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'usage des Objets connectés 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 des matières

Avant-propos 5
Introduction 5
Chapitre 1 : L'internet des Objets 7
Définition et présentation 7
Application de l'IoT 8
Les villes connectées 8
Les Maisons connectées 9
La santé connectée 9
Les technologies de L'IoT 9
RFID 9
Wireless Sensor Network (WSN) 11
Protocoles utililsés dans l'IoT 13
CoAP 13
MQTT 14
Enjeux 16
Economique 16
Sécurité des données et vie privée 18
Normalisation 19
Energétique 20
Conclusion 22
Chapitre 2 : L'IoT dans la santé 23
L'e-Santé 24
Les besoins dans le secteur de la santé 26
Services et application de l'IoT 26
Usage chez les patients 26
Usage dans les hôpitaux 28
Utilisation des capteurs 28
L'utilisation de la technologie RFID 29
Architecture de L'IoT dans la santé 31
Stockage de données 34
Sécurité des données 35
Menace et attaques 38

Les Politiques au sein de la sécurité de l'IoT dans le médical 38
La règlementation aux Etats-Unis 39
La règlementation en Europe 40
Conclusion 41
Chapitre 3 : Projet d'objet connecté permettant le Monitoring de patients atteint du Covid-19 43
Contexte 43
Besoin 44
Choix du capteur 45
Choix du Microcontrôleur 47
Méthode de communication 50
Méthode de Sécurité, Stockage et plateforme d'application 53
Authenticité de l'appareil 57
Confidentialité des données 58
Résultat : 59
Annexe 61
Bibliographie 68

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 sur les différentes technologies exploitées et pouvant être mis en place dans le futur.
Ma volonté initiale a été d'aborder l'utilisation des objets connectés dans ce domaine en pleine expansion. De plus, avec la crise sanitaire du Covid-19, ce choix devenait plus intéressant pour comprendre comment tout cela marchait dans les hôpitaux ou en télésanté.
Mon étude se base sur diverses études concernant le fonctionnement de ces objets dans ce domaine, et comment la mettre en place tout ce réseau d'objets.

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 l'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.

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. [31]
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.

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 de manière générale 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 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. 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, du microcontrôleur, 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. Ce concept est donc 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 (Application et Cloud)
- Présentation : 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 et la détection du niveau d'eau en cas d'inondation.
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, comme Barcelone, Montréal ou encore Montpellier et cela joue un rôle important dans l'économie. [16]

Les Maisons connectées

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. L'ajout de l'IoT dans la domotique a permis de pouvoir prendre en main le contrôle de la maison à distance grâce à des applications sur smartphone.

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 1
- La partie Application permet le stockage des données, la lecture et le traitement de ces données. Cette partie peut être une base de données et une application. [13]

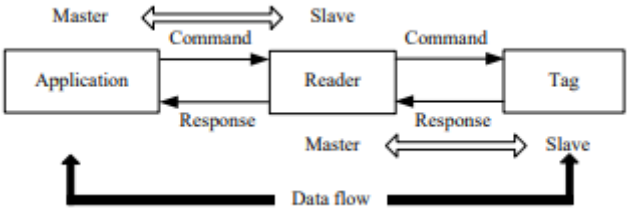


FIGURE 1 COMPOSANTS D'UN SYSTEME RFID

Les Tags sont des petits objets possédant un microsystème et une antenne permettant d'identifier un objet, le lecteur sont des Lecteurs redondant permettant de lire le contenu du tag RFID en utilisant les ondes radio. [13]
S'inspirant de la technologie de lecture des codes-barres, cette technologie aujourd'hui, s'est démocratisée dans divers domaines grâce à sa facilité d'utilisation, sa compacité sa faible consommation énergétique mais aussi la diminution du prix au fil des années.
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]
La RFID se développe sous différents supports :

- **Cartes et badges RFID** : permet l'identification des personnes, les contrôles d'accès et les paiements sans contact
- **Etiquette sans contact RFID** : permet l'identification et la traçabilité
- Etiquettes et stickers : Identification des biens, stockage et inventaire, lutte contre la contrefaçon, traçabilité.
- **Bracelets** : Identification des personnes, paiement sans contact.
- **Tags et porte-clés** : Accès à des locaux.

Autre élément à prendre en compte dans les solutions RFID, les fréquences, il existe quatre 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 haute et plus la portée ainsi que le débit de données à tendance à augmenter. [1]

TABLEAU 1 FREQUENCE DE FONCTIONNEMENT DU RFID

Type de fréquence	Fréquence de fonctionnement	Distance de lecture	Taux de transfert
Basse Fréquence	< 125kHz	0.5m	1kb/s
Haute fréquence	13.56MHz	1m	25kb/s
Ultra-Haute fréquence	800-930MHz	3 à 6m	28kb/s
Hyper Haute fréquence	2.45-5.8 GHz	Plus de 10m	100kb/s

Wireless Sensor Network (WSN)

Autre technologie en lien avec l'IoT. 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 un réseau de mesh permettant de capturer les données extérieures grâce au capteurs, le traitement des données et communiquer avec les autres nœuds.
Les mesh 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]

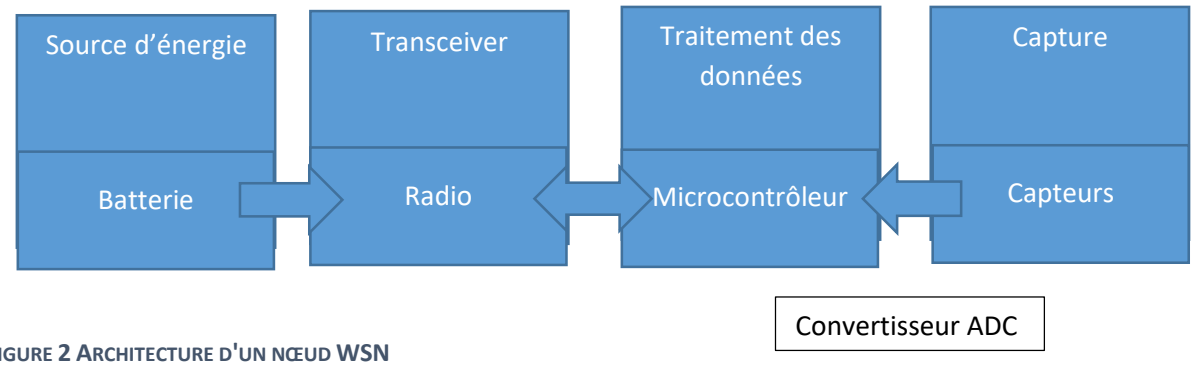


FIGURE 2 ARCHITECTURE D'UN NŒUD WSN

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 la 3G/4G ainsi que la technologie Zigbee IEEE 802.15.4.
L'utilisation des données cellulaires 3G/4G 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.

Protocoles utililsés dans l'IoT

L'architecture de l'IoT est définie par une multitude de protocoles et standards utilisés pour communiquer, traiter, connecter et visualiser les données.
Ces protocoles sont définis à travers les couches du modèle OSI afin d'avoir une vision plus claire du fonctionnement du transport des données.
La figure 3 représente le modèle TCP/IP des protocoles standards utilisés dans le fonctionnement d'un objet connecté pour connecter les objets. Chaque protocole va participer au traitement des données, à la communication entre capteurs ou au Gateway et à la communication entre le Cloud et les clients finaux.
Nous allons voir dans cette partie les protocoles utilisés dans la couche Application pour communiquer, nous discuterons des aspects sécurité, fiabilité et énergétique.

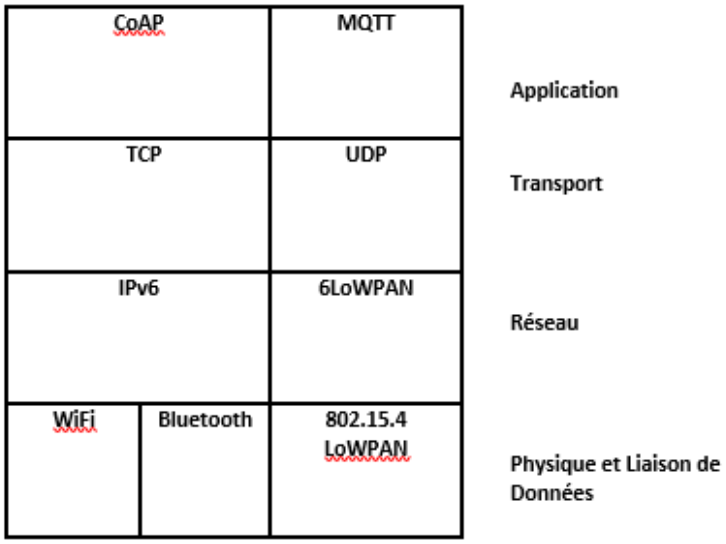


FIGURE 3 MODE TCP/IP DES PROTOCOLES UTILISES DANS L'IOT

CoAP

Le CoAP (Constrained Application Protocol) est un protocole d'Application développé par l'IETF (Internet Engineering Task Force) qui permet aux réseaux de capteurs sans fils contraints d'utiliser le protocole IPV6, ce protocole permet d'utiliser une taille de paquet limité, pour les microprocesseurs à faible puissance avec des taux de pertes importants. [37]

Il s'appuie sur la méthode http en se reposant sur un modèle de Requête / Réponse reprenant quelques parties tels que les requêtes GET, POST, PUT et DELETE afin de fournir des interactions entre le client et le serveur. De plus les échanges fonctionnent de manière asynchrones et synchrones à travers des échanges par UDP. L'utilisation d'un protocole basé sur l'UDP permet de réduire le besoin en bande passante et supprimer le surdébit généré par le TCP. La réduction de ces données permet également d'accroitre la fiabilité en réduisant la fragmentation de la couche Liaison et à réduire la latence dans les réseaux sans fil à faible puissance tel que l'IEEE 15.4 et le Bluetooth.

Afin d'assurer la sécurité le protocole DTLS (Datagram Transport Layer Security) est appliqué, principalement car il s'agit d'un protocole très complet permettant l'authentification, l'intégrité et la confidentialité des données, l'échange de clé entre deux parties et un algorithme de cryptographie. [40]

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. (Figure 4)

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.

Le broker est 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]

Il s'agit-là d'un modèle de fonctionnement différent du protocole CoAP puisque dans l'architecture MQTT, les clients vont s'abonner pour recevoir automatiquement l'information tandis que le protocole CoAP, le client va envoyer une requête au serveur pour reçevoir l'information. (Figure 5)

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

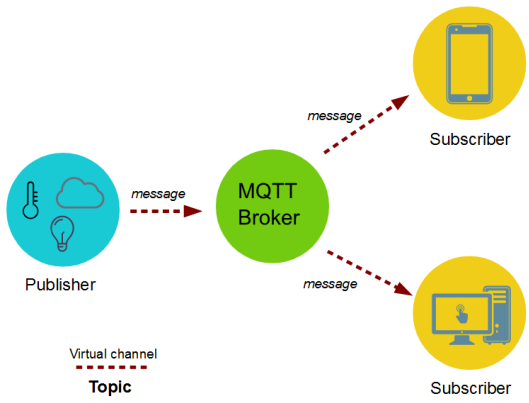


FIGURE 4 FONCTIONNEMENT DU MQTT

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 avec une authentification par Username/Password, 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.

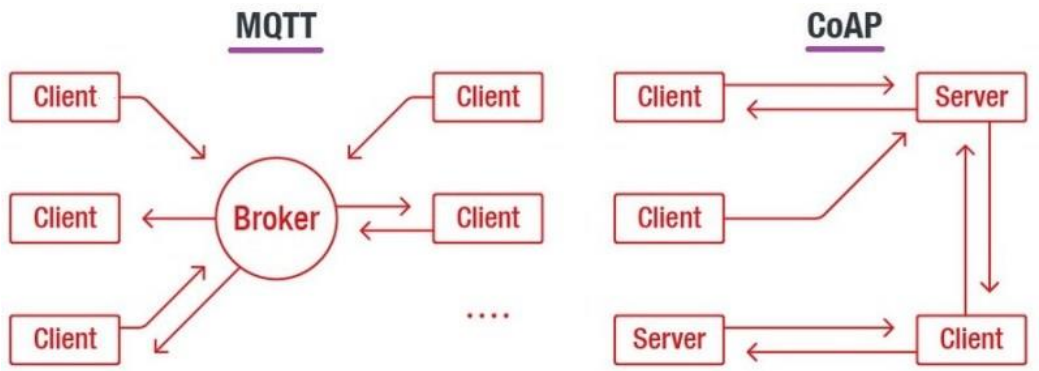


FIGURE 5 DIFFERENCE ENTRE MQTT ET COAP

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 mais également dans la mise en place de service applicatif pour les entreprises.

