6G Sustainable Privacy Preserving Framework Enabling Federated Learning for Health Data

Konstantinos Koutsopoulos
Qualtek Hellas
Athens, Greece
k.koutsopoulos@qualtek.eu

Pooja Mohnani
Eurescom GmbH
Heidelberg, Germany
mohnani@eurescom.eu
ORCID:0000-0002-0133-1309

Anastasius Gavras
Eurescom GmbH
Heidelberg, Germany
gavras@eurescom.eu
ORCID:0000-0003-4496-8358

Orazio Toscano
Ericsson Telecomunicazioni
Genova, Italy
orazio.toscano@ericsson.com

Benjamin Ertl
AGENTSCAPE AG
Berlin, Germany
b.ertl@agentscape.de

Giannis Ledakis
UBITECH
Athens Greece
gledakis@ubitech.eu

***Abstract*—In this paper, we present the framework evolution covering key concepts, principles and architectural approach of the EU funded Project PAROMA-MED. The project aims to provide privacy preserving techniques based on a hybrid edge/cloud approach that focuses on the establishment of high degree of trust between federation entities. This in turn introduces a new paradigm in the context of privacy and data protection that can streamline the roles and operations of data subject and data controllers/processors by artifacts in a context that has been aspired as functional GDPR. The approach attempts to create fusion between the flexibility of data driven ecosystems as they are formulated by modern Data Spaces and data protection practices based on trust establishment practices such as Hardware Root of Trust. Considering the fact that 6G prospects provide ample room for radically new approaches and enabling network architectures, this paper continues to elaborate on the project's vision as projected on future networks capabilities.**

Keywords— Health Data; Privacy Enhancing Technologies; Federated Learning; Edge; Hybrid Cloud; Network

I. INTRODUCTION

Data speeds for 6G networks will potentially offer data rates several times faster than 5G, potentially reaching terabits per second with minimal latency. Additionally, network and application automation as well as application deployment flexibility and enhanced end to end slicing techniques coupled with code-to-data practices are expected to revolutionize future applications. This fits perfectly in the context of data ecosystems in which data emerge as a highly valued commodity that requires protection both of value and privacy.

These projections aim to support, on the one hand, extremely high-capacity applications and facilitate advancements in various sectors, including healthcare, augmented reality, and the Internet of Things (IoT). On the other hand, beyond performance aspects, security and privacy schemes can be applied to isolate end to end setups and application artifacts that can provide the ground for high exploitation of user data under fully controlled conditions. In this way an Electronic Health Record (EHR) in a fully interconnected fabric will be possible, bridging together primary care, pharmacies and secondary care over 6G nodes with private bandwidth for healthcare.

This initiative focuses on leveraging data through Federated Machine Learning within the medical field, which presents significant opportunities for societal value but also demands rigorous data protection due to its sensitive nature. While GDPR has established stringent guidelines for data handling to safeguard fundamental rights, there is concern that compliance often centres on formal obligations that mainly address accountability after a data breach. In response, we propose an innovative approach, termed "Functional GDPR," emphasizing full transparency and control over data flows and continuous verification of entities involved in transactions. This approach ensures that privacy protections are validated through functional, automated methods rather than relying solely on human certification.

The overall aim is a sustainable data ecosystem by enabling participants to leverage their contributions and value. However, this sustainability will only be achievable if coupled with application and network architectures that are widely adopted and easily understood by all stakeholders. Given the widespread use of modern telecommunication networks and smart devices, we can assume that 6G capabilities can support the necessary features for sustainability. The following sections analyse these sustainable aspects, focusing on the needs of different users and stakeholders.

II. ECOSYSTEM AND STAKEHOLDER ROLES

Effective use of medical data, e.g. in the context of Artificial Intelligence (AI), requires solutions that ensure continuous trust, real-time protection, value creation, and preservation, while empowering individuals to exercise their rights. These needs extend beyond citizens and users, to include data scientists, doctors, and businesses, who generate and integrate this value into supply and service chains, ultimately benefiting society. We examine the needs of these user groups, identifying how its the proposed solutions can meet these needs and enhance user confidence.

