Enhanced IoT Data Sharing Management using semantic rule manager and Data Provenance

DMCESE 2021 Workshop

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

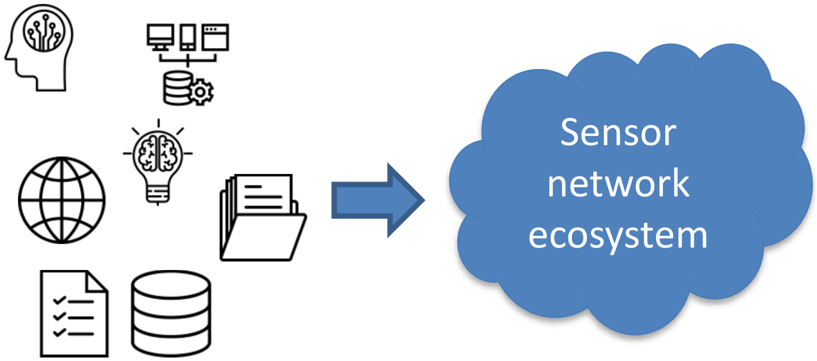
LIUPPA

Outline

- **Context & Problematic**
- **Proposed approach**
  - ○ Use case : Smart agriculture
  - ○ Proposition : IoT Data Sharing Management system
- **Challenges and discussion**
- **Conclusion**

