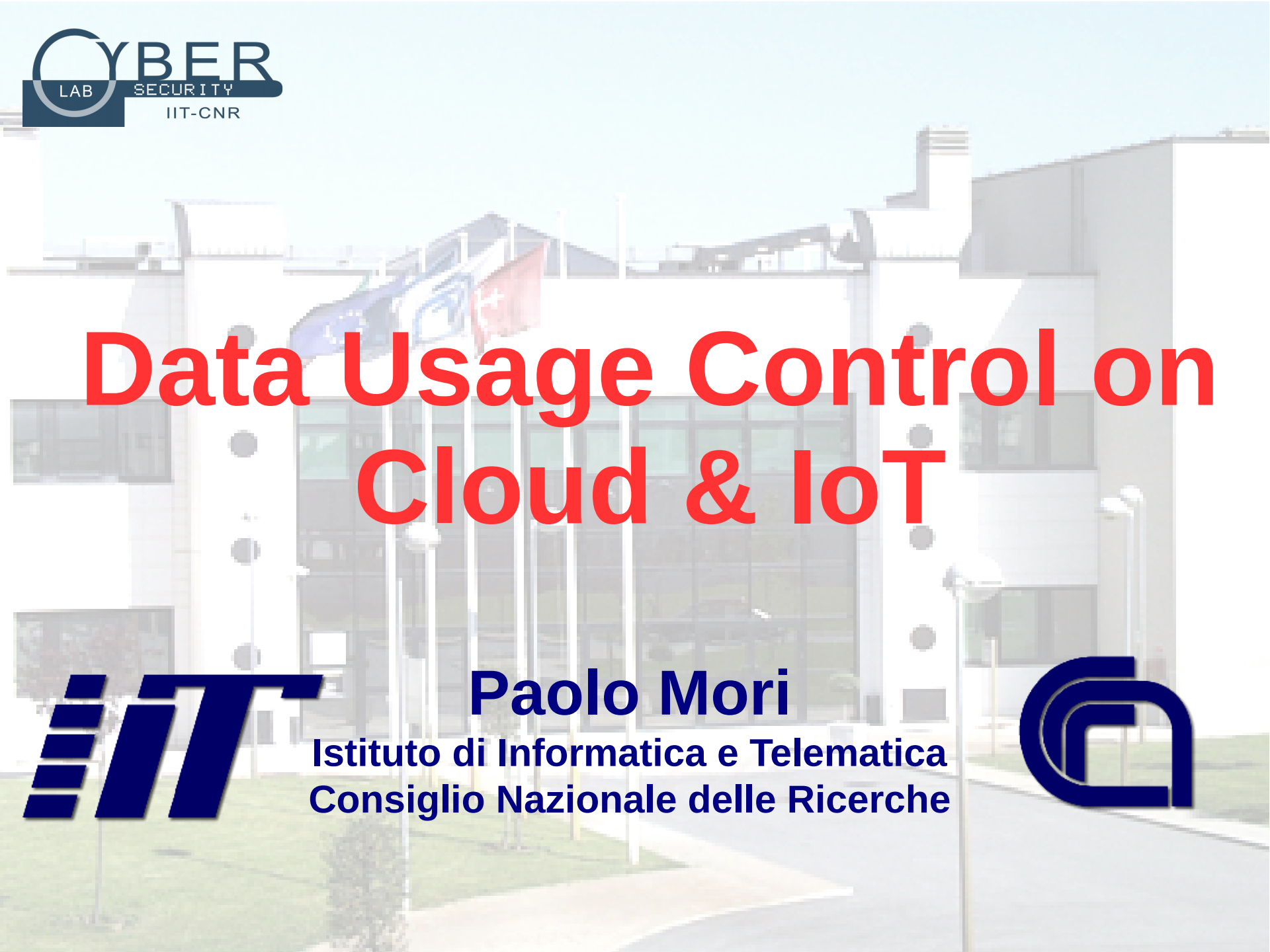


Data Usage Control on Cloud & IoT

Paolo Mori
Istituto di Informatica e Telematica
Consiglio Nazionale delle Ricerche

Data & IoT

- Large/Huge quantity of data generated by Smart Objects
  - –

Data & IoT

- Large/Huge quantity of data generated by Smart Objects
  -

Data & IoT

- Large/Huge quantity of data generated by Smart Objects
  -

Data & IoT

- Large/Huge quantity of data generated by Smart Objects
  -

Data & IoT

- Large/Huge quantity of data generated by Smart Objects
  -

Data & IoT

- Large/Huge quantity of data generated by Smart Objects
  -

Data & IoT

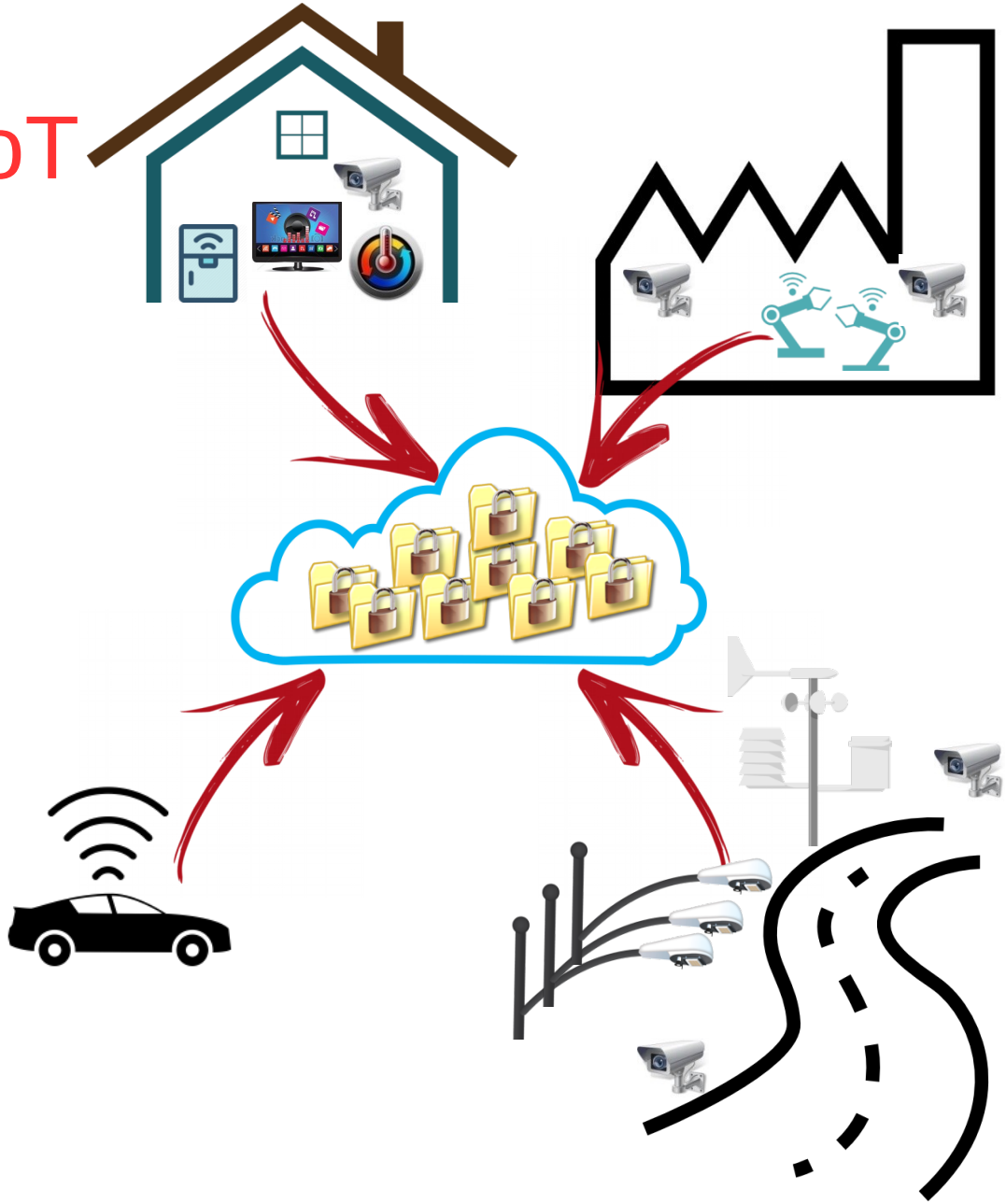
- Large/Huge quantity of data generated by Smart Objects
  -