A. Data Subject

We recognize the importance of providing user-centric solutions for two key reasons. First, to simplify privacy awareness, utilizing well-established smartphone practices like push notifications and wallet apps. Second, to empower users to take control of their data, whether for protection or making informed decisions, such as participating in data altruism. This transparency aims to reduce excessive protectionism and careless attitudes toward data rights. We ensure that individuals' choices are fully respected and enforced by offering tools that provide personalized, informed perspectives. Appropriate interfaces allow citizens to exercise their rights, with features like assisted consent management that facilitate informed decisions and enable users to negotiate additional permissions when needed. Ultimately, data subjects

will be fully aware and able to monitor any entity, process, timing, and purpose related to their data.

B. Data Scientist

Recognizing data scientists as important contributors to value creation, the project focuses on the essential need for rich, high-quality data to fully leverage the potential of AI. However, it also acknowledges that the drive for data access can sometimes overlook GDPR and other legal restrictions, which can consume valuable time and slow the development of significant solutions. Furthermore, the AI models created by data scientists must also be protected. To meet these needs, the project offers a data federation solution, which enables access to effectively unlimited data sources. Once data is created or collected, it is stored with consent options, allowing for near real-time discovery and use in various model training scenarios. This is achieved by implementing FAIR[1] principles in data processing and storage [1], continuously enforcing consent restrictions. This approach allows data scientists to query data availability and advance their work without legal concerns, confident that data use is permitted by consent and processing occurs in a fully protected environment. Additionally, the generated models are treated as data assets, with a managed and controlled lifecycle.

C. Health Experts

Recognizing the critical role of domain knowledge experts, we include physicians in its user focus, addressing their needs in creating value-added metadata that can enhance Machine Learning (ML)-based processing and yield better insights. In the AI era, contributing domain experts must be able to maintain control over their assets. The project treats metadata as valuable data assets, linked with ownership and consent options, ensuring traceability and providing a comprehensive view of how the data is used.

D. Businesses and Organizations in Health Domain

As data controllers or processors, organizations such as hospitals and medical centres bear the primary responsibility for protecting personal information. They are involved in data creation, storage, and utilization within value chains related to services and applications, with data monetization being a key focus. These organizations must ensure they can exploit data value, and at the same time prevent privacy breaches for which they are legally accountable. To address this, the project implements edge-based solutions that limit data movement by using Horizontal Federated Learning (HFL) [2]. In HFL, multiple clients collaboratively train a model with a central server, keeping data on the client side to maintain privacy. This approach ensures that local processing is secure, with data only shared among verified modules, providing organizations with the necessary assurance for protected and efficient data federation.

E. The role of 6G

6G technology will enhance social, environmental, and economic sustainability while continuing to deliver connectivity. It will introduce advancements by integrating key components, linking network entities, and introducing new technology concepts. 6G will create efficient, flexible, and intelligent AI-driven networks with sustainable designs, ultra-low latencies, and integrated communication and computing. Among others, the focus is on reducing latency, and boosting bandwidth and data throughput for critical applications, such as in the healthcare sector. From performance point of view, 6G slicing will be able to support, on the one hand, remote usage of data as if they were locally available while, on the other hand, protection practices based on attestation of communicating nodes will be ensuring controlled access according to data subject consent.

III. Concept

A. 2.1 Data Spaces Ready

PAROMA-MED has identified Data Spaces as the vehicle to enable data sharing and maximum exploitation according to well defined and adopted sovereignty principles. Although Data Spaces are clearly tailored to the facilitation of data exchange among business stakeholders and domain specific ecosystems, the involvement of personal data, as in the case of healthcare, cannot be easily overcome. In a collection of position papers by the Data Space Business Committee [3], it is clearly stated that “a more open market for health data in Europe” is required by innovative companies to achieve scale as initiatives, like GAIA-X [4], cannot resolve the highly fragmented and heterogeneous EU health market as well as the issues stemming from differences in “interpretation and local legislative variations” of GDPR.

