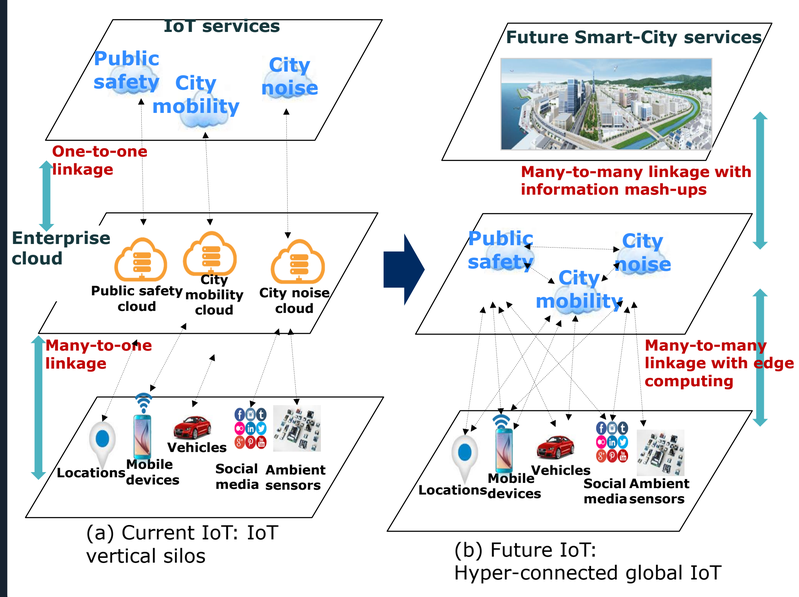
Flavio Cirillo

Tutor: Simon Pietro Romano

XXXIII Cycle - II year presentation

De-centralization of IoT Platforms: Federation, Interoperability, Scalability, Security, Privacy



(a) Current IoT: IoT vertical silos

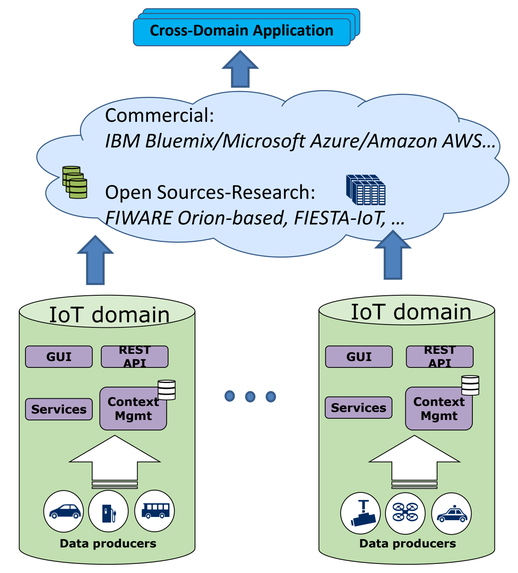
(b) Future IoT: Hyper-connected global IoT

Context

- IoT paradigm used in all the fields where data are produced and processed (e.g., automotive, health care, smart cities, industry)
- Emergence of a **plethora of IoT platforms**
- Typical approach to IoT is to leverage the scalability of the cloud:
  Single-scoped **disjoint IoT vertical silos**
- Hyper-connected IoT requires interoperability [2]
- Centralized
  → **Loss of data sovereignty**

Needs

- Enabling **data analytics** while ensuring **data access and usage control** (e.g., Secondary Usage Control, Anonymization, GDPR) through **technical enforcements**
- Preserve **privacy** and **data secrecy**
- Standards, data models and semantics [1][2]



Approach:

- Transparent **brokering of context** enabling data exchange between heterogeneous and multi-party IoT platforms
- **Sovereignty of data providers** by keeping data locally, thus maintaining their power over the owned data [6]
- In case data cannot be shared, **analytics moves towards the data**. Only the output data is returned but still controlled for secondary usage control within **secure data spaces**.
- Context and data analytics processes orchestrated in accordance to access and usage policies, latency, bandwidth consumptions, among edge and cloud.

