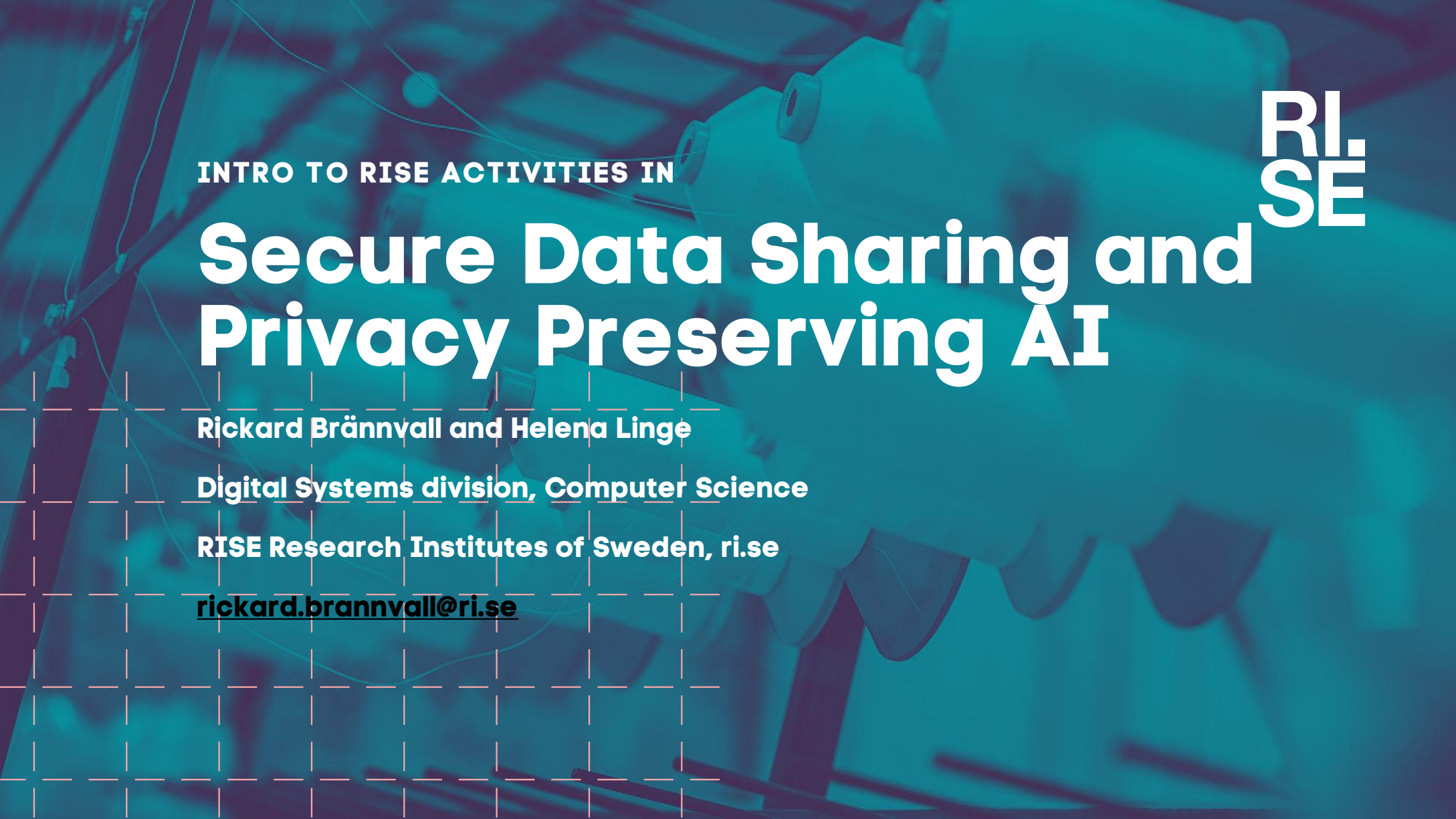


INTRO TO RISE ACTIVITIES IN

Secure Data Sharing and Privacy Preserving AI

Rickard Brännvall and Helena Linge

Digital Systems division, Computer Science

RISE Research Institutes of Sweden, ri.se

rickard.brannvall@ri.se

Outline

- Who are we
- Why is privacy important
- Two use cases
- The technology
- The start..
- The HEIDA project
- Progression of projects
- How to engage
- Q&A