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. [76]

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 6) [77]

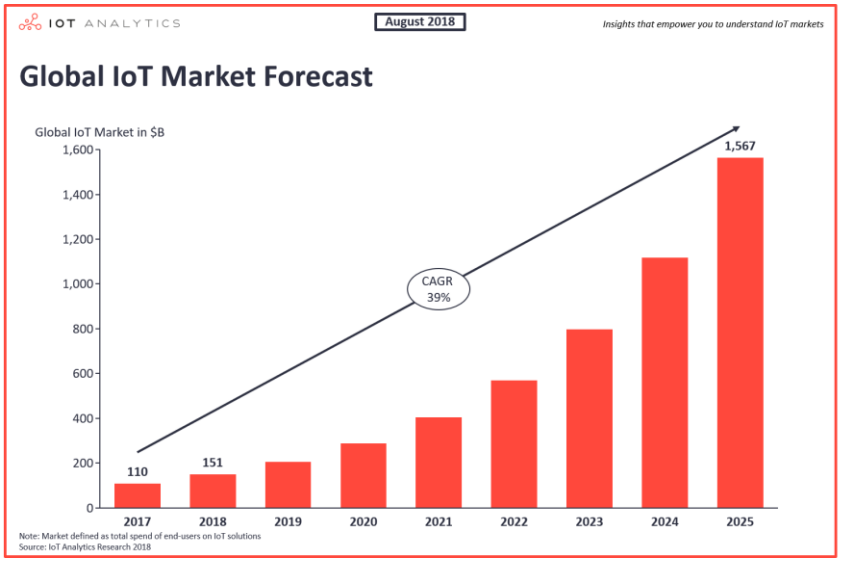


FIGURE 6 ESTIMATION DU MARCHE MONDIAL DE L'IOT JUSQU'EN 2025 [77]

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." [32] 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 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, l'entreprise doit demander à l'utilisateur, son consentement pour la collecte des données, avec l'explication de la finalité des données.

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 beaucoup 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 qui est l'une 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, de microcontrôleur plus efficient 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.

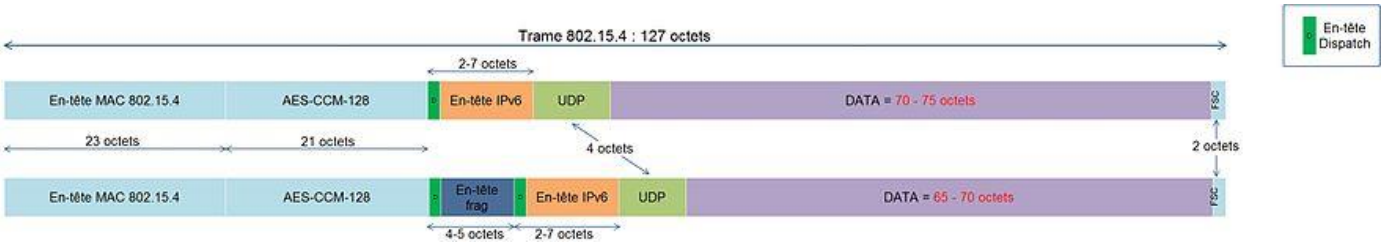


FIGURE 7 PAQUET RESEAU DU 6LOWPAN

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.

Conclusion

L'IoT a révolutionné le marché grâce à son potentiel d'utilisation dans de nombreux domaines tels que l'industrie, la santé ou encore l'automobile. Sa capacité de percevoir l'environnement qui l'entoure puis de transformer ces informations en données informatiques permet d'être exploité pour tout type d'utilisation.
Les technologies tels que le MQTT, le RFID, le WSN sont des technologies assez différentes et pourtant utilisés dans des divers domaines publics ou privé.
Cependant comme l'informatique, l'IoT doit faire face à plusieurs challenges pouvant nuire à sa capacité d'utilisation et la sécurité des données transitant dans le réseau. Les enjeux énergétiques, la sécurité et la vie privée des utilisateurs étant les principaux challenges de l'IoT, celles-ci peuvent être en partie résolus par des protocoles à faible consommation, des cryptages de données mais il reste encore du progrès à faire et les concepteurs font des recherches et progressent afin que l'IoT puisse être une technologie plus fiable et pouvant être adopté plus facilement par les utilisateurs.

Chapitre 2 : L'IoT dans la santé

Le domaine de la santé est un domaine où, la technologie s'installe le plus, elles permettent l'optimisation des processus et l'amélioration de la qualité des soins grâce au développement massif des technologies liées à la santé. Les hôpitaux, cliniques et autres établissement de soins adoptent ces technologies, en collectant et utilisant des données collectés pour l'automatisation et l'analyse des données.
L'Internet of Medical Things (IoMT) 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'étendue de la portée des services de santé, 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%), la collecte de données et transfert pour les machines à Rayon X et d'imagerie. [78]

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 pour un usage externe, les données sont stockées sur un cloud puis peuvent ensuite être visualisé grâce à des applications (ex : application mobile ou app)
Ces données reposent sur le principe du big-data.

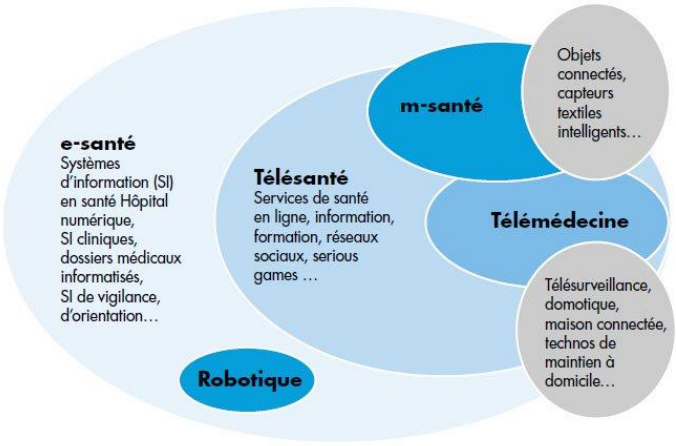
Le big data désigne l'ensemble des données numériques produites par l'utilisation des nouvelles technologies à des fins personnelles ou professionnelles. Il s'agit d'un ensemble de données massif sécurisé.
Dans le domaine de la santé, le big data est donc l'ensemble des données personnelles relatives 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.

L'e-Santé

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.

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 médicaux.
57% estiment que le recours à la téléconsultation pourrait permettre un meilleur accès aux soins et pallier le manque de médecins dans certaines spécialités. [79]

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.

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.

Les besoins dans le secteur de la santé

Le secteur de la santé doit cependant faire face à des challenges, souvent lié à l'humain ou des erreurs matériel. En cause, une surcharge de travail pour le personnel médical ou des défaillances de matériel. Selon l'Institut Mondial de la santé sur une étude réalisé dans plusieurs pays "un patient hospitalisé sur 300 décède d'un accident médical et 60 000 personnes décèdent par an de cette manière " [35], ce qui montre que l'usage de technologies permettant d'améliorer l'efficacité dans les hôpitaux est un enjeu primordial. L'autre challenge est d'assurer une meilleure prise en charge des patients et rendre accessible les soins pour tous.
5 problèmes majeurs sont identifiés dans le domaine médical tels que : les erreurs médicales, le cout des soins, l'accès aux soins et la charge de travail.
Diverses technologies de l'IoT permettent de répondre à ces problèmes tels que le RFID ou l'utilisation de capteurs WBAN.

Services et application de l'IoT

Les systèmes IoT peuvent être appliqués dans divers domaines dans les instituts de santé mais également en dehors grâce à une généralisation d'objets connectés destiné au grand public, tel que la surveillance de maladies chroniques, l'auto surveillance de sa santé, le soin des personnes âgés et des enfants.
La table 1 illustre les différents services et applications des objets connectés utilisés dans le secteur de la santé avec une liste d'usage et des technologies exploités.

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.
D'autres objets connectés destinés au grand publics s'appuie sur une surveillance de l'état de santé. De ce fait l'individu peut gérer sa propre santé avec plus d'autonomie et une proactivité sur leurs bien-être et pathologie.
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 et les problèmes respiratoires.
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 cloud, le médecin va ensuite pouvoir analyser les données du patient depuis une api et prendre une décision. (Figure 8)

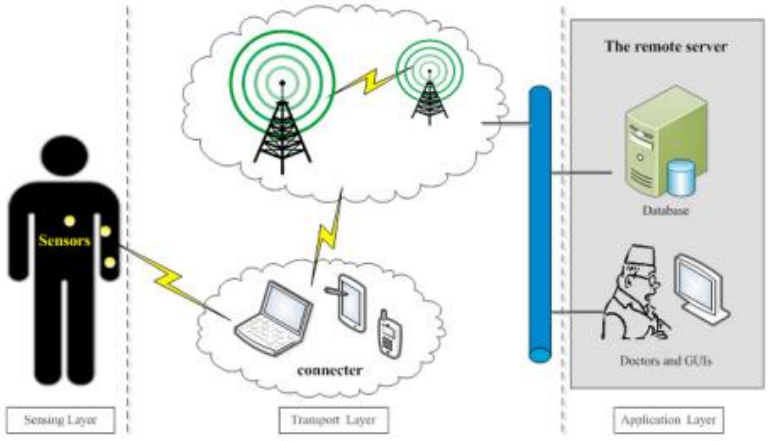


FIGURE 8 SUIVI A DISTANCE D'UN PATIENT A L'AIDE D'OBJETS CONNECTES

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. [80]

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.

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 chaque patient 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 grâce à des machines permettant la collecte et visualisation de ces données. [81]

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 la température du corps.

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. Des pompes à insulines automatiques ont également vu le jour permettant de surveiller et d'administrer automatiquement la quantité d'insuline nécessaire. Des projets comme OpenAPS, un projet Open-Source utilisant la technologie d'intelligence Artificielle pour délivrer de l'insuline en est un exemple parfait. [47]

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 en charge de la surveillance. [7]

L'utilisation de la technologie 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 et des lecteurs RFID présents dans l'hôpital qui vont pouvoir lire les RFID à proximité. 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.

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 9 et 10 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 Microcontrôleur par interface série afin de réaliser un traitement local, ces données sont ensuite envoyés au Gateway par liaison sans-fil grâce à des protocoles tels que le Bluetooth, Wifi, Zigbee ou 6LoWPAN.
- 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. Les données seront reçues sous forme analogique afin d'être traité par le Gateway pour en faire une donnée numérique, les données ensuite traités seront envoyés par Wifi ou liaison cellulaire sur Internet dans le Cloud.
- La partie Back-End est la partie Cloud Computing avec base de données permettant le stockage des données, la visualisation des données par les médecins grâce à des application Web. [25]

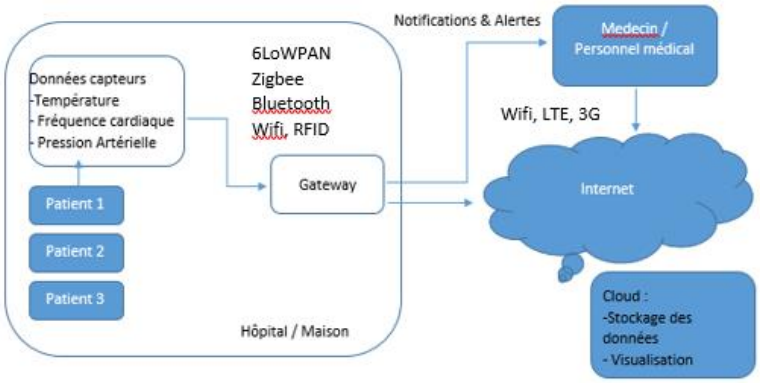


FIGURE 9 ARCHITECTURE POUR LES SYSTEMES IOMT

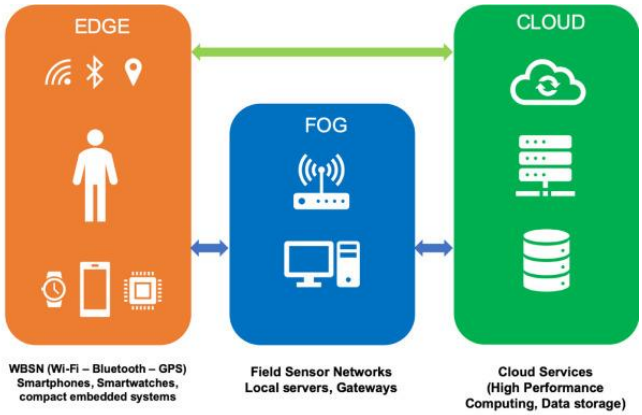


FIGURE 10 ARCHITECTURE SUR 3 NIVEAUX POUR LES SYSTEMES IOMT.