Data & IoT

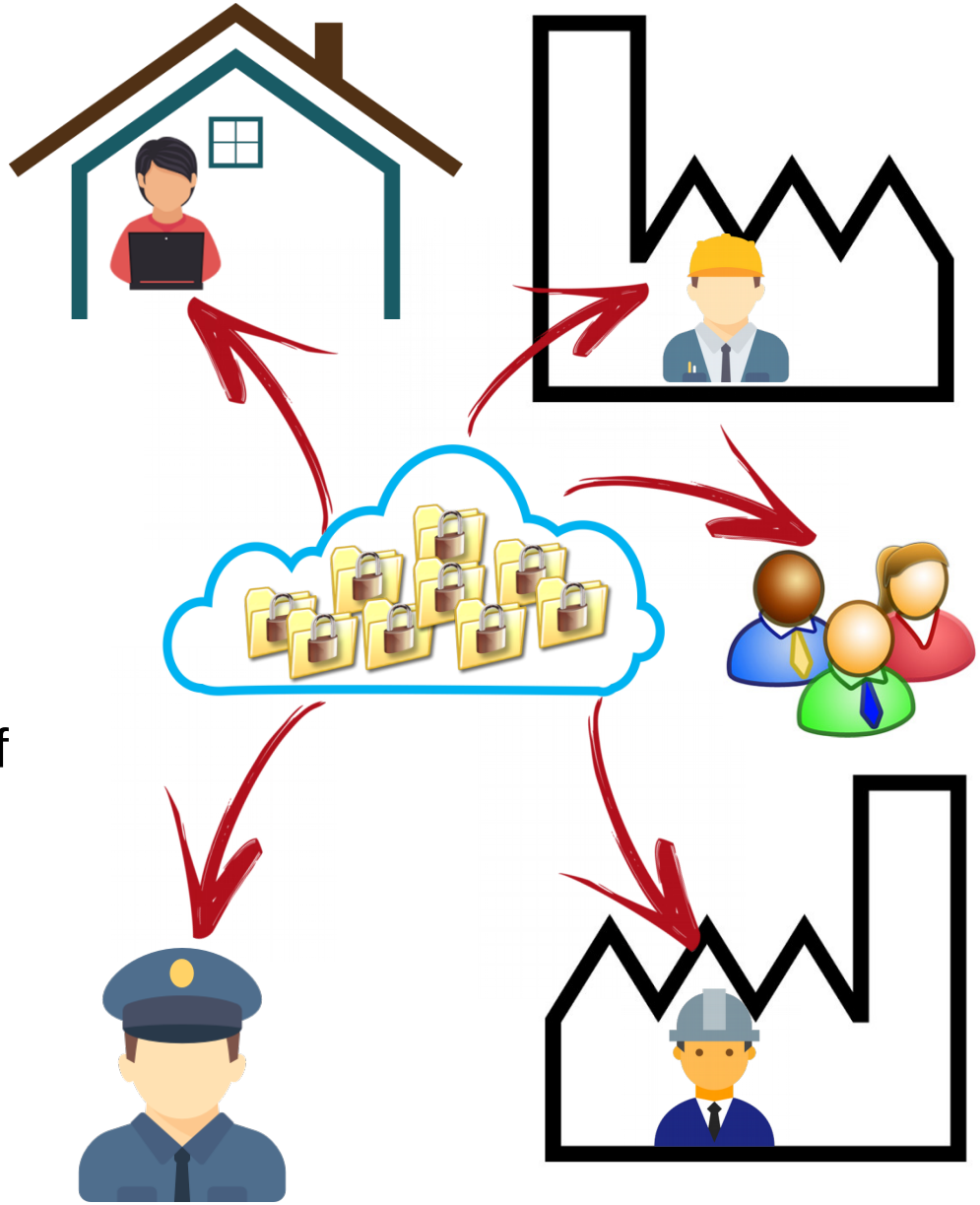
- Large/Huge quantity of data generated by Smart Objects
  -