Developments

- Transparent existence of **multiple levels of federations** [6]
- IoT Registrar, a glue components to create a **privacy-preserving knowledge graph** and **policies** [7]
- Blockchain technology used to attain immutable storage (knowledge graph and policies) and enabling **marketplace**
- Context exchange based on **open standards** and **Domain-Specific Language** (NGSI DSL), open **data models** (FWARE) and semantics [1][3][5]
- Designing the system to work with **standardized edge computing** (ETSI MEC) and **5G network slicing** [4]

IoT context is associated with the *status* of the real world. It refers to an entity representing a thing (e.g., a car, a building) together with its situation. The context can be physically measured or derived by analytics functions (e.g., crowd estimation [1]).

```
{ "contextElements": [{
"entityId": {"id":"bus18", "isPattern":false, "type":"bus"},
"attributes": [{"name":"speed", "type":"float", "contextValue":"25"}],
"domainMetadata":
[{"name":"SimpleGeolocation", "type":"point",
"value": {"latitude":43.4628, "longitude":-3.80031}}]}]}
```

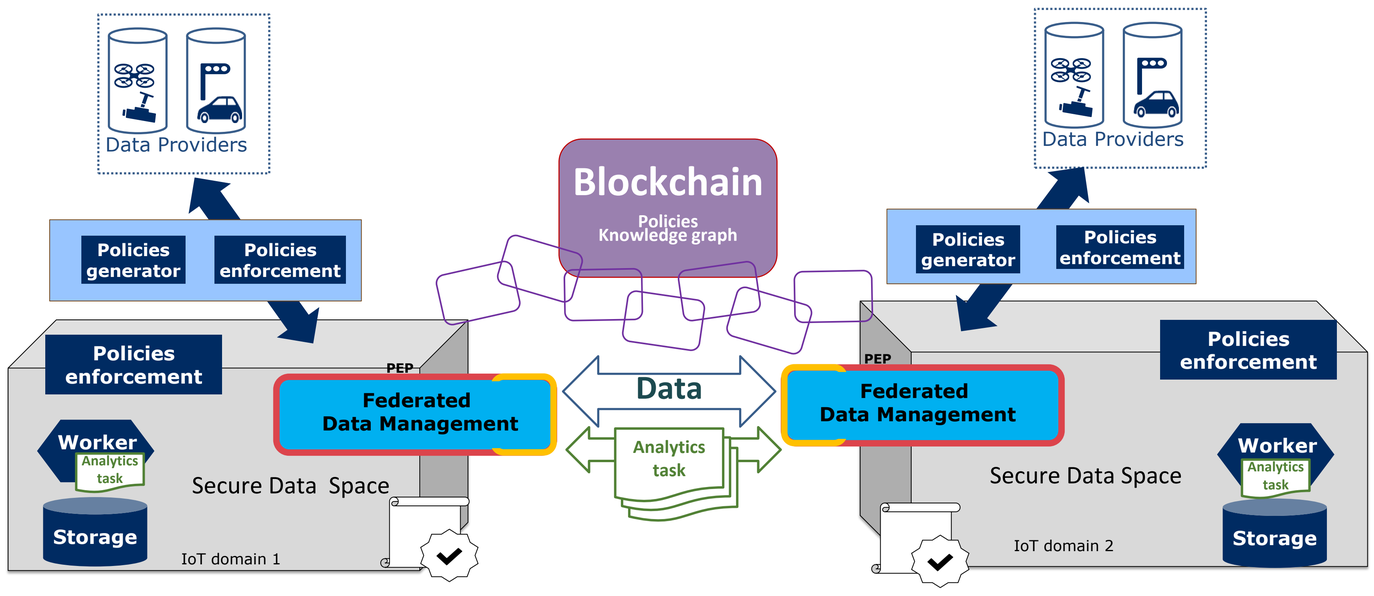
Sample of IoT context in NGSI

```
{ "reference":"http://172.17.0.1:8201/ngsi10/notify",
"entities":[{"id":".*", "isPattern": true, "type":"car"},
{"id":".*", "isPattern": true, "type":"bus"}],
"attributes": ["speed"]}
```