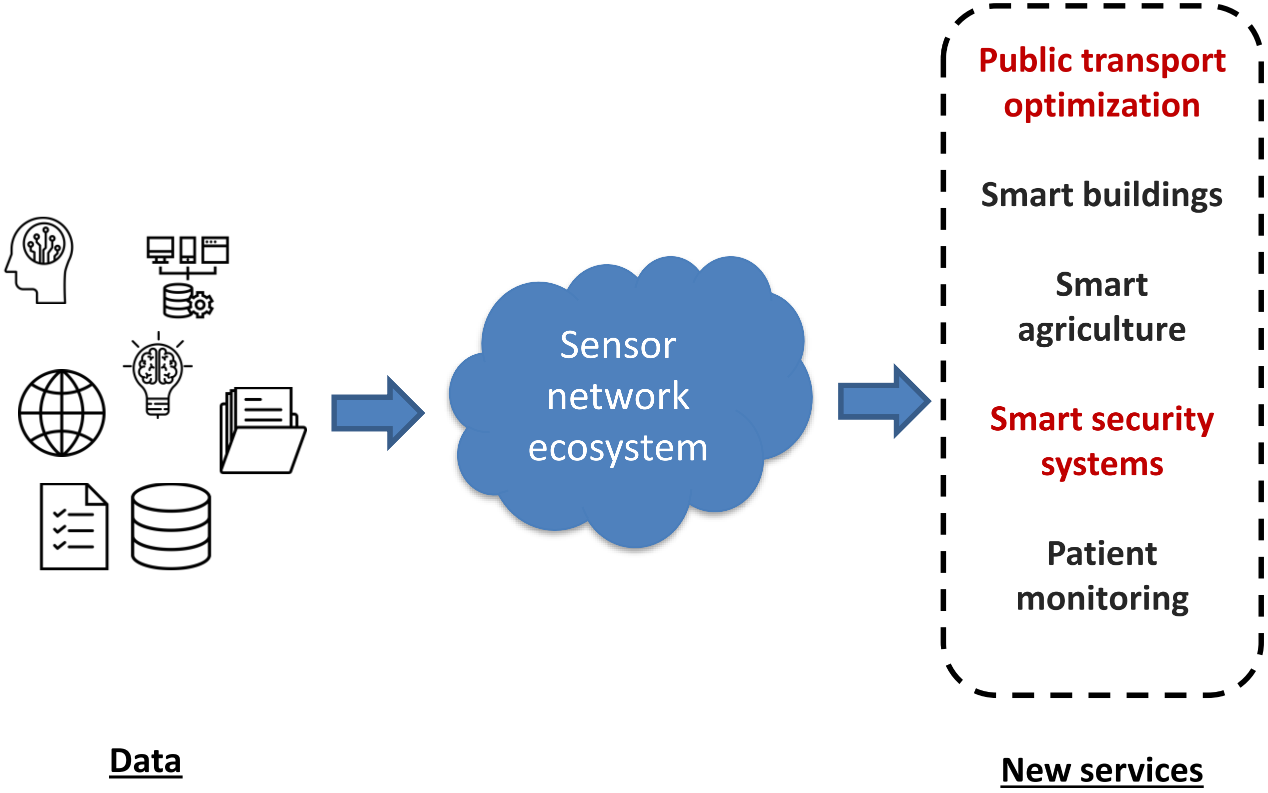
CONTEXT & PROBLEMATIC

Context



<u>Data</u>

Context



Data

Sensor network ecosystem

Public transport optimization

Smart buildings

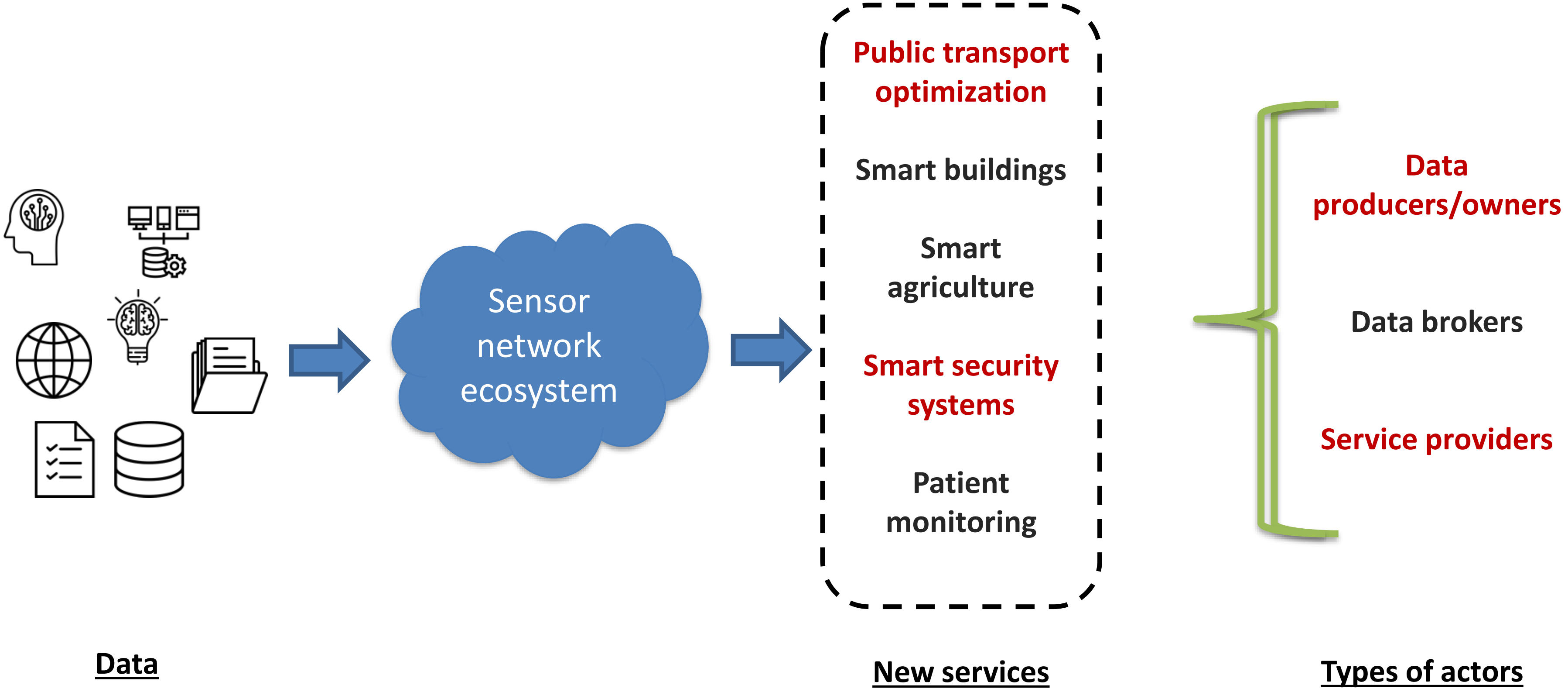
Smart agriculture

Smart security systems

Patient monitoring

New services

Context



Sensor network ecosystem

Public transport optimization

Smart buildings

