UNIVERSITÉ DE PAU ET DES PAYS DE L'ADOUR | COLLÈGE STEE SCIENCES ET TECHNOLOGIES POUR L'ÉNERGIE ET L'ENVIRONNEMENT

THE ENTERPRISE COMPUTING CONFERENCE EDOC2021 CONFERENCE

Towards a data provenance model for private data sharing management in IoT

PriSEM'21 Workshop

Nouha Laamech, Manuel Munier and Congduc Pham
Universite de Pau et des Pays de l'Adour, E2S UPPA

LIUPPA

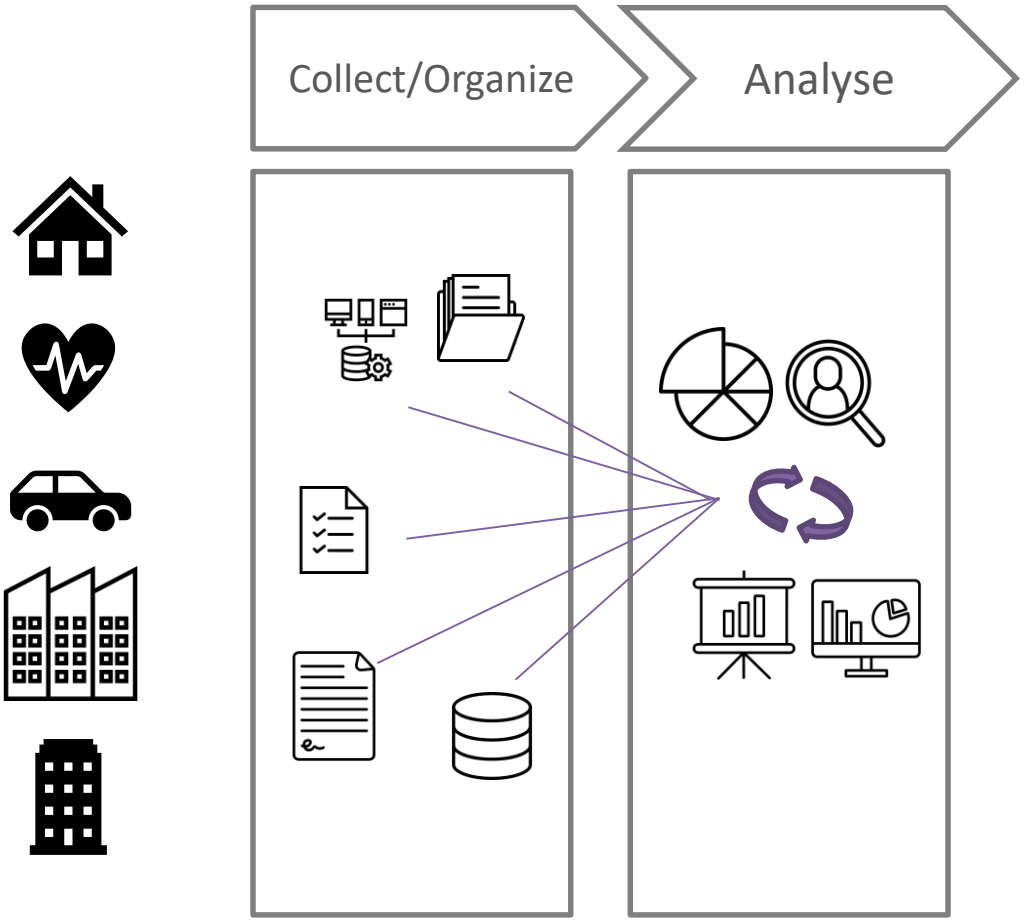
Outline

Towards a data provenance model for private data sharing management in IoT

- **Context & Problematic**
- **Proposed approach : IoT data sharing management system**
  - Value Proposition
  - Semantic Rule Manager
  - Data provenance system
- **Challenges & Discussion**
- **Conclusion**

