Securing INSPIREd geodata cloud services with CLARUS

INSPIRE conference 2016

(Barcelona)

Why cloud computing ?

- Increase flexibility
  - on-demand
  - elasticity
  - ubiquitous access
- Reduce costs
  - shared resources
  - pay as you use
  - metering
- Reduce risks
  - higher availability

The main barriers to cloud adoption

Geodata providers are often reluctant to move to the cloud

Data security

Loss of control

Data location

Solutions ?

Private Cloud

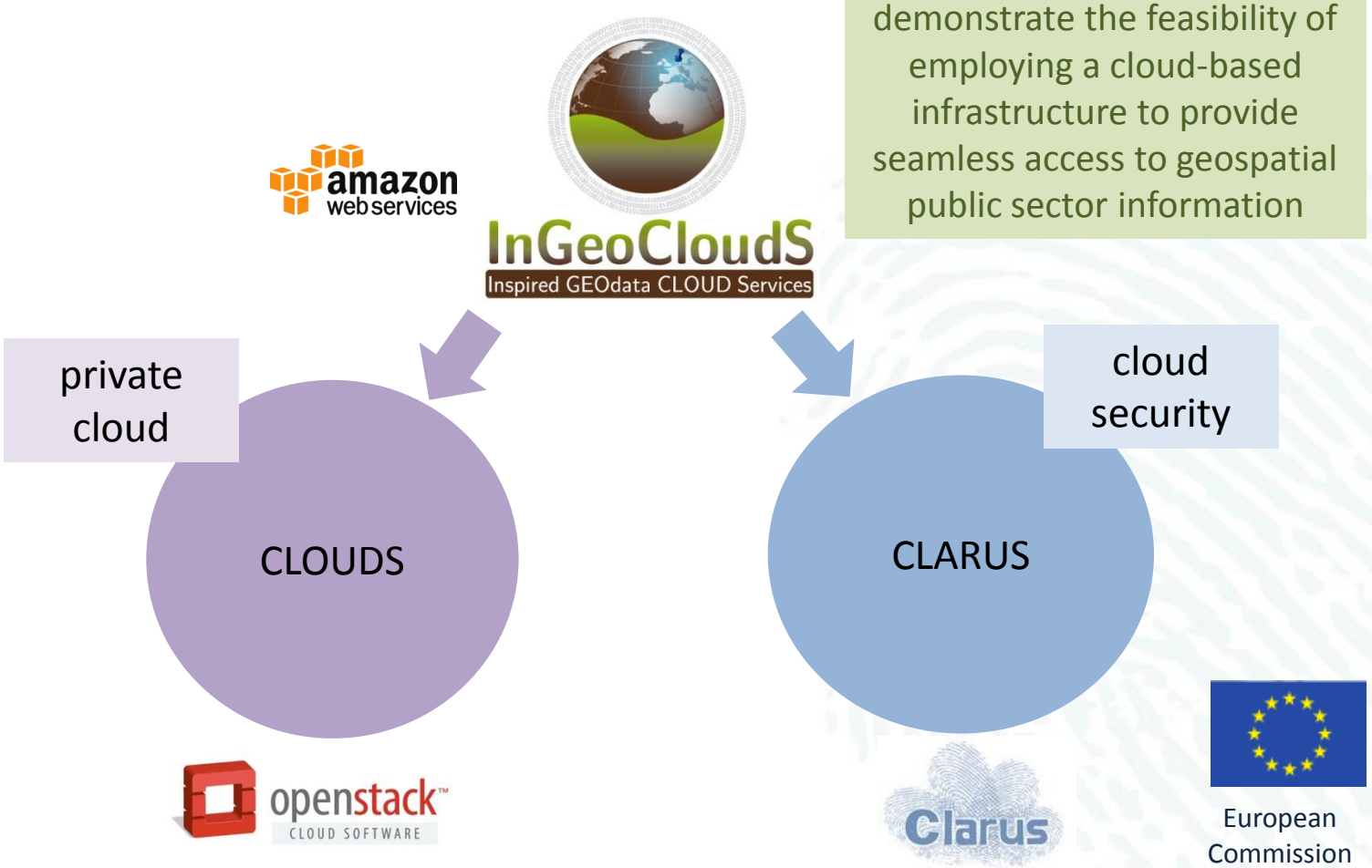
a **type of cloud computing** that delivers similar advantages to public cloud but **implemented within the corporate infrastructure**

Cloud Access Security Broker

on-premises or cloud-hosted software that acts as **a control point** to support **threat protection** and **security** for **cloud services**

AKKA Research roadmap

demonstrate the feasibility of employing a cloud-based infrastructure to provide seamless access to geospatial public sector information



European Commission H2020 programme

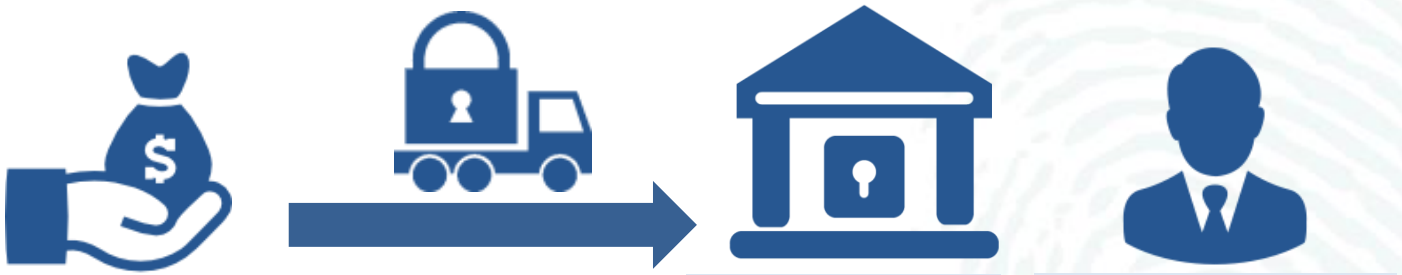
INSPIRE in the cloud security issues

- some geospatial data are sensitive
  - for public security matters
  - for commercial reasons
- their exploitation in the cloud raises security issues
- the mission of European geosurvey organisations
  - includes the management of sensitive environmental data (e.g. drinking water collection points)
  - beside the legal obligations to share public data to a large audience

