



HAL
open science

IoT: maîtrise des flux d'information

Manuel Munier, Vincent Lalanne, Tatiana Shulga-Morskaya

► **To cite this version:**

Manuel Munier, Vincent Lalanne, Tatiana Shulga-Morskaya. IoT: maîtrise des flux d'information. INFORSID 2019 - atelier "Génie logiciel et qualité de l'internet des objets", Jun 2019, Paris, France. hal-02412966

HAL Id: hal-02412966

<https://univ-pau.hal.science/hal-02412966>

Submitted on 16 Dec 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

IoT : maîtrise des flux d'information

Manuel MUNIER¹

Vincent LALANNE¹

Tatiana SHULGA-MORSKAYA²

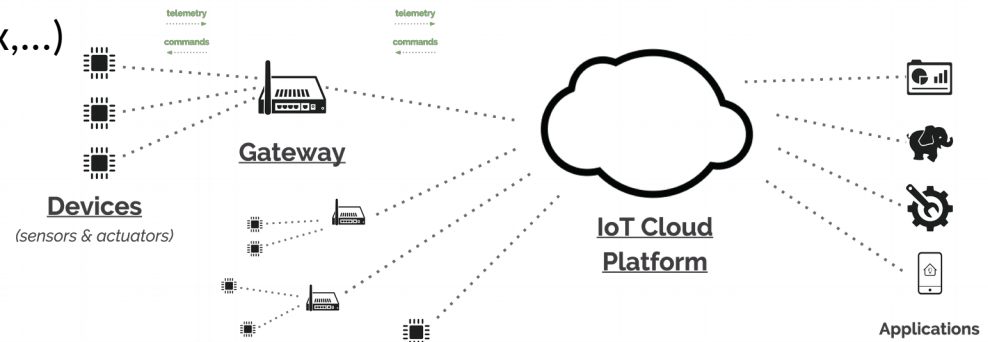
¹ Université de Pau et des Pays de l'Adour / E2S UPPA / LIUPPA – EA 3000

² Université de Bordeaux / CERCCLÉ – EA 7436

Problématique

Internet des objets → de nombreux travaux sur le volet technique

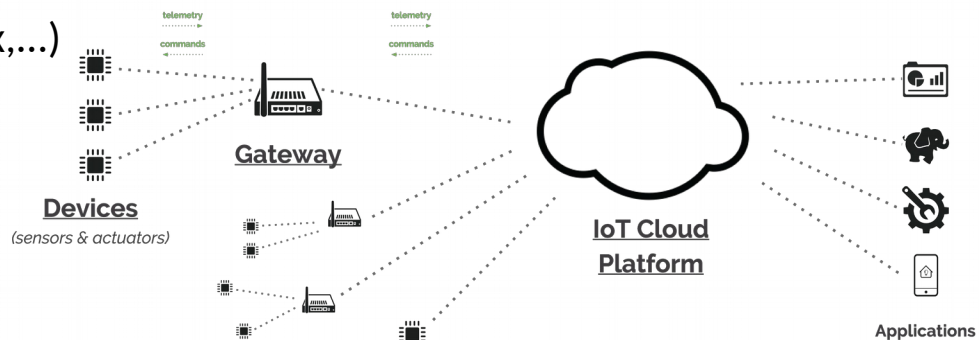
- Protocoles de communication (radio, réseaux,...)
- Architectures matérielles et logicielles
- Consommation énergétique
- Sécurité ?



Problématique

Internet des objets → de nombreux travaux sur le volet technique

- Protocoles de communication (radio, réseaux,...)
- Architectures matérielles et logicielles
- Consommation énergétique
- Sécurité ?