Medtech 4Health

VINNOVA
Sweden's Innovation Agency

Data sharing with preserved integrity for patients, health care providers and service providers

- RISE in cooperation with MedTech4Health is calling all small and medium sized companies in the health data community for a lunch seminar on homomorphic encryption. Catch up on how this technology, contributes to enabling end-to-end privacy protection for digital services, and help us understand what it could mean for the business development of your company.

RI. SE

About RISE RESEARCH INSTITUTES OF SWEDEN

RISE is

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

Digital systems division includes

- Cybersecurity, Applied AI and Privacy-enhancing technologies
- Digital health innovation and solutions for data sharing
- Partnership with private enterprise and public sector
- Wide experience of national, EU, and international projects.

RI.
SE

Helena Linge

- Senior researcher, RISE
- Associate professor Molecular Medicine Lund university
- Currently Strategist FoU Region Halland
- Previously co-founder and CEO of Concidera Health, medical follow up using health data
- Previously developer of area AI in Health care @AI Sweden

rickard.brannvall@ri.se

Rickard Brännvall

- Senior Researcher in Applied AI
- Background in Physics and Finance
- RISE Research Institutes of Sweden Computer Science, Digital Systems, ri.se
- www.ri.se/en/person/rickard-brannvall

RI.
SE

A changing regulatory landscape

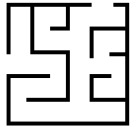
- GDPR, Data act, AI act, EHDS, SOU Sekundäranvändning av hälsodata
- Regulators are currently investigating how privacy enhancing technologies (PETs) can unlock the potential of data-driven applications.
- IMY, DIGG, e-Hälsomyndigheten on Swedish Government directive
- Regulatory sandboxes for exploratory, dialogue-based guidance
- "Decentralized AI in Healthcare – Federated Machine Learning between Two Healthcare Providers" by IMY together with AI Sweden, Sahlgrenska sjukhuset, and Region Halland.

Privacy legislation protects the individual

Here we consider the principles:

- **Purpose limitation:** Only collect personal data for specified, explicit, and legitimate purposes and process in a way compatible with those purposes.
- **Data minimization:** Personal data must be adequate, relevant, and limited to what is necessary for the purposes.
- **Storage limitation:** Personal data must not be kept for longer than necessary for the purposes for which it is processed.

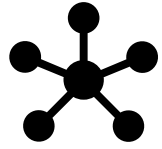
Två användarfall



Tjänster med inbyggt integritetsskydd

- Algoritmen (IP) ligger skyddad i molnet under ägarens kontroll.
- Användardata förblir krypterad. (end-to-end privacy protection)

Möjliggörs med homomorf kryptering.



Utökat skydd vid federad inlärning

- Krypterad aggregering av resultat utan att datamängder delas.
- Dataminimering, ändamåls- och datalagringsbegränsing.

Förstärks med homomorf kryptering.