The CLARUS solution

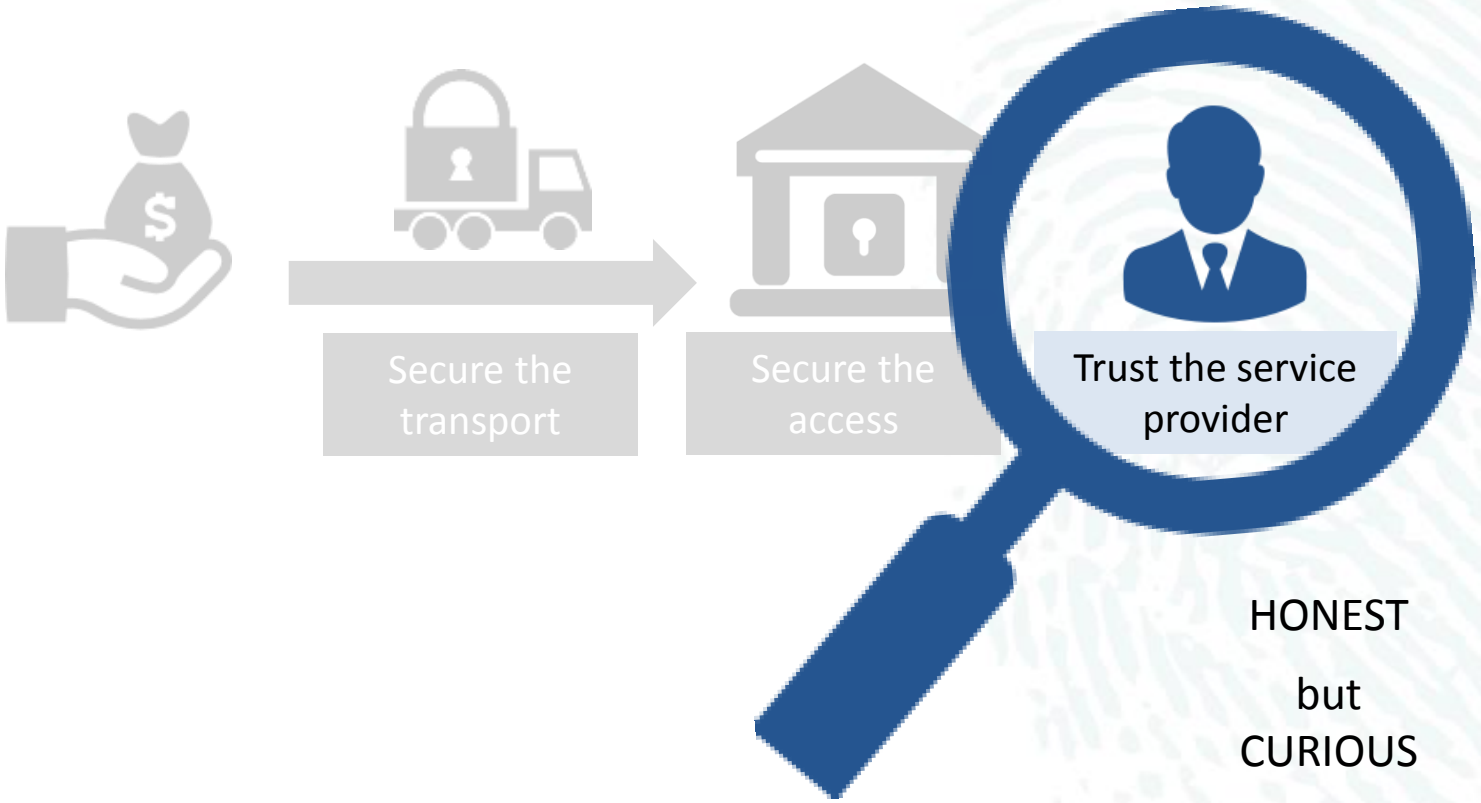
in the context of honest-but-curious
cloud service providers (CSP)

