REPUBLIQUE DU SENEGAL

Un Peuple – Un But – Une Foi

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE ET DE L'INNOVATION

UNIVERSITE GASTON BERGER DE SAINT-LOUIS

U.F.R DE SCIENCES APPLIQUEES ET DE TECHNOLOGIE

SECTION DE PHYSIQUE APPLIQUEE

Mémoire de fin d'études pour l'obtention du

Master Ingénierie en Electronique et Télécommunications (MIETEL)

Sujet : Internet des Objets (IoT) Et Enjeux de Sécurité

Présenté par :

Melle Ndéye Khady DIAGNE

Sous la direction de :

Dr. Chérif DIALLO

Jury :

Président :	M. Abdou Karim DIALLO
Examinateur :	M. Abdou Karim MBODJI
Examinateur :	M. Dame DIONGUE
Examinateur :	M. Mahamadou TRAORE
Encadreur :	M. Chérif DIALLO

Année Académique 2016/2017

REMERCIEMENTS

Je remercie d'abord mon créateur Allah (SWT) de m'avoir permis d'arriver au terme de ce mémoire en vie et en bonne santé.

Mes prières sur le prophète Muhammad que la paix et la bénédiction d'Allah soient sur lui.

Je tiens à remercier particulièrement mon professeur et encadreur Dr Cherif Diallo, qui n'a ménagé aucun effort pour la réussite de ce mémoire.

Je remercie également l'ensemble du corps enseignant et administratif de l'université Gaston Berger de Saint-Louis du Sénégal. Et enfin, un grand merci aux membres du jury pour leur évaluation et l'honneur qu'ils m'octroient par leur présence.

DEDICACES

Je dédie ce travail à ma mère qui se trouve être ma référence, ma raison de vivre, mon idole. Sans elle je ne serai même pas arrivée à ce niveau d'étude. Elle a été toujours présente pour moi, et pour tous ses enfants.
Son courage, sa bonté, son amour, et surtout sa piété m'épateront toujours.
Qu'Allah la garde près de nous encore plus longtemps parce qu'elle est notre lumière.

Je le dédie à mon père qui ne se lasse jamais de nous conseiller sur le chemin a emprunté pour réussir ; je le porte dans mon cœur et je prie Dieu pour qu'il ait une longue vie avec beaucoup de bonheur.

Je le dédie aussi à mes sœurs, mon frère, mes cousins et cousines, mes tantes, mes oncles et toute ma famille.

Je n'oublie pas ma deuxième famille à savoir mes amies, mes camarades de classe, mes collègues, vous m'avez beaucoup encouragé et le fait de vous dédié ce travail n'est qu'un petit geste le comparant à tout ce que vous méritez.

SIGLES ET ABREVIATIONS

IoT: Internet of Things

RFID: Radio Frequency Identification

Wi-Fi: Wireless-Fidelity

LPWAN: Low-Power Wide-Area Network

ISM: Industriel, Scientifique, Médical

SoC: System-on-Chip

LoRa: Long Range

BLE: Bluetooth Low Energy

MQTT: Message Queuing Telemetry Transport

IIoT: Industrial Internet of Things

PAN: Personal Area Network

LAN: Local Area Network

WAN: Wide Area Network

MAN: Metropolitan Area Network

IPv6: Internet Protocol version 6

NFC: Near Field Communication

3GPP: 3rd Generation Partnership Project

ETSI: European Telecommunications Standards Institute

GSM: Global System for Mobile communications

UMTS: Universal Mobile Telecommunications System

LTE: Long Term Evolution

EC-GSM: Extended Coverage GSM

ISO: International Organization for Standardization

LTE-M: LTE for Machines

NB-IoT: Narrowband IoT

MAC: Medium Acces Control

OID: Object IDentifiers

SIM: Subscriber Identity Module

MS-ISDN: Mobile Station ISDN Number

ICANN: Internet Corporation for Assigned Names and Numbers

RIPE NCC: Réseaux IP Européens - Network Coordination Centre

IETF: Internet Engineering Task Force

SNO: Sigfox Network Operators

ONS: Object Name System

DNS: Domain Name Server

AVANT-PROPOS

L'UFR de Sciences Appliquées et de Technologie de L'université Gaston BERGER de Saint-Louis propose un diplôme de Master d'Ingénierie en Electronique et Télécommunications (MIETEL) adapté aux besoins en ressources humaines compétentes dans les domaines des NTIC qui reposent sur la convergence des technologies, des services, des systèmes et des réseaux.

