Complex Cyber Infrastructures and AI for the Financial Industry

Sander Klous
Professor in AI & Audit
Group leader Complex Cyber Infrastructures Group
Scientific Director AI4Fintech
Partner @KPMG

17-12-2024

All-hands meeting Informatics Institute





The Internet: A Federated Bus Architecture

1

Many to Many Connectivity

The internet design aims to connect multiple nodes efficiently.

2

Federated Bus Architecture

This design transformed complex connections into a bus structure without central ownership

3

Foundation for Growth

This architecture became the backbone for future technological advancements.

The World Wide Web: Democratizing Information

1

One to Many Model

The Web introduced a scalable information distribution system on top of the internet

2

Global Access

It allowed content creators to reach audiences worldwide without intermediaries

3

Information Revolution

This model democratized access to knowledge and resources.





Social Media: The Many-to-Many Paradigm

User-Generated Content

Platforms empowered users to interact with each other

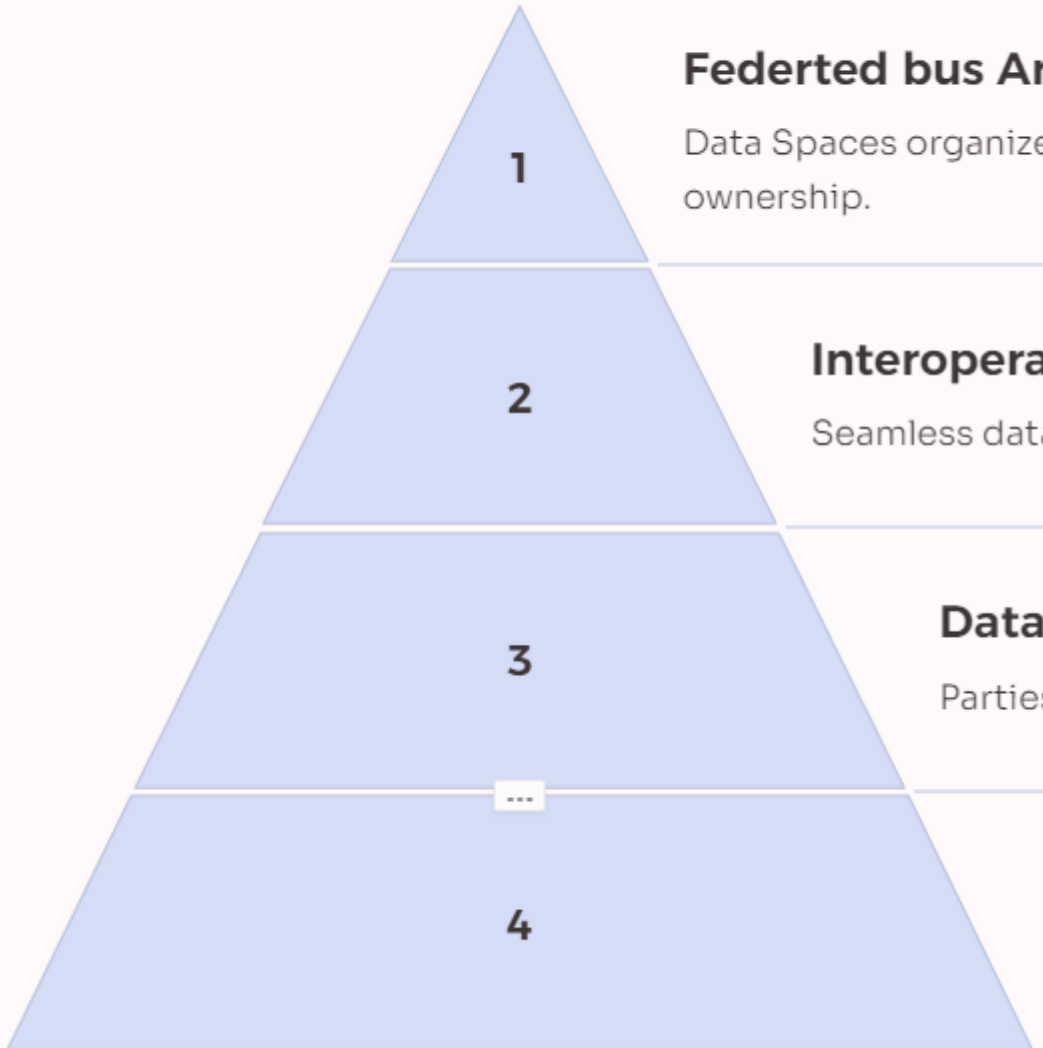
Network Effects

Connections between users amplified information spread exponentially.

Global Conversations

Facilitating real-time, worldwide information exchange

Data Spaces: The Next Frontier in Data Exchange



Federted bus Architecture for Data

Data Spaces organize information flow efficiently without centralized ownership.

Interoperability

Seamless data exchange between diverse systems.

Data Sovereignty

Parties maintain control over their data and algorithms.

Scalability

Data Spaces can grow to accommodate an increasing number of parties and data volumes.