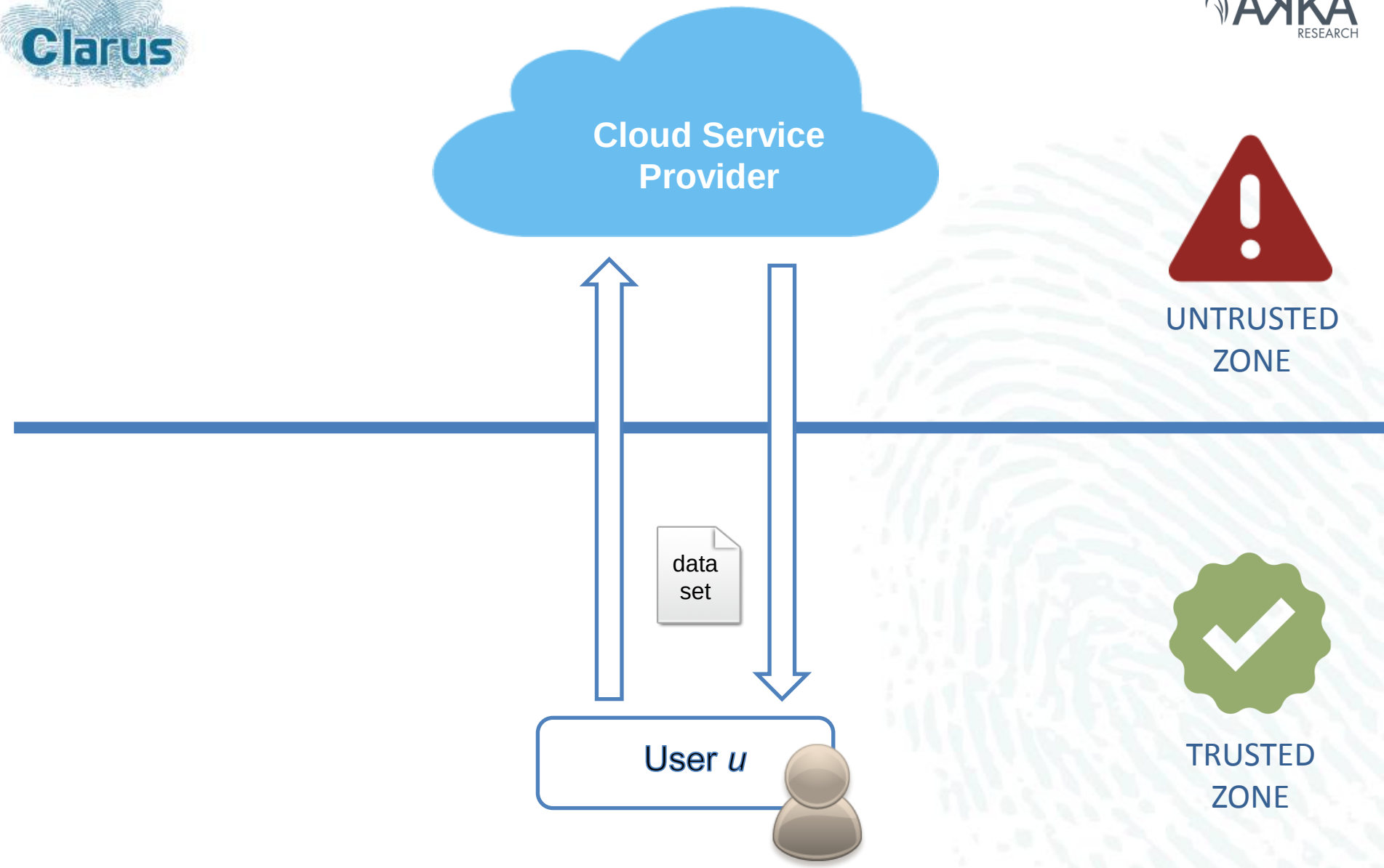
The « honest-but-curious » threat model

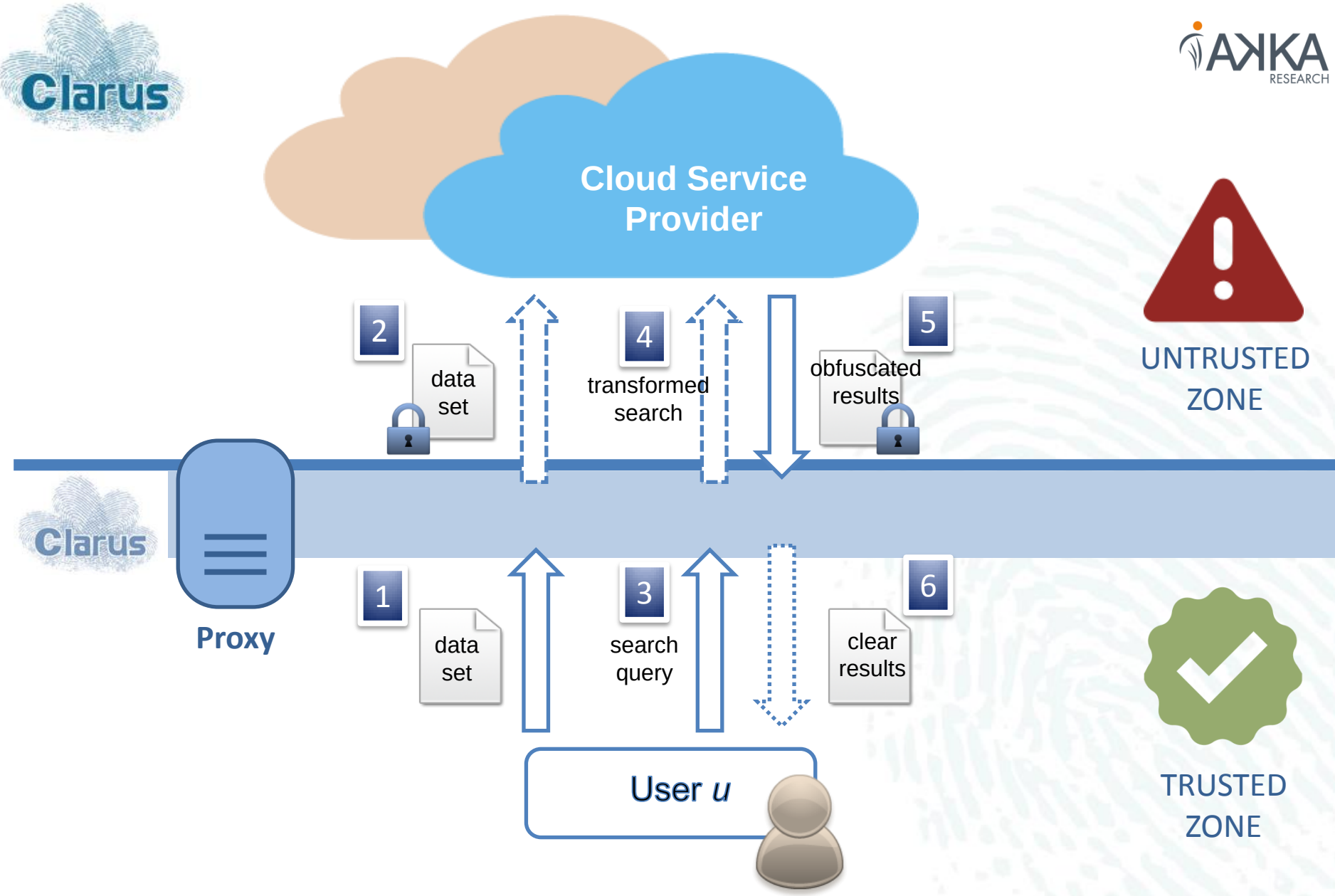


Secure the transport	Secure the access	Trust the service provider
Secure communication HTTPS SFTP SSH	Access control Authentication Authorization	?

The « honest-but-curious » threat model




Cloud Service Provider
UNTRUSTED ZONE
data set
User u
TRUSTED ZONE


Clarus
AKKA RESEARCH
Cloud Service Provider
2
data set
4
transformed search
5
obfuscated results
UNTRUSTED ZONE
Clarus
Proxy
1
data set
3
search query
6
clear results
User u
TRUSTED ZONE

