PAROMA-MED

www.paroma-project.eu

Privacy Aware
Privacy Preserving
Distributed
Robust Machine Learning

Newsletter

Issue 3 – Jul 2024

This project has received funding from the European Union Horizon 2020 research and innovation programme under grant agreement No. 101070222

PAROMA-MED

Editorial

Contents

Message from the project coordinator

Dear Reader,

As Paroma-Med embarks on its third year of development, we are pleased to announce that several of our technologies have reached a mature stage, particularly in our federated learning approach. Unlike traditional centralized learning, which involves training AI models with reference data from multiple sources and poses substantial security risks due to the handling of sensitive information, our federated learning method enhances data security by training models locally and then aggregating them at a central node.

In addition, Paroma-Med is working on an innovative crypto watermarking solution that combines watermarking with cryptography. This approach not only safeguards data ownership but also ensures traceability, providing a watermarking-based service to help prevent information leaks.

Moreover, one of our partners, Ericsson, has recently filed a patent for a method that defines metrics to assess and score network resources in terms of security. This patent also includes a way to calculate the optimal path for data transfer, prioritizing privacy and security.

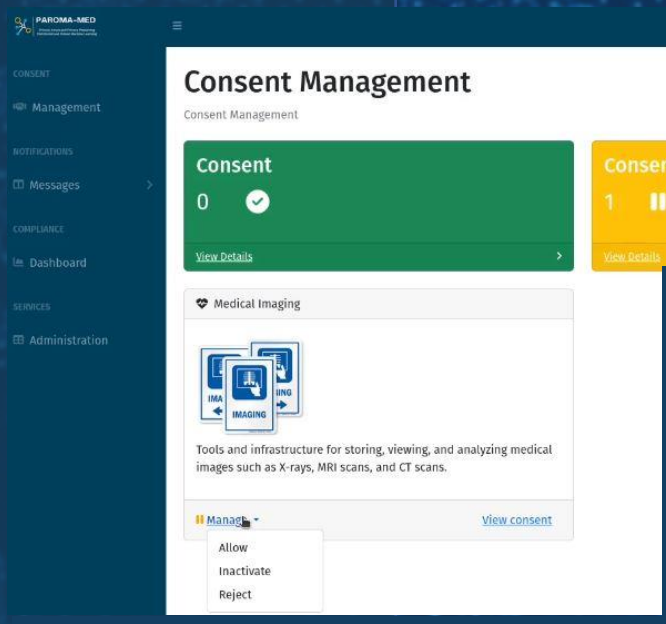
Stay secure, stay protected, stay informed!

Sincerely,
Alessandro Bassi

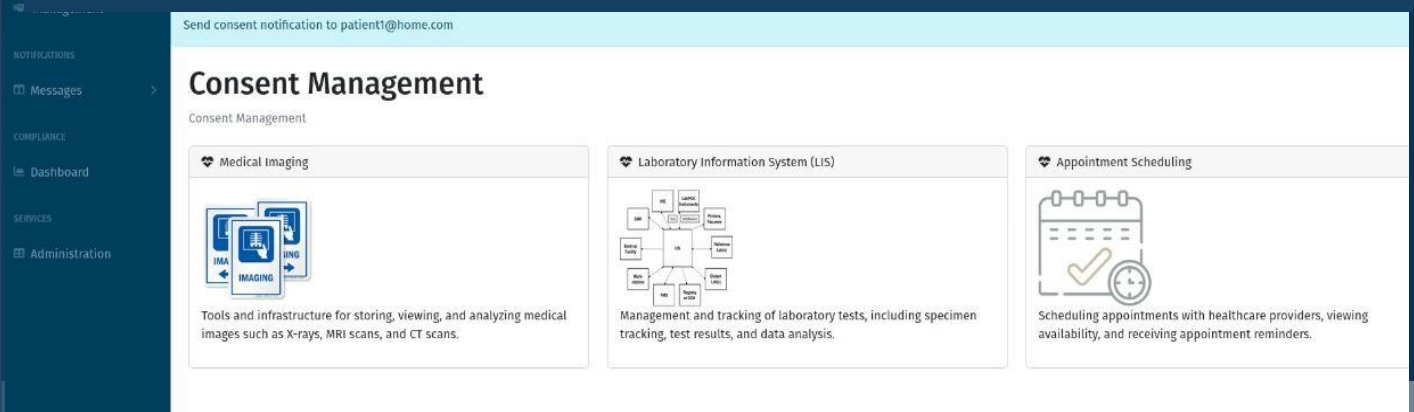
Consent

PAROMA-MED

The mgmt application



The demonstration of the consent management application, developed within the PAROMA-MED project, showcases an efficient and user-friendly process for managing consent between physicians and patients for medical services. The application enables physicians to request consent from patients for AI-based imaging services securely. Physicians log in using secure authentication credentials, select the specific patient, and initiate the consent request process. The patient is then notified of the new consent request and can log in with their secure credentials to access pending requests. Patients can review detailed consent statements and their implications thoroughly before deciding to agree or deny consent. This application ensures a clear and transparent consent management process for both physicians and patients

