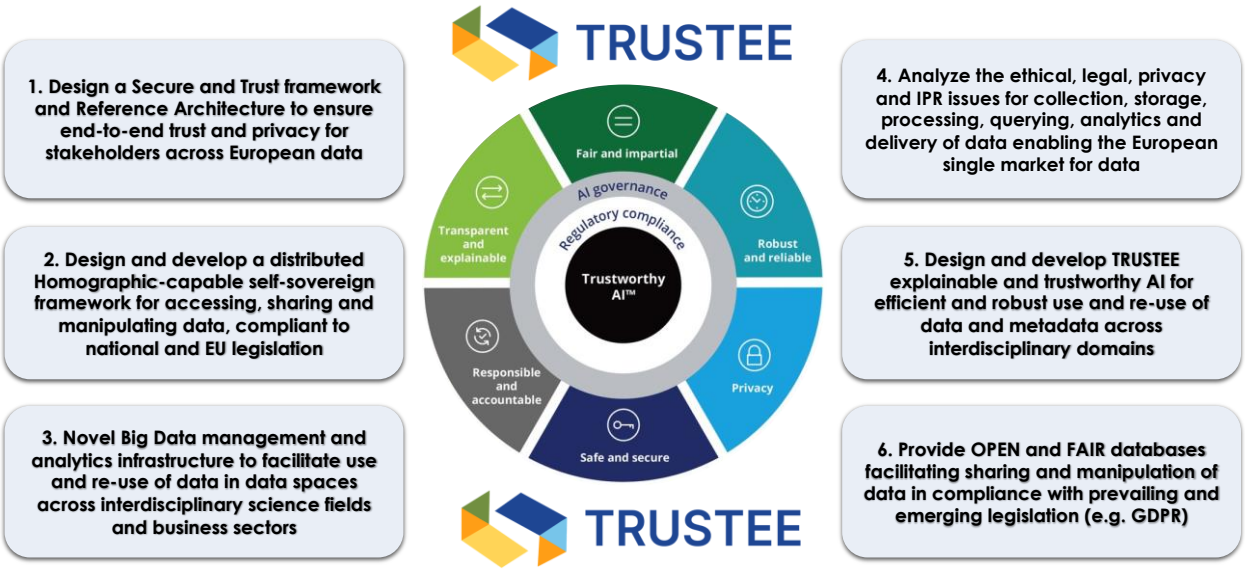

Figure 7: TRUSTEE project

The project underscores the importance of cross-functional collaboration and automation to construct swift and reliable data pipelines. Its innovation is structured around three key pillars:

- Foster Collaboration: TRUSTEE seeks to dismantle existing silos by reassembling request-response arrangements, fostering growth, and enhancing agility. The goal is to encourage active participation from all stakeholders, enabling them to contribute and extract insights from various services.
- Build Trusted Data Solutions: TRUSTEE places a strong emphasis on ensuring the trustworthiness of data. The trust module within TRUSTEE signals the reliability of data through quality flags, such as endorsements and deprecations.
- Automate Testing and Monitoring: Beyond infrastructure focus, TRUSTEE extends its attention to monitoring the health, age (validity/update), and changes of the data itself. Leveraging an API, TRUSTEE ensures that all stakeholders are informed in a distributed manner, allowing continuous training of AI/ML models and data products with the latest and most valid datasets.

TRUSTEE proposes advancements in Self-sovereign technologies by incorporating Blockchain for decentralized identifiers and Homomorphic encryption for cross-disciplinary data federation. This approach enables data consumers to utilize a framework that remains unaware of their identity or equipment, facilitating complex search queries across federated TRUSTEE data repositories. Robust authentication and authorization mechanisms ensure that only necessary data is revealed for any given transaction or interaction. TRUSTEE is committed to privacy preservation, green and responsible data management, providing individuals or organizations with complete ownership of their digital and analog identities. It empowers them to control how their personal data is shared and used, enabling encrypted domain searches while guaranteeing data privacy and confidentiality. The specific objectives of TRUSTEE are shown in the figure below.

3.6.2 TRUSTEE main architecture

TRUSTEE acknowledges that today consumers must be very careful about sharing/accessing data, and national and international regulators/legislators step up privacy requirements. The industry is in need to identify how investing in data protection and privacy can create a business advantage for the proper handling of data, consent, notice, and regulatory obligations; how data is securely shared with third parties; how data is legally collected or stored; how data can be collected for processing; and regulatory restrictions such as GDPR, HIPAA, GLBA, or CCPA. Several effective actions have emerged seeking to address enhanced consumer-privacy and data-protection requirements. These span the life cycle of enterprise data, and expand the processes of operations, infrastructure, and customer-facing practices, and are enabled by data mapping.

