



PAROMA-MED

Privacy Aware and Privacy Preserving
Distributed and Robust Machine Learning

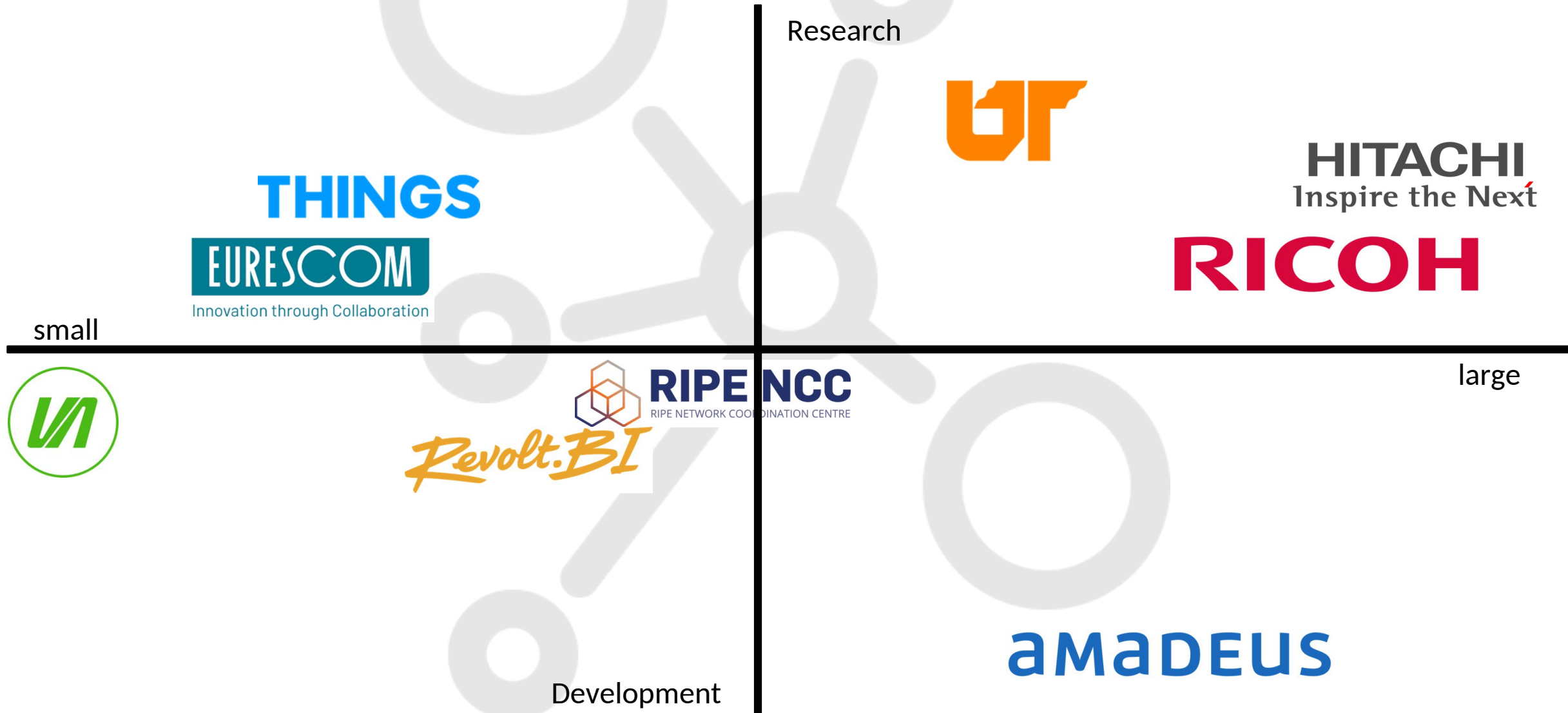
A privacy preserving Health Data Space approach for federated machine learning

Alessandro Bassi, Eurescom
PAROMA-MED project coordinator

Acknowledgement and disclaimer

- This project is funded by the European Union under Grant Agreement 101070222, project PAROMA-MED.
- Views and opinions expressed, are those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission (granting authority). Neither the European Union nor the granting authority can be held responsible for them.

Who am I? Why am I here?



The Problem: Fragmented, sensitive, and underutilized health data

- Despite the **exponential growth of medical data**, health systems across Europe struggle to leverage it due to fragmentation, privacy concerns, and lack of interoperable infrastructure.
- Sensitive patient data is siloed across institutions and borders, making it difficult to extract actionable insights, deliver preventive care, or respond to regional health crises in a coordinated manner.

The opportunity: Federated AI for Secure Cross-Border Collaboration

- Federated learning and distributed AI technologies present a powerful opportunity to transform healthcare by enabling insights from decentralized data—without compromising privacy or data sovereignty.
- Europe face unique demographic, economic, and health system pressures - federated AI enables collaborative intelligence while respecting national regulations and institutional trust boundaries.

Our Vision: A Trusted, Privacy-aware digital ecosystem for health

- PAROMA-MED envisions a federated digital health environment where AI-driven services can be deployed securely across countries and institutions, while maintaining rigorous privacy protections.
- This ecosystem will support the secure use of sensitive health data for personalized care, early warning systems, and policy support—empowering both clinicians and citizens.

Our Mission: Build and Validate a Privacy-by-Design AI Framework

- The mission of PAROMA-MED is to develop and demonstrate a privacy-aware, interoperable, and robust digital platform that enables secure health data use across borders.
- We aim to integrate Zero Trust architectures, privacy-preserving machine learning, federated identity management, and real-time data governance into a unified, modular framework tested in real-world conditions.

Our Innovation: Privacy + Federation + Resilience by design

- We have a combination of cutting-edge innovations:
 - federated learning architectures that eliminate data centralization;
 - zero-trust security protocols that ensure dynamic verification;
 - privacy-enhancing technologies (PETs) that safeguard patient confidentiality;
 - and zero-touch orchestration tools that simplify deployment and compliance across jurisdictions.

What we achieved: Technology, Governance, Validation

- We go beyond theory: we developed a complete reference architecture, implementation toolkit, and tested services that integrate AI with secure data sharing practices.
- Our outputs include privacy-preserving algorithms, decentralized access control, policy-compliant data flows, and practical deployment in a healthcare pilot.

Our Team



ERICSSON

agentscape



IMT Atlantique

Bretagne-Pays de la Loire
École Mines-Télécom



Innovation through Collaboration



**Université
de Rennes**

Healthcare: Opportunities and Challenges

Healthcare presents enormous opportunities for value creation across society

BUT

it is an area where data privacy and protection are paramount due to the sensitivity of personal health information.

the European General Data Protection Regulation (GDPR) establishes stringent guidelines to safeguard individuals' fundamental rights by dictating how personal data should be handled.

6 Major Trends in the Health Domain

Patient data are typically stored in Hospital Information Systems (HIS) which do not allow for easy data distribution

For a considerable time care models have been changing globally from centralized, hospital-oriented systems to distributed patient-centric care systems

As a consequence medical data bases have grown massively in number

Ongoing transition from **platform-based systems** (HIS) towards **protocol-based systems** (FHIR, EHDS) in the health domain

New enabling technologies such as 5G, B5G/6G and 5G RedCap

Transition from Health 3.0 towards Health 4.0

(what is GDPR?)