Comme mentionné précédemment le Gateway est un pont entre le microcontrôleur et le Cloud qui permet de stocker temporairement les données 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]

Stockage de données

Le stockage des données concernant les informations sur les patients sont centralisés dans le Cloud afin que les équipes médicales, puissent avoir accès aux dossiers médicaux des patients 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.
Les problèmes de sécurités dans le domaine médical sont issus du capteur et du Cloud, l'authentification, l'authenticité des informations, le consentement et l'autorisation du patient pour partager son dossier a un médecin, l'intégrité et la confidentialité de ces données. [33]

- L'authenticité et l'authentification des données est le fait de vérifier l'origine des données et si les données n'ont pas été modifiés après la transmission de celles-ci par le capteur.
  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 11 présente les potentiels attaques possibles sur un objet connecté médical pouvant être opéré dans le cadre d'une télésanté ou à l'hôpital. Dans ce cas de figure l'attaquant peut s'introduire dans le réseau de l'hôpital afin d'accéder aux dossiers des patients ou modifier certaines données sur l'administration des médicaments, en changeant ces données d'une pompe à insuline par exemple, le dosage peut être mortel. De ce fait l'utilisation de ces objets dans un cadre de dosage de médicaments se réalise avec une surveillance de l'objet connecté par une entité.

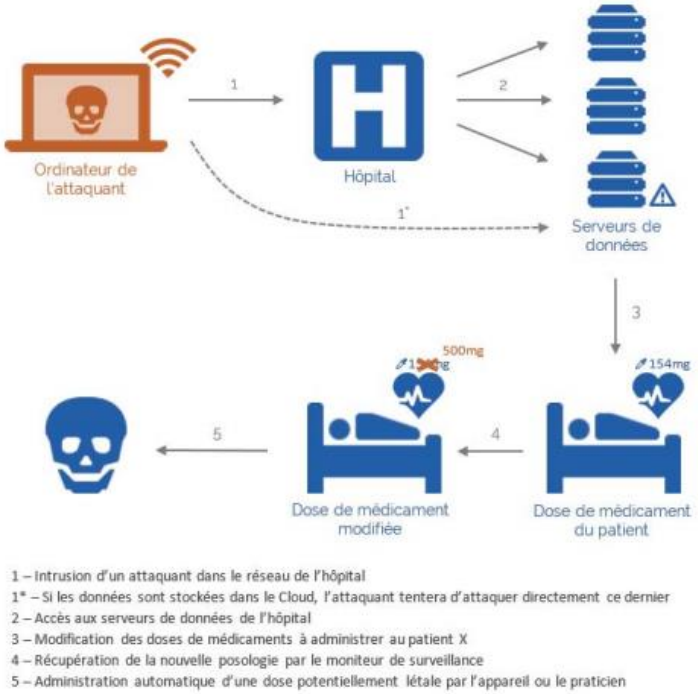


FIGURE 11 ATTAQUE CONTRE UN EQUIPEMENT CONNECTE MEDICAL

Les attaques tels que le Man-In-the-Middle étant la plus répandue, consistant à se faire passer pour une entité lors d'un échange entre deux entités.
L'attaque de MITM est catégorisée en deux parties : l'écoute et la manipulation. L'écoute est une attaque passive, l'attaquant est seulement intéressé par recueillir les informations transitant, tandis que la manipulation, l'attaquant va modifier les données en se faisant passer pour l'envoyeur. Ce type d'attaque se faisant principalement sur le Fog, étant moins puissant que le Cloud.

L'étude menée pour prévenir des attaque MITM [34] présente un système Intrusion Detection System (IDS) placé dans le réseau afin de détecter les intrusions de ce type en utilisant un système de cryptage AES. Les systèmes d'IDS sont placé entre les nœuds Fog, chaque nœud IDS va interroger chaque nœuds fog en envoyant des paquets cryptés. Il va ensuite observer le comportement de du Fog qui est censé décrypter le paquet, multiplier le payload par 2 puis le recrypter avant de le renvoyer à l'IDS. Si le paquet retourné ne correspond pas au critère ou qu'il n'est pas renvoyé, l'IDS conclut que le nœud en question est malveillant.
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.

Afin de sécuriser les objets connectés, il est important de sécuriser toute l'architecture, par exemple généralement dans la communication entre l'objet connecté et le Gateway, celui-ci est sécurisé par cryptage des données AES 256 sur la couche application. Quant à la communication entre le Gateway et le cloud, la sécurité est généralement assurée à travers l'HTTPS par un protocole TLS ou SSL. [45]

- Les données personnelles étant un doit privé, le patient est en choix de partager ses données en signant un accord avec les médecins pour autoriser ou non le partage de son dossier médical dans le système de soin. Le médecin ainsi que le personnel soignant doivent respecter cette accord en demandant d'abord si ces données peuvent être utilisés et doivent mentionner la finalité de celles-ci.
- La confidentialité des données se fait lors de la visualisation du dossier médical, le nom des médicaments et des données confidentielles sur l'api, les données doivent être protégés contre les utilisateurs non autorisés. Il doit y avoir des droits sur les comptes utilisateurs afin que ceux-ci puissent avoir accès aux données dont ils ont accès.

Challenges lié à la sécurité :

- **Mémoire :** Comme nous l'avons expliqué précédemment les objets connectés sont petits et ont donc une capacité de mémoire limitée utilisée pour stocker un OS. De ce fait les objets connectés ont peu d'espace pour exécuter des protocoles de sécurité complexes.
- **Mise à jour de sécurité :** L'infrastructure des objets connectés doit être mis à jours régulièrement afin de corriger les failles de sécurité et ainsi réduire les risques d'attaques.

Menace et attaques

Les attaques et menaces ciblant l'IoT sont catégorisés en 3 groupes :

Attaques sur l'appareil

Avec la généralisation de l'IoT dans le domaine médical, la conception de ces appareils permet d'être plus efficace, moins cher et plus petit, cependant les capteurs collectant continuellement les données en analogique et recueillant des données du patient, l'attaquant peut recueillir ces informations, remplacer le capteur ou réaliser une défaillance.

Attaque sur la communication

Il s'agit du principe de l'attaque du Man In The Middle permettant à l'attaquant d'observer et modifier les données transitant sur le réseau.

Attaque sur le Cloud

Les attaques peuvent également se dérouler chez les prestataires de service Cloud ou les cloud privés pouvant entrainer des pertes et vols de données considérables. Ces données étant particulièrement sensibles et confidentielles, relevant de la vie privée des patients et du secret médical. L'attaquant peut également rendre inaccessible l'utilisation du cloud, rendant le réseau défectueux. [36]

La table 2 catégorise et décrit les différentes attaques possibles dans un réseau IoT et son impact sur le réseau.

Afin de pouvoir sécuriser les données face à ces attaques des stratégies sont mis en place tels que le cryptage de données.

Les Politiques au sein de la sécurité de l'IoT dans le médical

Deux principes doivent être pris en compte dans la politique de l'Internet des objets. Les objets connectés ne doivent pas enfreindre l'identité humaine, l'intégrité, les droits de l'homme, la confidentialité et les libertés.

Les individus doivent pouvoir avoir le contrôle sur leurs données personnelles générés et gardés par les objets connectés. [41]

Afin de pouvoir appliquer des règles générales vis-à-vis de la sécurité des données, les politiques règlementent la sécurité des objets connectés lors de sa conception et lors de son usage afin d'améliorer la situation de protection des données à caractère personnelle.

La règlementation aux Etats-Unis

Aux Etats-Unis, le règlement concernant la confidentialité, l'HIPAA (Health Insurance Portability and Accountability Act) datant de 1996 imposant tous le secteur de la santé, de protéger les données personnelles détenues sur les patients. Elle définit une exigence de sécurité et de confidentialité sur toutes les technologies recueillant des données personnelles mais également une protection des informations personnelles identifiables concernant la santé tenue ou transmit par une entité. [42]

Egalement pour les objets connectés, la sécurité doit respecter des standards tel que des méthodes de cryptage utilisé durant tout le cycle.

L'HIPAA exige une conformité avec :

- **La règle de sécurité :** Les informations personnelles crées, reçu, utilisés et maintenus par une entité doivent avoir une surveillance administrative, une protection physique et technique pour assurer la confidentialité, l'intégrité et la sécurité des objets électroniques exploitant les données personnelles.
- **Règle de confidentialité :** Les informations personnelles requirent des mesures de protections et doivent respecter des conditions lors de l'utilisation et la divulgation des renseignements sans l'autorisation du patient. Le patient à également le droit d'avoir une copie de leurs dossiers médicaux et examiner.
- **Règle de notification en cas de violation :** La loi exige que les entités doivent fournir une notification après une violation des informations de santés non protégés. Cela peut être une divulgation des données d'un patient, une sécurité insuffisante compromettant une fuite de données. [43]

Chaque établissement de santé exploitant des technologies doit être en conformité avec le loi HIPAA, pour cela ces entités doivent régulièrement réaliser des audits, mettre à jour leurs technologies et vérifier régulièrement le réseau, de l'objet connecté au cloud ce qui mets en responsabilité les entités quant au bon fonctionnement de leurs réseaux.

La règlementation en Europe

Le règlement général sur la protection des données établit en Mai 2018 établit les principes du traitement des données et indique une norme quant à la protection des données pour toutes les technologies numériques ainsi que l'IoT.

Cette norme introduit des principes tels que l'accord du patient sur la collecte de données, les obligations de notifications, le principe de Privacy by design et privacy by default, une transparence algorithmique. Cette norme s'applique pour toutes les entités en Europe exploitant les données personnelles des utilisateurs. [44]

La notion de Privacy by design étant particulièrement important dans l'IoT, elle consiste à imposer aux entreprises de prendre en compte les principes de la RGPD dès la conception du projet. L'entité doit donc prendre en compte la sécurité et la confidentialité des données dès le début. La revue Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms [45] traitant sur le Privacy by Design dans l'IoT indique les directives à prendre lors du choix de la plateforme dans les entités.

- Réduction des données collectés : Seulement les données absolument nécessaires doivent être collectés, stockés et traités.
- Anonymiser les données et crypter les données lors de la communication, le traitement et le stockage.
- Eviter la diffusion des données quels soient traités ou non.
- L'agrégation des données
- L'audit régulier du parc et la possibilité de voir les logs pour chaque action.
- Utiliser des technologies Open-Sources et standardisés
- Utiliser des application IoT certifiés

La notion de Privacy By Default s'appliquant sur les concepteurs des systèmes, indique que la mise en place de sécurité, des mesures de confidentialité ainsi que le respect de la vie privée des utilisateurs doit être mis en place dès la conception.

En cas de non-respect du RGPD ou d'infraction, des sanctions peuvent être appliqués pouvant aller jusqu'à 20M€ ou 4% du chiffre d'affaire annuel.

Conclusion

Le marché de l'IoT dans le domaine de la santé ne va cesser de croitre et de plus en plus d'hôpitaux et cliniques vont adopter ces technologies grâce à ces multiples utilisations ses avantages. L'IoT permet de révolutionner le monde de la santé en améliorant les services de santé, des docteurs et des patients de part grâce à sa flexibilité, sa précision et sa facilité pour monitorer les patients. Elle permet également de réduire les coûts de soins de santé grâce à la généralisation de ces objets sur le marché et la diminution des coûts de fabrication avec la recherche et développement.

Dans les hôpitaux l'usage de l'IoT permet aux personnels de travailler plus facilement en réduisant leurs charges de travail grâce à l'utilisation de RFID pour surveiller les patients, médicaments et ainsi réduire les risques d'erreurs médicaux, l'utilisation de capteurs corporels permet aussi de monitorer en temps réel l'état de santé du patient afin de pouvoir recevoir un meilleur traitement lors de la prise de décision. [46]
De plus, la démocratisation des objets connectés dans la santé grâce aux montres connectés permettent d'avoir une approche plus simple sur l'état de santé de la personne. Il peut alors surveiller son corps et peut prévenir contre des maladies ou prévenir d'anomalie cardiaque.
Cependant le secteur de la santé doit faire face à divers challenges et enjeux plus importants que dans d'autres secteurs exploitant les objets connectés. Nous pouvons citer en autre l'exploitation de données personnelles concernant l'état de santé de l'individu qui est un enjeu important.

La confidentialité et l'intégrité des données personnelles est un point important, que le secteur doit impérativement prévenir, la mise en place de la RGPD en Europe ou de L'HIPAA aux Etats Unis empêche en quelque sorte l'utilisation de ces données à des fins malhonnêtes.
Les données étant stockés dans un Cloud elles sont ensuite consultés puis peuvent être transmis à d'autres entités tels que les assurances.
L'enjeu de la sécurité est également un point sensible tant bien d'un point de vue général de l'IoT que le secteur de la santé qui semble être la cible privilégiée des hackers en raison de son flux important de données personnelles sensibles. Il n'y a pour l'instant pas de solution propre au secteur de la santé au niveau de la sécurité. Exploitant seulement des méthodes de cryptage de données, de sécurisation sur l'application et d'une architecture à 3 niveaux.

Malgré ces points et la réticence de certains usagers à cause de problème de sécurité, l'IoT se démocratise de plus en plus et évolue, nous pouvons citer entre autre une meilleure précision dans la lecture des données mais également l'usage d'Intelligence Artificielle pour la prise de décision. De plus de nombreuses entreprises et startup se lancent dans la recherche et conception d'IoT innovant.

