Federated machine learning through edge ready architectures with privacy preservation as a service

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

Antoine Simon
Universite de Rennes I
Rennes, France
antoine.simon@univ-rennes1.fr

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

Spyridon Tompros
Qualtek Sprl.
Brussels, Belgium
s.tompros@qualtek.eu

Katarzyna Kapusta
Thales Six GTS France SAS
Gennevilliers, France
katarzyna.kapusta@thalesgroup.com

Gouenou Coatrieux
IMT Atlantique
Brest, France
gouenou.coatrieux@imt-atlantique.fr

Anastasius Gavras
Eurescom GmbH
Heidelbrg, Germany
gavras@eurescom.com

Giannis Ledakis
UBITECH
Athens, Greece
gledakis@ubitech.eu

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

Stefan Covaci
Agentscape AG
Berlin, Germany
s.covaci@agentscape.de

Christoph Thümmler
6G Health Institute GmbH
Leipzig, Germany
christoph.thuemmler@6ghi.net

***Abstract*—This paper presents the details of a novel approach, based on edge and advanced privacy preserving solutions, that tries to accelerate the adoption of personal data federation for the benefit of the evolution of valuable advanced AI models. The approach focuses on the establishment of high degree of trust between data owner and data management infrastructure so that consent in data processing is given by means of functional and enforceable options applicable at all levels of workloads and processes. The overall set of solutions will be delivered as an open-source set of implementations in the context of the PAROMA-MED project.**

***Keywords*—Health Data, Privacy Enhancing Technologies, Rights Management, Federated Learning, Edge, Hybrid Cloud, MLOps.**

I. Introduction

The growing adoption of cloud native architectures for data analytics such as machine learning (ML) based analysis of data over federated data sources brings benefits in terms of speed, efficiency and adaptability compared to legacy data pipeline architectures. However, immediate challenges arise in terms of privacy and security for the data, the distributed infrastructure and the virtualised services and applications. Such challenges are not new and have been previously described in in the context of the Software-to-Data paradigm for eHealth applications [1] and requirements engineering for digital Health [2]. In order to respond to these challenges, PAROMA-MED project has planned to deliver an open-source platform to deal with privacy preservation in scalable and reliable way that will be catering for the establishment of personal data federation practices.

II. Personal Data Federation Challenges

We define *federation* as the concept whereby a party uses data or resources beyond the boundaries of its administrative (usually organizational) domain, provided by another party. Federations aim to implement a common service, drawing upon data or resources committed by organizations that participate in the federation. This mechanism can be applied recursively. A federation might be visible as one administrative domain to third parties. A federation in PAROMA-MED does not imply a central authority.

A. The need to federate data

As AI/ML is considered to be the norm for application development is several sectors due to its potential to provide added value solutions, there is increasing need for availability of data and meta-information on which training and evolution of the machine learning models will be based. Although synthetic or real data which, however, remain available only within the borders of specific administrative domains can be used by scientists and researchers to advance their work on certain areas, the volume and quality of data sets that can be contributed to by all the relevant stakeholders in a particular application or business area would significantly boost the evolution in the field. Equally, the capabilities of data scientists and AI developers are in several cases underexploited due to legal or policy restrictions that are enforcing coupling employment of data scientists with data ownership. The emergence of Data Spaces practices along with the evolving EU regulation on Data Governance require concrete solutions in data and computing federation as a vehicle to accelerate digital transformation of both the society and the economy.

