SARDIN

Secure and Accountable Results-sharing with Data-minimization and Integrity-protected Network

Project Summary

Healthcare providers, researchers, and innovators need to share data, but there is still no national infrastructure that can support this. It is difficult to access data, scale up projects, and use data-driven methods. At the system level, the challenges are a lack of interoperability between systems and organizations. In addition, it is unclear in today's legislation how one may share and use healthcare data for research and development.

The European Commission is working on a new legislative proposal, the European Health Data Space (EHDS), which is intended to address many of these challenges.

Therefore, the SARDIN project focuses on the following questions:

- How do we build a platform that enables the use of healthcare data in a secure way?
- How do we design our solution so that it is adapted for the future EHDS legislation?

Project time-line:
Nov 2023 till Nov 2025

Total budget:
10.8 million SEK

Related project:
- HEIDA
- SID
- LeakPro

Contact: Anneli Nöu, Hanna Svensson, Johan Kristiansson, Rickard Brännvall, RISE

Objectives

The SARDIN project aims to enhance privacy and data security in healthcare data sharing through the development of the Health Data Bank. This platform leverages a network of edge nodes, each controlling how local data is used. Important legal questions that therefore need to be investigated within the project are when aggregated results can be considered as anonymized, and what legal basis the use of personal data in research needs to have, and how it changes with EHDS.

Technology stack

The platform leverages the following technologies:

- **Decentralized Data Analysis** that only shares results, not the personal data itself.
- **Cryptographic Signing** for all data processing to ensure it is appropriate and secure.
- **Data Wallet** is used to manage individual consent for data use, enhancing user control and privacy.
- **Privacy Enhancing Technologies** secure aggregation and differential privacy with strong privacy guarantees
- **ColonyOS;** an open-source meta-OS (see below)

Design principles

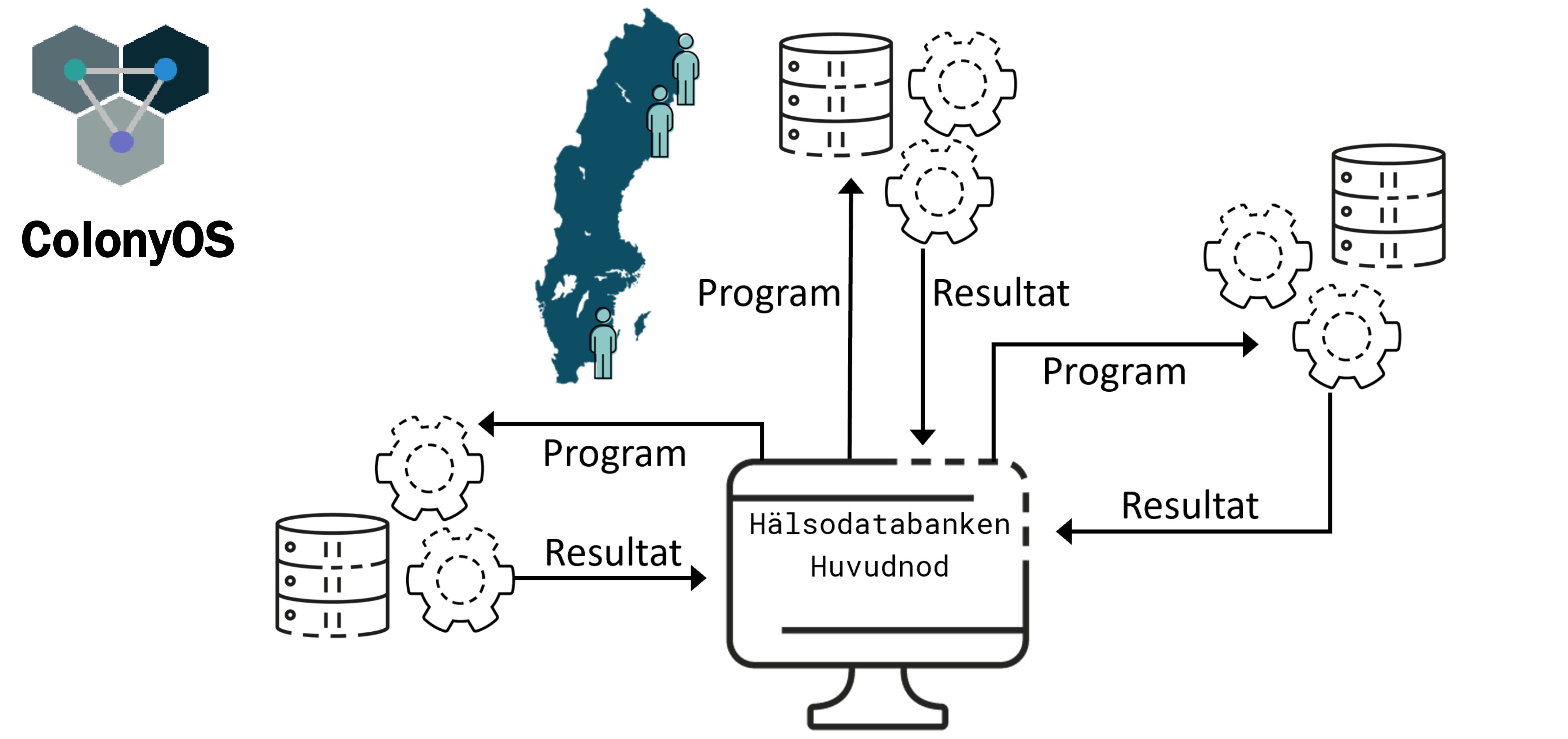
The architecture strives to meet privacy-by-design principles:

- **Data minimization** for using and sharing personal data.
- **Storage minimization**; encrypted data and decryption keys are deleted at end of processing task lifetime
- **Purpose limitation** such that personal data may only be used for explicit, approved purposes.
- **Transparency and accountability**; all activities handling data are logged so that follow-up is possible.
- **User empowerment** such that data subjects can control what their data is used for.

Projectpartners

Högskolan Kristianstad · iGrant.io · Nordic Health Innovation · RI.SE · SeeWound · Registercentrum Norr · region västerbotten · Region Östergötland

ColonyOS: The Health Data Bank platform is built on ColonyOS, an open-source research project developed by RISE to enable implementation and deployment of distributed applications. It operates as an overlay on top of existing platforms and operating systems, bridging the gap between various computing environments enabling secure and trusted execution of cross-platform workflows. This capability can be used to hide or abstract away the complexity of underlying platforms and streamline the execution of workloads across the edge network at the health care provider.



Only program code and encrypted aggregate results are communicated over the network, while source data remains at the edge node that is controlled by the health care provider.

Privacy by design · **Distributed processing** · **Empowerment**