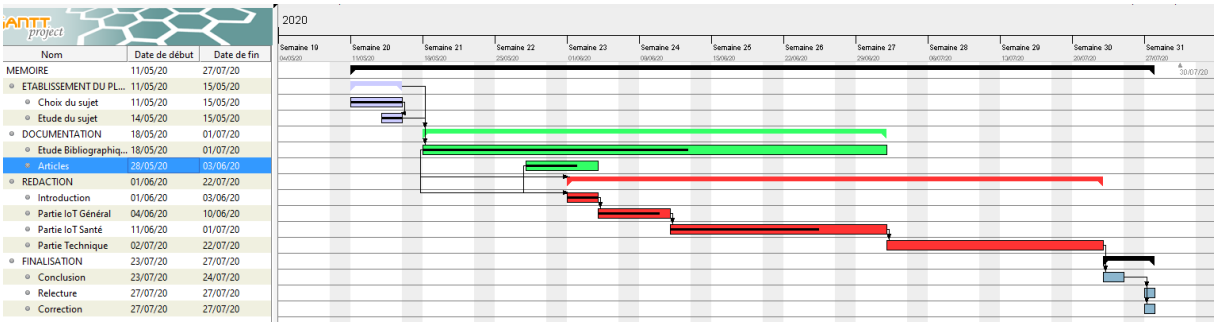
Répartition des taches :

Liste des Taches	Date de début	Durée (jours)	Progression
Choix du sujet	11/05	5	100%
Etude du sujet, Plan	14/05	2	100%
Etude Bibliographique	18/05	33	60%
Etude des Articles	28/05	5	60%
Redaction de l'introduction	01/06	3	100%
Partie IoT en Général	04/06	5	80%
Partie IoT dans la santé	11/06	15	70%
Partie Technique	02/07	15	0%
Conclusion	02/07	2	0%
Relecture	27/07	1	0%
Correction	27/07	1	0%



Etat d'avancement : Avancement des chapitres 1 et 2 (80%), mise au point sur la partie technique.

Mémoire de fin d'étude

Les objets connectés dans le domaine de la santé

Présenté par : CAM Davy

Iut de Béziers : **Licence Professionnelle MRIT Option Internet des objets**

Comment l'IoT permet-elle d'améliorer le secteur médical ?

Mémoire réalisé par CAM Davy

Dans le cadre de l'obtention du diplôme : Licence Professionnelle MRIT Option Internet des objets

Année 2019-2020

Sous la direction de Mr. Sébastien Druon

Table de matières

Avant-propos :

Ce mémoire est entrepris dans le cadre de la Licence Professionnelle MRIT Option Internet Des Objets à l'Iut de Béziers. Ce travail a pour but de présenter l'usage des objets connectés dans le domaine de la santé à travers un travail de recherche approfondis et théorique.

Introduction :

Dans notre société d'aujourd'hui, la technologie occupe une grande place dans notre quotidien afin de faciliter nos modes de vies nous pouvons citer parmi tant d'autres les Smart city (ville intelligente) qui permet d'améliorer nos déplacements, fluidifier le trafic.
De plus en plus d'objets que nous utilisons sont connectés à Internet, nous appelons l'Internet des objets (IoT) qui est apparu il y a 20 ans de cela (1999) dans un discours de Kevin ASHTON, un ingénieur britannique.
Le but de ces objets est de pouvoir transmettre, recevoir des données sur un réseau informatique. Parmi les technologies utilisant ce mode d'opération nous pouvons citer le Bluetooth ou encore les technologies sans contact.
Selon Pierre-Jean Benghozi [1] : « Certains définissent l'IdO comme des « objets ayant des identités et des personnalités virtuelles, opérant dans des espaces intelligents et utilisant des interfaces intelligentes pour se connecter et communiquer au sein de contextes d'usages variés »
Cette définition montre L'IoT comme une intelligence propre, ayant la capacité de communiquer.
De plus le marché de l'IoT est en pleine expansion, le nombre d'objets connectés dans le monde en 2020 est estimé à 50 milliards et la valeur du marché de l'IoT ne cesse d'augmenter comme le montre le graphique représentant la valeur du marché en milliards de dollars pour chaque année.

L'IoT se développe très rapidement dans de nombreux secteurs afin de faciliter les tâches des hommes dans divers secteurs, l'agriculture, l'industrie, l'automobile.
A travers ce mémoire nous allons nous intéresser au secteur de la santé, il s'agit d'un secteur très large avec beaucoup de demande donc qui possède un potentiel énorme dans le développement d'objets connectés.

Dans ce domaine il existe beaucoup de technologies permettant de faciliter les tâches du personnel soignant comme la surveillance à distance des patients, la gestion des stocks des médicaments et outils médicaux.
Les objets connectés dans le domaine médical vont permettre d'améliorer la qualité des soins dans les hôpitaux ou dans les cabinets mais aussi rendre plus accessible les soins.
Nous pouvons dire que le marché mondial de l'e-santé connait un véritable essor ces dernières années grâce aux avancés technologiques.
Le cabinet Frost & Sullivan, société de conseil aux entreprises impliqués dans les études et analyses de marchés mondialement reconnus estime à 234,5 milliards de dollars la valeur du marché mondial de la santé numérique d'ici 2023, soit une hausse de 160 % par rapport à 2019.
De plus, le nombres d'équipements connectés dédiés à la santé est estimé à 161 millions en 2020 contre 46 millions en 2015 d'après Business Insider.
Source :https://www.businessinsider.com/iot-healthcare?IR=T

Nous avons vu que les objets connectés sont en pleine expansion dans tous les domaines, ainsi que la santé mais par quel moyens permet-elle d'avoir une place dans un secteur ou souvent il peut y avoir des tâches critiques. La question que nous pouvons se poser est, comment l'usage des objets connectés permet –elle d'améliorer le secteur de la santé ?

Dans ce mémoire va être constitué de 3 parties :

- Tout d'abord nous verrons la définition de l'Internet des Objets, son utilisation dans de nombreux domaines, les différentes technologies liées à l'IoT puis nous monterons les enjeux au niveau économique, sécurité, collecte de données, juridiques.

- Nous recueillerons ensuite des informations sur l'E-Santé, L'ioT dans la santé, son usage à travers différents cas, l'utilisation de capteurs, puis nous verrons son impact économique, ses limites, et nous verrons le stockage et la collecte de données massives de données médicales, enfin nous verrons étudierons comment améliorer afin de répondre aux attentes.

- Enfin nous allons réaliser un petit projet par rapport aux faits déroulés cette année, le Covid-19, nous ferons donc une étude sur des patients atteint de cette maladie qui sont surveillés à distance grâce à des capteurs de température et de pression artérielle. Pour cela nous spécifierons les besoins et attentes, réaliser une architecture permettant la collecte, l'envoi, le stockage et la visualisation de ces données par une équipe médicale en charge de surveiller ces patients. Nous ferons ensuite des choix de capteurs, le moyen de communication possibles dans un hôpital.

Chapitre 1 : L'internet des Objets

Définition et présentation

Le terme d'objet connecté désigne la capacité d'un ''Objet'' à pouvoir communiquer et interagir ou non avec l'humain. Selon la revue The Internet of Things: A Survey [11], le terme la plus récurrente de désigner l'IoT sont des objets possédant des identités et des personnalités virtuelles opérant dans des espaces intelligents utilisant des interfaces intelligentes pour connecter et communiquer au sein de contextes sociaux, environnementaux et des utilisateurs.
Autre définition plus technique et plus centré sur l'usage de ces objets définit L'Internet Of Things comme un réseau de réseau permettant via des systèmes d'identification électronique, et des dispositifs mobiles sans fil, d'identifier directement des entités numériques et des objets physiques et ainsi pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant. [1]
Cette définition montre que les objets connectés sont des réseaux à part entières pouvant capter et communiquer avec le monde réel ou bien encore communiquer entre machines appartenant au réseau IoT, nous définissons ce terme par le concept Machine2Machine.
Autre concept lié au domaine de l'IoT, le Machine to Machine (M2M) désignant l'ensemble des solutions et Technologies permettant de communiquer entre eux de manière automatique. Le Machine To Machine permet entre autre de pouvoir automatiser les taches dans les divers services du quotidien. Entre autre ce concept est lié à l'IoT car cette méthode est utilisée dans l'IoT pour communiquer entre Objets, la différence est que le M2M exploite le réseau internet (TCP/IP) alors que l'IoT utilise les technologies Sans Fil.