- The **General Data Protection Regulation (GDPR)** is a comprehensive data protection law enacted by the European Union (EU). It regulates how organizations collect, use, store, and protect personal data of individuals within the EU.
- **Broad Applicability:** It applies not only to companies operating within the EU but also to those outside the EU if they process data of EU residents.
- **Personal Data Definition:** It includes any information that can identify an individual, such as names, email addresses, IP addresses, location data, etc.
- **Individual Rights:** GDPR grants individuals several rights over their data, including: Right to Access, Right to Rectification, Right to be Forgotten, Right to Data Portability, Right to Object.
- **Consent:** Organizations must obtain explicit and informed consent.
- **Accountability and Transparency:** Organizations must demonstrate compliance through detailed documentation, policies, and procedures.
- **Data Breach Notifications:** Organizations must notify authorities and affected individuals of data breaches within 72 hours.

Data Ecosystems with 6G

- **New capabilities to exploit**

- Terabit-per-second data rates and ultra-low latency
- Enhanced automation, flexible deployments, and end-to-end slicing techniques.



- **Expected impact**

- New application in high-capacity sectors: healthcare, augmented reality, IoT.
- Secure, private bandwidth for critical systems like Electronic Health Records (EHR).



- **Proposed innovations**

- Functional GDPR Approach
 - Continuous transparency and automated privacy validation.
- Moving beyond accountability to proactive data flow control.



What is PAROMA-MED?

The PAROMA-MED EU project aims

- to develop novel technologies, tools, services and architectures
- for patients, health professionals, data scientists and health domain businesses so that
- they will be able to interact in the context of data and ML federations,
- with complete respect to data owners' right
- Without penalties of performance or functionalities.

Stakeholder's roles and needs in data utilisation

Data Subject

- User-centric tools: push notifications, wallet apps, assisted consent management.
- Empowerment through transparency and control over data rights.
- Simplified interfaces for informed decisions and data monitoring.

Health Experts

- Empowering physicians with control over metadata creation.
- Metadata as assets: linked to ownership, consent, and traceability.
- Enhanced insights via ML-based processing

Data Scientist

- Access to rich, high-quality data using FAIR principles.
- GDPR-compliant workflows with continuous consent enforcement.
- AI models treated as data assets with a managed lifecycle.

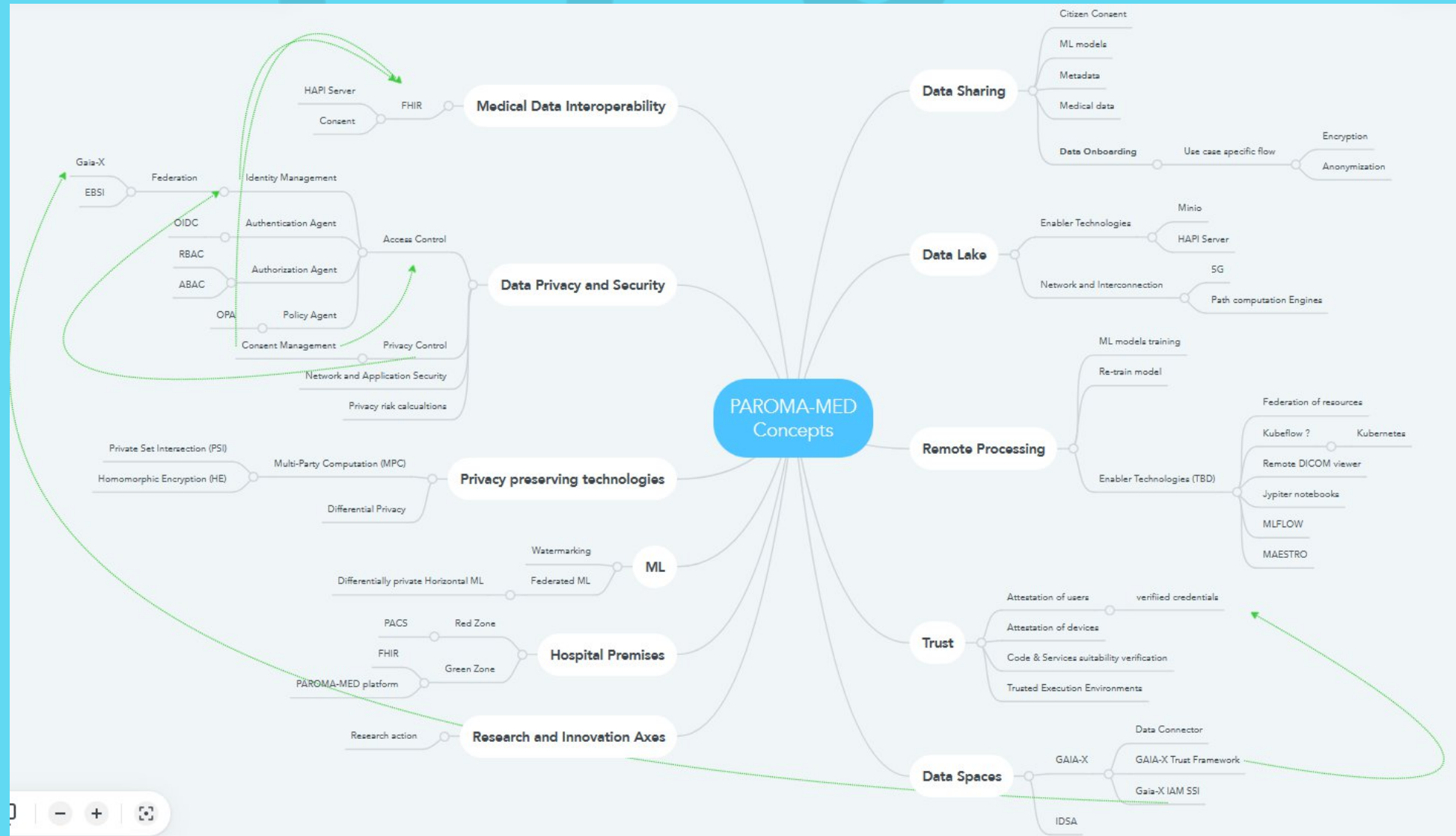
Businesses and Health Organizations

- Edge-based Horizontal Federated Learning to ensure data privacy.
- Secure local processing with data shared only among verified modules.
- Balancing data monetization with privacy compliance and accountability.