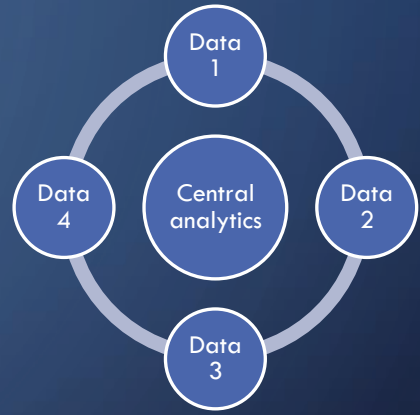
RI.
SE

Integritetsskydd vid datadelning eller analys av hälsorelaterad data

-Olika tekniker har olika användningsområden-

Block chain

Federated learning

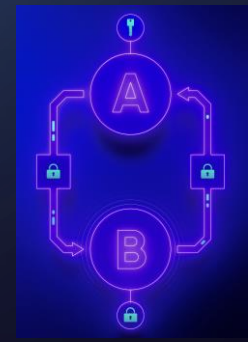


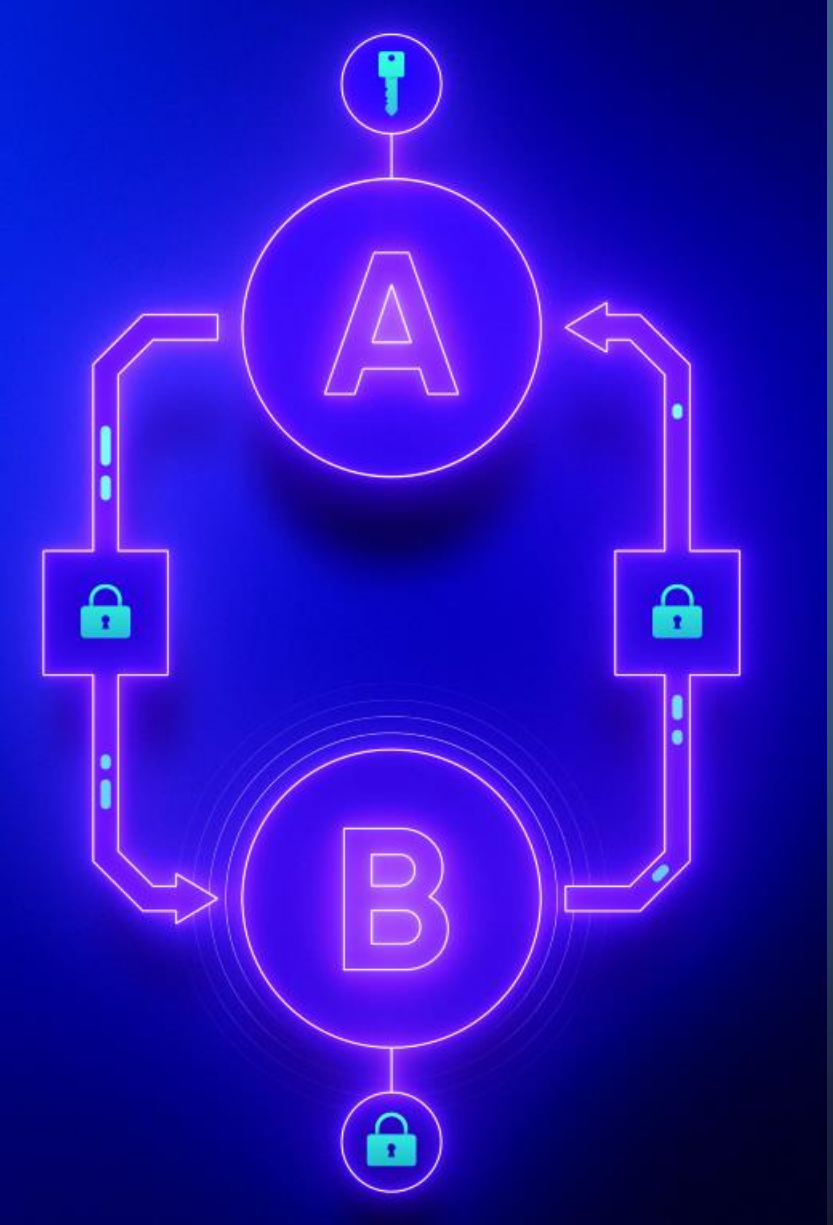
Trusted Execution Environments

Multi-party Computation

Differential privacy

Homomorphic encryption





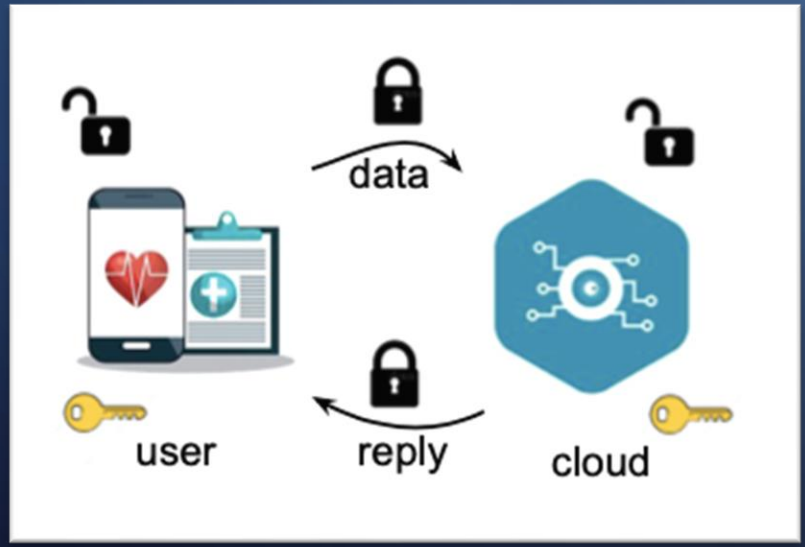
HOMOMORF KRYPTERING

- Skyddar data under beräkning
- Skyddar IP av algoritm hos tredje part.