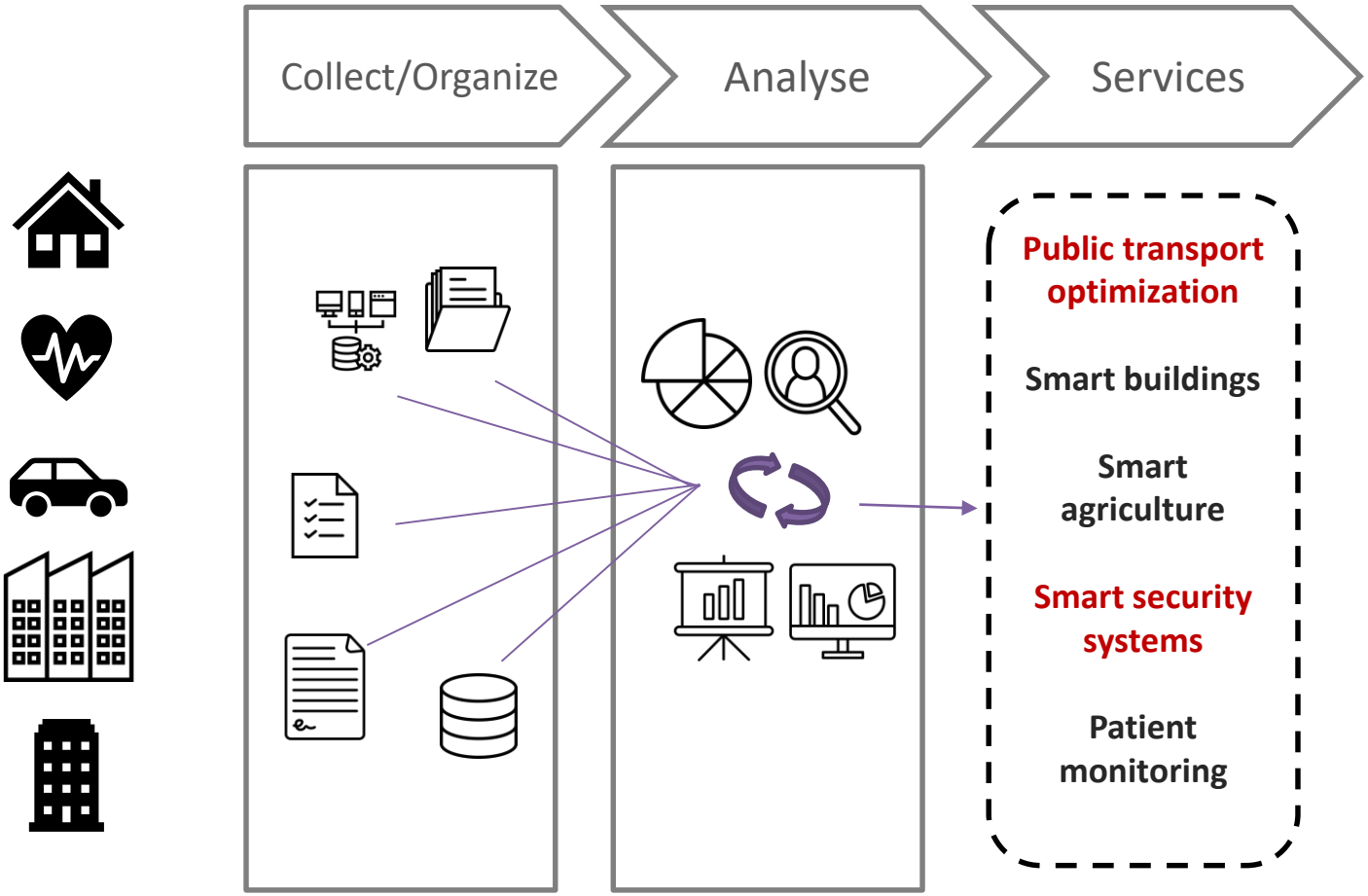
CONTEXT & PROBLEMATIC

Context



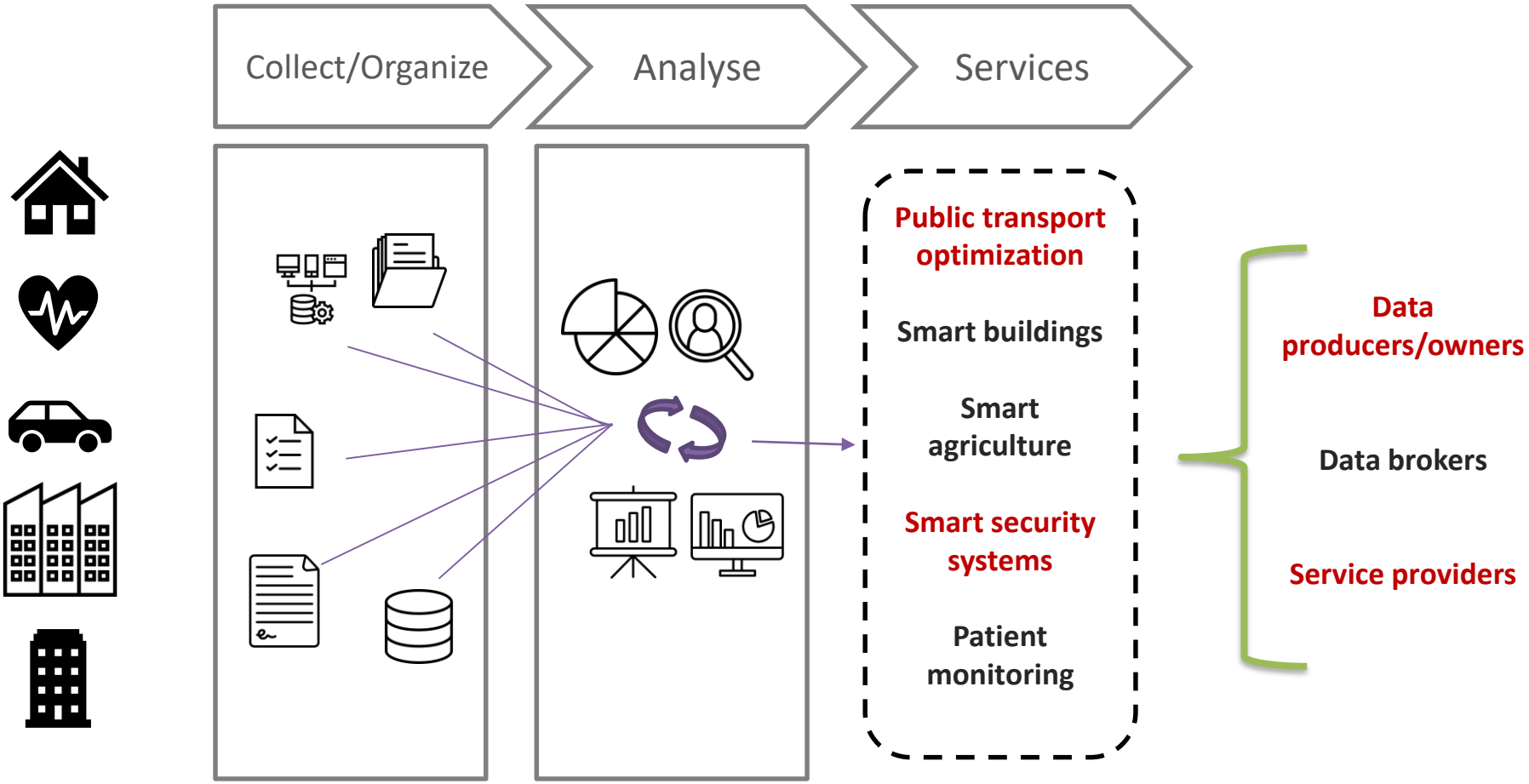
500 B objects connected by 2030 [1]

Context



500 billion objects connected [1]