Advanced Research Infrastructure for Data Spaces

Testbeds

Specialized environments for testing Data Space implementations are crucial. They allow researchers to simulate real-world scenarios and stress-test systems.

Research Facilities

Advanced computing facilities support Data Space development. These include high-performance computing clusters and specialized data analytics tools.

GreenDIGIT Project: Novel and Consolidating Approach
Shared Responsibility in Sustainability and Sustainability by Design

Users responsible for sustainability ***on*** the RI



Providers responsible for the sustainability ***of*** the RI

Researcher/ Project Responsibility:
Applications Development, Energy usage and KPI monitoring

Sustainability by Design Challenge

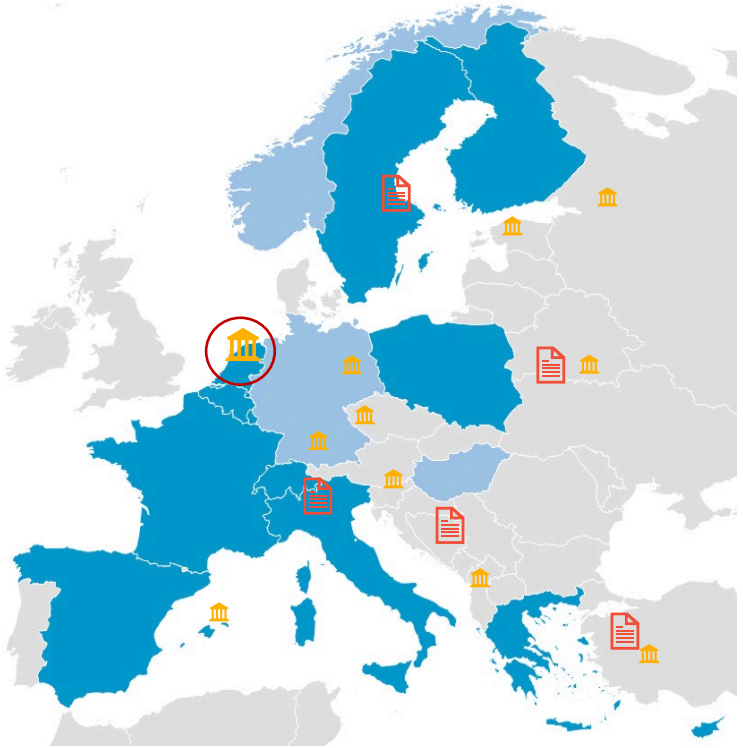
RI/Datacenter Provider/Operator Responsibility:
Monitoring Energy and environmental impact, metrics and KPI

- **Architecture for Sustainability by Design**
  - Functional components, layers, API, Requirements
- **Software and application components that can be optimised during design and controlled during operation**
  - Green aware API including necessary energy, performance, environment information
- **(!) Common information/data model and metadata (naming)**
  - Including Requirements, KPI, Metrics
  - + FAIR for Sustainability
- **RI and applications lifecycle**
  - RI lifecycle stages (concept, design, development, deployment, operation, decommissioning) and scientific workflow and research data

SLICES-RI for Research on Digital Infrastructures

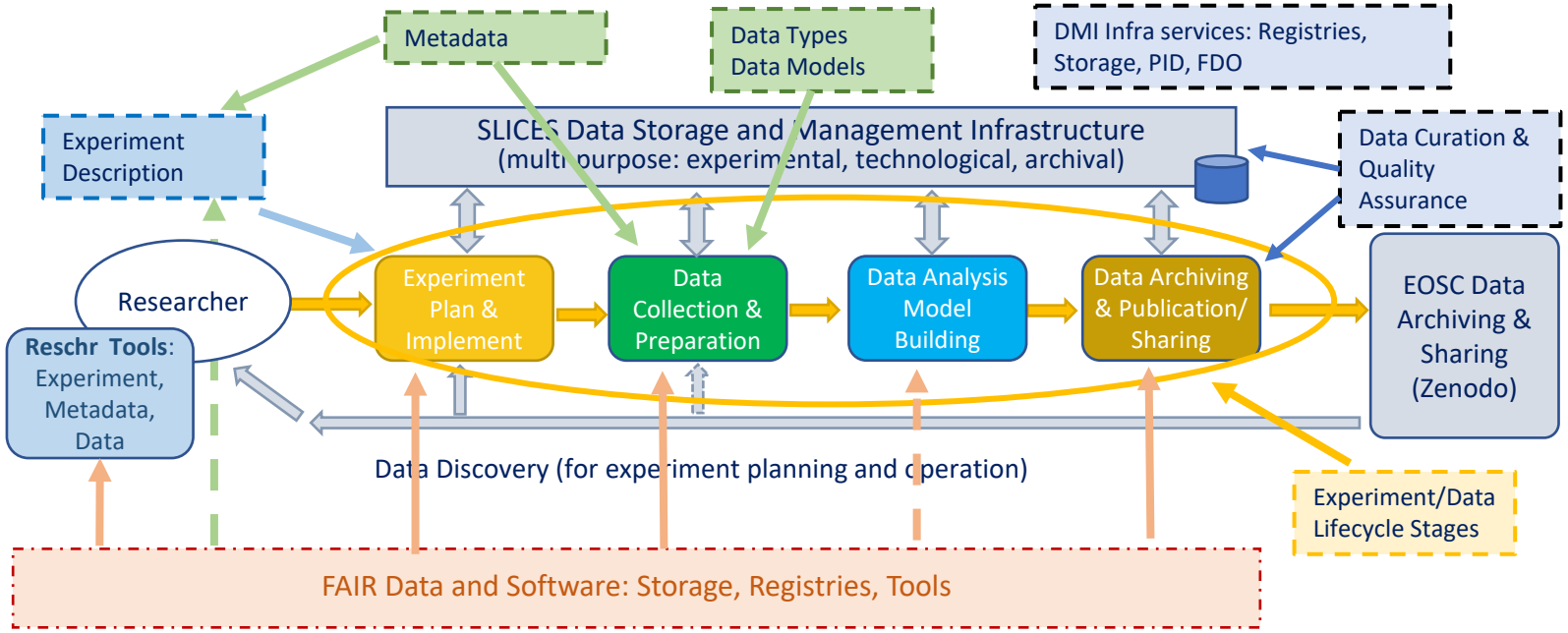
To support effective Experimental Research Automation and Data Management