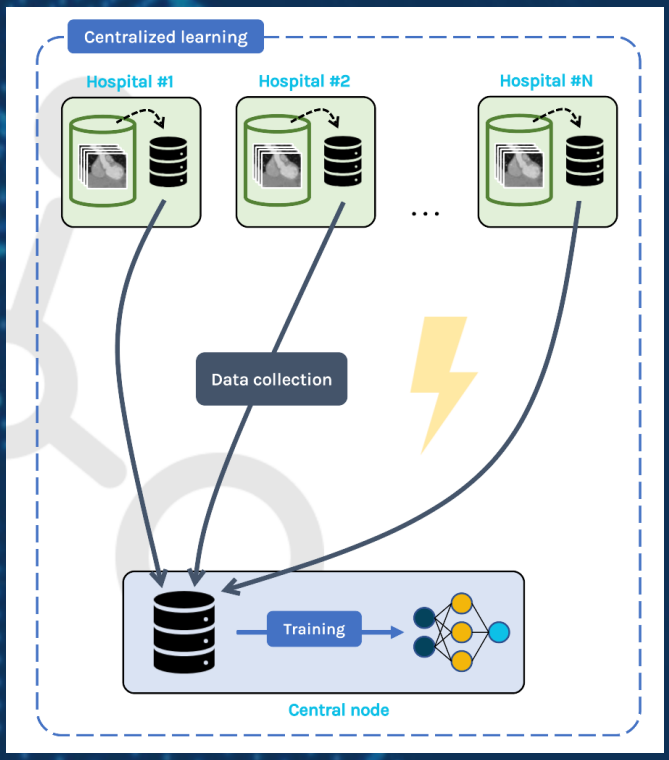


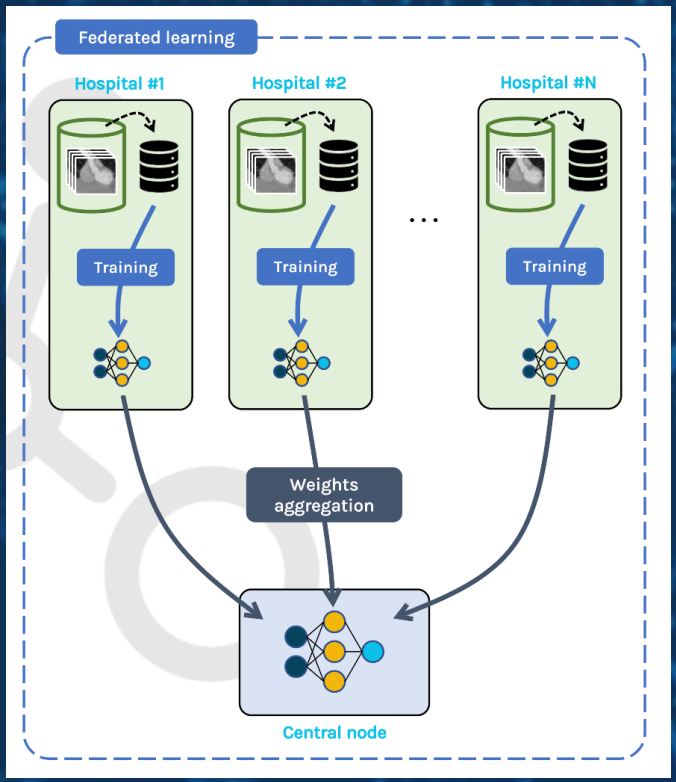
https://www.youtube.com/watch?v=_qws3pq3JQ0

PAROMA-MED

Medical Images Analysis Use Case

The PAROMA_MED medical image analysis use case focuses on medical image analysis, specifically heart segmentation, demonstrating the role of Artificial Intelligence (AI) in modern healthcare. Traditional centralized learning, which involves training AI models using reference data collected from multiple hospitals, poses significant security risks due to the transmission of highly sensitive data.



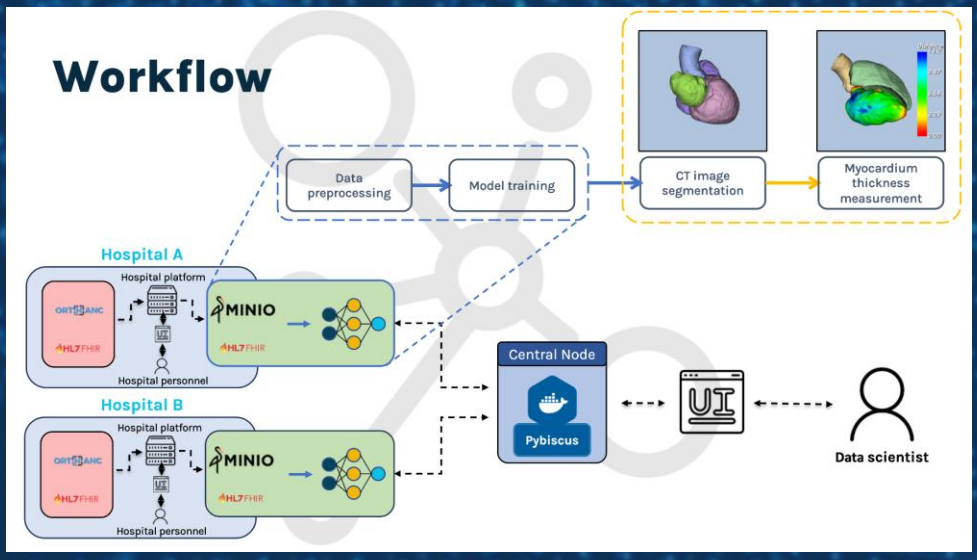


To address this, federated learning is employed, where the model, rather than the data, is transmitted. Within this framework, models are trained locally within hospital domains and subsequently aggregated at a central node, iteratively improving model performance. The PAROMA-MED platform supports this process, where input images, such as CT scans containing five structures (myocardium, left ventricle, right ventricle, left atrium, and aorta), are processed within hospitals. The resultant model is then used to compute myocardial thickness, a critical diagnostic parameter.