For PAROMA-MED the core principle [5] for tackling with such challenges as well as for providing enabling solutions that can accelerate the adoption and scaling of Healthcare Data Spaces is closely related with the elimination of the need for actual private data exchange on the one hand, while on the other with enabling unrestricted utilisation and processing of private data directly inside the data storage facilities according to well-articulated and accepted options set by the data subject [6].

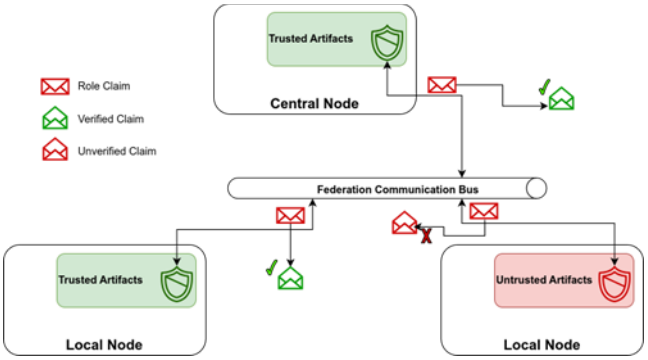

Fig. 1. Trust Establishment based on integrity of the participant

B. Data Protection and Consent in the Loop

Adopting FAIR practices throughout the data lifecycle, PAROMA-MED foresees the utilisation of a Fast Healthcare Interoperability Resources (FHIR) [7] server and an object storage solution, both protected under the supervision and encryption of the trusted domain artifacts of edge nodes (Fig. 1). Medical data end-up in secure storage along with data subject information the PAROMA-MED edge node. Initially data remain protected and associated with the identity of the subject but there are no options yet regarding how the data should be treated in terms of utilisation in a federated way. When absence of the consent is detected the subject is notified to provide their preferences via wallet or web dashboard applications. User options are used to assemble a FHIR

[1] Findability, Accessibility, Interoperability, and Reuse

Consent Statement that thereafter rules the way the particular data are treated. Once the consent options have been indicated, the trusted domain of the PAROMA-MED edge node filters the data access requests to ensure compliance with these options. In this way PAROMA-MED components create a protection layer that averts any action that is against the policy rules implied by the consent. This is either achieved by continuous evaluation of the intended actions or by assurance that the actions are performed by a trusted component. A positive evaluation results in enabling the execution of the action whereas a negative blocks it (Fig. 2).

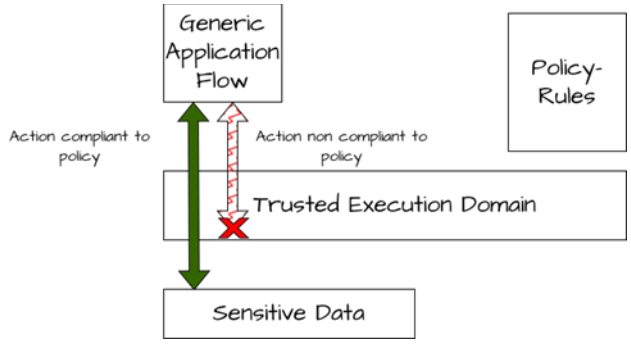

Fig. 2. Protection Layer

The role of the protection layer is not only to ensure that access to data is according to the policy stemming from the consent, it needs also to ensure that the artifact requesting the particular action/processing is also verifiable in terms of adherence to foreseen operation. Governance is exercised whenever data are to be used for some purpose. This can be done at the moment of data generation or whenever a not foreseen usage context is pending. Either due to initially limited usage policy or due to total absence of policy. In such case the data subject is presented with an incoming request detailing the usage context so that a clear decision can be taken in the form of an enforceable policy. In that case, consent details are updated and the additional usage possibilities are allowed (Fig. 3).