Chapitre 3 : Projet d'objet connecté permettant le Monitoring de patients atteint du Covid-19

Contexte

L'année 2020 a été un véritable désastre mondial à cause de la crise sanitaire du Covid-19 ayant affecté plus de 13 millions de personnes avec un nombre de 600 000 décès dans le monde, cela a généré un afflux massif de nombre de cas de personnes touchés par le Covid dans les hôpitaux et soins intensif. Générant ainsi une surcharge de travail pour le personnel soignant et docteurs, devant faire face à cette crise durant des mois afin de limiter la propagation du virus et soigner le plus de patients atteint du virus.
Les principaux symptômes liés au Covid-19 sont principalement la fièvre, la toux sèche et la fatigue mais apparaissent de manière progressive pouvant ensuite entrainer des symptômes graves, tels que des difficultés à respirer ou des douleurs chez les personnes âgées. [49]
Afin de pouvoir aider au mieux le système de santé, des dispositifs informatiques et médicaux IoT sont mis en place, de plus des géants de l'industrie tel que Sigfox encourage l'industrie spécialisé de l'IoT à apporter des solutions permettant de sauver des vies. Enfin, Sigfox étant un fournisseur de réseau de communication, une offre concernant la gratuité des coûts de connectivité jusqu'au 31 juillet 2020. [48]
D'après l'article de Product Coalition[51], les entreprises de l'IoT jouent un rôle majeur contre le Covid, nous pouvons citer Contus, Bridgera, Solution Analysts, Korewireless et Pattern Digital Technologies, développant ainsi des objets connectés dans le domaine médical pouvant être utilisés et respectant les normes et standards.
Des applications tels que des capteurs pour le monitoring de patient, des respirateurs artificiels ou encore la détection de cas positifs par géolocalisation sont proposés et utilisés dans le cadre de cette crise sanitaire pour limiter la propagation. De plus grâce au self-monitoring, toute personne peut surveiller son état de santé et peut donc prédire à l'avance la situation du patient afin qu'elle puisse être pris en charge rapidement.
Dans les hôpitaux, les dispositifs habituels cités dans le Chapitre 2 tel que la localisation de personnes et objets médicaux, le monitoring, la localisation de patients positifs ainsi que la mise en place d'espace réservé pour les soins de ce virus sont déployés. [50]

Autour du thème du Covid-19, nous allons aborder un projet de monitoring à distance de patients pouvant être atteint du Covid-19 dans les hôpitaux. Comme nous le savons les principaux symptômes sont une fièvre et une toux, grâce à l'utilisation de capteurs de température pouvant monitorer l'état de santé du patient périodiquement pour ensuite estimer si la personne doit se faire tester contre la maladie.
Le but de ce projet est de mesurer la température corporelle chez les patients par voie buccale ou axillaire, étant donné que la prise de température par ces voies est les plus optimal selon les sources du Gouvernement.
Une personne a un état de fièvre si la température dépasse 37.5°C par voie orale et 37,3°C sous l'aisselle. La prise de température doit également être prise périodiquement le matin ainsi que le soir (toutes les 12h). [55]

Besoin

Afin de pouvoir mesurer correctement la température corporelle des patients, sécuriser les données et pouvoir adopter cette technologie dans les hôpitaux, plusieurs problématiques doivent être pris en compte tel que le choix du capteur, le type de microcontrôleur, le type de sécurité à adopter de la méthode de communication jusqu'au stockage avec un contrôle d'accès, les interférences engendrées par les appareils électroniques pouvant créer du bruit et ainsi réduire la précision des capteurs.
Pour cela nous allons tous d'abord comparer les capteurs pouvant être utilisés dans ce projet et quel choix serait le plus pertinent, comparer la précision, la taille, l'interfaçage, la consommation, le type d'usage et le prix.
Pour les microcontrôleurs, les interfaces, les performances, l'autonomie, la taille, le cout et la mémoire sont à prendre en compte.
Nous allons ensuite regarder les méthodes de communications entre capteur et serveur, pouvant être utilisé dans le milieu Hospitalier et sur quelle fréquence afin de ne pas avoir d'interférence avec d'autres appareils électronique (RFID, autre capteur IoT…)
Puis enfin nous verrons l'aspect sécurité avec le choix du type de protocole de communication, la méthode de sécurité et l'accès aux données sur l'interface.

Choix du capteur

Le choix du capteur de température est important, il s'agit de la pièce permettant la prise de température et déterminer la situation du patient.
Afin de répondre à ce besoin, il faut que :

- La précision du capteur soit suffisamment précise : de l'ordre de +/- 0.1°C.
- Le capteur soit d'usage médical : Pouvant être waterproof pour un usage buccal et stérilisable pour de multiples usages. Le capteur doit également être protégé dans un embout métal comme l'inox chirurgicale.
- L'interfaçage : Conversion Analog – Digital dans le SOC ou Digital directement
- Le prix : Nous allons voir le prix des capteurs par quantité de 1000 (Etant dans un usage médical et devant être déployé)
- La taille du capteur doit être suffisamment petit pour plus d'ergonomie
- La consommation du capteur en actif et en repos doit être la moins élevée possible

Ainsi avec ces contraintes, nous avons dressé une liste des capteurs répondant à ces critères que nous allons pouvoir comparer pour ensuite choisir le capteur le mieux adapté.
Nous avons choisi des capteurs pouvant être utilisé comme capteur corporel, pour le type de capteurs il existe également 4 types utilisés pour des applications spécifiques : les Thermistance, les RTD, thermocouple et Semi-Conducteur ayant des précisions, des plages de température, une consommation et une sensibilité différente, la figure 3 permet de comparer ces différents types de capteurs. [56]
Parmi ces choix, le type de capteur le plus pertinent est le semi-conducteur en raison de leur précision, de leur faible consommation d'énergie ainsi que leur petite taille. Les Thermistors se sont imposés dans l'IoT en raison de leurs faibles prix et d'une bonne précision, il s'agit d'une alternative low-cost des RTD.
De plus dans un usage médical la précision est le point le plus important, il faut une précision d'environ +/- 0.1°C ou +/-0.2°C au maximum.

Les différents capteurs répondant à ces critères sont le LMT70 et TMP117 de Texas Instrument ainsi que le MAX30205 de chez Max Integrated.

Le capteur LMT70 possède des caractéristiques intéressantes tel que sa petite taille, son prix qui ne dépasse pas les 1€ et également sa consommation en mode actif de seulement 12uA et une consommation au repos de 50nA. Cependant sa précision est de +/-0.18°C sur la plage de température de 20 à 42°C et son interfaçage sur le microcontrôleur se fait par interface Analogique, ce qui implique que le capteur doit passer par interface ADC et donc générer une charge pour le microcontrôleur qui doit convertir les données analogiques en numérique. [57]

Le capteur TMP117 est le capteur le plus cher parmi les trois qui est de 1,64€, cependant sa précision de +/- 0.1°C sur une plage de 30 à 45°C ainsi que son interfaçage en Digital rendent ce capteur un choix intéressant. Sa consommation, bien que plus élevée que le LMT70 n'est pas énergivore.
Son interfaçage se fait également par interface I2C et SMBus. De plus le capteur possède une fonction d'alerte programmable. [58]
Le TMP117 se décline en plusieurs versions tel que l'usage médical avec le TMP117M, conforme aux exigences applicables aux thermomètres médicaux définies par l'American Society for Testing and Materials (ASTM E1112) et par l'Organisation internationale de normalisation (ISO 80601). [60]

Enfin le MAX30205 se plaçant entre les deux précédents capteurs au niveau du prix, étant de 1.39€, avec une précision de +/- 0,1°C de 37 à 39°C puis de +/-0.2 de 39 à 41 et de 35.8 à 37°C, ne donne pas une précision optimale pour notre usage en cas de fièvre. De plus sa consommation active est relativement élevée, grimpant à 600uA en mode Actif et 1.65uA en mode repos. Son interfaçage se fait également en Digital par liaison I2C sur le microcontrôleur. [59]

Parmi ces choix, le capteur le plus adapté pour notre utilisation serait le TMP117, malgré son prix plus élevé que les 2 autres capteurs, sa précision de +/-0.1°C entre -30 à 45°C reste la plus adéquate pour l'usage de contrôle de température dans les hôpitaux dans le cadre de la crise sanitaire qui demande une très grande précision. De plus son interfaçage en digital et sa consommation assez basse permet de réduire la charge du processeur.

TABLEAU 2 COMPARAISON DES CAPTEURS DE TEMPERATURE

Capteurs	LMT70	TMP117	MAX30205
Nom référence exact	LMT70YFQR	TMP117MAIYBGR	MAX30205MTA+
Type	Semi-conducteur	Semi-conducteur	Semi-conducteur
Prix (par 1000) €	0,86 €	1,64€	1,39€
Précision (°C)	+/- 0.18°C de 20 à 42°C	+/- 0.1°C de 30 à 45°C	+/- 0.1°C de 37 à 39°C
Taille	0.88 mm x 0.88 mm	2.00 mm × 2.00 mm	2.00 mm x 2.00mm
Forme	SMT	SMT	SMT
Interface	Analogue	Digital	Digital (I2C)
Consommation actif	12uA	135uA	600uA
Consommation repos	50nA	1.25uA	1.65uA

Choix du Microcontrôleur

Le microcontrôleur ou MCU en anglais est la partie qui va récupérer les données du capteur pour les traiter et réaliser la communication sans-fil.
Il faut donc que le microcontrôleur choisi soit alimenté par une batterie donc assez économe en énergie pour pouvoir tenir plusieurs journées pour gérer le capteur et la communication.
De plus la sécurité étant principalement géré principalement par des modules externes de communication afin de réduire la consommation tel que des modules Wifi ou radio fréquence (LoRaWan, Zigbee). Les sécurités utilisées sont principalement des méthodes de cryptographie (AES, SHA-2) ou également l'utilisation de certificat SSL, TLS.
Le microcontrôleur doit également être de petite taille pour être plus ergonomique sur le port de l'objet connecté. Egalement il servira seulement à réaliser les traitements et la communication, donc il n'y a pas besoin d'avoir un OS mais seulement la capacité d'exécuter un programme.

Parmi différents MCU répondant aux critères imposés, nous avons choisis 4 capteurs :

- L'ESP32 d'Espressif
- L'ATMEGA32U4 de Microchip Technology
- Le STM32 de ST Microelectronics
- Le SAMD21 de Microchip Technology

L'ESP32 est un microcontrôleur de petite taille (25.5 x 18.0 x 2.8mm) et facile d'utilisation avec l'implémentation de la WIFI 802.11 et le Bluetooth 4.2 opérant jusqu'à 4 Mbps.
L'ESP32 possède un CPU 2 cœurs Xtensa LX6 cadencé à 240MHz et une mémoire flash de 4Mb. Elle possède également 520Kb de mémoire vive, ce qui permet d'effectuer des taches lourdes.
La sécurité des données effectuée par le MCU est la cryptographie AES, SHA2 et RSA.
La consommation également en mode actif dépend de l'utilisation du Wifi, Bluetooth. La figure 12 montre la consommation énergétique du MCU avec la Wifi sur plusieurs distances et le Bluetooth lors de l'envoi et réception de données. [62]
L'ESP32 possède également plusieurs modes d'alimentation qui vont réduire la cadence du processeur tel que le Modern Sleep jusqu'à l'hibernation. Ces consommations sont listées sur la table 4.
L'ESP32 étant Open Source, les langages de programmation se font en C, les librairies API étant essentiellement dans ce langage. Cependant il peut également être programmé en C++ avec Arduino, grâce à plusieurs librairies Arduino permettant l'exploitation de ce MCU. [61]

Mode	Min	Typ	Max	Unit
Transmit 802.11b, DSSS 1 Mbps, POUT = +19.5 dBm	-	240	-	mA
Transmit 802.11g, OFDM 54 Mbps, POUT = +16 dBm	-	190	-	mA
Transmit 802.11n, OFDM MCS7, POUT = +14 dBm	-	180	-	mA
Receive 802.11b/g/n	-	95 ~ 100	-	mA
Transmit BT/BLE, POUT = 0 dBm	-	130	-	mA
Receive BT/BLE	-	95 ~ 100	-	mA

FIGURE 12 CONSOMMATION ACTIVE DE L'ESP32 [62]

L'ATMEGA32U4 est un microcontrôleur basé sur une architecture AVR 8 bits peu gourmand en énergie avec de bonnes performances, ces MCU se retrouvant principalement sur les cartes Arduino.