PAROMA-MED and Data Spaces Ready Approach

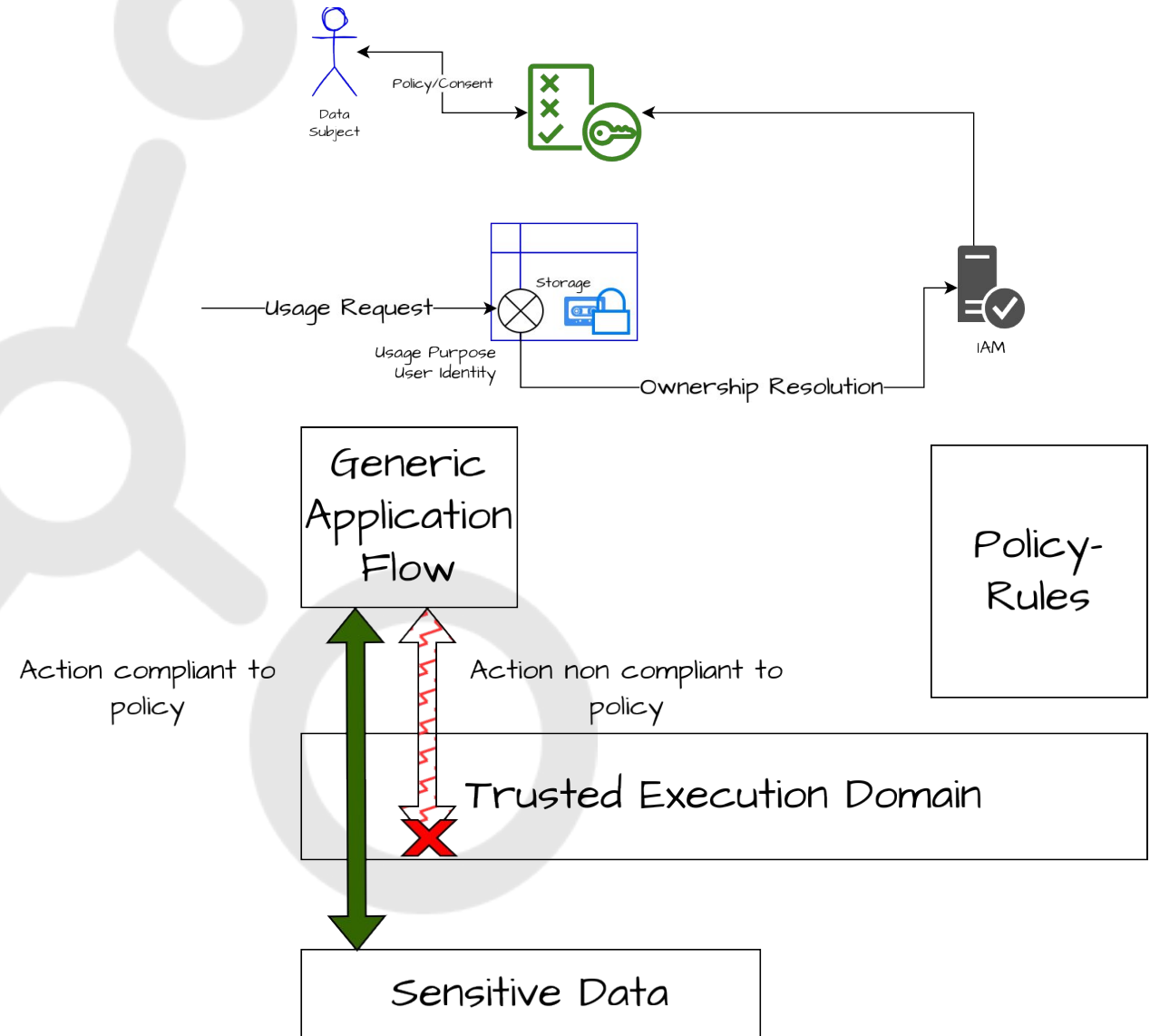
- Take advantage of Data Spaces features:
 - Enable data sharing while maintaining sovereignty principles.
 - Address healthcare-specific challenges like GDPR variations and market fragmentation.
- Apply as core principle:
 - Eliminate actual private data exchange while enabling in-place data processing.
- With overall goal:
 - Support scalable, privacy-respecting Healthcare Data Spaces.
- Ensure data utilization aligns with user-defined consent options.

Mindmaps of Concepts



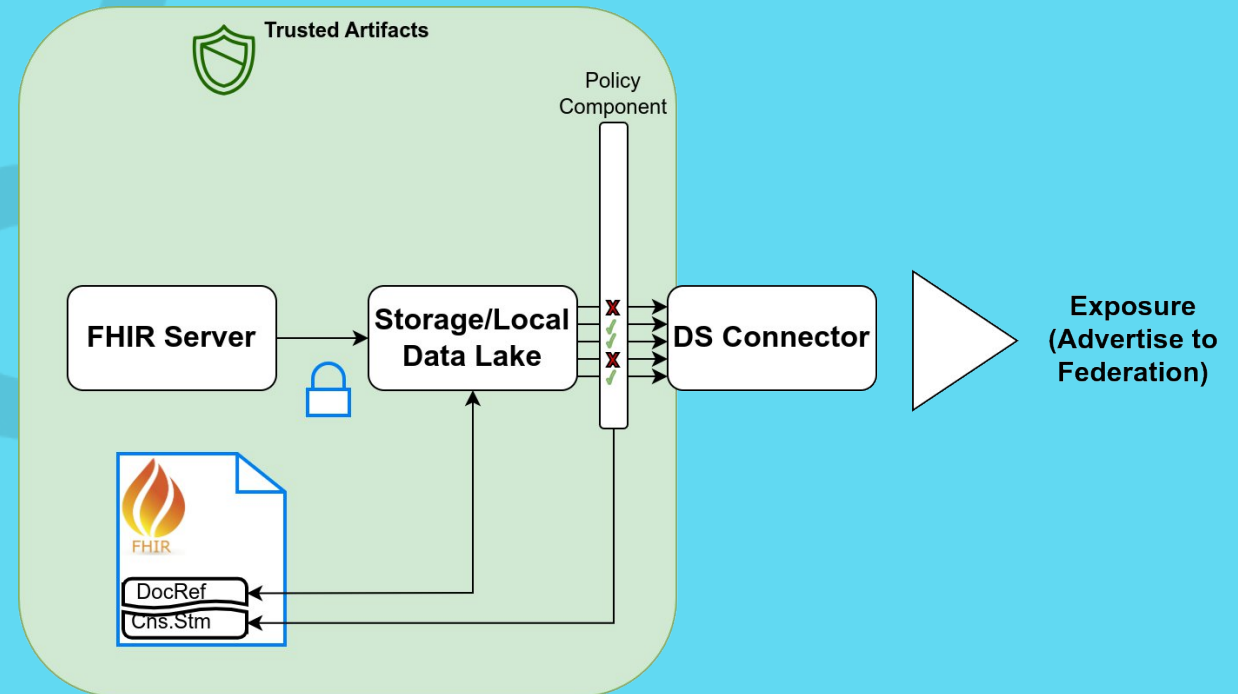
Data Protection and Consent Management

- Dynamic Consent Management:
 - Notifications for missing consent via wallet or web dashboard apps.
 - Consent statements govern data use, enforced by a Protection Layer.
- Protection Layer Roles:
 - Validate adherence to consent policies.
 - Block non-compliant actions dynamically.
 - Enable updates to consent policies as needed.