https://www.youtube.com/watch?v=Wh5xW31vOWM

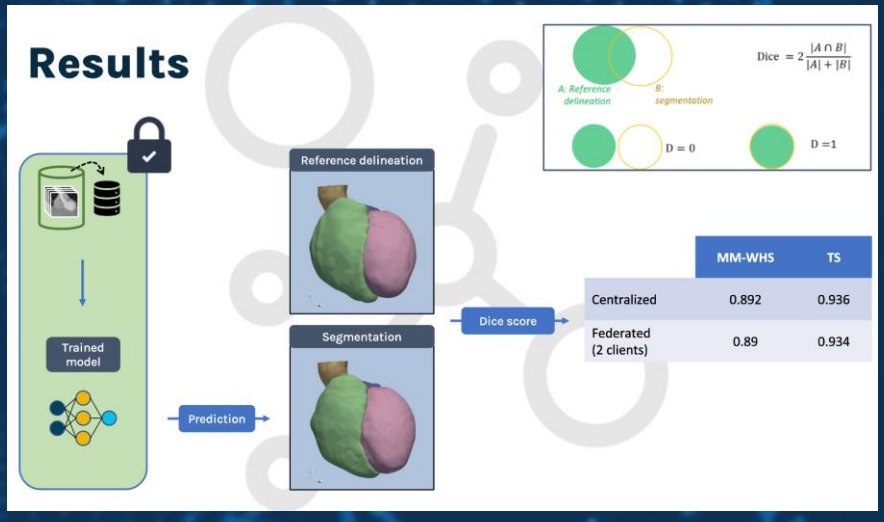
Medical Images Analysis Use Case

PAROMA-MED



This process relies on the PAROMA-MED platform. Data processing and model training take place inside the hospitals, and once the final model is obtained can be used on new images. Performance assessment of the final model is conducted using the Dice Score, a metric ranging from 0 to 1 that measures geometric correspondence between reference delineation and segmentation, with a score of 1 indicating a perfect match.

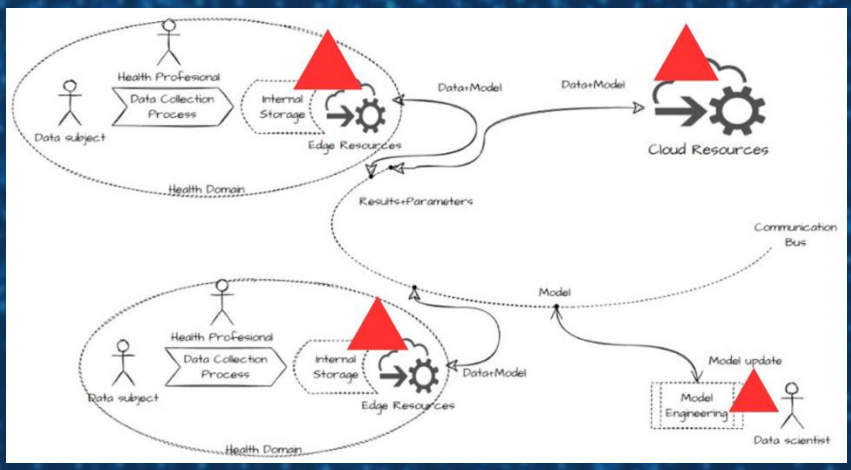
The PAROMA-MED project demonstrates that federated learning can achieve performance equivalent to centralized learning while maintaining patient data privacy.



	MM-WHS	TS
Centralized	0.892	0.936
Federated (2 clients)	0.89	0.934

PAROMA-MED

Crypto Watermarking



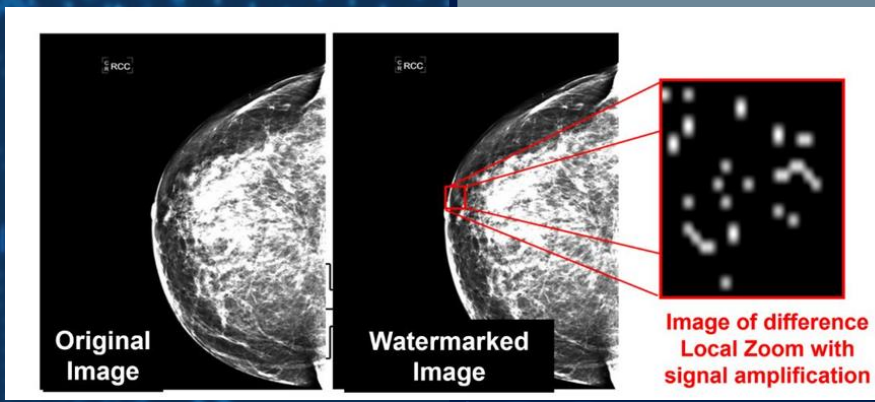
Principle of Image Watermarking

Image differences encode a message (a watermark) that protects the image in terms of:

(a) Ownership,
(b) Traceability (recipient identification)
(c) Data Integrity.