Le processeur est cadencé à 16Mhz, avec une consommation active de 10mA et possédant plusieurs modes d'économie d'énergie, listés sur la table 4.
L'Atmega possède également une mémoire flash de 32Kb et une mémoire vive de 2.5Kb ce qui est suffisant pour effectuer de légères opération sans pouvoir stocker localement les données.
La programmation peut se faire en C ou également en C++ avec Arduino.
Cependant le microcontrôleur ne possède pas de mode de connectivité tel que la Wifi ou le Bluetooth, donc pas de sécurité. Un module doit donc être ajouté afin de pouvoir communiquer et sécuriser les données. [63]

Le STM32 est un microcontrôleur spécialement conçu pour un usage médical et industriel, possédant une architecture ARM Cortex M4 32bits et cadencé à 120MHz. Avec une consommation énergétique active d'environ 40mA, il possède également plusieurs mode d'économie d'énergie tel que le Sleep Mode, le Stop Mode et le Standby Mode.
Le microcontrôleur possède 1Mb de mémoire flash permettant le stockage de programme et 128Kb de mémoire vive.
La sécurité quant à elle, est assuré par une méthode de cryptage AES128,192, 256, DES et SHA-1. Cependant comme l'ATMEGA, ce microcontrôleur ne communique qu'en liaison série, l'usage d'un module externe tel que la Wifi doit être ajouté pour communiquer sans-fil. [64]

Le dernier MCU à comparer, le SAMD21 est un microcontrôleur très basse consommation, se situant entre le ATMEGA et le STM32 en terme de performance. Il s'agit également du microcontrôleur présent dans les cartes de développement Arduino Zéro. Possédant une architecture ARM M0 32bits d'une puissance de 48MHz. Elle possède une mémoire flash de 256Kb et mémoire vive de 32Kb.
Quant à la consommation énergétique, elle consomme 6.8mA en mode active et possède plusieurs modes d'économie d'énergie. Le MCU n'intègre pas de sécurité, ni de module de communication. [65]

Afin de pouvoir répondre aux exigences lié à la sécurité médicale, la consommation énergétique, la quantité de mémoire suffisante afin de programmer le microcontrôleur avec les librairies du capteur de température et la gestion de la méthode de communication.
Les choix reviennent à l'ESP32 et au STM32.

L'ESP32 possédant une connectivité sans-fil intégré et étant le microcontrôleur le plus puissant parmi ces choix avec une mémoire flash de 4Mb et une ram de 520Kb permettant de réaliser diverses tâches. La sécurité des données étant cryptés, l'ajout d'une sécurité supplémentaire sur la communication avec du TLS et SSL est possible.
Le prix étant également très attractif, nous pouvons retrouver la puce à 1.40€ chez des fournisseurs tel que Mouser.
Il s'agit cependant d'un microcontrôleur assez énergivore avec une consommation de 210mA en mode active.

Le STM32 se situant en dessous par rapport à l'ESP32 en terme de performance mais elle est cependant la moins énergivore avec une consommation de seulement 40mA. Elle intègre également une sécurité des données directement sur le microcontrôleur afin de pouvoir prévenir des attaques sur le MCU. Le prix cependant, étant relativement élevée (8€) est un des points négatifs de ce microcontrôleur, à cela il faut également ajouter un module de communication sans-fil qui va s'ajouter au prix et une consommation plus élevée en fonction du module choisi.
Le choix final revient donc à l'ESP32.

Méthode de communication

Les communications sans-fil ont un rôle important dans les hôpitaux, ils servent à interconnecter les patients et objets et fournissent une vitesse de communication élevé pour certaines tâches importantes.
Plusieurs modes de communication peuvent être envisagés, cependant étant un milieu fermé et utilisant beaucoup d'objets électroniques, l'acquisition des données et la communication ne doivent pas être perturbé par du bruit électronique généré par les autres appareils électroniques.
De plus il ne faut pas que la fréquence de communication soit perturbé par d'autres objets différents utilisant la même fréquence. Les fréquences liées au RFID mais aussi des technologies comme le Bluetooth, Zigbee et Wifi utilisant la fréquence 2.4GHz peuvent poser problèmes s'ils fonctionnent sur les mêmes canaux de communication. [67]
Les communications sans-fil les plus utilisés dans les hôpitaux sont la Wifi, le WSN, le WBAN, le RFID mais également les données cellulaires tel que la 4G. [66]

Dans notre cas d'utilisation, plusieurs choix s'imposent à nous, l'hôpital étant un lieu restreint, une communication sur moyenne distance ou courte distance peut être envisagée. L'ajout de Gateway entre le microcontrôleur et le Cloud permet aussi un traitement des données plus efficace mais relève un prix élevé.
Parmi les différents modes de communications, le Wifi et Zigbee peuvent être choisis pour ce projet de relève de température. Nous allons comparer ces modes de communication différents pour ensuite choisir la plus appropriée.

Zigbee : Le protocole de communication Zigbee été développé par la Zigbee alliance en 2003, est une méthode permettant la communication à courte distance, avec une faible vitesse de transmission des données mais avec une consommation électrique très faible, ce qui permet d'avoir une très longue durée de batterie pour les objets connectés (Plusieurs années). [68]
Etant très utilisé dans le domaine de la domotique notamment dans le contrôle de la maison, ce protocole est également utilisé dans la santé pour le monitoring de patients et les équipements de santé dans les hôpitaux. Ce protocole à la particularité de fonctionner en réseau mesh, ce qui est utile dans les hôpitaux ou il peut y avoir des interférences avec les murs et autres appareils.
Le protocole Zigbee s'appuie sur le design du standard IEEE 802.15.4 (Low Rate Wireless Personal Area Network) en réutilisant la couche d'accès et physique de celui-ci, tout en rajoutant une partie propre à Zigbee tel que la partie réseau et le support d'application pour les appareils Zigbe avec la sécurité sur les couches. (Figure 13)
En exploitant la fréquence 2.4GHz utilisée par les protocoles de communications IEEE802.11 tel que le Wifi 2.4Ghz et le Bluetooth, des problèmes d'interférences peuvent apparaitre entre d'autres appareils exploitant la bande 2.4GHz. Le problème peut être réglé en sélectionnant un canal non utilisé. [71]
Cependant le protocole possède une faible vitesse de transmission des données en fonction de la fréquence, qui est de 40kb/s sur entre 860-960MHz et 250kb/s sur 2.4GHz.

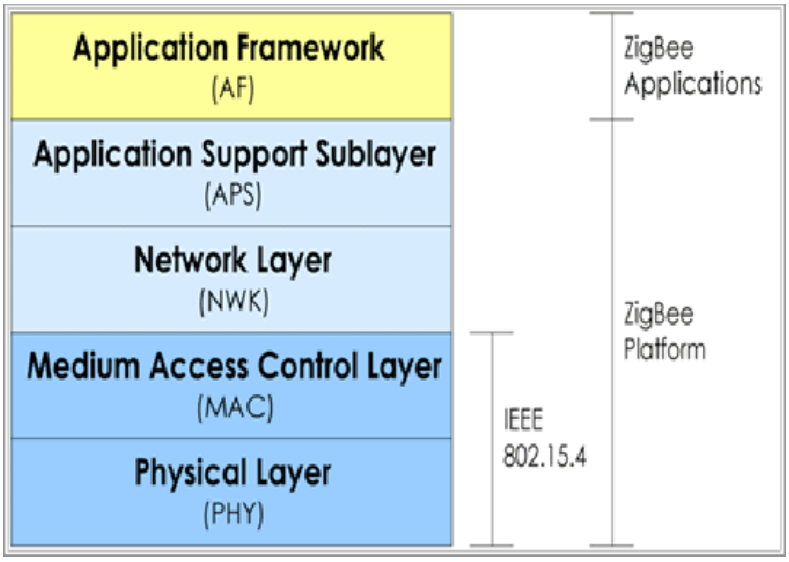


FIGURE 13 ARCHITECTURE DU PROTOCOLE ZIGBEE

Le protocole Zigbee inclut également une sécurité robuste, grâce à un cryptage des données en AES sur la couche Réseau et une authentification entre les appareils entrant dans le réseau par l'échange de clé. [69]

Le réseau Zigbee se compose de 3 modules :

- Le coordinateur est un module gérant les opérations de haut niveau sur le réseau tel que la sécurité et l'authentification
- Les routeurs permettent d'agir en tant que Gateway c'est-à-dire d'étendre la portée du réseau en répétant les signaux de module en module, similaire à la fonction Multi-Hop des WSN. Elles permettent également aux autres modules de s'enregistrer auprès de ces routeurs au lieu du coordinateur afin d'éviter la surcharge de celui-ci.
- Les End-Devices sont les modules terminaux tels que les capteurs, actionneurs. [70]

Wifi : La wifi est un standard de la communication sans fil basé sur le standard IEEE 802.11, fonctionnant sur les fréquences 2.4GHz et 5GHz et ayant une portée entre 30 et 50m. La particularité de cette technologie est que la vitesse de transmission des données est relativement élevée allant entre 150 et 200Mbps.
De plus la sécurité est fournie par un cryptage AES 128 ainsi que le WPA2 pour l'authentification fournissant une sécurité supplémentaire.
Cependant l'utilisation de la Wifi implique une consommation élevée à cause de la vitesse de transmission des données. [67]

Il s'agit d'une technologie très exploitée et peu onéreuse et pouvant être fourni directement sur le microcontrôleur ou par le biais d'un module Wifi.

Nous avons vu 2 méthodes de communication, le protocole Zigbee peut être une solution adéquate pour notre utilisation grâce à une sécurité fiable et une durée de vie des batteries très longue, cependant cette technologie implique l'installation d'un réseau Zigbee comportant 3 modules particulièrement onéreux.
La Technologie Wifi quant à elle possède une vitesse de transmission assez élevée ainsi qu'une portée suffisante dans les hôpitaux, cependant la consommation énergétique avec l'utilisation de la Wifi est relativement supérieure au protocole Zigbee mais pour notre utilisation de prise de température de manière journalière, la Wifi convient parfaitement, de plus la Wifi est une technologie de communication qui s'est démocratisée et l'installation de Wifi est particulièrement simple avec des bornes Wifi. De plus le microcontrôleur ESP32 possède une communication par Wifi intégré, ce qui permet de ne pas à avoir à acheter un module supplémentaire.

Méthode de Sécurité, Stockage et plateforme d'application

Les données seront stockés sur une base de données MySQL hébergé sur un Cloud local privé, qui est plus adapté dans un usage médical en terme de sécurité et confidentialité.
De plus le cloud sera de type IaaS (Infrastructure as a Service), il s'agit d'un modèle de cloud permettant à l'entreprise de gérer complètement la partie traitement, application, stockage et la gestion de leurs machines virtuelles. Seul l'hébergeur fournit le matériel. Cependant la responsabilité de protéger les données des patients en fournissant une sécurité respectant les normes. [33]

Avant le stockage des données sur le serveur, les données doivent d'abord être traités par une plateforme IoT. L'objet connecté va se connecter sur la plateforme afin de pouvoir communiquer les données brutes.
Des protocoles applicatifs sont utilisés comme plateforme pour pouvoir réaliser cette méthode de traitement.
Les protocoles applicatifs les plus utilisés dans l'IoT sont le MQTT, XMPP, les API REST, CoAP. [72]

Ces plateformes servent également comme interface de visualisation des données en interrogeant la base de données comme expliqué sur la figure 14.

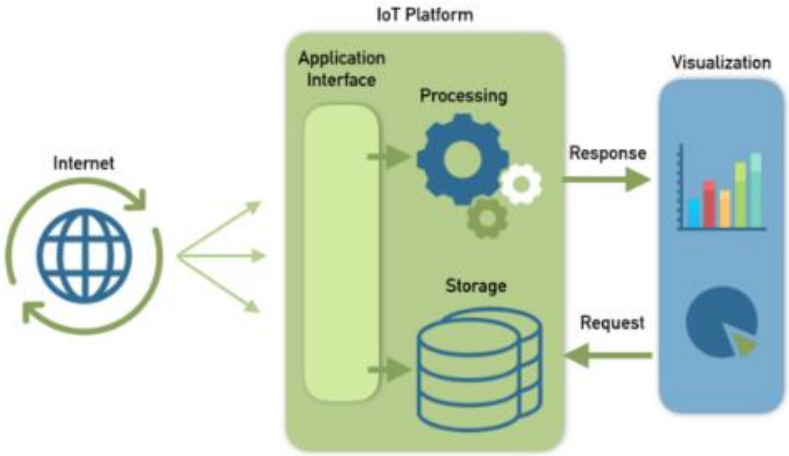


FIGURE 14 SCHEMA DE TRAITEMENT DES DONNEES

Dans notre projet, nous allons partir sur une plateforme d'API Rest qui permet de gérer, identifier et manipuler des ressources par une interface d'application. En utilisant le protocole HTTP pour communiquer grâce à des requêtes tels que GET, PUT, POST, DELETE), le microcontrôleur peut envoyer grâce à la fonction POST, une prise de température à l'API qui s'occupera de traiter la requête et enverra une réponse avec un code indiquant l'état de la réponse dans la trame HTTP.
Pour la visualisation des données, le client va envoyer une requête GET permettant d'interroger la base de données afin de récupérer les données issues du patient.