Le concept d'Internet des objets a tout d'abord été un concept dans les années 1990, le but étant de pouvoir contrôler des équipements électriques à distance, mais les technologies étant peu développé ce concept n'a pas pu être envisagé.
Ce n'est qu'en 1999 que le terme d'Internet Of Things fut cité par Kevin Ashton, directeur exécutif d'Auto-IDCentre, entreprise de recherche de technologies RFID. [12]
Les objets connectés utilisent des technologies à distance comme le Bluetooth, la Wifi, et la 3g/4g pour pouvoir communiquer puis stocker les données sur le cloud.
Les éléments de L'IoT se distinguent en 3 parties pour fonctionner correctement : [14]

- Hardware (Matériel) : Capteurs, actionneurs et appareil de communication
- MiddleWare(Intergiciel) : Technologie de stockage et outil d'analyse de données (Cloud)
- Presentation : Outil ou logiciel de visualisation des données

Application de l'IoT

Avec l'émergence des objets connectés, de nombreux secteurs d'applications utilisent cette technologie qui va grandement aider dans la surveillance, l'automatisation de tâches, parmi les plus représentatifs d'évolution de cette technologie nous retrouvons les villes connectées, les voitures connectées ou encore la santé.

Les villes connectées

Plus communément appelé Smart-City utilisent de nombreux capteurs dans la gestion du trafic, du transport afin d'éviter les embouteillages, donner des informations de stationnement.
L'IoT joue également un rôle dans l'environnement et la consommation électrique, en fonction du trafic, l'éclairage nocturne peut être désactivé grâce à des capteurs de mouvement.
Elle permet de surveiller la qualité de l'air, diminuer la consommation d'eau.
Il existe aujourd'hui beaucoup de villes dans le monde ayant adopté l'IoT et cela joue un rôle important dans l'économie. [16]

Les Maisons connectés

Autre secteur émergent de l'IoT, les smart-Home évolution de la domotique, permet d'automatiser certaines actions telles que l'extinction des lumières lorsque l'on sort, la gestion du chauffage, l'allumage des caméras de surveillances lors d'intrusion.

La santé connectée

Sujet de ce mémoire, l'IoT joue également un rôle important dans le domaine de la santé grâce à l'utilisation de capteur permettant le monitoring du corps pour surveiller la température, la pression artérielle.
De nombreux objets connectés sont développés pour un usage professionnel ou encore pour les particuliers tels que des smart-watches, des bracelets ou encore du matériel pour les hôpitaux.

Les technologies de L'IoT

Le domaine de l'IoT est vaste étant donné qu'il ne s'agit pas d'une technologie spécifique mais bien diverses solutions techniques ayant pour même but de capter, stocker et traiter les données d'un environnement. [1]
Il existe à ce jour beaucoup de technologies qui s'adaptent pour chaque domaine d'application, nous allons citer les plus courantes.

RFID

Les premiers objets connectés apparus sur le marché sont la technologie de RFID (Radio Frequency Identification), il s'agit d'un système en 3 parties, une partie Tag (Transmetteur/ Répondeur) un Lecteur (Transmetteur/Receveur) qui permet l'activation des tags et transmets / reçoit les données à la partie Application. Voir Figure 2
La partie Application permet le stockage des données, la lecture et le traitement de ces données. Cette partie peut être une base de données ou une application. [13]

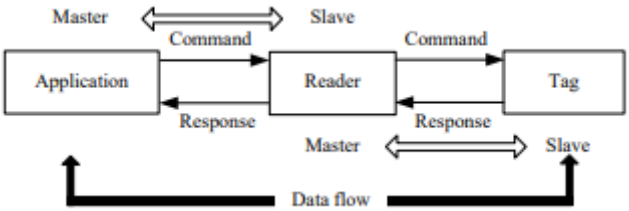


Figure 1 Composants d'un système RFID

Les Tags sont des petits objets possédant un microsystème et une antenne permettant d'identifier un objet, le lecteur sont des Lecteurs RFID permettant de lire le contenu du tag RFID en utilisant les ondes radio. [13]
Ce système s'inspire de la technologie de lecture des codes-barres.
Cette technologie aujourd'hui, très utilisé dans divers domaines grâce à sa facilité d'utilisation, sa compacité mais aussi sa faible consommation énergétique.
Il existe plusieurs types de tag RFID, les tags RFID passives ne possèdent pas de batterie et utilisent les lecteurs RFID pour lire leurs informations, cela fonctionne comme les technologies de code barre et sont très utilisés dans les industries de commerces ou encore dans les cartes de crédits utilisant la technologie de Sans contact.

Les tags RFID active sont alimentés par une source d'énergie comme une batterie ou une pile, cela permet d'émettre les données. Utilisés principalement dans le secteur de la santé, la domotique, la sécurité ou le transport. Ces tags permettent le monitoring de température, mouvement. Cela permet donc le suivi et l'identification de personnes ou objets à longue portée. [14]
Autre élément à prendre en compte dans les solutions RFID, les fréquences, il existe quatres types de fréquence : basse (125kHz), haute (13,56 MHz), ultra-haute (800-930MHz) et hyper (2,45 et 5,8 GHz). De plus, plus la fréquence est basse et plus le débit de données à tendance à augmenter. [1]

MQTT

Le MQTT (Message Queuing Telemetry Transport) est un protocole de communication Machine To Machine permettant la collecte d'information développé en 1999 par Andy Stanford-Clark et Arlen Nipper, chercheurs à IBM qui avaient pour objectif de proposer un protocole léger et efficace dans un environnement ou la latence est haute et la bande passante est faible notamment dans l'industrie du gaz et du pétrole pour monitorer les températures, pressions dans les silos et pipelines.
Aujourd'hui, le MQTT est très utilisé dans de nombreuses industries car elle facilite beaucoup d'opération tels que le suivi et la surveillance des ressources dans la Logistique et le domaine Médical. Le suivi et l'enregistrement de personnes dans les domaines du transport. La collecte d'information sur des capteurs dans les usines et la production d'énergie.

Le fonctionnement du MQTT s'appuie sur la technologie de server Push, c'est-à-dire un modèle d'abonnement Publisher / Subscriber.

Les capteurs vont avoir le rôle de Publisher vont envoyer des informations sur un topic sur le broker, un serveur chargé de réceptionner les informations puis les retransmettre.

Les Subscriber (Clients sur Pc ou smartphone) vont pouvoir s'abonner à une information précise. Voir Figure 3

Le rôle du broker est de recevoir les messages publiés par les clients, procéder aux requêtes des utilisateurs tel que les abonnement / Désabonnement, envoyer les données au clients ayant souscrit à un topic après réception.

Il s'agit de la pièce centrale du MQTT puisqu'il assure la connexion entre les capteurs et les applications, la sécurité et la qualité de service des transmissions d'informations.

Parmi les applications Brokers utilisés nous retrouvons Mosquitto, RSMB, MQTT.js [17]

Les Topics sont utilisés pour catégoriser et filtrer les messages, le client va s'abonner au topic qu'il veut.

Par exemple dans le secteur du pétrole, les informations seront catégorisées sur ces topics

Silo1/temperature

Silo2/capteur1/temperature

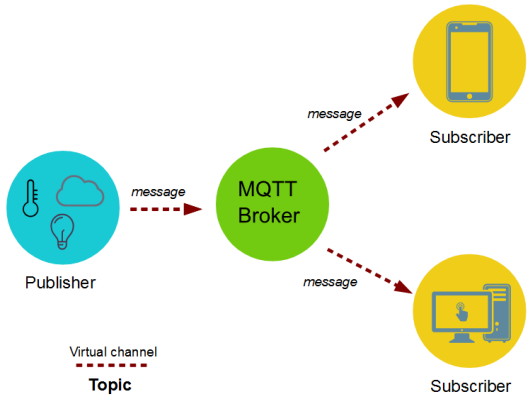


Figure 2 Fonctionnement du MQTT

Le protocole MQTT possède néanmoins plusieurs limites tels que la sécurité, le stockage des messages, la priorité des messages :

Au niveau sécurité selon le choix du broker, le niveau de sécurité peut varier ce qui peut rendre le broker plus léger. Le système de sécurité le plus utilisé est le protocole SSL/TLS mais affecte grandement les performances du broker. [17]

Stockage des messages : Il n'y a pas d'expiration de message donc tout est stocké et gardé sur le broker. S'il n'y a pas de Subscriber qui récupère le message, celui reste indéfiniment sur le broker ce qui peut nuire au performances.