- Kvant-dator säkrat
  - Bygger på matematiska problem som är mycket svåra att lösa
- Begränsar sekundär dataanvändning

C. Gentry, “Computing arbitrary functions of encrypted data,” Communications of the ACM, vol. 53, pp. 97–105, mar 2010.
D. Augot et al., “Initial recommendations of long-term secure post-quantum systems,” 2015.

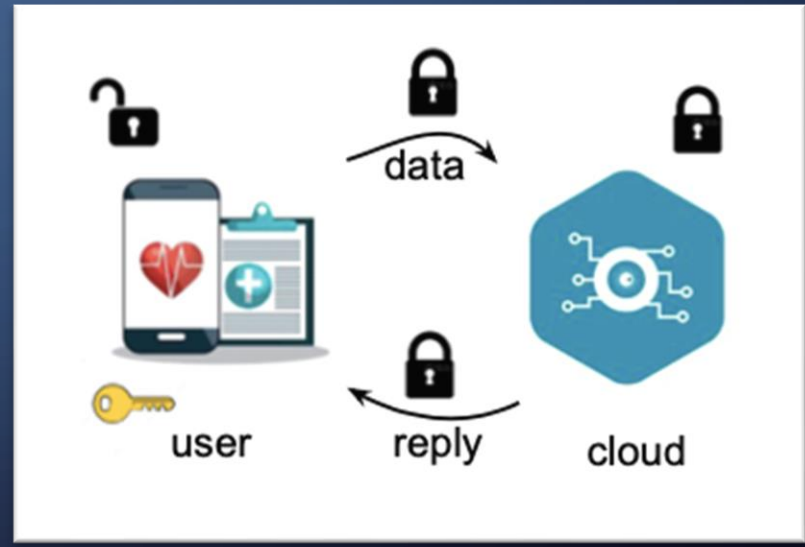
Konventionell lösning

- data krypterad i vila och i rörelse, men inte under beräkningar
- användare måste lita på molnet med den hemliga nyckeln