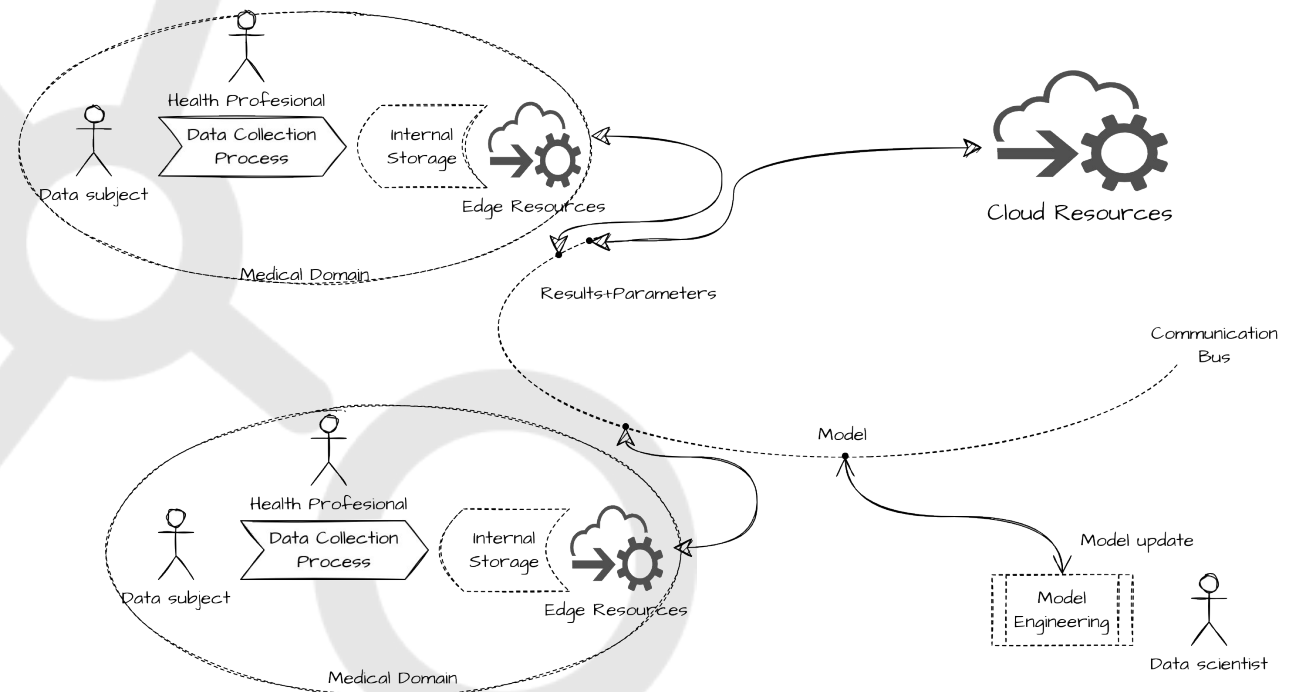
Data Exposure Approach

- Fast Healthcare Interoperability Resources (FHIR) server combined with secure object storage.
- Constraints from policies indicated by the individual consents are applied and the result updates are pushed through the Data Space Connector



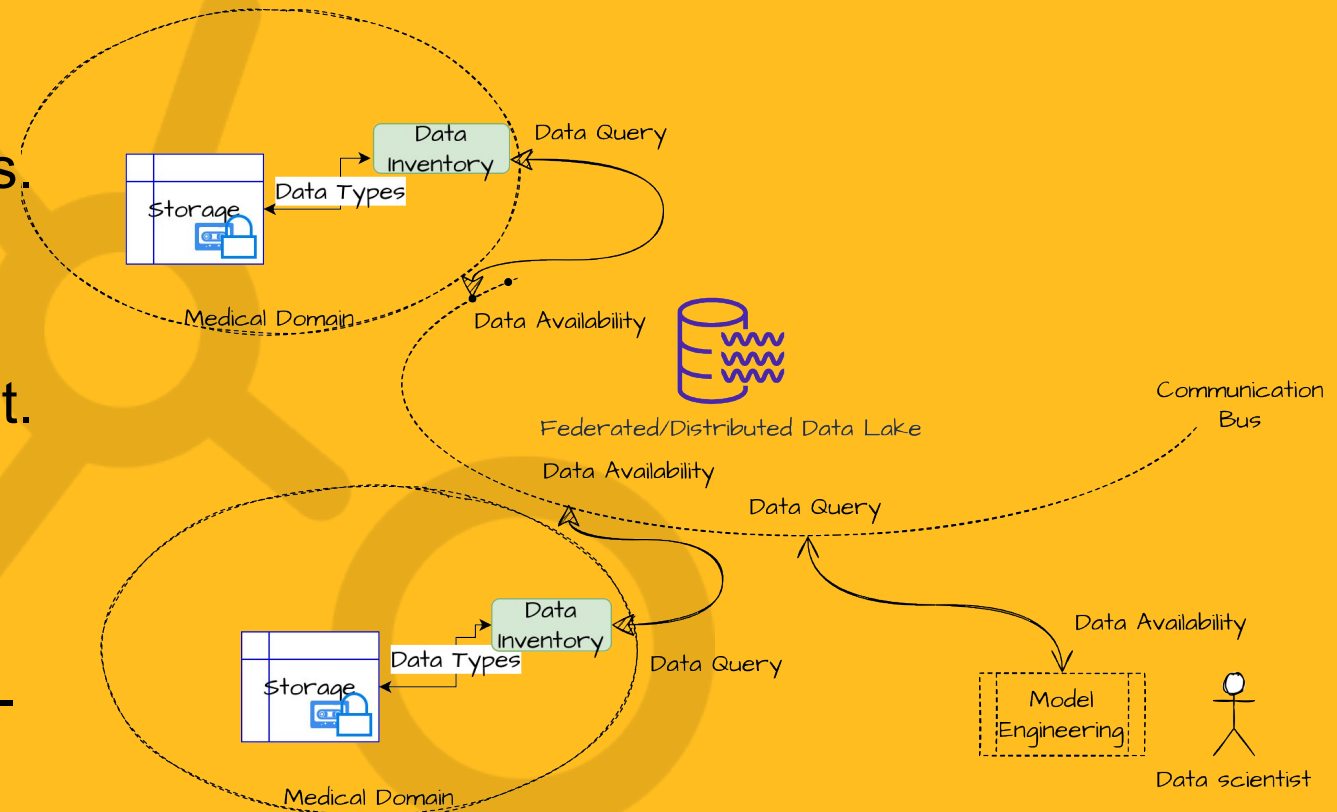
Data Federation and Inventory

- Data Inventory Layer:
 - Organizes data types in secure storage.
 - Publishes data for discovery in Data Spaces via connectors.
 - Updates performed in batches to preserve privacy.
- Federation Benefits:
 - Enables data discovery without direct transfer.
 - Streamlines availability checks for data scientists.



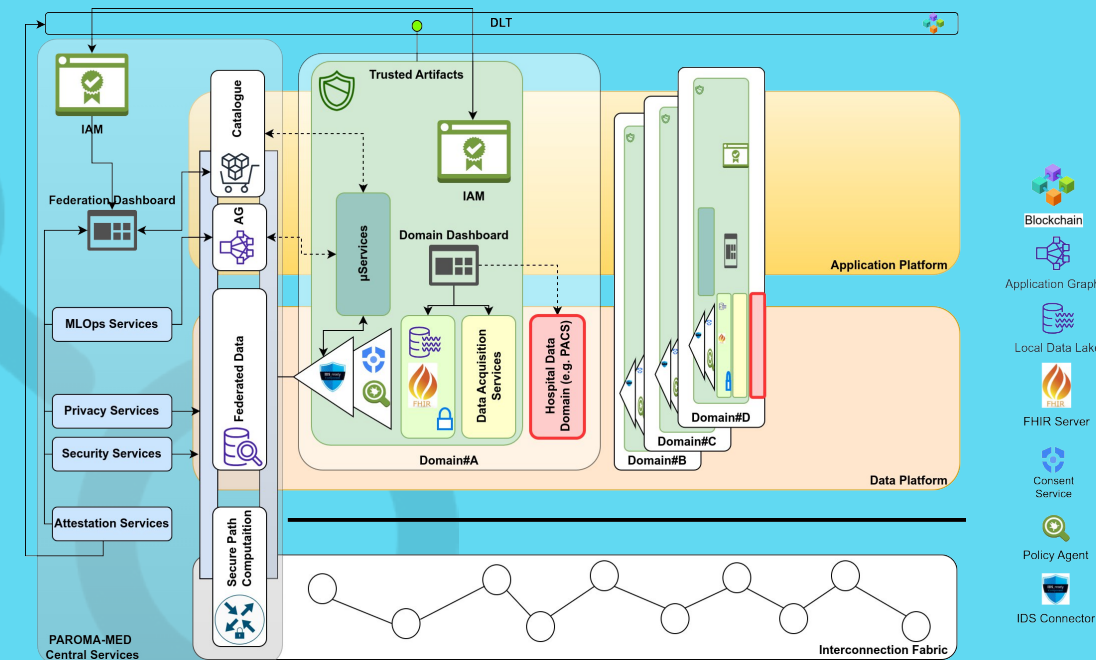
Enabling Federated Learning

- Federated Query Process:
 - Queries resolve across domains while adhering to privacy policies.
- Data categorized into:
 - Directly usable data.
 - Data requiring additional consent.
 - Unknown relevance/quantity data.
- AI Model Training:
 - Data processed in isolated, time-limited environments.