Data & IoT

- Large/Huge quantity of data generated by Smart Objects
  - Stored on the Cloud

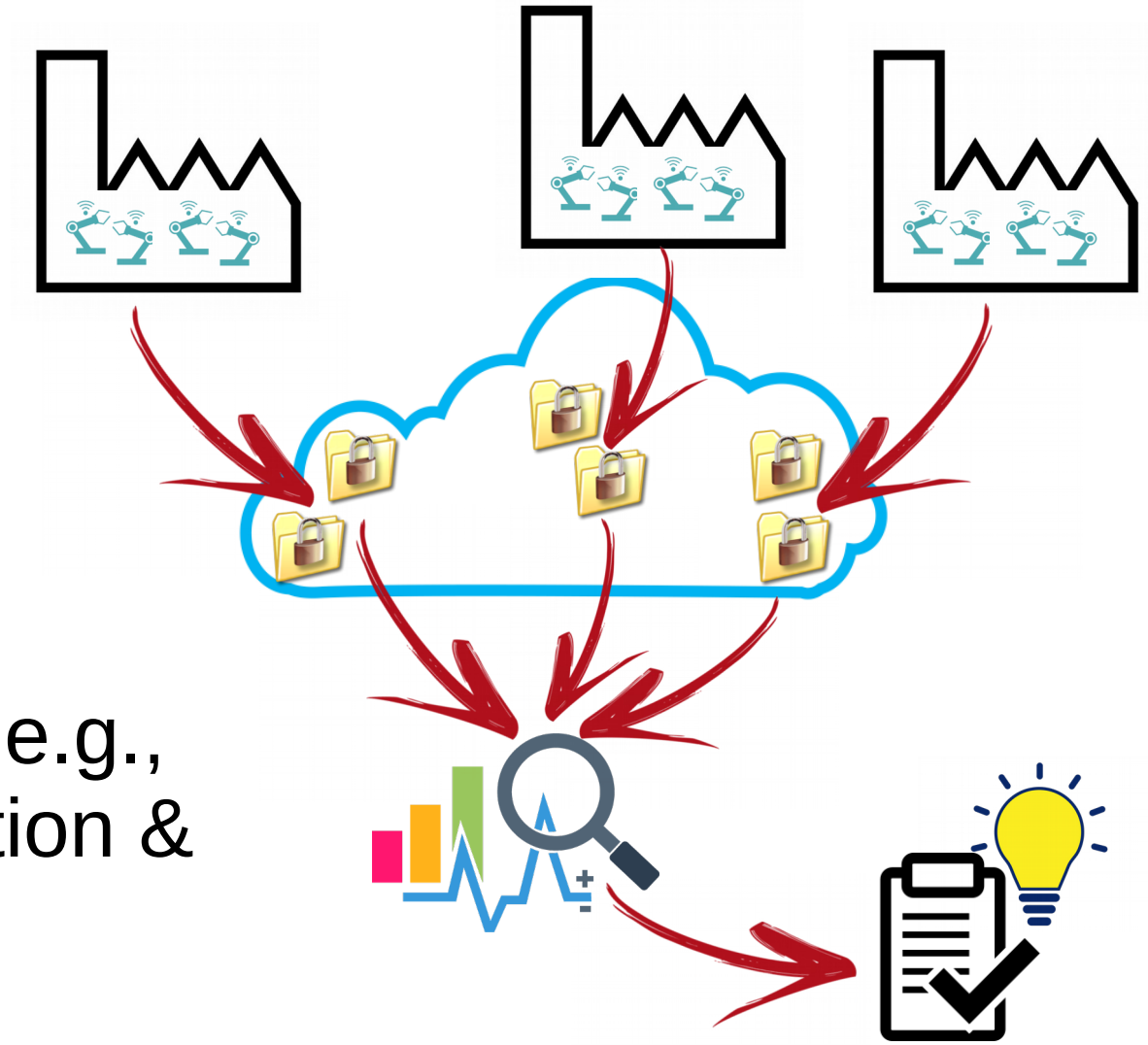


Data & IoT



- These data are exploited
  - Individually
  - Together with other data of
    - The same producer
    - Other producers (collaborative analitics)

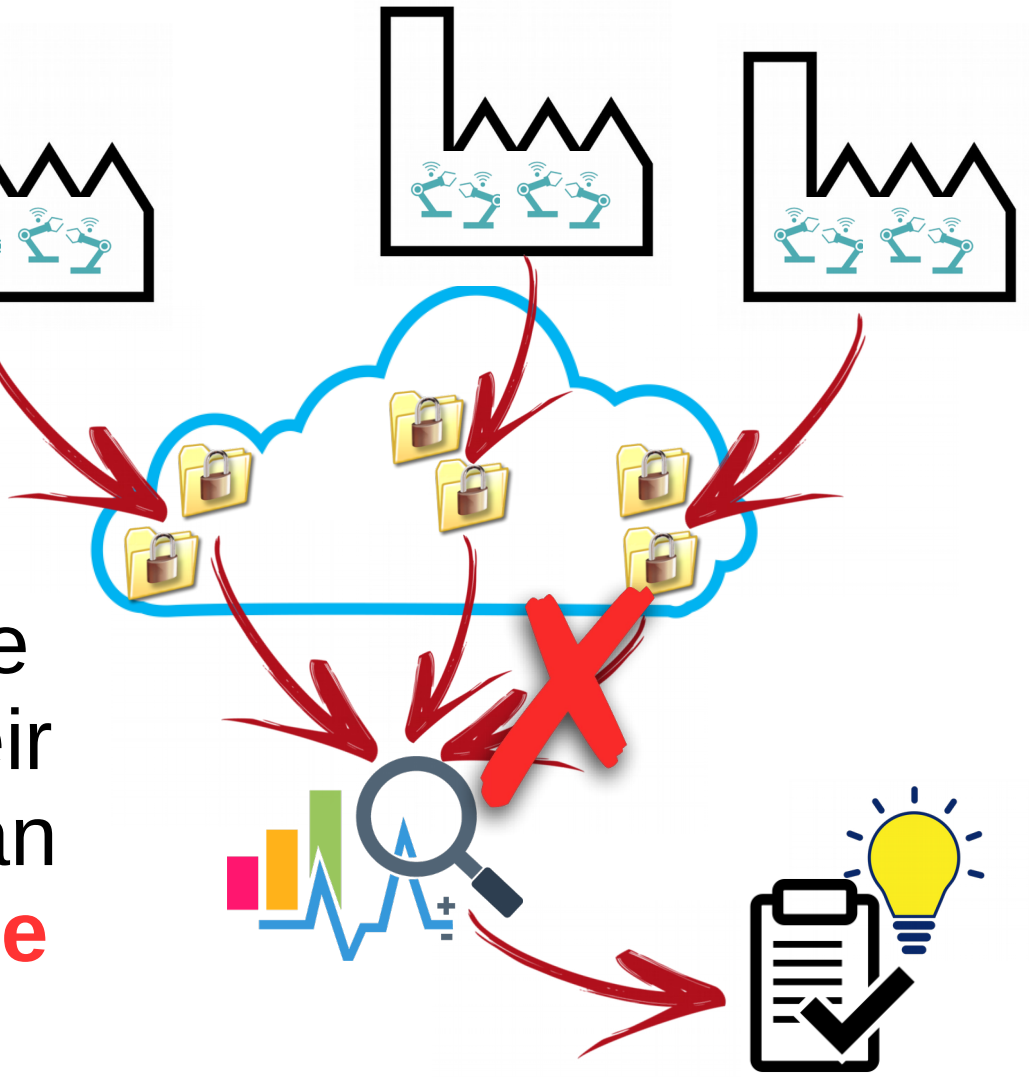
Collaborative Analytics



Advantage:

Better results, e.g., incident detection & response

Collaborative Analytics



Challenge:

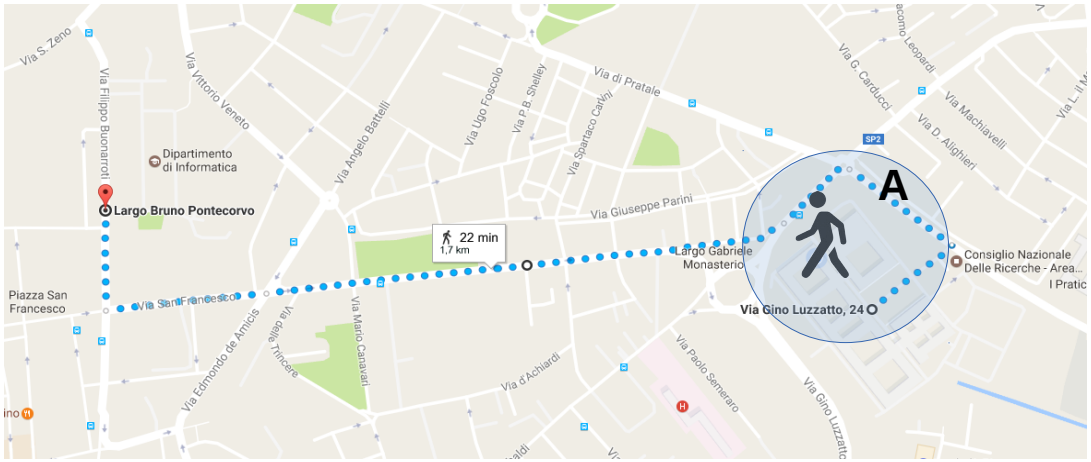
Data producers are willing to share their data only if they can **control** their **usage**

WHY Usage Control?

