

الجمهورية الجزائرية الديمقراطية
الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد – تلمسان

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE



MEMOIRE

Présenté pour l'obtention du **diplôme de MASTER**

En : Télécommunications

Spécialité : Systèmes des Télécommunications

Par : MEDJADJI ABDELMOUNAIM

Sujet

Développement d'une application mobile en utilisant un modèle IoT pour l'automatisation d'un site intelligent

Soutenu publiquement, le 18/09/2018, devant le jury composé de :

M. MERZOUGUI Rachid	MCA	Univ. Tlemcen	Président
M. MOUSSAOUI Djilali	MAA	Univ. Tlemcen	Examineur
M. HADJILA Mourad	MCB	Univ. Tlemcen	Directeur de mémoire

Remerciements

Je tiens tout d'abord à remercier ALLAH le tout puissant et miséricordieux, qui m'a donné la force et la patience d'accomplir ce modeste travail.

En second lieu, je tiens à remercier sincèrement Monsieur M.Hadjila, qui, en tant que Directeur de mémoire, s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'il a bien voulu me consacrer et sans sa contribution ce mémoire n'aurait jamais vu le jour.

Mes vifs remerciements vont également aux membres du jury composé de Messieurs R.Merzougui et D.Moussaoui pour l'intérêt qu'ils ont porté à ma recherche en acceptant d'examiner mon travail et de l'enrichir par leurs propositions.

J'adresse mes sincères remerciements à mes parents. Si je suis ici aujourd'hui, c'est grâce à eux.

Enfin, j'adresse mes plus sincères remerciements à tous mes proches et amis qui m'ont toujours encouragé au cours de la réalisation de ce mémoire.

Merci à toutes et à tous.

Résumé

Le développement des technologies de l'information et de la communication génère de plus en plus des objets qui deviennent embarqués avec des capteurs capables de communiquer avec d'autres objets, transformant ainsi le monde physique en un système d'information et de savoir. L'Internet des objets permet aux objets dans notre environnement d'être active, i.e., ils partagent l'information avec autre objets ou membre du réseau, en utilisant le même protocole qui connecte l'Internet, l'IP. Le but de ce projet est de valoriser l'importance d'Internet des Objets dans notre vie quotidienne en tant que technologie prometteuse ; il y avait deux parties principales dans ce mémoire. Une partie était de construire un circuit électronique qui ferait fonctionner une maison intelligente. On a commencé par introduire brièvement la plupart des composants matériels utilisés, puis on a décrit les schémas des circuits électroniques en montrant leurs connections.

L'autre partie consistait à développer une application servant à contrôler le matériel et exécuter certaines opérations demandées par l'utilisateur. Cette application a été développée pour le client. Le client a été implémenté en utilisant le niveau standard d'API Android. Le back-end du logiciel client a été initialement développé avec le langage Java Standard Edition avant de le porter sur la plate-forme Android.

Mots clés : Internet des Objets (IdO), Capteur, Actionneur, ESP8266, Android, Java.

Abstract

The development of information and communication technologies increasingly generates objects that become embedded with sensors and able to communicate with other objects, thus transforming the physical world into a system of information and knowledge. The Internet of Things allows objects in our environment to be active, i.e., they share information with other objects or network members, using the same protocol that connects the internet, the IP. The purpose of this project is to highlight the importance of the Internet of Things in our daily lives as a promising technology; there were two main parts in this memoir. Part of it was to build an electronic circuit that would run a smart home. We started by briefly introducing most of the hardware components used, then we described the diagrams of the electronic circuits showing their connections.

The other part was to develop software that would control the hardware and perform certain operations requested by the user; this software was developed for the client. The client was implemented using the standard level of Android API. The client software back-end was initially developed with the Java Standard Edition language before bringing it to the Android platform.

Keywords : Internet of Things (IoT), Sensor, Actuator, ESP8266, Android, Java.

Table des matières

Résumé	i
Introduction générale.....	1
Chapitre I : Introduction à l’Internet des Objets	
I.1. Introduction	2
I.2. Type d’objet	6
I.2.1. Capteur et Actionneur	6
I.2.2. L’importance de la précision des capteurs	8
I.3. Applications d’IoT.....	9
I.4. Applications adaptatives.....	14
I.5. Illustrer le concept d'intégration de machine à machine (M2M)	14
I.6. Les Applications M2M	16
I.6.1. Energie Intelligente (Smart Energy)	16
I.6.2. Médecine Intelligente (Smart Health Care)	16
I.6.3. Domotique (Smart Home Security)	16
I.6.4. Manutention intelligente (smart cargo handling)	17
I.6.5. Smart traffic Management.....	17
I.6.6. Smart Inventory and Replenishment Management	17
I.6.7. Smart Cash Payment.....	17
I.6.8. Smart Tracking	18
I.6.9. Smart Displays.....	18
I.6.10. Smart Manufacturing.....	18
I.6.11. Smart Asset Management	19
I.6.12. Smart Retailing	19
I.6.13. Agriculture intelligente	20
I.7. IoT Vision	21
I.8. Les défis de sécurité et de confidentialité concernant l'utilisation des smartphones dans les réseaux IoT et IoE.....	21
I.9. Conclusion.	23

Chapitre II : Protocoles et technologies de communication

II.1. Introduction	24
II.2. Structure de l'IdO	24
II.3. IoT technologies	24
II.3.1. Radio-frequency identification (RFID)	24
II.3.2. Electronic product code (EPC)	25
II.3.3. Barcode.....	25
II.3.4. Internet protocol (IP)	26
II.3.5. Wireless Fidelity (Wi-Fi)	26
II.3.6. Bluetooth	26
II.3.7. ZigBee	27
II.3.8. Near-Field communication (NFC)	27
II.3.9. Wireless Sensor Networks (WSNs)	27
II.3.10. Artificial intelligence (AI)	28
II.4. IoT architecture.....	28
II.5. Aperçu de la communication internet.....	29
II.5.1. Protocole IP.....	29
II.5.2. TCP	30
II.5.3. Protocole TCP/IP SUITE.....	30
II.5.4. Protocole UDP.....	30
II.6. IP ADDRESSES.....	32
II.6.1. Adresse IP statique	33
II.6.2. DYNAMIC IP ADDRESS ASSIGNMENT	34
II.7. DNS.....	35
II.8. Adresse MAC.....	36
II.9. Protocole http.....	37
II.10. Push Versus Pull	41
II.11. Conclusion	42

Chapitre III : Description matérielle et logicielle de l'application IoT intelligente

III.1. Introduction	43
III.2. Spécifications des besoins.....	43
III.2.1. Besoins fonctionnels.....	43
III.2.2. Besoins non fonctionnels	44
III.3. Architecture globale du système	44

III.3.1. Partie Utilisateur	45
III.3.2. Partie Matérielle.....	45
III.3.2.1.le node MCU N°1	45
III.3.2.2. le node MCU N°2	45
III.3.2.3. le node MCU N°3	45
III.3.3. Parite Cloud.....	46
III.4. Diagramme des cas d'utilisation.....	46
III.4.1. Les exploiters	46
III.4.2. les cas d'utilisation	46
III.5. Fonctionnement du système.....	48
III.6. Moyens utilisés	48
III.6.1. Partie Hardware	48
III.6.1.1. Définition du module ESP8266-12E (Node MCU v1.0)	49
III.6.1.2. Correspondance des broches entre Arduino et ESP8266 (NodeMCU)	49
III.6.1.3. Librairies ESP8266Wifi	49
III.6.1.4. En Lua (NodeMCU)	50
III.6.1.5. Description de fonctionnement des capteurs et actionneurs	50
III.6.1.5.1. Capteur de température et d'humidité : DHT	50
III.6.1.5.2. Capteur de gaz MQ-2	52
III.6.1.5.3. Capteur de Flamme	53
III.6.1.5.3. Capteur d'humidité du sol	53
III.6.1.5.4. Servomoteur	54
III.6.1.5.5. Relais	54
III.6.1.5.6. Photorésistance LDR	54
III.6.2. Partie Software.....	55
III.6.2.1. Arduino IDE	55
III.6.2.1.1. Structure du programme Arduino.....	56
III.6.2.2. ANDROID.....	56
III.6.2.2.1. Présentation de l'interface	57
III.6.2.2.1.1. Interface des actionneurs	57
III.6.2.2.1.2. Interface des capteurs	58
III.7. Conclusion	58
Conclusion générale	59
Bibliographie	60

Liste des figures

Figure I.1: Internet connected (source: cisco).....	4
Figure I.2. Prolifération de dispositifs et applications dans l'Internet des Objets (IoT)	5
Figure I.3 : exemple d'IoT – système de Capteur vers actionneur	7
Figure I.4 : les domaines de l'IoT.....	12
Figure I.5 : les Technologie de communication de l'Iot.....	13
.....	
Figure II.1 : Structure de l'IoT	24
Figure II.2: IoT Architecture (Source: ITU-T)	28
Figure II.3 : TCP/IP Protocol Suite.....	31
Figure II.4: Client send request message, server answer with response	37
.....	
Figure III.1 Architecture globale du système.....	44
Figure III.2 : Diagramme d'utilisateur	47
Figure III.3 : Diagramme d'utilisation de développeur	47
Figure III.4 : Fonctionnement du système.....	48
Figure III.5 : Module ESP8266-12E	49
Figure III.6 : Branchement ESP8266-12E/DHT.....	52
Figure III.7 : Branchement ESP8266-12E/MQ-2	52
Figure III.8 : Branchement ESP8266-12E/Capteur de flamme	53
Figure III.9 : Branchement ESP8266-12E/Humidité du sol	53
Figure III.10 : Branchement ESP8266-12E/LDR	55
Figure III.11 : Description de l'interface Arduino IDE	56
Figure III.12 : Interface d'actionneur.....	57
Figure III.13 : Interface des capteurs.....	58

Liste des abréviations

RFID: Radio-Frequency **I**dentification.

IoT: Internet **of** Thing.

IdO: Internet **des** Objets.

API : Application **P**rogramming **I**nterface

Java **SE :** Standard Edition.

IP : Internet **P**rotocol

Introduction générale

Introduction Générale

L'Internet des objets a pour but de concrétiser la vision informatique ubiquitaire comme Mark Weiser avais imaginé en 1991, où cette technologie soit intégrée et synchronisée avec l'environnement quotidien des utilisateurs. Dans les objets qui nous entourent, cette technologie sera représentée non seulement par un objet unique, mais par tout ce qui entoure l'utilisateur, i.e. Smartphones, smart TV, montres connectées, maisons intelligentes, etc.

Ce terme IoT (Internet of Things) a été utilisé/mentionné en 1999 pour la première fois par Kevin Ashton, en décrivant des objets équipés de puces d'identification par radiofréquence (puce RFID). Donc, c'était l'initialisation de cette idée d' "Objets", un monde de technologie à détection de ce qui entoure.

Ce sujet a été choisi parce qu'un tel projet couvre plus ou moins les compétences d'un étudiant gradué dans le domaine des technologies de l'information et de communication. De plus, les technologies utilisées tout au long du projet étaient également assez récentes.

Le but de ce projet de fin d'études est de valoriser l'importance d'Internet des Objets dans notre vie quotidienne en tant que technologie prometteuse. Il s'agit du développement d'une application mobile en utilisant un modèle IoT pour l'automatisation d'un site intelligent. Ce mémoire contient deux parties principales. Une première partie consiste à construire un circuit électronique qui ferait fonctionner le site intelligent. On a introduit brièvement la plupart des composants matériels utilisés suivis par des schémas décrivant leurs connections.

L'autre partie consiste à développer une application servant à contrôler le matériel et exécuter certaines opérations demandées par l'utilisateur. Cette application a été développée en utilisant le niveau standard d'API Android. Le back-end du logiciel client a été initialement développé avec le langage Java SE avant de le porter sur la plate-forme Android. Certaines parties du projet ont nécessité des études supplémentaires pour faire le travail. Une plus grande importance du travail était sur la partie de développement de logiciel du projet.

Ce mémoire est organisé dans un document comportant trois chapitres :

Dans le premier chapitre intitulé « Introduction à l'Internet des Objet », nous présentons une vue générale sur l'Internet des Objets (IoT). Dans un premier temps, nous décrivons brièvement le concept de l'IoT, ainsi que leurs domaines d'applications et leur importance dans la vie quotidienne.

Une description générale des différents protocoles ainsi que les différentes technologies de communications utilisées font l'objet du deuxième chapitre.

Le troisième chapitre est consacré à la commande de notre site intelligent via une application mobile. Nous décrivons les parties matérielles et logicielles requises pour la conception finale du notre projet. Ensuite, nous expliquons toutes les étapes pour le réaliser.

Nous finalisons notre mémoire par une conclusion générale où nous résumons le travail proposé suivi par quelques directions de recherche possibles visant des perspectives à être étudiées.

Chapitre I

Introduction à l'Internet des objets

I.1. Introduction [1]

L'Internet des objets, également connu sous le nom d'IoT, est un terme composé de deux mots : le premier mot "Internet", qui est "un réseau de réseaux et un système global de réseaux informatiques interconnectés utilisant TCP / IP comme Internet standard", protocole (IP) pour connecter des millions d'utilisateurs et de multiples réseaux privés, publics, universitaires, commerciaux et gouvernementaux ». Le deuxième mot «Choses» se compose de n'importe quel objet du monde réel tel que des appareils ménagers, des vêtements, etc. ou des êtres vivants tels que des plantes, des animaux et des personnes. Le terme «Internet of Things» a été inventé par Kevin Ashton, directeur exécutif du Centre Auto-ID au MIT, en 1999 et sa définition variait parmi les académiciens et les chercheurs. La meilleure définition de IoT serait : "Un réseau ouvert et complet d'objets intelligents qui ont la capacité d'auto-organiser, partager des informations, des données et des ressources, réagir et agir face aux situations et aux changements dans l'environnement". L'IoT vise à fournir la vision de «permettre une connectivité à tout moment et n'importe où pour n'importe quoi et pas seulement en fournissant une identité unique à chaque objet». Dans les réseaux IoT déployés, des capteurs sont attachés à des objets physiques et gardent une trace de leurs données, pour permettre leur suivi sur Internet.

Les prochaines années nous réservent d'autres surprises en raison de l'émergence de l'IdO. Votre téléphone mobile et votre ordinateur sont déjà connectés à Internet, peut-être même le GPS de votre véhicule. Dans les années à venir, votre voiture, votre bureau, votre domicile et tous les appareils électroménagers qu'ils contiennent, y compris les compteurs d'électricité, de gaz et d'eau, l'éclairage public, le système d'arrosage automatique, les pèse-personnes, les tensiomètres et même les murs seront connectés à l'IdO. Demain, les appareils électroménagers profiteront de nombreuses améliorations. Par exemple, le chauffage ne sera pas déclenché si la météo prévoit des températures clémentes mais sera déclenché plus tôt que prévu si le vent permet d'accéder à de l'énergie propre à ce moment, le jardin ne sera arrosé automatiquement

que s'il ne pleut pas, une assistance routière sera apportée immédiatement en cas de besoin, etc. Ces améliorations faciliteront nos vies et permettront une utilisation plus efficace des ressources naturelles. [2]

S'appuyant sur un réseau complexe reliant des milliards d'appareils et d'humains dans une technologie multiple, une infrastructure à multi-protocole et multi-plateforme, l'Internet des Objets, dont la vision principale est de créer un monde intelligent où le monde physique, le monde numérique et le monde virtuel seront converger pour créer des environnements intelligents qui fournissent plus d'intelligence à l'énergie, la santé, les transports, les villes, l'industrie, les bâtiments et bien d'autres domaines de notre vie quotidienne.

Les attentes sont d'interconnexion des millions d'îles de réseaux intelligents permettant l'accès à l'information à n'importe quand et n'importe où mais aussi en utilisant n'importe qui et quoi que ce soit idéalement à travers n'importe quel chemin, réseau et tout service. Cela sera atteint quand les objets qu'en manipulant quotidiennement équipé de détection, d'identification et de dispositifs de positionnement et dotés d'une adresse IP pour devenir des objets intelligents, capables de communiquer avec non seulement d'autres objets intelligents mais aussi avec des humains dans l'attente d'atteindre des domaines que nous ne pourrions jamais atteindre sans les progrès réalisés dans la détection, l'identification et technologies de positionnement.

Tout en étant globalement détectables et interrogés, ces objets intelligents peuvent également découvrir et interagir avec des entités externes en interrogeant des humains, des ordinateurs et d'autres objets intelligents. Les objets intelligents peuvent également obtenir des renseignements en rendant ou en permettant des décisions liées au contexte tirer parti des canaux de communication disponibles pour fournir des informations sur eux-mêmes tout en accédant à des informations qui ont été agrégées par d'autres objets intelligents.

Il est estimé que l'IoT atteindra 50 milliards d'appareils connectés d'ici 2020, lorsque la population mondiale atteindra 7,6 milliards (figure 1.1), et que son impact économique potentiel passera de 3 900 milliards de dollars à 11 100 milliards de dollars par an d'ici 2025 [3]. Dans l'ensemble, l'IoT permettrait l'automatisation de tout ce qui nous entoure. La prolifération des dispositifs et de ses applications est illustrée à la figure I.2.