B. Privacy Concerns

Adhering to the constraints of the EU General Data Protection Regulation (GDPR), great attention is devoted by international research on the best methods (often context dependent) to anonymize datasets in an effective way from the point of view of minimizing the residual risk, and on the other hand, without excessive impacts on the performance of the following elaboration. According to the GDPR risk-based approach the residual risk has to be precisely quantified in

The work described in this paper is funded by the EU Horizon Europe programme under Grant Agreement 101070222

2022 IEEE Future Networks World Forum (FNWF) | 978-1-6654-6250-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/FNWF55208.2022.00067

2770-7679/22/$31.00 ©2022 IEEE
DOI 10.1109/FNWF55208.2022.00067

probabilistic terms and is, however, never completely voidable. Many recent works have shown that machine learning models themselves can be used to derive personal information, as demonstrated by recent membership inference attacks (MIAs: ability to identify whether a data record was included in the training dataset of the target machine learning model) and attribute inference attacks (AIAs: ability to infer missing attributes of a partially known record used in the training dataset by accessing the machine learning model). An important aspect towards federation of data is, therefore, to ensure privacy protection by selecting, evaluating and improving the best private-data protection techniques or introducing innovative ones to achieve better and more robust protection levels, quantifying and minimizing the probabilistic risks and the performance related penalties.

C. *Scalability Challenges*

Although the processing capabilities of cloud data centres can play a significant role in the training phase of AI Models, transfer of private data sets to the cloud is subject to restrictions and regulation constraints and there are several cases where such transfer is not allowed. On the other hand, training of AI models within local domains lack the option of extended data availability. It is necessary, therefore, to design solutions for taking advantage of the centralised cloud computing capabilities as well as of data protection that can be achieved by the local distributed entities. The solutions should be, however, scalable in terms of dynamic inclusion of additional parties contributing to and benefiting from the collaborative training schemes without neglecting aspects such as the value and quality of individual contributions as means to fairly [3] calculate the updates distributed from the trained models.

D. *User Friendly Aspects - Data Owner*

The most important aspect towards personal data federation regards the decision of the data owner on specific permission over the use of their data. As the value of data is nowadays continuously elevated and the privacy protection is mandatory, the typical approach that involves manual or even handwritten declaration on data usage options is highly outdated and most importantly not enforceable as the data misuse can be only proven after a period of time, once intentional or unintentional disclosure has already taken place. Therefore, there is high demand for establishing practices that allow the data owner to indicate fine grained options pertaining to consents regarding parts of their data as well as to the required constraints regarding levels of privacy and security to be applied. Obviously, such options should be enforceable by engagement of specific operational artifacts that will in turn help in building user trust towards the involved systems and services. In the context of such practices, information should be clearly presented in a contextualized way so that the average user can easily understand and make well informed decisions. It is expected that establishment of such practices will contribute to increasing user awareness on privacy and security aspects and cultivate a new approach regarding systems and services and the way users establish trust with consumed services.

E. *User Friendly Aspects - Researcher*

With AI involved in several fields and the relevant technical roles decoupled (e.g. Machine Learning Engineer, Artificial Intelligence Engineer, Business Intelligence Developer, Research Scientist, Data Scientist, Big Data Engineer, Robotics Scientist, etc.) there is increasing need to allow business domains to take advantage of AI practices, under the variety of conditions according to which they participate in federated environments. This requires the provision of enabling artifacts and services that can eliminate the need for setting up a complete team of experts for experimenting and researching with AI based solutions either as a proof of concept prior to opting for production investments or as new type of business development that can focus on the provision of added value AI models through relevant marketplaces. As in the case of data owners, AI researchers should be given the option to define their requirements on data, the related security and privacy constraints as well as their intentions with respect to the produced AI models and how these can be federated also for the benefit of the participating entities in terms of data or processing contributions. Contextualization plays an important role regarding the streamlining, adoption and ease of use of federations.

III. An Edge Based Platform to Ensure Trust Through Privacy Preserving Federated Solutions

The federation challenges listed above necessitate the engagement of edge-based solutions as a means to establish bidirectional (to and from the federation ecosystems) trust anchors on top of which privacy mechanisms can be applied with confidence for all involved parties. Such approach is already gaining ground in service architectures with the adoption of hybrid central-edge cloud solutions and the approach presented in this study relies heavily on this hybrid model as a key aspect for the establishment of federations with automatic attestation of involved parties, zero-touch deployment and automatic life-cycle management of services and applications, flexible and secure access to private-data and service resources, managed privacy and security operations for automated policy enforcement and cyber-threat detection and mitigation.