- 2xx indique le succès du traitement de la requête du client (exemple : 200 pour OK)
- 3xx redirige le client vers un autre lien
- 4xx indique une faute dans la requête du client (exemple : 404 pour Not Found)
- 5xx indique une erreur de la part du serveur (exemple : 500 pour Internal Server Error)

Nous allons utiliser l'API REST Node.js qui est très utilisé dans le domaine de l'IoT, cela permettra de recevoir les données température et DeviceId du microcontroleur afin de les traiter et d'avoir une interface accessible au personnel se connectant sur l'interface grâce à des fonctions GET interrogeant la Base de données par des requêtes SQL.
La base de données que nous allons exploiter sera MySQL.

La base de données sera composée de 3 tables, PatientInfo, TemperatureMeasure, DeviceAttribution comme il est montré sur la figure 15.

La table PatientInfo contiendra l'Id du patient ainsi que son Nom, Prénom.
TemperatureMeasure stockera les températures relevées, l'alerte en cas de température anormalement élevée ou basse grâce à la propriété d'alerte du capteur de température, la date/heure du relevé.
DeviceAttribution est une table indépendante permettant, en cas de changement de patient pour un capteur, de pouvoir assigner le bon appareil pour le patient lors du stockage de données et donc éviter l'erreur.
Lorsque les données issues du capteur seront reçues sur l'API, les données reçues seront l'ID du microcontrôleur, la température relevée et l'alerte.
L'API va tout d'abord sélectionner le PatientID présent sur la table DeviceAttribution dans lequel le DeviceID correspond à celle du capteur sur la requête POST.
Puis Insérer les données sur la table TemperatureMeasure avec le PatientID relevé sur la table DeviceAttribution. Voir Figure 16
En cas de changement opéré sur l'API, une fonction permettra de réaliser une requête SQL Update pour changer les données sur la table DeviceAttribution, le changement s'opèrera également sur la Table TemperatureMeasure lors des prochaines insertions.

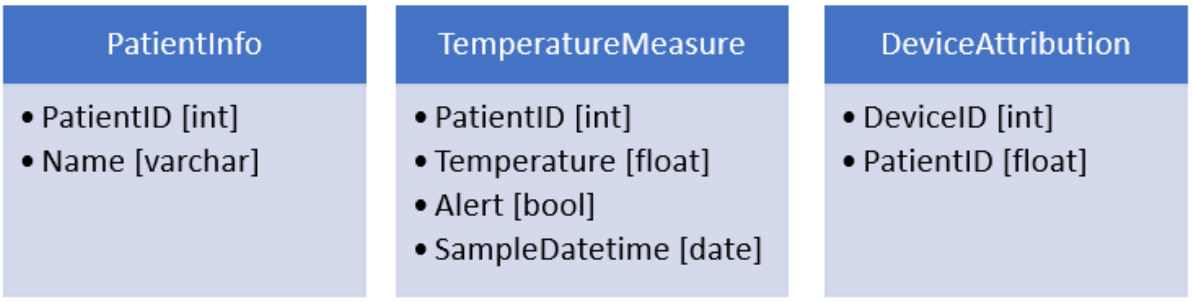


FIGURE 15TABLES DE LA BASE DE DONNEE

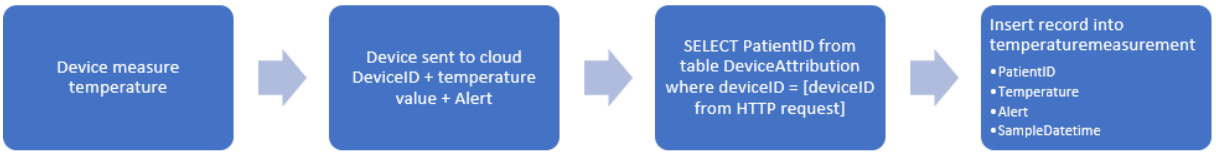


FIGURE 16 SCHEMA DE TRAITEMENT DES DONNEES

La principale fonctionnalité des API Rest est la particularité d'utiliser des routes, c'est-à-dire créer un chemin permettant d'exécuter des fonctions définis. En spécifiant dans l'url le chemin suivi d'une ou plusieurs valeurs, la fonction définie sur ce chemin va récupérer les valeurs et exécuter cette fonction. [73]

Lors d'une demande de visualisation de données d'un patient, l'url spécifiée sera https://test/temperature/:**patientid**

Dans lequel la route sera Temperature et PatientId sera la valeur récupérée par la fonction permettant à l'API d'interroger la Base de données de récupérer les données du patient.

Le programme ci-dessous représente le programme Node.js permettant d'interroger la base de donnée via une route GET pour la récupération des données issus du patient portant l'id inscrit sur l'url.

En utilisant la méthode post sur l'url : www.cloud.hospital/temperature/get?id=4

Les paramètres récupérés seront id correspondant à l'id du microcontrôleur, qui va ensuite être stocké dans une variable id. La requête SQL sera ensuite envoyée avec la valeur de la variable id.

La requête va tout d'abord sélectionner les valeurs Temperature, Date, Alert de la table TemperatureMeasure dans lequel le Patientid correspondant au Patientid de la table DeviceAttribution est égale au DeviceID qui correspond à la valeur fournie dans la variable. Le résultat de la requête sera ensuite envoyé au client.

```
var mysql = require('mysql');

var con = mysql.createConnection({
  host: "host",
  user: "username",
  password: "password",
  database: "temperature"
});

router.get('/temperature/get', function(req, res) {
  var id = req.param('id');

  con.connect(function executesql(err) {
     if (err) throw err;
con.query("SELECT (Temperature, SampleDatetime, alert) FROM TemperatureMeasure
IN ( SELECT Patientid WHERE DeviceID = id", function(err, result, fields) {
 if (err) throw err;
    res.send(result);

});
```

```
});
});
```

Le programme Js ci-dessous correspond à l'insertion des données provenant de requêtes POST des capteurs : www.cloud.hospital/temperature/post?id=4&temp=38&alert=1
Tout d'abord le JS va récupérer les valeurs transmises sur l'url id=4 temp=38 et alert=1 puis va les stocker dans des variables.

```
var mysql = require('mysql');

var con = mysql.createConnection({
  host: "host",
  user: "username",
  password: "password",
  database: "temperature"
});

router.get('/temperature/post', function(req, res) {
  var patientid = req.param('id');
  var temp = req.param('temp');
  var alert = req.param('alert');

  con.connect(function executesql(err) {
     if (err) throw err;
con.query("INSERT INTO Temperaturemeasure (Temperature, SampleDatetime, alert)
VALUES (temp, now(), alert) SELECT DeviceID FROM DeviceAttribution WHERE
patientid = patientid", function(err, result, fields) {
 if (err) throw err;
    console.log(result);

});
});
});
```

Authenticité de l'appareil

Pour vérifier que les microcontrôleurs envoyant les données sur l'API soient bien authentiques, il faut vérifier leurs authenticités afin d'éviter toute attaque contre le réseau, permettant à un attaquant de se faire passer pour un microcontrôleur et donc envoyer des données frauduleuses ou récupérer des données des patients.

Une solution d'authentification du Microcontrôleur doit donc être mis en place par le biais d'une récupération de l'identifiant constructeur du microcontrôleur qui sera envoyé à l'API à travers une requête, l'id sera alors comparé à celle inscrit sur la base de donnée. Si l'id est correcte, le microcontrôleur aura l'accès en écriture et pourra envoyer les données sur l'API. Sinon les données ne seront pas transmises.
L'obtention du ChipId de l'ESP32 se fait grâce à cette commande :

```
chipid=ESP.getEfuseMac();
```

Le chipId est une adresse MAC de longueur 6 bytes.

Une authentification par certificat TLS sur Node.js est également possible avec une génération de certificat. Les certificats doivent être placés sur le serveur Node.js et sur les ESP32 en uploadant sur Arduino dans le dossier **/sketch/data/.** [74]
Le programme Arduino doit également réaliser la vérification de certificat en s'authentifiant à l'API.

Confidentialité des données

Les données personnelles des patients ne doivent pas être vus par tout le personnel médical, seul les personnes en charge du patient peuvent avoir accès à ces données sans pouvoir les modifier ou supprimer lors de l'accès à l'interface de visualisation Node.js.
Un contrôle d'accès doit donc être défini sur l'API.

Les données étant relevés par l'objet connecté puis envoyé l'API, ces données ne doivent ni n'être modifiés, supprimés et crée manuellement par l'utilisateur.
De plus ces données ne doivent seulement être lus par un groupe de personnel de la section Coronavirus ainsi que certains médecins en charge des patients en question.
La fonction **acl** issue de la librairie express-acl permet de configurer les contrôles d'accès sur des ressources spécifiques. [75]
La propriété group permet de définir le groupe qui aura des droits. Le groupe Covid correspond aux utilisateurs du groupe en charge de la section COVID.
Ressource permet d'indiquer la route dans laquelle le groupe aura des droits.
Methods correspond au type de droit entre POST, GET et PUT, dans notre cas le groupe Covid aura seulement le droit de lecture GET.

Pour finir nous établissons une règle d'interdiction pour le reste des utilisateurs afin qu'ils n'aient pas accès aux données des patients.

```
[
  {
    "group": "covid",
    "permissions": [
      {
        "resource": "temperature/*",
        "methods": ["GET"],
        "action": "allow"
      }
    ]
  }
{
    "group": "*",
    "permissions": [
      {
        "resource": "*",
        "methods": "*"
      }
    ],
    "action": "deny"
  },]
```

Résultat

Le capteur de température TMP117 est donc relié à l'ESP32 par 6 pin, Le Serial Clock (SCL), SDA (Serial Data), V+ pour l'alimentation, ALERT pour l'utilisation de la fonctionnalité d'alerte, GND et ADD0.
Les pin SDA et Alert doivent être mis en place avec des résistances de rappel, comme il est montré sur la table 6.
Afin de pouvoir ensuite, capter la température puis les envoyer sur la plateforme, un programme doit être mis en place sur la plateforme Arduino, le programme complet est également disponible sur la Table 7.
Le programme va tout d'abord initialiser les PIN du TMP 117 (Figure 17) puis initialiser la WIFI.
La fonction Alerte du capteur étant programmé, nous pouvons définir le seuil d'alerte, qui est de moins de 20°C pour une température trop faible et plus de 38°C pour une température élevée.

Une fois connecté au réseau Wifi défini, le programme va récupérer le Chip ID de l'ESP32 et va mesurer la température.

En cas de température anormale, la variable Flag, étant en Booléen, va avoir la valeur True.

Une fois la température prise, une requête HTTP POST avec toutes les données recueillis :

https://cloud.hospital/temperature/post"?id="chipid + "&temperature="temp + "&alert="alert_flag ;

Le mode de conversion défini dans le programme étant : ONE SHOT, c'est-à-dire une seule prise, les données ne seront envoyés qu'une fois.

Une fois les données envoyées sur la plateforme Node.js, les données seront traitées puis mis dans la base de données, comme expliqué précédemment, avec un comparatif de l'ID Patient avec le CHIP ID.