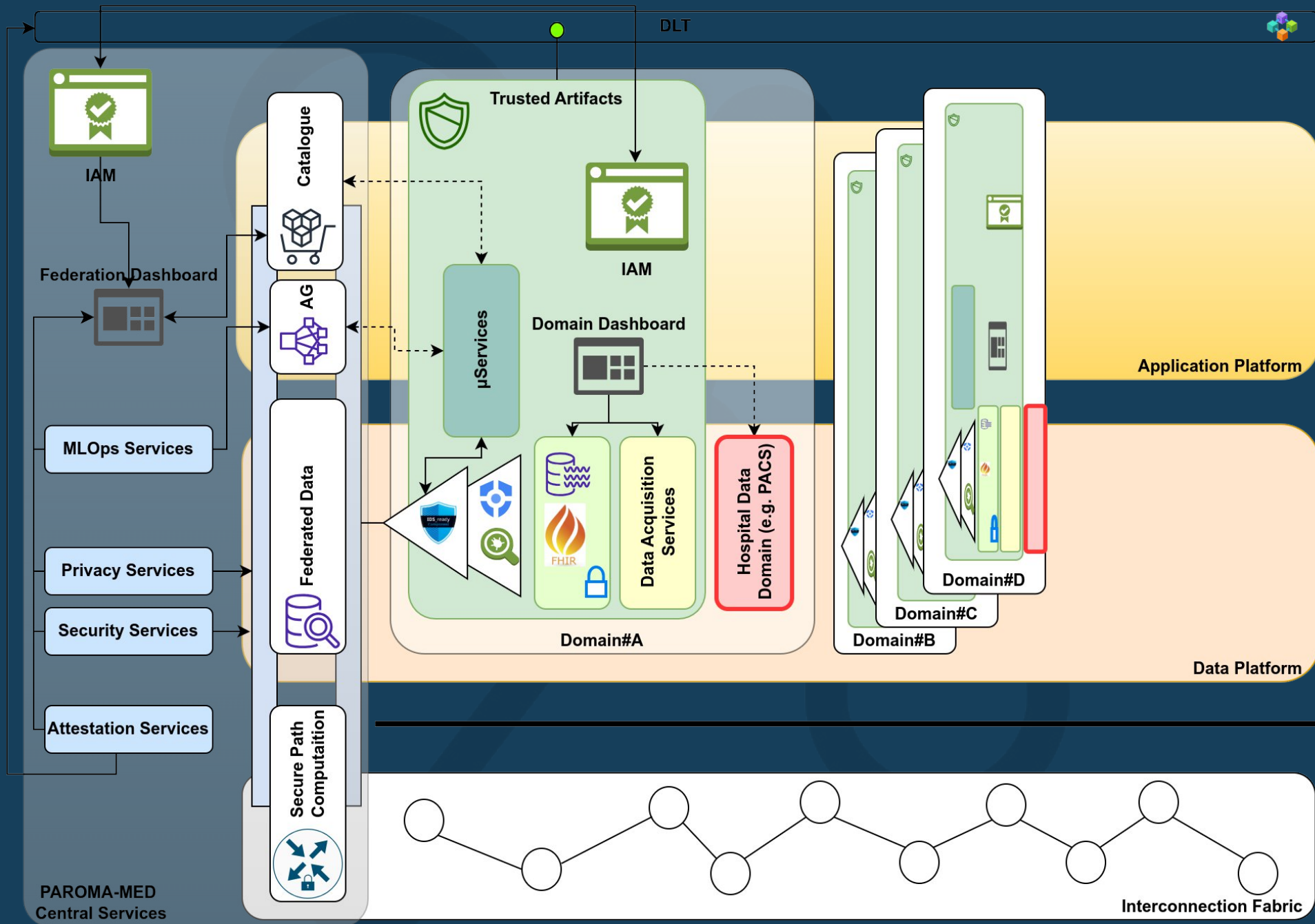


PAROMA-MED Architecture

- Hybrid Cloud Design:
 - Combines centralized and decentralized components for domain sovereignty and transparency.
 - Supports compliance with current and evolving legislation.
- Layered Structure:
 - Interconnection Layer: Secure Path Computation for controlled data flow.
 - Data Layer: Federation and ergonomic tools for sovereign data management.
 - Application Layer: Simplified deployment, operation, and monitoring with privacy preservation at its core.