Involves **25 partners** from 15 countries initiatives

- Supported by **SLICES-NL initiative** coordinated UvA
- Focused to enable **reproducible experiments and** efficient **Data Management Infrastructure**



SLICES Data Management Infrastructure for Experimental Research Reproducibility

SLICES to enable **innovation in the ICT domain**, strengthening the **impact of European research**, addressing **societal challenges**



Policy and Compliance in Data Spaces

Policy Management by Design

Data Spaces incorporate policy management frameworks from the ground up. This ensures consistent governance across the entire data ecosystem.

Compliance by Design

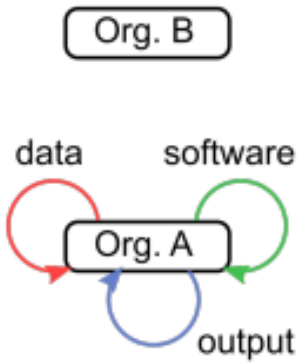
Built-in compliance mechanisms safeguard data integrity and privacy. They automate adherence to regulations like GDPR.

Adaptable Governance

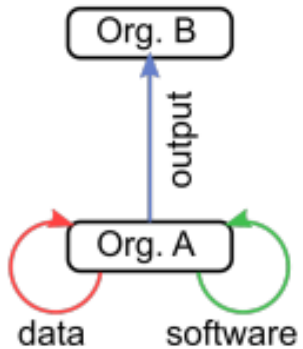
Flexible policy structures allow Data Spaces to evolve with changing regulations and contractual agreements. This future-proofs the infrastructure against regulatory changes.

