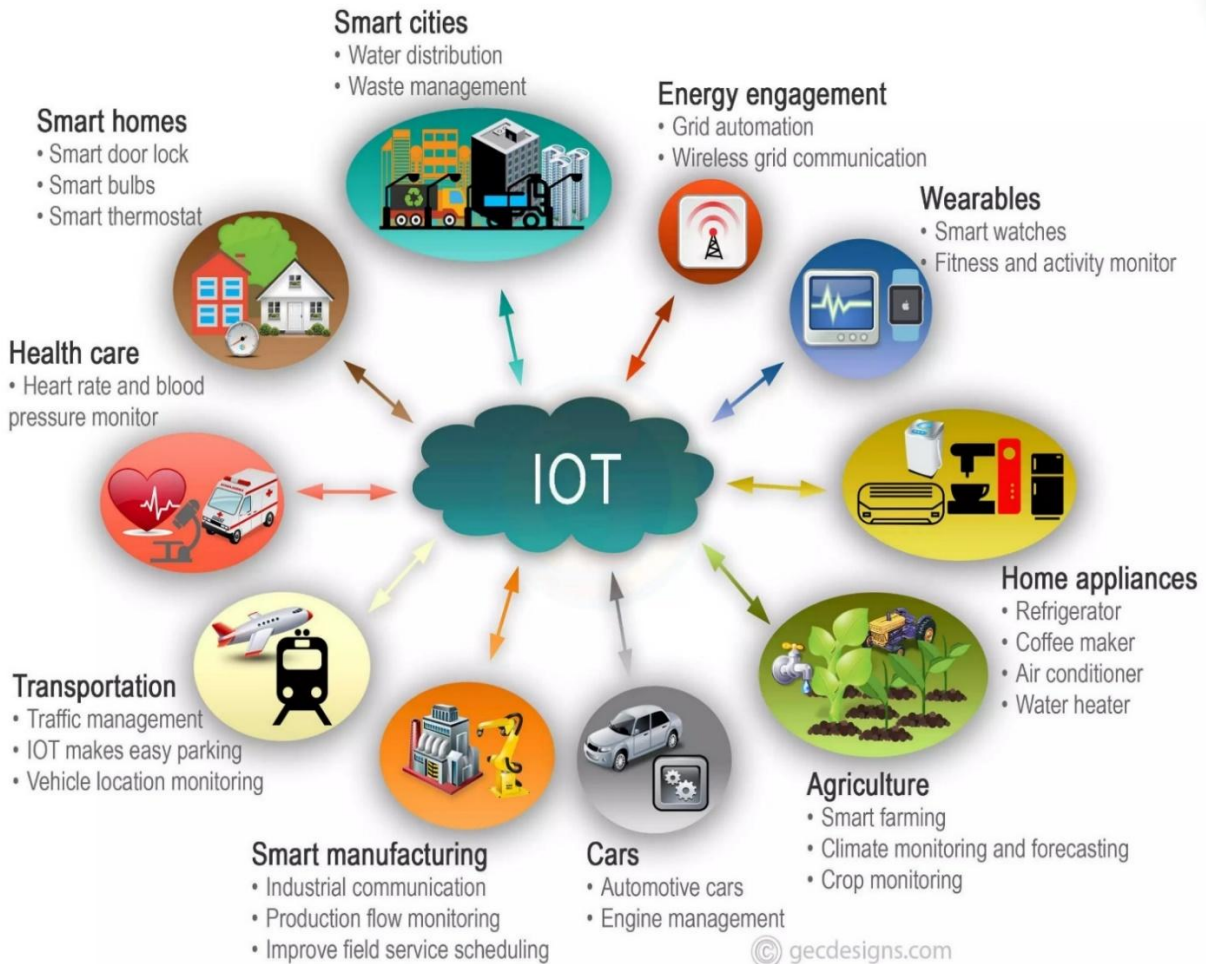


IoT – Internet of Thing

L'Internet des objets

Les objets connectés sont de plus en plus présents dans notre quotidien.