Smart agriculture

Smart security systems

Patient monitoring

Data producers/owners

Data brokers

Service providers

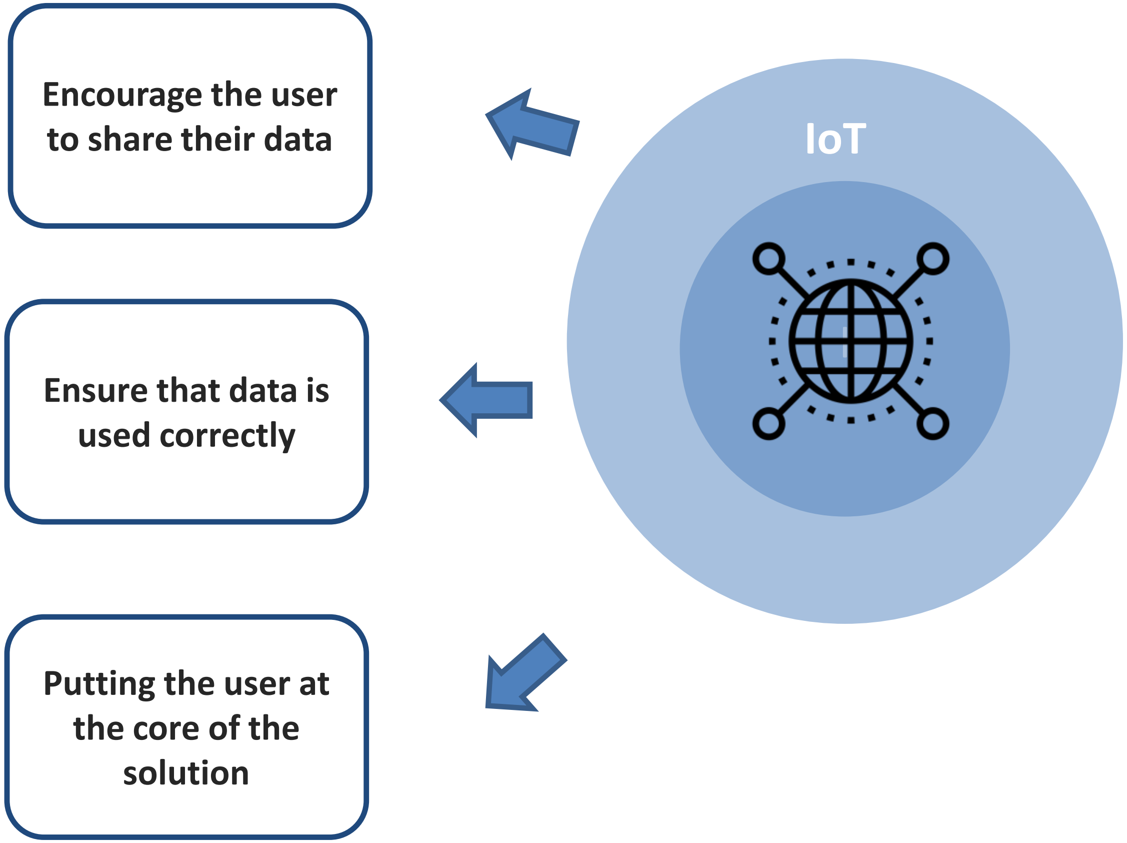
Data

New services

Types of actors

Problematic

Security issues



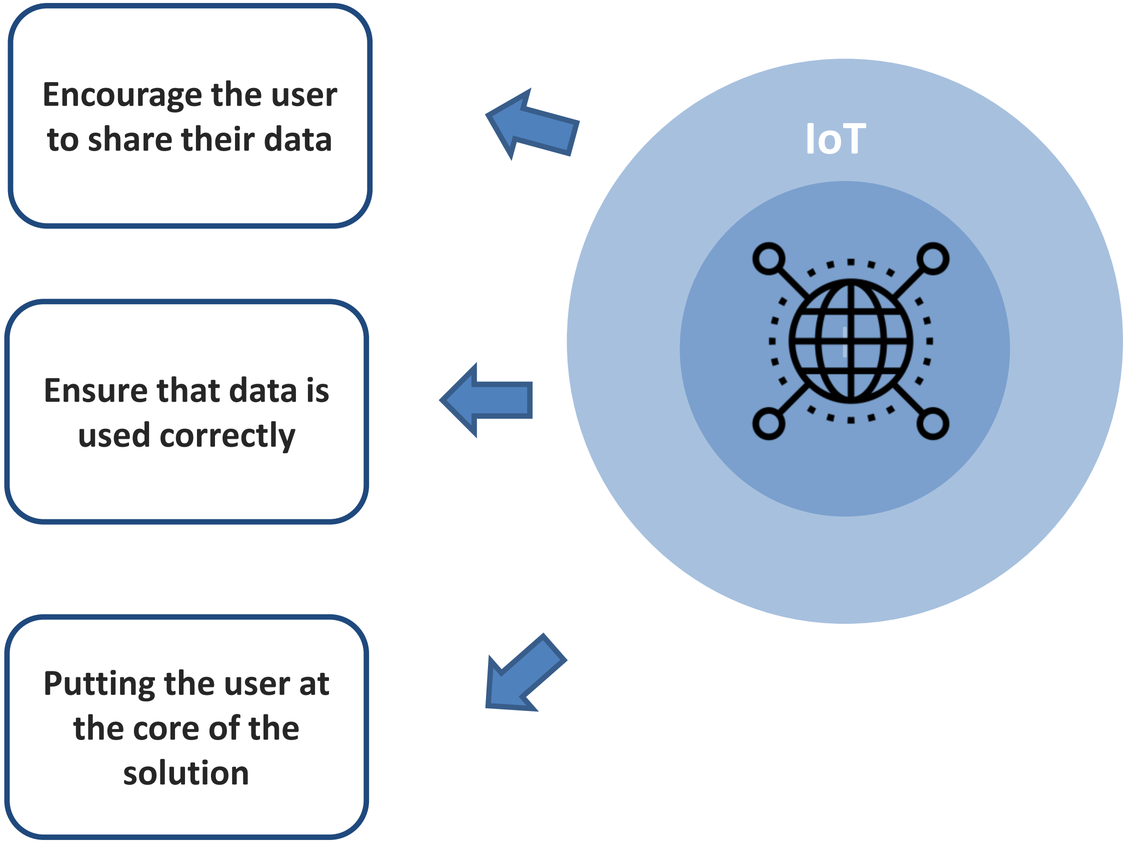
Encourage the user to share their data

Ensure that data is used correctly

Putting the user at the core of the solution