Application cases considered

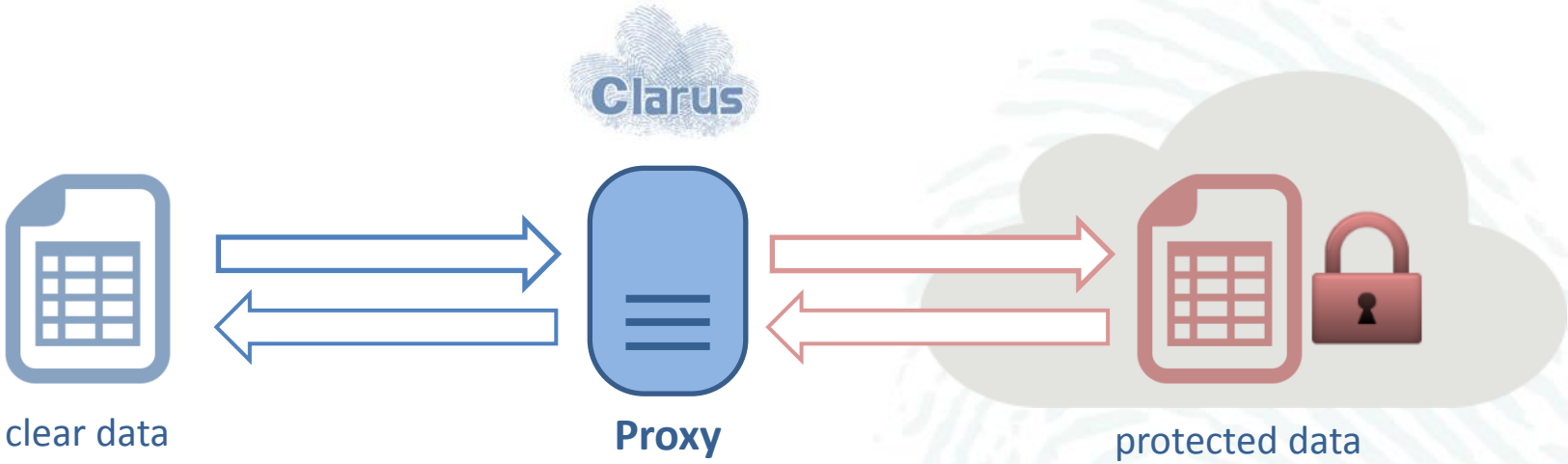
e-Health

FUNDACIÓ CLÍNIC BARCELONA

Geo-Data

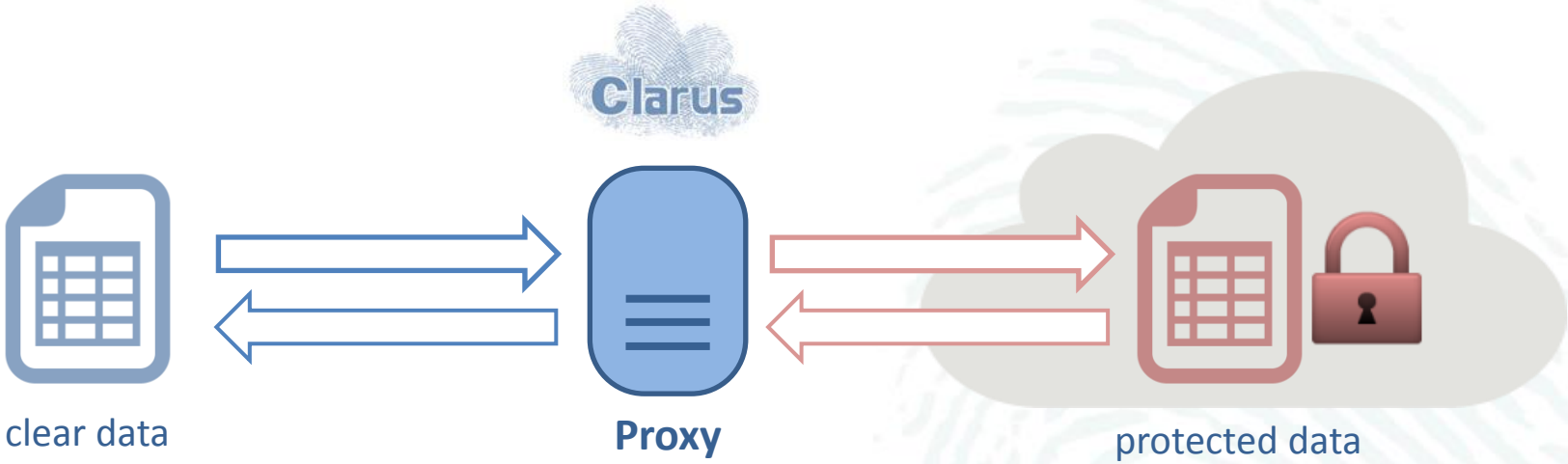
AKKA RESEARCH

Data operations



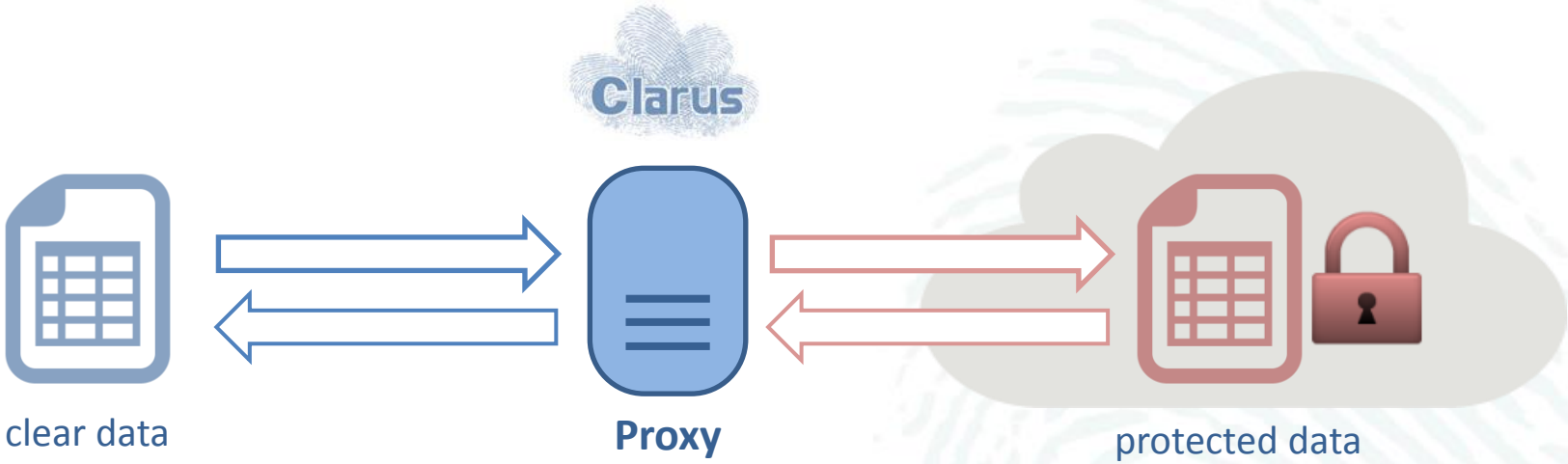
data anonym.	encryption
data coarsening	searchable encryption
data splitting	homo-morphic encryption

Encryption techniques



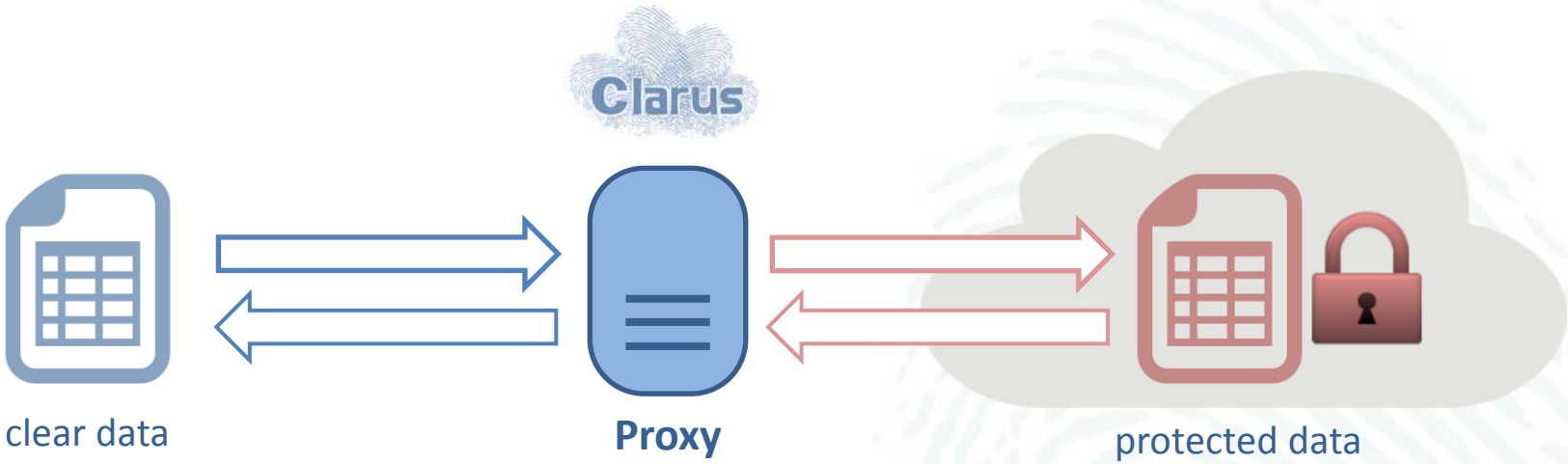
data anonym.	encryption
data coarsening	searchable encryption
data splitting	homo-morphic encryption

Privacy-preserving techniques



data anonym.	encryption
data coarsening	searchable encryption
data splitting	homo-morphic encryption