Type A

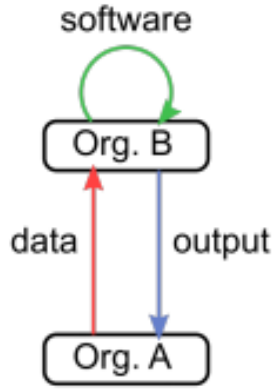
Private Operation



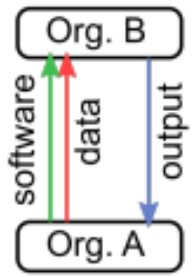
Sharing Results



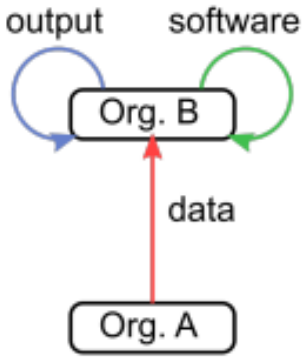
Software as a Service



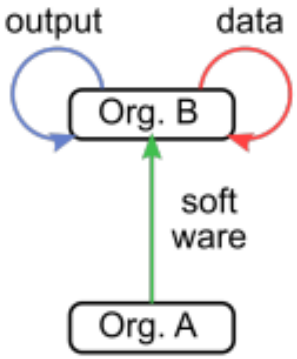
Infra as a Service



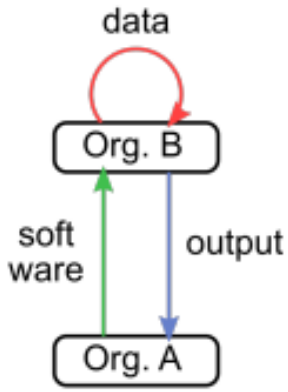
Sharing Data



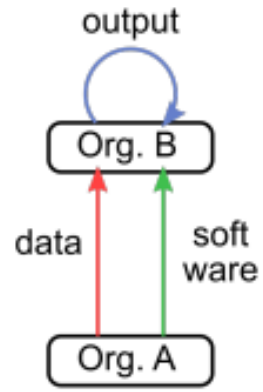
Sharing Code



Compute to Data

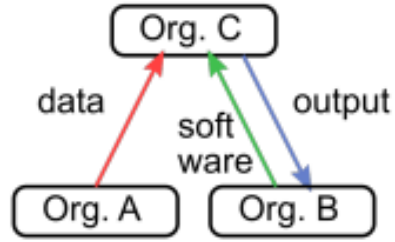


Reproducible Science

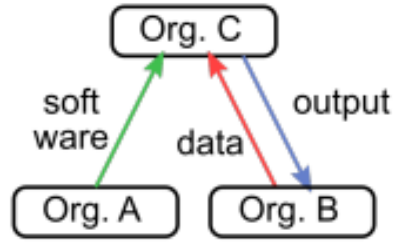


Type B

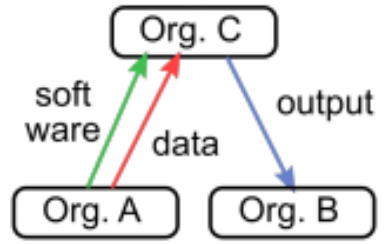
Sharing Data via TTP



Sharing Code via TTP



Share Code and Data via TTP



Topic: Analysis and control of systems via formal specifications

$$
\begin{array}{rll}
o : \mathcal{O} & := + \mid - \mid * \mid \div \mid \wedge \mid \vee \mid = \mid \neq & \text{(binary operators)} \\
e, e_1, e_2 : \mathcal{E} & := d : \Delta \mid v : \mathcal{V} \mid e_1\ o\ e_2 \mid \neg e & \text{(expressions)} \\
s, s_1, s_2 : \mathcal{S} & := \textbf{done} \mid \textbf{sync} \mid \textbf{write}\ e \twoheadrightarrow v \mid s_1\ ;\ s_2 & \text{(computation statements)} \\
& \mid \textbf{if}\ e\ s_1\ \textbf{else}\ s_2 \mid \textbf{while}\ e\ \textbf{do}\ s & \text{(control flow statements)} \\
& \mid \textbf{send any}\ (\hat{e} : \mathcal{E}^2) \hookrightarrow p \mid \textbf{recv}\ p \hookrightarrow v & \text{(communication statements)}
\end{array}
$$

$$
\textbf{send}\ e \hookrightarrow p \triangleq \textbf{send any}\ \{e\} \hookrightarrow p \qquad \textbf{loop}\ s \triangleq \textbf{while}\ 1\ \textbf{do}\ s
$$

$$
\textbf{assert}\ e \triangleq \textbf{if}\ e\ \textbf{done else (loop done)} \qquad \textbf{end} \triangleq \textbf{loop sync}
$$

Fig. 1. The syntax of PDL expressions $\mathcal{E}$ and primitive protocol(statement)s $\mathcal{S}$.

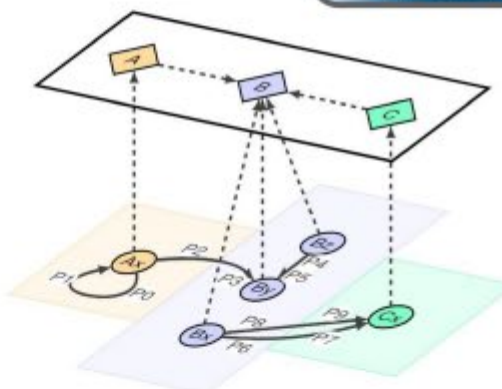
Specifications define intended / expected / possible behaviour. They can focus on parts of the system:

- High-level legal relations
- Multi-party communication protocols …

We (automatically) reason about and control software via their specifications.

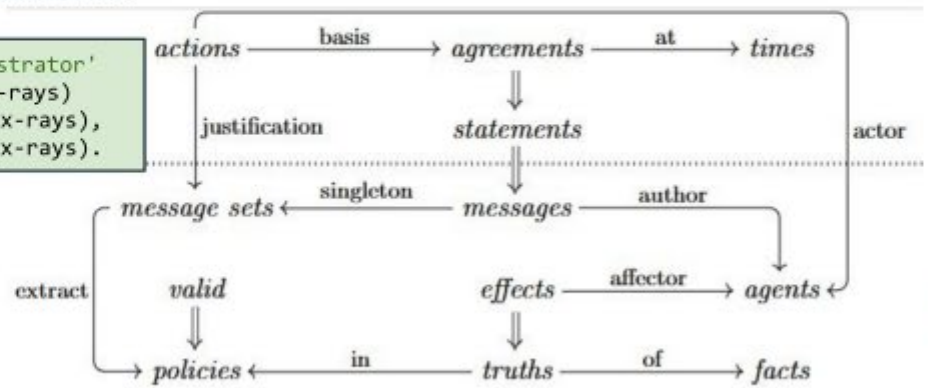
Various research lines focus on sub-problems:

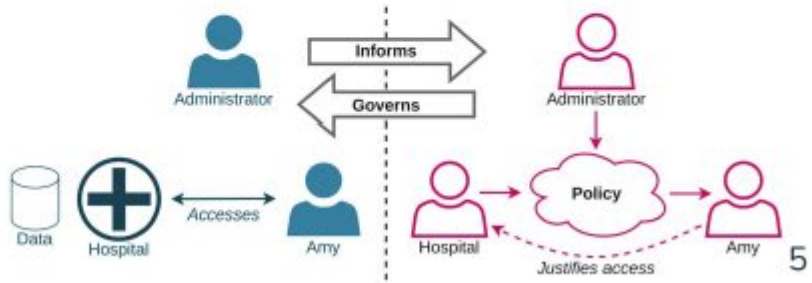
- Offline analysis
- Composition
- Communication
- Controlled change



```
% Statement 's6' authored by 'administrator'
ctl-authorises(administrator, bob, x-rays)
        :- ctl-authorises(h1, bob, x-rays),
           ctl-authorises(h2, bob, x-rays).
```

eflint





Responsible AI Integration in Data Spaces

1

Ethical AI Principles

Implement AI systems with strong ethical guidelines.

2

Transparency

Ensure AI decision-making processes are explainable and auditable.

3

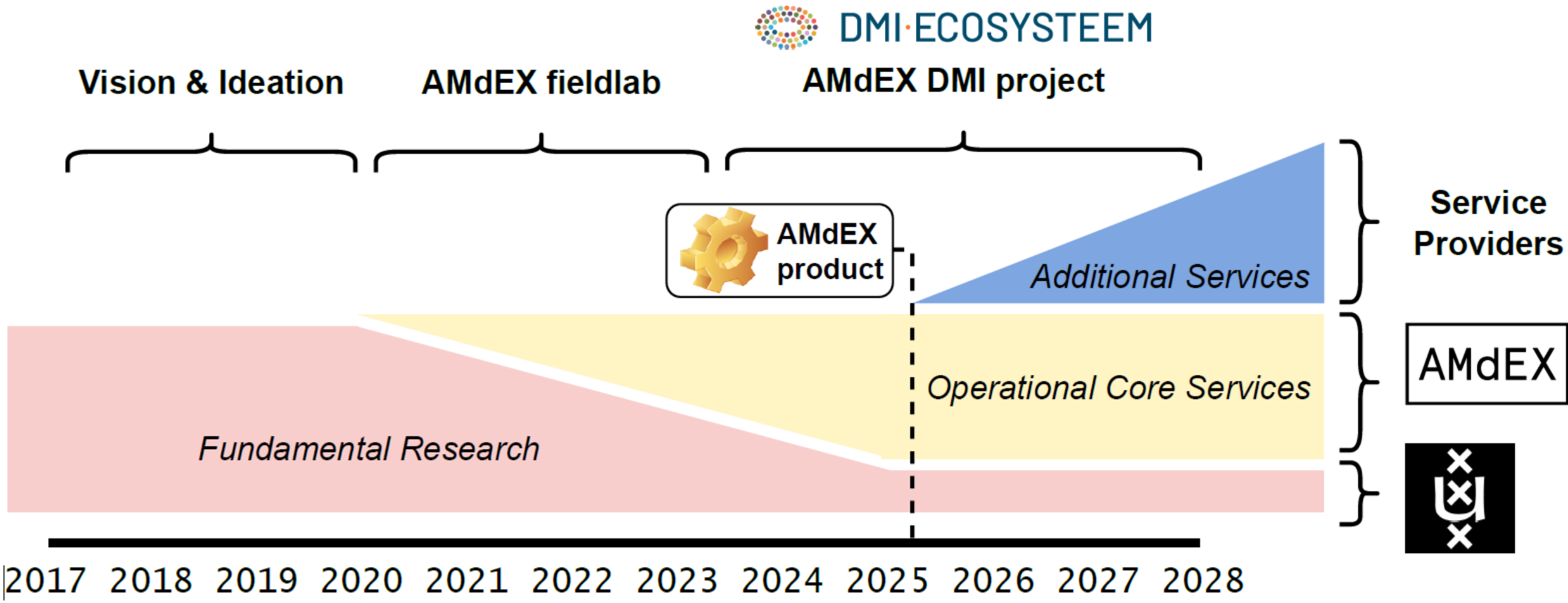
Sustainability

Design AI systems to be environmentally and socially sustainable.

4

Continuous Monitoring

Regularly assess AI performance and impact within Data Spaces.


DMI·ECOSYSTEEM
Vision & Ideation
AMdEX fieldlab
AMdEX DMI project
AMdEX product
Additional Services
Service Providers
Operational Core Services
AMdEX
Fundamental Research
2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028

Education

Broad involvement in IVI BSc programs:

- **Graduation project** coordination (per 2/3 and 5/6)
  - BSc Kunstmatige Intelligentie (140 students/year)
  - BSc Informatiekunde (110 students/year)
- New **Keerpunten Introduction Course** (IK/INF/KI)
- **Stages** BSc KI & BSc IK
- Support **coordination standardization** over **KI/IK/INF** projects
- Support for accreditation of BSc Informatiekunde 2025