Traditional Access Control is not effective when the access context is mutable over time

EXAMPLE:

Users can read the document only when they are located in the area A

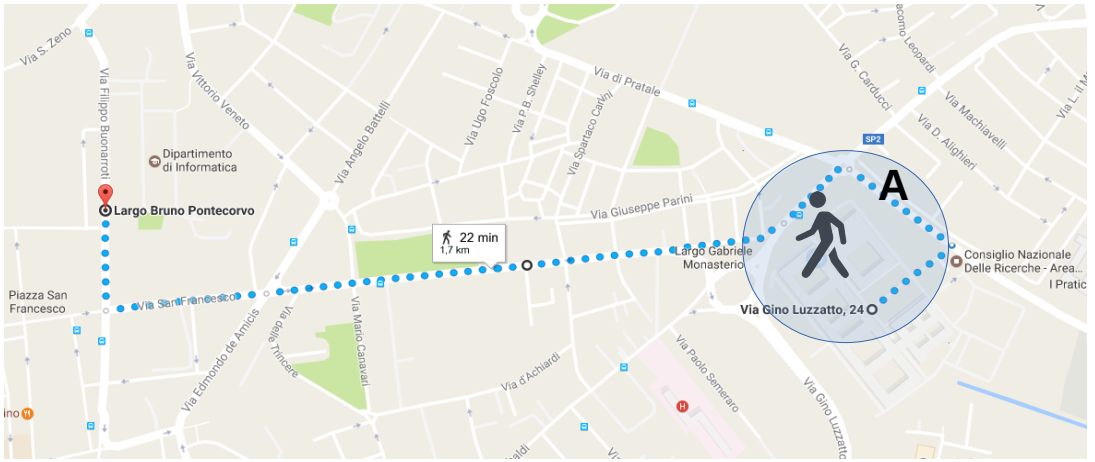


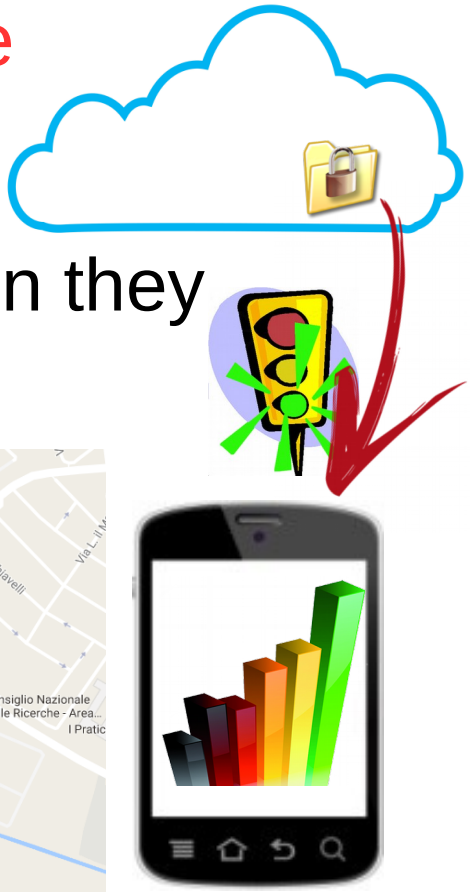
WHY Usage Control?

Traditional Access Control is not effective when the access context is mutable over time

EXAMPLE:

Users can read the document only when they are located in the area A



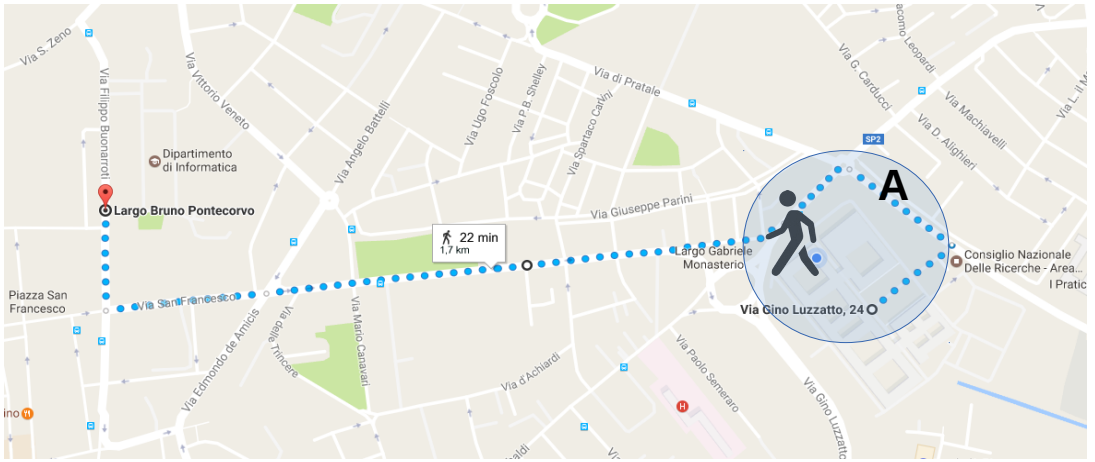


WHY Usage Control?

Traditional Access Control is not effective when the access context is mutable over time

EXAMPLE:

Users can read the document only when they are located in the area A

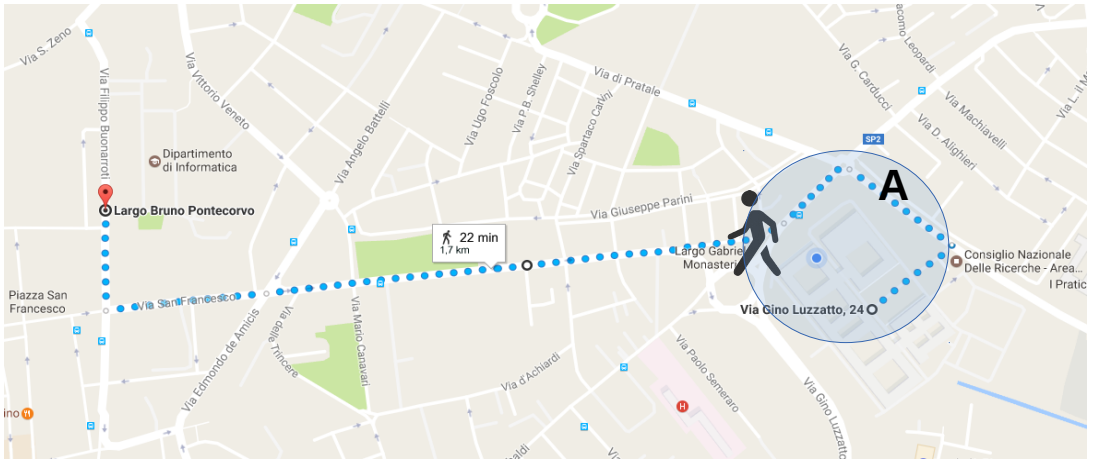


WHY Usage Control?