PAROMA-MED architecture

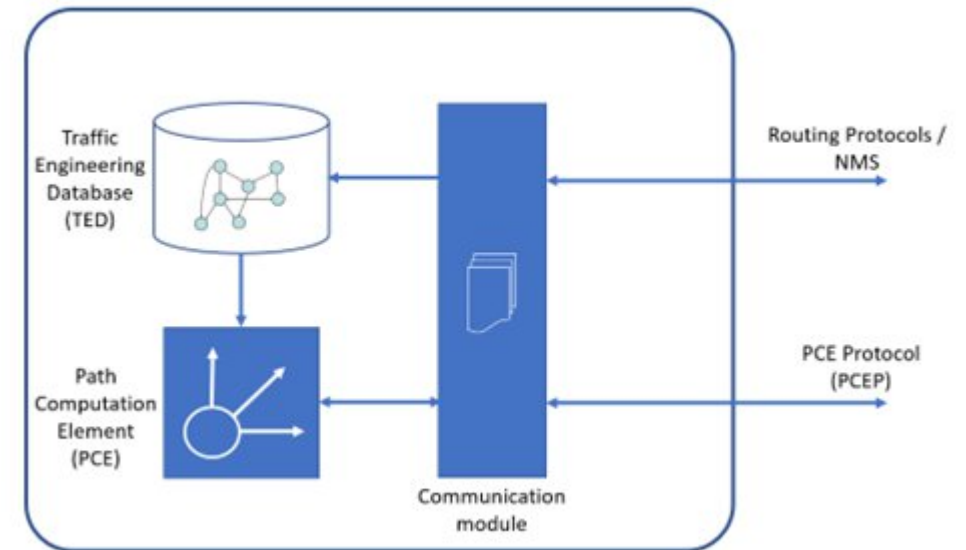


Interconnection Fabric

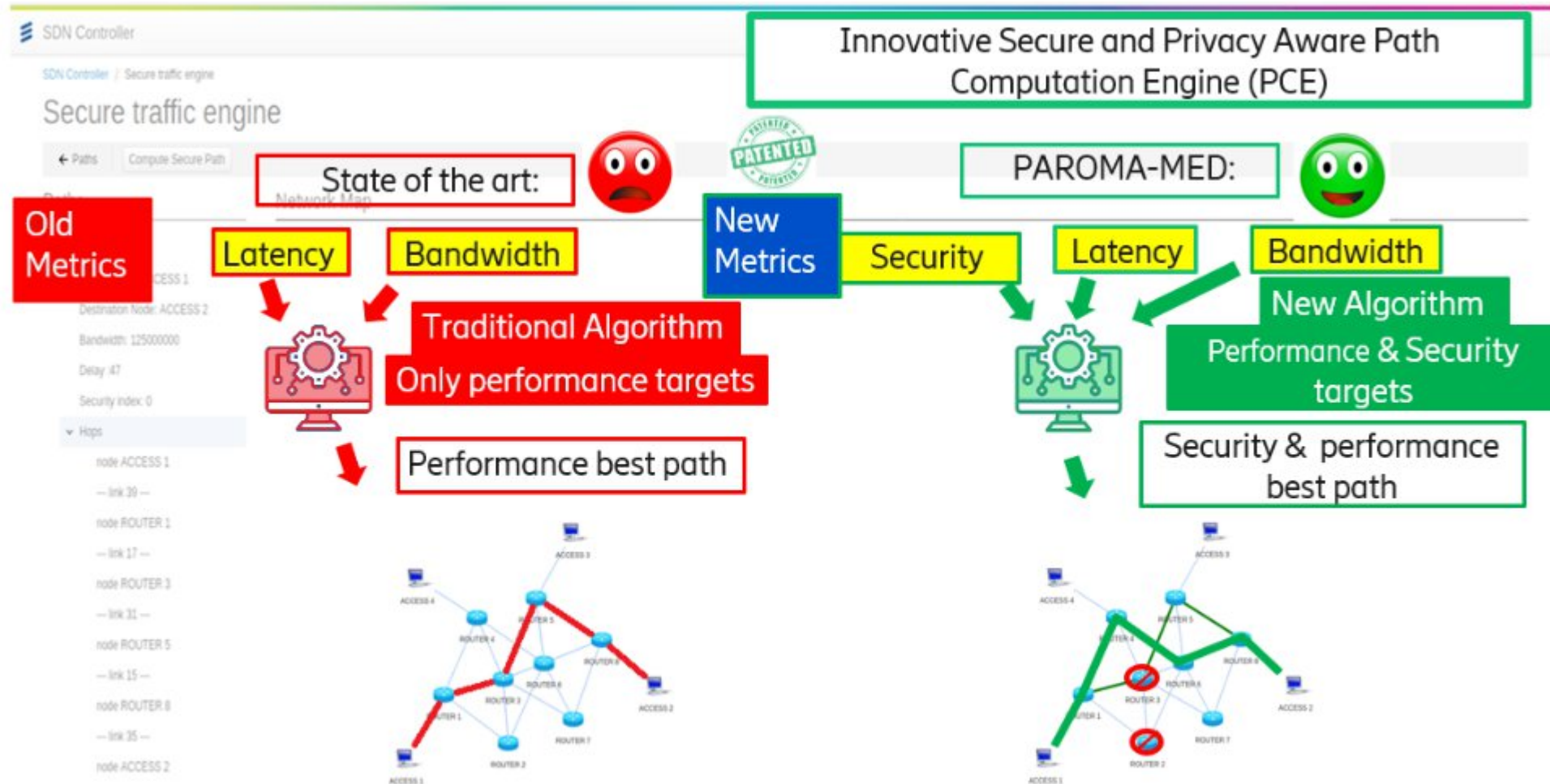
- This underlying infrastructure is pivotal in ensuring robust interconnectivity among remote sites while strengthening the privacy levels assured by the upper layers.
- With the multiple Clinical Environments connected with the Central Federated Processing Environment, the connectivity plays a critical role, linking various hospitals involved in model development with a centralized research centre responsible for model aggregation and the distribution of results across multiple iterations.
- This connectivity embodies a sophisticated set of protocols and systems designed to ensure the highest possible degree of data protection and security.
- Automated, scalable, and dynamic management of any changes across this network layer is essential to provide seamless, reliable service to higher-level applications.
- Such complexity is deftly managed through advanced operational support systems (OSS) and intricate algorithms, collectively referred to as "Secure Path Computation".

PAROMA-MED Network and Interconnect Platform

- Path Computation Element (PCE):
 - A specialized network entity for:
 - Dynamic path computations optimizing network performance.
 - Gathering data from Network Management Systems (NMS) for enhanced routing.
- Key Features:
 - Supports multi-layer networks with Quality-of-Service (QoS) guarantees.
 - Offloads computational tasks from network nodes for efficient Traffic Engineering (TE).
 - Integrates multi-dimensional optimization:
 - Security, privacy, performance, and traffic volume constraints.
- Innovations:
 - Patent-protected framework: “Path Computation in a Communication Network.”
 - Advances beyond traditional bandwidth/latency paradigms.
 - Tailors network slices for secure, private, and trustworthy 5G/6G communications.



Secure Networking



PAROMA-MED approach

- The basic innovative idea introduced in the PAROMA-MED context is to use, for the probabilistic and proactive evaluation of the node vulnerability (defined as probability to fall victim of an attack), a formulation capable of taking into account:
 - the specific weight of the vulnerability itself (repeated for all the relevant vulnerabilities for that kind of node) combined with
 - the level of remediation actions (a.k.a. hardening) performed on the node itself to reinforce it against its attacks.
- These two factors (summarized for all the node relevant vulnerabilities) are clearly the principal and most effective values to proactively evaluate the node vulnerability.
- Moreover, the numerical score reflecting the single vulnerability severity (CVSS, Common Vulnerabilities Scoring System) is freely provided and continuously update, by a premier United States national government agency, NIST, that has become a world reference for these aspects.
- The security metrics based on a simple and straightforward elaboration of the CVSS value (automatically retrieved using Web Services technologies), properly combined with the node Remediation Actions, demonstrate to be an effective, simple and practical choice with multi-fold advantages.

CVSS based algorithm advantages

Final Objective: provide a centralized Network Management System able to automatically manage the Path Computation Engine, its evolutions, and the related run-time tables (CVSS values and Remediation Actions) and to modify in real time the optimal Security-aware best path at any new vulnerability or new Remediation Action

The advantages are several:

- 1)Simplicity. The described elaboration is very light and allow a very convenient implementation in terms of: Costs, Reactivity, Latency, Scalability
- 2)Fairness. The proposed metrics, as hereinafter illustrated, are self-comprehensive, with no need to be composed to a linear combination and no need to run-time manage the relative weighs.
- 3)Based on the real crucial factors: Vulnerabilities and Remediations.
- 4)Existing PCE algorithm compatible. The implemented metrics, as hereinafter described, are effectively mapped to the network links and the physical interpretation allows an additive treatment fully compatible with the PCE standard algorithms.
- 5)Multi-vendors compatibility.