3.6.3 TRUSTEE main technologies

The TRUSTEE data-driven platform envisions avant-garde solutions to advance the realms of trustworthy, green, and responsible data management and processing. This is to be achieved through the implementation of value-based digital technologies and solutions, encompassing compliance, privacy-preserving homomorphic encryption, and preservation strategies. The ensuing discourse outlines our architectural designs, meticulously crafted to meet the exigencies of citizens (i.e., consumers), industry, and research sectors. This includes the provision of federated and FAIR (Findable, Accessible, Interoperable, Reusable) data access within a private framework comprising both public and private organizations. The practical implementation of this architecture involves subjecting it to proof-of-concept pilots.

The TRUSTEE platform is geared towards achieving FAIR communication with open data silos and platforms such as GAIA-X, EOSC, and EGI. This entails the exchange of existing and future data derived from diverse EU data spaces, following the tenets of open science EU data policies and procedures. TRUSTEE stakeholders are envisioned to wield user-friendly, secure, trustworthy, transparent, accountable, and environmentally sustainable Information and Communication Technology (ICT) services. These services encompass the entire data lifecycle, including data collection, storage, processing, querying, and delivery.

The architectural design incorporates cutting-edge technologies, notably homomorphic encryption, in strict adherence to EU legislation, including the General Data Protection Regulation (GDPR). This compliance extends to data processors, data subjects, and other stakeholders involved in data-related processes. A focal point of TRUSTEE's approach is the integration of social innovation and privacy impact assessment, achieved through the optimization of processing at the edge, bolstering resilience, facilitating secure data transfer, and storage. This approach aligns with the principles of responsible and trustworthy Artificial Intelligence (AI).

Furthermore, TRUSTEE adopts a Software-Oriented Architecture, fostering adaptability and accommodating the future evolution of the platform. This architectural strategy ensures the delivery of a comprehensive suite of information services tailored for diverse stakeholders, including citizens and professionals. The platform seamlessly integrates existing domain knowledge and services pertinent to the TRUSTEE initiative. The following table summarizes the main subsystems of TRUSTEE.

3.6.4 TRUSTEE use cases

Towards a Privacy Preserving a Secure Framework TRUSTEE aims to utilize Self-Sovereign technologies and with State-of-the-Art homomorphic encryption, to offer a socially and environmental-aware

framework for cross discipline federation of Data. TRUSTEE's fully encrypted solution will be validated through six different use cases supporting GAIA-X, EOSC, EGI, etc. demonstrating a multi-disciplinary, Pan-European federated FAIR (Findable, Accessible, Interoperable, and Reusable) and private data ecosystem.

TRUSTEE use cases are briefly described in this section and are the following:

- **Space**: TRUSTEE will focus on how to support ISS (International Space Station) for research and space missions, based on a series of detailed scenarios developed in the early phase of the project. Through these we will identify the technical and non-technical requirements, as well as the structure of the tests executed to check functionality and user acceptance.
- **Education**: TRUSTEE recognizes the responsibility that educational institutions carry to generate, manage, store, secure and ensure individual privacy of students and administration. We aim to make their job easier by improving data sharing according to GDPR rules and enabling data interoperability with cross-border.
- **SSI - Data**: TRUSTEE's goal is to establish the necessary pathway for multi-stakeholder data exchange and data sovereignty across its platform, by implementing a set of IDS interfaces with the GAIA-X federation layer to allow secure data inference across the entire platform.
- **Health**: TRUSTEE'S platform will be used by the researchers at UCSC in areas such as Epidemiology & Bio statistics, Bioinformatics, Artificial Intelligence and Big Data processing to support clinical research and healthcare process improvement.
- **Automotive**: TRUSTEE focuses on enhancing the safety indexes for autonomous driving in the presence of sensor and data sources, by assessing drivers' behavior and HMI evolution and by using the output as informed experimental feedback for evolving the HMI.
- **Energy**: TRUSTEE aims to help customers that have invested in energy solutions to continuously monitor PV (photovoltaic production, energy consumption and battery storage/charging status to be able to offer Virtual Power Plant services while respecting privacy and data security.

3.7 REWIRE

The rapid growth of emerging technologies, especially in the fields of Internet of Things (IoT) and Edge Computing has significantly grown during the last decade, along with the occurrence of several, major cybersecurity challenges and significant considerations on cybersecurity implications. Even though several approaches aim to meet the needs for secure IoT devices, they do not holistically approach this issue, and they rather focus on applying additional security measures to guarantee security during runtime and after systems' deployment. To this end, major challenges in modern IoT ecosystems still remain unresolved.