DEVICE TWO-WIRE ADDRESS	ADD0 PIN CONNECTION
1001000x	Ground
1001001x	V+
1001010x	SDA
1001011x	SCL

FIGURE 17 ADRESSES BINAIRES DES PIN

Annexe

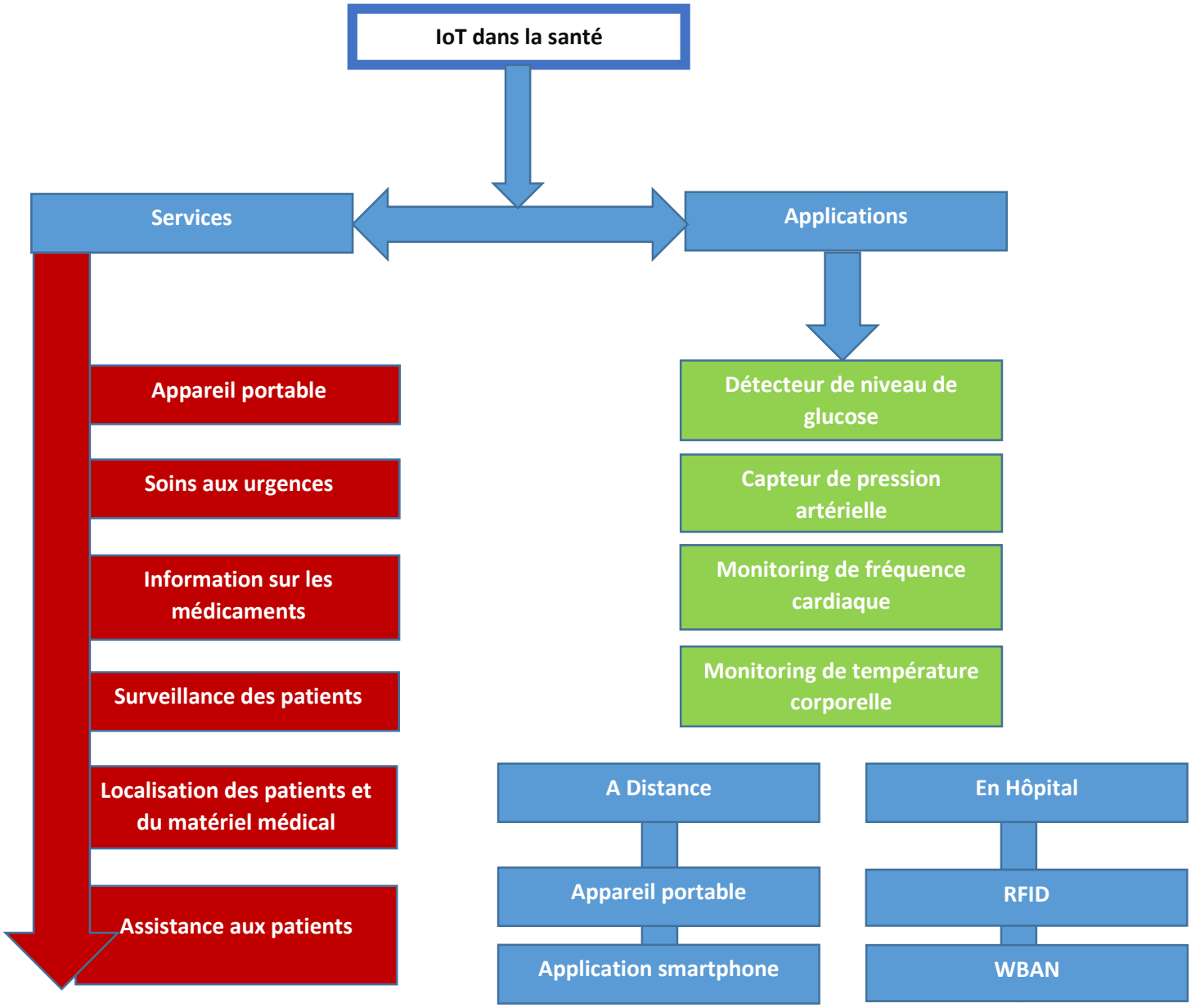


TABLE 1: SERVICES ET APPLICATIONS DE L'IOT DANS UN USAGE MEDICAL

Type d'attaque	Attaque	Description
Cloud	Denial of service	L'attaque par déni de service a pour but d'endommager le réseau entier et le rendre inaccessible aux utilisateurs. L'attaquant va envoyer des paquets en même temps au réseau ce qui va le ralentir et empêcher les capteurs d'entrer en mode veille, ce qui va réduire drastiquement la batterie.
Appareil	Worm hole	Un ou plusieurs nœuds attaquants pouvant communiquer entre eux via un tunnel, permettent d'intercepter, capturer les paquets pour ensuite les envoyer à un autre nœud dans le tunnel [51]
Appareil	Sybil Attack	La Sybil Attack est une méthode consistant à créer des faux nœuds, identités afin de compromettre le système. Le système peut générer des spams et pour d'autres utilisateurs et donc peut permettre de perdre leurs confidentialités. [52]
Appareil	Hello Flood	Le principe de cette attaque est d'utiliser des appareils se faisant passer pour des capteurs authentiques dans le réseau. A travers ces faux capteurs, ceux-ci vont inonder le réseau avec des requêtes Hello afin de réduire la sécurité dans le réseau. [36]
Appareil	Sinkhole	Attaque redirigeant les paquets destinés à un receveur légitime vers un nœud attaquant permettant ainsi de capturer les données. [53]
Communication	Man In the Middle	Attaque consistant à se faire passer pour une entité lors d'un échange entre deux entités. Il permet de l'écoute des données ou la manipulation de ces données en se faisant passer pour l'envoyeur
Communication	Brouillage par fréquence radio	Attaque consistant à brouiller un signal radio par la transmission d'une ou plusieurs signaux radios sur les mêmes fréquences. [54]

TABLE 2 TYPE D'ATTAQUE POUVANT ETRE OPERE SUR UN OBJET CONNECTE

Type de capteur	Thermistance	RTD	Thermocouple	Semi-Conducteur
Plage de température	**-100 à 325°C**	**-200 à 650°C**	**200 à 1750°C**	**-55 à 150°C**
Précision	**0.05 à 1.5°C**	**0.1 à 1°C**	**0.5 à 5°C**	**0.1 à 3°C**
Linéarité	**Exponentielle**	**Assez linéaire**	**Non Linéaire**	**Linéaire**
Sensibilité au bruit électrique	**Rarement sensible7**	**Rarement sensible**	**Sensible**	**Relativement insensible**
Prix	**Faible à modéré**	**Elevé**	**Faible**	**Faible**

TABLE 3 COMPARATIF DES CAPTEURS DE TEMPERATURE A USAGE MEDICAL

MCU	ESP32	AVR	STM32	SAMD21
Nom référence exact	ESP32-D0WDQ6-V3	ATMEGA32U4	STM32F205	ATSAMD21G18
Architecture	XTENSA LX6	AVR 8bit	ARM Cortex M4	ARM M0
Coremark	991	Inconnu	398	118
Prix	1,40€	3,58€	8€	2,80€
Communication	Wifi 802.11, Bluetooth v4.2	Module externe	Module externe	Module externe
Puissance CPU	Dual Core 32bits 240MHz	16 Mhz	32Bits 120MHz	48 Mhz
Mémoire flash	4MB	32 KB	1MB	256KB
RAM	520KB	2.5 KB	128KB	32KB
Sécurité	Cryptographie: AES, SHA-2, RSA	Pas de sécurité dans Le MCU	AES 128, 192, 256, DES, MD5, SHA-1	Pas de sécurité
Consommation Active	210mA	10mA	49mA à 120MHz 26mA à 60MHz	6.8 mA
Consommation en veille	Modern Sleep :20mA-68mA Light Sleep :0.8mA Deep Sleep :100uA Hibernation:5uA	Idle: 6mA ADC Noise Reduction Power-save Power-down Standby Extended Standby	Sleep Mode : 38mA Stop Mode :0.50mA Standby Mode:4µA	IDLE0: 2.2 mA IDLE1: 1.58 mA IDLE2: 1.28 mA Standby XOSC32K + RTC running = 12.8 µA Standby XOSC32K + RTC stopped: 12.2 µA

Programmation	C, C++ (Arduino)	C, C++ (Arduino)	C, C++ (Arduino)	C, C++ (Arduino)