Context



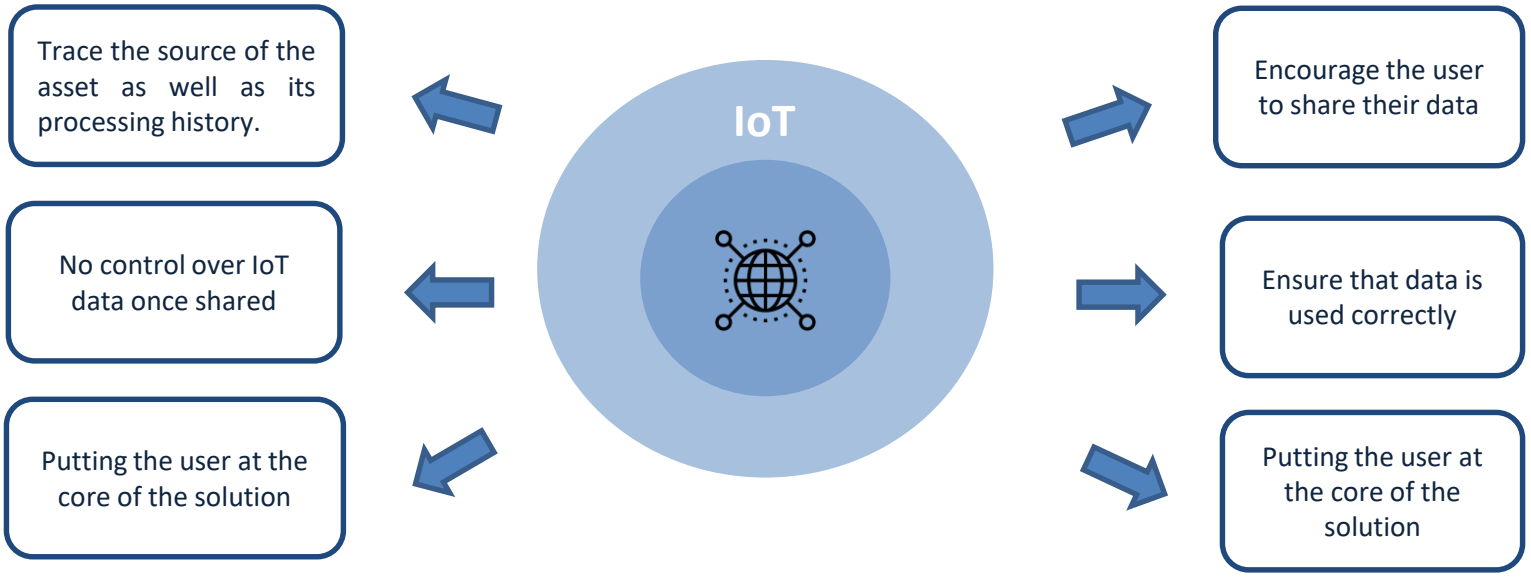
500 billion objects connected [1]