CCI – research collaboration on (re-)configuration of microservices

Collaboration with HvA Maintenance Lab on cross-discipline graduation projects

UvA AI4FinTech Program

Objectives and Scope

- **AI4FinTech: Application of AI Methods and Technology to the Financial Sector**
- **Develop an ecosystem for top fundamental and applied research and education in the domain of AI4FinTech by**
  - Building on the expertise of existing groups across different faculties (Science Faculty, Economics & Business and Law)
  - Stimulating interactions between the different research groups
  - Intensifying collaboration with financial industry, start-ups and governmental institutes and other academic partners
- **Main Themes**
  - Explainability and Compliance of AI algorithms in Finance
  - Fraud detection and money laundering using AI
  - Risk management with AI and Computational/Mathematical modelling
  - Applications to Sustainable Finance
  - AI in Ecosystems

AI4FinTech

Cross-faculty PhD research projects

1. **AIDA: Artificial Intelligence for Due-diligence Analysis**

   External partners: Imprima, Zuva AI

2. **Environment, Social and Governance (ESG) regulation impact on financial stability**

   External partner: ING

3. **HyperMining: Explainable Anti-Money Laundering using Process Mining on Hypergraphs**

   External partner: ABN AMRO

4. **Knowledge-Driven Learning for XAI in Fraud Detection**

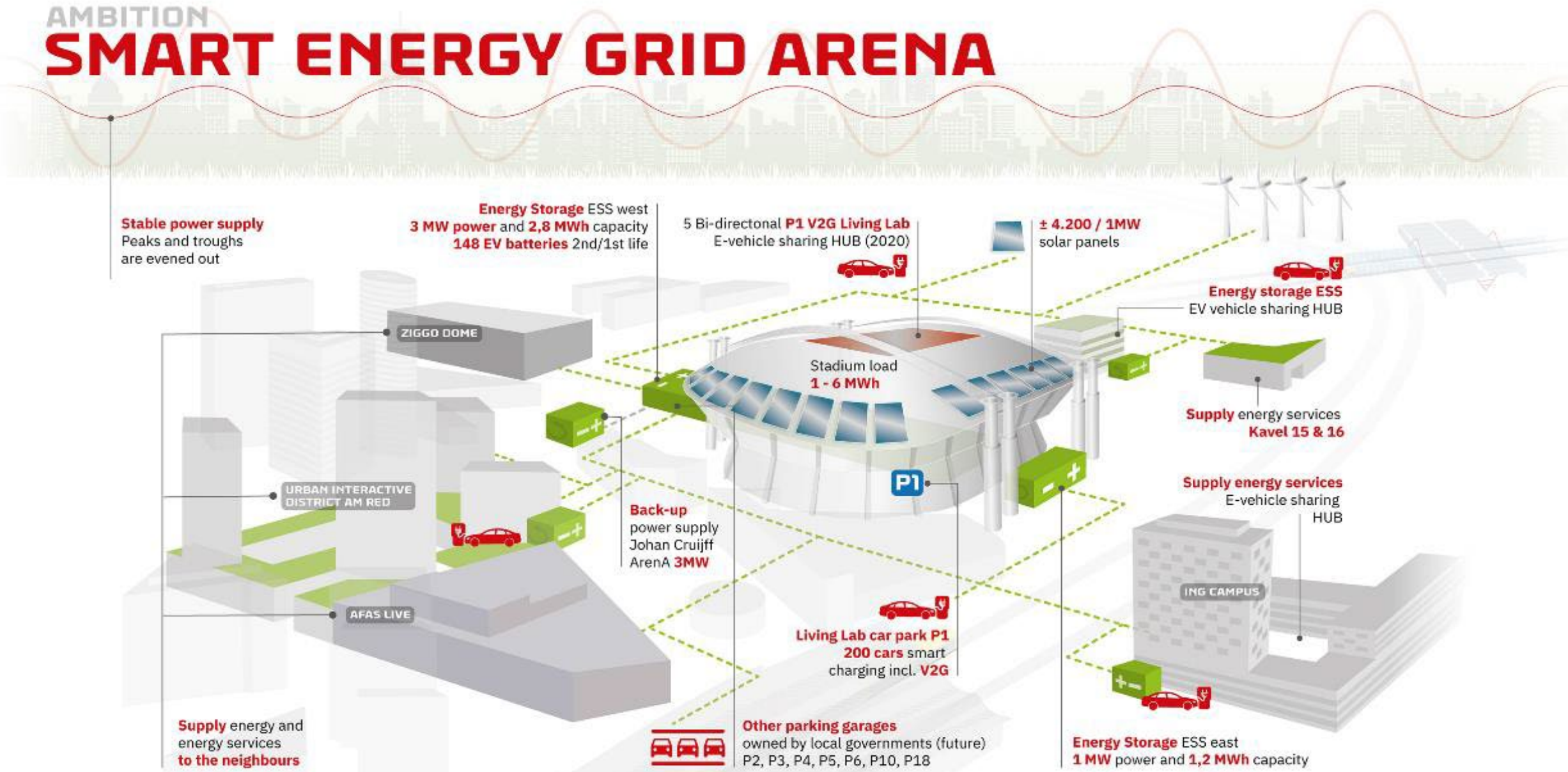
   External partners: Mollie, ING

From empowering to motivating (Xin Zhou)