Traditional Access Control is not effective when the access context is mutable over time

EXAMPLE:

Users can read the document only when they are located in the area A

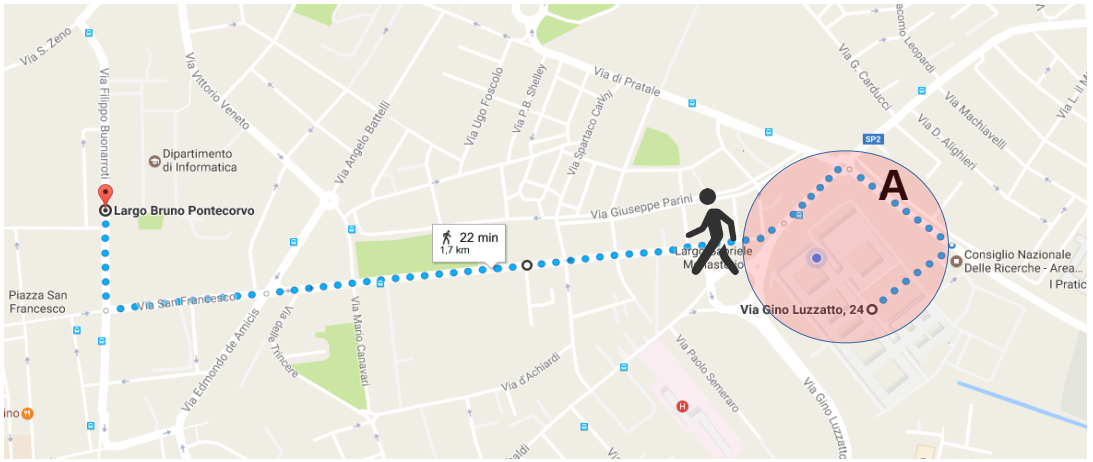


WHY Usage Control?

Traditional Access Control is not effective when the access context is mutable over time

EXAMPLE:

Users can read the document only when they are located in the area A



Data Usage Control in Cloud & IoT

Data Usage Control in Cloud & IoT

Framework for the enforcement of usage control policies to regulate the usage of data produced by IoT devices and stored on the Cloud

Usage Control Policy

- Authorization and Conditions to be satisfied
  - To allow operations
  - When operations are in progress
- Obligations
  - Data Manipulation Operations to be executed before the operations
  - Countermeasures to be executed when authorizations or conditions are violated

Obligations

Data Manipulation Operations

- Convert (from proprietary to standard format)
- Filter-out (discard not-relevant data)
- Anonymise/mask (remove confidential data)
- Compress (optimise network traffic)

Contermeasures

- Send email
- Suspend/interrupt

Authorizations

Subject attributes

- Role
- Position

Data attributes

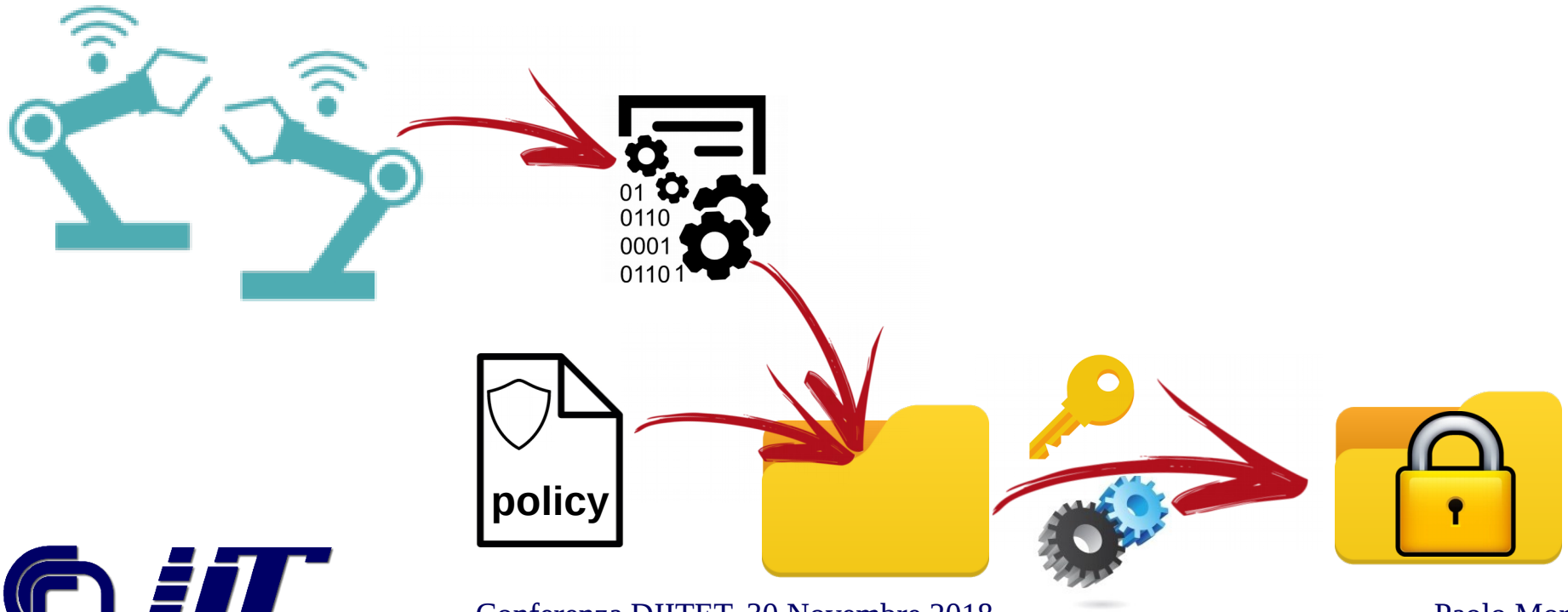
- Type
- # Copies

Conditions

- Date / Time
- System state

Data Production

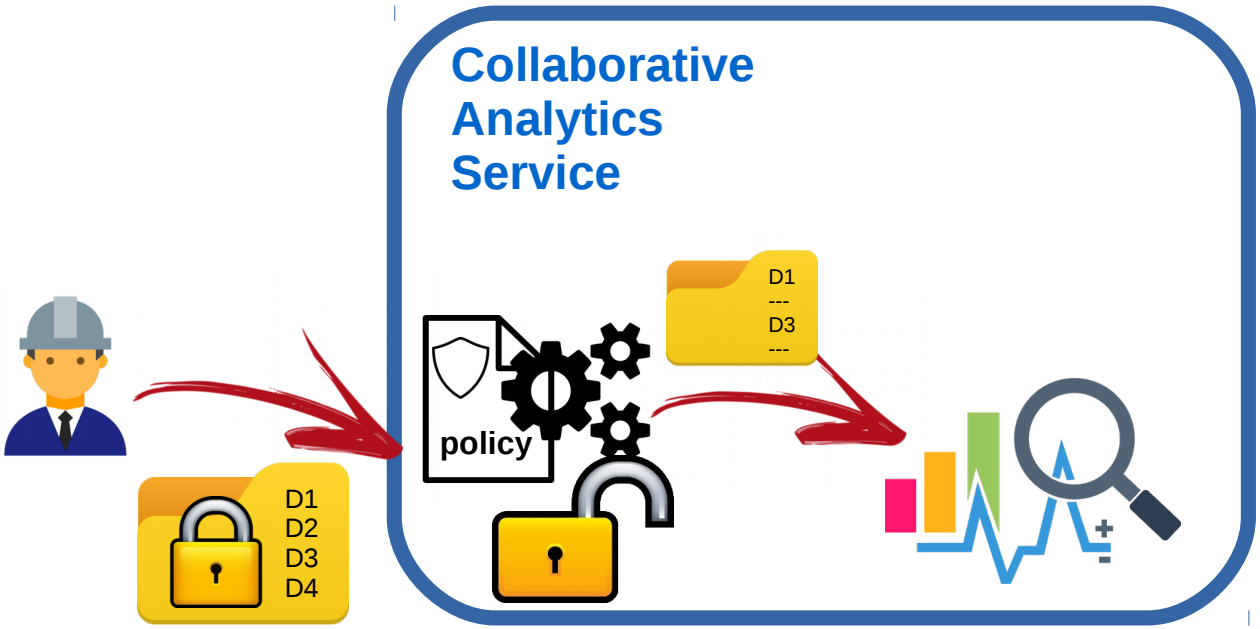
- Data are
  - Paired with their own usage control policy
  - Enclosed in Encrypted Bundles