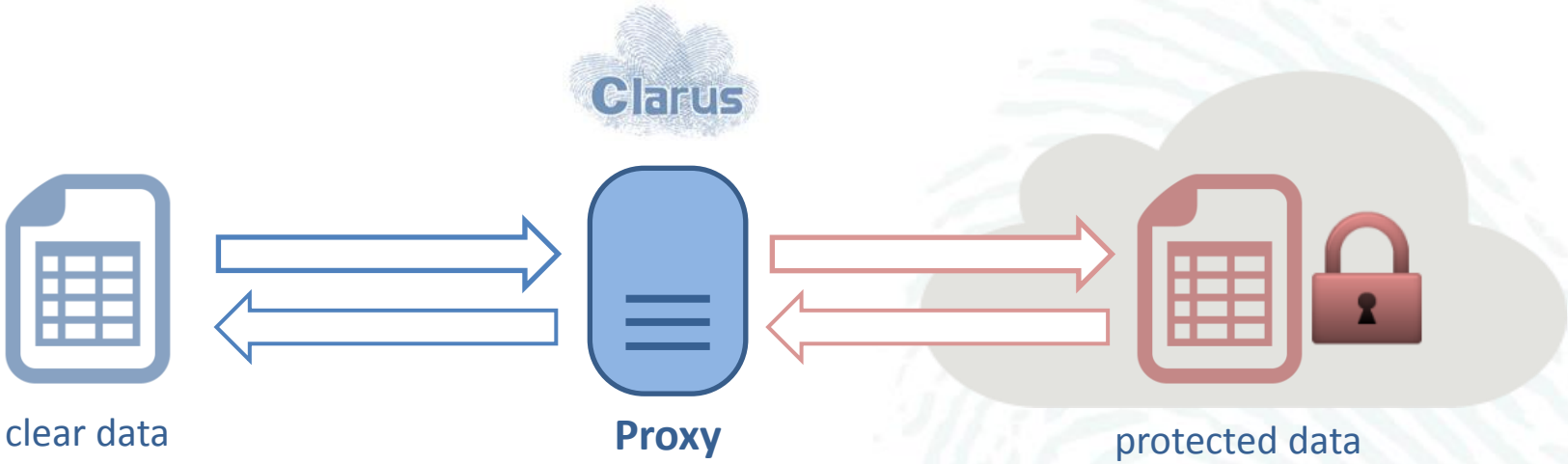
Data anonymisation



data anonym.	encryption
data coarsening	searchable encryption
data splitting	homo-morphic encryption

- ✓ Sensitive data are made indistiguishable
- ✓ in order to avoid reidentification
- ✓ and confidential data disclosure

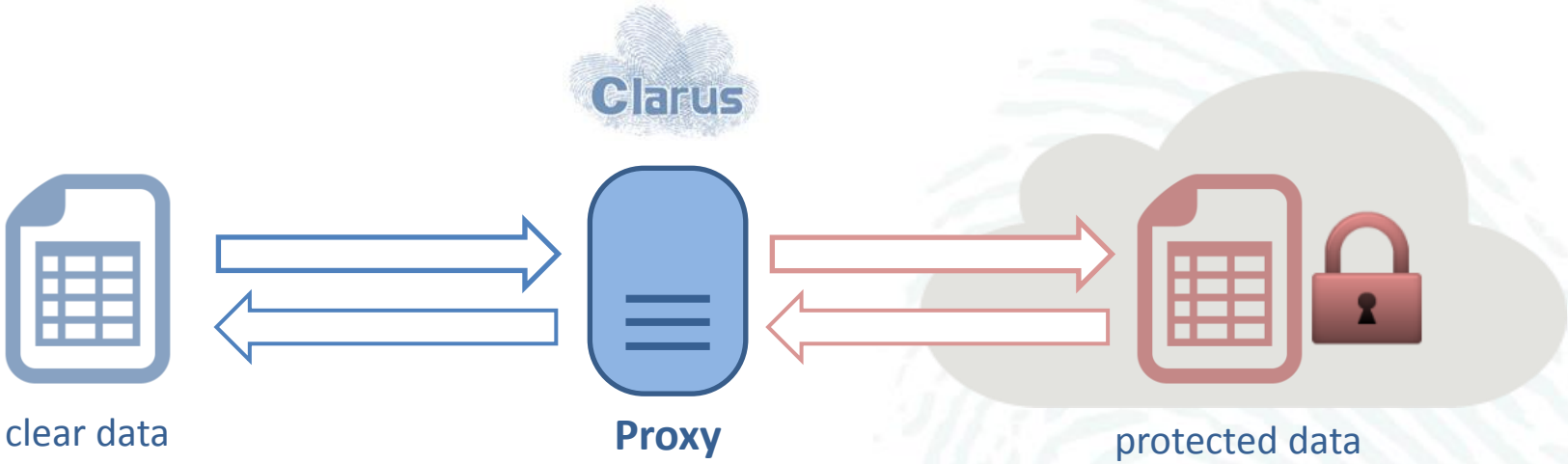
Data coarsening



data anonym.	encryption
data coarsening	searchable encryption
data splitting	homo-morphic encryption

- ✓ Data are generalized
- ✓ in order to lower their level of details
- ✓ and thus avoid disclosure