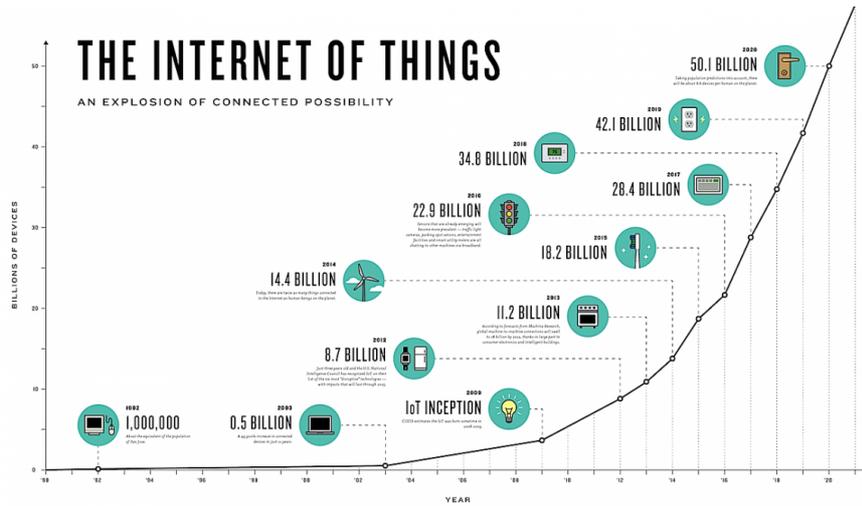


Figure I.1: Internet connected (source: cisco)

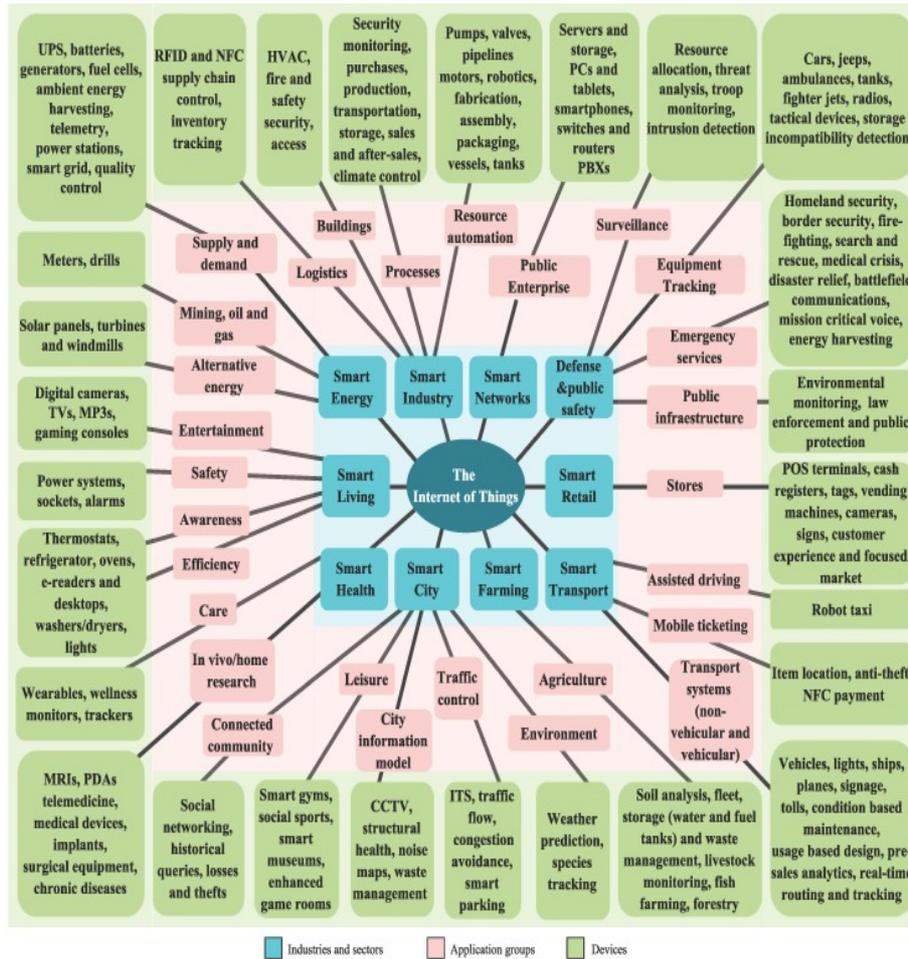


Figure I.2. Prolifération de dispositifs et applications dans l'Internet des Objets (IoT)

Au cours des dernières années, certains documents de recherche axés sur l'évolution des organisations de SP ont été publiés, Certains de ces articles ont un intérêt particulier dans les défis pour faire évoluer l'architecture du réseau LTE vers la 5G afin de supporter les réseaux PS émergents. En ce qui concerne l'IoT, plusieurs articles publiés couvrent différents aspects de la technologie IoT appliquée à la défense et au PS. [3]

L'IoT représente la convergence de plusieurs domaines interdisciplinaires : réseautage, matériel embarqué, spectre radioélectrique, informatique mobile, technologies de communication, architectures logicielles, technologies de détection, efficacité énergétique, gestion de l'information et analyse de données. La croissance rapide de l'IoT est motivée par quatre avancées majeures dans les technologies numériques. Le premier est le coût décroissant et la miniaturisation des

microélectroniques de plus en plus puissantes telles que les transducteurs (capteurs et actionneurs), les unités de traitement (microcontrôleurs, microprocesseurs, SoCs (System-on-a-Chip), FPGA (Field-Programmable Gate Array). Le deuxième facteur est la rapidité et l'expansion de la connectivité sans fil, le troisième est l'expansion du stockage de données et la capacité de traitement des systèmes de calcul, enfin, le quatrième est l'avènement d'applications et d'analyses les progrès dans les techniques d'apprentissage automatique pour le traitement de données volumineuses. Ces quatre facteurs sont présents dans les couches de la pile technologique IoT, par exemple l'IoT peut inclure des transducteurs qui collectent des données sur les conditions physiques et environnementales, réseau de communication vers des serveurs et des ordinateurs qui stockent et traitent des données à l'aide d'applications logicielles et d'analyses peut être utilisé pour la détection, le contrôle, la prédiction, la surveillance et l'optimisation des processus et des systèmes.

I.2. Type d'objet

Chaque objet est équipé d'un capteur ou d'un actionneur, un microprocesseur, une source d'énergie, et un dispositif de communication.

Chaque objet a une fonction : envoyer, recevoir, ou communiquer une information. Dans chaque cas, cet objet a été connecté à internet, ce n'était ni un pc, ni une tablette ou un smart phone, mais un objet. Chaque objet est conçu pour un but spécifique. [4]

Les capteurs peuvent détecter les grandeurs suivantes : température, humidité, lumière, pression, bruit, accélération, l'humidité du sol ...etc. L'idée d'IoT c'est d'avoir un plus grand nombre de périphériques.

Les capteurs et/ou les actionneurs sont ceux qui permettent une interaction avec le monde réel. Ils seront connectés via le protocole utilisé pour l'interconnexion d'internet IP (Internet Protocol). [5]

I.2.1. Capteur et Actionneur [6]

L'Internet des Objets est rarement discuté sans que la conversation soit orientée vers les données et la nouvelle économie de données. L'intelligence et la valeur d'un système IoT sont basées sur ce qui peut être appris à partir des données. Les capteurs sont la source des données d'IoT.

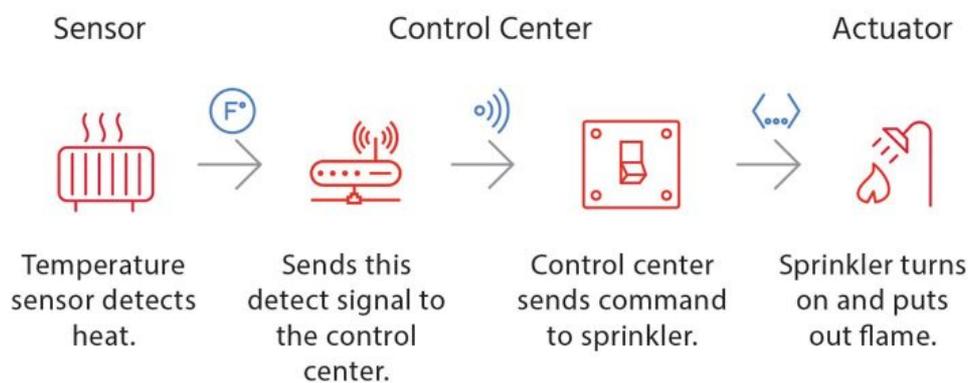
Le capteur a l'habilité d'interagir avec l'environnement e.g. (température, humidité, lumière, etc.) et sauvegarder cette interaction et la transformer en information, dont cette dernière peut être compréhensible à l'humain.

Poussée par de nouvelles innovations dans les matériaux et la nanotechnologie, la technologie des capteurs se développe à un rythme jamais vu, avec une précision accrue, une taille et un coût réduits, et la possibilité de mesurer ou de détecter des choses auparavant impossibles. En fait, la technologie de détection se développe si rapidement et devient si avancée que nous verrons un billion de nouveaux capteurs déployés chaque année dans quelques années.

Un meilleur terme pour un capteur est un transducteur. Un transducteur est un dispositif physique qui convertit une forme d'énergie en une autre. Ainsi, dans le cas d'un capteur, le transducteur convertit un phénomène physique en une impulsion électrique qui peut ensuite être interprétée pour déterminer une lecture. Un microphone est un capteur qui prend l'énergie vibratoire (ondes sonores) et la convertit en énergie électrique d'une manière utile pour que d'autres composants du système corrélent avec le son original.

Un autre type de transducteur que vous rencontrerez dans de nombreux systèmes IoT est un actionneur. En termes simples, un actionneur fonctionne dans le sens inverse d'un capteur. Il prend une entrée électrique et le transforme en action physique. Par exemple, un moteur électrique, un système hydraulique et un système pneumatique sont tous différents types d'actionneurs.

Dans les systèmes IoT typiques, un capteur peut collecter des informations et acheminer vers un centre de contrôle où une décision est prise et une commande correspondante est renvoyée à un actionneur en réponse à cette entrée détectée.



Sensor to **Actuator** Flow

Figure I.3 : exemple d'IoT – système de Capteur vers actionneur

Il existe plusieurs types de capteurs. Les capteurs de débit, les capteurs de température, les capteurs de tension, les capteurs d'humidité et la liste continue. En outre, il existe plusieurs façons de mesurer la même chose. Par exemple, le débit d'air pourrait être mesuré en utilisant une petite hélice comme celle que vous verriez sur une station météo. Alternativement, comme dans un véhicule mesurant l'air à travers le moteur, le débit d'air est mesuré en chauffant un petit élément et en mesurant la vitesse à laquelle l'élément se refroidit.

Différentes applications appellent différentes façons de mesurer la même chose.

1.2.2. L'importance de la précision des capteurs

Imaginez que vous êtes propriétaire d'une cafétéria et que vous voulez mesurer la quantité de café qui sort de l'un de vos robinets. Une façon de le faire est d'installer un capteur en ligne avec la ligne qui va du fût du café au robinet. Ce capteur aurait probablement une petite roue à l'intérieur de celui-ci. Lorsque le café traversait le capteur, la roue tournait, tout comme l'hélice d'une station météorologique.

Lorsque la roue tourne, elle envoie un flux d'impulsions électriques à un ordinateur. L'ordinateur va interpréter les impulsions pour déterminer combien de café coule à travers. Cela semble simple, non ?

C'est là que les capteurs deviennent intéressants. Si vous revenez sur notre description, vous verrez que nous n'avons jamais mesuré directement la quantité de café qui coule à travers le capteur ; nous l'avons interprété à partir d'un courant d'impulsions électriques. Cela signifie que nous devons d'abord comprendre comment interpréter l'étalonnage.

Pour calibrer le capteur, nous devons prendre un conteneur avec une capacité de charge connue, disons, un verre à pinte. Ensuite, nous devons remplir ce conteneur dans diverses conditions pour déterminer à quoi ressemblait le signal d'impulsion électrique.

Par exemple, le premier déversement d'un nouveau fût pourrait avoir tendance à avoir plus de mousse, ce qui se traduirait différemment d'un déversement provenant du milieu du fût qui était entièrement du café. Ce n'est que par le biais d'essais répétés et de nombreuses données que nous avons acquis la confiance que nous pouvons interpréter les données et déterminer la quantité de café qui a été versée.

Une fois que la corrélation est bien connue, un protocole peut être développé pour toujours s'assurer que le capteur est correctement lu. C'est ce qu'on appelle l'étalonnage. Les fabricants réputés fourniront des dispositifs entièrement étalonnés et

fourniront des instructions sur la façon de recalibrer pour vérifier la précision du capteur.

L'exactitude des données détectées est primordiale, puisque vous prendrez des décisions critiques sur la base d'une analyse ultérieure des données, qui ne contiendront que peu de valeur si les données sont erronées.

I.3. Applications d'IoT [7]

Les informations générées et communiquées par les objets habilitants dans IoT peuvent conduire de nombreuses applications possibles dans de nombreux domaines tels que la gestion de la chaîne logistique (SCM), le transport, les soins de santé, la surveillance de l'environnement et des catastrophes, etc. [8]

Au cours des prochaines années, alors que l'Internet des Objets apportera des milliards de nouveaux appareils connectés dans le monde, il existe un énorme potentiel pour débloquent des informations auparavant cachées sur les processus physiques à la fois pour les entreprises et les consommateurs. Cependant, pour accéder à la valeur de toutes ces nouvelles choses connectées, nous avons besoin d'une foule de nouvelles applications logicielles qui peuvent donner un sens au flux de données constant.

Grâce à des capteurs intégrés et de l'intelligence, nous pouvons donner des nerfs aux produits, services et opérations. Maintenant, nous devons réfléchir à la façon dont nous allons traiter les signaux de nos nouveaux sens. Nous ne pouvons certainement pas examiner toutes les données générées par ces systèmes : la surcharge d'informations est déjà un problème important. Des logiciels bien conçus et des analyses prédictives nous aident à faire certaines de ces déterminations, mais nous devons encore décider quels éléments machine et numérique constitueront le système nerveux autonome de nos solutions IoT, et inversement, ce qui constituera le système nerveux somatique, nécessitant intervention humaine pour la prise de décision critique.

La création d'applications qui tirent de la valeur de l'IoT implique beaucoup plus que la génération d'une interface utilisateur sur un site Web ou un appareil mobile. S'il est vrai que certains logiciels IoT peuvent prendre la forme d'une application qui offre à l'utilisateur une nouvelle expérience sur un produit connecté et intelligent, elle peut également consister en une prédiction d'un modèle analytique dérivé de l'apprentissage automatique et assimilé après un examen de multitudes, de données, ou cela pourrait signifier l'intégration d'un flux de données d'une opération connectée dans un autre système d'entreprise.

La conception d'une application IoT commence par l'établissement d'un modèle de l'appareil connecté et des mondes - physiques et numériques - dans lesquels l'appareil

est adapté. Ce modèle permet aux API, aux interfaces utilisateur, aux intégrations d'entreprise et aux analyses d'accéder à un cadre de solution commun, même en cas de modification de la technologie sous-jacente. Pour concevoir et développer efficacement des applications IoT, nous devons modéliser le domaine de problème spécifique, appliquer le logique métier et faire remonter cette information aux utilisateurs.

L'IoT connecte les mondes numérique et physique afin que les appareils intelligents et les opérations puissent fournir une rétroaction aux utilisateurs via une représentation numérique. Lorsque vous vous lancez dans la conception de votre logiciel, vous devez d'abord vous demander : «À quel article me connecte-t-on et comment le représente-t-on numériquement ?» La réponse à ces questions varie énormément selon que vous modélisez un produit intelligent ou plus système complexe tel qu'un bâtiment intelligent, ou même une ville intelligente.

Un modèle sémantique est un bon moyen de construire un pont entre la chose physique et son «jumeau numérique» afin qu'un utilisateur puisse comprendre la relation. Il donne à une personne un moyen de donner un sens au dispositif physique ou à l'opération qui peut être située à une grande distance. Considérez le modèle sémantique comme similaire à une API, une interface de programme d'application pour l'objet ou le système. Il est utile de considérer votre produit ou votre environnement connecté comme ayant des routines et des protocoles. Demandez-vous : «Comment les utilisateurs doivent-ils réfléchir et travailler avec cette représentation numérique dans le nuage (cloud) ?» L'API de votre périphérique ou opération connecté définit les propriétés et les services que vous souhaitez exposer aux développeurs d'applications. Les questions à considérer comprennent :

Propriétés

Quelles sont les propriétés que je veux exposer ? Dans le modèle sémantique d'un produit tel qu'un tracteur connecté, ces propriétés pourraient être des mesures opérationnelles critiques telles que la consommation et la consommation de carburant, la température du moteur, la température du sol, l'emplacement (latitude et longitude), niveau d'huile, niveau de carburant et régime du moteur.

Prestations de service

Quels sont les services fournis par mon appareil I.o.T ? Dans notre exemple de tracteur connecté, les utilisateurs peuvent avoir besoin d'obtenir des diagnostics et des entrées de maintenance, voire même d'arrêter la machine à distance.

Événements

Quels événements mon appareil émet-il ? Le tracteur connecté peut indiquer qu'il est temps de procéder à l'entretien ou d'envoyer un code d'erreur en cas de dysfonctionnement.

En fin de compte, les personnes informées par votre solution IoT n'interagiront pas directement avec les appareils et services connectés, mais avec les informations à travers ce modèle partagé. Le modèle sémantique jette un pont entre le cerveau humain et le périphérique ou le système connecté afin que nous puissions fournir des applications et des expériences utilisateur qui créent de la valeur, génèrent des informations et permettent une action utile. [9]

Le développement de certaines technologies habilitantes telles que la nanoélectronique, les communications, les capteurs, les téléphones intelligents, les systèmes embarqués, le cloud computing et les logiciels, sera essentiel pour soutenir d'importantes innovations des produits IoT dans de nombreux secteurs industriels.

Les perspectives pour l'avenir sont l'émergence d'un réseau d'objets uniques identifiables interconnectés et leurs représentations virtuelles dans une structure similaire à Internet qui est sur-positionnée sur un réseau d'ordinateurs interconnectés permettent de créer une nouvelle plate-forme pour la croissance économique.

Aujourd'hui, de nombreux projets et initiatives européens traitent des technologies et des connaissances de l'Internet des objets. Étant donné que les sujets peuvent être très diversifiés et spécialisés, il existe un fort besoin d'intégration des résultats individuels.

Dans ce contexte, l'intégration des connaissances est conceptualisée comme le processus par lequel des connaissances disparates et spécialisées situées dans plusieurs projets en Europe sont combinées, appliquées et assimilées.

Les principaux domaines d'application de l'IoT sont la création d'environnements / espaces intelligents et d'objets sensibles (e.g. smart transport, villes, bâtiments, énergie, vie, etc.) pour le climat, l'alimentation, l'énergie, la mobilité, la société numérique et la santé applications.

Dans ce contexte, le nouveau concept d'Internet de l'énergie exige des architectures Web pour garantir facilement la fourniture d'informations à la demande et transformer le système d'alimentation traditionnel en un réseau intelligent en réseau largement automatisé, en appliquant plus d'intelligence pour fonctionner, appliquer des politiques, surveiller et auto-guérison si nécessaire. Cela nécessite l'intégration et l'interfaçage du réseau électrique au réseau de données représenté par Internet, englobant la production d'énergie, la transmission, la livraison, les sous-stations, le contrôle de distribution, le comptage et la facturation, les diagnostics et les systèmes d'information.