The main scope of REWIRE is to establish a holistic framework for guaranteeing the continuous and holistic security assessment of interconnected IoT devices synthesizing complex and dynamic operational ecosystems. REWIRE's vision is the enhancement of the security posture of next-generation smart connectivity "Systems-of-Systems" (SoS) by safeguarding the entire lifecycle of heterogenous IoT environments, starting from the *Design phase* and covering also the *Runtime phase* of systems. To this extent, the REWIRE leverages a gamut of emerging and cutting-edge technologies, such as Formal Verification of hardware/software co-designs, open-specification hardware for open-source software based on open instruction set specifications, Trusted Computing, Blockchain and Artificial Intelligence (AI) for the provision of a unified framework that will guarantee a high level of operational assurance of SoS-enabled environments.

3.7.1 REWIRE objectives

REWIRE introduces a straight-forward vision for a set of innovations on designing a holistic architectural framework for its MVP development, that provides robust solutions to major challenges of cybersecurity for IoT ecosystems. REWIRE has been structured based on a seven-pillar framework defined by its objectives. The core objectives that REWIRE considers essential for both the architecture design and the evolution of beyond the state-of-the-art developments are the following:

1. The framework aims to guarantee **continuous security assessment and management of IoT devices throughout the entire lifecycle** (bootstrapping, commissioning, operation, upgrade) under zero-trust conception.
2. **Security-by-design** through formally verified open-source software and open standard hardware designs for attack surface minimization.
3. **Runtime verification of IoT trustworthiness,** through cryptographically verifiable security proofs and efficient attestation.
4. **Cyber Security situational awareness in heterogeneous IoT environments,** through auditable security patch management and misbehavior detection, to achieve interoperability of the framework.
5. **Trust-aware continuous authentication and authorization** for secure communication and identity management in IoT ecosystems.
6. **Simulation, Validation & Evaluation** of REWIRE Framework in the field of Smart Cities, Smart Satellites and Smart Automotive.
7. The **successful exploitation of the results and the contribution to standardization** for broader adoption of REWIRE outcomes and the maximization of overall impact.

3.7.2 REWIRE main architecture

Towards meeting the aforementioned objectives, the REWIRE consortium has delivered the 1st version of architecture (See Figure 8). The latter is divided into two major parts. On the left-hand side, the design-time phase is illustrated, following a top-to-bottom approach to the description of the workflows that take place in that part of the architecture. On the right-hand side, the runtime phase of the architecture is presented, including the REWIRE-enabled edge device and the cloud-based backend infrastructure of the framework.

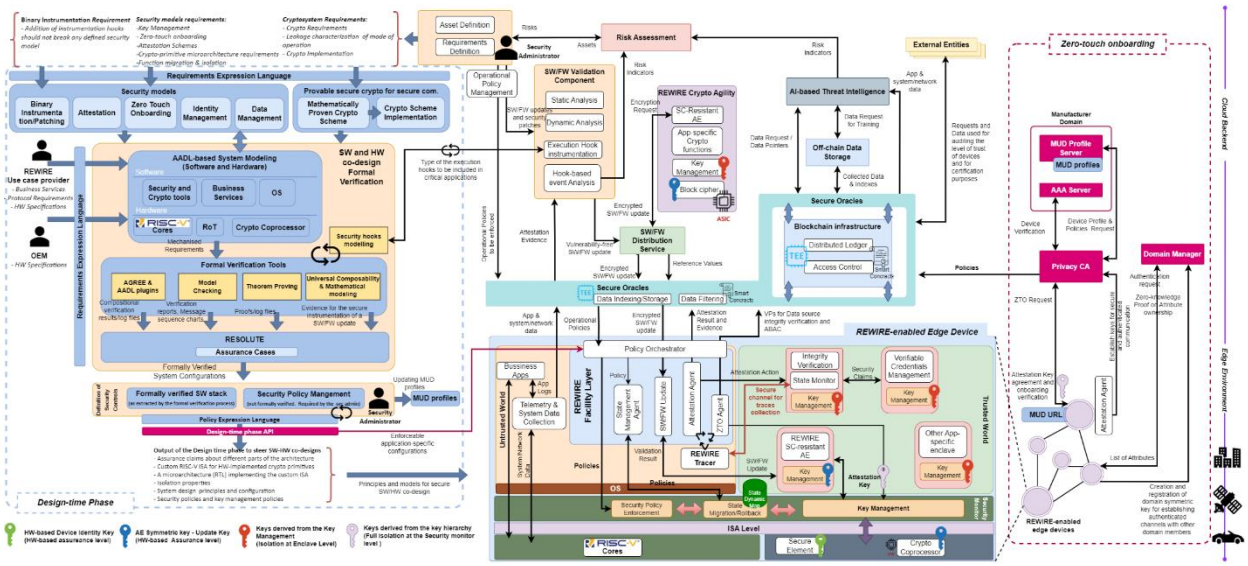

Figure 8: REWIRE Conceptual Architectural Framework

The design phase of the REWIRE project focuses on formal SW/HW co-design verification and establishing security requirements for system deployment. Security administrators, use case providers, and OEMs define essential security requirements, which are then formally verified to ensure the system is secure by design. Based on this verification, secure-by-design elements are identified, and additional security controls can be established through a Security Policy Management process to minimize the attack surface further.