New services

Types of actors

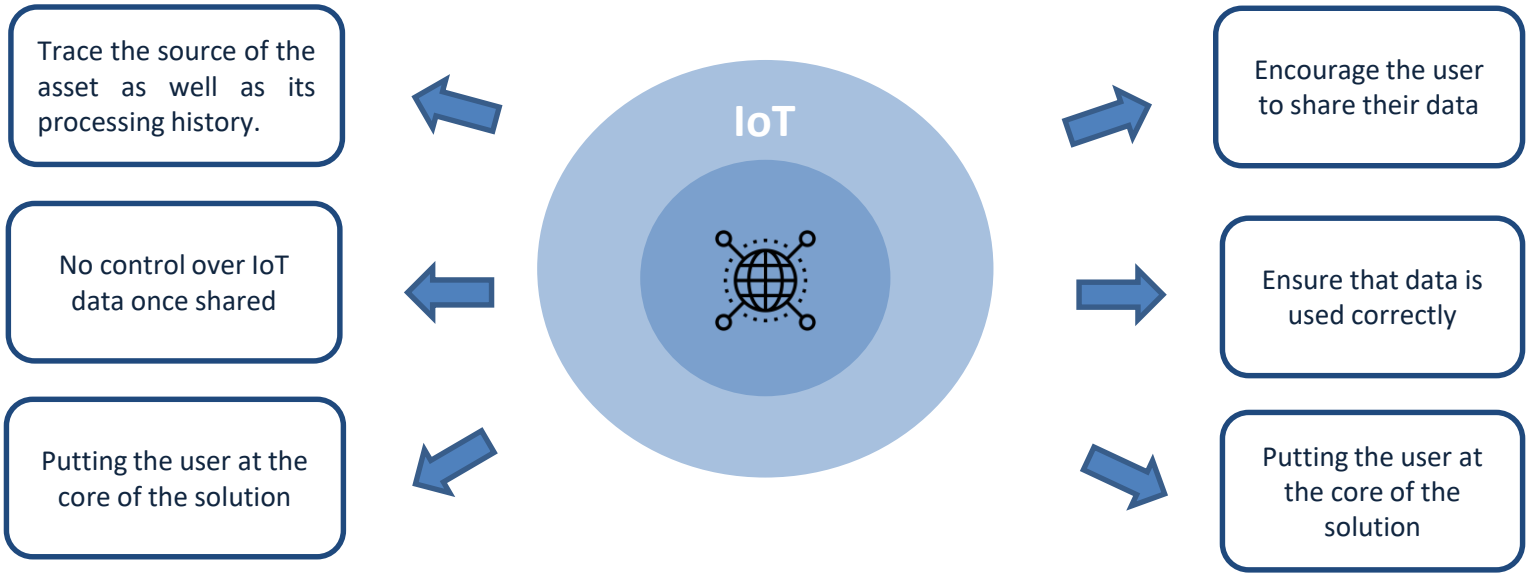
Problematic

Security issues



Problematic

Security issues



(i) allow data owners to be informed where their data is being involved

(ii) allow service provider entities to ensure they meet the technical and legal requirements of a given activity

PROPOSED APPROACH

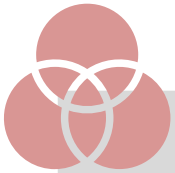
IoT data sharing management system

Value Proposition

Iot data sharing management system supports :

Building user trust and encourage data sharing

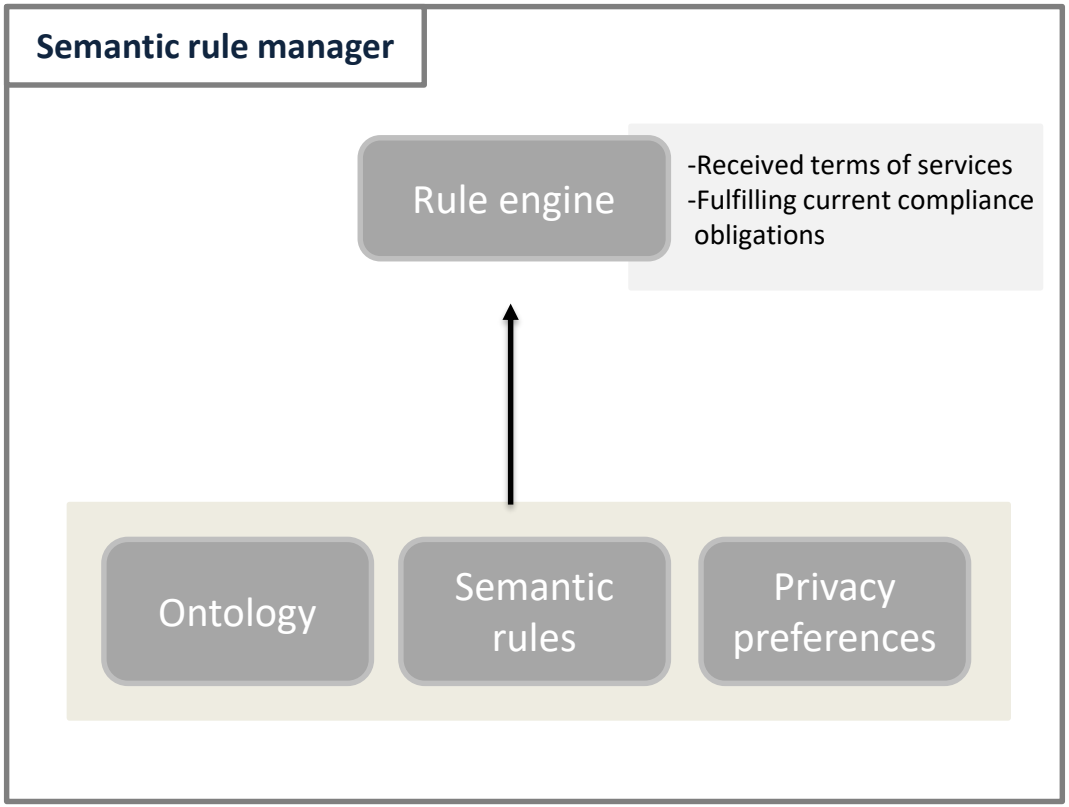
Fulfilling current compliance obligations