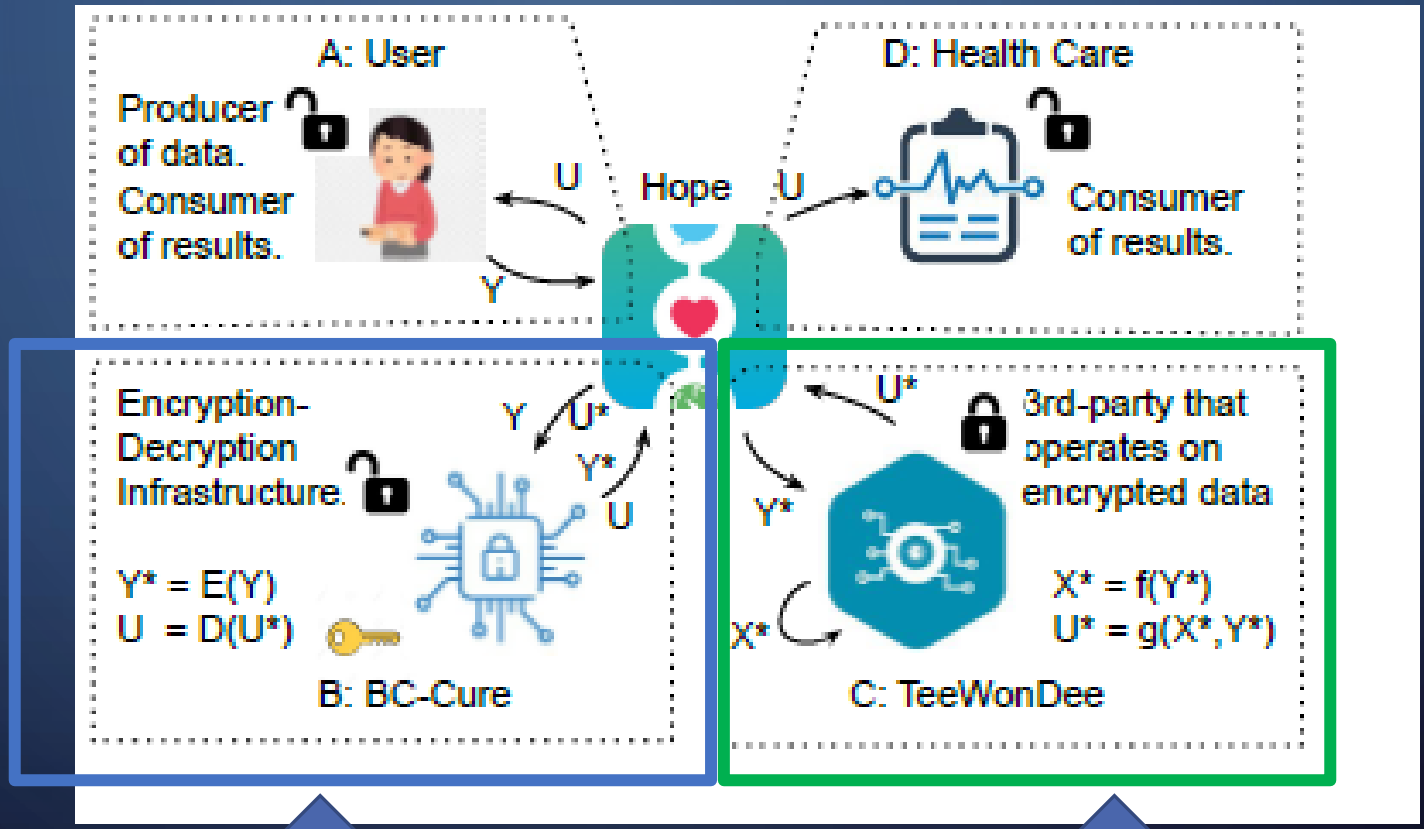


Homomorfisk kryptering

- data krypterad också under beräkning
- data och resultat är inte tolkningsbara för molnet eller nyfiken part