Du développement de leurs infrastructures techniques, que l'on appelle l'« Internet des objets », à celles de l'« Internet du tout connecté », les technologies convergent aujourd'hui avec l'intelligence artificielle et le big data vers un « Internet des comportements » dont l'enjeu est désormais l'analyse comportementale.



Qu'est-ce que l'IoT ?

L'Internet des objets (IoT) désigne l'interconnexion de millions d'appareils et de capteurs intelligents connectés à Internet. Ces capteurs et ces appareils connectés collectent et partagent des données qui seront utilisées et analysées par des organismes, des entreprises, des villes, des gouvernements, des hôpitaux et des particuliers.

Par exemple, un thermostat connecté règle la température intérieure de votre logement avant votre arrivée après une journée de travail sans intervention de votre part.

Pour prévoir le moment optimal de réglage du thermostat avant votre retour, votre système IoT (voiture, maison, services Internet ...) peut s'appuyer sur une modélisation du trafic en temps réel dans votre zone, utiliser des données relatives à vos trajets habituels et à la géolocalisation de votre voiture en temps réel.

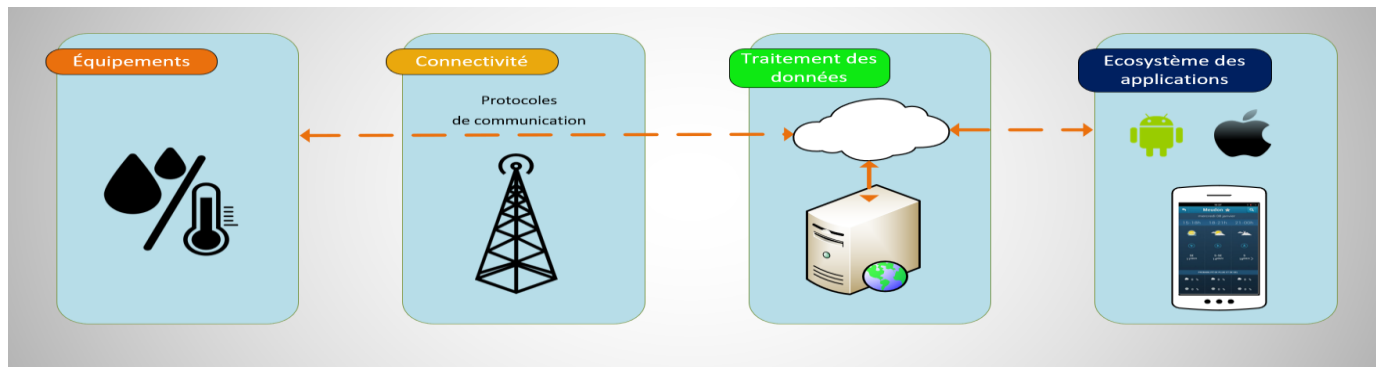
De plus, les données IoT relatives aux thermostats de chaque client peuvent être analysées par des fournisseurs d'énergie dans le but d'optimiser la production d'énergie.

Quelques aspects à améliorer :

- Le volume des données produites par un système IoT peut devenir très important (on parle de Big Data) et pose un problème de sauvegarde.
- La sécurité des données est devenue un enjeu mondial entre les pays, les entreprises et les citoyens.

La chaîne de valeur de l'IoT

La chaîne de valeur de l'IoT est constituée d'**équipements**, dotés de moyen de **communication**, publient des données auprès d'**un serveur**. Ce serveur traite ces données et les mets à disposition de **services** qui peuvent les "consommer".



Les équipements

- Simples capteurs capables de communiquer des grandeurs physiques (fonctionnement en émetteur).
- Capteurs pilotés à distance (fonctionnement bidirectionnel).
- Objets complexes : robots, voitures autonomes, ...

La connectivité des objets (filaire ou hertzien)

Le module de connectivité permet aussi de gérer le « cycle de vie de l'objet », c'est-à-dire, l'authentification et l'enregistrement dans le réseau, la mise en service, la mise à jour et la suppression de l'objet du réseau

Traitement des données

Ce traitement s'appuie sur des serveurs. Leur fonction est de :

- Collecter les données reçues
- Les exploiter grâce à des algorithmes. L'exploitation va consister à associer de nombreuses données afin de déduire de nouvelles informations et proposer de nouvelles actions.
- Mettre à disposition des données traitées ou brutes que les applications pourront consommer.