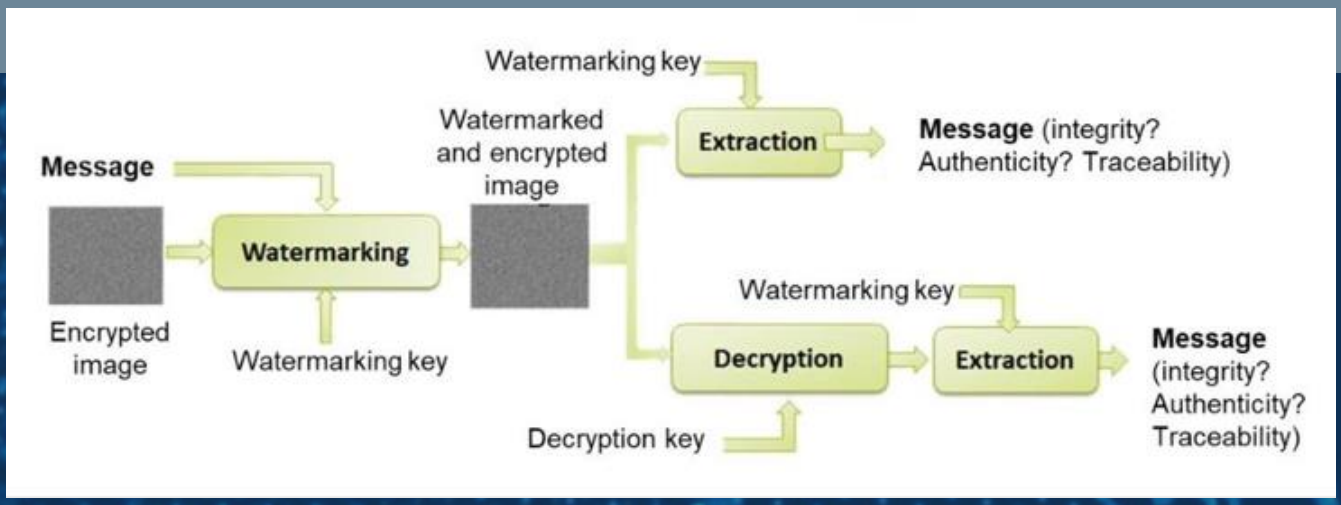
In line with the PAROMA-MED research project's objective to integrate advanced Privacy-by-Design solutions into its platform, a novel micro-service has been introduced, offering watermarking-based traceability services for encrypted and decrypted data to mitigate information leaks.

The primary goal is to deter illegal data rerouting and identify any compromised nodes or components that leak data. As shown in the following picture The PAROMA-MED context includes multiple high-risk locations for data leaks, including local health domain storages, the cloud domain, and centralized model elaborations. These areas are susceptible to unauthorized data breaches and require robust protection mechanisms.



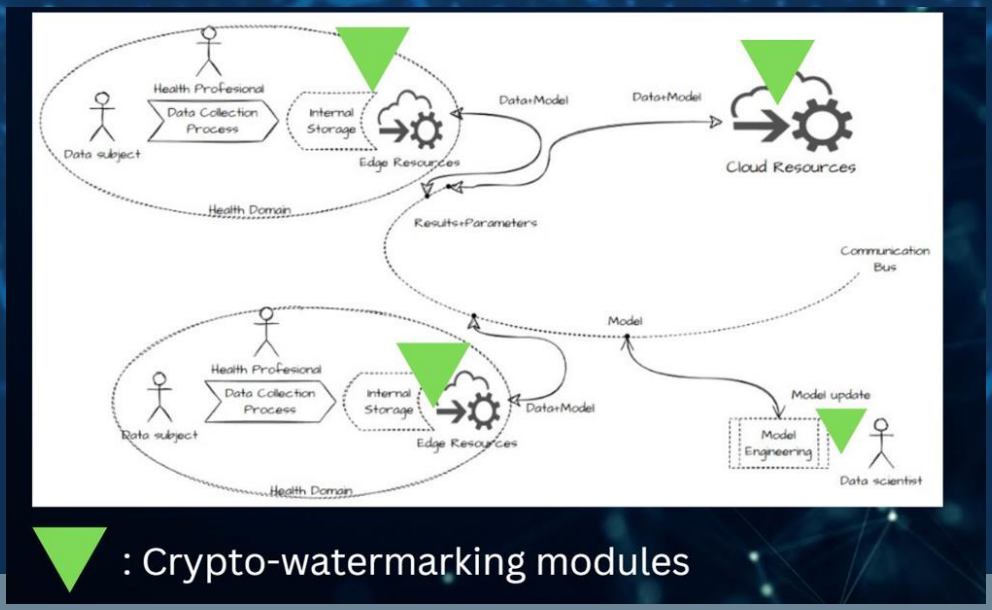
Crypto Watermarking

PAROMA-MED



Crypto-watermarking, a technique that combines watermarking (for a posteriori protection) with data encryption (for a priori protection), has been applied across all identified high-risk locations. This dual-layered security approach not only protects data ownership and integrity but also enables precise traceability, making it easier to identify and mitigate the source of any data leaks. The integration of these advanced watermarking solutions within the PAROMA-MED platform exemplifies the project's commitment to enhancing data security and privacy. By leveraging such techniques, PAROMA-MED aims to provide a secure environment for sensitive medical data, ultimately reducing the risk of data breaches and ensuring the integrity and confidentiality of patient information.

