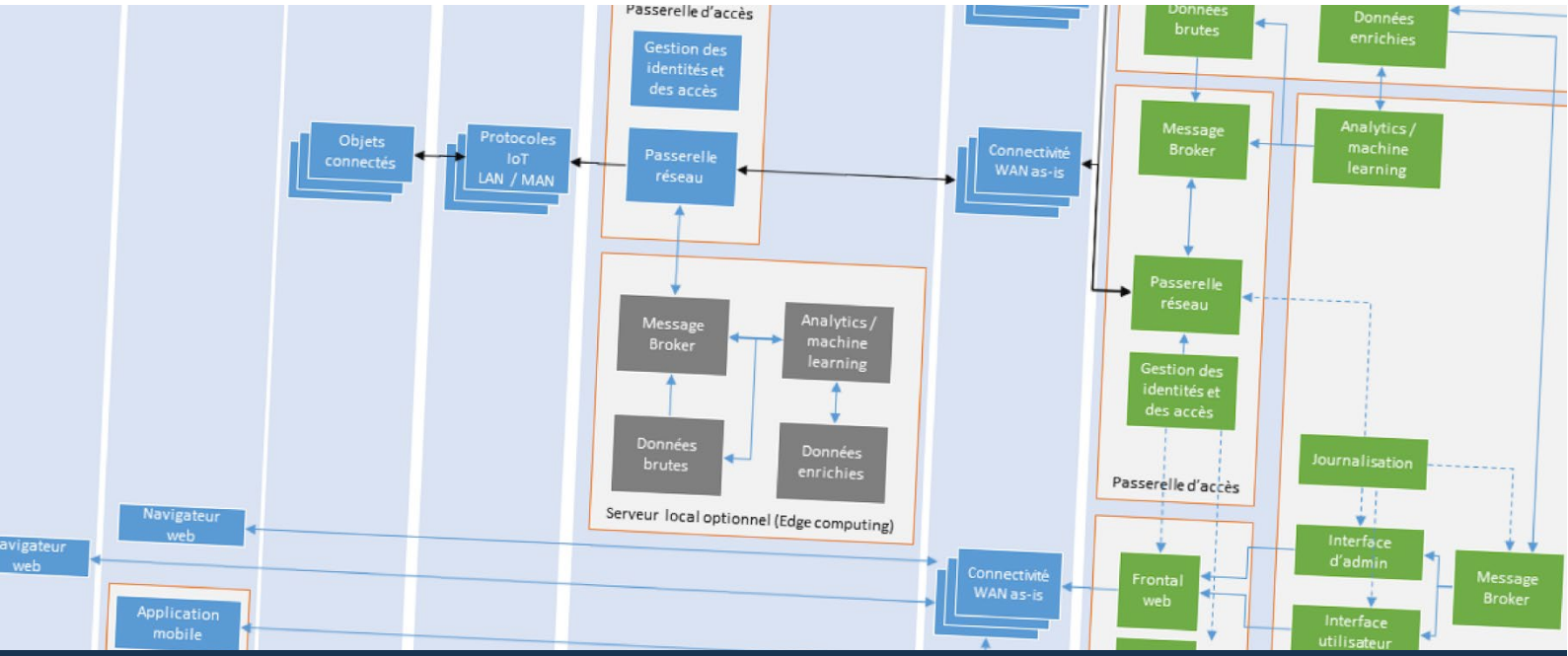
LES FICHES PRATIQUES du CLUSIF - IoT



Peut-on éviter que les objets connectés ne traquent l'activité de leurs utilisateurs ?

Version 1.0

1. Le risque de la surveillance par les objets

La multiplication du nombre d'objets connectés les entourant dans leur vie de tous les jours fait courir à leurs utilisateurs un risque accru de surveillance directe ou indirecte par ces objets :

- Un tracker d'activité révélant vos trajets réalisés en course à pied permettant de déduire l'adresse de votre domicile, celle de votre employeur ou d'autres informations plus sensibles encore
- Un réfrigérateur dévoilera vos habitudes de consommation et permettra potentiellement de déduire vos goûts culinaires douteux ou dangereux pour votre santé. Ils pourraient révéler d'autres information comme votre religion ou votre statut de femme enceinte, etc.

Pour ces raisons, certains utilisateurs seront heureux de pouvoir échapper à cette surveillance et pourraient souhaiter se tourner vers une approche protectrice : le pseudonymat (pensez à la manière dont une plaque d'immatriculation vous permet d'échapper à la surveillance du quidam, mais pas forcément des forces de l'ordre)

2. Etablir la confiance

Un des enjeux de la sécurité des IoT sera d'établir une relation entre son propriétaire ou un usager occasionnel et l'ensemble des services avec lesquels cet objet autonome pourra collaborer.