Ecosystème des applications

Ce sont les applications qui vont travailler en relation avec les serveurs de la plateforme. Ces applications consomment les données et proposent à l'utilisateur une interface homme/machine qui exploite ces dernières. On parle d'écosystèmes car les applications peuvent être de différentes natures et s'appuyer sur des plateformes différentes (mobilité, réseaux sociaux, communication, domotique...)

Les réseaux de télécommunication des objets

	GSM Solution qui consiste à utiliser les réseaux de données existants (4G, 5G, etc.). Très peu adaptée dans la majorité des cas, elle nécessite une carte SIM, et utilise une technologie très consommatrice d'énergie. De plus, elle est relativement onéreuse.
	Bluetooth basse consommation : BLE (Bluetooth Low Energy) - Portée courte. - Faible consommation.
	- Protocole de communication sans fil pour les objets connectés. - Bande de fréquence dédiée. - Portée étendue et faible consommation énergétique.
	- Bande fréquence ultra-étroite (UNB pour Ultra Narrow Band en anglais). - Communication longue distance.

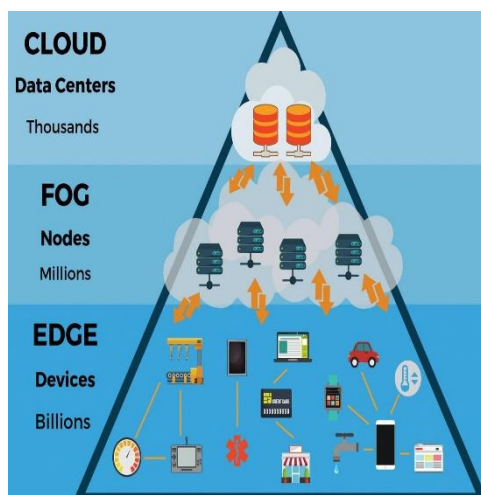


- Simple et faible consommation.
- Communication courte distance.

Les menaces

- Utilisation commerciale des données personnelles/sensibles.
- Piratage.
- Problème de l'atteinte à la vie privée des utilisateurs.

Fog computing



Le fog computing est une architecture qui utilise les clients ou les appareils de "périphérie" des utilisateurs finaux pour réaliser une partie importante du prétraitement et du stockage dont une entreprise a besoin.

Le fog computing a été conçu pour maintenir les données au plus près de la source pour le prétraitement.

Les données de capteur, peuvent être préalablement traitées près de l'endroit où elles ont été collectées. Les informations recueillies avec le traitement préalable peuvent être retransmises au système de l'entreprise afin de modifier les processus. Les communications entre les serveurs et les terminaux sont plus rapides. Cette opération nécessite moins de bande passante que l'accès continu au cloud.

Révolution industrielle 4.0

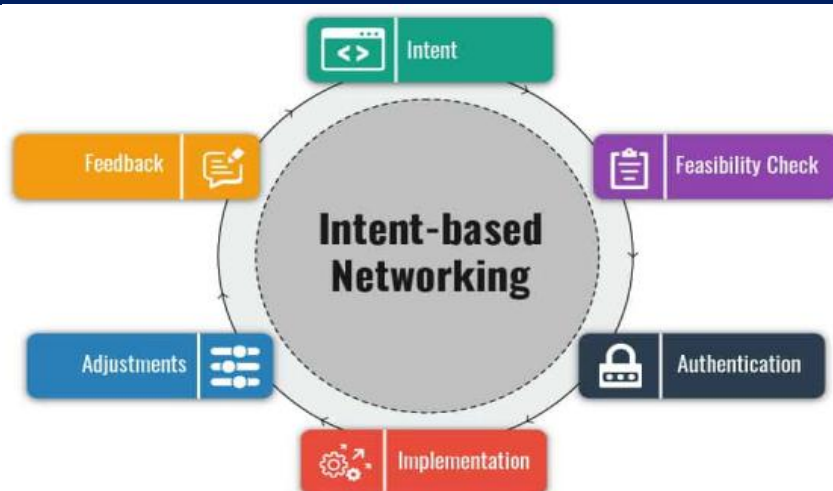
L'IoT industriel regroupe les machines, l'analyse avancées et les personnes. Il s'agit d'un réseau d'outils de fabrication et de capteurs, connectés à l'aide de technologies de communication haut débit sécurisées. Cela se traduit par des systèmes qui peuvent surveiller les processus, collecter les données, les analyser, puis les utiliser pour ajuster en continu le processus de fabrication.