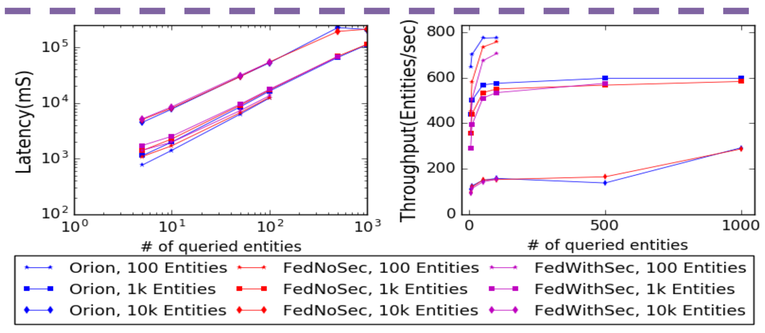
Sample of request (subscription) in NGSI DSL

```
{ "contextRegistrationResponses": [{
"contextRegistration": {
"providingApplication": "http://172.18.2.70:8060/ngsi10",
"entities": [{"id":".*", "type":"bus", "isPattern":true}]}]}]}
```

Sample of data availability in NGSI for building knowledge graph



Evaluation [6]



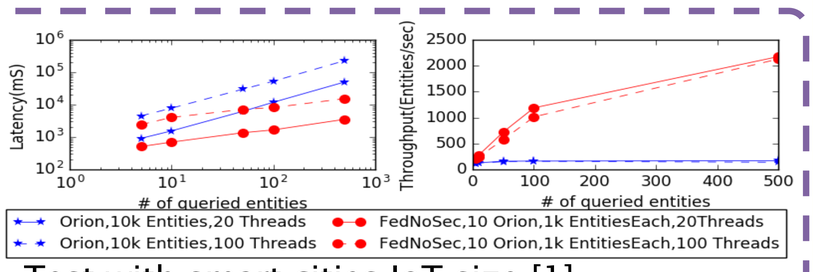
Architecture tested: centralized, non-secured federation, secured federation
Tests varying: number of IoT objects in the deployment, amount of data requested

Federated data management implemented using **FIWARE** open source framework

Negligible overhead for hefty data exchange

Greater the IoT deployment size more negligible is the overhead
→ Context Layer is the bottleneck

For big deployment: **linear scalability** of federated architecture compared to a centralized approach.



Test with smart cities IoT size [1]
Architecture tested: single centralized provider handling 10000 IoT objects, federation with 10 providers handling 1000 IoT objects each.

[1] L. Sanchez *et al.*, "Smartsantander: Iot experimentation over a smart city testbed," *Computer Networks*, 2014
[1] G. Solmaz, F-J. Wu, F. Cirillo, E. Kovacs, J.R. Santana, L. Sánchez, P. Sotres and L. Munoz. "*Towards Understanding Crowd Mobility in Smart Cities through Internet of Things*". IEEE Communications Magazine.
[2] F. Cirillo, F-J. Wu, G. Solmaz and E. Kovacs, *"Embracing the Future Internet of Things"*, MDPI Sensors Journal
[3] F. Cirillo, D. Straeten, D. Gomez, J. Gato, L. Diez, I. Elicegui Maestro, R. Akhavan, "*Atomic Services: sustainable ecosystem of smart city services through pan-European collaboration*", IEEE Global IoT Summit 2019, Aarhus, DK
[4] L. Zanzi, F. Cirillo, S. Mangiante, V. Sciancalepore, F. Giust, X Costa-Perez and G. Klas, "*Evolving Multi-Access Edge Computing to support enhanced IoT deployments*", IEEE Communications Standards Magazine
[5] F. Cirillo, E. L. Berz, G. Solmaz, M. Bauer and E. Kovacs. "*A Standard-based Open Source IoT Platform: FIWARE*", IEEE Internet of Things Magazine (IoTM)
[6] F. Cirillo, Nicola Capuano, Ernoe Kovacs, Simon Pietro Romano. *LIoTS: League of IoT Sovereignties. A Scalable-approach for a Transparent Privacy-safe Federation of Secured IoT Platforms*, IEEE LCN 2019 , Osnabrück, DE
[7] US 16/384,989, F. Cirillo, Method and System for an Internet of Things Platform. Privacy-preserving IoT data availability announcement and regulating method for federating IoT platforms.

flavio.cirillo@unina.it
spromano@unina.it

Future Works:

- Definition and design of data usage control system
- Implementation of data usage control enforcements system using data analytics orchestration framework
- Implementation of pilot data usage control scenarios
- Testing performances also when involving blockchain
- Move towards the evolution of standards: ETSI NGSI-LD