Secure Sharing of Health Data

Research description of the VINTER, DELFIN, and HEIDA projects.

Helena Linge and Rickard Brännvall,
RISE Research Institutes of Sweden

VINNOVA
Sweden's Innovation Agency

Medical Informatics Europe
MIE 2023
EFMI

This research plan explores the use of integrity preservation in health-related data sharing. Secure and accurate data sharing can improve healthcare delivery, governance, and commercial offerings, while maintaining societal trust.

Data sharing between providers and outside traditional healthcare settings holds great potential. Legal boundaries are a challenge in health information exchange. Compliance with regulations like GDPR and HIPAA presents interoperability challenges. Privacy-by-design solutions may be necessary to maintain social trust in new digital analytical health services.

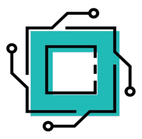
VINTER PROJECT: Diabetes self-care with privacy preservation

- Assume a third-party that offers a superior service from the cloud
- Encrypted personal data is sent from device, e.g. blood glucose, carb intake, physical activity
- Homomorphically processed results sent back t o user as risk scores or gamified advice
- Winner of the infrastructure class in Vinnova competition Vinter 2021-22

HEIDA PROJECT:

- Privacy-by-design solutions for third-party cloud-based digital services
- FHE enhanced federated learning
- Investigating business models for implementation with two public sector healthcare entities in western Sweden

DELFIN PROJECT:



- Pre-study to build a large-scale demon-strator for system change in using health data
- Exemplify the value of a unified infrastructure where data can be accessed and analyzed by many different parties
- Initial focus relates to foot ulcers, a preventable complication of diabetes

Advanced privacy preservation technologies can enable applications not previously feasible due to legal considerations It is however necessary to explore the technical circumstances and how behaviors, policies, regulations, infrastructure, and markets need to be changed for data sharing with integrity preservation to be practiced

Fully Homomorphic Encryption (FHE) is an emerging technology that enables privacy preserving cloud services. Our research explores what kind of applications are feasible in the near future?

The set-up is similar to a conventional cloud service with the exception that the secret decryption key doesn't have to be shared.

- Quantum computer proof cryptology
- Prevents unintended secondary use
- Data life-cycle privacy guarantees

Computationally demanding

- Orders of magnitude slower execution
- Large data file size and key size
- Manage noise accumulation

Scalable performance

- Homomorphic processing of one hour of blood glucose measurement data takes 30 s.
- A single 24 core server can serve 1500 users at an annual cost of about $2 per user.

FHE enhanced federated learning

- Swedish agency for privacy protection (IMY) evaluated federated learning between healthcare providers
- Explore the privacy/utility trade-off with Privacy Enhancing Technologies
- Numerical experiments with Differential Privacy (DP) and Homomorphic Encryption (FHE)
- Discuss how to navigate the regulatory context and enable an AI leap in Swedish healthcare while maintaining data protection.

Other applications

- Remote Monitoring and Control
- Occupancy detection by encrypted filter
- Private localization by encrypted geo-fencing

Conclusions

- Homomorphic encryption enables cloud services with strong privacy
- The technology is appropriate for certain high value applications of low to moderate complexity
- While inference is feasible, the training of AI models on encrypted data is still very challenging
- FHE is a promising privacy-enhancing technology in combination with federated learning
- Results for DP are inconclusive. Sometimes very unfavourable privacy vs utility trade-off

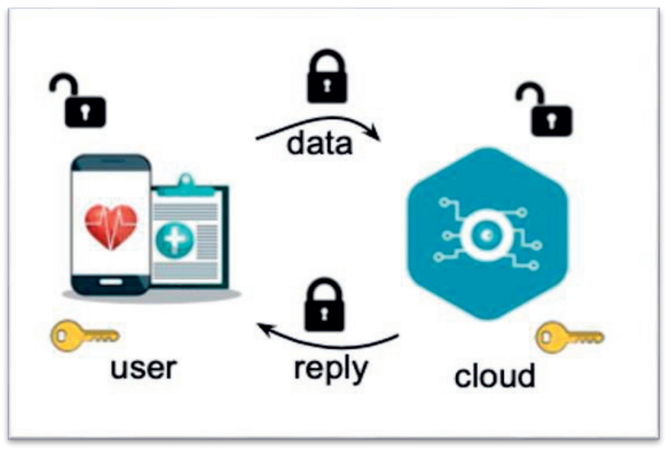


Fig 1. Conventional solution where cloud must have the key. Data encrypted only in motion.

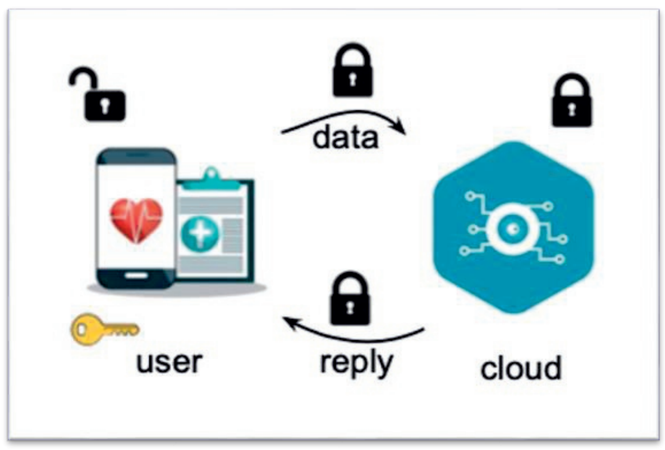


Fig 2. The cloud can process homomorphic encrypted data without access to the key.

On-going work at RISE

- Collaboration with two regional health care providers on personal data protection
- Investigate new neural network architectures that execute more efficiently under encryption
- Develop open-source software library with building blocks for data and key management
- Natural language processing applications
- Explore synergies between different advanced privacy preserving technologies
- Privacy vs Energy trade-off
- Near-to-market as well as cutting-edge

We wish to collaborate with businesses or public sector actors to explore precision-performance trade-offs and derive value from data

ABOUT RISE

- Sweden's research institute and innovation partner.
- Independent, State-owned research institute.
- 3100+ employees and over 130 testbeds.
- Innovation support, research, and certification

RISE Research Institutes of Sweden
www.ri.se / info@ri.se

CONTACT
Rickard Brännvall, Senior Researcher in Applied AI,
Department of Computer Science, Digital Systems division

rickard.brannvall@ri.se

RI.SE