Problematic

Security issues



Encourage the user to share their data

Ensure that data is used correctly

Putting the user at the core of the solution

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

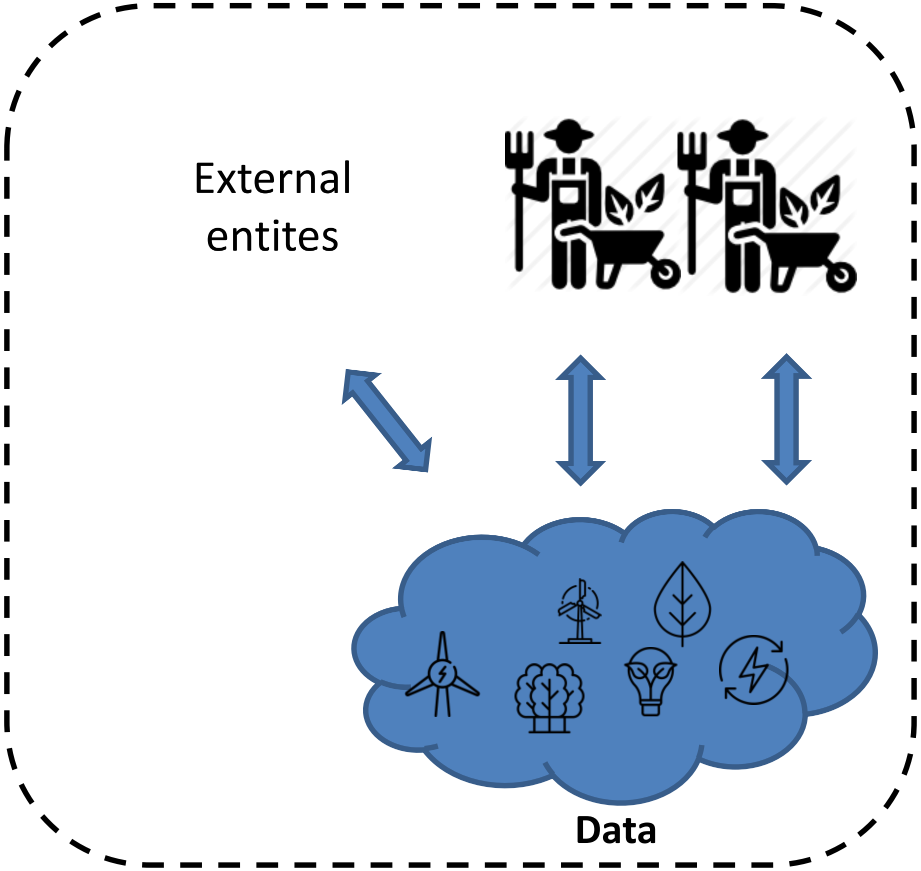
(ii) allow service provider entities to ensure they meet the technical and legal requirements of a given activity