Wireless Sensor Network (WSN)

Autre technologie en lien avec l'IoT mais assez différent. Les Wireless Sensor Network ou Réseau de Capteur sans fil. Il s'agit d'un large réseau de nœuds de 100-1000 capteurs placé dans un environnement communiquant à distance.
D'abord utilisé dans le domaine militaire, au fil du temps cette application est très utilisée dans de nombreux domaines tel que les Smart-City pour monitorer le trafic, dans l'environnement pour surveiller les conditions environnementales ainsi que dans l'agriculture.
L'architecture d'un WSN est constituée de nœuds permettant de capturer les données extérieures grâce au capteurs, le traitement des données et communiquer avec les autres nœuds.
Les nœuds sont constitués d'un Transceiver (Transmetteur / Receveur) pour capter et recevoir les données provenant des capteurs ou d'autres noeuds, un microcontrôleur permettant le traitement des données, une mémoire flash permettant de stocker les données collectées des différents capteurs, une source d'énergie (batterie). [15]

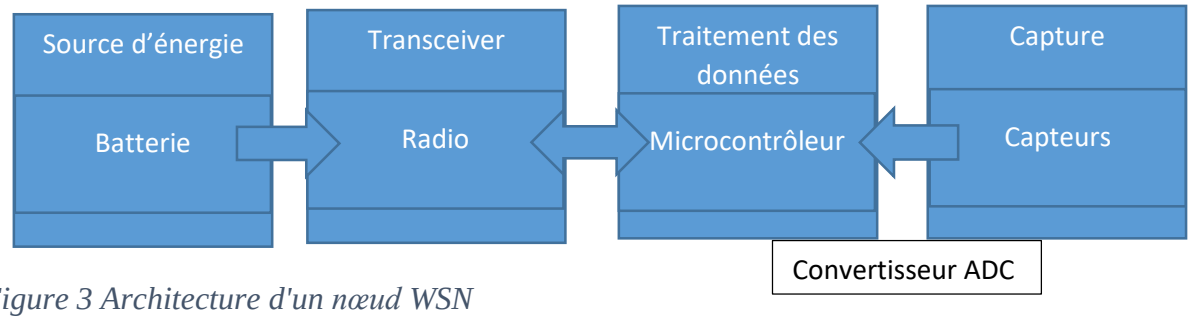


Figure 3 Architecture d'un nœud WSN

Le microcontrôleur possédant un convertisseur Analogique-Numérique, le processus de traitement des données se fait sur chaque nœud du réseau grâce à des algorithmes permettant de recueillir les données environnementales et les transformer en informations.
Il est aussi possible d'étendre la durée de vie des capteurs en rechargeant les capteurs grâce à l'utilisation de cellules photovoltaïques ou autre source d'énergie de l'environnement.

Autre caractéristique d'un WSN, la fonction de multi-hop, afin d'assurer une qualité de service élevé. En effet en fonction de la distance entre un capteur et la station il se peut que les données ne transitent pas correctement, consomment plus d'énergie et mettent plus de temps à arriver. La fonction Multi-Hop permet de communiquer entre capteurs afin de transmettre le message par petits transferts.

La partie communication se fait par liaison radio, les protocoles standards sont le Bluetooth ainsi que la technologie Zigbee IEEE 802.15.4.
Le Bluetooth à la particularité de délivrer les données à grande vitesse sur de grandes distances mais consomme beaucoup d'énergie.
Le standard 802.15.4 faisant partie des LR WPAN (Low Rate Wireless Area Network) va consommer très peu d'énergie, a une faible portée et un faible débit.

Enjeux

Le marché de l'IoT est en pleine expansion, de plus en plus de domaine d'activités ont recours à cette technologie cependant il existe encore de nombreux challenges que les développeurs doivent résoudre tel que la sécurité face à l'important flux de données transitant sur internet ou encore les défis au niveau énergétique comme la consommation et l'économie d'énergie pour ces capteurs.
Il faut également savoir que la sécurité des données et la protection des données personnelles est le défi le plus important dans la conception d'objet connecté, en effet des millions de données transitent et peuvent fournir des informations sur les habitudes, les compétences ou les relations des usagers. [18]

Economique :
Il est certain que le marché de l'Internet des Objets va croitre au fur et à mesure du temps et que cela va toucher beaucoup de secteurs.
De plus il y aura des conséquences économiques pour les entreprises développant et fabriquant les objets connectés mais également les entreprises les utilisant puisque les objets connectés sont modulables et peuvent être utilisés pour diverses utilisations.

Face à l'accroissement du nombre d'objets connectés le prix moyen des capteurs utilisés dans les objets connectés est passé de 1,30$ à 0.60$ en 2015 et le coût de la bande passante a été divisé par 40. [19]

Cela montre que les technologies de l'IoT deviennent plus accessibles mais aussi que le marché est de plus en plus exploité par diverses compagnies développant ces objets. Les principaux acteurs sont Microsoft, IBM, Google, Cisco et Intel qui participent à l'avancée de cette technologie notamment dans en recherche et développement, la concurrence étant rude dans ce marché il est difficile de se faire une place parmi les géants a moins d'être innovant.

Selon des études de Strategy Analytics, le nombre d'objets connectés est estimé à 22 milliards dans le monde, tous secteurs confondus, le secteur professionnel est pour l'instant le domaine ou les objets connectés sont les plus utilisés mais les maisons connectées ou encore le secteur de l'automobile sont en pleine expansion.

En 2030, le nombre d'objets connectées s'élèverait à plus de 50 milliards.

https://www.mac4ever.com/actu/143604_il-y-aurait-22-milliards-d-objets-connectes-dans-le-monde-strategy-analytics

Quant au marché de l'IoT, selon IoT Analytics celui-ci s'élèverais à 151 milliards de dollars en 2018 et s'élèverais à 1567 milliards de dollars en 2025.

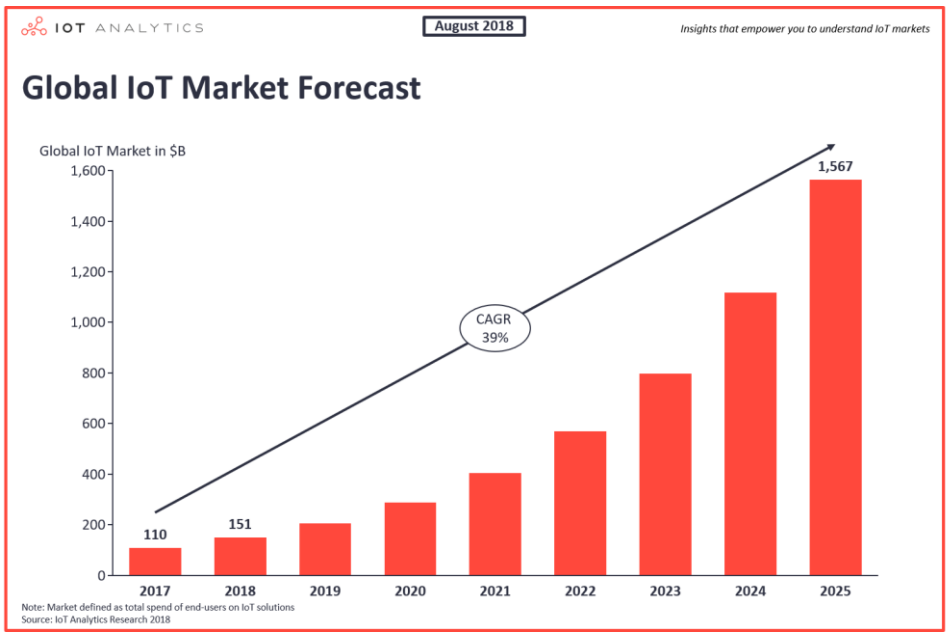


Figure 4 Estimation du marché mondial de l'IoT jusqu'en 2025

Ce marché de l'IoT ne cesse de se développer grâce à l'expansion des objets connectés dans de nombreux secteurs grâce aux innovations. Tous les secteurs finiront par adopter l'internet des objets.

De plus certains experts estiment que le marché de l'IoT pourrait créer de nouveaux emplois et donc créer une montée économique pour l'emploi dans tous les secteurs notamment pour l'entretien des objets, la surveillance ou encore dans le développement de ces derniers.
Cependant face à impact significatif sur de nombreux secteurs avec le temps le nombre d'employés seront ramenés à être réduit de moitié qui vont laisser place à ces technologies. Cela permettra cependant de réduire les charges d'une entreprise investissant dans cette technologie d'objets connectés.
Dans le secteur de l'industrie, l'automatisation des taches permettront de remplacer les hommes sur les chaînes de production, dans les processus de suivi et de gestion des flux. Elle offre également une meilleure qualité de service sur la gestion en temps réel des stocks et sorties. [1]
Aujourd'hui encore la demande des objets connectés ne fait qu'augmenter avec la généralisation de ces derniers. L'utilisation massive de puce RFID pour le scan de cartes dans les transports en communs (Tam, Oyster, Navigo) ou encore le suivi de personnes, objets dans le secteur de la santé dont nous y reviendrons plus tard.

Sécurité des données et vie privée :

La sécurité des données transitant dans le réseau IoT est le point le plus important dans le développement de la technologie IoT, tout comme Internet il existe des failles exploitables dans ce réseau. Cela peut servir à réaliser des cyberattaques pour reprogrammer les capteurs ou s'en servir à des fonctions malveillantes, cela peut donc poser problèmes sur la question de confidentialité, l'intégrité et la vie privée des données transitant dans le réseau.
Selon une étude réalisée par Kasperky : les attaques contre les équipements IoT en 2019 ont atteint 105 millions d'attaques provenant de 276 000 adresses Ip différentes contre seulement 12 millions issues de 69 000 adresses Ip différentes. Nous constatons l'importance de la sécurité de l'IoT et face au la croissance d'utilisation d'objets connectés dans le monde, les développeurs doivent redoubler d'effort afin d'apporter des solutions pour limiter les attaques. L'architecture toute entière de l'IoT doit être sécurisé que ce soit au niveau des capteurs, du transfert des données ou encore au niveau du serveur Cloud.
Mais la propriété des objets connectés est que ces objets doivent être à bas prix, peu consommateur en énergie et pouvant être déployé en milliards. Cependant face à ces
https://www.informatiquenews.fr/les-objets-connectes-se-multiplient-les-attaques-encore-plus-64005

contraintes les fabricants d'objets connectés doivent pouvoir proposer une sécurité fiable tout en répondant à ces critères.