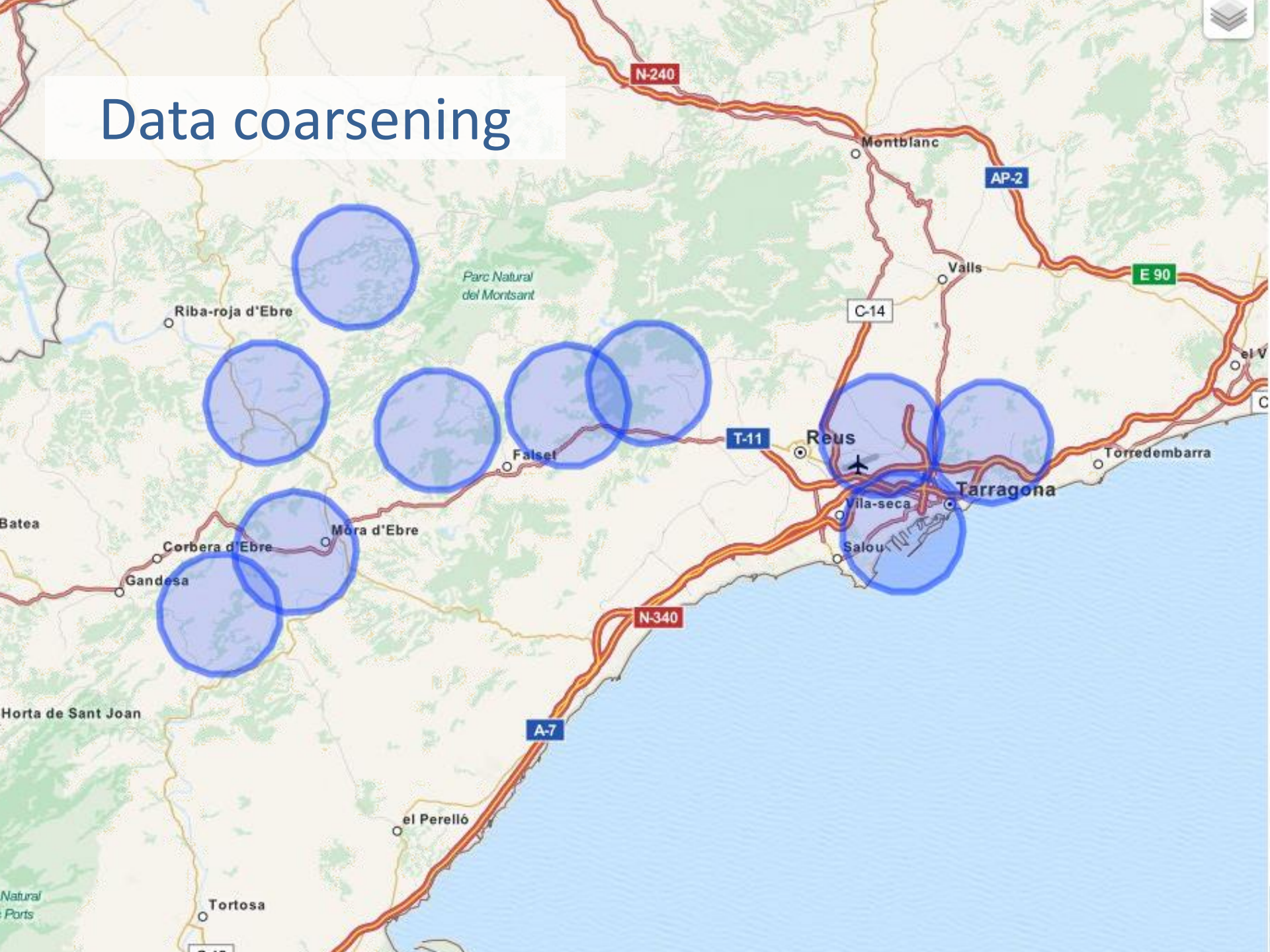
Data splitting



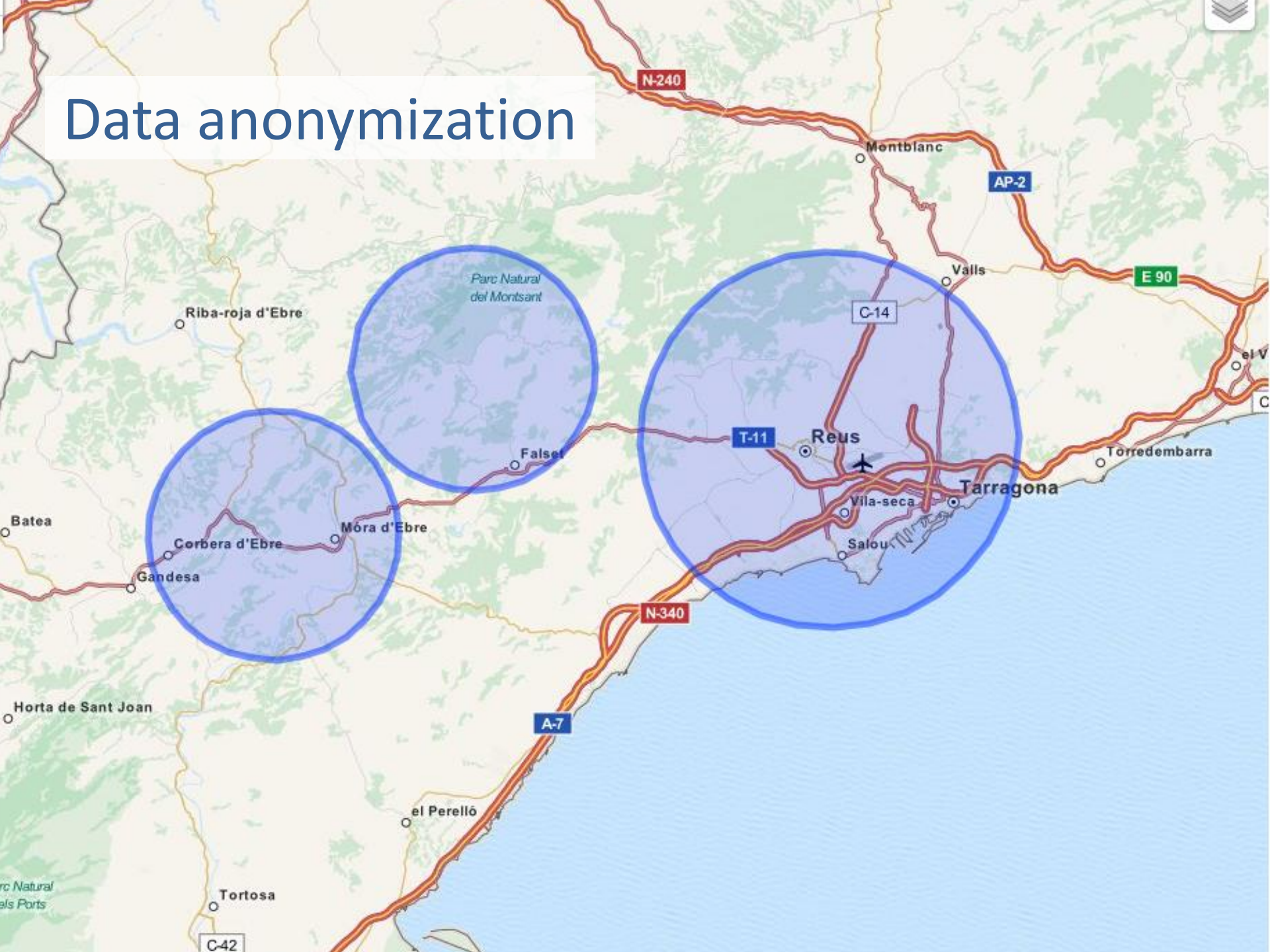
data anonym.	encryption
data coarsening	searchable encryption
data splitting	homo-morphic encryption

- ✓ Data are fragmented
- ✓ into different cloud providers
- ✓ so that individual pieces do not cause disclosure