Mais il y a également un volet organisationnel

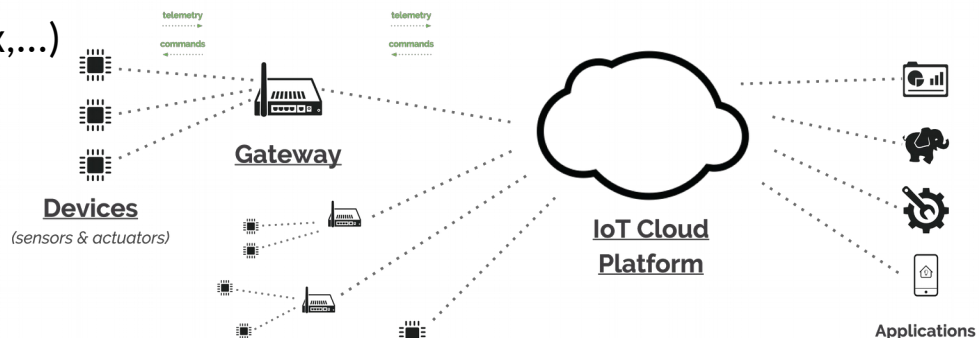
- De nombreux acteurs, avec des objectifs / enjeux propres
- De nombreuses informations, parfois à caractère personnel
- Des réglementations différentes
- Et des usagers...



Problématique

Internet des objets → de nombreux travaux sur le volet technique

- Protocoles de communication (radio, réseaux,...)
- Architectures matérielles et logicielles
- Consommation énergétique
- Sécurité ?



Mais il y a également un volet organisationnel

- De nombreux acteurs, avec des objectifs / enjeux propres
- De nombreuses informations, parfois à caractère personnel
- Des réglementations différentes
- Et des usagers...



Constat

- Les usagers ne sont vus que comme des capteurs
- Malgré l'évolution des lois, les usagers n'ont toujours que peu de moyens pour exercer leurs droits



Bâtiments intelligents, IoT & co.

Contexte IoT

- Bâtiments intelligents (→ villes intelligentes)
 - Prolifération de capteurs : données sur les usagers, leur environnement, leurs profils,...
 - Actionneurs → impact sur l'environnement de l'utilisateur
 - Objectif : proposer de nouveaux services
 - ➔ *Gestion intelligente l'énergie dans les bâtiments*
 - ➔ *Optimisation des transports en commun*
 - ➔ *Ciblage de l'information diffusée*
 - ➔ *Smart environments*
- Les infrastructures identifient 3 types d'acteurs
 - Les **producteurs** → données primaires
 - Les **data brokers** : collecte, stockage, agrégation, diffusion de données (→ données enrichies)
 - Les **tiers** de traitement



Problématique

- Consentement (initial) de l'utilisateur : lorsqu'il fournit des données (en échange d'un « service »)
- Mais inquiétude quant à la diffusion « non maîtrisée » de ces données à des acteurs (inconnus)
- Si l'utilisateur devient réticent à fournir « ses » données, remise en cause du paradigme « smart xxx »



Autodétermination informationnelle

Contexte juridique

- Loi pour une République numérique (7 octobre 2016)
 - « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant. »
 - Ce droit présuppose que l'utilisateur doit
 - ➔ Être (re)placé au cœur du système de traitement
 - ➔ Être suffisamment informé pour faire des choix éclairés
 - ➔ Avoir des moyens techniques pour les imposer aux responsables de traitement
- RGPD (26 mai 2018)
 - Droit d'accès (art. 15)
 - Droit de rectification (art. 16)
 - Droit à l'effacement (art. 17)
 - Droit d'opposition (art. 21)
 - Droit à la limitation du traitement (art. 18)
 - Droit à la portabilité (art. 20)
 - Droit à ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage (art. 22)

Problématique

- Pour exercer son droit à l'ADI, tout utilisateur, même sans connaissances en informatique, devrait avoir des moyens techniques, faciles à comprendre et à utiliser, ainsi que des moyens juridiques pour faire valoir ses droits auprès des responsables de traitement, l'autorité de protection et le juge.



Approche & challenges (1/3)

Sécurité des communications

● Architecture

- Capteurs, passerelles, brokers, nœuds intermédiaires,...
- Topologie, distribution

● Protocoles

- Quelles données échangées ? Quel format ? Quelles métadonnées ?
- Sécurité informatique « classique » (authentification, chiffrement, sémantique,...)
- Environnement « Systèmes de Systèmes » → pas de contrôle à 100 % sur l'infrastructure
- Pas de contrôle global → contrôles locaux, contrats point à point
- Expression des politiques d'usage → contrats point à point



Approche & challenges (2/3)