Afin d'assurer une sécurité sur le réseau IoT plusieurs paramètres et mécanismes doivent rentrer en comptes :

- Toute données transitant dans le réseau constitue un risque de vulnérabilité sur l'intégrité et la confidentialité, un mécanisme de chiffrement est donc nécessaire pour les données situés dans les appareils du réseau afin que celles-ci soient totalement confidentielles en cas d'attaque et ne puissent pas être modifiés. Des systèmes de clé secrète accessible seulement par le destinataire comme par exemple de type AES256 ou Ciphers. Nous reviendrons plus tard sur ces méthodes de chiffrement de données dans un contexte précis.

- L'authentification est requise entre deux parties afin de pouvoir sécuriser la communication. Les appareils du réseau doivent pouvoir être authentifiés. Les utilisateurs désirant accéder aux données doivent également s'authentifier et ne doivent seulement pouvoir accéder aux données les concernant. De plus la communication doit rester sécurisé avec un système de certificat. [22]

Les données portant sur la vie privée des utilisateurs sont également un point important, en effet des données à caractère personnel, confidentiel et critiques transitent sur le réseau. Tout comme internet, des utilisateurs craignent la divulgation de leurs données personnelles pour des fins malveillantes ou commerciales. En effet les données collectées doivent rester personnelles et ne doivent pas être vu par les compagnies exploitant le réseau IoT.
Par exemple les données collectées sur une voiture connectée communiquent l'emplacement et les destinations de l'utilisateur ou encore les habitudes de conduite.
De plus afin de garder la confiance des utilisateurs, la compagnie doit tenir un engagement de confidentialité mais aussi appliquer la loi RGPD (Règlement général pour la protection des données) qui stipule que l'entreprise doit effacer les données de l'utilisateur si celui-ci le demande mais aussi d'assurer une protection des données et garder les données vraiment nécessaires.

Normalisation :

Le principe de l'IoT est un vaste réseau d'objets, protocoles qui n'est pas limité à une solution mais par un choix vaste mais l'interopérabilité des technologies sont soumis à des choix des fabricants. Un objet connecté doit être capable de pouvoir communiquer avec n'importe quel autre appareil connecté ou un système. Les développeurs d'objets connectés doivent donc rendre leurs équipements interopérables afin que les utilisateurs aient le choix d'utiliser les solutions qu'ils veulent. [23]
Dans l'exemple d'un grand réseau dans un bâtiment ou d'une smart-city, l'interopérabilité des différentes sources doivent être permise afin de pouvoir communiquer entre eux et utiliser n'importe quelle application pour pouvoir accéder aux données.
Cependant il y a également un enjeu économique puisque les développeurs veulent que les utilisateurs utilisent seulement les logiciels propriétaires ce qui cause des problèmes.
Néanmoins en l'absence de normes et de réglementation contraignante, les constructeurs ne se préoccupent pas tellement de cette interopérabilité.

Energétique :

La consommation électrique d'un objet connecté est un aspect primordial dans sa fabrication, avec plus de 20 milliards d'objets connectés dans le monde et face à la durée de vie limitée des batteries il s'agit là d'une des principales limites de cette technologie. Le but étant de fournir la même qualité de service tout en utilisant une énergie suffisante pour réaliser les échanges de données.
Pour répondre à cette problématique, il existe des méthodes pour améliorer la durée de vie des batteries comme l'utilisation de protocoles de communications légers (IEEE 802.15.4), l'utilisation d'émetteur-récepteur à faible puissance ou encore l'utilisation de la technologie de récupération d'énergie issu de l'environnement (Energy Harvesting). [20]
Nous allons expliquer dans cette partie comment fonctionne ces technologies et comment leurs utilisations permettent de prolonger la durée de vie des batteries des objets connectés.

Protocoles de communications à faible puissance :

Parmi les protocoles de communication à faible puissances nous retrouvons le protocole IEEE 802.15.4 du fait de leur faible consommation et de leur faible portée ou encore le LPWAN pour des communications à longue portée à faible débit.
Plusieurs normes tels que la norme 6LOWPAN ou encore ZigBee exploitent le standard 802.15.4 afin d'implémenter leur propre technologie ou améliorer certains aspects du standard.

6LoWPAN : Standard développé par l'IETF crée en 2004 pour concevoir une couche d'adaptation de l'IPV6 sur l'IEEE 802.15.4 fonctionnant par radiofréquence.
Ce protocole permet l'utilisation de l'IPV6 et de compresser l'entête, l'IPV6 utilise 40 octets d'entêtes ce qui est énorme dans l'espace d'adresse 802.15.4 qui est de 127 octets.
L'utilisation de la compression d'entête permet la transmission des paquets IPV6 sur seulement 4 octets.
La fragmentation et la reconstitution de trame permet de limiter le temps de transmission et donc le coût énergétique. [21]
L'architecture réseau du 6LoWPAN contient 3 éléments : l'hôte, le routeur 6LoWPAN et le routeur EDGE. L'hôte permet de capter l'environnement grâce aux capteurs et actionner des dispositifs. Le routeur va récupérer et envoyer les paquets de l'hôte au routeur Edge ou une autre destination dans le réseau. Le routeur EDGE quant à lui va assurer la communication entre le réseau et Internet.

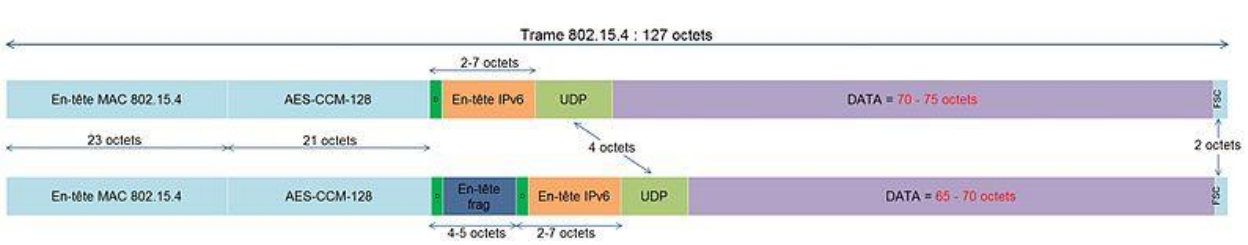


Figure 5 Paquet réseau du 6LoWPAN

Une étude plus approfondie du standard 6LoWPAN se trouve dans le document : [21]

LPWAN : le standard Low-Power Area Network a été conçu pour être utilisé sur de longues distances avec une faible consommation énergétique mais avec un débit de transfert faible.
Des propriétaires tels que Sigfox, LoRaWAN exploitent ce standard afin de changer la portée, le débit ou encore rajouter des fonctions propriétaires tels que la sécurité.

Les propriétés du LPWAN sont caractérisés par un faible prix, une capacité de traitement très limité, une petite taille de mémoire et une consommation d'énergie très faible.
D'un point de vue réseau, le standard utilise un taille d'entête petite et un débit faible.
L'architecture des technologies LoRaWAN et SigFox contient 4 éléments : l'hôte qui va capter les informations, les données seront ensuite transférées à la station de base radio par la Radio-Fréquence (LoRa RF ou SigFox LTN radio), les données seront ensuite transférées au serveur Cloud par connexion cellulaire (4G, Wifi ou Satellite) puis sont ensuite remis aux utilisateurs finaux.
Contrairement au 6LoWPAN les hôtes ne peuvent pas communiquer aux autres hôtes mais seulement à la station ce qui rend cette technologie plus économe en énergie.

Protocole	LPWAN	6LoWPAN	Zigbee	Bluetooth
IEEE		802.15.4	802.15.4	802.15.1
Besoins mémoire		4-22 Kb	4-32 Kb	250 Kb+
Autonomie	Années	Années	Années	Jours
Nombre de noeuds		2^{64}	65 000 +	32
Vitesse de transfert			250 Kb/s	1 Mb/s
Portée	10-50 km	10-100m	10-100m	10-100m

Environnemental : L'utilisation de batteries dans les objets connectés participent à la pollution de l'environnement

Conclusion :

Chapitre 2 : L'IoT dans la santé

Qu'est-ce que L'e-Santé ?