(iii) Informational self-determination

PROPOSED APPROACH

IoT data sharing management system

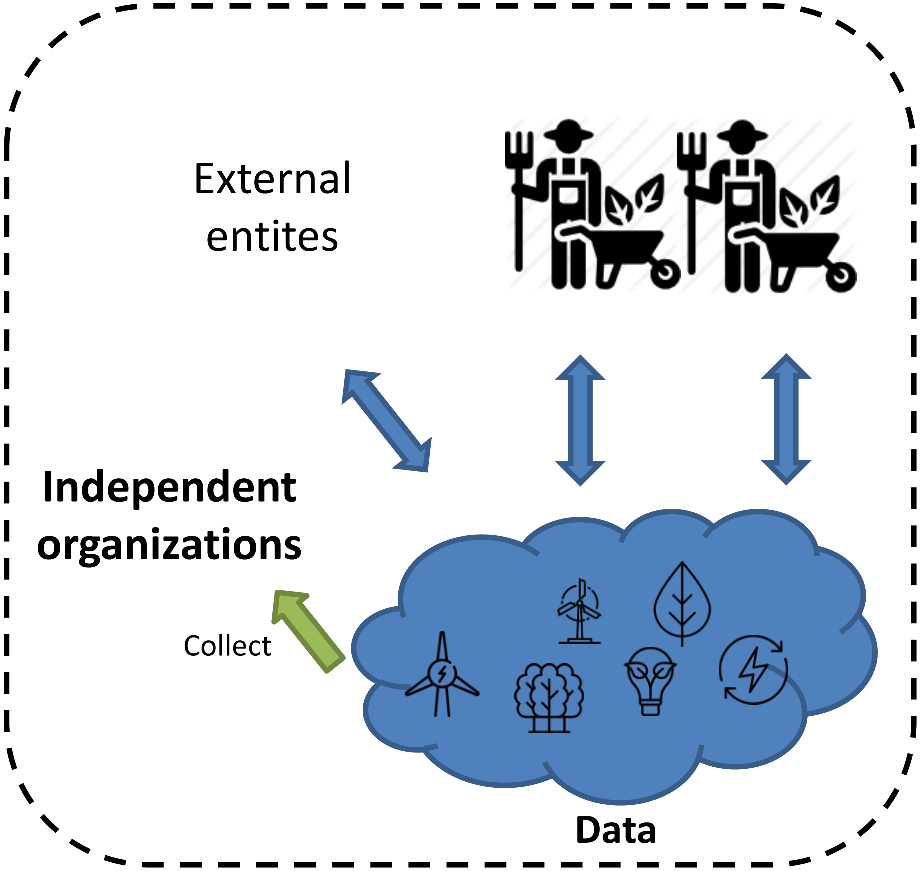
Case study: smart agriculture



....