Figure I.4: les domaines de l'Iot

Ce concept permettrait de produire, stocker et utiliser efficacement l'énergie, tout en équilibrant l'offre / demande en utilisant un Internet cognitif de l'énergie qui harmonise le réseau énergétique en traitant les données, informations et connaissances via Internet. En fait, Internet of Energy exploitera l'autoroute de l'information fournie par Internet pour relier les ordinateurs, les appareils et les services au réseau d'énergie intelligent distribué qui permet aux intervenants d'investir dans les technologies vertes et de revendre l'énergie excédentaire.

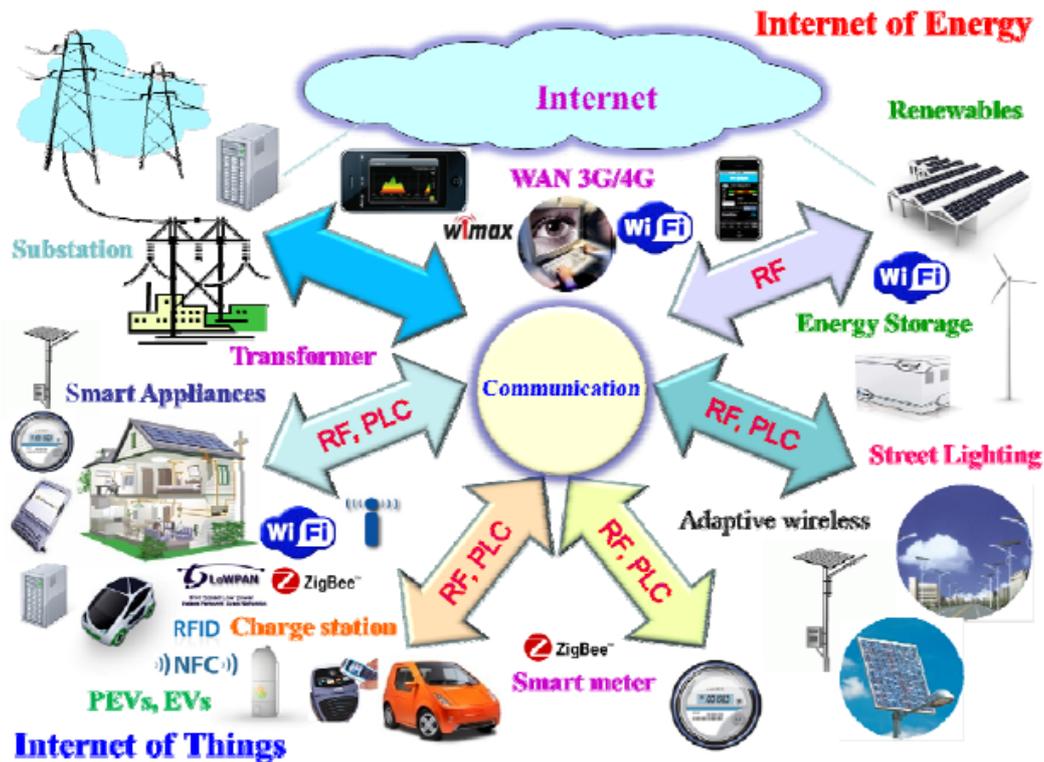


Figure I.5 : les Technologie de communication de l'Iot

Les applications Internet of Energy sont connectées via le Future Internet et IoT, permettant des interactions transparentes et sécurisées et la coopération de systèmes embarqués intelligents sur des infrastructures de communication hétérogènes.

I.4. Applications adaptatives [10]

Les données du capteur et du périphérique sont scientifiquement capturées, nettoyées et analysées pour produire des informations pragmatiques qui sont ensuite transmises aux applications d'entreprise, Web, mobiles, transactionnelles, cloud, opérationnelles et analytiques afin d'être dynamiquement adaptables dans leurs prises de décision, transactions, actes et les livraisons. Ainsi, les objets numérisés, les dispositifs connectés et les applications adaptatives formeront la majeure partie de l'ère des connaissances à venir.

En résumé, il existe une plus grande variété de machines, appareils, électronique grand public, instruments, smartphones, tablettes, ordinateurs portables, robots sophistiqués, spécifiques et génériques, gadgets personnels et compacts et gadgets polyvalents, ustensiles de cuisine, etc. D'un autre côté, il existe des éléments intelligents et sémantiques à faible coût, à faible consommation d'énergie et à ressources multiples, ainsi que des entités telles que des capteurs miniaturisés mais multifonctionnels, des actionneurs, des microcontrôleurs, et des étiquettes. La vraie beauté ici est que tous ces éléments se connectent entre eux dans leur voisinage, ainsi qu'avec les plates-formes de cloud et les infrastructures distantes. Les services connectés, contextuels et cognitifs deviendront la chose normale à cette époque perçue.

I.5. Illustrer le concept d'intégration de machine à machine (M2M)

Une grande partie de la valeur de l'IoT est générée par l'automatisation, ce qui permet aux systèmes de réagir plus rapidement et avec plus de précision que les humains. Peu de systèmes militaires comprennent des réponses entièrement autonomes. Par exemple, la plupart des systèmes sans pilote déployés ne sont pas autonomes mais contrôlés à distance par les opérateurs. [11]

Cet effort de gestion nécessite le développement de nouveaux protocoles de gestion légers. Par exemple, la surveillance des communications M2M des objets IoT est importante pour assurer une connectivité constante. LightweightM2M est une norme développée par l'Open Mobile Alliance (OMA) pour l'interface entre les périphériques M2M et les serveurs afin de créer un système indépendant de l'application pour la gestion à distance de divers périphériques. Le protocole NETCONF Light est un effort de l'IETF (Internet Engineering Task Force) pour la gestion des périphériques à ressources limitées. Dans, les auteurs proposent un cadre de gestion IoT basé sur le concept d'interception de nœuds intermédiaires dans lequel ils exécutent de lourdes tâches de gestion de périphériques sur les routeurs de périphérie ou les passerelles de réseaux contraints. Le groupe de travail OMA Device Management spécifie des protocoles pour la gestion des périphériques mobiles dans les environnements à ressources limitées.

L'omniprésence des technologies de communication ultra-haute (câblées et sans fil) facilite l'objectif important et de longue date de permettre aux dispositifs d'interagir de manière transparente et spontanée les uns avec les autres pour partager leurs potentiels. Le domaine de la communication traverse un flux de transformations méritoires. Il y a de nouveaux paradigmes tels que la communication autonome, unifiée et ambiante. Avec la maturité et la stabilité des plates-formes de communication adaptatives et des infrastructures, il se crée un ensemble de fonctionnalités et de modèles de communication très bénéfiques. Même les processus d'affaires sont étroitement liés aux capacités de communication, de sorte que des processus plus intimes et intensifs sont voués à éclater et à évoluer rapidement vers l'accomplissement net et agréable des aspirations des gens.

Cette capacité de connectivité ad hoc récemment trouvée parmi un grand nombre de dispositifs allant des balises invisibles et infinitésimales, de la poussière intelligente, des autocollants et des étincelles dans nos environnements quotidiens aux machines hautement sophistiquées dans les usines et les hôpitaux a donné naissance à une série de XXXXX et les applications et services premium. Plusieurs domaines industriels sont très optimistes et attendent avec impatience ce changement de paradigme dans la conceptualisation et la concrétisation d'un éventail croissant d'applications créatives et cognitives pour leur communauté d'utilisateurs. Les fournisseurs de services de télécommunication sont les partenaires essentiels pour le succès sans précédent et inhibé de l'intégration de l'appareil à l'appareil (D2D). Une foule d'applications de nouvelle génération est conçue et construite sur la base de cette transformation grandiose apportée par l'idée d'intégration D2D.

Il y a un certain nombre de cas d'utilisation et d'affaires remarquables escalade la popularité saisissante de l'idée de la communication de machine-à-machine (M2M). Les plus importants d'entre eux comprennent des solutions d'intégration résidentielle (propriétaires et normalisées) qui sont en abondance ces jours-ci afin de simplifier et de rationaliser les tâches difficiles et associées au réseautage domestique et à l'automatisation. Cela a conduit à d'innombrables maisons intelligentes au moins dans les pays avancés.

Une fois encore, le comptage intelligent de tous les modules et dispositifs des réseaux électriques donne lieu à des dizaines de réseaux intelligents à travers le monde. La communication transparente entre les différents composants des voitures classiques a abouti à des voitures connectées ou intelligentes. Cela continue et encore. Alimenté par un enthousiasme et un optimisme si généreux parmi les fournisseurs de produits et de plateformes, les sociétés de télécommunications, les fournisseurs de services informatiques, les intégrateurs de systèmes, les départements gouvernementaux, les organismes de normalisation et les laboratoires de recherche. Parmi tous les types de dispositifs de tailles, de portées et de structures variables, il existe une multitude de services robustes et résilients.

I.6. Les Applications M2M

Avec la stabilité et la maturité croissantes des normes, des plates-formes et des infrastructures M2M, les innovateurs inspirés, les individus et les institutions pourraient présenter un certain nombre de cas d'utilisation uniques pour renforcer et soutenir la campagne technologique M2M.

I.6.1. Energie Intelligente (Smart Energy)

L'énergie est devenue une denrée rare, et sa conservation est donc très obligatoire. En outre, plus de consommation d'énergie signifie plus de dissipation de la chaleur dans notre environnement fragile. Autrement dit, grâce à l'utilisation efficace de la précieuse énergie électrique, la dégradation de l'environnement tant redoutée et le réchauffement de la planète peuvent être considérablement minimisés pour atteindre la durabilité environnementale.

Les solutions de comptage intelligent (Smart metering) (c'est une solution M2M connectant chaque dispositif d'énergie-englobant dans un réseau avec le compteur intelligent centralisé) sont très acceptées et utilisées dans les pays avancés afin de comprendre exactement l'utilisation. En d'autres termes, les compteurs d'électricité intelligents aident les consommateurs d'énergie à décoder comment les économies d'énergie peuvent être réalisées sur la base des lectures et des alertes fournies par les compteurs intelligents. L'infrastructure de mesure avancée (AMI) est un domaine de recherche actif et en cours pour générer des solutions pour l'efficacité énergétique.

I.6.2. Médecine Intelligente (Smart Health Care)

Les soins de santé s'avèrent être une énorme industrie dans les années à venir. Il existe un certain nombre de dispositifs spécifiques pour mesurer et gérer un certain nombre de paramètres de santé de l'homme. Les solutions M2M sont capables de rappeler le patient et les membres de sa famille ainsi que le médecin en cas d'urgence résultant de toute anomalie dans l'une des lectures de santé.

I.6.3. Domotique (Smart Home Security)

La domotique peut être rendue possible grâce aux technologies IoT pour nous permettre de contrôler à distance les appareils de notre maison en fonction de nos besoins. Les exemples d'applications comprennent, sans s'y limiter, la surveillance des compteurs, de l'énergie et de l'eau pour éviter les surcharges ou les fuites, ainsi que des capteurs de jardinage qui pourraient être utilisés pour arroser les plantes selon leurs besoins et mesurer leur vitalité. L'énergie et la maintenance des bâtiments intelligents pourraient être optimisées et prédites, ainsi qu'un confort, une sécurité et une sécurité accrue pour les utilisateurs du bâtiment.

Des mécanismes sophistiqués de mise en réseau domestique, d'intégration, d'automatisation, de sécurité et de contrôle arrivent très souvent sur le marché. Les solutions M2M pour la sécurité domestique fusionnent avec la gestion de l'énergie pour fournir des commandes d'alarme à distance ainsi que des commandes de chauffage, de ventilation et de climatisation (HVAC : Heating, Ventilation, and Air Conditioning) à distance pour les maisons et les entreprises via les téléphones mobiles.

I.6.4. Manutention intelligente (smart cargo handling)

Les solutions M2M sont fabriquées dans une variété de conteneurs de stockage ou de manutention, y compris les conteneurs de fret, les sacs d'argent et de documents et les fûts de déchets nucléaires. L'emplacement en temps réel du conteneur, qu'il soit ouvert ou fermé, et la façon dont les conteneurs sont manipulés par des détecteurs de mouvement, peuvent être facilement obtenus pour prévenir les risques de sécurité et de vol et augmenter la capacité de récupération des matériaux volés ou perdus.

I.6.5. Smart traffic Management

Les solutions M2M sont en mesure de fournir des informations routières en temps réel aux conducteurs des véhicules via des dispositifs GPS automobiles afin de leur permettre d'envisager de meilleures alternatives.

I.6.6. Smart Inventory and Replenishment Management

Les solutions M2M peuvent être intégrées dans les capteurs mesurant la quantité de produit en vrac dans un bac de stockage. Cette information peut être mise à la disposition du fournisseur et de l'utilisateur, de sorte que des réarrangements proactifs peuvent être initiés lorsque les stocks atteignent un niveau prédéterminé. Ceci est très bénéfique pour le processus de fabrication qui ne consomme pas une quantité constante et prévisible de produit ou le temps de transport du produit en vrac entraîne une rupture du produit.

I.6.7. Smart Cash Payment

Les solutions M2M permettent aux lecteurs de cartes de crédit ou de débit mobiles de fournir des transmissions de données sécurisées et cryptées aux guichets de transaction et de billetterie dans les hypermarchés, les hôtels, les cinémas, les magasins d'alimentation, etc. La vente au détail devient une affaire facile sans être dans la file d'attente pour le paiement en espèces. La connectivité transparente entre les balises, les lecteurs d'étiquettes, les cartes de paiement, les banques d'affaires, les détaillants, etc. contribue grandement à améliorer considérablement l'expérience client.

I.6.8. Smart Tracking

Les solutions M2M permettent aux parents de suivre très précisément leurs enfants assis au bureau et d'habiliter les soignants à suivre à distance les personnes handicapées ainsi que les personnes vivant seules, malades, affaiblies et alitées. Les gestionnaires peuvent surveiller leurs employés effectuant des tâches dans des endroits difficiles et dangereux. En particulier ceux qui travaillent dans les puits de pétrole, combattent un feu de forêt, aident dans des endroits frappés par des catastrophes, se battent dans des zones de guerre, font de la randonnée dans les montagnes, etc. bénéficient immensément de ces innovations technologiques.

Les articles à l'intérieur des distributeurs automatiques peuvent communiquer avec leurs fournisseurs et fournir toutes les informations pertinentes sur le nombre de bacs et de bouteilles à l'intérieur et combien de plus sont nécessaires pour remplir le distributeur automatique. C'est certainement une nette amélioration par rapport à la pratique actuelle.

I.6.9. Smart Displays

Toutes sortes de machines telles que les guichets automatiques, les distributeurs automatiques, les téléviseurs, les caméras vidéo de sécurité, les panneaux de signalisation et les tableaux de bord peuvent être reliés entre eux à des endroits stratégiques. Avec une telle intégration intime à travers une solution M2M compétente, des vidéos personnalisées, ainsi que des images statiques, peuvent être envoyées à ces machines pour afficher des détails et des affichages sensibles au temps. Une personne affamée peut commander ses pizzas sur son téléphone mobile, mais voir les détails de la pizza et les images sur l'écran plus grand de l'une de ces machines ou avec des projecteurs connectés montrant les images sur un mur blanc pour donner une vision claire.

I.6.10. Smart Manufacturing

Une voiture est ramenée à son garage pour la nuit, et son port de données est branché. Ensuite, des choses passionnantes commencent à arriver. Tout d'abord, la voiture envoie des informations de diagnostic au fabricant pour vérifier contre tout système qui nécessite une réparation, une maintenance ou un remplacement. Le fabricant télécharge ensuite une sélection de nouvelles expériences de conduite, y compris un style d'accélération différent (choix de sport ou lisse), un logiciel de navigation et de cartographie amélioré, et de nouvelles caractéristiques de sécurité dans la voie.

D'un point de vue extérieur, l'IoT offre une sélection illimitée d'innovations, allant d'une brosse à dents électrique qui surveille le style de brossage correct aux capteurs de pression des pneus dans les flottes de camions aux capteurs de géolocalisation attachés au bétail. Le potentiel pour leur utilisation est illimité, et cela inclut dans l'usine. La fabrication connectée est l'IoT. L'analyse proactive permet à un

périphérique d'identifier les besoins futurs, par exemple lorsqu'une pièce peut être défaillante, lorsqu'elle doit être réparée ou lorsque des fournitures doivent être commandées. Lorsque la machine elle-même peut envoyer les commandes appropriées à un humain ou à une autre machine, elle assure un fonctionnement régulier, sûr et économique.

I.6.11. Smart Asset Management

Chaque industrie a son propre ensemble d'actifs spécifiques. Par exemple, les hôpitaux devraient avoir un certain nombre de machines de balayage, d'équipement de diagnostic, de moniteurs de santé, de robots et d'autres instruments. Autrement dit, il existe une variété de dispositifs à la fois petits et grands. Le véritable défi réside dans l'identification efficace de leur emplacement en cas d'urgence, d'entretien, de gestion, de surveillance, d'inventaire, de sécurité, etc.

Il y a plusieurs avantages uniques d'une solution M2M dans ce scénario compliqué. Une solution M2M avancée réduit considérablement le temps passé par les employés à localiser précisément l'emplacement des actifs, augmente considérablement leur utilisation et permet de partager des actifs de grande valeur entre les départements et les installations. Avec tous les actifs dans un environnement hospitalier intégrés les uns avec les autres et avec les plates-formes web ou cloud distantes via le produit M2M, la surveillance, la réparation et la gestion à distance sont largement facilitées. Grâce à la connectivité établie avec les applications de soins de santé hébergées dans le cloud, chaque machine pouvait mettre à jour et télécharger ses données vers les applications centralisées et cyber, permettant ainsi d'automatiser un certain nombre d'activités en évitant toute intervention manuelle, interprétation et instruction.

Les professionnels et les experts explorent, expérimentent et exposent un éventail croissant de cas d'affaires et d'utilisations à valeur ajoutée pour divers segments de l'industrie afin de maintenir l'élan sur l'espace M2M. Il y a une autre tendance qui s'accélère rapidement avec la participation active des universitaires et des vétérans de l'industrie. Les systèmes cyber-physiques (CPS : Cyber-Physical Systems) sont les nouvelles entités puissantes qui prennent de l'ampleur. C'est-à-dire que toutes sortes de systèmes physiques sur le terrain sont dotées de dizaines d'applications, de services et de données génériques et spécifiques. Autrement dit, non seulement la connectivité, mais aussi l'autonomisation inspirée par le logiciel est en train de devenir l'évolution de la prochaine génération dans l'espace de la machine.