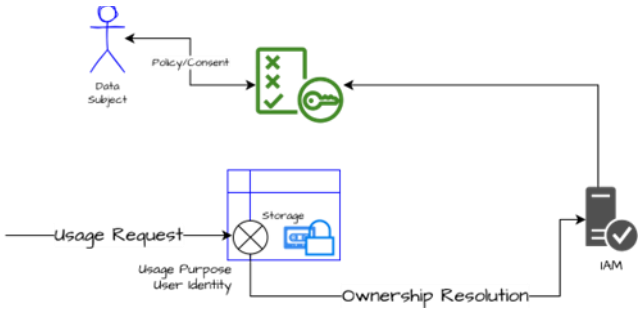

Fig. 3. Dynamic Consent Updates

C. Data Federation

In order for data to be subject to usage in the context of particular actions, they have to be discoverable at least as far as federation purposes are concerned. For this purpose, a Data Inventory layer is produced out of the data types available inside the protected storage (Fig. 4). Inventory updates are performed in batch mode to avoid statistical variation to be linked with certain identities. The flow to populate the content of the Data Inventory layer takes into account constraints from policies indicated by the individual consents. The overall result is subject to be published for discovery in a Data Space ecosystem through the appropriate Connector (Fig. 5).

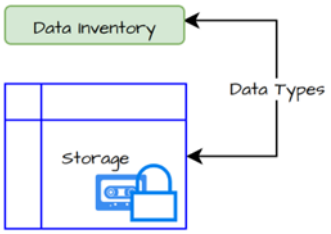

Fig. 4. Data Inventory

D. Enabling Federated Learning

Once the data sources are exposed in the Data Space federation they can be utilized in AI model engineering. Exposure does not mean direct transfer to some external storage system but only the availability to be contributed to the resolutions of queries. Data scientists are able to query the federation for availability of types and volumes of data according to certain protection levels. The outcome is collected from all the participating domains. Each of the domains contributes to the query resolution by applying internally user policies and resolving the portions of the stored data that can be made available according to the query options (Fig. 6).

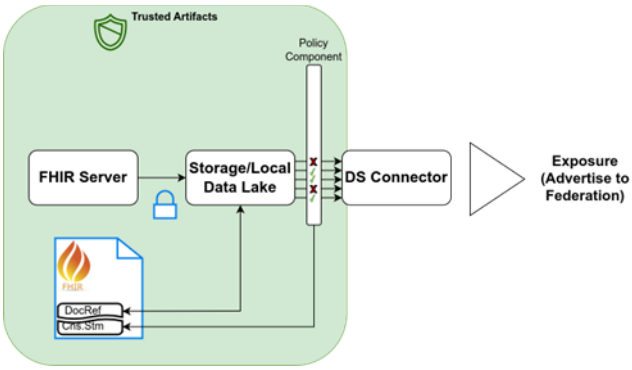

Fig. 5. Data Space Exposure

This process aims at a streamlined and ergonomic approach that relieves the data scientists from the burden of locating data that are highly distributed, but most importantly from the burden of taking all measures to remain within the legal restrictions that private data protections legislation requires. This leads to an one stop shop service and enabling mechanism. At this stage availabilities are presented under three main categories (assuming local processing in all cases):

- Directly usable data
- Data of application relevance that need additional consent
- Data without known relevance and quantity

In case the first category suffices, the ML flow can continue. If not, the consuming side (Data Scientist on behalf of any organisation or only by themselves) can suggest rewards for the other two categories in an effort to secure adequate data availabilities for the proper development of the intended ML model. As the usage of data is constrained by the intentions and identity of the consumer, based on the options of the producer or the subject the privacy of which is to be protected, there is need to firmly enclose the entire flow to be followed within the strict borders of an instantiated environment both in terms of deployed functionality and data with limited lifespan. The approach is based on GAIA-X

Conceptual and Composition Module which foresees that resources can be [8]:

- Virtual Resource: it represents static data in any form and necessary information such as dataset, configuration file, license, keypair, an AI model, neural network weights, etc.
- Instantiated Virtual Resource: it represents an instance of a Virtual Resource. It is equivalent to a Service Instance and is characterized by endpoints and access rights.