Informational self-determination

IoT data sharing management system

Semantic Rule Manager



- Data owners set the requirements that other parties need to respect to be able to use their assets.
- Matching the data owner's preferences with the requester's demand for access entails using the same vocabulary that describes the privacy requirements.

IoT data sharing management system

Data provenance system

- Storing information about the origin of the data the transactions performed on the data, and the history of the processing from its initial source to its current state.
- **Ascending traceability** : data requesters to trace the origin of a data item.
- **Descending traceability**: data providers to be informed where their data is distributed

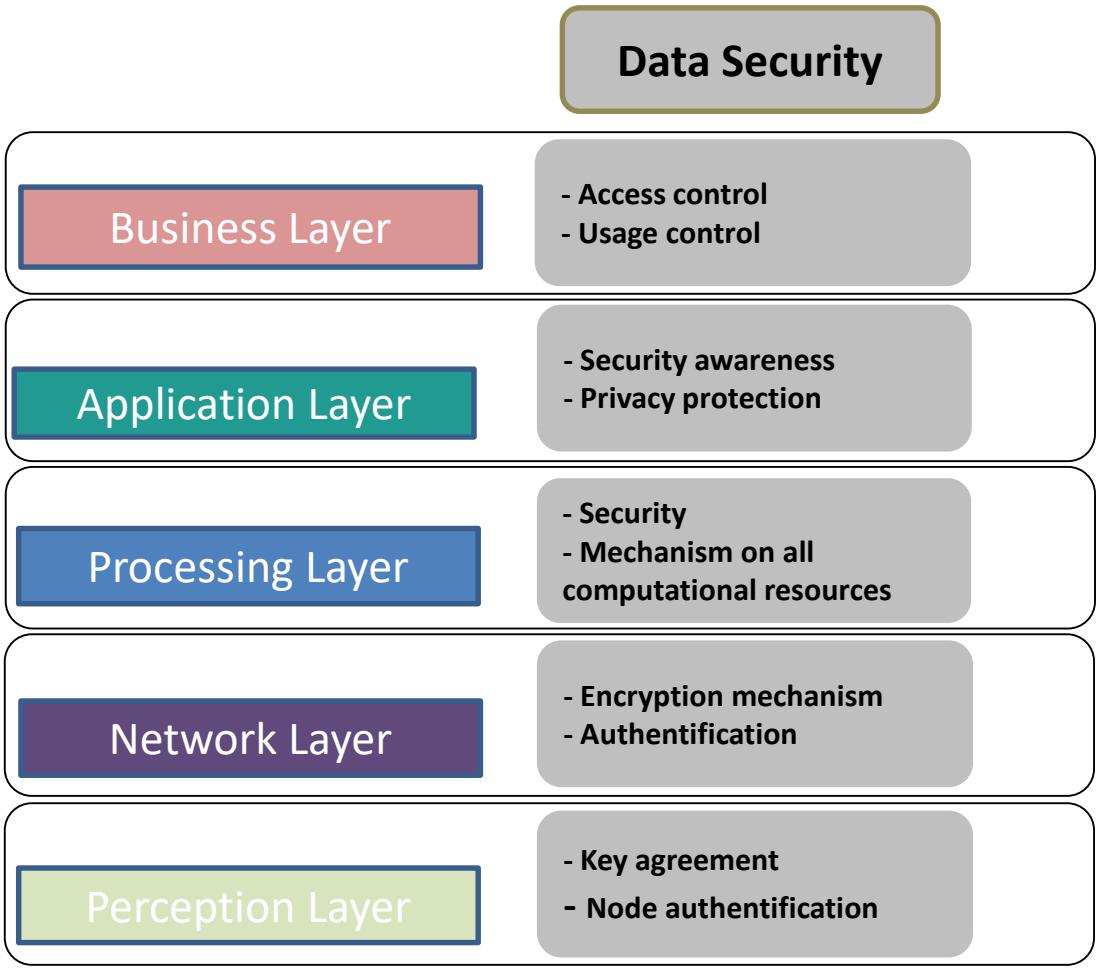
IoT data sharing management system

Data provenance

Models	Architectures	techniques
• PROV [2] • UML2PROV [3] • Ontology-based data provenance (ORDM) [4]	• Centralized architectures • Distributed architectures • N-tier architectures	• Semantic-based techniques • Blockchain-based techniques : BlockPro [5]

IoT data sharing management system

Proposition



M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of internet of things," in 2010 3rd international conference on advanced computer theory and engineering (ICACTE), vol. 5. IEEE, 2010, pp. V5–484.

IoT data sharing management system

Proposition

Data Security

Information Security

Business Layer	- Access control - Usage control
Application Layer	- Security awareness - Privacy protection
Processing Layer	- Security - Mechanism on all computational resources
Network Layer	- Encryption mechanism - Authentification
Perception Layer	- Key agreement - Node authentification

- Data provenance
- Rule manager based on semantic modeling

Our approach

Data transmission

Data collection

IoT data sharing management system

Proposition

	Data Security	Information Security
Business Layer	- Access control - Usage control	- Data governance strategy - Ethical and legal practice
Application Layer	- Security awareness - Privacy protection	- Tools for data monitoring - Metrics to measure rule compliance
Processing Layer	- Security - Mechanism on all computational resources	- Data provenance - Rule manager based on semantic modeling