I.6.12. Smart Retailing

McDonald's est parti pour une expérience unique en matière d'engagement des utilisateurs. Un mélange d'appareils IoT et de promotions contextuelles a permis à l'exploitant de restaurant d'adapter ses offres d'applications mobiles et sa publicité à des informations telles que l'emplacement, la météo, les habitudes d'achat et la réponse aux promotions. Par exemple, si quelqu'un se déplace rapidement lors d'une

chaude journée d'été, l'application, qui s'exécute sur une plate-forme d'analyse contextuelle Vmob, montre une offre pour un soda à un drive-through à proximité. Cela a reçu un accueil enthousiaste de la part des clients.

Pour les détaillants, l'utilisation de l'IoT pour le marketing et les ventes revient à créer des expériences significatives afin d'augmenter la fidélité et l'engagement des clients. Starbucks, la chaîne de café, a choisi de lancer un certain nombre de balises à distance dans ses établissements de Seattle. Pour les clients avec l'application Starbucks, les balises diffusent des notifications sur les bières les plus fraîches et des promotions personnalisées. L'idée est de faire passer le client occasionnel à des mélanges haut de gamme qui sont offerts à Starbucks.

Faciliter les transactions des clients et récompenser les interactions avec la marque sont des moyens efficaces de renforcer la fidélité des clients. Home Depot tire parti de l'IoT pour accroître l'engagement des clients dans la deuxième dimension, en fournissant un service et des informations personnalisés à leurs clients pour les aider dans leur processus de prise de décision. Leur application mobile permet aux acheteurs de localiser l'inventaire, comparer les magasins, demander des experts sur les projets, et voir comment les produits se ressemblent dans leurs maisons. Une fois à l'intérieur du magasin, l'application peut les guider dans les allées pour trouver les produits.

L'IoT propose des propositions intéressantes pour différents secteurs industriels, y compris les détaillants. Les écrans interactifetouch, la publicité contextuelle, les promotions géolocalisées, les environnements personnalisés en magasin et la réalité augmentée ne sont que le début. Cependant, il est important de se rappeler que la valeur de l'IoT ne réside pas dans les progrès technologiques mais dans l'amélioration et la création d'expériences client immersives.

I.6.13. Agriculture intelligente

Les technologies IoT, telles que les capteurs de terrain, peuvent être utilisées pour surveiller l'humidité, l'humidité et la nutrition du sol, ajuster automatiquement la température pour maximiser la production agricole et communiquer avec les stations météorologiques pour obtenir les dernières prévisions [50, 39]. Ils peuvent également aider à une fertilisation et un arrosage précis [50]. Les capteurs utilisés pour le suivi des animaux aident à surveiller le bétail pour détecter les maladies et les accidents, et offrent de meilleures possibilités d'élevage [39]. Les "fermes intelligentes" peuvent également partager des données avec d'autres fermes, consommateurs et régulateurs [39]. Les principales opportunités offertes par l'IoT pour l'agriculture sont de maximiser les rendements en identifiant automatiquement les mauvaises herbes nuisibles et en signalant leur localisation aux propriétaires ou aux machines de désherbage autonomes, en améliorant la traçabilité des aliments et en informant les consommateurs de leur origine, origine et méthodes de production. Des défis tels que l'utilisation d'accéléromètres 3D pour détecter les blessures chez les vaches et les

surveiller au sein du bétail, ce qui permet une adoption précoce de mesures préventives [39].

I.7. IoT Vision

Internet of things est un concept et un paradigme qui considèrent la présence omniprésente dans l'environnement d'une variété de objets qui à travers des connexions sans fil et filaires et des schémas d'adressage uniques sont capables d'interagir et de coopérer avec d'autres choses / objets, applications / services et atteindre des objectifs communs. Dans ce contexte, les défis de la recherche et du développement pour créer un monde intelligent sont énormes. Un monde où le réel, le numérique et le virtuel convergent pour créer des environnements intelligents qui rendent l'énergie, les transports, les villes et bien d'autres domaines plus intelligents. L'objectif de l'Internet des objets est de permettre aux objets d'être connectés n'importe quand, n'importe où, avec n'importe quoi et n'importe qui, idéalement, en utilisant n'importe quel chemin / réseau et n'importe quel service. IoT est une nouvelle révolution de l'internet. Les objets se rendent reconnaissables et obtiennent l'intelligence en prenant ou autorisant des décisions contextuelles grâce au fait qu'ils peuvent communiquer des informations sur eux-mêmes et qu'ils peuvent accéder à des informations agrégées par d'autres éléments ou qu'ils peuvent être des composants de services complexes. [12]

I.8. Les défis de sécurité et de confidentialité concernant l'utilisation des smartphones dans les réseaux IoT et IoE [13]

La sécurité et la confidentialité des smartphones dans IoT et IoE devraient être garanties au maximum, car le smartphone est considéré comme l'appareil personnel majeur utilisé dans IoT. Les menaces et les attaques sur les téléphones intelligents et les appareils IoT peuvent être réparties dans les catégories suivantes :

Ressources : GPS, camera, NFC, et autre capteurs.

Données : messagerie, appels, contacts, photos...etc.

Information sur le système : telles que l'adresse MAC, l'IP, qui peuvent être divulguées sans l'autorisation de l'utilisateur.

Worms : qui sont des programmes qui se copient sur les différents appareils d'un réseau et peuvent compromettre la sécurité du smartphone.

Spyware and malware applications : qui peut surveiller les données des utilisateurs à son insu et envoyer les données au hacker.

D'autres attaques sur les smartphones discutés dans [14] incluent "les attaques de logiciels malveillants financiers, les attaques de spoofing de réseau, les attaques de phishing, les attaques de surveillance et les attaques de congestion de réseau" [14].

Les auteurs de [14] divisent la violation de la sécurité en cinq catégories,

1. Breach of confidentiality : quand une personne non autorisée lit et obtient l'accès aux données.

2. Breach of integrity: quand l'attaquant écrit et modifie les données.

3. Breach of availability: lorsque l'attaquant détruit et supprime les données.

4. Denial of service : lorsque l'attaquant attaque les ressources limitées du smartphone comme tuer sa mémoire, vider sa batterie, etc. et le rend donc incapable de communiquer avec d'autres appareils IoT.

5. Theft of services: lorsque les ressources sont utilisées par une personne non autorisée.

Les cinq catégories d'atacks mentionnées ci-dessus ont différents effets sur les smartphones comme principaux appareils IoT, par exemple, un déni de service d'un smartphone affectera l'IoT et le réseau cellulaire, une fuite de données sur un smartphone révélera des données privées telles comme des transactions en ligne, et un atack spam envoie des messages à d'autres smartphones et appareils IoT.

I.9. Conclusion [15]

L'Internet of Things (IoT) et Internet of Everything (IoE) sont en train de tracer rapidement leur chemin dans nos vies modernes, permettant de connecter et d'automatiser tout ce qui nous entoure. Ce chapitre a donné un aperçu de ces nouvelles tendances, de leurs technologies habilitantes, de l'architecture et des applications telles que les maisons intelligentes et les soins de santé. Dans ce chapitre, nous avons également parlé des différentes technologies d'activation IoT et IoE disponibles dans le smartphone et des exemples de son utilisation dans les scénarios IoT et IoE. Nous avons proposé un modèle pour la mise en œuvre de l'Internet des objets qui utilise les capteurs du smartphone pour détecter et transmettre des données à plusieurs applications backend à l'aide d'une couche de middleware. Les applications peuvent être exécutées sur un smartphone, qui reçoit les données et les présente à l'utilisateur final, c'est-à-dire le patient, l'administration de l'hôpital ou le médecin dans le cas des soins de santé. Ces données pourraient être stockées dans des bases de données spéciales ou dans le cloud et récupérées ultérieurement par l'utilisateur en cas de besoin, en utilisant l'application dédiée au smartphone. Nous avons également couvert les différences entre les réseaux IoT et les réseaux cellulaires mobiles en termes de besoin de réseaux IoT pour une longue durée de vie, de prise en charge d'un grand nombre de périphériques, d'évolutivité du réseau, de coûts de déploiement et de déploiement. Enfin, les opportunités et défis futurs de l'IoT et de l'IoE ont été abordés en particulier les risques de sécurité et de confidentialité liés à l'utilisation du smartphone dans ces réseaux et les contre-mesures possibles. En abordant l'utilisation intensive du smartphone dans les applications IoT et IoE de ce chapitre, nous considérons que le smartphone est l'ultime IoT et IoE. Dans le chapitre suivant, nous allons aborder les différents protocoles et technologies de communication.

Chapitre II

Protocoles et technologies de communication

II.1. Introduction

Dans ce chapitre, on va introduire les éléments basiques dans la communication via internet, les technologies utilisées dans l'internet des objets ainsi que la structure de ce dernier.

II.2. Structure de l'IdO

L'IoT est un réseau mondial reliant les choses à travers de nombreuses technologies telles que la RFID et les codes à barres pour n'en nommer que quelques-uns. L'Union Internationale des Télécommunications (UIT) a structuré l'IoT en quatre dimensions : (1) marquer les choses, (2) ressentir des choses, (3) rétrécir les choses, et (4) penser les choses. Lors de l'étiquetage, les étiquettes RFID sont utilisées pour identifier et suivre automatiquement l'objet attaché. En ressentant les choses, les capteurs sont utilisés pour collecter des données de l'environnement physique telles que la température, la pression, etc. En rétrécissant les choses, la nanotechnologie est utilisée pour de petites choses : par exemple, "l'utilisation de nanocapteurs pour surveiller la qualité de l'eau". Dans la réflexion, les choses intelligentes ont besoin, en plus de la communication, de traiter l'information, de s'auto-entretenir et de prendre des décisions indépendantes ; cette vision change la voie de la communication d'information de l'humain-humain à la chose-chose. La structure de l'IoT est illustrée dans la figure ci-dessous.

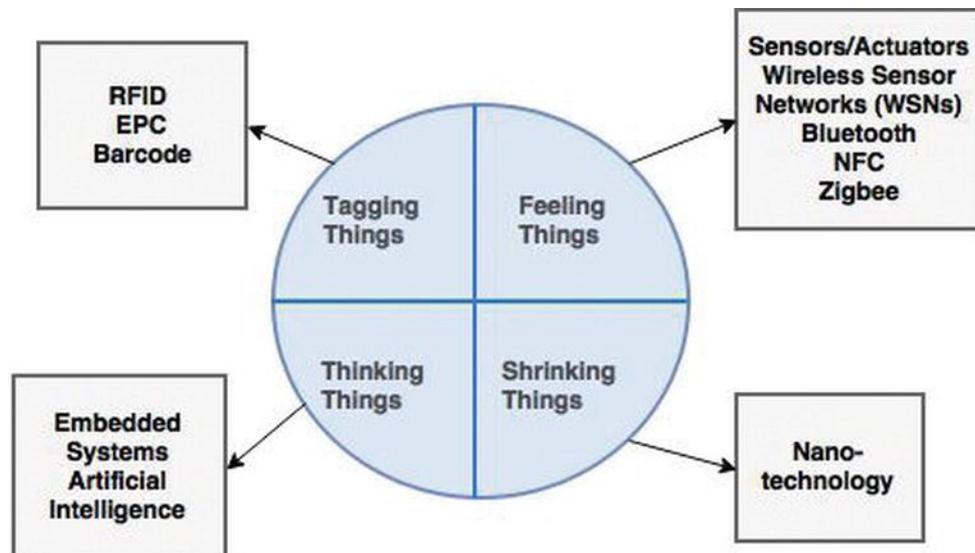


Figure II.1 : Structure de l'IoT

II.3. IoT technologies

II.3.1. Radio-frequency identification (RFID)

RFID est une technologie d'identification sans fil qui utilise des ondes radio pour identifier un objet ou une personne. La RFID a été utilisée pour la première fois lors de la seconde guerre mondiale pour identifier des avions amis ou ennemis en 1948. La

technologie a ensuite été fondée au centre Auto-ID du MIT en 1999. Les systèmes RFID se composent essentiellement de trois éléments : l'étiquette RFID sert à identifier de manière unique l'objet attaché et transporte des données, le lecteur RFID est l'équipement utilisé pour alimenter l'étiquette et lire / écrire des données sur l'étiquette. Les données lues par le lecteur RFID à partir des étiquettes RFID dans son voisinage doivent être traitées ensuite par un système logiciel, connu sous le nom de middleware RFID, qui est le troisième composant d'un système RFID. Le middleware RFID sert à gérer les lecteurs, à filtrer, à formater et à traiter les données RFID brutes capturées par les étiquettes et à envoyer les données traitées aux différentes applications backend intéressées. Il existe trois versions différentes d'étiquettes RFID en fonction de l'alimentation électrique : les étiquettes passives, les étiquettes actives et semi-passives. Les étiquettes peuvent également être classées en fonction de leur type de mémoire, par exemple en lecture seule, en lecture-écriture ou en écriture-une fois et en lecture-multiple. Les étiquettes RFID utilisent les gammes de fréquences ISM (industrielles, scientifiques ou médicales) et ont trois types de fréquences : basse fréquence (LF), haute fréquence (HF), ultra haute fréquence (UHF) et fréquence micro-ondes. La technologie RFID est rentable, elle est considérée comme très importante dans les réseaux IoT pour faciliter le suivi et l'identification des objets, et elle est utilisée dans un très large éventail de domaines d'application.

II.3.2. Electronic product code (EPC)

Développé par le centre AutoID en 1999 au MIT, le code EPC (64/98 bits) peut stocker des informations sur le numéro de série unique d'un produit, ses spécifications et les détails du fabricant. L'EPC comprend quatre composants : "service de dénomination d'objet (ONS)", "service de découverte EPC (EPCDS)", "services d'information EPC (EPCIS)" et "services de sécurité EPC (EPCSS)". Le réseau EPCglobal a été créé par l'organisation EPCglobal pour partager les données EPC et constitue un cadre constitué du système d'identification ; Étiquettes et lecteurs EPC ; Middleware EPC, qui prend en charge le formatage des données de base ; EPC Information Services, qui permettent l'échange d'informations entre les partenaires ; et Discovery Services, qui permettent aux utilisateurs d'obtenir et de rechercher des données EPC. L'EPC a été essentiellement conçu pour être stocké sur une étiquette RFID afin d'identifier un article spécifique et ses données associées telles que le point d'origine et la date de production.

II.3.3. Barcode

Le système de codes à barres utilise un lecteur de codes à barres pour interpréter la valeur dans l'étiquette du code à barres afin d'obtenir un code unique utilisé pour l'identification d'objet. Les codes à barres sont des "étiquettes optiques lisibles par machine attachées à des éléments pour enregistrer des informations à leur sujet, et elles sont généralement lues par des scanners laser". Il existe trois types de codes à barres: alpha numérique utilisé pour coder les chiffres et les caractères, numérique utilisé pour coder des paires de nombres et bidimensionnel, qui ressemble à des carrés

ou des rectangles contenant de nombreux petits points individuels. L'inconvénient de ce système est l'exigence de ligne de vue entre le code à barres et le lecteur.

II.3.4. Internet protocol (IP)

Le protocole Internet (IP), développé dans les années 1970, est considéré comme le protocole réseau principal utilisé pour l'envoi de paquets sur Internet. Il existe deux versions différentes d'adresses IP : IPv4 (version par défaut) et IPv6. IPv6 a été développé pour étendre le nombre d'adresses IP disponibles et supportées.

II.3.5. Wireless Fidelity (Wi-Fi)

Wi-Fi (fidélité sans fil) permet aux périphériques de communiquer via un signal sans fil et contient tout type de périphérique de réseau local sans fil (WLAN) prenant en charge l'une des versions de spécification IEEE 802.11 suivantes : 802.11a, 802.11b, 802.11g et 802.11n. Aujourd'hui, le Wi-Fi offre la connectivité WLAN haute vitesse aux hôtels, aux foyers, aux aéroports et aux cafés grâce à l'utilisation de points d'accès sans fil. Bien que le cryptage soit considéré comme optionnel en Wi-Fi, trois techniques de cryptage ont été définies et appliquées au Wi-Fi pour assurer la sécurité. Ces techniques sont "Wired Equivalent Privacy (WEP)", "WPA (WiFi Protected Access)" et "IEEE 802.11i / WPA2". Pour accéder à un réseau Wi-Fi, des périphériques compatibles Wi-Fi (par exemple, des ordinateurs portables) sont nécessaires, qui peuvent communiquer sans fil dans n'importe quel emplacement équipé du Wi-Fi.

II.3.6. Bluetooth

Bluetooth est une technologie de communication bon marché, déployée sur de petites distances (10-100 mètres), qui permet la connexion entre des appareils, par exemple, ordinateurs portables, PDA, smartphones, imprimantes, caméras, etc. sans avoir besoin de câblage. Bluetooth est considérée comme la technologie principale pour créer un réseau personnel (PAN) afin de partager des données telles que du texte, des images, des vidéos et des sons, et il utilise la norme IEEE 802.15.1. Bluetooth permet aux utilisateurs des connexions instantanées entre plusieurs appareils et assure une protection contre les interférences et la sécurité dans les informations envoyées. La technologie Bluetooth fonctionne dans la bande ISM, qui est 2,45 GHz. Certaines applications Bluetooth standard incluent, mais ne sont pas limitées à la communication entre un appareil mains libres et un téléphone portable ou un autoradio, et le transfert de fichiers entre appareils. Bluetooth peut comporter des risques de sécurité, car il s'agit d'un système ouvert. La sécurité peut être mise en œuvre au niveau des appareils et des services.

II.3.7. ZigBee

La technologie ZigBee a été créée et développée en 2001 par l'Alliance ZigBee. Comme défini dans, ZigBee est "un protocole de réseau sans fil de faible puissance, faible coût, faible débit et courte portée (environ 100 mètres) basé sur la norme IEEE 802.15.4". ZigBee est largement utilisé dans la domotique, la surveillance médicale, les contrôles industriels et l'architecture numérique. ZigBee a été développé pour améliorer les caractéristiques des réseaux de capteurs sans fil (WSN) et est largement utilisé pour les systèmes domotiques sans fil (WHAS); Cependant, il présente de nombreux défis tels que des contraintes de ressources, une mémoire insuffisante, une batterie limitée, une puissance de traitement limitée, une portée limitée, des limitations technologiques liées à la norme IEEE 802.15.4, des interférences avec des systèmes fonctionnant dans la même bande libre et qui est nécessaire dans WHAS pour la surveillance à distance.