Sécurité de l'information

● Traçabilité

- Ascendante : d'où viennent les données ? Qui les a fournies ?
- Descendante : où sont diffusées mes données ? Dans quels traitements sont-elles utilisées ?
- Objectif : mieux contrôler les flux d'information
- NB : dilemme traçabilité / anonymisation

● Gestion des risques

- Environnement « Systèmes de Systèmes » → pas de contrôle à 100 % sur l'infrastructure
- Nouvelles vulnérabilités & nouvelles menaces
- Nouveau critère « maîtrise de l'information » dans les démarches gestion des risques
- Objectifs : résilience, « qualité » des données, identification des responsabilités



Approche & challenges (3/3)

Droit

- Conformité des mécanismes proposés
 - Respect des réglementations (ex : anonymisation, vie privée, secret industriel,...)
 - Validité des « preuves » déduites

- Impacts sur les acteurs
 - Exercice du droit à l'ADI pour les utilisateurs
 - Identification des responsabilités en cas de litige
 - Qui doit implémenter ces technologies ? Quels moyens ?
 - Notion de « propriété des données » ?



Travaux connexes

● CNIL

- Plusieurs cahiers IP ont déjà été publiés
- Notamment le n°5 sur les smart cities
 - *Enjeux de l'information dans les villes numériques*
 - *Modèles économiques, à qui profitent ces flux d'information*
 - *Équilibre entre datafication de la ville et protection de nos libertés*
 - *Redonner la main aux autorités garantes de l'intérêt général*

● **Urbanistik** (par JCDecaux !) → 2 cahiers : « la ville collaborative », « la donnée dans la ville »

● **DECODE**

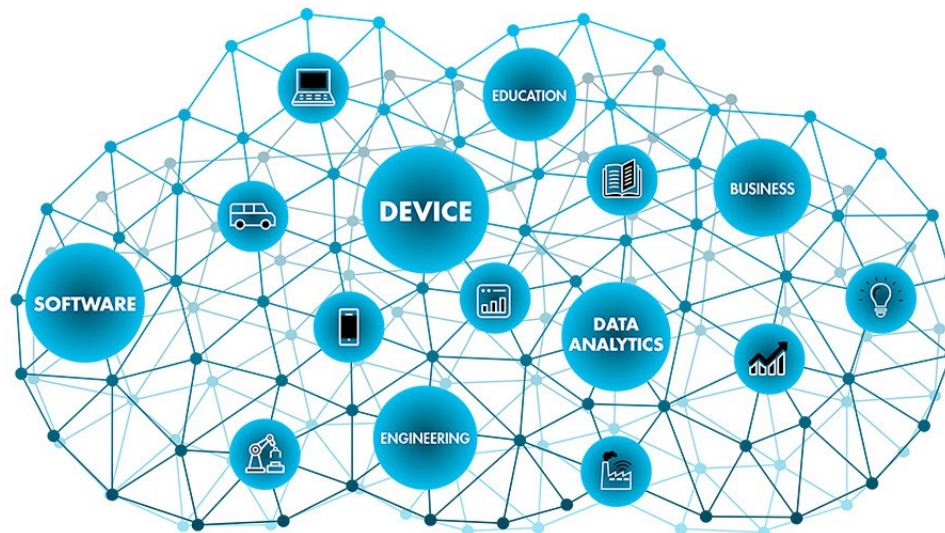
- Projet européen Horizon 2020
- Entièrement basé sur la blockchain pour garantir une sécurité à 100 %
- Politiques de sécurité orientées accès (et non usage)

● Norme **ISO 30141:2018**

- « Internet of Things (IoT) – Reference Architecture »
- Sécurité ???

Vision plus générale

- Protection de la vie privée
 - **Autodétermination informationnelle** → replacer l'utilisateur au centre du dispositif
 - *Privacy and security by design*, droit & numérique,...
- Gestion des risques & sécurité de l'information
 - Enjeux similaires dans les SI des entreprises
 - Traçabilité & co. → **maîtrisabilité**
 - Contrats, confiance, investigation numérique, *data lineage*, *business intelligence*,...



Merci de votre attention

CONTACT

Manuel MUNIER

LIUPPA, EA 3000 – Univ Pau & Pays Adour / E2S UPPA
Mont-de-Marsan, France

manuel.munier@univ-pau.fr

<http://munier.perso.univ-pau.fr/>