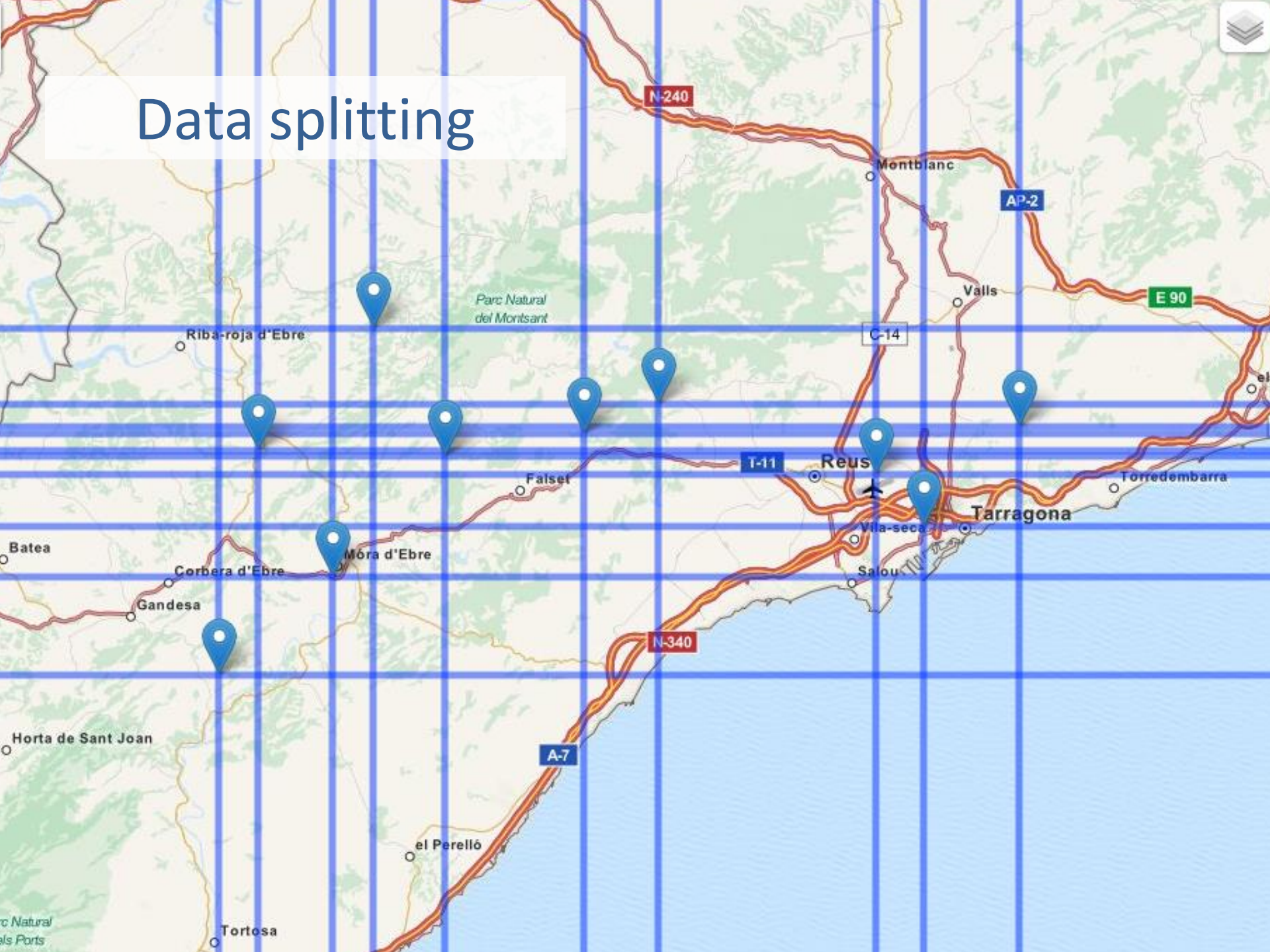
Data coarsening



Data anonymization



Data splitting



What about encryption ?

The challenges of encryption

Full encryption is advised

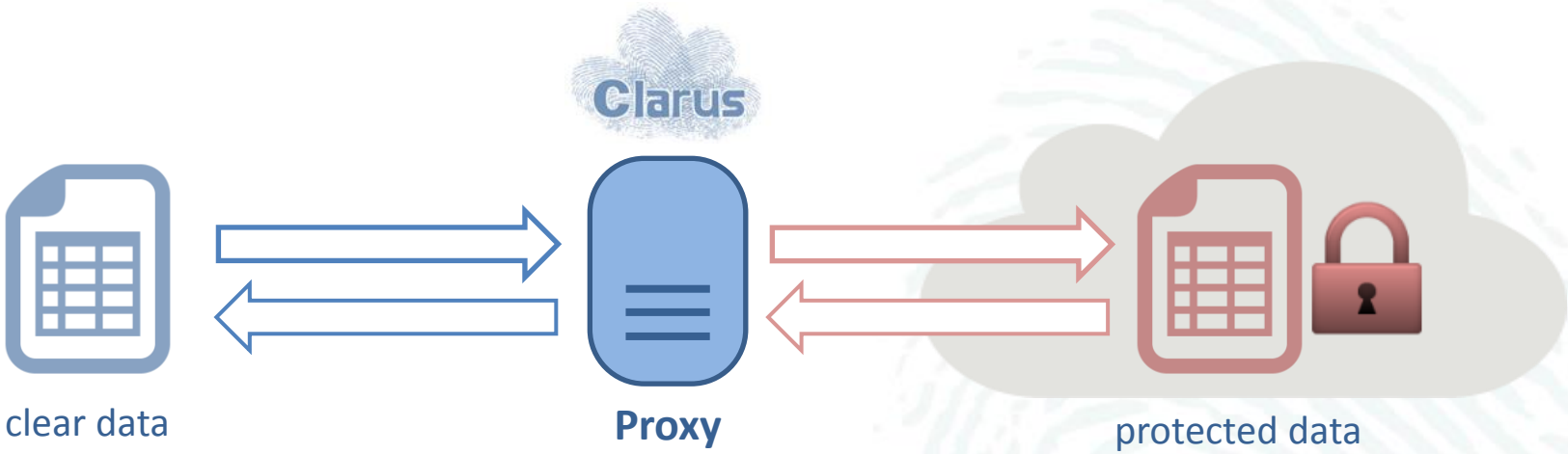
(Partial encryption reveals search patterns to the CSP that can be used to derive information about the protected data)

…. but ….

How to fully encrypt without breaking functionality ?

For vector datasets stored in a spatial DB, it is not possible

Combining techniques



USE CASE
Kriging computation (geoprocessing)

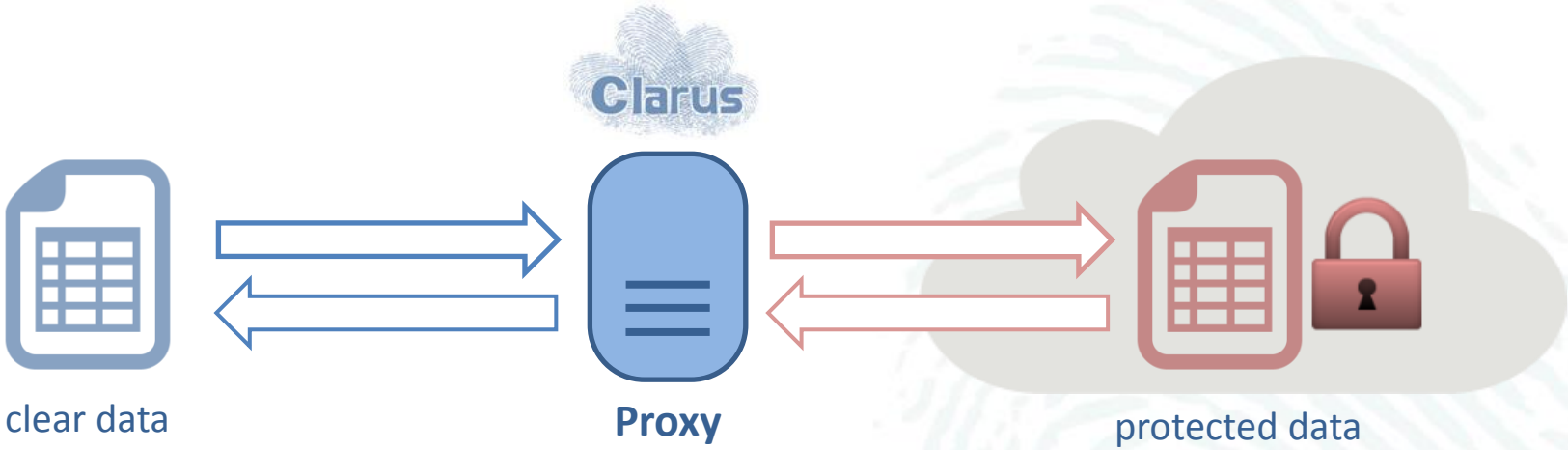
data anonym.	encryption
data coarsening	searchable encryption
data splitting	homo-morphic encryption