TABLE 4 COMPARATIF DES MICROCONTROLEURS

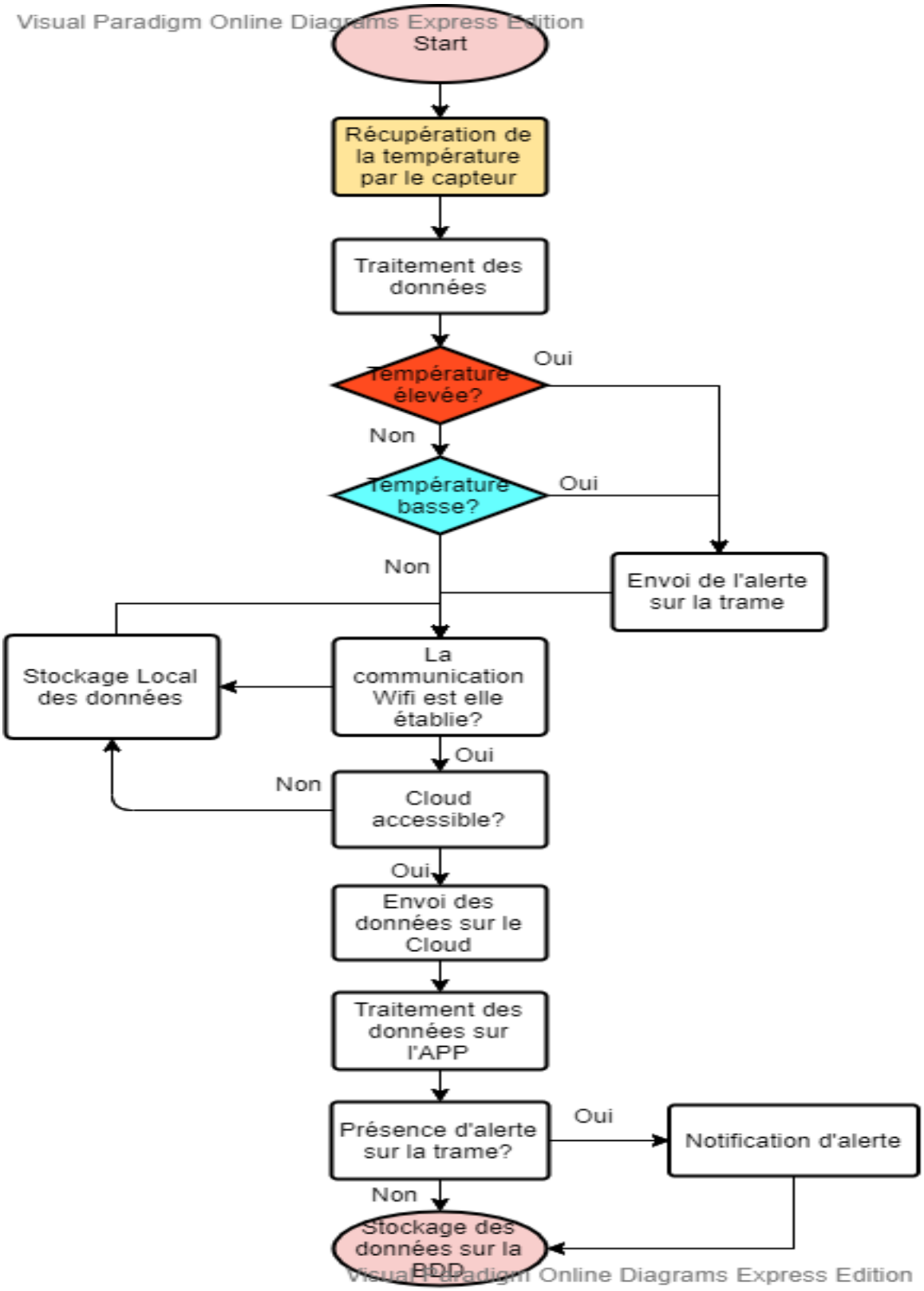


TABLE 5 DIAGRAMME DE FONCTIONNEMENT DE L'OBJET

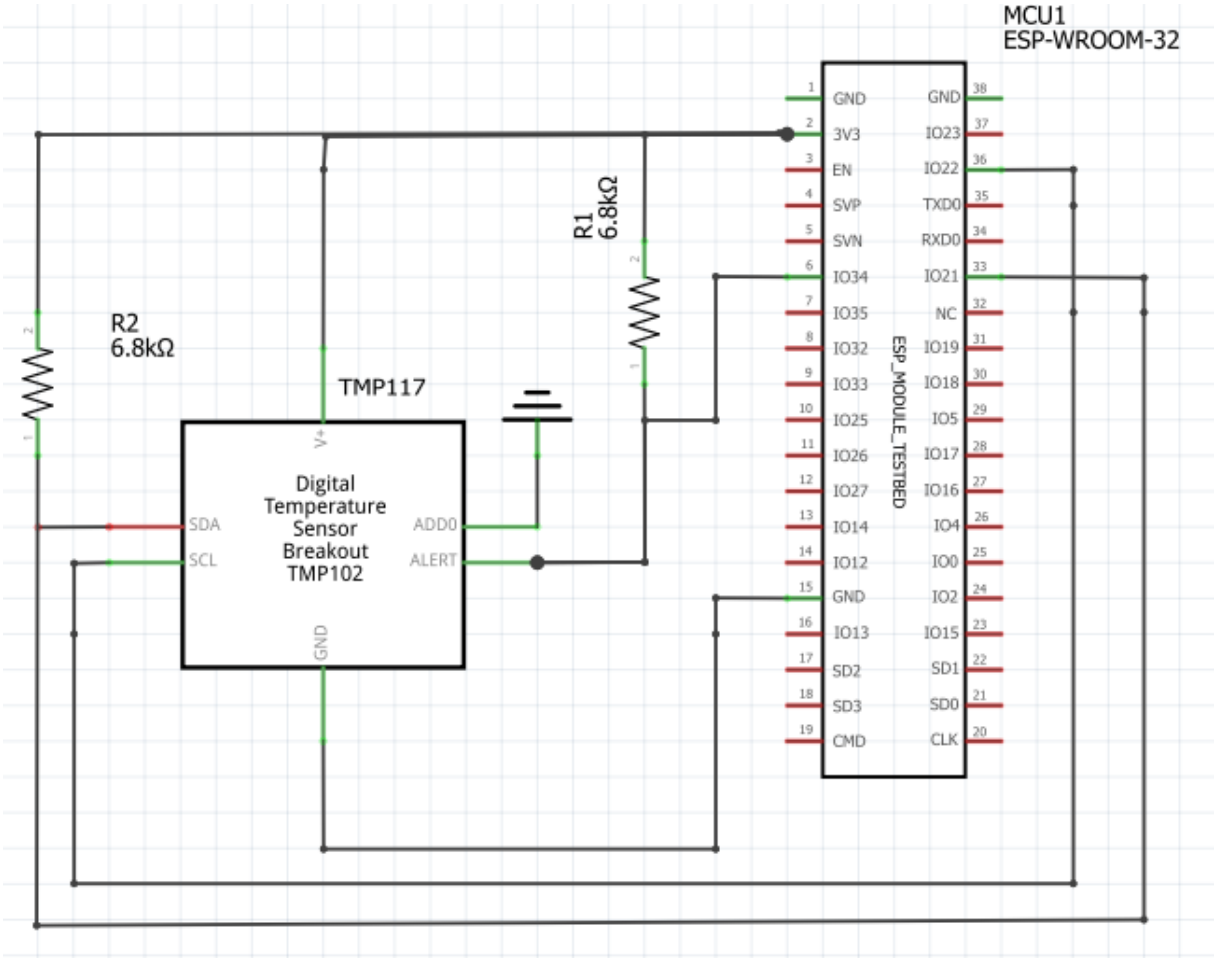


TABLE 6 VUE SCHEMATIQUE DE LA CONNECTIVITE

```
#INCLUDE "WIFI.H" // LIBRAIRIE POUR L'UTILISATION DU WIFI
#INCLUDE "TMP117.H" //LIBRAIRIE DU CAPTEUR DE TEMP
#INCLUDE <HTTPCLIENT.H> //LIBRAIRIE POUR REQUETES HTTP
 CONST CHAR* SSID="WIFI_HOPITAL";
 CONST CHAR* PASSWORD="12345678";
 STRING SERVERNAME = "HTTPS://CLOUD.HOSPITAL/TEMPERATURE/POST"; //DEFINITION DU SERVEUR NODE.JS POUR LE POST
UINT8_T ADDR_GND =  0X48;  // 1001000 //CONNEXION PIN
UINT8_T ADDR_VCC =  0X49;  // 1001001
UINT8_T ADDR_SDA =  0X4A;  // 1001010
UINT8_T ADDR_SCL =  0X4B;  // 1001011
UINT8_T ADDR =  ADDR_GND;
UINT64_T CHIPID;


#DEFINE ALERT_PIN          10   // LOW ACTIVE ALERT PIN
```

```
#define LOW_TEMPERATURE_ALERT  20   // Alerte temp faible 20°C
#define HIGH_TEMPERATURE_ALERT  38   // Alerte temp elevee 38°C
bool alert_flag = false;
TMP117 tmp(ADDR);

Void setup() {
Wire.begin();
Serial.begin(11520) ;
tmp.init ( new_temperature );    // set callback function. will be called if there is new sensor data
tmp.setConvMode (ONESHOT);      //MESURE SUR UNE PRISE SEULEMENT

tmp.init ( new_temperature );
tmp.setConvTime (C15mS5);       // 1. setup C125mS+NOAVE = 15.5 mS measurement time
tmp.setAveraging (NOAVE);

tmp.setAlertMode(ALERT);        // Activation de la fonction alerte
tmp.setAllertCallback ( temperature_allert, ALERT_PIN );
tmp.setAllertTemperature (LOW_TEMPERATURE_ALERT, HIGH_TEMPERATURE_ALERT);

Serial.println("") ;
 WiFi.mode(WIFI_STA) ; // Configurer en Station WiFi
WiFi.begin(ssid,password); // Demande de connexion au reseau WiFi
 while(WiFi.status() != WL_CONNECTED)
 {
 Serial.println("Tentative de connexion...") ;
  delay(1000);
 }
Serial.println("Connecte au reseau WiFi !");
 }
}

void loop() {
 chipid=ESP.getEfuseMac(); //Recuperation du Chipid de l'esp

 tmp.update();
```

```
// SI LA TEMPERATURE EST ANORMALEMENT FAIBLE OU ELEVE


 IF (ALERT_FLAG) {
  IF (TMP.GETALERTTYPE () == HIGHALERT) {
  SERIAL.PRINT("HIGH TEMPERATURE ALLERT : ");
  SERIAL.PRINT (TMP.GETTEMPERATURE());
  SERIAL.PRINTLN (" °C");
  }
  ELSE IF (TMP.GETALERTTYPE () == LOWALERT) {
   SERIAL.PRINT("LOW TEMPERATURE ALLERT : ");
   SERIAL.PRINT (TMP.GETTEMPERATURE());
   SERIAL.PRINTLN (" °C");
   SERVER
  }
  ELSE {
   ALERT_FLAG = FALSE;
  }
 }



// PRISE DE TEMPERATURE
VOID NEW_TEMPERATURE ( VOID ) {
 IF (!ALERT_FLAG) {
  SERIAL.PRINT ("TEMPERATURE : ");
  FLOAT TEMP = TMP.GETTEMPERATURE()
  SERIAL.PRINT (TEMP);
  SERIAL.PRINTLN (" °C");


  IF(WIFI.STATUS()== WL_CONNECTED){
  HTTPCLIENT HTTP;
 STRING SERVERPATH = SERVERNAME + "?ID="CHIPID + "&TEMPERATURE="TEMP + "&ALERT="ALERT_FLAG;
 HTTP.BEGIN(SERVERNAME);
 INT HTTPRESPONSECODE = HTTP.POST(SERVERPATH); //REQUETE POST
```

```
  SERIAL.PRINT("HTTP RESPONSE CODE: ");
    SERIAL.PRINTLN(HTTPRESPONSECODE);
    HTTP.END();

}

 }
}
// FONCTION DE RAPPEL LORSQU'UNE ALERTE DE TEMPERATURE SE PRODUIT
VOID TEMPERATURE_ALERT (VOID) {
 ALERT_FLAG = TRUE;
}
}
```

TABLE 7 PROGRAMMATION SUR ARDUINO

Abréviation :

IoT : Internet Of Things

API : Application Programming Interface

HIPAA : Health Insurance Portability and Accountability Act

JS : JavaScript

MCU : Microcontrôleur

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.

[31] https://www.businessinsider.com/iot-healthcare?IR=T

[32] https://www.informatiquenews.fr/les-objets-connectes-se-multiplient-les-attaques-encore-plus-64005

[33] Zhang, Rui & Liu, Ling. (2010). Security Models and Requirements for Healthcare Application Clouds. 268-275. 10.1109/CLOUD.2010.62.

[34] Aliyu, Farouq & Sheltami, Tarek & Shakshuki, Elhadi. (2018). A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing. Procedia Computer Science. 141. 24-31. 10.1016/j.procs.2018.10.125.

[35] https://www.leparisien.fr/societe/erreurs-medicales-il-faut-faire-tomber-l-omerta-23-11-2017-7409418.php

[36] Dang, L. Minh & Min, Kyungbok & Han, Dongil & Jalil Piran, Md & Moon, Hyeonjoon. (2019). A Survey on Internet of Things and Cloud Computing for Healthcare. 8. 10.3390/electronics8070768.

[37] Karagiannis, Vasileios & Chatzimisios, Periklis & Vázquez-Gallego, Francisco & Alonso-Zarate, J.. (2015). A survey on application layer protocols for the Internet of Things. Trans. IoT Cloud Comput.. 3. 11-17.

[38] Castellani, Angelo & Gheda, Mattia & Bui, Nicola & Rossi, Michele & Zorzi, Michele. (2011). Web services for the Internet of Things through CoAP and EXI. 1 - 6. 10.1109/iccw.2011.5963563.

[40] Sye Loong Keoh, Sandeep S. Kumar, Hannes Tschofenig, Securing the Internet of Things: A Standardization Perspective, Internet of Things Journal IEEE (Volume: 1, Issue: 3), June 2014, pp. 265-275.

[41] "IoT Privacy , Data Protection , Information Security." .

[42] In Hudson, F. D. (2019). Women Securing the Future with TIPPSS for IoT: Trust, Identity, Privacy, Protection, Safety, Security for the Internet of Things

[43] https://cloud.google.com/security/compliance/hipaa?hl=fr

[44] Wachter, Sandra. (2017). Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. Computer Law & Security Report. 34. 436-449. 10.2139/ssrn.3083554.

[45] Charith Perera and Ciaran McCormick and Arosha K. Bandara and Blaine A. Price and Bashar Nuseibeh, "Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms" 2016

[46] Joyia, Gulraiz & Liaqat, Rao & Farooq, Aftab & Rehman, Saad. (2017). Internet of medical things (IOMT): Applications, benefits and future challenges in healthcare domain. Journal of Communications. 12. 240-247. 10.12720/jcm.12.4.240-247.

[47] https://openaps.org/

[48] https://www.objetconnecte.com/sigfox-iot-lutte-covid19/

[49] https://www.who.int/fr/emergencies/diseases/novel-coronavirus-2019/advice-for-public/q-a-coronaviruses

[50] Singh, R. P., Javaid, M., Haleem, A., & Suman, R. (2020). Internet of things (IoT) applications to fight against COVID-19 pandemic. *Diabetes & metabolic syndrome*, *14*(4), 521–524. Advance online publication. https://doi.org/10.1016/j.dsx.2020.04.041

[51] https://productcoalition.com/five-covid-19-critical-use-cases-iot-healthcare-companies-must-focus-e5dc21a12187

[51] Palacharla, Swetha & Chandan, Madhavarapu & Gnanasuryateja, K & Varshitha, G. (2018). Wormhole Attack: a Major Security Concern in Internet of Things (Iot).

[52] Sushama Pawar, Pankaj Vanwari, "Sybil Attack in Internet of Things"

[53] Cervantes, Christian & Poplade, Diego & Nogueira, Michele & Santos, Aldri. (2015). Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of

Things. Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015. 606-611. 10.1109/INM.2015.7140344.

[54] Namvar, Nima & Saad, Walid & Bahadori, Niloofar & Kelley, Brian. (2016). Jamming in the Internet of Things: A Game-Theoretic Perspective. 1-6. 10.1109/GLOCOM.2016.7841922.

[55] https://www.gouvernement.fr/info-coronavirus/comprendre-le-covid-19

[56] https://www.digikey.fr/fr/articles/effectively-sense-temperature-iot-applications--solid-state-technology

[57] https://www.ti.com/lit/gpn/lmt70

[58] http://www.ti.com/lit/gpn/tmp117

[59] https://www.maximintegrated.com/en/products/interface/sensor-interface/MAX30205.html

[60] http://www.electronique-mag.com/article14411.html

[61] Maier, Alexander & Sharp, Andrew & Vagapov, Yuriy. (2017). Comparative Analysis and Practical Implementation of the ESP32 Microcontroller Module for the Internet of Things. 10.1109/ITECHA.2017.8101926.

[62] https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf

[63] http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-7766-8-bit-AVR-ATmega16U4-32U4_Datasheet.pdf

[64] https://www.st.com/resource/en/datasheet/stm32f205rb.pdf

[65]http://ww1.microchip.com/downloads/en/DeviceDoc/SAM_D21_DA1_Family_DataSheet_DS40001882F.pdf

[66] Ahmed, I., Karvonen, H., Kumpuniemi, T. *et al.* Wireless Communications for the Hospital of the Future: Requirements, Challenges and Solutions. *Int J Wireless Inf Networks* **27,** 4–17 (2020). https://doi.org/10.1007/s10776-019-00468-1

[67] https://fr.slideshare.net/JordanEller1/radio-frequencies-for-iot-94888372

[68] Alharbe, N. & Atkins, Anthony & Sheikh Akbari, Akbar. (2013). Application of ZigBee and RFID Technologies in Healthcare in Conjunction with the Internet of Things. 10.1145/2536853.2536904.

[69] M. Clarke, J. de Folter, V. Verma and H. Gokalp, "Interoperable End-to-End Remote Patient Monitoring Platform Based on IEEE 11073 PHD and ZigBee Health Care Profile," in IEEE Transactions on Biomedical Engineering, vol. 65, no. 5, pp. 1014-1025, May 2018, doi: 10.1109/TBME.2017.2732501.

[70] https://blog.domadoo.fr/guides/principe-du-protocole-zigbee/

[71] A Sikora, V.F. Groza. “Coexistence of IEEE802.15.4 with other Systems in the 2.4 GHz-ISM-Band”. Instrumentation and Measurement Technology Conference, 2005. IMTC 2005. Proceedings of the IEEE 16-19 May 2005 Volume: 3, On page(s): 1786- 1791

[72] https://blog.engineering.publicissapient.fr/2018/04/16/internet-des-objets-quels-protocoles-applicatifs-utiliser-1-2/

[73] https://www.digitaljunky.io/make-your-own-data-platform-for-the-internet-of-things-using-node-js-and-express-js/

[74] https://medium.com/@keleko34/esp32-tls-connection-to-node-js-9fa796fbcd32

[75] https://www.npmjs.com/package/express-acl

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

[77] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[78] https://www.arubanetworks.com/assets/infographic/Aruba_IoT_Healthcare_Infographic.pdf

[79] https://buzz-esante.fr/le-sante-vue-par-les-patients/

[80] https://donnees.banquemondiale.org/indicateur/SP.POP.65UP.TO.ZS?end=2018&start=2010

[81] http://ijiet.com/wp-content/uploads/2016/09/67.pdf