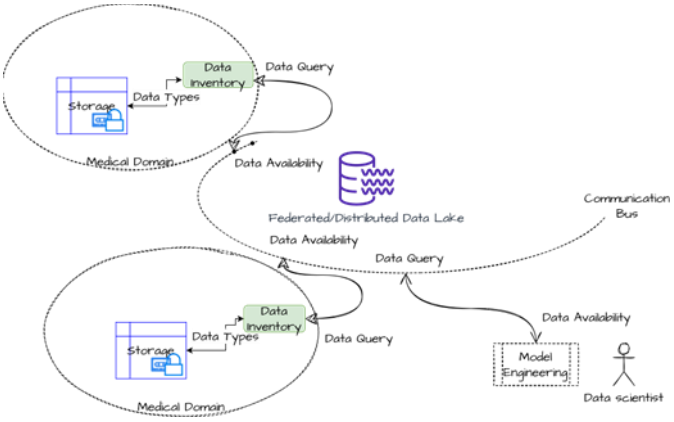

Fig. 6. Federated Query

According to the envisaged approach, data at rest (stored in local Data Lake and FHIR server) are the Virtual Resources that can instantiated within a volatile and isolated software enclosure where the intended processing is applied. This step requires that data are exposed in a uniform manner independently to the actual storage format forming a Data Usage Layer. Additionally, if this step requires certain filtering, encryption, anonymisation, watermarking to be applied, it is also performed during the provision phase of the Data Usage Layer (Fig. 7). Once there is adequate data availability for the model training purposes, data are prepared and remain available for the foreseen processing (constrained in terms of usage and time limits).

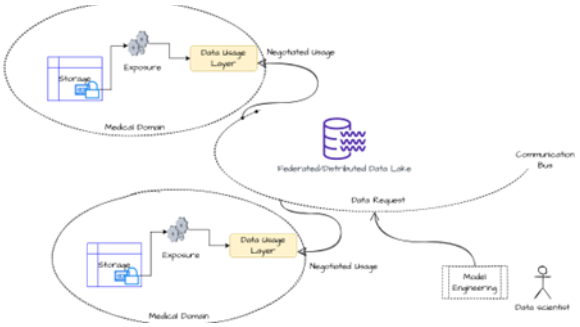

Fig. 7. Data Usage Layer – Provisioning

IV. Architecture

A. System Architecture

PAROMA-MED architecture follows the hybrid cloud pattern that foresees both centralised and local components with as much distribution and decentralisation of functionalities as possible. The decentralisation is considered as an enabling aspect to ensure both domain sovereignty and enough transparency to cater for all the constraints imposed by current and future legislation.

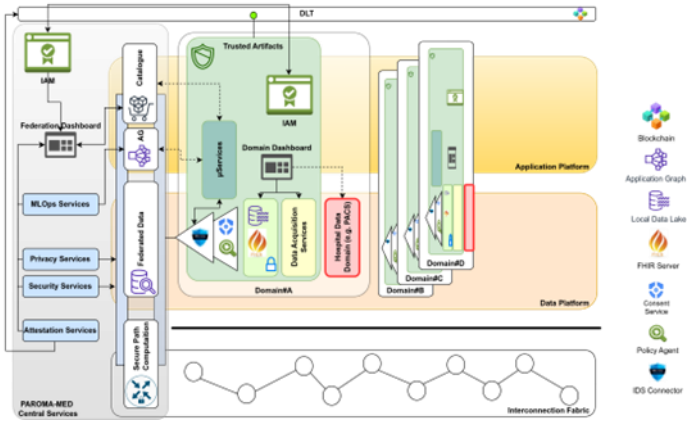

Fig. 8. Architecture

The architecture design Fig. 8 evolves by assuming that centralised and local/edge components contribute to the formation of three main categories of functionality (bottom up): i) An interconnection layer controlled by the Secure Path Computation controls logic that the project will deliver, ii) A data layer catering for all federation and ergonomic features to ease data application and service evolution on the hand, while on the other ensuring sovereign management of data assets through trusted operations, and iii) An application layer that eases deployment, operation and monitoring of application and service artifacts in the context of trust and transparency with privacy preservation at the core of the overall flows.