II.3.8. Near-Field communication (NFC)

NFC est une technologie sans fil à courte portée (théoriquement 20 cm, mais dans la plupart des scénarios, typiquement 4 cm) développée par "Philips et Sony" qui fonctionne à la fréquence de 13,56 MHz et permet aux clients du monde entier de dispositifs, et échanger du contenu numérique. La technologie NFC est compatible avec l'infrastructure RFID existante et les cartes à puce sans contact et utilise les mêmes normes que la norme ISO / IEC 14443, ce qui constitue l'un de ses plus grands avantages. NFC a une méthode de connexion facile et simple, peut travailler aussi dans un environnement sale, et ne nécessite pas une ligne de vue pour lire et exécuter des transactions. Quelques exemples d'applications de NFC incluent, mais ne sont pas limités au paiement mobile tel que Google Wallet, et la billetterie mobile comme Oyster Card.

II.3.9. Wireless Sensor Networks (WSNs)

Un WSN est constitué de centaines à des milliers de "nœuds de capteurs" communiquant entre eux et transmettant des données relatives à des "conditions physiques" ou "environnementales" telles que pression, température, mouvement, localisation, son, etc. Les WSN sont largement utilisés dans l'IoT pour de nombreux types d'applications telles que la surveillance de l'agriculture, la surveillance des patients, les applications militaires, la surveillance routière, les applications civiles et environnementales, les incendies de forêt, l'automatisation industrielle, le domotique, etc. Un exemple de l'utilisation des réseaux sociaux dans les soins de santé est l'utilisation de capteurs pour surveiller les réponses médicamenteuses du corps d'un patient. Un problème clé rencontré lors de la conception d'un réseau WSN est l'efficacité énergétique, c'est-à-dire la conception d'une "longue durée de vie du réseau et de coûts de maintenance et de déploiement réseau limités". Un système middleware est nécessaire pour fournir les services multiples requis par les applications WSN et

permettre l'évolutivité, l'économie d'énergie et la qualité de service (QoS) lors de la conception des applications WSN.

II.3.10. Artificial intelligence (AI)

L'intelligence a été intégrée et cachée dans les périphériques connectés au réseau qui aident les gens à faciliter leurs activités quotidiennes. L'IA se réfère alors aux «environnements électroniques et dispositifs sensibles à la présence et aux activités des personnes». L'intelligence artificielle est considérée comme «intégrée», car les périphériques utilisés sont intégrés de manière transparente dans l'environnement des personnes, «sensibles au contexte» parce que ces dispositifs sont utilisés pour connaître les situations et les contextes contextuels des personnes. "Adaptatif" car il évolue en fonction des besoins des utilisateurs, et "anticipatoire" car il peut prédire les besoins de l'utilisateur sans médiation consciente.

II.4. IoT architecture [16]

Comme suggéré par ITU, une infrastructure pareil sera construite vers une architecture à multicouches comme l'indique la figure 2.2.

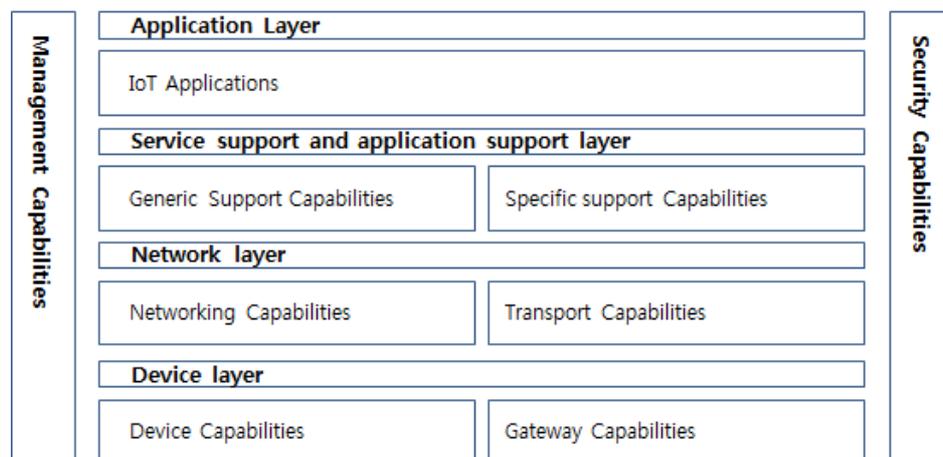


Figure II.2: IoT Architecture (Source: ITU-T)

Device Level inclut tous les capteurs et actionneurs IoT (e.g. les objets dans IoT).

Network Level inclut tous les composants de réseau IoT tels que les passerelles IoT, routeurs et commutateurs. Le niveau réseau IoT (e.g. Internet dans IoT).

Application Services Platform Level inclut les fonctions du logiciel de gestion des clés pour permettre la gestion globale des appareils IoT et du réseau. Il comprend également des fonctions principales reliant le périphérique et les niveaux réseau avec la couche application.

Application Level inclut toutes les applications fonctionnant dans le réseau IoT.

Dû aux contraintes de la bande passante et d'énergie, les périphériques prennent principalement en charge les unités de données faibles avec une puissance de calculs limités et un taux de détection limité.

Certaines applications nécessitent une détection multi-mode, de sorte que chaque appareil peut avoir plusieurs capteurs sur planche.

II.5. Aperçu de la communication internet :

II.5.1. Protocole IP

Les données sont envoyées d'une machine à une autre dans un paquet, avec une adresse de destination et une adresse source dans un format normalisé (un "protocole"). L'expéditeur ne connaît pas toujours le meilleur itinéraire vers la destination à l'avance. La plupart du temps, les paquets de données doivent passer par un certain nombre de machines intermédiaires, appelées routeurs, pour atteindre leur destination. Les réseaux sous-jacents ne sont pas toujours les mêmes : comme nous avons utilisé le téléphone, le service postal et la livraison à la main, les paquets de données peuvent être acheminés via des réseaux filaires ou sans fil, via le système téléphonique ou par satellite.

Un paquet IP est un bloc de données avec le même type d'informations que vous écririez sur une enveloppe physique : le nom et l'adresse du serveur, et ainsi de suite. Mais si un paquet IP est transmis sur votre réseau câblé local via un câble Ethernet - le câble qui connecte votre routeur haut débit domestique ou votre réseau local de bureau (LAN) à un PC de bureau - alors le paquet entier sera regroupé dans un autre type d'enveloppe, un cadre Ethernet, qui ajoute des informations supplémentaires sur la façon de compléter les dernières étapes de son voyage vers votre ordinateur.

II.5.2. TCP

Le protocole TCP (Transmission Control Protocol) est le protocole de transport le plus simple sur Internet. TCP est construit sur le protocole IP de base et ajoute des numéros de séquence, des accusés de réception et des retransmissions. Cela signifie qu'un message envoyé avec TCP peut être arbitrairement long et donner à l'expéditeur l'assurance qu'il est réellement arrivé à la destination intacte.

Parce que la combinaison de TCP et IP est si utile, de nombreux services sont construits à son tour, tels que le courrier électronique et le protocole HTTP qui transmet des informations à travers le World Wide Web.

II.5.3. Protocole TCP/IP SUITE

La combinaison de TCP et d'IP est si omniprésente que nous nous référons souvent simplement à "TCP / IP" pour décrire une suite entière de protocoles superposés, chaque couche reposant sur les capacités de celle ci-dessous :

- Les protocoles de bas niveau de la couche liaison gèrent le transfert de bits d'informations à travers une liaison réseau. Cela peut se faire par un câble Ethernet, par WiFi, ou sur un réseau téléphonique, ou même par des normes radio à courte portée telles qu'IEEE 802.15.4 conçues pour transporter des données sur le réseau personnel (PAN), c'est-à-dire entre appareils porté par un individu.
- La couche Internet se trouve alors au-dessus de ces différents liens et extrait les détails sanglants en faveur d'une adresse de destination simple.
- Alors TCP, qui vit dans la couche de transport, s'assoit sur IP et l'étend avec un contrôle plus sophistiqué des messages transmis.
- Enfin, la couche application contient les protocoles qui traitent de l'extraction de pages Web, de l'envoi de courriels et de la téléphonie Internet. Parmi ceux-ci, HTTP est le plus omniprésent pour le Web, et en effet pour la communication entre les appareils de l'Internet des Objets. Nous examinons brièvement les normes telles que MQTT dans les titres qui suit.

II.5.4. Protocole UDP

Comme vous pouvez le voir, TCP n'est pas le seul protocole de la couche de transport. Contrairement à TCP, mais comme avec IP elle-même, dans UDP, chaque message peut arriver ou non. Aucune handshake ou retransmission ne se produit, et il n'y a aucun délai pour attendre les messages en séquence. Ces limitations font que TCP est préférable pour de nombreuses tâches pour lesquelles les périphériques Internet of Things seront utilisés.

Cependant, le manque de surcharge rend UDP utile pour des applications telles que le streaming data, qui peut gérer des erreurs mineures mais n'aime pas les retards. La téléphonie basée sur l'ordinateur voix sur IP (VoIP), comme Skype par exemple, l'absence d'un paquet peut causer un petit problème dans la qualité du son, mais attendre que plusieurs paquets arrivent dans le bon ordre, sera difficile à comprendre le discours. UDP est également le transport pour certains protocoles très importants qui fournissent des fonctionnalités communes de bas niveau, telles que DNS et DHCP, qui se rapportent à la découverte et la résolution des périphériques sur le réseau. Nous examinons ce sujet en détail dans la section suivante.

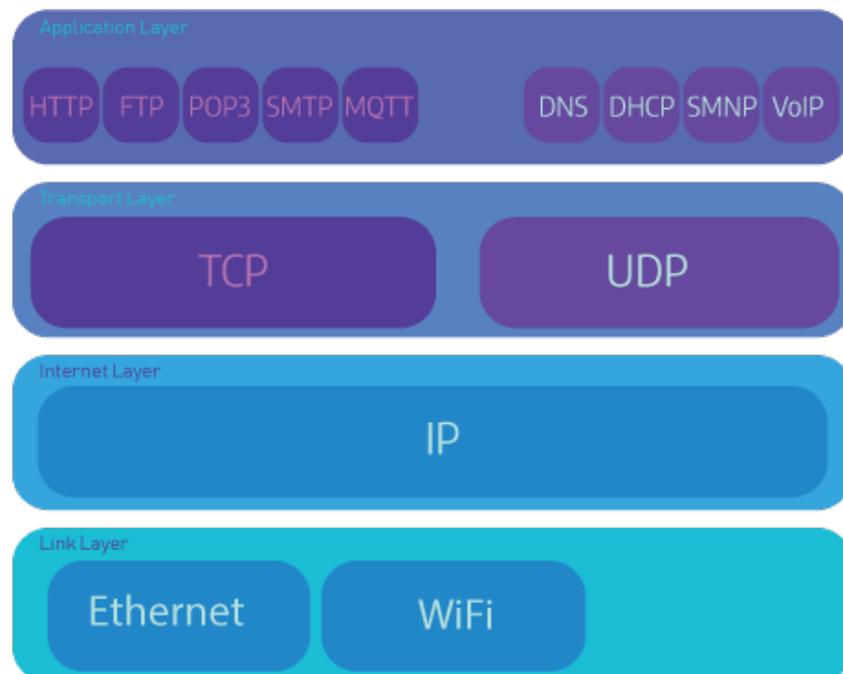


Figure II.3 : TCP/IP Protocol Suite

II.6. IP ADDRESSES

Nous avons mentionné précédemment que le protocole Internet connaît les adresses des périphériques source et destination. Mais en quoi consiste une "adresse" ?

Dans le monde des réseaux informatiques de bas niveau, les nombres sont beaucoup plus faciles à traiter. Ainsi, les adresses IP sont des nombres. L'Internet Protocol version 4 (IPv4), offre 4,3 milliards d'adresses IP possibles, 4 294 967 296 pour être précis, soit 2^{32} . Bien que cela soit pratique pour les ordinateurs, les adresses IP sont généralement écrites en quatre numéros séparés par des points (de 0.0.0.0 à 255.255.255.255), e.g. 192.168.1.1 (qui est souvent l'adresse de votre routeur domestique) ou 8.8.8.8 (qui est l'adresse de l'un des serveurs DNS de Google).

Ce "quadri pointillé" est toujours exactement équivalent au nombre de 32 bits. En plus d'être simplement plus facile à retenir pour les humains, il est également plus facile de déduire des informations sur l'adresse en regroupant certains blocs d'adresses. Par exemple,

8.8.8.x – Une des plages IP attribuées à Google.

192.168.x.x - Une plage assignée pour les réseaux privés. Votre routeur de réseau domestique ou professionnel peut attribuer des adresses IP dans cette plage.

10.x.x.x - Une autre plage privée.

Chaque machine sur Internet a au moins une adresse IP. Cela signifie que chaque ordinateur, chaque imprimante connectée au réseau, chaque smartphone et chaque périphérique d'Internet des objets en possède un. Si vous disposez déjà d'un Raspberry Pi, une carte Arduino ou de l'un des autres microcontrôleurs, ils s'attendent également à obtenir leur propre adresse IP. Quand vous considérez ce fait, ces 4 milliards d'adresses semblent soudainement ne pas suffire.

Les plages privées telles que 192.168.x.x offrent une solution à ce problème. Votre réseau domestique ou professionnel peut avoir une seule adresse IP visible

publiquement. Toutefois, vous pouvez affecter toutes les adresses IP comprises entre 192.168.0.0 et 192.168.255.255 ($2^{16} = 65\,536$ adresses) à des périphériques distincts.

Une meilleure solution à ce problème est la prochaine génération de protocole Internet, IPv6.

II.6.1. Adresse IP statique

Comment vous est-il attribué une adresse IP ? Si vous avez acheté un pack d'hébergement de serveur auprès d'un fournisseur de services Internet (ISP : Internet Service Provider), vous pouvez généralement recevoir une seule adresse IP. Mais la société elle-même a reçu un bloc d'adresses à attribuer, il s'agissait de plages de tailles différentes, généralement séparées en "classes" de 8 bits, 16 bits ou 24 bits :

Class A — 1.0.0.1 à 126.255.255.254

Class B — 128.1.0.1 à 191.255.255.254

Class C — 192.0.1.1 à 223.255.254.254

Class D — 224.0.0.0 to 239.255.255.255

Remarque : Les adresses de classe A 127.0.0.0 à 127.255.255.255 ne peuvent pas être utilisées et sont réservées aux fonctions de bouclage et de diagnostic.

La plage de classe C avait seulement 8 bits (256 adresses), alors que les plages de classe A avaient beaucoup plus d'adresses, donc cette classe a été réservée aux plus grandes organisations Internet. La séparation rigide des plages d'adresses en classes n'était pas très efficace ; chaque entité voudrait garder suffisamment d'adresses de rechange pour une expansion future, mais cela signifie que de nombreuses adresses resteraient inutilisées. Avec la croissance du nombre de périphériques connectés à Internet, le schéma a été remplacé depuis 1993 par CIDR (Classless Inter-Domain Routing), qui vous permet de spécifier exactement combien de bits de l'adresse sont fixé (Voir RFC 1518 et 1519, à <http://tools.ietf.org/rfc/>). Ainsi, les adresses de classe A que nous avons mentionnées ci-dessus seraient équivalentes à 0.0.0.0/8, alors qu'une classe C pourrait être 208.215.179.0 / 24, e.g, vous avez vu précédemment que Google avait la plage : 8.8.8.x (which is equivalent to 8.8.8.0/24 in CIDR notation).

Google a choisi de donner à l'un de ses serveurs DNS publics l'adresse 8.8.8.8 de cette plage, en grande partie parce que cette adresse est facile à retenir.

Cependant, dans de nombreux cas, l'administrateur du système affecte simplement les numéros de serveur dans l'ordre. L'administrateur note les adresses et met à jour les enregistrements DNS et ainsi de suite pour pointer vers ces adresses. Nous appelons ce type d'adresse statique car une fois assignée, elle ne changera plus sans intervention humaine.

Considérez maintenant votre réseau domestique : chaque fois que vous connectez un ordinateur de bureau à votre routeur, connectez votre ordinateur portable ou votre téléphone mobile au réseau sans fil ou allumez votre imprimante réseau, cet appareil doit obtenir une adresse IP (souvent dans la plage 192.168.0.0 / 16). Vous pouvez vous-même attribuer une adresse de manière séquentielle, mais la personne typique à la maison n'est pas un administrateur de système et n'a pas d'information détaillée/technique. Si votre frère, qui avait l'habitude d'utiliser l'adresse 192.168.1.8 mais qui n'a pas été à la maison depuis longtemps, et après son retour, il trouve que votre nouvelle imprimante laser a maintenant cette adresse, il ne pourra pas se connecter à Internet.

II.6.2. DYNAMIC IP ADDRESS ASSIGNMENT

Heureusement, nous n'avons généralement pas à choisir une adresse IP pour chaque appareil que nous connectons à un réseau. Au lieu de cela, lorsque vous connectez un ordinateur portable, une imprimante ou même une machine à bulles sur Twitter, il peut demander une adresse IP à partir du réseau lui-même à l'aide du protocole DHCP (Dynamic Host Configuration Protocol). Lorsque le périphérique essaie de se connecter, au lieu de vérifier sa configuration interne pour son adresse, il envoie un message au routeur demandant une adresse. Le routeur lui attribue une adresse. Ce n'est pas une adresse IP statique qui appartient à l'appareil indéfiniment ; il s'agit plutôt d'un "bail" temporaire qui est sélectionné dynamiquement en fonction des adresses actuellement disponibles. Si le routeur est redémarré, le bail expire, ou si le périphérique est éteint, un autre périphérique peut se retrouver avec cette adresse IP.

Cela signifie que vous ne pouvez pas simplement pointer une entrée DNS vers un périphérique à l'aide de DHCP. En général, vous pouvez vous fier à l'adresse IP qui est probablement la même pour une session de travail donnée, mais vous ne devriez pas coder l'adresse IP n'importe où que vous pourriez essayer de l'utiliser une autre fois, quand elle pourrait avoir changé.