JOHAN CRUYFF ARENA
Multi-domain Dynamic Policy Enforcement



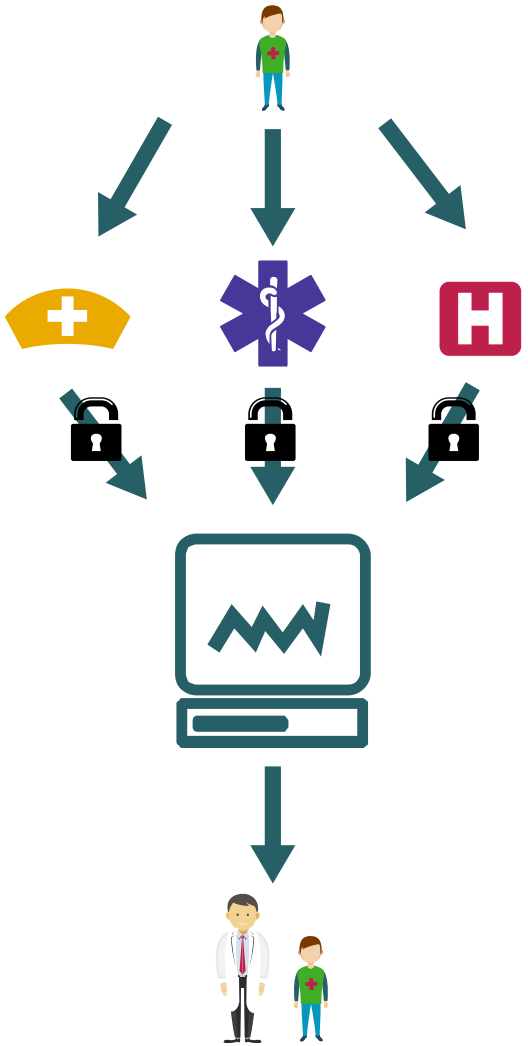
AI for Auditing and Auditing of AI



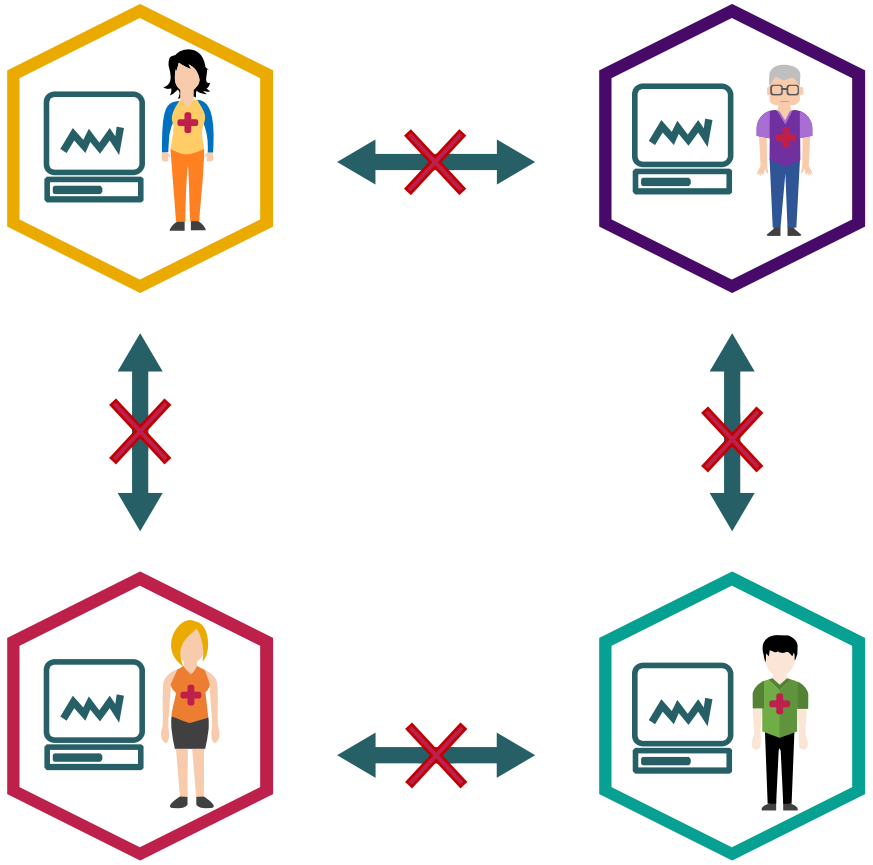
www.enablingpersonalizedintervenstions.nl