B. Security and Privacy

The PAROMA-Med-project is primarily about the protection of personal data, the aspect of security and privacy is fundamental to the success of the project. Thus, the PAROMA-MED access and privacy control architecture incorporates various concepts and models such as identity and access management (IAM), data classification and handling, anonymization and pseudo anonymization, privacy impact assessment (PIA), and OpenID Connect (OIDC) integration etc. These components collectively support privacy-by-design principles like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) access control, user consent control, secure data handling, and comprehensive privacy risk assessments. The architecture follows a Zero Trust security model and implements Zero Trust API security.

Through the integration of these concepts and models, PAROMA-MED establishes a robust access and privacy control framework. It enables automatic attestation of federation partners, privacy and security by design, federated identity and access management based on Zero Trust principles, privacy-preserving data storage and processing, and flexible and secure access to private data and services. This ensures compliance with privacy regulations, respects user preferences, and promotes a trustworthy environment for data-intensive applications in federative cross-border environments, particularly within the healthcare sector.

V. Deployment of PAROMA-MED in Real World Setting

A. Network needs

Today, 5G is known to provide 10x higher wireless speeds, low latency, and ultra-reliable connectivity, around the corner is 6G which promises to increase the transmission

bandwidth and boosts data throughput to new levels using (sub) THz band communication in order to foster and make feasible challenging applications that bring virtual and real worlds closer. However, the interoperability and ubiquity of telecommunication networks, which support and fulfill key aspects of modern day living, is taken for granted and this fact has been underlined very recently in the context of the most current and important European research projects which have reaffirmed how the discussions about data sovereignty and data-based business models often forget the technical underpinnings: the network infrastructure that carries our data that necessarily had and have to evolve very quickly to keep pace [9].

Highlighted by important European research projects the challenge is to [10], make the systems of network providers and cloud platforms interoperable, easier and faster set up for end-to-end network connections. Whilst addressed by the top 5G world infrastructure providers [11] and by the most important recommendation entities [12], full end-to-end automation of network and service management has also become an urgent necessity for delivering services with agility and speed and ensuring the economic sustainability of the very diverse set of services offered by Digital Service Providers. The ultimate automation target is to enable largely autonomous networks which will be driven by high-level policies and rules; these networks will be capable of self-configuration, self-monitoring, self-healing and self-optimization without any human intervention. All this requires a new horizontal and vertical end-to-end architecture framework designed for closed-loop automation and optimized for data-driven machine learning and artificial intelligence algorithms [11].

B. Network and Interconnect Platform

The PAROMA_MED network interconnect platform is important for a security and privacy-aware management of the network infrastructure that constitutes the interconnection layer PAROMA-MED leverages on and evolves to PCE. According to the IETF definition [14] Path computation element (PCE) is defined as “an entity component, application, or network node that is capable of computing a network path or route based on a network graph and applying computational constraints”. The growing interest in path computation element (PCE) architectures can be attributed to their ability to offer practical and effective routing solutions fulfilling the Quality-of-Service requirements for single or multi-layer networks and addressing the challenge of connecting services across multiple domains [14]. IETF (The Internet Engineering Task Force) has conceived the PCE architecture, promoting a specialized and flexible network entity able to effectively tackle visibility limitations and distributed provisioning inefficiencies. The Path Computation Element gathers information about the network & link-state and conducts path calculations on behalf of network nodes. Moreover, the PCE can utilize other sources of information (Fig. 9), such as the network management system (NMS), to obtain specific data regarding resource usage (e.g., wavelengths in use) or physical network characteristics (e.g., link distance, impairments).