An important aspect that is introduced in the described approach relates to the proper management and utilization of the Trusted Execution Environment of the embedded processors of the edge nodes. The software tools and libraries that will be implemented will offer in the form of user selectable options the isolation and privacy levels that can be achieved through this type of processing.

A. *User Friendly Consent Management and Enforcement*

The introduction of edge-based approaches not only ensures that processing is performed close to data sources and repositories, but it also allows for the development of user centred procedures without exposing user identities and roles beyond the borders of business domains and service infrastructures with which users are already familiar. Such practices contribute to better fusion between users and systems on the grounds of established trust. From a functional point of view, the PAROMA-MED platform will offer fine grained identity and role management, targeting specifically the constraints relating to personal data, so that user interfacing will be contextualized as a means to ease consent management and relevant opt-in/out decisions ensuring that users are properly informed and fully aware about the presented options. In a similar way, AI/ML researchers will be expressing the high-level requirements for privacy and security (privacy and security by design) during the training phase of their models so that the platform marketplace backend service can apply automatically the deployment of the MLOps artifacts, ensuring enforcement of the security constraints through smart contracts and policy agents, during the training and distribution of the produced models. MLOps refers to the application of DevOps-like technologies for standardising and simplifying the lifecycle management of machine learning mechanisms.

User interfaces will be designed to present users with views that are ergonomic and easily conceivable to allow them making the proper choices regarding which part of their data can be federated, under which privacy options, for how long and most importantly by whom these can be used. The profile of the potential user of a person's data, as a federation partner, will be also subject to inspection and consent and the enforcement of the selected options will be subject to the automatic attestation mechanisms involved in the overall platform operation.

B. Functional GDPR – Smart Contracts

Smart contracts define rules and penalties around agreements between two or multiple parties and automatically enforce the associated obligations. Such a mechanism can provide a functional approach to privacy policies, such as the EU GDPR, by describing opt-in and opt-out requests of users to privacy policies. Smart contracts with this kind of information published to a distributed ledger allow service providers to build a fully trusted environment for personal data protection.

A possible use-case would enable service providers to write opt-in requests to their privacy policy on the distributed ledger while users can remain pseudonymised. Smart contracts can describe privacy policies' opt-in requests as timestamped signatures to the agreed terms with automatic expiration. Similar opt-out requests can be written to the distributed ledger and proven by the non-repudiation of cryptographic signatures when a service provider signs the received requests outside the distributed ledger and removes the associated opt-in request on the distributed ledger.

Such an example use-case shows how distributed ledger technology can provide an innovative and autonomous solution for functional GDPR compliance seamlessly and transparently, using the distributed ledger as an opt-in ledger. However, with the advances toward distributed autonomous services, smart contracts can further utilise functional and programmable mechanisms for privacy regulatory bodies, users, and user-independent services and applications, self-sufficiently agreeing on privacy terms between services and applications.

C. Policy Enforcement Agents

With the advances in microservice architectures, smart agents for policy enforcement can be implemented as sidecar proxies (deployed as separate processes but attached to, and correlated to the main application component). Policy enforcement agents following a sidecar proxy pattern enable the creation of unified and target specific policies and privileged access at the microservice level. With input and output bindings, this approach decouples the decision making with enforcement, for example accepting structured data as input and returning either a decision or arbitrary structured data as output. The decoupling of authorisation decisions from business logic in microservices delegates the responsibility to generate authorisation policies to individual microservice owners, where neither the microservice owners nor the system administrators have to deal with an area outside their boundaries. In practice, policy enforcement agents on the microservice level can authorise requests to API Endpoint based on meta and contextual information and information from external data sources, allowing granular decisions for service and data access to resources. The Open Policy Agent (OPA) [4] is a prominent example of an open-source, general-purpose policy engine that unifies policy enforcement across the application stack. OPA provides a high-level declarative language that specifies policy-as-code and provides simple APIs to offload policy decision-making from the software.