Enabling Personalized Interventions

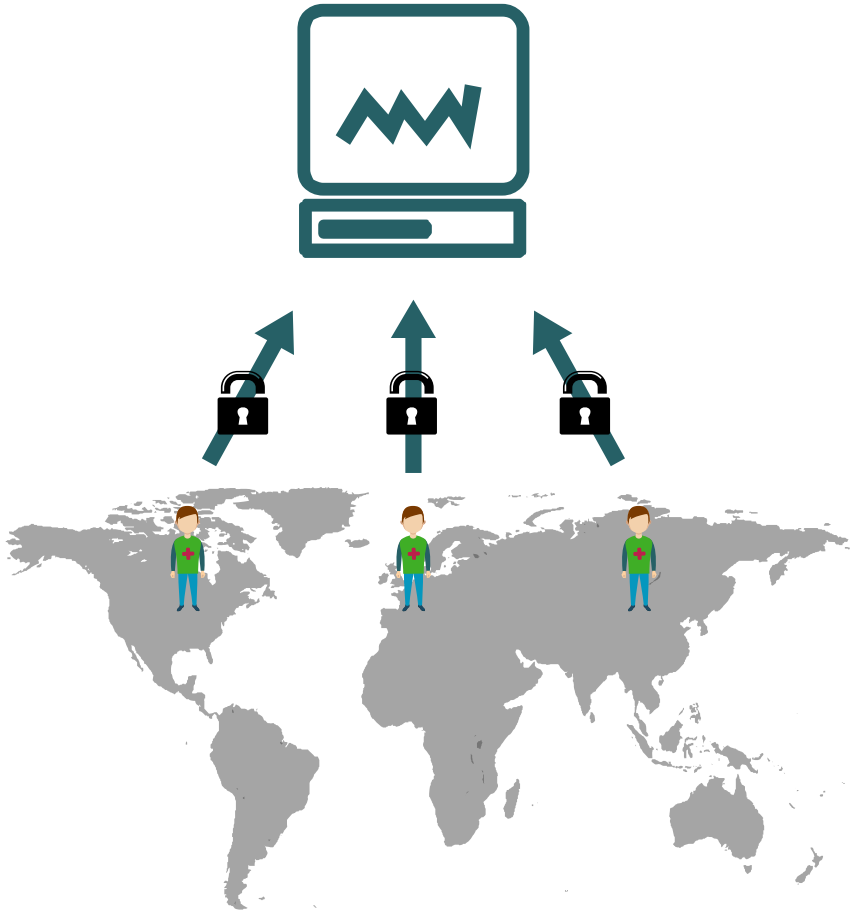
CVA



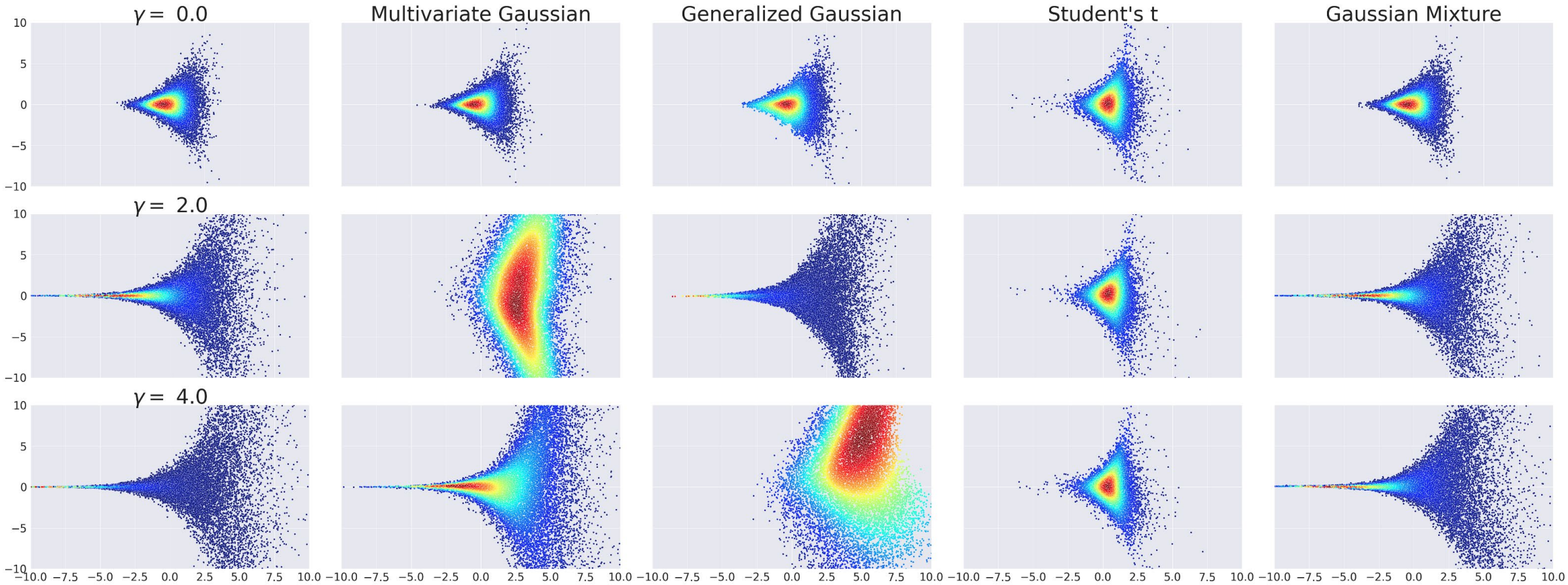
Psychiatry



DIPG



Privacy and IP in ecosystems: synthetic data



https://openreview.net/pdf?id=PbvyJ8XpNn (Saba Amiri)

Conclusion

- We are doing a lot of cool and societally relevant stuff