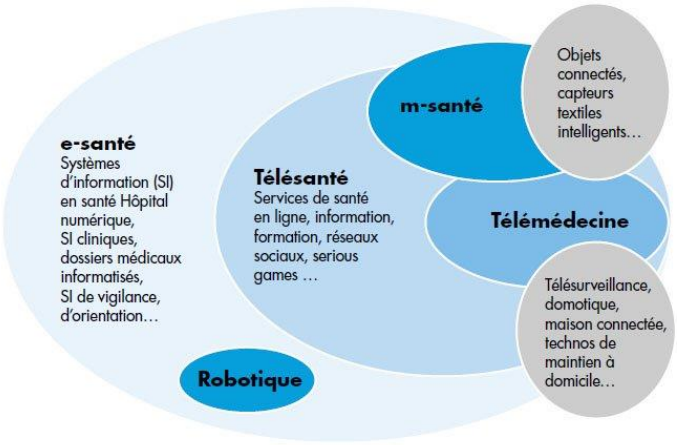
Définition :

L'E-Santé ou Santé Electronique est un terme recouvrant les domaines de la santé et les technologies de l'information et de la communication (TIC).

Parmi les services de l'E-Santé, nous retrouvons :

Les systèmes d'information en santé permettant une meilleure coordination des soins au sein d'un établissement de santé

- **La télémédecine** offrant des possibilités de soins à distance et regroupant 5 catégories d'actes médicaux : la téléconsultation, la télé expertise, la télésurveillance, la téléassistance, et la régulation médicale.
- **La télésanté** intégrant des services de suivi et de prévention des individus dans un objectif principal de bien être (objets connectés, applications mobiles d'auto-mesure, plateforme web, …) En fonction des utilisateurs, il est possible de distinguer au sein de ces champs d'application trois types de dispositifs technologiques génériques
- **Les dispositifs technologiques centrés patient ou grand public** : Soin Mobile (m-health) ou santé Mobile (m-santé) applications de santé mobiles, applications de santé web, objets connectés, réseaux sociaux (communautés de patients)



Avoir recours à l'e-santé permet en outre d'avoir accès aux soins à distance, avoir des informations sur son corps en temps réel et donc pallier quelques problèmes.

Il y a un véritable enjeu économique dans ce domaine car cela permet de réduire les déplacements, réduire les couts et avoir une meilleure accessibilité des soins.

D'après une enquête réalisée par le laboratoire Pfizer et le Cercle P auprès de près de 300 associations de patients sur la question : L'E-Santé vue par les patients : risque ou opportunité ? 77% estiment que l'e-santé est une solution efficace pour lutter contre les déserts.

57% estiment que le recours à la téléconsultation pourrait permettre un meilleur accès aux soins et pallier le manque de médecins dans certaines spécialités.

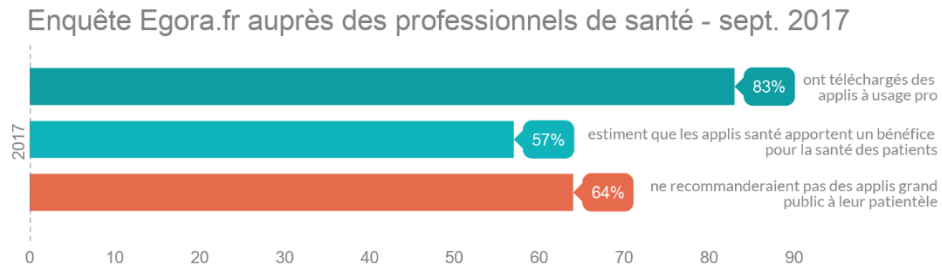
Source : https://buzz-esante.fr/le-sante-vue-par-les-patients/

Ce système permettra de réduire les coûts, d'améliorer la qualité des soins et rendre l'assurance et les soins médicaux abordables pour tous les citoyens [2].

De plus grâce aux réseaux sociaux, portails et forum, tout le monde à accès à des conseils sur quel type de soins apporter.

La santé mobile (m-santé) correspond à l'utilisation de téléphone, tablette, outil sans fil chez le patient ou les professionnels de la santé.

Leurs usages sont assez diversifiés, ils permettent en outre la prise de rendez-vous médicaux, le suivi et conseils aux patients afin de prévenir de certaines pathologies, l'aide au diagnostic, dictionnaire de médicaments.



Les objets connectés sont liés au domaine de l'e-santé puisque nous trouvons dans cette partie des capteurs, objets médical permettant l'envoi de données.

Nous allons voir dans la partie suivante L'IoT dans ce domaine, son utilisation :

L'IoT médical :

Définition :

L'IoMT : Internet of Medical Things ou Internet des objet Médicaux est l'ensemble des dispositifs et applications d'usage médicaux qui se connectent aux Systèmes Informatiques de santé par le biais de réseaux informatiques en ligne.

Les 3 principaux problèmes médicaux ou l'IoT peut avoir un gros impact est l'âge de la population, en effet beaucoup de personnes malade sont âgés et ne peuvent pas se rendre dans les hôpitaux, elle permet également de résoudre les maladies chroniques (Asthme, Diabète et l'obésité) grâce à des préventions mais également faciliter les soins dans les hôpitaux avec une meilleure prise en charge des patients.

En 2020 le marché global de L'IoT medical est estimé à 148 milliard d'euro, de plus 87% de d'organisations dans ce domaine ont déjà adoptés les solutions IoT.

D'après une enquête réalisée par ArubaNetwork, les organisations utilisent l'IoT pour : le monitoring de patient (64%), les machines à Rayon X et d'imagerie.

https://www.arubanetworks.com/assets/infographic/Aruba_IoT_Healthcare_Infographic.pdf
L'IoT dans la santé sont des systèmes communiquant entre des réseaux d'objets connectés, applications et appareils permettant d'aider les patients et docteurs à surveiller et récolter les données médicales des patients. [6]
Parmi les objets connectés dans le domaine médical nous pouvons citer les capteurs de tensions, température, des outils médicaux ou encore des réseaux connectés entre le patient et le docteur qui le prends en charge pour l'envoi d'informations médicaux pour l'analyse ou encore monitorer en temps réel les personnes en situation critique (problème cardiaque) afin d'intervenir rapidement.
Les objets connectés collectent les informations et vont les transmettent via une connexion internet, les données sont stockées puis peuvent ensuite être visualisé grâce à des applications (ex : application mobile ou app comme Grafana)
Ces données reposent sur le principe du big-data.
Le big data désigne l'ensemble des données numériques produites par l'utilisation des nouvelles technologies à des fins personnelles ou professionnelles. Il s'agit d'un ensemble de données massif sécurisé.

Dans le domaine de la santé, le big data est donc l'ensemble des données personnelles relatives à la santé, les professionnels de la santé ont accès aux données du patient, ses dossiers afin de garantir un suivi et une meilleure approche des soins pouvant être réalisés.

Architecture de L'IoT dans la santé :

La mise en place d'une bonne architecture est importante dans la santé, en effet il y a plus facteurs à prendre en compte tel que la consommation énergétique du capteur, la vitesse de transfert et la précision des données. Les données santés étant importants il ne faut pas d'erreur dans le traitement, calculs et transfert. De plus étant donné que les capteurs utilisés dans le domaine médical sont des capteurs corporels pouvant être implantés, ces capteurs sont relativement économes en énergie donc ne peuvent pas réaliser de calculs, les données générées ne pouvant pas être stockés sur les capteurs il faut passer par un réseau permettant le traitement et le stockage.
Dans les hôpitaux la plupart des systèmes de monitoring se reposent sur un système qui se compose d'un appareil WBAN (Wireless Body Area Network) qui va capturer les données du capteur et les envoyer par radiofréquence (Wifi ou IEEE.802.15.4) et les envoyer directement sur un serveur Cloud qui va s'occuper du stockage et calcul des données. Il s'agit d'un système simple et facile à mettre en place et peu onéreux cependant il y a plusieurs inconvénients tel que le pourcentage d'erreur lors des transmissions de données, la latence car tout repose sur le serveur s'occupant du traitement et stockage.

La solution proposée [9] est de mettre en place d'une technologie de Fog Computing qui consiste à mettre en place un appareil servant de passerelle entre le capteur et le serveur Cloud et peut également être utilisé dans les hôpitaux ou pour un usage à distance.
Le Gateway va aider à réduire la latence du réseau IoT en traitant directement les données sur celui-ci avant de les envoyer sur le serveur mais aussi un taux d'erreur relativement nul.
Le Fog Computing est un principe d'exploitation d'infrastructure qui fournit un support de calcul, de stockage et de réseau entre les capteurs et le cloud qui va permettre de réduire la charge de travail du Cloud.
L'étude montrée [24] montre que l'utilisation de cette solution permet de réduire drastiquement la latence lors de la transmission de données avec une moyenne de 5ms en combinant le cloud avec le fog. De plus face à l'importante échange de données dans le réseau avec la surveillance de multiples patients, cette solution reste la plus optimale.