D. Data Privacy Mechanisms

The platform will be enriched with novel privacy-preserving and trust enhancing mechanisms. Trust issues between participants of the machine learning federation ecosystem will be addressed using collaborative fairness [2]: an approach in which, during the FL training process, each participant receives model updates according to the quality of their past updates.

To secure the trained ML models against violation of ownership rights or attacks on their integrity, ML watermarking techniques and services will be developed, enabling model identification in a way similar to cryptographic signature but adapted to the ML context. A particular focus will be set to provide efficient watermarking techniques and protocols, adapted for the collaborative setting, where multiple model creators are involved.

Besides secure ML, micro-services for secure processing of private data will be provided leveraging advanced cryptography techniques, such as Homomorphic Encryption (HE) or Multi-Party Computation (MPC). Based on the well-established Private Set Intersection (PSI) [5] algorithm, the micro-services will apply secure comparison and analysis of private data-sets. The classical version of the PSI algorithm will be adapted to the multi-user setting as well as to support image data-sets as inputs.

Additionally, the platform will also offer newly developed crypto-watermarking [6] tools for pieces of information that are shared or externalized for the training task of machine learning models. The main objective is to provide watermarking [7] based data traceability services from encrypted and decrypted data to fight against information leaks (dissuasion, detection, accountability, remediation).

E. Edge Platform and Cloud Ready Solution for Future Networks

Edge computing takes place at or near the physical location of either the user or the source of data, in order to comply with latency or data-residency constraints. The proposed approach, adopts a hybrid cloud architecture that allows for workload portability, orchestration, and management across multiple environments, that is required for the operation of central and distributed services (e.g., MLOps, Data Access, Identity & Access Management) according to the concept of Multi-access Edge Computing [8] (formerly mobile edge computing).

The central cloud offers security and privacy services that are implemented as microservices and follow a sidecar deployment pattern. Theses microservices are smart agents that are deployed along platform services and applications, federation parties and connected devices. Notably microservices implement a Security-as-a-Service (SECaaS) and a Data-Privacy-as-a-Service (DPaaS) pattern.

The microservices ensure privacy and security "by design" and are embedded automatically in the application and service graphs, thus enabling the application developers to deal only with the business-logic of their application. The application provider or operator specifies privacy and security requirements at a high-level by means of policies, which are translated automatically by the SECaaS and DPaaS into specific configurations and deployments of the smart agents.

Utilizing microservices in this context requires a service and event mesh architecture. A service mesh (overlay network) provides connection-level routing and traffic management for synchronous request/reply communications through sidecar microservices. An event mesh handles the asynchronous event-driven routing of information through event brokers (also known as Context Brokers, where an event is a context update).

Platform APIs are exposed via API gateways towards the application layer (northbound APIs) and towards the access & interconnect and device layers (southbound APIs). An API gateway is a centralized access and security policy enforcement point to a microservice deployment and the entry point that screens all incoming request-messages for security and QoS features.

The approach offers a variety of APIs for users/developers at the application layer, e.g., domain specific APIs (healthcare APIs) with regulatory compliance, data APIs for data services (e.g., analytics, visualisation) and control APIs, that allow the orchestration, deployment and integration of platform applications (e.g., AI models, dashboard). APIs will follow the OpenAPI standard [9].

Connectivity APIs are exposed towards the device layer to connect and integrate different devices (e.g., mobile user devices, medical devices, sensors). Devices can connect via 5G, LoRaWAN or Bluetooth to the overall platform and access data and services.

In the reflected paradigm, a data lake storage concept is utilized to store the large amounts of data that are produced in the medical domain (e.g. medical images, long time-series of sensor data). A data lake is a repository that holds a large amount of structured and unstructured data, providing unique identifiers and metadata tags. Unlike most data warehouses and databases, data lakes can handle all types of data, including unstructured and semi-structured data such as images, video, and audio, that are required for machine learning use cases.

Additionally, via its north- and southbound APIs, the approach offers access to federation parties, in order to integrate with their Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) or Anything-as-a-Service (XaaS) solutions. This offers flexibility for the distribution of the data-sourcing / storage and data-processing tasks among parties in the application provisioning / value-chain federation and enables integration of further ecosystem stakeholders and actors.