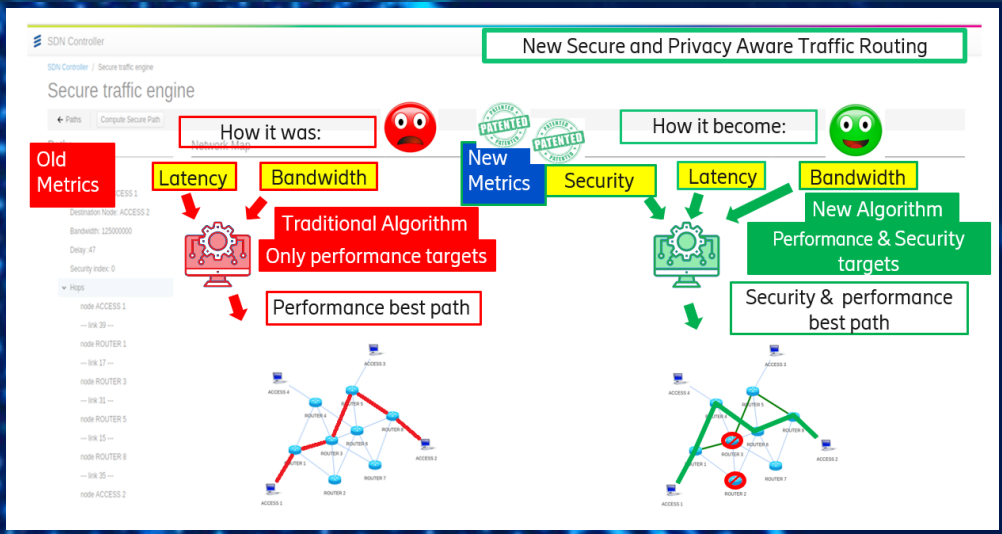
.



PAROMA-MED

Privacy Aware PCE

In the realm of 5G telecommunications, one fundamental concept that stands out is Network Slicing. This innovative method allows for the creation of multiple, discrete virtual networks on a single physical infrastructure, each tailored to meet specific requirements. The primary advantages of Network Slicing include isolation, optimization, and enhanced performance for different services and applications. By isolating network slices, each virtual network operates independently, ensuring that the performance of one slice does not impact the others. This results in optimized resource allocation, improved service quality, and the ability to meet diverse performance requirements for various applications ranging from enhanced mobile broadband to ultra-reliable low-latency communications.



CyberSecurity Metrics

Based on the NIST CVSS Vulnerabilities System Scores

REmediation level applied to the specific nodes

CVSS v3.0 Ratings	
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

$$P_{ij} = \frac{\alpha_{ij} * CVSS_i^{norm} / RE_{ij}}{\sum_{i=1,j=1}^{m,n} \alpha_{ij} * CVSS_i^{norm}}$$

$$SI_j = (1 - P_j) \times 100$$

NIST Information Technology Laboratory NVD NATIONAL VULNERABILITY DATABASE

Patent awarded

Network slices are created and maintained using sophisticated traffic routing algorithms that determine optimal paths based on network requirements and available resources. These algorithms belong to the family of Path Computation Engines (PCE). Among the most well-known and commonly used algorithms is Dijkstra's algorithm, which efficiently finds the shortest path in a network, thereby ensuring optimal routing of traffic.

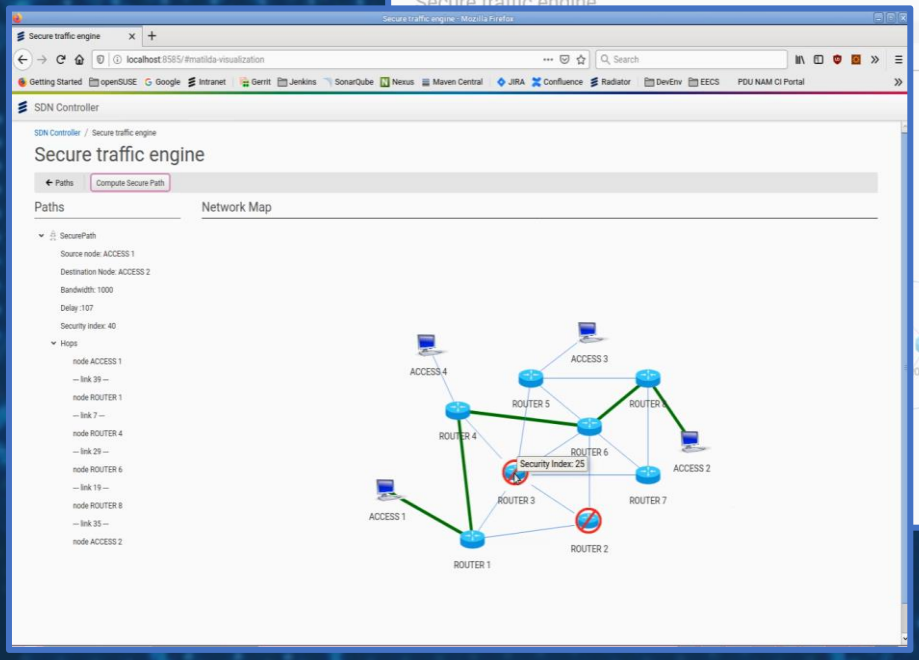
However, the current applications of PCE predominantly focus on optimizing latency and bandwidth. There is a notable lack of consideration for security and privacy criteria within these algorithms. This gap exists because of the absence of appropriately defined metrics and methodologies for assessing and scoring network resources with respect to security and privacy. As a result, existing PCE implementations fall short in providing comprehensive protection and confidentiality in network operations.