La figure 5 et 6 montrent une vue détaillée de l'architecture IoT utilisé dans les hôpitaux ou à la maison pour surveiller les patients avec des capteurs corporels. L'architecture repose sur un système sur 3 niveaux :

- La partie Edge qui représente les capteurs médicaux et les outils permettant l'envoi de données. Les capteurs vont capter, récupérer des données puis les envoyer au Gateway par liaison sans-fil ou filaire grâce à des protocoles tels que le Bluetooth, Wifi, Zigbee ou 6LoWPAN. Une étude de ces technologies a été présenté dans le précèdent chapitre.
- Le réseau de Gateway formant le Fog permettant le support de différents protocoles de communications et permet la conversion de protocole. Il permet également l'agrégation de données et la réduction des paquets.
- La partie Back-End est la partie Cloud Computing permettant le stockage des données, la visualisation des données par les médecins grâce à des application Web. [25]

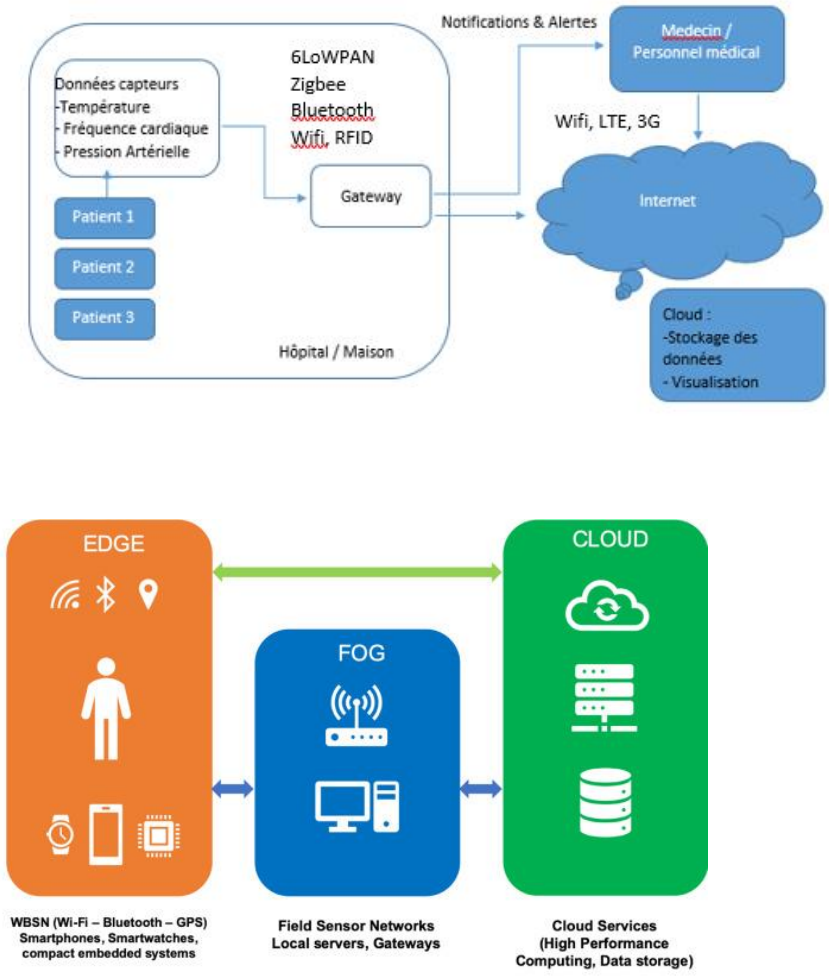


Figure 6 Architecture sur 3 niveaux pour les systèmes IoMT.

Comme mentionné précédemment le Gateway est un pont entre les capteurs et le Cloud qui permet de stocker temporairement les données brutes afin de pouvoir les traiter puis pouvoir appliquer l'agrégation, le filtrage et la fusion.

Nous allons voir dans cette partie le fonctionnement de traitement de données.

- Filtrage des données : Les données n'étant pas traités par les capteurs, ils sont envoyés sur le gateway par différent procoles de communications. Le gateway permet de filtrer ces données digitalisées et récupérer seulement les données importantes étant donné que lors de la capture des données par le capteur, du bruit peut être crée par des interférences d'autres appareils et donc fausser les réelles informations.
- La compression des données est utilisée pour réduire la latence et réduire la consommation d'énergie lors des échanges. Avec un flux important d'échange de données cette fonctionnalité permet en autre de réduire la charge sur le réseau grâce à un algorithme de compression
- La fusion des données permet de réduire drastiquement le volume de données et ainsi réduire la consommation d'énergie nécessaire lors des transmissions de données. La fusion des données est catégorisé par 3 différents types de capteurs : Complementary, Competitive et Cooperative. [26]

  La fusion de données complementary permet d'obtenir une donnée plus détaillée par exemple récupérer la différence de température entre le corps d'un patient et l'environnement extérieur avec la récupération des données de 2 capteurs différents.
  La fusion de données Competitive est utilisé lorsque plusieurs données similaires sont capturées par différents capteurs afin de récupérer une information plus complète. Elle permet également en cas de défaillance d'un capteur, de pouvoir appliquer une redondance et ainsi récupérer l'information ce qui est indispensable dans le domaine médical.
  Enfin la fusion de données Cooperative permet de récupérer des informations de diverses sources ne pouvant pas être récupérés par seul capteur. Dans le domaine médical cette fusion de données permet de récupérer des informations plus complètes sur le patient.
- Le système applique également une analyse des données sur le Gateway qui permet de pouvoir prédire des situations d'urgences comme par exemple lors d'insuffisance respiratoire d'un patient. Le système va donc réagir rapidement face à la situation et pouvoir donner l'alerte en temps réel. De plus en cas de perte de connexion internet qui peut arriver fréquemment, le traitement reste toujours opérationnel et les données sont conservés sur le Gateway local puis sont ensuite synchronisés avec le Cloud une fois la connexion rétablie.

Face au nombre d'objets connectés qui nous entoure, le nombre d'adresses IPV4 disponibles sont très limités, le total d'adresse IPv4 est à peu près à 4.3 milliards mais s'épuise d'années en années à cause de la croissance d'internet. [10]
La transition vers un adressage IPV6 est plus adaptée pour les objets connectés, nous parlons d'une quantité colossale d'adresse IPv6 disponibles (2^{96} plus d'adresse que l'IPv4) [8]

Usage chez les patients :

Pour le suivi à distance des patients les dispositifs médicaux portables connectés possédant des capteurs corporels permettant de surveiller des points vitaux, nous pouvons citer des capteurs de pression sanguine, glucomètre, accéléromètre, fréquence cardiaque.
Parmi les objets connectés les plus utilisés nous pouvons citer les objets pouvant être portés tels que des montres connectés (SmartWatches) ou encore des bracelets connectés.
Cela donne au patient des alertes en temps réel sur ce qu'il manque ou pour prévenir mais aussi de pouvoir envoyer ces données au médecin en charge de suivre le patient.
Le terme utilisé pour le monitoring est **Remote Patient Monitoring (RPM)**, lorsque celles-ci sont prescris par un médecin ces objets connectés sont principalement utilisés pour les maladies cardiaques, les problèmes respiratoires et les cancers.
Dans l'autre cas il s'agit de suivre des problèmes liés au diabète, l'obésité ou encore des problèmes mentaux.
Le patient va utiliser l'objet connecté qui va ensuite mesurer les données, les envoyer dans un serveur, le médecin va ensuite pouvoir analyser les données du patient depuis une application.
Voir Figure 4

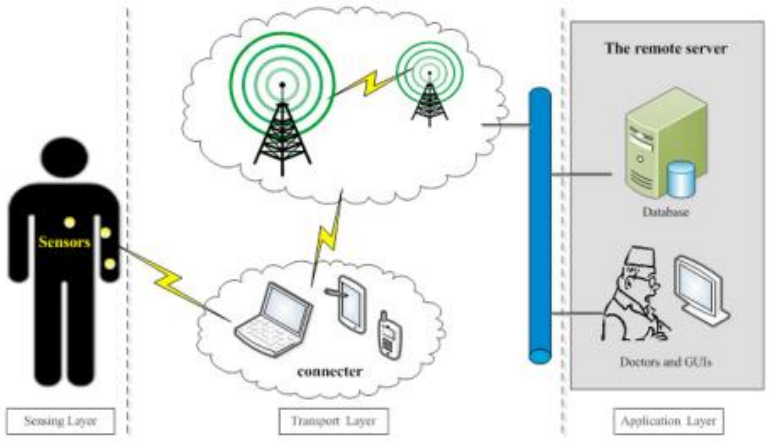


Figure 7 Suivi à distance d'un patient à l'aide d'objets connectés

L'avantage de ces objets est la facilité d'utilisation, la plupart des patients sont des personnes âgées n'ayant pas connaissances des nouvelles technologies.
On estime que la population mondiale ayant plus de 65 ans en 2018 représente 8% de la population soit une augmentation par rapport aux années précédentes.
Source :https://donnees.banquemondiale.org/indicateur/SP.POP.65UP.TO.ZS?end=2018&start=2010

Application de L'IoT

La plupart des services de soins ne se pratiquent seulement que dans les hôpitaux et centre de soins, rendant difficile l'accès aux personnes âgés et handicapés.
La généralisation des objets connectés a pour but de délivrer un service que l'on retrouve dans les hôpitaux pour tout le monde, n'importe où et n'importe quand. [7]
Les différents objets connectés liés à la santé ont pour objectif : la surveillance en temps réel, la prévention, les alertes pour les interventions en urgences et le soin à distance.

