EPI Framework: Dynamic infrastructures to secure data sharing across healthcare domains

Jamila Alsayed Kassem[1]

[1]UvA, MNS group

The effective sharing of medical data and electronic health records (EHR) is a key enabler in health research advancements and achieving personalised medicine. Due to the inherently sensitive nature of this information, it is vital to securely transmit, store, and process the shared datasets. With that in mind, the main challenge is to dynamically set up a collaborative environment/data sharing application request to ensure undegraded security across different healthcare domains. A data-sharing framework is needed to bring together cooperative efforts of research centres, health institutions, and patients groups. The framework should consider policies, different parties' infrastructural capabilities (network and security functions supported), and the methods to dynamically match requirements to setup actions.

Our work is part of the EPI (Enabling Personalised Interventions) [1] project that ultimately aims to empower patients through self/joint management of their personalised treatment and recovery cycle. We propose the EPI Framework (EPIF) [2], a dynamic health data sharing framework that accommodates to different domains' infrastructural capabilities by shipping and managing containerised security services (bridging functions). As a result, the EPIF supports health use cases (*e.g.* medical data streaming, EHR and backup, machine learning model training) by allowing different collaboration data sharing models (archetypes).

Many research efforts have been made to secure computing and communicating medical data. However, some of them address security without considering the environments with multiple domains. Moreover, most of the time the solution offered is a static approach of a one-fits-all function and it doesn't consider the possibility of a dynamic policy (*e.g.* retracted consent, new security requirement, etc). In [4] [3], the framework utilises cloud computing to store, process, and manage data. The framework addresses security concerns that arise with a third-party cloud service provider using Attribute-based encryption cryptography techniques. Other approaches like RoboChain [1] utilises blockchain tools to share data and learning models in a secure and decentralised way. The proposed methods are secure against possible attacks but are limited to a numbered archetypes. The frameworks are also rigid and do not consider different requirements, policy rules, and heterogeneous environments.

In our framework, we estimate the setup needed for nodes across multiple health domains to communicate, store, and process data according to the agreed policy, the initial infrastructural capabilities, and the feasibility of patching any security imbalance between domains. New infrastructures and services will be "manufactured by software" by the EPIF, and then hosted in an "infrastructure factory" (Proxy shown in Figure 1) such that network functions are dynamically and flexibly traded and provisioned.

Figure 1 shows the EPIF's main components: EPI middleware, proxy, and Middleware Interaction Node (MIN). The middleware acts as a multi-domain orchestrator that manages and fires-up containerised network services according to the nodes registry and policy rules. The proxy is the EPI actor running at the edge of a network and maintaining a pool of bridging container images. The MIN acts as a user-infrastructure point of interaction. The nodes pass the requested collaboration archetype

[1]https://delaat.net/epi/

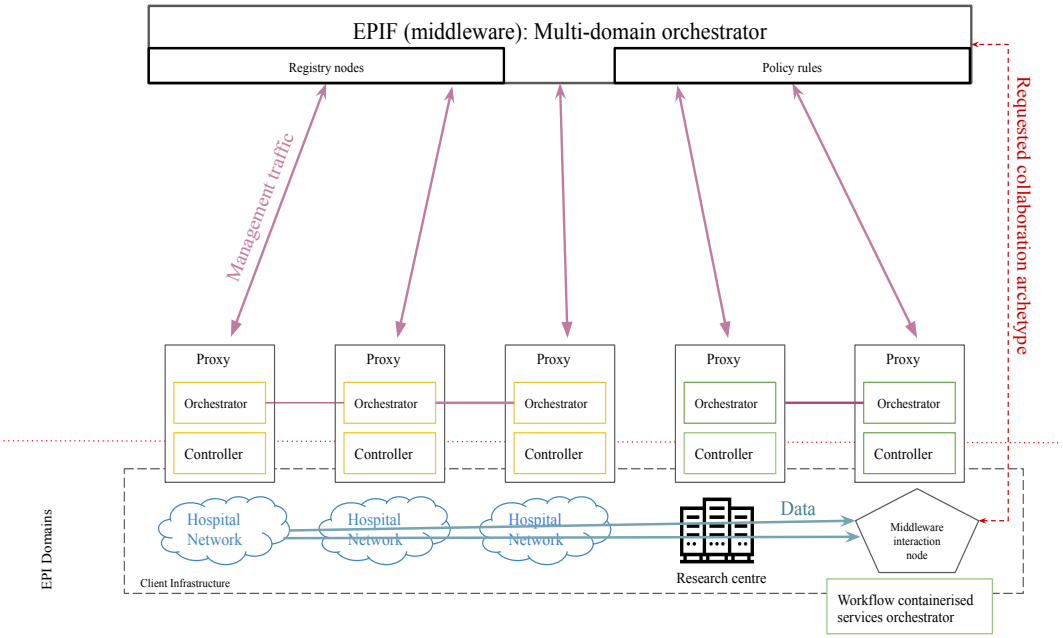

Figure 1: The EPI framework and its components to set up a collaborative environment between different EPI domains.

via the Domain Specific Language (DSL) to the MIN. The MIN communicates that to the middleware, and it matches the request with a list of actions run and bridges to instantiate.

The framework proposed in [2] will be our main focus in the ICT-Open presentation where we will discuss how to facilitate secure data sharing and support various data sharing archetypes. In the future, we will apply a healthcare-specific use case, deploy the middleware, and implement dynamic scaling and chaining of bridging containers. We plan to test and evaluate the overhead implied with this method. The limitations that we foresee encountering are mainly: acceptability of the framework by health institutions, and the lack of bridgeability of some security functions. We address the first concern by working closely with healthcare institutions, ethical boards, and hospital IT experts.

References

[1] FERRER, E. C., RUDOVIC, O., HARDJONO, T., AND PENTLAND, A. Robochain: A secure data-sharing framework for human-robot interaction. *CoRR abs/1802.04480* (2018).

[2] KASSEM, J. A., DE LAAT, C., TAAL, A., AND GROSSO, P. The epi framework: A dynamic data sharing framework for healthcare use cases. *IEEE Access 8* (2020), 179909–179920.

[3] MIAO, Y., TONG, Q., CHOO, K. R., LIU, X., DENG, R. H., AND LI, H. Secure online/offline data sharing framework for cloud-assisted industrial internet of things. *IEEE Internet of Things Journal 6*, 5 (2019), 8681–8691.

[4] SHEN, J., LIU, D., SHEN, J., LIU, Q., AND SUN, X. A secure cloud-assisted urban data sharing framework for ubiquitous-cities. *Pervasive and Mobile Computing 41* (2017), 219 – 230.