Data Fruition

The usage control policy paired with the data is enforced

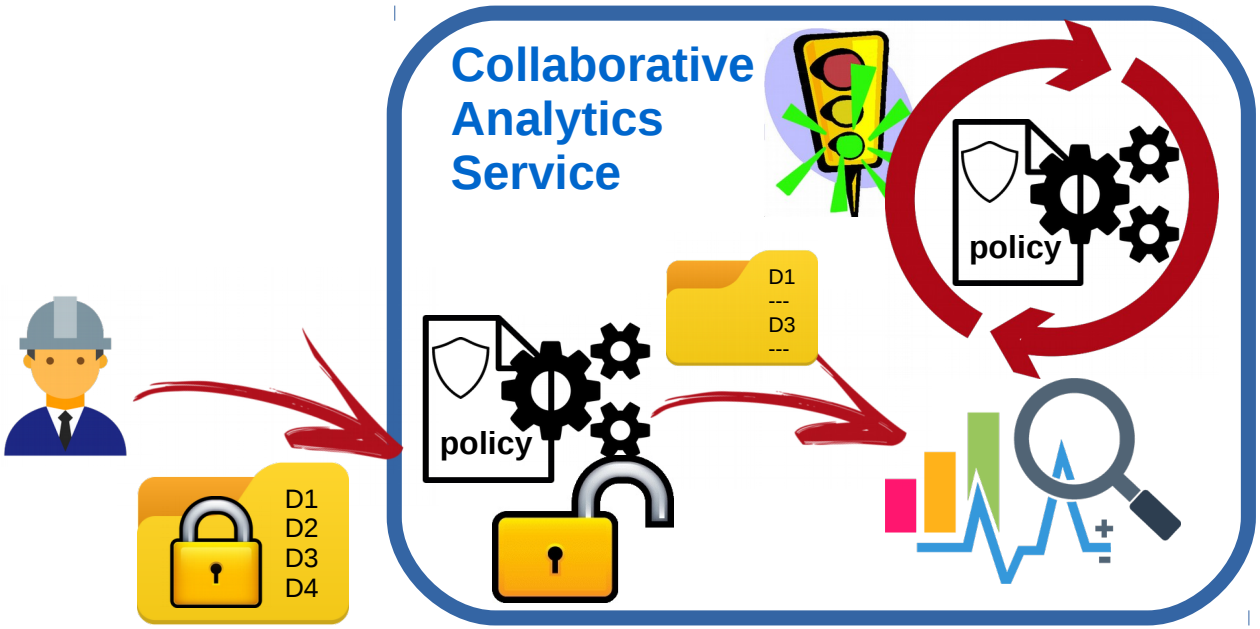
- Before opening the data
-



Data Fruition

The usage control policy paired with the data is enforced

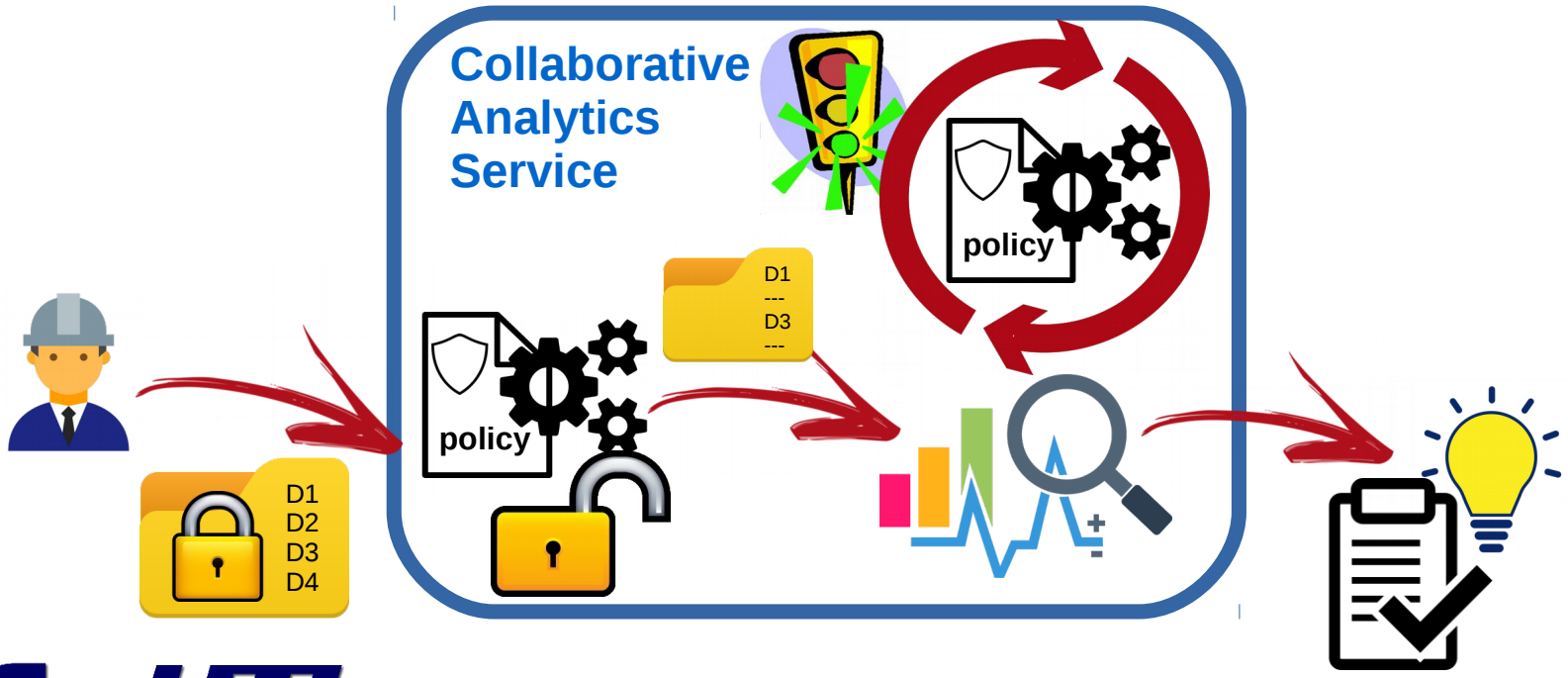
- Before opening the data
- During data usage