Détecteur du niveau de Glucose : Le taux de diabétiques est estimé à 422 millions en 2017, il s'agit d'une maladie qui atteint essentiellement les personnes âgées et il n'y a pas de traitement contre cette maladie, autrement dit pas de remède.
L'utilisation d'un capteur de niveau de glucose va permettre aux personnes diabétiques de pouvoir mesurer le taux de glucose dans le sang et pouvoir ensuite indiquer quand administrer de l'insuline [5]. Cette technologie permet d'aider dans la planification de plats, des activités sportives et la régulation d'insuline dans le sang [4].
Le capteur doit être placé sur une partie du corps, relié à un ordinateur ou un smartphone qui fonctionnera en mode Fog, les données seront traitées, visualisés puis envoyés sur le cloud.

Surveillance de la pression artérielle : La mesure de la pression artérielle est une pratique constante à chaque consultation médicale, elle permet de connaitre la pression du sang dans les artères. Si le patient possède une tension anormale ou une hypertension, le risque de maladie cardiovasculaire augmente. [4]
A ce jour il existe de multitudes d'objets connectés permettant une surveillance continue ou non continue selon la gravité de la maladie du patient, l'objet va d'abord recueillir les informations et va ensuite les envoyer à une passerelle qui peut être une application

smartphone, les données sont ensuite traitées, visualisés et envoyés sur un serveur ainsi qu'au médecin. [7]

Usage dans les hôpitaux :

Dans les hôpitaux ou cabinets medical, l'IoT participe à une nette amélioration sur le fonctionnement quotidien des services de soin mais aussi dans la sécurité et contrôle des établissements. On appelle cela un hôpital intelligent. Les hôpitaux basés sur les technologies IoT permettent un meilleur diagnostic, un traitement, une prise de décision et un management des patients plus avancé. Grâce à cela les informations de chèques patients entrant dans l'hôpital peuvent être consultés rapidement par les médecins et peut ensuite prescrire les traitements les plus adaptés.
Pour chaque patient, des technologies tels de monitoring des patients sont appliqués, avec l'utilisation de WBAN (Wireless Body Area Network) tels que des capteurs de fréquence cardiaque, de température.
De plus des capteurs de température ou d'humidité sont installés dans chaque chambres afin de vérifier la situation.

Utilisation des capteurs

Monitoring de fréquence cardiaque : Afin de surveiller l'état de santé du patient, l'usage d'un capteur de fréquence cardiaque est indispensable. Dans les hôpitaux les patients sont surveillés constamment

Monitoring de la température corporelle : Le contrôle de température corporelle est un point important dans les services de soins qui permettent d'évaluer le patient.
Le contrôle de la température se fait grâce à des capteurs de températures utilisant l'infrarouge pour pouvoir mesurer le corps.

Usage du RFID :

Les RFID (Radio Frequency Identification) est une technologie qui utilise les ondes radios pour la collecte et le transfert de données, il peut capturer les données de manière efficace et automatiquement sans intervention humaine.

Dans le domaine médical, les tag RFID sont indispensables pour le repérage et l'automatisation de processus complexes.

Le RFID est utilisé dans :

- La localisation de biens ou de patients par détection est l'usage le plus courant dans les hôpitaux, les tags RFID Active sont utilisés pour retrouver des pompes à insuline, des lits, des chaises roulantes ou encore la localisation des patients, les informations sur celui-ci (Date de naissance, nom, maladie, date d'admission) grâce à des bracelets. Il s'agit là d'un gain de temps puisque les objets perdus sont retrouvés, de coûts mais aussi d'une charge moins élevé pour le personnel hospitalier. Le RFID est également utilisé pour retrouver le personnel soignant dans des grands hôpitaux.
- La gestion des médicaments, pour gérer les stocks et les processus d'approvisionnement : grâce à l'intégration de d'étiquettes RFID sur chaque médicaments, fournitures et dispositifs médicaux ainsi qu'un lecteur RFID pour chaque entrée, sortie de stock. Le personnel médical peut voir en temps réel les stocks de chaque fourniture et peut donc savoir lorsqu'un d'approvisionnement est nécessaire et éviter une rupture de stock, un superflu et des produits périmés.
  L'usage de tags RFID sur chaque médicament permet également l'identification et la vérification afin de prévenir sur les erreurs médicales.
- La gestion de chaque processus de soins, en implantant sur des bracelets des solutions RFID pour chaque patient, nous pouvons suivre l'avancement de son processus de soins de son admission jusqu'à la mise en place du traitement.

L'utilisation de la technologie RFID n'offre pas seulement la capacité de suivi pour localiser les équipements et les personnes en temps réel, mais offre aussi un accès efficace et précis pour les docteurs et les professionnels. De plus elle n'offre pas seulement un gain de cout et améliorer la localisation des objets et patients, elle offre également la réduction d'erreur médicales, améliorer la sécurité du patient et sauver des vies. [3]
Cependant la technologie présente des limites notamment dans un usage médical, étant connecté sans fil dans les hôpitaux il peut y avoir des interférences avec d'autres objets médicaux la plupart pouvant être des problèmes d'interférence importants pouvant générer des erreurs sur d'autres capteurs.

Le cout des capteurs, logiciels, bases de données et gateway présentent un coût important pour les maintenances et la mise à niveau.

Scenario : Dans un contexte d'une entrée dans un hôpital, nous allons décrire le processus d'enregistrement du patient, de la lecture du dossier par le personnel puis la mise en place d'objet connecté pour monitoring.

Stockage de données :

Le stockage des données concernant les informations sur les patients sont centralisés dans le Cloud afin que les équipes médicales puissent y avoir accès pour voir les antécédents, le type de maladie, sa localisation et sa date d'admission à travers des applications web IoT afin de pouvoir fournir un service médical adapté. Les patients peuvent également avoir accès à leurs données. But étant de pouvoir avoir l'accès à ces informations dans différents lieux comme les hôpitaux, les ambulances, cliniques mais également à l'extérieur.
Egalement le monitoring permanent des patients génère un flux important de données qui va s'accumuler dans le cloud pour un stockage sur le long terme. [27]
Le stockage massif de données médicaux sur le cloud est un véritable challenge tant bien dans l'IoT en général que dans le domaine médical, en effet le système doit être sécurisé contre des attaques et intrusions dans le cloud mais il y a également des problèmes de confidentialité car certaines personnes ont accès aux données et peuvent divulguer des informations.
Nous allons voir dans cette partie les différents type d'attaques possibles dans le domaine médical, les différents challenges liés à l'échange et le stockage de ces données mais également l'avenir des objets médicaux dans les années à venir.

Sécurité des données :

La sécurité des données est le point le plus important dans le domaine médical puisque des données sur le patient sont stockés et ne doivent pas être divulgués ou modifiés à des fins désastreuses.
Selon une étude de l'association américaine Himms (Healtcare Information and Management Systems Society) près de 76% des établissements de santé ont subi une cyberattaque au cours de l'année 2019 notamment par des fuites de données, des vols d'informations d'authentification et des attaques internes. [29]

Le domaine de la santé est donc une des cibles des hackers à cause un flux d'information personnel important.

L'utilisation d'objet connectés lié à la télésanté présente également un risque d'attaque, en effet l'objectif de la télésanté est de suivre un patient à distance et d'appliquer des soins grâce à des objets connectés connecté au réseau de l'hôpital (Architecture à 3 niveaux). En échangeant les informations en temps réel le médecin en charge du patient, le médecin peut modifier les prescriptions et dosages opérées par l'objet connecté. Cependant un attaquant ayant accès au réseau pourrait prendre le contrôle de l'équipement et modifier les données. [28]

La figure 8 présente les potentiels attaques possibles sur un objet connecté médical pouvant être opéré dans le cadre d'une télésanté ou à l'hôpital.