Secure Networking

Based on the NIST CVSS Vulnerabilities System Scores

CVSS v3.0 Ratings

Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0



REmediation level applied to the specific nodes

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

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



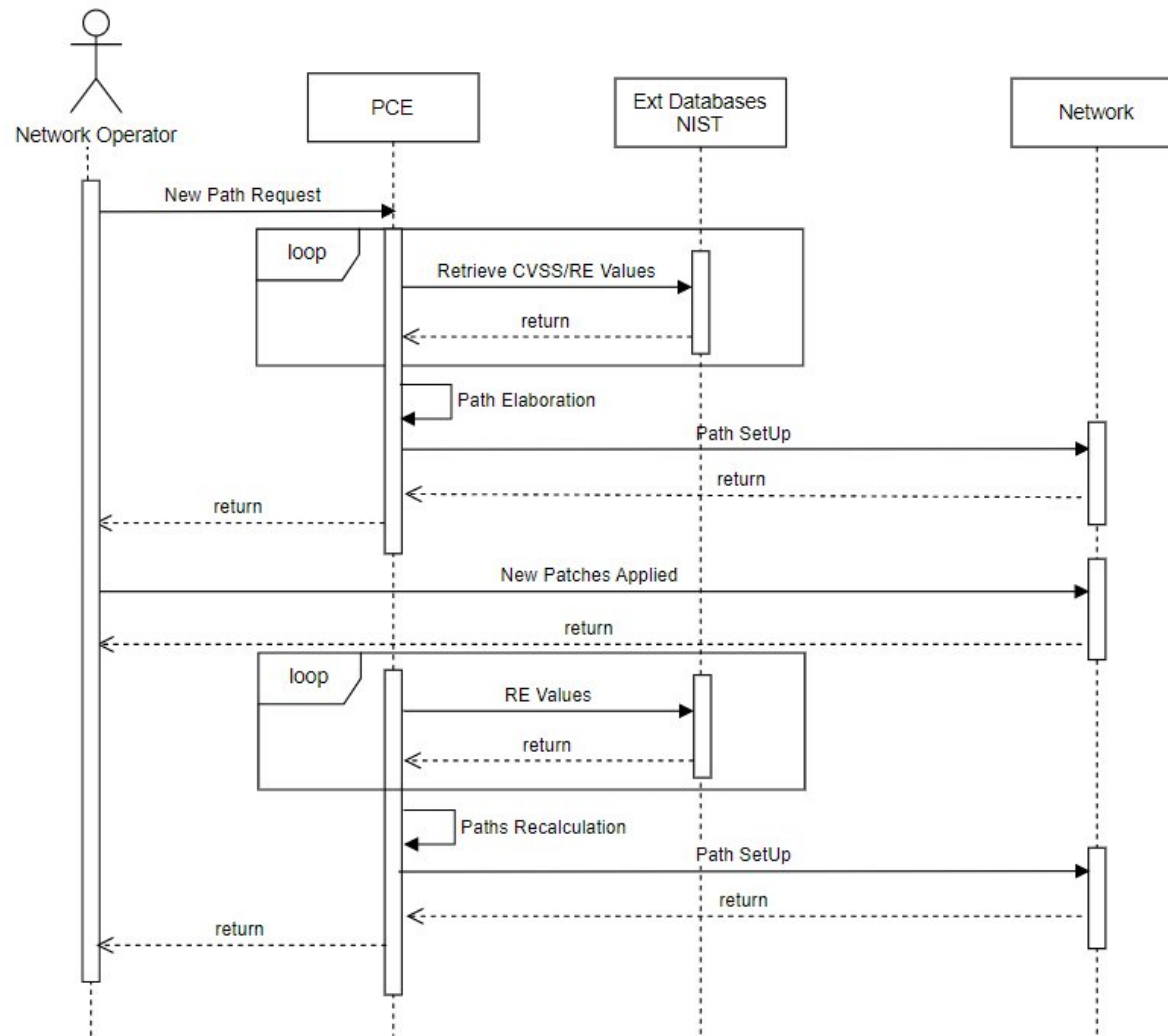
Patent awarded

Formula explanation

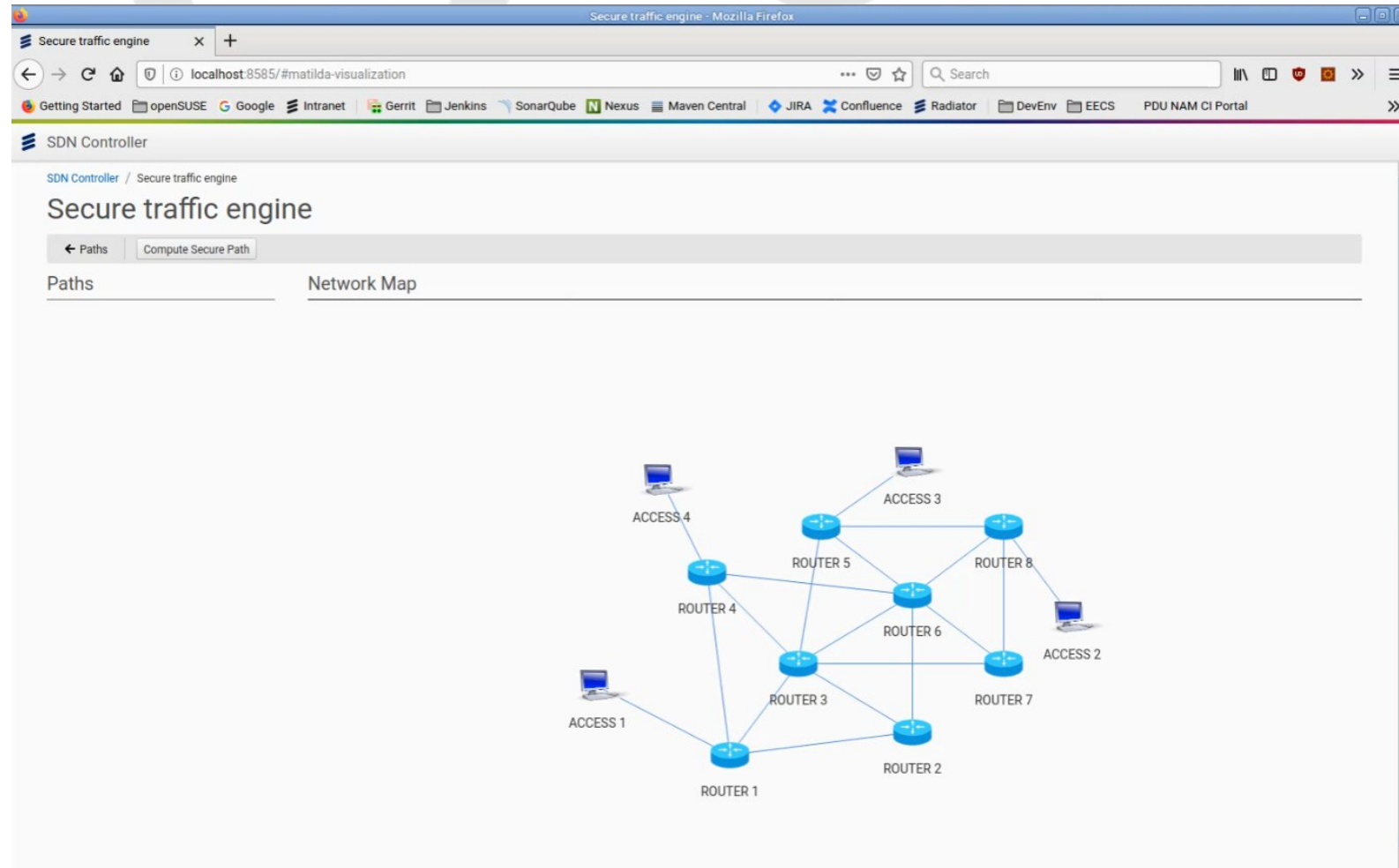
$$P_i = \frac{\alpha_i * CVSS_i^{norm} / RE_i}{\sum_{i=1}^m \alpha_i * CVSS_i^{norm} / RE_i}$$

- $CVSS_i$ is the CVSS score of the i-th vulnerability,
- norm is its normalized valued [divided by ten];
- RE_i is the remediation level
- α_i is an optional tuning parameter.
- m indicates the set of all the possible attacks
- P_i = probability that the attack was of type i.