VINTER
INNOVATION MED HÄLSOD



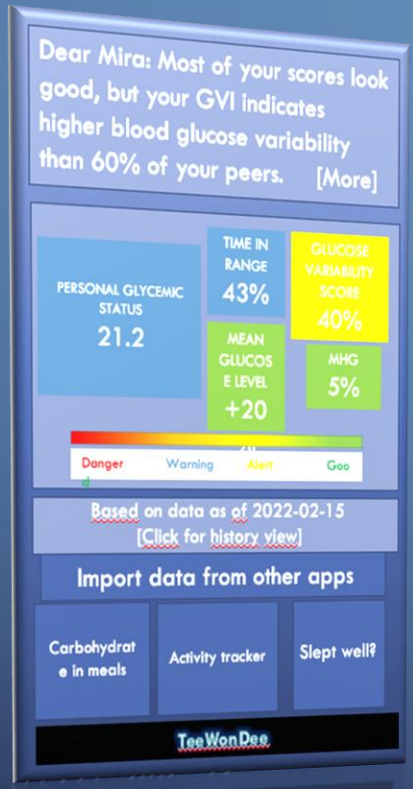
VÅRT BIDRAG TILL VINTER

FÖR ATT KUNNA VISA UPP EN TJÄNST SOM MÖJLIGGÖRS AV VÅRT INFRASTRUKTURBIDRAG

Vad är RISE roll i datadelning?

- Nyckelhantering
- Kontroll på datas livslängd
- Verka för interoperabilitet

GÅR DET INTE FÖR LÅNGSAMT?



Blodglukosvärden (1 timme)		30-60 sekunder
24 core server		1500 användare
Årlig kostnad		SEK 22 per användare

TABLE IV

DATA TYPE READINESS

Data type	Examples	Comments	Readiness
Numerical data	- Weight and height - Blood glucose level - Activity measurements - Diet composition - Numerical patient records	Scalar or low dimensional data	Early adaptors (2022).
Categorical data	- Diagnose categories - Disease management - Other patient records	Discrete categories and enumerations	Early adaptors (2022).
Images	- T1D foot status - T1D eye status - X-ray, MRI, CT, etc	Very large data volumes unless resolution is limited. Large deep learning models required.	Proof of concept [16]. On the horizon (2025).
Video	- Live monitoring - Gait, emotional state, etc	Extremely large data volumes. Very large models required.	Not feasible today.
Free text	- Q&A chatbots - Mental haelth bots - Free text patient records	Unstructured free text has unknown length. Requires very large models and large vocabularies.	Proof of concept [24]. Very challenging.

A. Qaisar Ahmad Al Badawi et al., "Towards the alexnet moment for homomorphic encryption: Hcnn, the first homomorphic cnn on encrypted data with gpus," IEEE Transactions on Emerging Topics in Computing, pp. 1–1, 2020.
A. A. Badawi et al., "Privft: Private and fast text classification with homomorphic encryption," IEEE Access, vol. 8, 2020.

RI. SE

VINNARE I KATEGORIN INFRASTRUKTUR I INNOVATIONSTÄVLINGEN VINTER:

RISE Research Institutes of Sweden AB

ENCRYPTED HEALTH AI

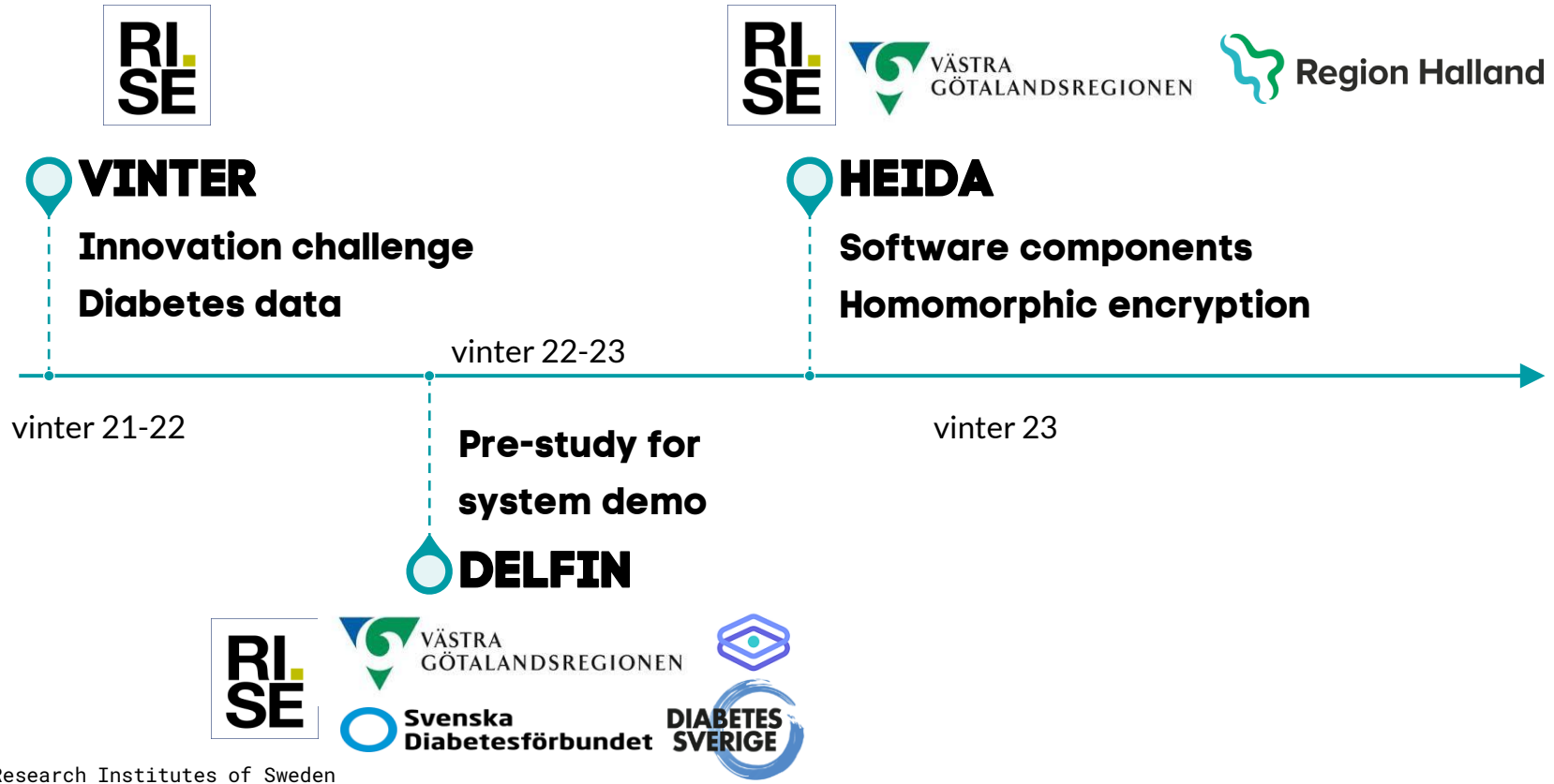
Med en lösning som skänker lugn och tillit både till personer med diabetes och lagstiftare, skyddar man innovatörers algoritmer och begränsar obehörig delning eller bearbetning av data. Den föreslagna infrastrukturen kan såväl förenkla förändring av lagstiftningen som bli ett framtida byggblock i den förvaltningsgemensamma infrastrukturen.

Grattis RISE för Encrypted Health AI!