IoT data sharing management system

Case study: smart agriculture



External entites

Independent organizations

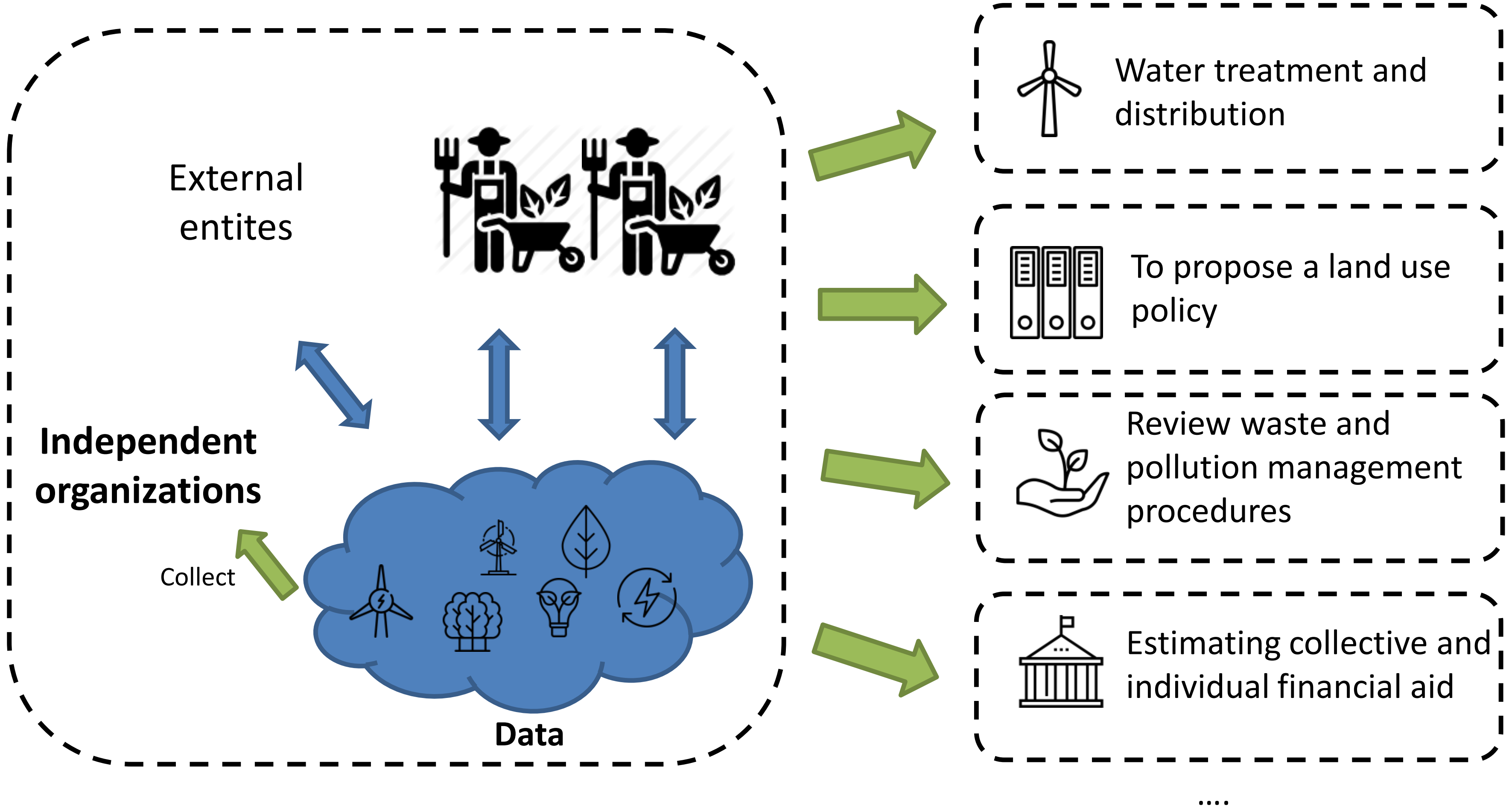
Collect

Data

....

IoT data sharing management system

Case study: smart agriculture



External entites
Independent organizations
Collect
Data
Water treatment and distribution
To propose a land use policy
Review waste and pollution management procedures
Estimating collective and individual financial aid
....

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.

Data provenance

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.

Data provenance

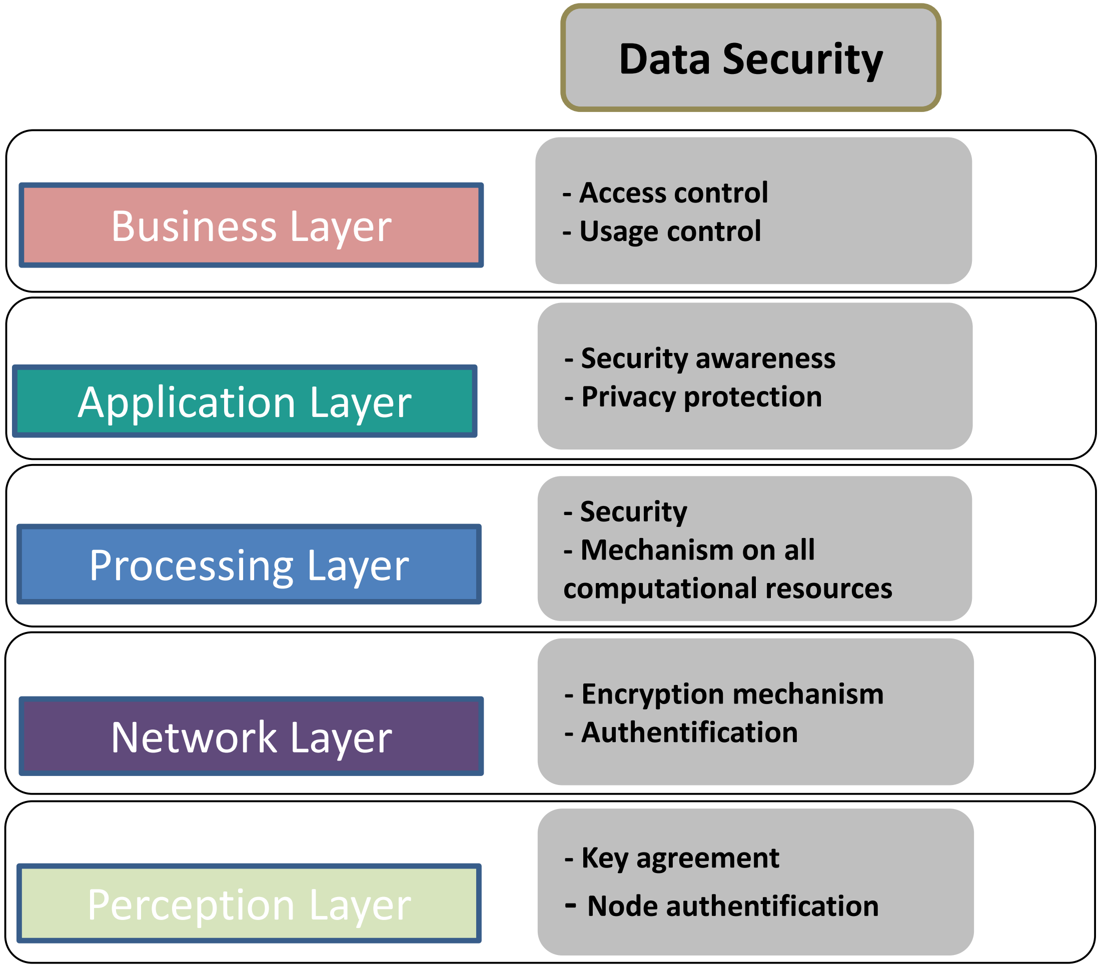
- Storing information about the origin of the data, the transactions performed on the data, and the history of the processing from its initial source to its current state.