Sequence diagram



Secure Traffic Engine main view



Compute Secure Path

The Compute Secure Path Input form opens on the right part of the GUI, The operator is required to fill the form fields with the following information:

- Path Name: a proper name assigned by the operator and useful for path identification;
- Source Node: The Path starting node, sometimes referred as Ingress Node;
- Destination Node: The Path ending node, sometimes referred as Egress Node;
- Required Bandwidth (Mbit/sec): The bandwidth that must be assured by the path;
- Max Delay (uSec): The maximum end-to-end acceptable latency in milliseconds;
- Minimum Security Threshold: The minimum Security level for a node to be eligible to be selected and participate to the end-to-end path. Please note that a 0 value is equivalent to disabling the PCE security and privacy enhancement, in other words in this case a classical bandwidth + latency path calculation is performed.

Secure Traffic Engine - cont.

Secure traffic engine - Mozilla Firefox

Secure traffic engine

localhost:8585/#matilda-visualization

Getting Started openSUSE Google Intranet Gerrit Jenkins SonarQube Nexus Maven Central JIRA Confluence Radiator DevEnv EECS PDU NAM CI Portal

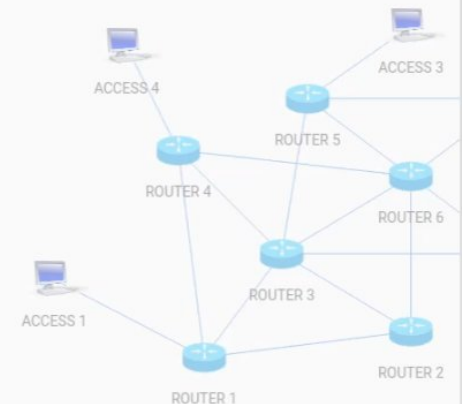
SDN Controller

SDN Controller / Secure traffic engine

Secure traffic engine

← Paths Compute Secure Path

Paths Network Map



The Network Map displays a topology with 6 routers (ROUTER 1 to ROUTER 6) and 4 access nodes (ACCESS 1 to ACCESS 4). The routers are interconnected in a mesh-like structure. ACCESS 1 is connected to ROUTER 1. ACCESS 2 is connected to ROUTER 2. ACCESS 3 is connected to ROUTER 5. ACCESS 4 is connected to ROUTER 4.

Compute Secure Path

Path Name
Path

Source Node
ACCESS 1

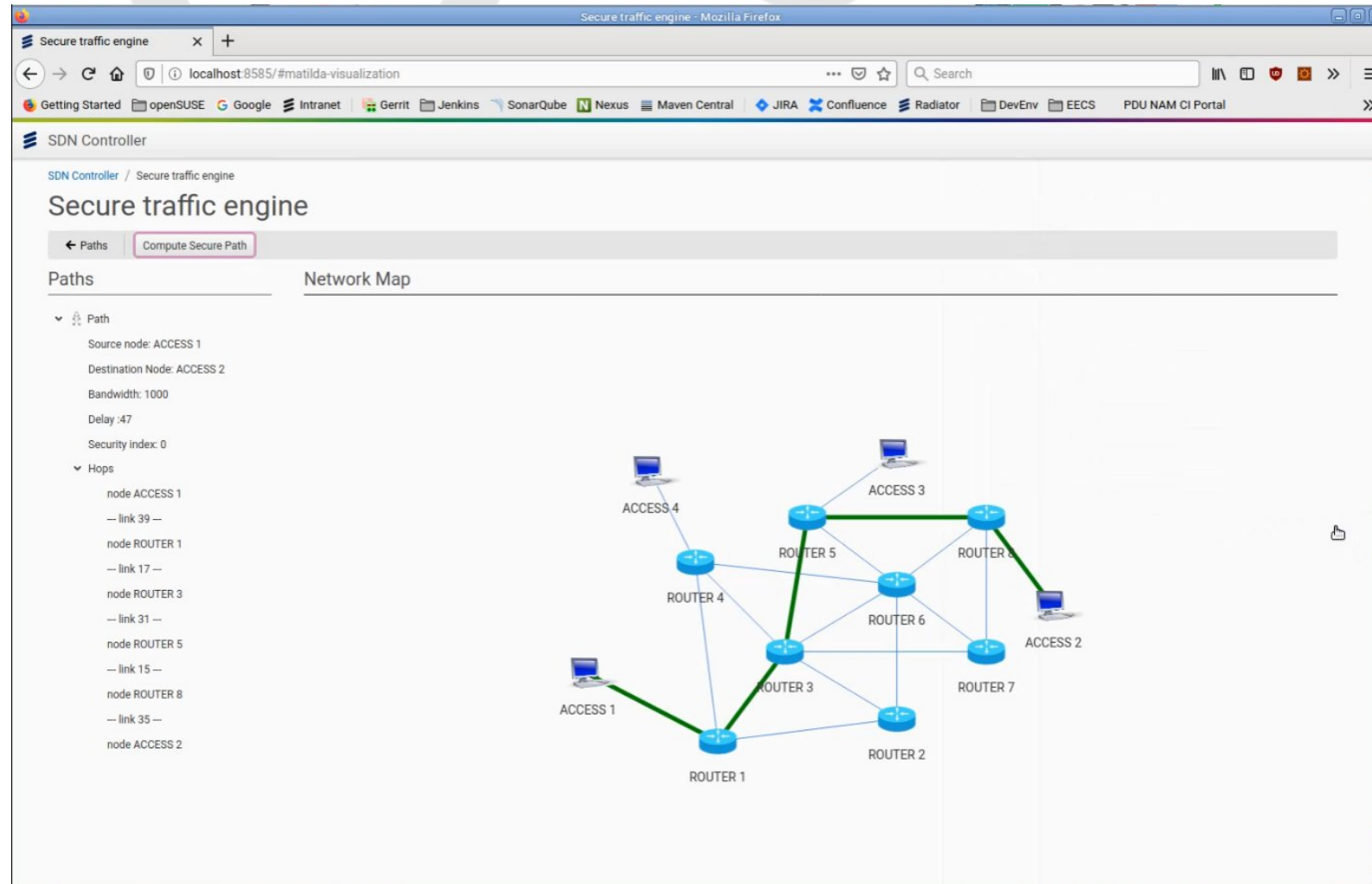
Destination Node
placeholder

- ACCESS 4
- ACCESS 3
- ACCESS 2
- ACCESS 1

Minimum Security Threshold

Cancel Search

Secure Traffic Engine - showing path





PAROMA-MED

Privacy Aware and Privacy Preserving
Distributed and Robust Machine Learning

Thank you for your attention!

For more info, please visit <https://paroma-med.eu/>



Funded by the
European Union

This work is funded by the European Union under Grant Agreement 101070222. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission (granting authority). Neither the European Union nor the granting authority can be held responsible for them.