Même les dispositifs informatiques les plus simples tels que la carte Arduino, peuvent utiliser DHCP. Bien que la bibliothèque Ethernet de l'Arduino vous permette de configurer une adresse IP statique, vous pouvez également en demander une via DHCP. Utiliser une adresse statique peut convenir au développement (si vous êtes la seule personne connectée avec cette adresse), mais pour travailler en groupe ou préparer un périphérique à distribuer à d'autres personnes sur des réseaux arbitraires, vous avez presque certainement besoin d'une adresse IP dynamique.

II.7. DNS

Bien que les ordinateurs puissent facilement gérer des nombres de 32 bits, même formatés en quadruplés, ils sont faciles à oublier pour la plupart des humains. Le DNS (Domain Name System) nous aide à naviguer sur Internet. Les noms de domaine, tels que les suivants, nous sont familiers sur le Web, ou peut-être à partir d'e-mails ou d'autres services :

- ✓ google.com
- ✓ linkedin.com
- ✓ youtube.com
- ✓ arduino.cc

Chaque nom de domaine a un domaine de premier niveau (TLD : Top-Level Domain), comme .com ou .dz ou .uk qui se subdivise en .co.uk et .gov.uk, et ainsi de suite. Ce domaine de premier niveau sait où trouver plus d'informations sur les domaines qu'il contient, e.g, .com sait où trouver google.com.

Les domaines ont alors des informations sur l'endroit où diriger les appels vers des machines ou des services individuels. Par exemple, les enregistrements DNS pour .google.com savent où vous diriger pour les éléments suivants :

- ✓ www.google.com
- ✓ mail.google.com
- ✓ calendar.google.com

Les exemples précédents sont tous immédiatement reconnaissables en tant que noms de sites Web, ce qui signifie que vous pouvez les entrer dans votre navigateur Web, par exemple, <http://www.google.com>.

Mais le DNS peut également pointer vers d'autres services sur Internet, par exemple :

pop3.google.com : réception des emails de Gmail.

smtp.google.com : l'envoi des emails de Gmail.

ns1.google.com : l'un des adresses DNS de plusieurs serveurs de Google.

Configurer DNS est une question de changement de quelques paramètres. Votre registraire (la société qui vous vend votre nom de domaine) a souvent un panneau de contrôle pour modifier ces paramètres. Vous pouvez également exécuter votre propre serveur DNS faisant autorité. Les paramètres peuvent contenir des entrées comme celle-ci pour roomofthings.com : *book A 80.68.93.60 3h*

Cette entrée signifie que l'adresse book.roomofthings.com (qui héberge le blog pour ce livre) est desservie par cette adresse IP et sera pour les trois prochaines heures.

II.8. Adresse MAC

En plus d'une adresse IP, chaque périphérique connecté au réseau a également une adresse MAC, qui est comme l'adresse finale sur une enveloppe physique. Elle est utilisée pour distinguer différentes machines sur le même réseau physique afin qu'elles puissent échanger des paquets. Cela concerne la "couche de liaison" de niveau le plus bas de la pile TCP / IP. Bien que les adresses MAC soient globalement uniques, elles ne sont généralement pas utilisées en dehors d'un réseau Ethernet (par exemple, au-delà de votre routeur domestique). Ainsi, lorsqu'un message IP est routé, il saute d'un nœud à l'autre, et lorsqu'il atteint finalement un nœud qui sait où se trouve la machine physique, ce nœud transmet le message au dispositif associé à cette adresse MAC.

MAC est synonyme de Media Access Control. C'est un nombre de 48 bits, généralement écrit en six groupes de chiffres hexadécimaux, séparés par des deux-points, par exemple : 01:23:45:67:89:AB

La plupart des périphériques, tels que votre ordinateur, votre smart phone sont livrés avec l'adresse MAC gravée dans les puces Ethernet. Cependant, certaines puces, telles que WizNet de l'Arduino Ethernet, n'ont pas d'adresse MAC implémenté. C'est pour des raisons de production : si ces puces sont produites en série/gros, ils sont, bien sûr, identiques. Donc, ils ne peuvent pas, physiquement, contenir une adresse distinctive. L'adresse pourrait être stockée dans le microprogramme de la puce, mais cela nécessiterait que chaque puce soit construite avec du code personnalisé compilé dans

le microprogramme. Alternativement, on pourrait fournir une puce de données simple qui stocke juste l'adresse MAC et fait lire la puce WizNet. Évidemment, la plupart des appareils grand public utilisent un processus similaire pour s'assurer que la machine démarre toujours avec la même adresse MAC unique. La carte Arduino, en tant que plate-forme de prototypage à bas prix pour les développeurs, ne se soucie pas de cette finesse, pour gagner du temps et de l'argent. Pourtant, elle est livrée avec un autocollant avec une adresse MAC imprimée dessus. Bien que cela puisse sembler un peu étrange, il y a une bonne raison à cela : cette adresse MAC est réservée et donc garantie unique si vous voulez l'utiliser. À des fins de développement, vous pouvez simplement choisir une adresse MAC connue pour ne pas exister sur votre réseau.

II.9. Protocole http [17]

Bien qu'il soit possible d'exécuter n'importe quel type de protocole propriétaire sur TCP / IP, il existe quelques protocoles standards populaires et largement supportés. Si vous utilisez un protocole standard pour transmettre vos données de capteur, vous serez en mesure de travailler avec beaucoup plus de périphériques et d'applications que si vous aviez développé votre propre protocole propriétaire.

Le protocole standard le plus important est de loin le protocole HTTP (HyperText Transfer Protocol), le protocole du World Wide Web. HTTP décrit comment un client interagit avec un serveur, en envoyant des messages de requête et en recevant des messages de réponse via TCP / IP, comme illustré dans la Figure ci-dessous :

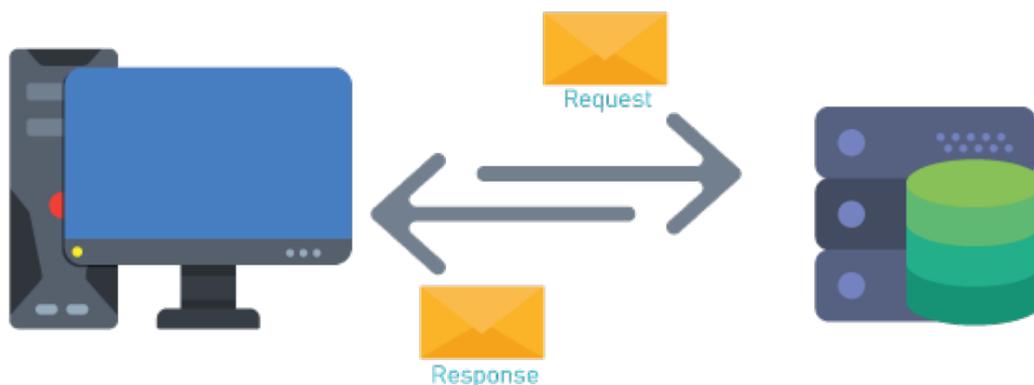


Figure II.4 : Client send request message, server answer with response.

Les navigateurs Web sont les clients HTTP les plus populaires, mais vous pouvez facilement écrire vos propres clients et vos propres serveurs. Si vous utilisez un navigateur Web pour accéder à un périphérique, celui-ci joue le rôle d'un serveur Web fournissant un service Web sur Internet.

Un serveur contient des ressources qui peuvent présenter un intérêt, par exemple un document (généralement une page Web HTML), la mesure la plus courante d'un capteur ou la configuration d'un dispositif. Lorsque vous concevez un service Web, vous devez décider quelles ressources il doit exposer au monde.

HTTP utilise des URI (Uniform Resource Identifiers) pour indiquer au serveur la ressource que le client souhaite lire, écrire, créer ou supprimer. Vous connaissez les URIs de la navigation Web ; ils ressemblent à ceci :

- ✓ <http://www.example.com/index.html>
- ✓ <http://www.example.com/temperatures>
- ✓ <http://www.example.com/temperatures/actual>
- ✓ <http://www.example.com:50000/temperatures/actual>
- ✓ <http://www.example.com/temperatures?alarm=none>
- ✓ <http://www.example.com/temperatures?alarm=high>
- ✓ <http://www.example.com/temperatures?alarm=low>
- ✓ <http://www.example.com/valve/target>

Un URI indique le schéma (par exemple, `http`), l'hôte (par exemple, `www.example.com`), éventuellement le port (par exemple, `50000`), et le chemin (par exemple, `/temperatures/actual`) à la ressource détenue et gérée par cet hôte, comme le montre la figure 2.4. Facultativement, un URI peut également contenir une requête (par exemple, `alarm=haute`) après un caractère `?` qui suit le chemin.

Pour le protocole HTTP, le port 80 est utilisé par défaut sauf si un autre port est choisi explicitement, peut-être à des fins de test. Le chemin est appelé URI de requête dans HTTP ; il indique la ressource cible d'une requête HTTP.

Il existe plusieurs types de requêtes HTTP qu'un client peut envoyer, mais les plus populaires sont GET pour lire une ressource, PUT pour écrire dans une ressource, POST pour créer une ressource et DELETE pour supprimer une ressource. Les

navigateurs Web émettent principalement des requêtes GET, qui constituent la grande majorité des requêtes HTTP. Dans une application Web of Things, une requête GET a un URI, tel que :

`http://www.example.com/temperatures/actual`

Peut retourner la mesure la plus récente d'un capteur de température, alors qu'un PUT a un URI, tels que :

`http://www.example.com/valve/target`

Peut changer le réglage d'un actionneur - dans ce cas, une vanne. Les requêtes POST ajoutent des sous-ressources à une ressource, ce qui revient à placer un fichier dans un répertoire. Par exemple, un POST d'une mesure a la ressource suivante :

`http://www.example.com/temperatures`

Peut créer une nouvelle ressource :

`http://www.example.com/temperatures(42135)`

Une requête DELETE supprime une ressource, par exemple, elle peut supprimer le / températures ressource :

`http://www.example.com/temperatures`

du serveur. Bien sûr, cela ne supprimerait pas physiquement le capteur de température du matériel.

Les requêtes PUT, POST et GET portent des représentations de la ressource adressée. La représentation la plus connue est l'HyperText Markup Language, mieux connu sous le nom de HTML. Un navigateur Web est un client HTTP qui sait comment afficher des pages HTML à l'écran.

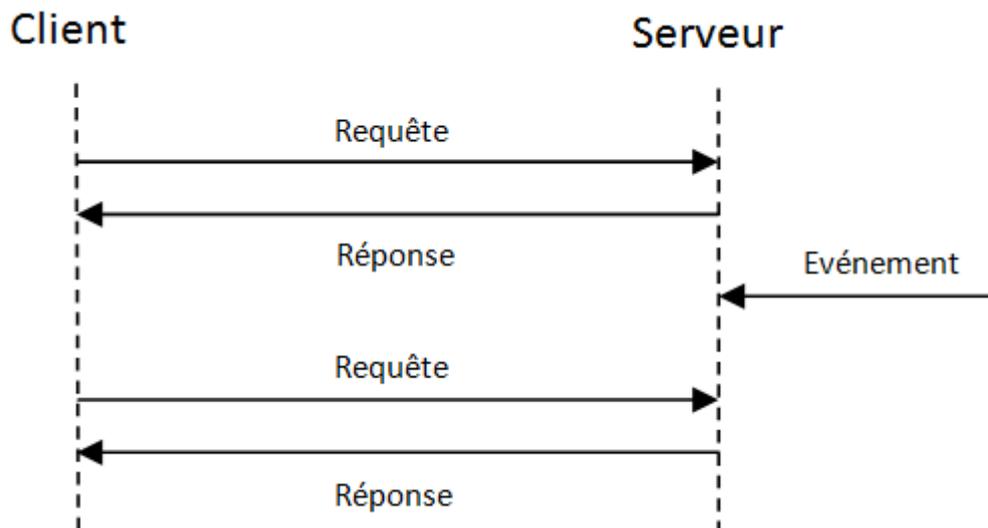
Un service Web peut prendre en charge une ou plusieurs représentations pour une seule ressource. Par exemple, une mesure de température peut être représentée dans une représentation en texte brut, comme ceci :

29 deg

or dans un XML representation, like this:

```
<sample>
  <value>23.5</value>
  <unit>deg</unit>
</sample>
```

Certaines représentations sont standardisées, comme le HTML, mais vous pouvez aussi définir vos propres représentations, comme celles ci-dessus. Certaines représentations sont des documents autonomes ; d'autres soutiennent des liens vers d'autres ressources. Vous connaissez les liens hypertexte de HTML, qui utilisent des URI pour adresser d'autres ressources. En cliquant sur un lien, le navigateur envoie une requête GET pour obtenir une représentation de cette ressource. Cette requête est envoyée à l'hôte contenu dans l'URI du lien.



FigureII.5 : requête / réponse HTTP

Regardons un exemple complet d'interaction requête / réponse HTTP (Figure II.5).

1. Ce diagramme montre une requête GET, car elle peut être envoyée par un navigateur Web ou votre propre programme client. Le client demande une représentation de la «température réelle mesurée par le capteur de

température» de la ressource, dont l'URI est constituée de l'hôte `www.example.com` et de l'URI de la demande.

`/temperatures/actual.`

2. Le service de l'hôte `www.example.com` reçoit la demande, mesure la température et renvoie un message de réponse. Dans cet exemple, la réponse indique la réussite (200 OK) et une représentation en texte brut de 8 octets. La représentation est de 25,3 degrés.

Même les interactions Web les plus complexes consistent en de tels échanges de messages. Le Web comprend plusieurs centaines de millions de clients et plusieurs centaines de milliers de serveurs avec leurs ressources, et il produit un torrent de messages véhiculant des représentations de ressources. Le terme technique pour cette architecture est le transfert d'état représentationnel, ou REST. Pour plus d'informations sur REST, voir RESTful Web Services de Leonard Richardson et Sam Ruby (O'Reilly).

L'objectif de la mise en route de l'Internet des objets est de montrer comment REST et les standards Web communs peuvent être utilisés comme moyen privilégié de création d'applications de l'Internet des objets. De telles applications sont parfois appelées applications Web of Things, pour mettre l'accent sur l'utilisation de standards Web en plus des protocoles Internet de base.

Le Web of Things est constitué de services Web RESTful qui mesurent ou manipulent les propriétés physiques.

Ainsi, le terme "Web of Things" se concentre sur la couche d'application et les «choses» du monde réel qui sont mesurées ou manipulées. Le terme «Internet des objets» se concentre sur les couches de réseau sous-jacentes et les moyens techniques pour mesurer et manipuler l'environnement physique, c'est-à-dire les capteurs et les actionneurs.

II.10. Push Versus Pull

Votre appareil peut communiquer avec un autre ordinateur sur le Web de quatre manières différentes :

1. Device is the client, pushing data to a server

2. Device is the client, pulling data from a server
3. Device is the server, providing data to clients
4. Device is the server, accepting data from clients

Ces modèles peuvent être visualisés comme illustré à la Figure 2.6. Une flèche noire indique la direction d'un message de demande et une flèche en pointillé indique la direction dans laquelle les données circulent, c'est-à-dire, dans quelle direction une représentation de ressource est envoyée.

Dans les applications de surveillance, un dispositif produit des données, c'est-à-dire, des mesures à partir de ses capteurs attachés. Pour de telles applications, les modèles d'interaction 1 et 3 conviennent : les flux de données de l'appareil vers un autre ordinateur ; l'appareil est client (1) ou serveur (3).

Dans les applications de contrôle, un dispositif consomme des données, c'est-à-dire des commandes provenant d'un navigateur Web ou d'un autre client. Pour de telles applications, les modèles d'interaction 2 et 4 conviennent : les flux de données vers l'appareil proviennent d'un autre ordinateur ; l'appareil est client (2) ou serveur (4).

Dans la partie II, je vais me concentrer sur l'appareil en tant que client (c'est-à-dire sur les scénarios 1 et 2). Étant donné qu'en général, un périphérique ne peut pas savoir à l'avance si vous souhaitez lui envoyer une commande (par exemple, pour configurer un actionneur ou reconfigurer un capteur), il est logique de prendre également en charge les périphériques en tant que serveurs. Par conséquent, je vais discuter des scénarios 3 et 4 de la partie III. Je crois que le potentiel de l'Internet des objets ne sera atteint que si les appareils peuvent devenir des clients, des serveurs ou les deux.

II.11. Conclusion

Dans ce chapitre, nous avons présenté les différents protocoles utilisés dans le domaine de l'Internet des objets ainsi que les différentes technologies de communication telles que WiFi, Bluetooth, ZigBee, etc. Dans le chapitre suivant, nous allons présenter les parties matérielle et logicielle de notre application mobile.

Chapitre III

Description matérielle et
logicielle de l'application
IoT intelligente

III.1. Introduction :

Au fil du temps, l'électronique devient de plus en plus programmable et les composants deviennent de plus en plus miniaturisés. On parle des systèmes embarqués ou l'informatique embarqué, dont le but de simplifier l'électronique et par conséquent réduire l'utilisation de composants électroniques, réduisant ainsi le coût de fabrication d'un produit. Il en résulte des systèmes plus performants pour un espace réduit.

L'électronique a eu une croissance fulgurante jusqu'à aujourd'hui, depuis son existence. L'électronique est devenue accessible à toutes personnes en ayant l'envie, ce que nous allons apprendre dans ce travail est un mélange d'électronique et de programmation.

Cette partie sera consacrée aux réalisations d'un prototype IoT, et aux étapes fondamentales pour le développement de ce dernier.

III.2. Spécifications des besoins

Cette phase consiste à comprendre le contexte du système. Il s'agit de déterminer les fonctionnalités et les exploiters et identifier les cas d'utilisation.

III.2.1. Besoins fonctionnels

Il s'agit des fonctionnalités du système qui se traduisent par des besoins spécifiant un comportement clair In/Out du système.

Dans ce cas, le système peut posséder deux exploiters :

- Un utilisateur.
- Un développeur.

Les services destinés à l'utilisateur se traduisent comme suit :

- Signalement de la fuite de gaz.
- Détection de feu.
- Consulter la température et l'humidité.
- Manipuler les portes externes sans contact et à distance.
- Allumer / Eteindre l'éclairage automatiquement.

- Surveiller l'humidité du sol.