An important benefit offered by the PCE is that it enables network nodes to avoid computationally intensive path calculations, resulting in the ability to achieve effective Traffic Engineering (TE) solutions even for legacy network nodes. The PAROMA-MED solution is built on top of refined definitions of the security and privacy level of the network components whose novelty has been protected with a dedicated patent [15] - “PATH COMPUTATION IN A COMMUNICATION NETWORK” and evolution of the classical “bandwidth/latency” optimization paradigm towards an effective multi-dimensional optimization (Security and Privacy constraints, Performance constraints, Traffic volume constraints etc.). The patent outlines a framework for integrating these advanced metrics into PCE algorithms, thereby enhancing the overall robustness and trustworthiness of network slices. This development represents a crucial step forward in 5G/6G telecommunications, as it addresses the growing need for secure and private virtual networks in an increasingly interconnected world.

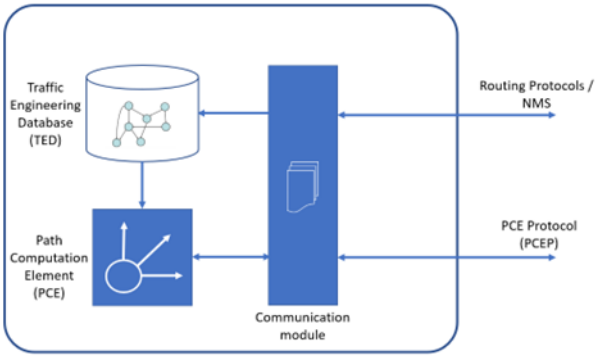

Fig. 9. Functional modules of a Path Computation solution

VI. INTEGRATION WITH EXISTING SYSTEMS

A. Use Case and Pilot Deployment

At the core of the federation aspects of PAROMA-MED lies the Dataspace Connector[17] [17] facilitating seamless data interoperability and usage control policies within data spaces. By integrating and expanding the usage of the connector into the PAROMA-MED platform, the system can ensure that data sharing practices adhere to industry standards and best practices, thereby enhancing the platform's capability to handle sensitive healthcare data securely and compliantly.

B. Integration of the EU Digital Identity Wallet

The EU Digital Identity Wallet [18] is designed to enhance privacy and security while providing a seamless user experience across different online platforms. Users have full control over their personal data, deciding which information to share and with whom, which aligns with the stringent data protection principles of the General Data Protection Regulation (GDPR). The wallet aims to eliminate the need for multiple digital identities and third-party authentication services, simplifying the process of digital identification across Europe.

In the context of the PAROMA-MED platform, integrating the EU Digital Identity Wallet plays a crucial role in strengthening access and privacy control architecture. The integration ensures that user authentication is standardized, secure, and compliant with EU regulations. When users access the PAROMA-MED platform, the EU Digital Identity Wallet facilitates their authentication process by providing a secure and verified digital identity. This integration not only enhances user trust by ensuring that their personal data is protected but also streamlines access to the platform’s healthcare services.

Moreover, the integration of the EU Digital Identity Wallet within PAROMA-MED supports robust consent management and usage control. By utilizing the wallet, users can manage their consent preferences for data usage directly within the platform. This ensures that all data handling activities comply with the users' consent and regulatory requirements. The wallet's interoperability and secure design align with PAROMA-MED's objectives to maintain high standards of data security and privacy, ensuring that sensitive healthcare data is managed responsibly and in compliance with GDPR.

VII. Conclusion

PAROMA-MED implements edge-based solutions that primarily restrict data movement and exchange in a federated way. The value is created by engagement of local processing with assurance that the product of the processing is protected and moved only among attested and verified modules in external domains. Overall, this can provide the assurance required by the user types and allow efficient and protected federation with full protection of both rights and value. As the platform continues to evolve, ongoing efforts will focus on refining these integrations and exploring ways to enhance the security and privacy control architecture. The implementation of the EU Digital Identity Wallet, holds significant promise for improving federated identity management across the platform. In conclusion, the outlined framework ensures that the platform is well-equipped to handle the complexities of healthcare architectural evolution towards 6G by maintaining a focus on security, compliance, and user privacy. The envisioned platform is poised to support innovative 6G healthcare solutions while safeguarding the sensitive data that underpins these advancements. The continued commitment to integrate advanced technologies and adhering to regulatory standards will ensure the platform remains at the forefront of secure healthcare data management.