IV. Next Steps and Validation Plans

The platform of PAROMA-MED will be developed and validated according to a 3 years project plan until mid-2025. The project is currently performing the requirements consolidation and initial design phase.

The platform will be validated through Use Cases involving medical image analysis, including the qualitative assessment of cardiac anatomy from Computed Tomography (CT) images. ML methods that will be used to automatically extract myocardium wall boundaries, and thus to compute its thickness which is a descriptor of large clinical interest, will be based on Deep Learning (DL) techniques, which have demonstrated their ability to analyse cardiac images. The main limitation of the widely used DL methods is their lack of generalization capabilities when presented with unseen data, typically images acquired with another imaging system, or even with the same system but configured differently, or corresponding to other pathologies. Another limitation is the need for annotated (e.g. manually delineated) images to train and evaluate the models. The developed platform will enable to tackle these challenges. Clinical centres, as edge nodes, will provide annotated data (e.g., delineated images). All resulting data will be stored on the local edge nodes. Privacy policies will be managed through the platform mechanisms, including smart contracts. Different scenarios will be implemented to generate models exploiting data from all edge nodes, from partial models merging to full federated learning remotely exploiting edge nodes data. 3D-Unet deep learning [10] architectures will be exploited, since they have demonstrated to be particularly successful for 3D medical images analysis. All the generated models will be evaluated on local edge nodes and on the central node.

Acknowledgement and Disclaimer

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.

References

[1] Thuemmler C., Mueller J., Covaci S., Magedanz T., de Panfilis S., Jell T., Schneider A., and Gavras A., "Applying the Software-to-Data Paradigm in Next Generation E-Health Hybrid Clouds," 2013 10th International Conference on Information Technology: New Generations, 2013, pp. 459-463, doi: 10.1109/ITNG.2013.77.

[2] Fricker S. A., Thuemmler C., and Gavras A. (2015). Requirements Engineering for Digital Health. Springer International Publishing. ISBN 978-3-319-09797-8. DOI https://doi.org/10.1007/978-3-319-09798-5

[3] Lyu L., X. Xinyi and W. Qian. “Collaborative Fairness in Federated Learning.” Federated Learning (2020).

[4] Policy-based control for cloud native environments, Open Policy Agent, online: https://www.openpolicyagent.org, accessed May 2022

[5] Ion M., Kreuter B., Nergiz A., Patel S., Saxena S., Seth K., Raykova M., Shanahan D. and Yung M. (2020). On Deploying Secure Computing: Private Intersection-Sum-with-Cardinality. 370-389. 10.1109/EuroSP48549.2020.00031.

[6] Kapusta K., Thouvenot V., Bettan O., Beguinet H., and Senet H. 2021. A Protocol for Secure Verification of Watermarks Embedded into Machine Learning Models. In Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '21). Association for Computing Machinery, New York, NY, USA, 171–176. https://doi.org/10.1145/3437880.3460409

[7] Kapusta K., Thouvenot V., and Bettan O. Watermarking at the service of intellectual property rights of ML models. In Actes de la conférence CAID 2020, online: https://hal.archives-ouvertes.fr/hal-03206297

[8] ETSI, Multi-access Edge Computing, accessed May 2022, online: https://www.etsi.org/technologies/multi-access-edge-computing

[9] The OpenAPI Initiative, online: https://www.openapis.org, accessed May 2022

[10] Çiçek, Ö., Abdulkadir, A., Lienkamp, S.S., Brox, T., Ronneberger, O. (2016). 3D U-Net: Learning Dense Volumetric Segmentation from Sparse Annotation. In: Ourselin, S., Joskowicz, L., Sabuncu, M., Unal, G., Wells, W. (eds) Medical Image Computing and Computer-Assisted Intervention – MICCAI 2016. MICCAI 2016. Lecture Notes in Computer Science, vol 9901 (pp. 424-432). Springer, Cham. https://doi.org/10.1007/978-3-319-46723-8_49