Note :

- Tous ces services peuvent être utilisés à tout moment.
- Le système est synchronisé,

III.2.2 Besoins non fonctionnels

Il s'agit des besoins qui caractérisent le système, ce sont des besoins en matière de performance, de type matériel ou de type conception.

Le système doit répondre aux critères suivants :

- La rapidité de traitement.
- La performance.
- La facilité d'utilisation.

III.3. Architecture globale du système

Le schéma suivant illustre l'architecture du système IoT :

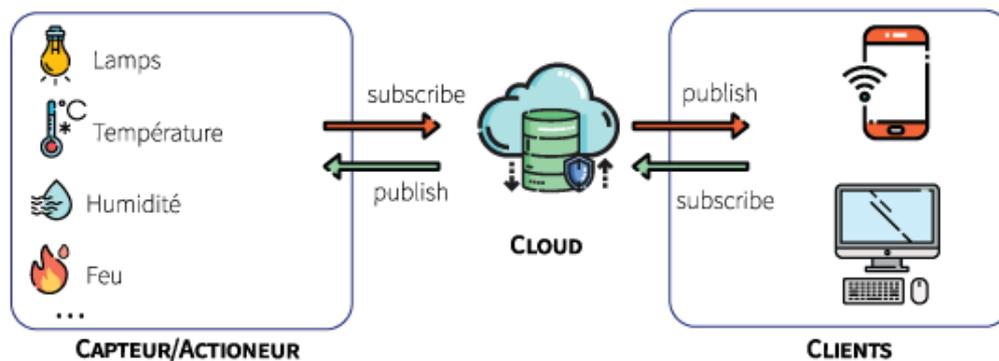


Figure III.1 Architecture globale du système

Selon la figure ci-dessus, on remarque que l'architecture du système se compose de 3 parties :

- Partie utilisateur.
- Partie matérielle (capteurs et actionneurs).
- Partie serveur, pour interconnecter les deux parties précédentes.

III.3.1. Partie Utilisateur

L'utilisateur peut contrôler et consulter les capteurs et/ou actionneurs via un Smartphone, tablette ou un PC, il suffit d'être connecté à Internet.

III.3.2. Partie matérielle

C'est la partie la plus importante dans le système dont l'utilisateur a besoin pour communiquer. Cette partie est composée d'équipements qui contrôlent le site tels que capteurs, actionneurs et moyens de communication dont on va les détailler dans ce qui suit.

Pour les composants, on a choisi les capteurs suivants :

III.3.2.1. Le node MCU N°1 :

On choisit un capteur de gaz qui est sensible au gaz butane et un autre capteur de flamme. On a aussi choisi un capteur de température et humidité, en plus des LEDs pour l'éclairage intérieur.

III.3.2.2. Le node MCU N°2 :

Pour les capteurs, on a choisi un capteur d'humidité de sol (Soil Moisture) accompagné d'un capteur de l'humidité et température, en plus 2 relais pour le contrôle de la pompe à eau.

III.3.2.3. Le node MCU N°3 :

On a choisi un servomoteur qui contrôle la porte du garage, ainsi un LDR (Light-Dependent Resistor), une résistance lumineuse avec un module laser, pour le système de sécurité.

Toutes ces cartes (NodeMCU) communiquent avec la technologie WiFi, ce qui facilitera la communication avec un modem, et avec le cloud.

III.3.3. Partie Cloud

Cette partie a pour but d'obtenir et d'envoyer les données des capteurs et des actionneurs du système ensuite les synchroniser avec l'application dont elle possède l'utilisateur.

III.4. Diagramme de cas d'utilisation

Les cas d'utilisation sont une technique de description du système étudié privilégiant le point de vue de l'utilisateur. Un cas d'utilisation est une façon spécifique d'utiliser le système, déclenchée en réponse à la simulation d'un exploitateur.

III.4.1. Les exploitateurs

On distingue deux types d'exploiteurs :

- Les exploitateurs principaux : cette catégorie regroupe les personnes qui utilisent les fonctions principales du système.
- Les exploitateurs secondaires : cette catégorie regroupe les personnes qui effectuent des tâches administratives ou de maintenance.

Dans le cas de ce projet, on a deux exploitateurs :

- ✓ **L'utilisateur** : c'est le résident du site qui est l'utilisateur principal du système pour la prestation des services.
- ✓ **Le développeur** : c'est celui qui se charge des tâches de maintenance et l'entretien du système, en cas d'erreur ou de rajout d'un nouveau service dans le site.

III.4.2. Les cas d'utilisation

Les cas d'utilisation se déterminent en observant et en précisant, les séquences d'interaction, les scénarios du point de vue de l'utilisateur. Ils sont des abstractions de dialogue entre les exploitateurs et le système.

- ✓ L'utilisation dans notre cas.
- ✓ Allumer / Eteindre une lampe.
- ✓ Activer / Désactiver le système d'alarme.
- ✓ Ouvrir / Fermer la porte.
- ✓ Consulter les valeurs des capteurs.

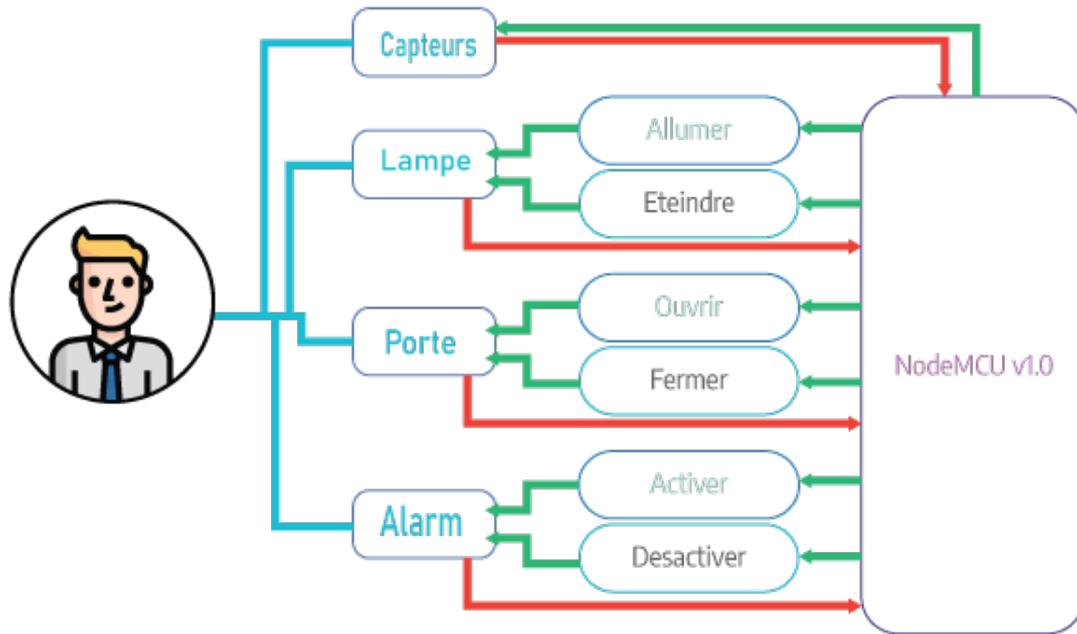


Figure III.2 : Diagramme d'utilisateur

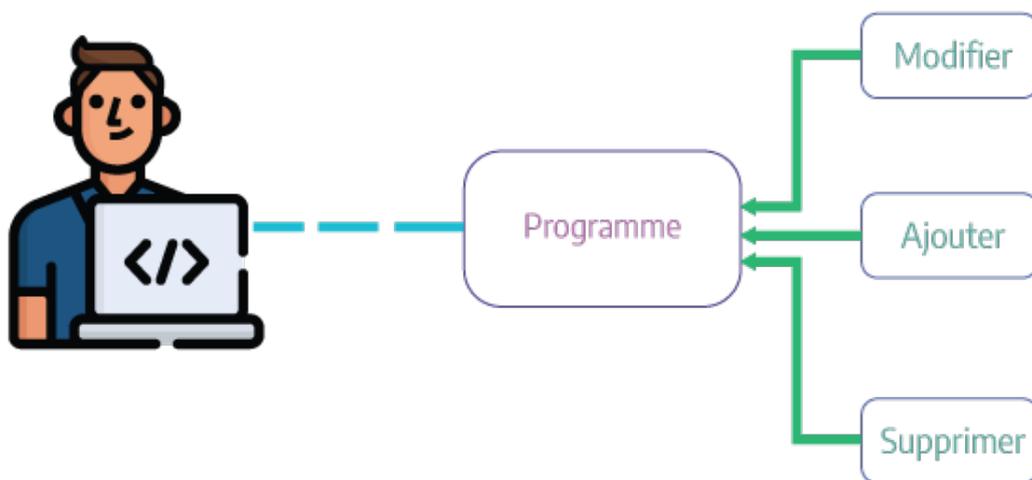


Figure III.3 : Diagramme d'utilisation de développeur

D'après le diagramme, les tâches d'utilisateur sont :

- Consulter les capteurs.
- Allumer / Eteindre les lampes.
- Ouvrir /Fermer la porte.
- Activer / Désactiver l'alarme.

Et pour l'utilisateur, les tâches sont :

- Modifier, ajouter et/ou supprimer un service.

III.5. Fonctionnement du système

Le principe de fonctionnement du système est décrit par la figure ci-dessous :

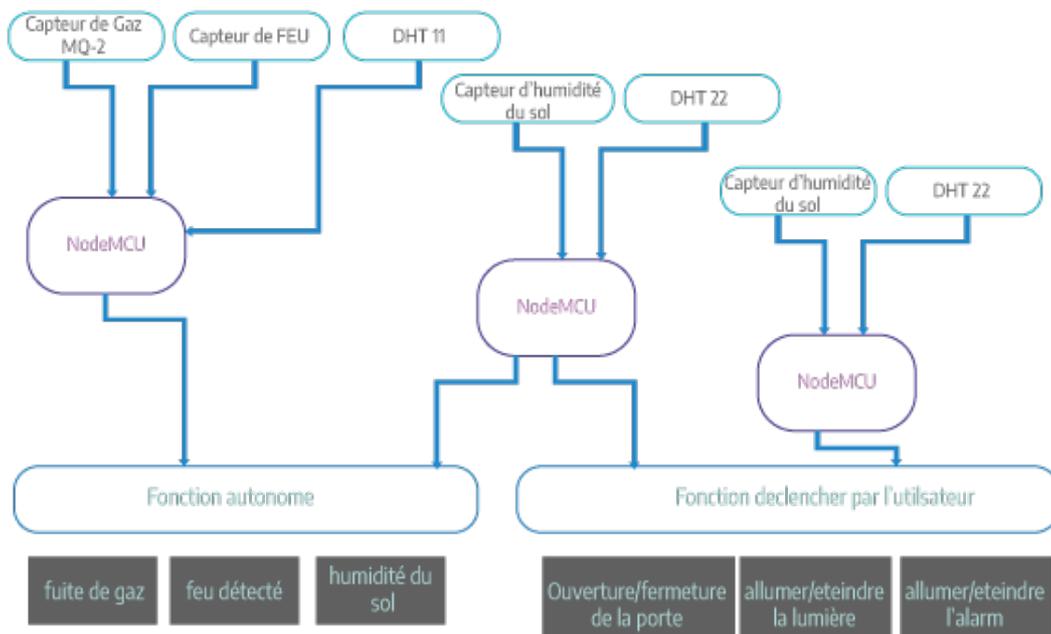


Figure III.4 : Fonctionnement du système

III.6.Moyens utilisés :

III.6.1.Partie Hardware :

Nous avons utilisés trois cartes ESP8266-12e et plusieurs composants (capteurs/actionneurs) pour réaliser ce travail.

III.6.1.1. Définition du module ESP8266-12E (Node MCU v1.0)

L'ESP8266 se programme exactement comme un Arduino. Il faudra juste rechercher la correspondance des broches pour votre carte, e.g. la correspondance des broches ESP8266 12E.

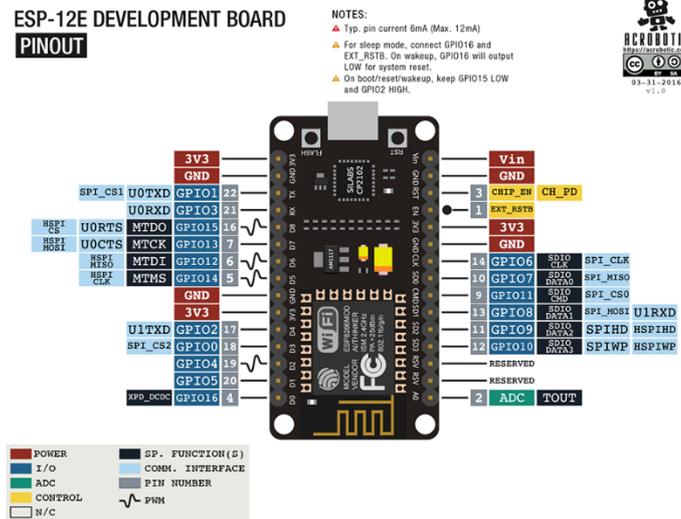


Figure III.5 : Module ESP8266-12E

L'ESP8266-12E est une version améliorée de l'ESP8266-12. L'ESP8266-12E possède 11 broches GPIO ainsi qu'un convertisseur analogique/numérique (ADC) avec une résolution de 10 bits.

C'est le module employé par presque toutes les cartes NodeMCU. Il est compact et polyvalent, c'est la carte idéale pour réaliser des projets d'objets connectés.

III.6.1.2. Correspondance des broches entre Arduino et ESP8266 (NodeMCU)

Si vous débutez la programmation Arduino ou que vous découvrez les modules ESP8266, c'est sans doute la solution la plus simple pour débiter. La librairie ESP8266Wifi est maintenant très aboutie et simplifie grandement la programmation. C'est un argument qui penche également en faveur de l'IDE Arduino.

III.6.1.3. Bibliothèques ESP8266Wifi

Le projet de la librairie ESP8266Wifi se trouve sur github. Cette librairie propose les fonctions suivantes :

- Connexion à un point d'accès.
- Connexion à un serveur (un Broker MQTT par exemple).
- Envoi / réception de messages à un serveur.
- Re-connexion automatique.

III.6.1.4. En Lua (NodeMCU)

NodeMCU est un firmware qui permet de programmer les modules ESP8266 dans un langage appelé Lua. Vous pouvez consulter le projet open-source NodeMCU [ici](#). Il existe deux versions de NodeMCU :

- NodeMCU v0.9 pour les modules ESP8266-12
- NodeMCU v1.0 pour les modules ESP8266-12E

Pour programmer en Lua, le plus simple est d'utiliser ESPlorer. ESPlorer, est un programme qui a été conçu pour les trois plateformes : MAC OS, Windows, LINUX, programmé avec JAVA, à condition d'avoir java dans la machine, minimum java 7.

III.6.1.5. Description de fonctionnement des capteurs et actionneurs

III.7.1.5.1. Capteur de température et d'humidité : DHT

Le capteur d'humidité et de température DHT facilite grandement l'ajout de données d'humidité et de température à vos projets. Il est parfait pour les stations météorologiques éloignées, les systèmes de contrôle de l'environnement à la maison et les systèmes de surveillance de la ferme ou du jardin.

Voici les plages et la précision du DHT11 :

- Humidity Range: 20-90% RH
- Humidity Accuracy: $\pm 5\%$ RH
- Temperature Range: 0-50 °C
- Temperature Accuracy: $\pm 2\%$ °C
- Operating Voltage : 3V to 5.5V

Qu'est-ce que l'humidité relative ?

Le DHT11 mesure l'humidité relative. L'humidité relative est la quantité de vapeur d'eau dans l'air par rapport au point de saturation de la vapeur d'eau dans l'air. Au

point de saturation, la vapeur d'eau commence à se condenser et à s'accumuler sur les surfaces formant la rosée.

Le point de saturation change avec la température de l'air. L'air froid peut contenir moins de vapeur d'eau avant d'être saturé et l'air chaud peut contenir plus de vapeur d'eau avant d'être saturé.

La formule pour calculer l'humidité relative est :

$$RH = \left(\frac{\rho_w}{\rho_s} \right) \times 100\%$$

RH : Relative Humidity

ρ_w : Density of water vapor

ρ_s : Density of water vapor at saturation

L'humidité relative est exprimée en pourcentage. À 100% d'humidité relative, la condensation se produit et à 0% d'humidité relative, l'air est complètement sec.

Comment le DHT11 mesure l'humidité et la température ?

Le DHT11 détecte la vapeur d'eau en mesurant la résistance électrique entre deux électrodes. Le composant de détection d'humidité est un substrat contenant de l'humidité avec des électrodes appliquées sur la surface. Lorsque la vapeur d'eau est absorbée par le substrat, les ions sont libérés par le substrat, ce qui augmente la conductivité entre les électrodes. La variation de résistance entre les deux électrodes est proportionnelle à l'humidité relative. Une humidité relative plus élevée diminue la résistance entre les électrodes, tandis qu'une humidité relative plus faible augmente la résistance entre les électrodes.

Le DHT11 mesure la température avec un capteur de température NTC (thermistance) monté en surface intégré à l'appareil.