- **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

Proposition

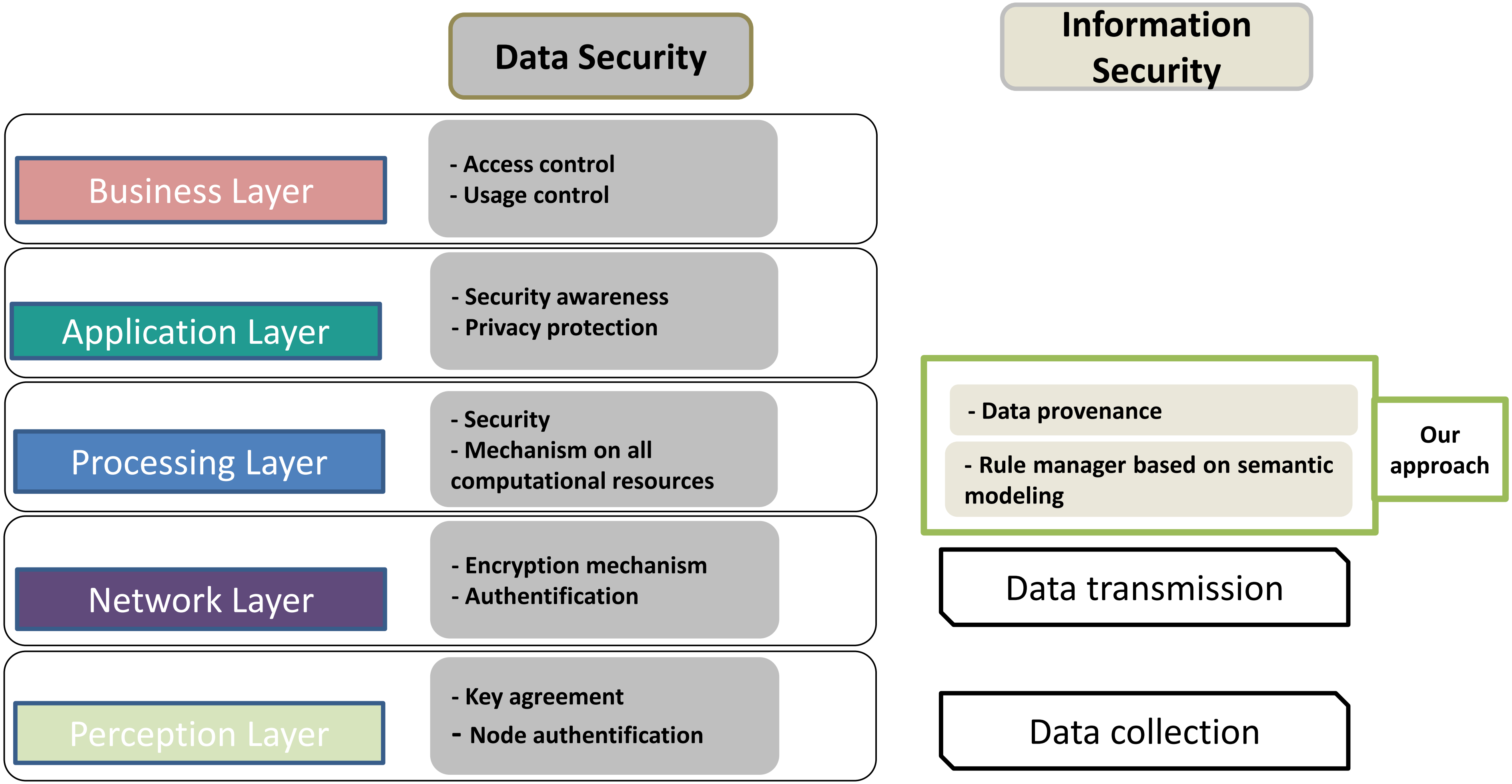


	Data Security
Business Layer	- Access control - Usage control
Application Layer	- Security awareness - Privacy protection
Processing Layer	- Security - Mechanism on all computational resources
Network Layer	- Encryption mechanism - Authentification
Perception Layer	- Key agreement - Node authentification