Network Layer	- Encryption mechanism - Authentification	Data transmission
Perception Layer	- Key agreement - Node authentification	Data collection

Our approach

CHALLENGES & DISCUSSION

Challenges and discussion

- Legal requirements for IoT security in Europe are rarely considered through the building of IoT data management systems.

- A flexible Data provenance system : the system must remain loose enough to not shut down all access at once

- Operational objectives and strategic visions of the involved entities are different and vary from one organization to another, leading to a potentially biased quality of the produced data.

CONCLUSION

Conclusion

- The **data producer** has little to no control over his IoT data once shared, and **data requesters** don't have the ability to trace the source of the asset as well as its processing history to tailor it to their business needs.
- Place agents at the core of a distributed solution : data producers set the requirements that service providers need to respect to be able to use their assets.
- Semantic model based rule manager and data provenance and as a privacy preservation mechanism for IoT applications.
- It is not limited to personal data (GDPR).

Sources

[1] Cisco. (2016) Internet of things at-a-glance. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/se/internetof- things/at-a-glance-c45-731471.pdf?dtid=osscdc000283.
[2] P. Buneman, A. Gascon Caro, L. Moreau, and D. Murray-Rust, “Provenance composition in PROV,” 2017.
[3] C. Sàenz-Adàn, L. Moreau, B. Pérez, S. Miles, and F. J. Garcia- Izquierdo, “Automating provenance capture in software engineering with uml2prov,” in International Provenance and Annotation Workshop. Springer, 2018, pp. 58–70.
[4] H. Olufowobi, R. Engel, N. Baracaldo, L. A. D. Bathen, S. Tata, and H. Ludwig, “Data provenance model for internet of things (iot) systems,” in International Conference on Service-Oriented Computing. Springer, 2016, pp. 85–91.
[5] U. Javaid, M. N. Aman, and B. Sikdar, “Blockpro: Blockchain based data provenance and integrity for secure iot environments,” in Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, 2018, pp. 13–18.

ANY QUESTIONS?