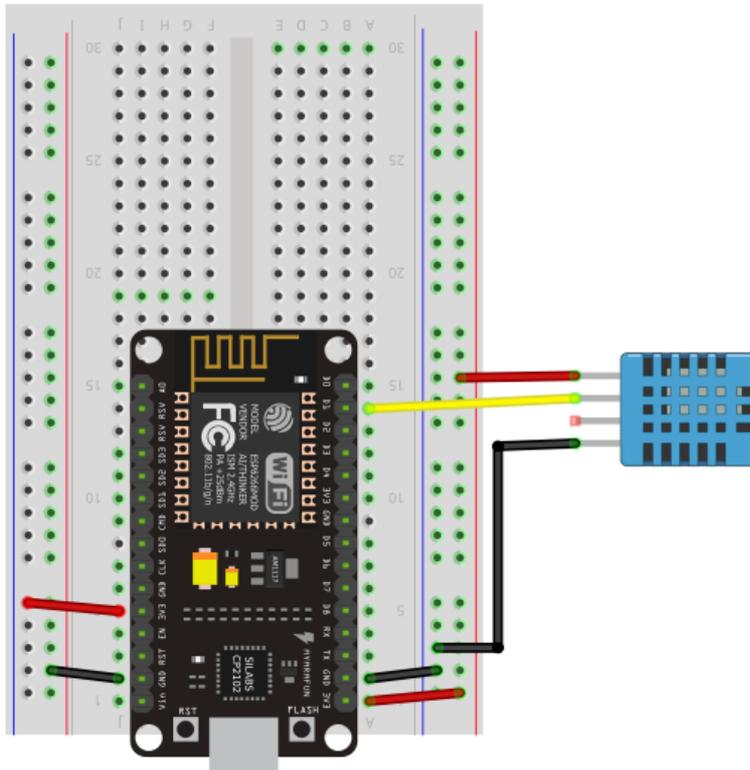
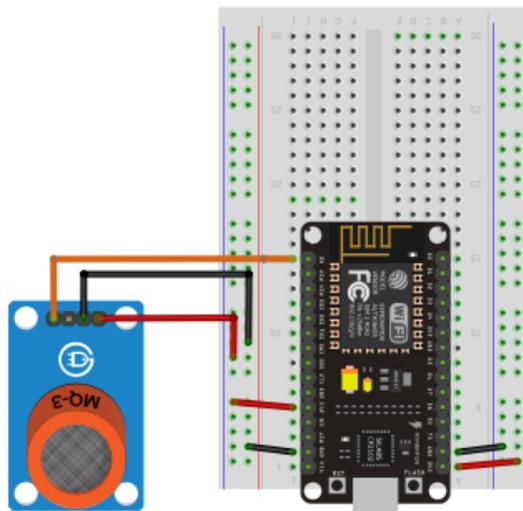


Figure III.6 : Branchement ESP8266-12E/DHT

III.6.1.5.2. Capteur de gaz MQ-2

Le capteur de gaz MQ-2 peut être utilisé pour la détection des fuites de gaz dans le site (la fumée du feu, l'isobutane, le propane et le gaz naturel liquéfié). La sensibilité



peut être réglée dans le programme.

Figure III.7 : Branchement ESP8266-12E/MQ-2

III.6.1.5.3. Capteur de Flamme

Ce capteur est sensible au rayonnement infrarouge émis par les flammes d'un foyer ainsi qu'à la présence du CO₂ résultant.

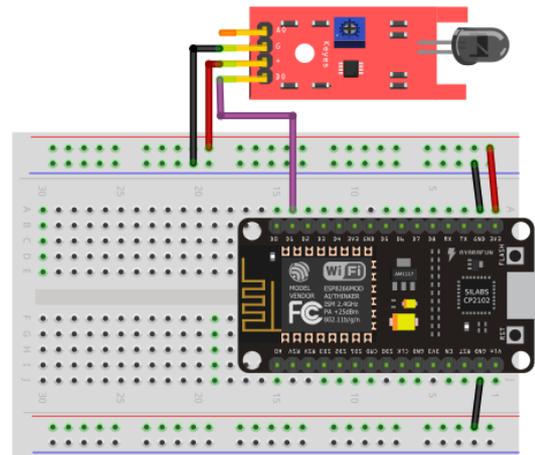


Figure III.8 : Branchement ESP8266-12E/Capteur de flamme

III.6.1.5.3. Capteur d'humidité du sol

Ce capteur d'humidité peut être utilisé pour détecter l'humidité du sol ou déterminer s'il y a de l'eau autour du capteur. Laissez les plantes de votre jardin solliciter l'aide de l'homme. Ils peuvent être très faciles à utiliser, il suffit de l'insérer dans le sol puis de le lire. Avec l'aide de ce capteur, il sera possible de faire en sorte que la plante vous rappelle : hé, j'ai soif maintenant, donnez-moi de l'eau s'il vous plaît.

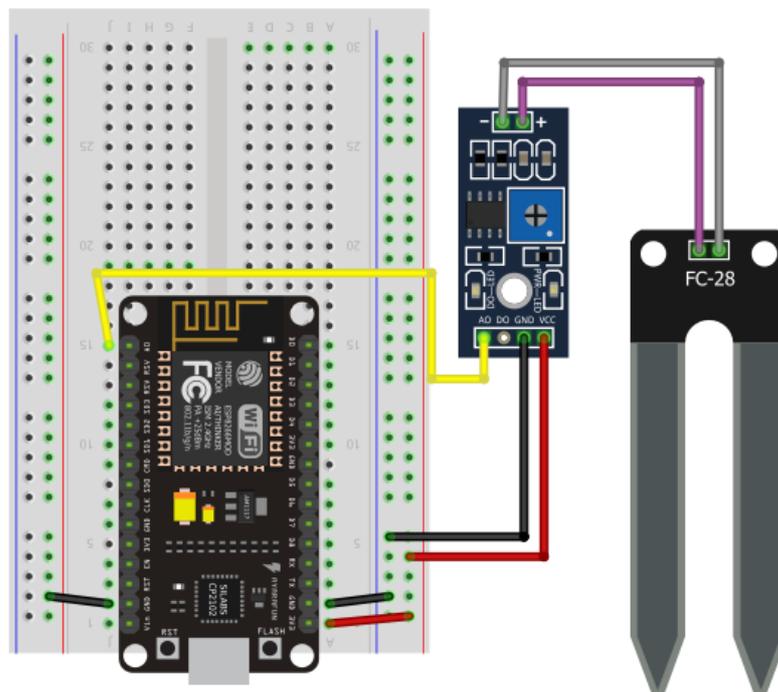


Figure III.9 : Branchement ESP8266-12E/Humidité du sol

III.6.1.5.4. Servomoteur

Un servomoteur est un dispositif capable de maintenir une opposition à un effort statique et dont la position est vérifiée en continu et corrigée en fonction de la mesure. C'est donc un système asservi.

III.6.1.5.5. Relais

Un relais est un organe électrique permettant de dissocier la partie puissance de la partie commande : il permet l'ouverture et la fermeture d'un circuit électrique par un second circuit complètement isolé et pouvant avoir des propriétés différentes.

III.6.1.5.6. Photorésistance LDR

Une photorésistance est une résistance qui varie en fonction de la lumière qu'elle capte. Le modèle qu'on dispose est une photorésistance qui varie d'environ $700K\Omega$ dans le noir à 400Ω au soleil ; cette résistance diminue en fonction de la lumière captée.

L'utilisation est diverse et variée :

- Mesure de la lumière ambiante pour une station météo.
- Détection de la lumière dans une pièce.
- Eclairage extérieur.
- Etc.

III.6.2.1.1. Structure du programme Arduino

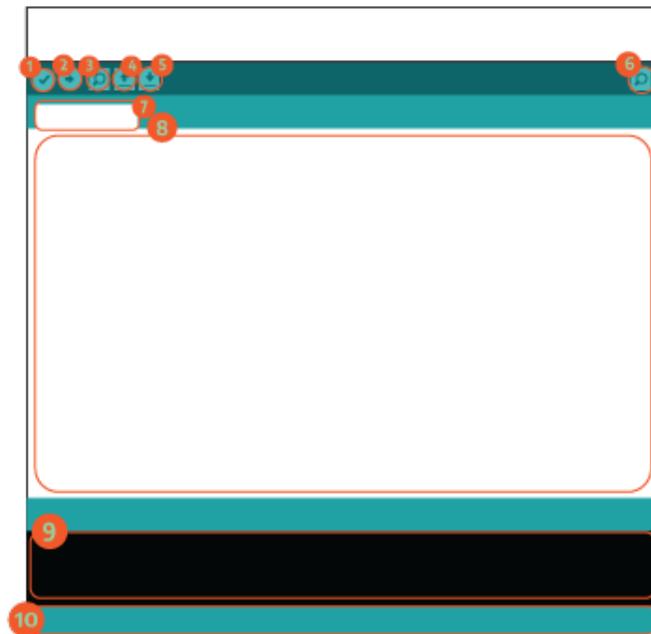


Figure III.11 : Description de l'interface Arduino IDE

1. Bouton : compiler et vérifier le code.
2. Bouton : compiler et télécharger e code vers la carte.
3. Bouton : créer un nouveau sketch.
4. Bouton : ouvrir un projet.
5. Bouton : sauvegarder le projet ouvert.
6. Bouton : ouvrir le moniteur série (pour le debug).
7. Onglet en cours d'utilisation.
8. Espace ou le code sera écrit, se décompose en deux partie : la fonction **setup(){}**, qui se lance avec le démarrage du carte, la fonction **void loop(){}**
La fonction dont la carte exécutera en répétition.
9. Zone des erreurs, info sur le téléchargement.
10. Type de la carte qui on travail avec.

Injection du programme

Avant de télécharger le programme dans une carte, il est nécessaire de sélectionner le type de cette carte, ainsi que le numéro du port USB utilisé.

III.6.2.2. ANDROID

La deuxième partie de ce projet consiste à créer une application servant à contrôler la partie Hardware, ainsi que de recevoir les données des capteurs.

Cette application a été créée avec le logiciel Android Studio, en utilisant le langage de programmation JAVA pour gérer les événements de l'application, et le XML pour créer l'interface utilisateur.

III.6.2.2.1. Présentation de l'interface

III.6.2.2.1.1. Interface des actionneurs

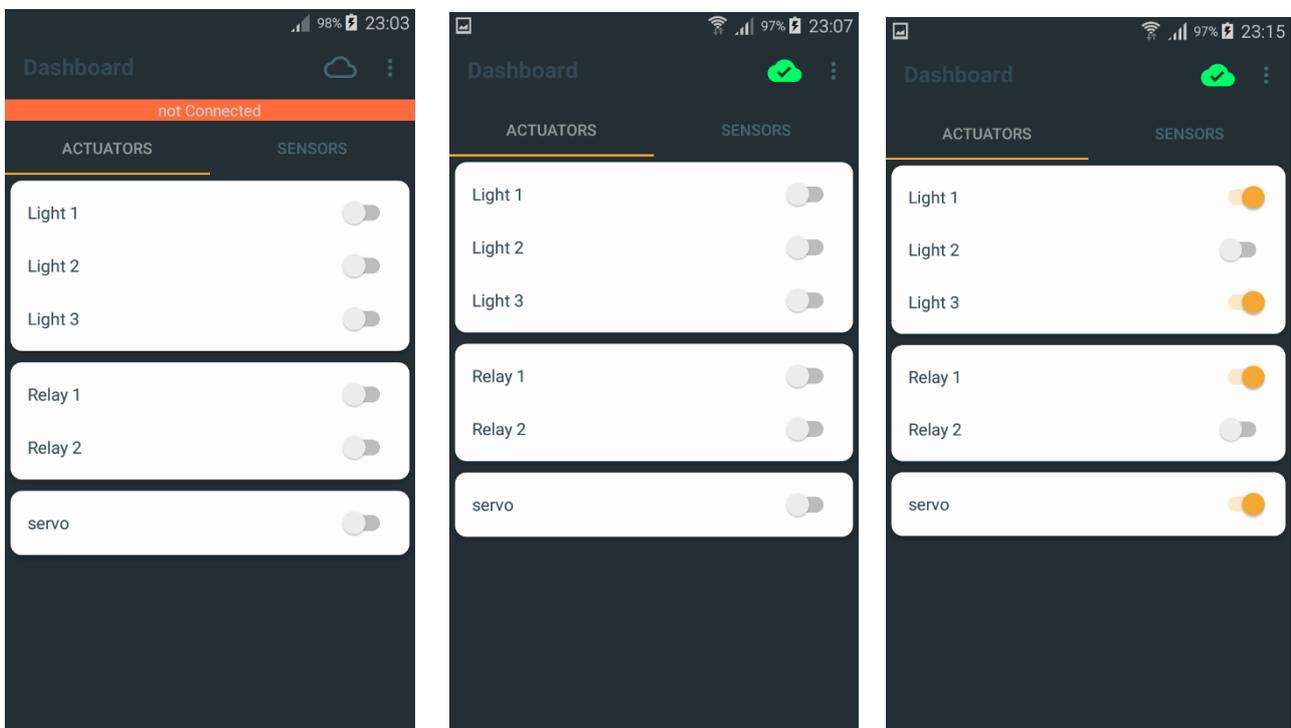


Figure III.12 : Interface d'actionneur

Une fois connectée à Internet, l'utilisateur peut contrôler les actionneurs du site, comme les lumières dans chaque pièce. La figure ci-dessus représente le fragment des actionneurs.

III.6.2.2.1.2. Interface des capteurs

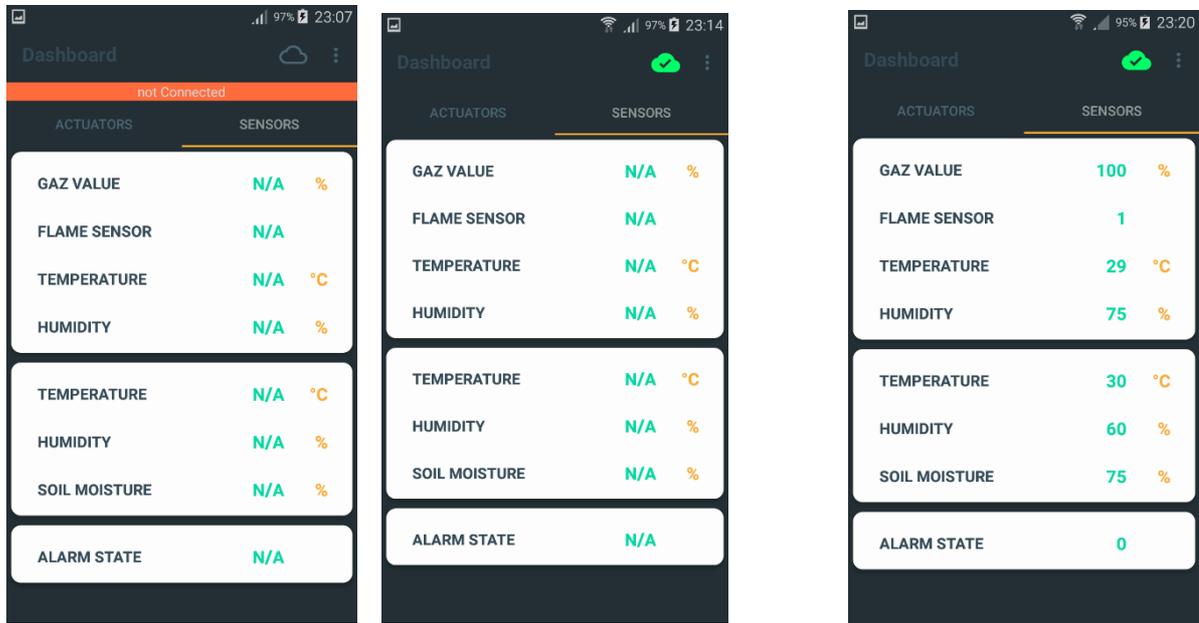


Figure III.13 : Interface des capteurs

La figure ci-dessus représente le fragment du capteur de site, ainsi que la réception des valeurs émanant des capteurs.

III.7. Conclusion

Dans ce chapitre, nous avons décrit les parties matérielle et logicielle de notre système IoT qui permet de contrôler notre maison intelligente. Dans la partie matérielle, nous avons présenté tous les composants utilisés tels que DHT11, DHT22, ESP8266-12E, etc. La partie logicielle concerne en premier lieu la présentation du logiciel Arduino puis les différentes interfaces de l'application mobile.

Conclusion générale

Conclusion Générale

Notre étude du système impliqué dans l'implémentation de maison connectée nous a permis de mieux comprendre les composants et la technologie concernés par ce domaine de l'Internet des objets. Elle nous a introduit à l'environnement mobile et aux applications multiplateformes ainsi qu'au monde de open hardware. La réalisation a été initiée par une mise en évidence de la problématique, l'objectif, puis nous avons établi une analyse de notre application.

Que ce soit pour une maison intelligente ou un autre projet d'informatique embarqué, la connaissance de l'environnement Arduino est nécessaire pour implanter ce genre de projet. Nous avons par conséquent dans le dernier chapitre, présenté l'un des types de carte électronique ainsi que leur environnement logiciel permettant de les programmer.

L'électronique commence à se démocratiser avec les concepts de l'open hardware et de l'Arduino en essayant d'éviter les long discours trop techniques et en réduisant cela à des bibliothèques prêtes à l'emploi, comme par exemple l'intégration des capteurs DHT ou le servomoteur.

Bien évidemment, des améliorations futures peuvent être apportées à ce projet pour qu'il soit versatile, plus fiable, et adaptable. En perspectives nous prévoyons :

- Différentes interfaces adaptées à chaque type de terminal (Smartphone, Tablette, Desktop, etc.).
- Amélioration de l'interface d'utilisateur en personnalisant le design de l'application.
- Ajout de l'option de personnalisation de l'application selon le besoin de l'utilisateur.
- Intégration d'un système de notification par exemple alerter l'utilisateur quand il y aura une fuite de gaz.

Bibliographie

Bibliographie

- [1] <https://www.intechopen.com/books/smartphones-from-an-applied-research-perspective/smartphone-the-ultimate-iot-and-ioe-device#B24>
- [2] L'INTERNET DES OBJETS - Les principaux protocoles M2M et leur évolution vers IP – p.1
- [3] <https://www.intechopen.com/books/smartphones-from-an-applied-research-perspective/smartphone-the-ultimate-iot-and-ioe-device>
- [4] Designing the Internet of Things
- [5] web Technologies for the Internet of Things – HUANG, Fuguo – p.23
- [6] <https://dzone.com/articles/iot-systems-sensors-and-actuators>
- [7] Foundational Elements of an I.o.T Solution. P.51-52
- [8] <https://www.intechopen.com/books/smartphones-from-an-applied-research-perspective/smartphone-the-ultimate-iot-and-ioe-device>
- [9] i.o.t European Research Cluster on the Internet of Things, p.4-8
- [10] i.o.t enabling technologies,platforms, and use cases, p.10-14
- [11] <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5087432/>
- [12] lot beyond the hype : research, innovation and deployment, Chap.3,p.15
- [13] Smartphone: The Ultimate IoT and IoE Device. p.156.
- [14] Khan MH, Shah MA. Survey on security threats of smartphones in Internet of Things. In: Proceedings of the International Conference on Automation and Computing (ICAC); 7-8 September; University of Essex Wivenhoe Park Colchester, UK. 2016. DOI: 10.1109/IConAC.2016.7604979
- [15] Smartphone: The Ultimate IoT and IoE Device. p.156.
- [16] Internet of Things From Hype to Reality_ The Road to Digitization-Springer International Publishing , p.7 (1.2 IoT Reference Framework)
- [17] Getting started with iot, p. 30-35.