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

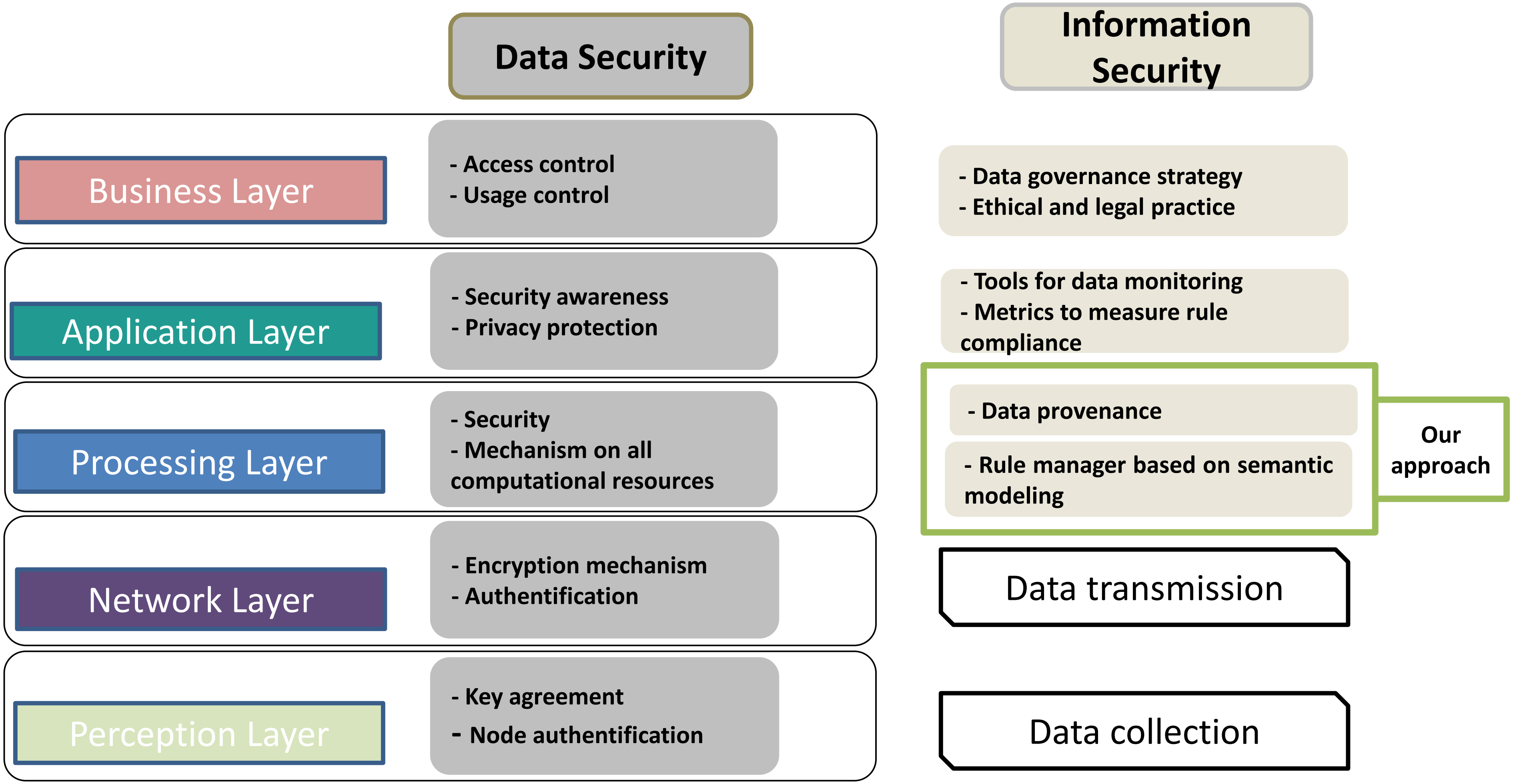
Our approach

Data transmission

Data collection

IoT data sharing management system

Proposition



Data Security

Information Security

Business Layer

- Access control
- Usage control

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 governance strategy
- Ethical and legal practice

- Tools for data monitoring
- Metrics to measure rule compliance

- Data provenance

- Rule manager based on semantic modeling

Our approach

Data transmission

Data collection

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).

ANY QUESTIONS?