Nous assistons actuellement à la quatrième révolution industrielle (révolution industrielle 4.0).

Ce terme correspond à un environnement où les machines et les équipements sont capables d'améliorer les processus grâce à l'automatisation et à l'auto optimisation.

La révolution industrielle 4.0 englobe les processus de fabrication, la chaîne d'approvisionnement et le développement de produits.

Qu'est-ce qu'un réseau basé sur l'intention (IBN) ?



Un réseau IBN, ou Intent-Based Networking, est une approche de gestion et de configuration des réseaux informatiques qui repose sur l'intention ou les objectifs définis par l'administrateur du réseau. L'IBN vise à simplifier et à automatiser la gestion des réseaux en permettant aux administrateurs de définir des politiques réseau haut niveau, tandis que les détails de mise en œuvre sont automatiquement gérés par des systèmes informatiques.

Imaginons une grande entreprise qui souhaite mettre en place un réseau IBN pour gérer son infrastructure réseau de manière plus efficace et flexible.

1. Définition des intentions

L'administrateur réseau définit les intentions commerciales et opérationnelles de l'entreprise :

- Assurer des performances élevées pour les applications métier critiques.
- Garantir un niveau élevé de sécurité pour les données sensibles.
- Optimiser l'utilisation des ressources réseau pour réduire les coûts opérationnels.

2. Automatisation et mise en œuvre

Une fois les intentions définies, l'IBN utilise des outils d'automatisation pour configurer automatiquement les appareils réseau selon les politiques définies :

- Les commutateurs et les routeurs sont configurés pour prioriser le trafic des applications métier critiques et pour appliquer des politiques de qualité de service (QoS) appropriées.
- Les règles de pare-feu sont mises en place pour contrôler l'accès aux données sensibles et pour détecter et bloquer les menaces de sécurité.
- Les ressources réseau sont optimisées pour maximiser l'utilisation et minimiser les goulots d'étranglement.

3. Surveillance et adaptation continue

Le réseau IBN surveille en permanence les performances du réseau et réagit automatiquement aux changements dans l'environnement réseau ou aux besoins commerciaux.

- Si un lien réseau devient saturé, l'IBN peut ajuster dynamiquement le routage du trafic pour éviter les congestions.
- En cas de détection d'une activité suspecte sur le réseau, l'IBN peut déclencher des actions de sécurité telles que l'isolation des segments compromis.
- Si de nouveaux services ou applications sont déployés, l'IBN peut automatiquement provisionner les ressources réseau nécessaires pour les prendre en charge (mémoire, CPU, ...).

4. Analyse et optimisation : L'IBN utilise des analyses avancées pour détecter les tendances, les anomalies et les opportunités d'optimisation dans le réseau.

- L'analyse des modèles de trafic permet d'anticiper les pics de demande et de dimensionner les ressources réseau en conséquence.
- L'analyse des journaux de sécurité aide à identifier les menaces potentielles et à renforcer les politiques de sécurité.

Les réseaux IBN tirent parti du pouvoir de l'automatisation, de l'IA et de l'apprentissage automatique (ML).

Ils permettent à l'équipe informatique de spécifier, dans un langage simple, ce qu'elle veut que le réseau accomplisse.

Ces réseaux sont en mesure de convertir les intentions en politiques, puis d'utiliser l'automatisation pour déployer les configurations appropriées requises sur tout le réseau.