PAROMA-MED has integrated in its architecture the community version of the Dataspace Connector 6 from Sovity [21][21]that is based on the Eclipse Dataspace Componets [21]. Additionally, the project has deployed the Dynamic Attribute Provisioning Service [22] and the Broker Extensions [23] also from Sovity. Although currently the Broker is an archived project, it is still applicable for the proof of concept sought after by the project and the experience gained will allow PAROMA-MED to consider additional integrations as emerge due to the involvement of Sovity in the tehcnical realization of artifacts in the Mobility Dataspace [24].

The next main component integrated in the architecture is the FHIR Server. HAPI-FHIR [25]has been selected in the Emulated Hospital Nodes. The FHIR server is coupled with a a production grade object storage solution [26]and the project has successfully integrated with DICOM backends for data ingestion. The FHIR consent management is the central element that holds Data Subject GDPR options in fine grained manner with provisions to accommodate consent options for each field of personal data and medical exam details. The current configuration is tailored to the Use Case but can be parametrized to cater for other scenarios. PAROMA-MED utilises the consent options for the advertisement of availability of data through the Dataspace Connectors. The contract negotiation foreseen by the Dataspace protocol is exploited both to manage provisioning of data volumes for federated learning for data directly usable and for those cases that explicit consent is required.

Overall, the pilot usage indicates the applicability of the designed solution for GDPR compliant exploitation of data in federated learning scenarios and it is expected to be evaluated from several perspectives in workshops involving both citizens and medical experts.

VIII. Acknowledgments

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.

IX. References

[1] https://www.go-fair.org/fair-principles/

[2] Fairness and accuracy in horizontal federated learning: https://www.sciencedirect.com/science/article/abs/pii/S0020025521013244?via%3Dihub#preview-section-abstract

[3] Data Space Business Committee – Position Papers Consolidated Version for Industry Verticals. 13 August 2021

[4] https://gaia-x.eu/

[5] PAROMA-MED D1.2: Concept and Evaluation Framework - first version, July 2023

[6] PAROMA-MED D1.1: Requirements and Use Case Definition, March 2023

[7] https://www.hl7.org/fhir/overview.html

[8] Gaia-X Architecture Document - 22.10 Release

[9] Gaia-X Compliance Service deployment scenario, September 2, 2022

[10] Why Europe's Gaia-X Data Ecosystem needs a more powerful Network Infrastructure - May 22, 2023 - https://www.gxfs.eu/tellus/

[11] Ericsson "Service automation Towards zero-touch with service automation" - Service automation - the journey towards 5G – Ericsson

[12] ETSI ZSM (Zero-touch network and Service Management) - ETSI - ZSM - Zero touch network & Service Management

[13] "https://gaia-x.eu/"A. Farrel, J.P. Vasseur, and J. Ash, "A path computation element (PCE)-based architecture," IETF RFC 4655, pp. 1–40, August 2006. Online (Dec. 2009): http://tools.ietf.org/html/rfc4655.

[14] IETF PCE working group home page. Online (Dec. 2009): http://www.ietf.org/html.charters/pce-charter.html

[15] https://zenodo.org/records/10943056

[16] https://www.freepatentsonline.com/WO2024091149A1.html

[17] "Dataspace Protocol 2024-1 | IDS Knowledge Base." Accessed: Jul. 19, 2024. [Online]. Available: https://docs.internationaldataspaces.org/idsknowledgebase/v/dataspace-protocol/

[18] "International Data Spaces," International Data Spaces. Accessed: Jul. 19, 2024. [Online]. Available: https://internationaldataspaces.org/

[19] https://sovity.de

[20] https://github.com/sovity/edc-ce

[21] https://github.com/eclipse-edc

[22] https://github.com/sovity/sovity-daps

[23] https://github.com/sovity/edc-broker-server-extension

[24] https://mobility-dataspace.eu/

[25] https://hapifhir.io/

[26] https://min.io/