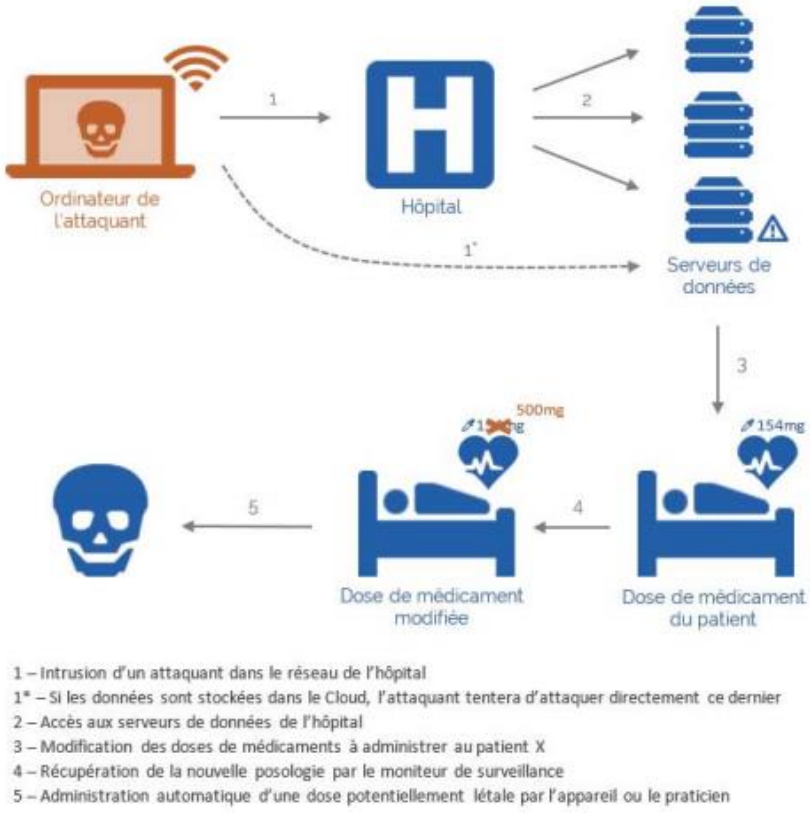


Figure 8Attaque contre un équipement connecté médical

Les attaques contre les équipements médicaux connectés peuvent se faire dans le Gateway, les données étant traités puis stockés temporairement, l'attaquant peut accéder à ces informations après le traitement ou pendant la transmission des données grâce à une analyse du trafic entre le Gateway et le cloud. Des technologies de cryptages des données tels que l'AES peuvent être employés pour garder une sécurité dans ces situations. [30]

Le cryptage de données est un processus d'encodage de message, les données sont donc illisibles et ne sont lisibles seulement par le destinataire qui possède la clé secrète pour pouvoir décrypter le message. Le cryptage utilisé dans les objets connectés est un cryptage permet d'assurer une confidentialité des données mais également une sécurité, l'origine du message est vérifiée, la vérification de l'intégrité du message si le message a été modifié depuis son envoi.

Cloud :

Données personnelles :

L'avenir de l'IoT médical

Conclusion

Chapitre 3 :

Bibliographie

[1] Pierre-Jean Benghozi, Sylvain Bureau, Françoise Massit-Folea. L'Internet des objets. Quels enjeux pour les Européens ?. 2008. ffhal-00405070f
[2] Koop, C & Mosher, Robyn & Kun, Luis & Geiling, Jim & Grigg, Eliot & Long, Sarah & Macedonia, Christian & Merrell, Ronald & Satava, Richard & Rosen, Joseph. (2009). Future delivery of health care: Cybercare. IEEE engineering in medicine and biology magazine : the quarterly magazine of the Engineering in Medicine & Biology Society. 27. 29-38. 10.1109/MEMB.2008.929888.
[3] Yao, Wen & Chu, Chao & Li, Zang. (2010). The use of RFID in healthcare: Benefits and barriers. 128 - 134. 10.1109/RFID-TA.2010.5529874.
[4] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," in *IEEE Access*, vol. 3, pp. 678-708, 2015, doi: 10.1109/ACCESS.2015.2437951.
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7113786

[5] Tuan Nguyen Gia, Mai Ali, Imed Ben Dhaou, Amir M. Rahmani, Tomi Westerlund, Pasi Liljeberg, Hannu Tenhunen, IoT-based continuous glucose monitoring system: A feasibility study
https://www.sciencedirect.com/science/article/pii/S1877050917310281
[6] P. Gupta, D. Agrawal, J. Chhabra and P. K. Dhir, "IoT based smart healthcare kit," 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), New Delhi, 2016, pp. 237-242, doi: 10.1109/ICCTICT.2016.7514585.
http://www.kresttechnology.com/krest-academic-projects/krest-mtech-projects/IOT/Mech%20IOT-2017-18/IOT%20Basepaper%202017-18/56.IoT%20based%20smart%20healthcare%20kit.pdf
[7] Chao Lia, , Xiangpei Hua, Lili Zhangb, "The IoT-based heart disease monitoring system for pervasive healthcare service" International Conference on Knowledge Based and Intelligent Information and Engineering Systems, KES2017, 6-8 September 2017, Marseille, France
[8] Imadali, Sofiane & Karanasiou, Athanasia & Petrescu, Alexandre & Sifniadis, Ioannis & Vèque, Véronique & Angelidis, Pantelis. (2012). eHealth Service Support in Future IPv6 Vehicular Networks. Future Internet. 5. 579-585. 10.1109/WiMOB.2012.6379134.

[9] Nguyen gia, Tuan & Jiang, Mingzhe & Rahmani, Amir M. & Westerlund, Tomi & Liljeberg, Pasi & Tenhunen, Hannu. (2015). Fog Computing in Healthcare Internet-of-Things: A Case Study on ECG Feature Extraction. 10.1109/CIT/IUCC/DASC/PICOM.2015.51.
[10] Suivi de l'épuisement des adresse IPv4, Arcep https://www.arcep.fr/la-regulation/grands-dossiers-internet-et-numerique/lipv6/suivi-epuisement-adresses-ipv4.html
[11] Atzori, Luigi & Iera, Antonio & Morabito, Giacomo. (2010). The Internet of Things: A Survey. Computer Networks. 2787-2805. 10.1016/j.comnet.2010.05.010.
[12] P. Suresh, J. V. Daniel, V. Parthasarathy and R. H. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," 2014 International Conference on Science Engineering and Management Research (ICSEMR), Chennai, 2014, pp. 1-8, doi: 10.1109/ICSEMR.2014.7043637.
[13] X. Jia, Q. Feng, T. Fan and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, 2012, pp. 1282-1285, doi: 10.1109/CECNet.2012.6201508.

[14] Vashi, Shivangi & Ram, Jyotsnamayee & Modi, Janit & Verma, Saurav & Prakash, Chetana. (2017). Internet of Things (IoT): A vision, architectural elements, and security issues. 492-496. 10.1109/I-SMAC.2017.8058399.

[15] Patel, Ashish & Jhaveri, Rutvij & Dangarwala, Kruti. (2013). Wireless Sensor Network Theoretical Findings and Applications. International Journal of Computer Applications. 63. 25-29. 10.5120/10503-5270.

[16] Al-Fuqaha, Ala & guizani, mohsen & Mohammadi, Mehdi & Aledhari, Mohammed & Ayyash, Moussa. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. IEEE Communications Surveys &amp Tutorials. 17. Fourthquarter 2015. 10.1109/COMST.2015.2444095.

[17] Soni, Dipa & Makwana, Ashwin. (2017). A SURVEY ON MQTT: A PROTOCOL OF INTERNET OF THINGS(IOT).

[18] Imad, Saleh. (2017). Les enjeux et les défis de l'Internet des Objets (IdO). Internet des objets. 17. 10.21494/ISTE.OP.2017.0133.

[19] Objets connectés : quels impacts dans le futur ? https://www.connaissancedesenergies.org/objets-connectes-quels-impacts-dans-le-futur-150227

[20] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung and Y. L. Guan, "Wireless energy harvesting for the Internet of Things," in IEEE Communications Magazine, vol. 53, no. 6, pp. 102-108, June 2015, doi: 10.1109/MCOM.2015.7120024.

[21] Geoff Mulligan, "The 6LoWPAN Architecture"

[22] M. M. Hossain, M. Fotouhi and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," 2015 IEEE World Congress on Services, New York, NY, 2015, pp. 21-28, doi: 10.1109/SERVICES.2015.12.

[23] The Internet Society "The Internet of Things : An Overview" https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf

[24] Anand Paul,[1] **Hameed Pinjari,**[1] Won-Hwa Hong,[2] **Hyun Cheol Seo,**[2] **and Seungmin Rho Fog Computing-Based IoT for Health Monitoring System** **https://doi.org/10.1155/2018/1386470**

[25] Rahmani, A. M., Gia, T. N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., & Liljeberg, P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Computer Systems, 78, 641–658. doi:10.1016/j.future.2017.02.014

[26] Elmenreich, Wilfried. (2020). An Introduction to Sensor Fusion.

[27] S. Alasmari and M. Anwar, "Security & Privacy Challenges in IoT-Based Health Cloud," in *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, 2016 pp. 198-201.

[28] C.Baland, D.Cauquil, T.Gayet, J.Juvigny, R.Lifchitz, N-K.Nguyen "La sécurité de l'Internet des Objets"

https://www.cesin.fr/document/view/9cfdf10e8fc047a44b08ed031e1f0ed1

[29] https://www.journaldunet.com/ebusiness/internet-mobile/1424589-pourquoi-la-securite-des-objets-connectes-medicaux-doit-etre-rapidement-prise-au-serieux/

[30] M. Hassanalieragh et al., "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges," 2015 IEEE International Conference on Services Computing, New York, NY, 2015, pp. 285-292, doi: 10.1109/SCC.2015.47.