This phase is structured into five steps:

1. Defining overarching security requirements, including security models, cryptosystems, and binary instrumentation, which introduces SW instrumentation hooks for secure software behavior analysis.

2. Mapping these requirements to system artifacts using AADL-based System Modelling for SW and HW, preparing for formal verification.

3. Conducting formal verification using model checking, theorem proving, and universal composability to design security hooks.

4. Implementing formal verification results into enforceable security policies for device operation, including attestation policies for identifying compromised components.

5. Defining the Manufacturer Usage Description (MUD) profile, setting rules and behaviors for runtime behavior comparison and deviation identification.

The runtime phase involves the operation of REWIRE-enabled devices and cloud infrastructure, supporting secure device lifecycle management. This includes secure onboarding, dynamic system updates, threat detection, system introspection, operational assurance, device state management, risk assessment, and secure data sharing. Key to these functionalities is the REWIRE Customizable Trusted Execution Environment (TEE), ensuring secure execution and acting as the trust root for cryptographic operations throughout the IoT deployment lifecycle.

3.7.3 REWIRE use cases

REWIRE platform will be tested and validated in three complex and heterogeneous pilot IoT ecosystems a) Smart Cities, b) Automotive and c) Smart Satellites. These UCs can meet the radically innovative objectives of the project and set the scene for multi-dimensional real-world testbeds. More specifically, the customizable REWIRE RISC-V-based TEE will empower the entire business workflows of secure processing in the pilot's environments. The pilot's infrastructures will be augmented with the REWIRE artifacts by providing new trust management mechanisms for offering auditable and certifiable IoT lifecycle management.

To this extent in the Smart Cities context the project tests and validates the Secure device on-boarding processes, the collaborative threat and misbehavior detection, and FW/SW updates for critical IoT devices. Accordingly, in the Automotive use case, REWIRE ensures the resilient operation of safety-critical functions and dynamic vehicle updates, while in the Smart Satellites use case the focus is on the isolation of critical services for software and security patching of spacecrafts in a secure manner. All the above systems follow the formally verified security-by-design approach for HW/SW co-design, while runtime security mechanisms guarantee the operational assurance of deployments during runtime. The adoption of the REWIRE architecture in the critical application domains of the use cases will lead to state-of-the-art applications by addressing the open challenges for secure IoT systems designs.

4 Future Directions and Joint Activities

As we conclude this collaborative white paper, we look forward to the future directions and joint activities that will further enhance the collective impact of our consortium of European projects dedicated to advancing the field of cyber security. Building on the synergies and shared objectives that have brought us together, we envision several key initiatives to strengthen our collaboration and continue our mission of safeguarding digital landscapes.

4.1 Organizing Workshops

One of the primary avenues for fostering collaboration and knowledge exchange within our consortium is the organization of workshops. We plan to host regular workshops that will serve as platforms for project members to present their latest research findings, discuss emerging trends, and share best practices. These workshops will not only facilitate the cross-pollination of ideas but also provide opportunities for networking and building partnerships that can lead to joint research efforts.

4.2 Joint Journal Paper

We recognize the importance of consolidating our collective expertise into a comprehensive publication that will contribute significantly to the field of cyber security. To achieve this, we propose the development of a joint journal paper. This paper will serve as a comprehensive overview of our collaborative efforts, highlighting the key contributions and insights from each project. It will undergo a rigorous peer-review process to ensure its quality and relevance. By publishing a joint paper, we aim to establish our consortium as a thought leader in the field and disseminate our findings to a wider audience.

4.3 Book Chapters for Every Project

Another avenue for sharing our research outcomes is through the publication of book chapters. Each project within our consortium will contribute chapters to a collaborative book. These chapters will delve into the specific domains and expertise of each project, providing in-depth insights into their respective contributions to cyber security. The book will serve as a valuable resource for researchers, practitioners, and policymakers seeking comprehensive knowledge in the field.

In conclusion, our consortium of European projects is committed to not only advancing the frontiers of cyber security but also to deepening our collaboration and knowledge-sharing efforts. Through workshops, a joint journal paper, and book chapters, we will continue to leverage our collective expertise for the benefit of the broader cyber security community. By working together, we are confident that we can address the ever-evolving challenges in cyber security and contribute to a safer digital environment for all.

EU projects details

ENCRYPT https://encrypt-project.eu/

AI4CYBER https://ai4cyber.eu/

CERTIFY https://certify-project.eu/

CROSSCON https://crosscon.eu/

KINAITICS https://kinaitics.eu/

TRUMPET https://trumpetproject.eu/

TRUSTEE https://www.linkedin.com/company/horizon-trustee/

REWIRE https://rewireproject.eu/