Data Fruition

The usage control policy paired with the data is enforced

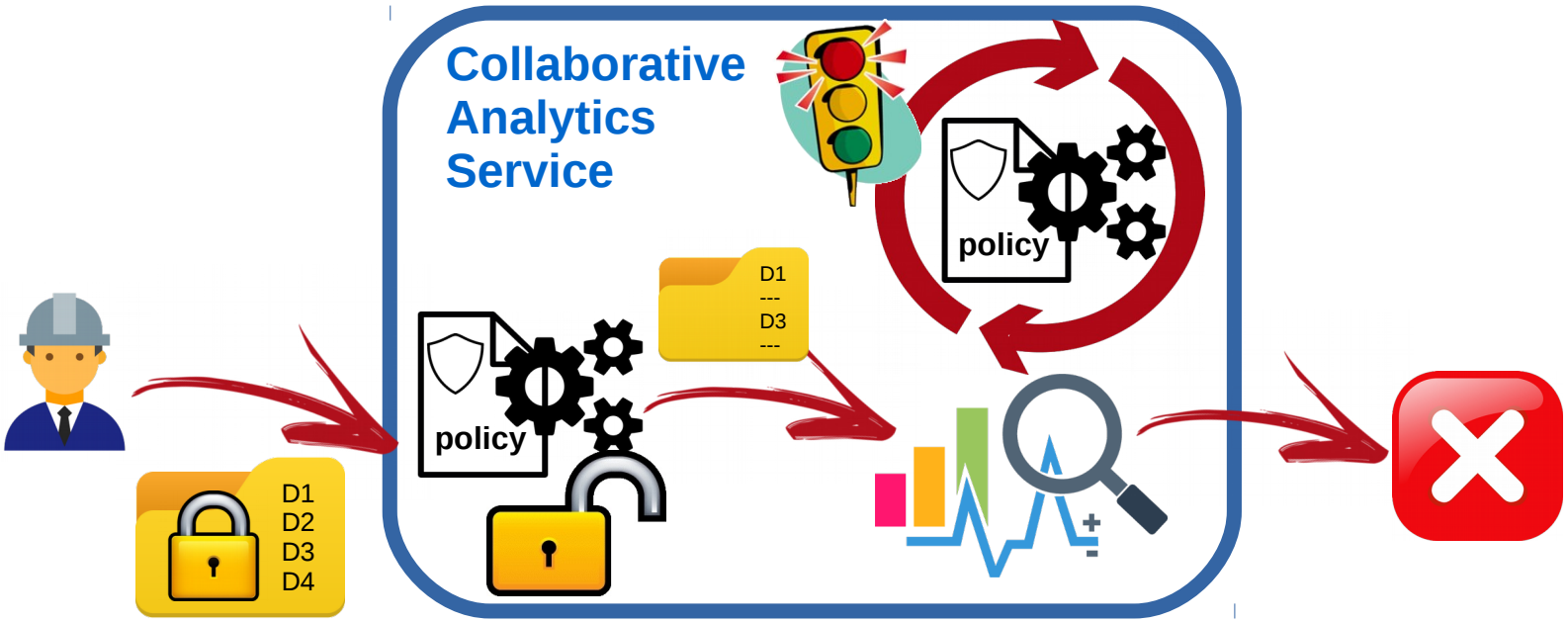
- Before opening the data
- During data usage



Data Fruition

The usage control policy paired with the data is enforced

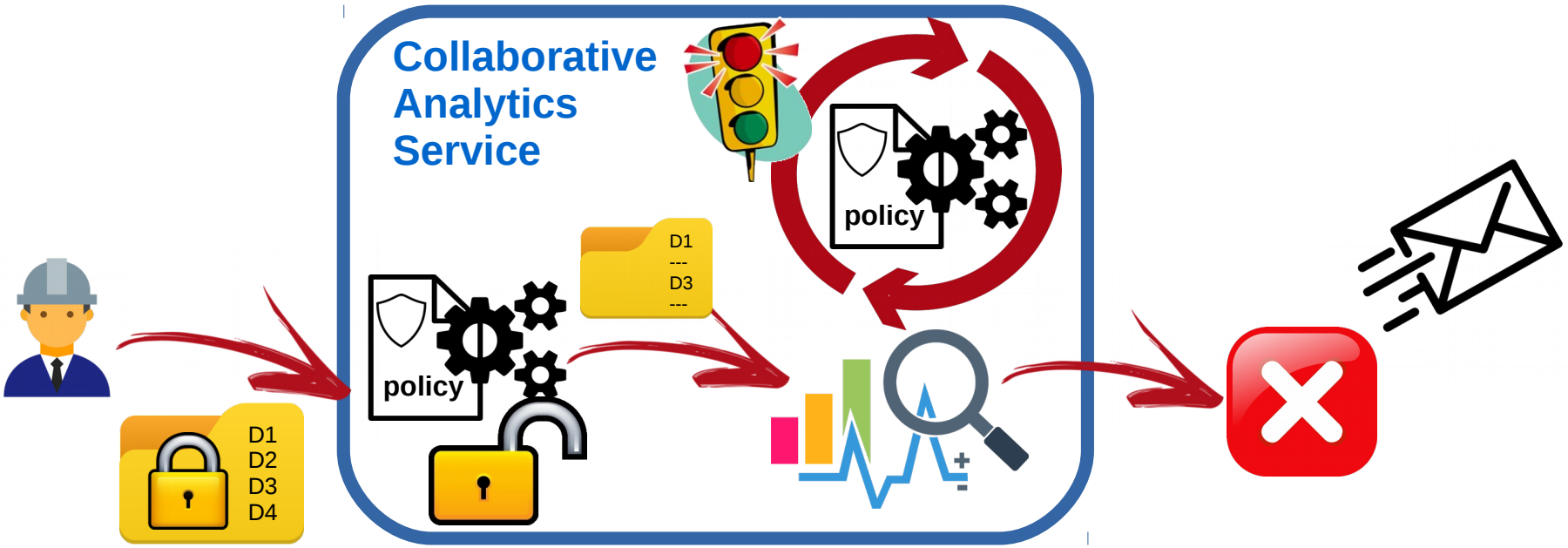
- Before opening the data
- During data usage ➡ Access revocation



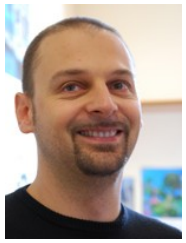
Data Fruition

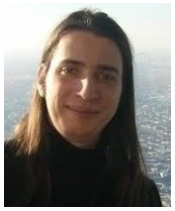
The usage control policy paired with the data is enforced

- Before opening the data
- During data usage ➡ Access revocation + countermeasures



CYBER LAB SECURITY IIT-CNR





C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

eit Digital

Trusted Cloud & IoT

IIT

Data Usage Control in Cloud & IoT:

Technical Details

Based on: Extensible Access Control Markup Language 3.0 (**XACML**)

XACML defines:

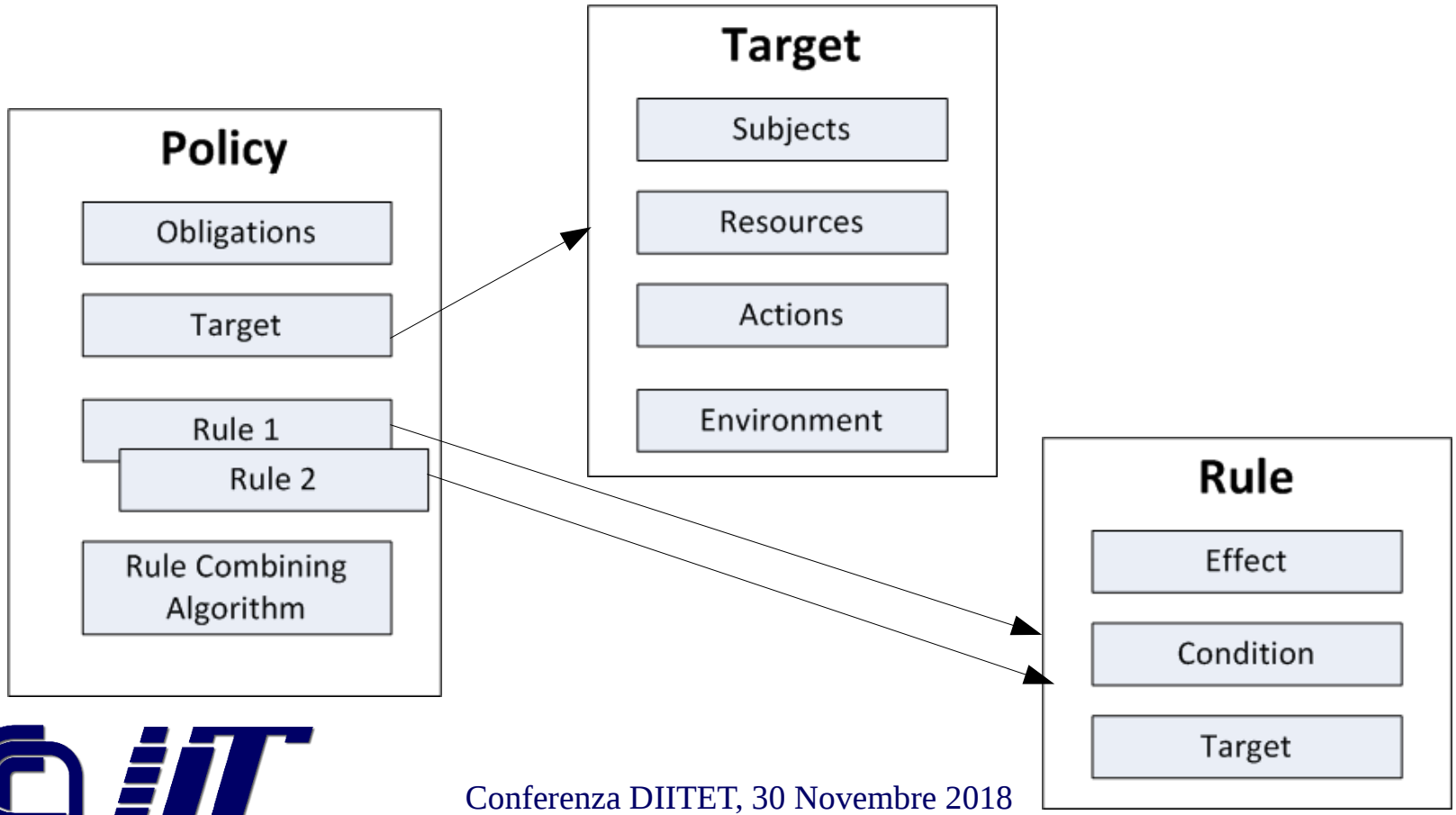
- A XML-based Language to express Attribute based Access Control Policies
- A reference architecture for the Access Control Framework

eXtensible Access Control Markup Language (XACML) Version 3.0 Plus Errata 01. OASIS Standard incorporating Approved Errata. 12 July 2017

Policy Language: U-XACML

- Extension of the XACML 3.0 language

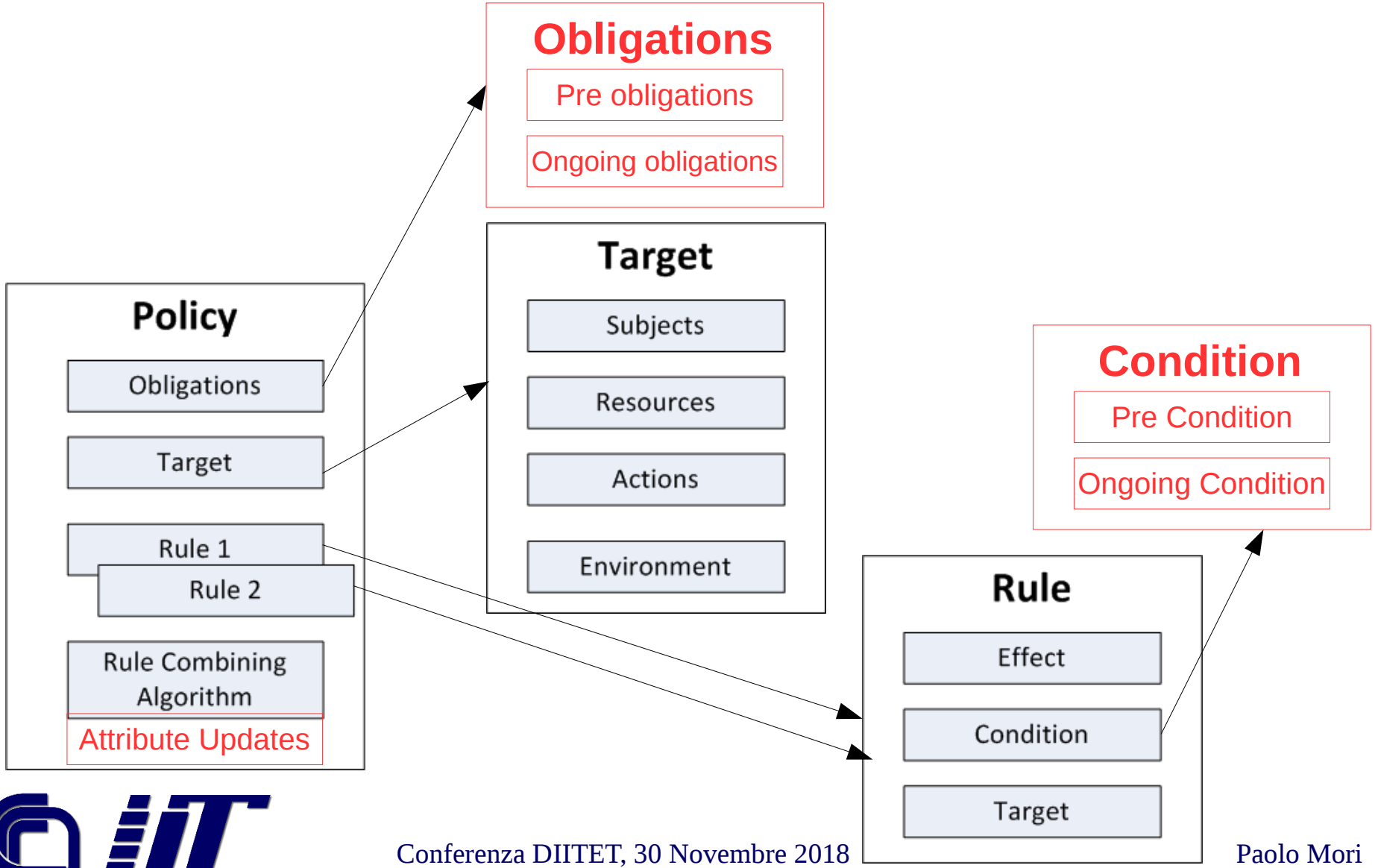
Extensible Access Control Markup Language 3.0 (XACML)



Policy Language: U-XACML

- Extension of the XACML 3.0 language
  - Ongoing Authorizations e Conditions
  - Ongoing Obligations
  - Attribute Updates

U-XACML


Obligations
Pre obligations
Ongoing obligations
Target
Subjects
Resources
Actions
Environment
Policy
Obligations
Target
Rule 1
Rule 2
Rule Combining Algorithm
Attribute Updates
Condition
Pre Condition
Ongoing Condition
Rule
Effect
Condition
Target

Usage Control Authorization Service

- Extension of the XACML reference architecture
  - Mutable Attributes management
  - Continuous policy enforcement
    - Access sessions management
    - Access revocation

Usage Control Authorization Service