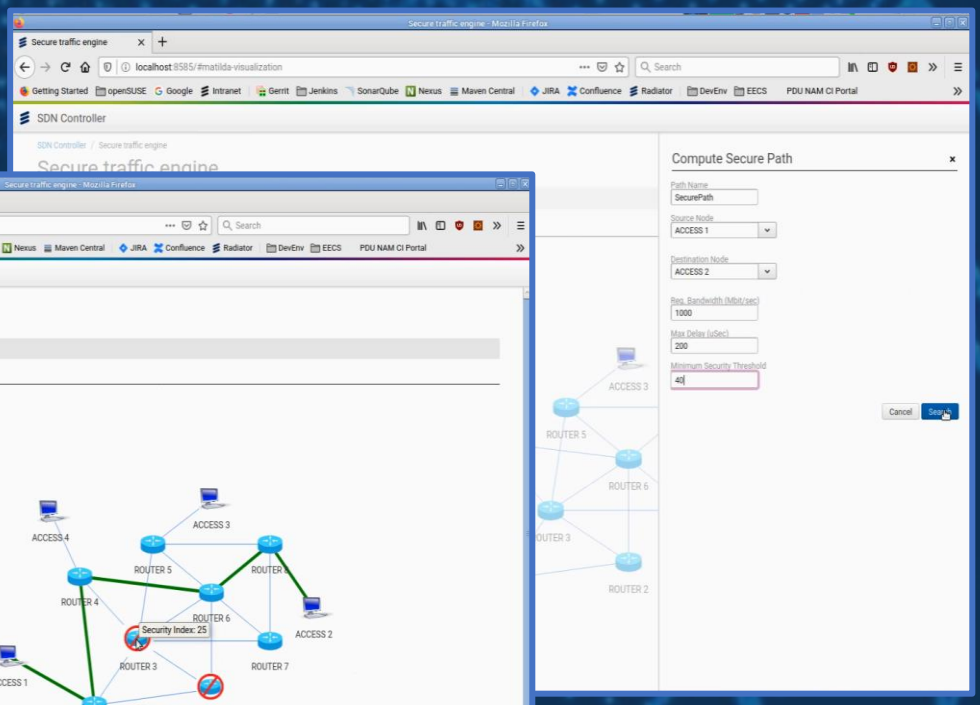
https://www.youtube.com/watch?v=zytrteZMEKg

Privacy-Aware PCE

PAROMA-MED

To address this significant gap, we conceived and published a new patent which has proposed the definition of advanced metrics for assessing and scoring network resources in terms of security and privacy. This innovative approach extends current PCE algorithms to make them privacy-aware and security-aware. By incorporating these advanced metrics, the new algorithms can better evaluate the security and privacy implications of different routing paths, ensuring that network slices are not only efficient but also secure.





The advantages of this approach include:

- Simplicity and Cost-Effectiveness: Automatic, low-cost retrieval and processing of CVSS data.
- Scalability and Reactivity: Real-time operations keep pace with network and cybersecurity changes.
- Fairness: Metrics are straightforward and do not require complex weight management, offering transparent physical interpretation.
- Compatibility: The proposed metrics align with standard PCE algorithms, ensuring seamless integration with existing systems.
- Vendor Homogeneity: Utilizing globally recognized CVSS data ensures consistent values across multi-domain networks, facilitating cooperation between different vendors.

PAROMA-MED

News

The consortium recently met in Athens!

Between 26th and 28th February 2024, the PAROMA-MED partners gathered in Athens, Greece!

The meeting was arranged by our project partner Ubitech, https://www.ubitech.eu

Consortium Meeting in Athens

The fifth project consortium meeting, after Heidelberg 23rd and 24th January 2023, Genoa 4th and 5th May 2023, Vienna 4th and 5th July 2023 and Paris 13rd to 15th November 2023 was held in Athens from 26th to 28th February 2024, just after the end of the first activity period of the EU-funded project "PAROMA-MED". After the first part ot the project with a main focus about the architectural and specification phases, the partners focus has progressively moved to implementation and validation effort. On 26th February 2024, all partners met in the beautiful meeting locations arranged by Ubitech in the wonderful city of Athens, Greece, to discuss activity updates and jointly examine the best actions and decisions needed to ensure the project's ongoing success, addressing both technical, strategical and management elements.