Darja Isaksson, generaldirektör Vinnova

VINNOVA

Project progression



HEIDA: HOMOMORPHIC ENCRYPTION FOR INTEGRITY PROTECTION IN DATA SHARING ACTIVITIES WITH HEALTH DATA

Målbild

- Utveckla mjukvaruexempel för homomorf kryptering av hälsodata
  Öppen källkod med fokus på praktisk användning
- Affärsmodeller och juridik kring teknik för inbyggt integritetsskydd
  (även i kombination med exv federerad inlärning)

IMY federated learning sandbox

Question 1: Is there a legal basis for the local processing of personal data?

Yes, for development of operations.

Question 2: Does personal data disclosure occur in federated machine learning?

Yes, there is a risk.

Question 3: Is there a legal basis for the disclosure of personal data between healthcare providers?

It depends.

KOMPLEMENTERANDE INTEGRITETSSKYDD

Homomorf kryptering

- Kryptografiskt dataskydd
- Tvåpartslösning, till exempel en molntjänst som levererar analys av en individs hälsodata (**primäranvändning**)
- Skyddar även algoritmen (mot reverse-enginering)
- Säker nyckelhantering viktig
- **Lämplig när AI tjänst levereras!**

Federerad inlärning

- Minimerad datadelning
- Federation av dataägare som gemensamt tränar ett AI verktyg för analys av hälsodata (**sekundäranvändning**)
- Alla i federationen får del av modellen (men ej andras data)
- Koordinerande roll är speciell
- **Lämplig när AI tjänst utvecklas!**

Project progression

VINTER

Innovation prize

Diabetes data

HEIDA

Software components

Homomorphic encryption

LEAKPRO

Build testbed for privacy attacks

Pre-study for system demo

DELFIN

Prototype platform

Distributed analysis

SARDIN

m fl

Integrate health data

Centralized platform

HDIP

vinter 21-22

vinter 22-23

vinter 2024 and forward

SARDIN

Systemdemonstrator

Analys

Resurseffektivitet

Datadelning

Integritetsskydd

Nyttiggörande

Pågående projekt

HEIDA

Sjyst data!

TEF Health

Crane

Rehabkompassen®

TEHDAS

Projektkonsortium

Region Östergötland

RI. SE

Högskolan Kristianstad

NORDIC HEALTH INNOVATION

region västerbotten

iGrant.io Your data, your choice.

Medicinsk teknik-FoU

Neuro-huvud-hals centrum

Norrlands Universitetssjukhus

Registercentrum Norr

SeeWound

Dermacut

Referensgrupp

VÄSTRA GÖTALANDSREGIONEN

eHälsomyndigheten

Socialstyrelsen

sfmi SVENSK FÖRENING FÖR MEDICINSK INFORMATIK

TechSverige

region västerbotten

Glesbygdsmedicinskt centrum, GMC

RI. SE region västerbotten Registercentrum Norr Region Östergötland Högskolan Kristianstad iGrant.io NORDIC HEALTH INNOVATION SeeWound

Secure Sharing of Health-Related Data: Research Description of the VINTER, DELFIN, and HEIDA Projects.

Linge HM, Brännvall R.

Stud Health Technol Inform. 2023 May 18;302:143-144. doi: 10.3233/SHTI230087.

PMID: 37203632

HEIDA: Software Examples for Rapid Introduction of Homomorphic Encryption for Privacy Preservation of Health Data.

Brännvall R, Forsgren H, Linge H.

Stud Health Technol Inform. 2023 May 18;302:267-271. doi: 10.3233/SHTI230116.

PMID: 37203660

RI.
SE

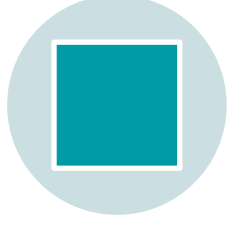
Comments, feedback, questions…

6 survey questions eagerly await your response

… **THANK YOU!**

FOR HOMOMORPHIC ENCRYPTION
RICKARD.BRANNVALL@RI.SE

FOR SARDIN,
ANNELI.NOU@RI.SE



FOR TEF
ALIREZA.SALEHI@RI.SE