Measurements (z) are encrypted and outsourced to one cloud

Outsourced coordinates (x,y) are split (latitude/longitude) in different clouds

Kriging computation on protected data is possible

Searchable encryption for geo-referenced data

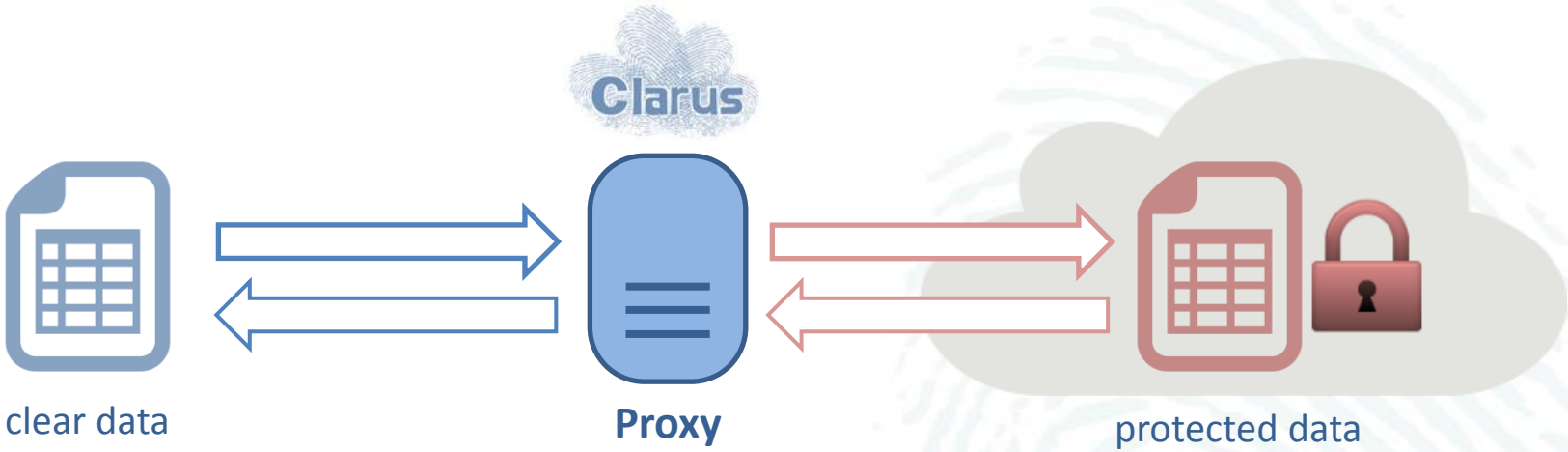


data anonym.	encryption
data coarsening	searchable encryption
data splitting	homo-morphic encryption

RESEARCH PAPER

UNIVERSITAT ROVIRA I VIRGILI

Homomorphic encryption for secure geoprocessing

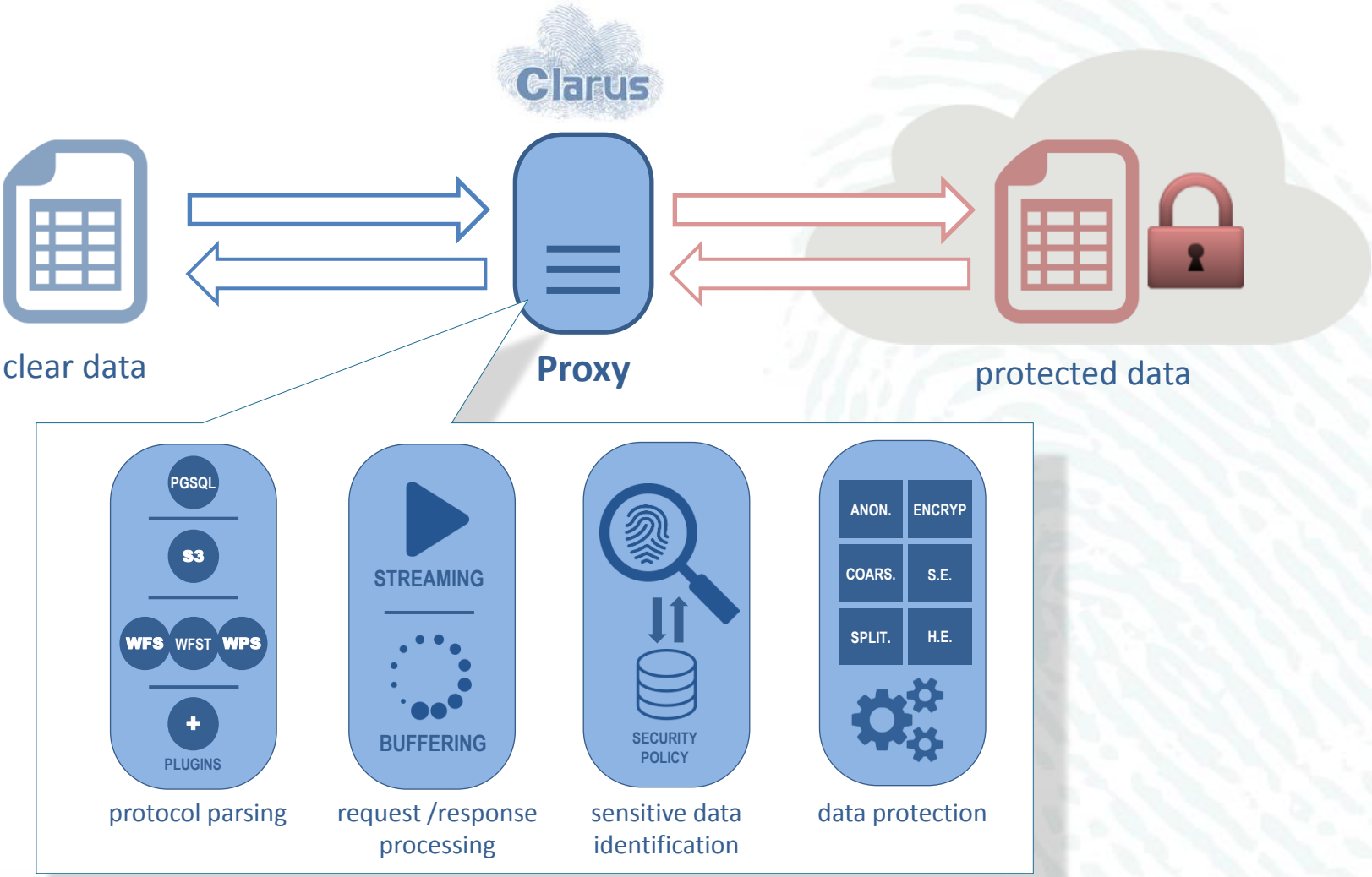


data anonym.	encryption
data coarsening	searchable encryption
data splitting	homo-morphic encryption

RESEARCH PAPER

ROYAL HOLLOWAY UNIVERSITY OF LONDON

under the magnifying glass



Geospatial datasets for CLARUS

contain geographical coordinates

contain scientific attributes (measurements)

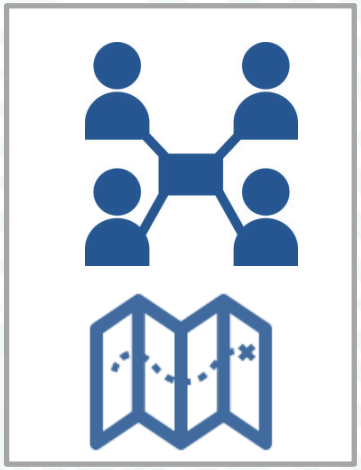
require a certain level of security (confidential)

conforming to standards (OGC, ISO)

relating to one of the INSPIRE thematic groups

held by public authorities or third-parties

INSPIRE use cases for CLARUS

storage	geo publication	geo processing	geo collaboration
			
any	 groundwater boreholes	 geology (kriging)	 energy supply networks

INSPIRE use cases for CLARUS

Other (possible) applications

- Health geostatistics
  - privacy-preserving statistics and geography
- Location privacy
  - privacy-preserving location based services (LBS)
  - for smart cities, smart phones, connected cars
- Satellite imagery
  - protect high resolution products

A framework for user centred privacy and security in the cloud

THANK YOU

Thierry Chevallier
(AKKA Technologies)

www.clarussecure.eu | contact@clarussecure.eu | @Clarusecure

CLARUS has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud.
Contract No. 644024