Collaborations with other Projects

encrypt

TRANSCEND

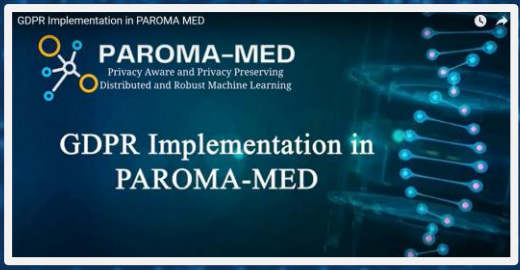
DataVaults

TRUMPET

PAROMA-MED

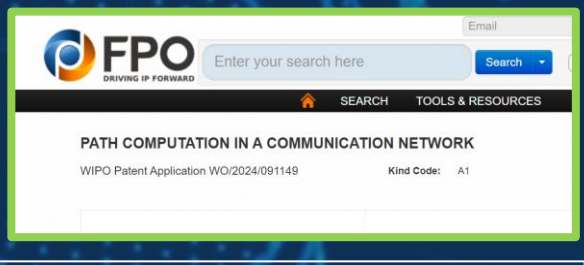
Breaking news

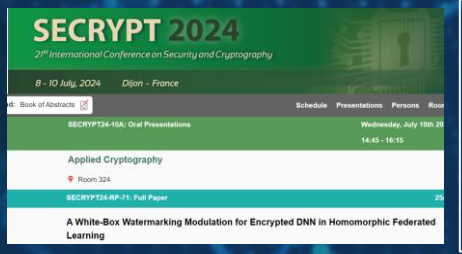
The PAROMA-MED Consortium is finalizing the contributions of many important Chapters of the Springer Editorial “Beyond Health 4.0, connecting the dots” – Publication foreseen within the end of 2024!



A new important video explaining the importance of GDPR in the PAROMA-MED Project and the concept of functional GDPR has bee uploaded to the PAROMA-MED YouTube Channel and is now available for you at the following link:
https://www.youtube.com/watch?v=-NeF37zkhOU

We just published a groundbreaking patent developed during the PAROMA-MED project. Our enhanced PCE revolutionizes #NetworkSlices creation with a cutting-edge privacy & security network resource scoring system. 👉
:https://www.freepatentsonline.com/WO2024091149A1.html





Participation to the SECRYPT Conference on Security and Cryptography, with the Mohammed Lansari Speech about "White-Box hashtag#Watermarking Modulation for Encrypted DNN in Homomorphic hashtag#Federated Learning“
https://www.insticc.org/node/TechnicalProgram/SECRYPT/2024/presentationDetails/127643

CrossTalk arranged for the 22 October in Brussel by TRUMPET (organizer), HARPOCRATES, AI4EOSC, ENCRYPT, WARIFA, PAROMA-MED, ONCOVALUE, KATY etc.
Invited authorities: POs of the projects, ENISA, ECSO, EUROPEAN DATA PROTECTION SUPERVISOR

Dissemination

PAROMA-MED

PAROMA-MED at 2024 EuCNC & 6G Summit

From 3rd June to 6th June EuCNC & 6G Summit was held in the diamond city of Europe – The Antwerp. This conference focuses on all aspects of telecommunications ranging from 5G deployment and mobile IoT to 6G exploration and future communications systems and networks, including experimentation and testbeds, applications and services. For the project Paroma- Med it was a good opportunity to exchange and share the ongoing work with AI/ Federated learning enthusiasts within research projects from EU R&I programmes. The event brings more than 900 delegates from more than 40 countries all over the world, to present and discuss the latest results hence for the project Paroma-Med it was event to explore synergies and learn from its peers.

From the project, the dissemination and communication leader Pooja Mohnani, project Manager at Eurescom was present at the event and engaged with questions from the audience

PAROMA-MED

Deliverables

- WP1
  - D1.1 “Requirements and Use Case Definition” - Report that provides the functional and not functional requirements for the realization of the project concepts, and also the details of the Use Cases (Task 1.1).
  - D1.2 “Concept and Evaluation Framework - first version” - Report that provides the first version of the platform architecture and the related evaluation methodology.
  - D1.3 “Concept and Evaluation Framework - final version” - Report that details the updated version of the platform architecture as refined in the progress of the technical work performed in the other WPs.
- WP2
  - D2.1 “Access and Privacy Control Architecture and Models” - Report that presents the models and the resulting architecture for access and privacy control within the PAROMA architecture.
  - D2.2 “Data Platform Architecture and Models” - Report that documents the architecture for the privacy-preserving data storage and logging as well as for the data-movement in a federated environment, as part of the PAROMA architecture.
  - D2.3 “Network and Interconnect Platform - ver. 1” - Reports the network and interconnecting platform focusing about the privacy-aware Network Slices conceived, to assure an inter-connectivity privacy level compliant with the project requirements.
  - D2.4 “Application Platform v.1.0” - First version of the application platform, comprising the prototypes of the produced software artefacts and of an accompanying document highlighting the development and deployment details.
  - D2.6 “Integrated Platform v.1.0” - First version of the integrated platform, constituting a direct outcome of T2.5, integrating the first version of the software artefacts produced in the context of WP2 accompanied by a document highlighting the development and deployment details of the platform..
- WP3
  - D3.1 “Security and Data Privacy Services vers. 1” - Report that collects and presents all the security and data privacy services defined and developed in Tasks T3.1 and T3.2. This document reports on the first iteration of the components defined and developed.
  - D3.2 “Security and Privacy Awareness - ver. 1” - Report that collects and presents all the security and privacy awareness concepts and models defined and developed in Task T3.3 as well as a first prototype GUI for situational awareness.