Par exemple je loue un gîte dans lequel je trouve un réfrigérateur connecté. Je souhaite utiliser mon compte et mon moyen de paiement chez mon épicier en ligne afin de gérer mes repas à l'aide de cet équipement.

Que faut-il pour mettre en place ce scénario dans un cadre de confiance ?

Le réfrigérateur ne devra pas connaître mon identité, seulement ma solvabilité.
L'approche proposée par le pseudonymat est celle d'un tiers de confiance délivrant des pseudonymes en échange de la fourniture des garanties requises pour me retrouver si les choses tournent mal. Pour réaliser ce service de pseudonymat, un registre distribué, par exemple une blockchain, peut être envisagé, mais c'est loin d'être suffisant. Un opérateur de pseudonymat pour l'IoT doit :

- Établir une relation avec forte avec l'identité d'un futur usager ou propriétaire d'IoT
- Être garant qu'un IoT actif pourra être réassocié à son usager en cas d'enquête
- Être garant de l'origine des métadonnées portées par l'IoT (pseudonyme, bitcoin wallet…)
- Ne pas être à l'initiative de l'association entre un usager et un IoT
- Ne pas être à l'initiative de la révocation de la liaison d'un IoT et son usager.

3. Pour une chaîne de confiance et un écosystème

Il existe ensuite un véritable risque de mettre des attributs qui rendent le pseudonyme relativement trivial à révéler, mais aucun système n'est parfait, tant que l'on peut faire des croisements de différentes sources.
La blockchain NameCoin pourrait être le dépositaire des pseudonymes et des métadonnées des objets connectés assurant une fonction de tiers de confiance entre les propriétaires de ces derniers et les services qui seraient sollicités par les objets. La vérification de la blockchain est une opération simple et son intégrité est une des clés du système.
Le rôle d'intermédiaire de confiance peut être tenu par tous les services qui répondront à un simple cahier des charges concernant l'identification de clients demandant des pseudonymes, la conservation sécurisée des secrets utilisés (eg. clés privées), l'usage réglementé de ces derniers en cas d'enquête.

Ces services pourront fixer librement le prix de leur prestation et offrir des services supplémentaires en rapport avec les objets et leur gestion (portefeuille d'objet, surveillance d'objet, mutualisation d'objet, prêt d'objet, communication / échange entre objets, fonction de paiement…). Le besoin d'interopérabilité entre ces différents services est essentiel et devra reposer sur des protocoles standards, encore à l'état de travaux de spécification (eg. Decentralized IDentifiers[1]).

Pour définir un cycle de vie de l'objet et de sa projection (digital twin) il faudrait définir au moins un attribut indiquant son état au regard du pseudonyme. Comme un pseudonyme est fortement lié à un propriétaire quand celui-ci cède l'objet, il doit désactiver son pseudonyme, afin que les nouvelles transactions portent sur le nouveau propriétaire et le nouveau pseudonyme. Un objet sans pseudonyme actif serait disponible pour un nouvel utilisateur.

4. Vers des agents autonomes

Il existe un énorme enjeu sur les plates-formes IoT car elles vont capter tous les états des objets. Mais il y a bien plus, c'est l'autonomie des objets, ou plutôt des agents. Un capteur peut seulement dire s'il fait froid ou chaud, un agent est lui capable de combiner plusieurs sources de données (capteurs, historique, données météo) pour déterminer une conduite à tenir.
L'agenda familial pourra dire : il va faire chaud mais la maison sera inoccupée, je vais appliquer une mesure passive (fermeture des stores, réduction des échanges d'air, limitation de la production de chaleur intérieur par les appareils électrique). Cette approche agent autonome pose aussi la question de leur cycle de vie.

Pourquoi réinitialiser un agent climatisation si l'on change de propriétaire ? Son expérience acquise sur le bâtiment sera profitable aux prochains occupants.
Il devra sans doute être mis au courant des nouvelles contraintes (taille famille, fournisseur d'énergie, équipements, travaux …), mais son autonomie devrait lui permettre de s'adapter. On sent poindre la science-fiction ...

ⓘ Point de vue du RSSI

*Dans une optique de responsabilité vis-à-vis des utilisateurs des objets, le RSSI, qu'il soit concepteur ou acheteur d'objets connectés, doit être attentif à ne pas permettre une surveillance de ces utilisateurs. Une approche «*privacy-by-design *» doit prévaloir en amont de ces projets.*

[1] https://w3c-ccg.github.io/did-spec/

LES FICHES PRATIQUES

L'intégralité de la FAQ IoT et la liste des membres qui ont contribué
à son élaboration sont consultables sur le site du CLUSIF : **www.clusif.fr/publications**

CLUSIF