Deliverables

PAROMA-MED

❑ WP5

- D5.1 “Roadmap for communication, dissemination, standardization activities” - Report that provides an overview of the strategy and the main actions implemented for communication, dissemination, standardization, clustering. It describes relevant targets for communication/dissemination, together with the appropriate means to reach them.
- D5.2 “Setup of communication and dissemination media” - Report about the first communication and dissemination activities, such as the public website and leaflet; it includes the project vision, objectives, activities, expected outcomes and benefits, and points of contact. Project accounts on selected social media.
- D5.3 “IPR management” - This report provides the list of background knowledge inside the Consortium, identifying specific IPR, and reporting on internal agreements for sharing knowledge and software tools.
- D5.4 “1st Report and updated plan for communication, clustering, dissemination” - Deliverables that listw the communication, clustering, standardization, and dissemination actions implemented every year by the Project.
- D5.5 “1st Exploitation, business plan, and IPR management” - Report providing information about exploitation and business planning elaborated in Task 5.3.

❑ WP6

- D6.1 “Data management plan” - Defines the rules for the project participants to ensure data is findable, accessible, interoperable and re-usable, and governed by the applicable data security and ethics standards.
- D6.3 “Ethics requirements” - Report on all measures that will be implemented in the project to comply with ethics requirements: REQ Humans, REQ Personal Data, REQ Artificial Intelligence

❑ WP7

- D7.1 “Project management handbook” - This report includes description of all necessary project management procedures (reporting, approvals, etc.) to be performed by consortium members and lay down the needed project management structure and corresponding project bodies.

PAROMA-MED

www.paroma-project.eu

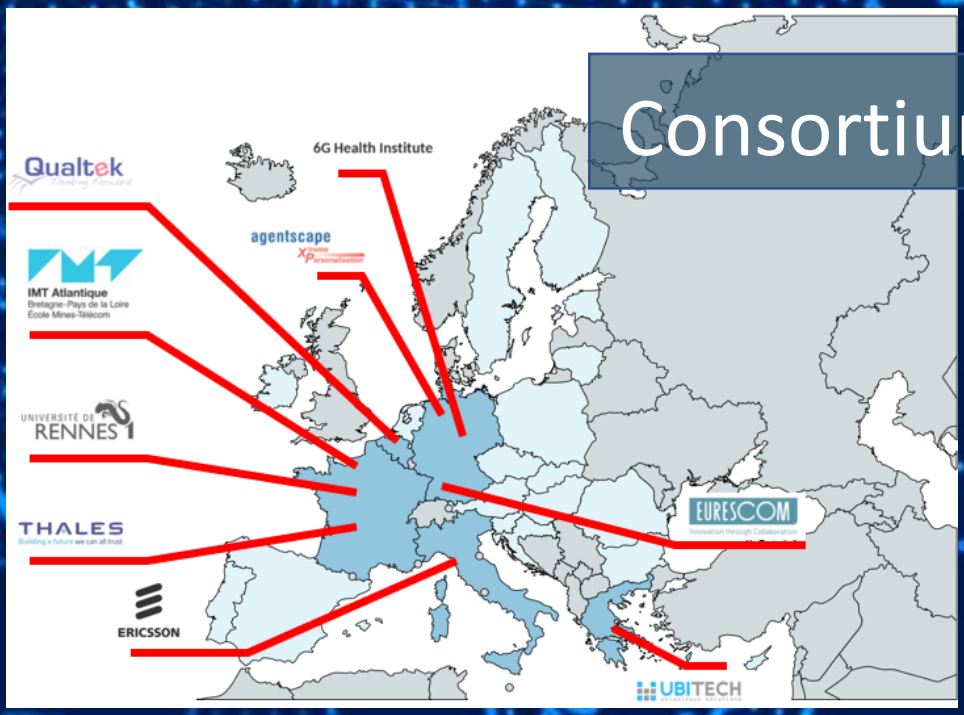
Contacts

Project Coordinator
Dr. Alessandro Bassi
bassi@eurescom.eu

Technical Coordinator
Ing. Konstantinos Koutsopoulos
k.koutsopoulos@qualtek.eu

Project Acronym	PAROMA-MED
Project ID	101070222
Starting Date	1 June 2022
Ending Date	31 May 2025
Call	HORIZON-CL3-2021-CS-01
Topic	HORIZON-CL3-2021-CS-01-04
Total Cost	4 280 497.50
EU Contribution	4 280 497.50
Funding Scheme	RIA

Consortium



Socials

contact@paroma-med.eu
https://paroma-med.eu/
@ParomaMed
company/paroma-med-project/
@paroma-medproject9497

Scan to visit PAROMA-MED website

Issue 3 – Jul 2024

This project has received funding from the European Union Horizon 2020 research and innovation programme under grant agreement No. 101070222