Pour l'obtention de ce diplôme, les étudiants doivent présenter un mémoire à la fin de la formation.

C'est dans cette optique que ce présent mémoire intitulé «l'internet des objets et enjeux de sécurité » a été réalisé.

LISTE DES TABLEAUX

TABLEAU 1: caractérisques des réseaux PAN et WAN 32
TABLEAU 3 : bande ISM 36

LISTE DES FIGURES

FIGURE 1: Lampe DAL.....15
FIGURE 2: Karotz.....15
FIGURE 3: Système IoT.....19
FIGURE 4 :1er exemple d'architecture d'une solution connectée.....20
FIGURE 5 : 2eme exemple d'architecture d'une solution connectée 20
FIGURE 6: les différents types de réseaux dans l'internet des objets.....22
FIGURE 7: illustration de la domotique.....23
FIGURE 8: illustration d'une smart city.....24
FIGURE 9: voiture connectée.....25
FIGURE 10: illustration de l'e-santé.....26
FIGURE 11: laptop et périphériques bluethooth 27
FIGURE 12: industrie 4.0.....28
FIGURE 13: technologies de connectivité 30
FIGURE 14: Réseau LPWAN 34
FIGURE 15: Cyberattaque contre un équipement médical connecté 57
FIGURE 16: logo Proteus.....68
FIGURE 17:fonctionnement de l'IoT builder 69
FIGURE 18: Interface d'acueil de proteus.....70
FIGURE 19: fenêtre d'enregistrement du nom du projet.....70
FIGURE 20: fenêtre pour le choix du design de schematic 71
FIGURE 21: fenetre pour le choix de la création de PCB.....71
FIGURE 22 : fenêtre pour le choix de la carte et de la manière de coder 72
FIGURE 23: fenêtre de résumé des choix effectués.....73
FIGURE 24: fenêtre du « schematic capture » 73
FIGURE 25: fenetre du « visual designer ».....74
FIGURE 26: fenêtre des périphériques.....74
FIGURE 27 : fenêtre de "schematic capture "avec le périphérique 75
FIGURE 28: fenêtre du choix des boutons.....74
FIGURE 29: fenêtre du choix du thermomètre 75
FIGURE 30: fenêtre du choix du repère
FIGURE 31: fenêtre du choix du message reset.....76
FIGURE 32: fenêtre de 'main controls'.....76
FIGURE 33: fenêtre de 'main controls' avec les 'iot controls''.....76
FIGURE 34: Les Algorigrammes 77
FIGURE 35: Bouton minute actionné.....77
FIGURE 36: Bouton heure actionné.....78

FIGURE 37: Bouton jour actionné……77
FIGURE 38: Bouton reset actionné 78
FIGURE 39: Reset effectué 78
FIGURE 40: Fenêtre d'accueil de l'IoT controller……77
FIGURE 41: Menu de l'IoT controller 79
FIGURE 42: Fenêtre d'ajout d'adresse IP 79
FIGURE 43: L'interface graphique sur un smartphone..... 80

TABLE DES MATIERES

RESUME 12

INTRODUCTION 13

CHAPITRE 1: GENERALITE SUR LES OBJETS CONNECTES

I. HISTORIQUE DES OBJETS CONNECTES 14

II. DEFINITION 16

1. QU'EST-CE-QU'UN OBJET 16
2. QU'EST-CE-QUE L'INTERNET DES OBJETS 16
3. LES QUATRE POINTS FONDAMENTAUX DE L'IOT 17

III. ECOSYSTEME DES OBJETS CONNECTES 19

1. INFRASTRUCTURE D'UNE SOLUTION CONNECTEE 19
2. PLATEFORMES MATERIELLES 20
3. MICROLOGICIELS ET SYSTEMES D'EXPLOITATION 21

IV. QUELQUES APPLICATIONS DE L'INTERNET DES OBJETS 22

1. LA DOMOTIQUE 22
2. LA SMART CITY 23
3. AUTOMOBILE 4.0 24
4. E-SANTE 25
5. PC ET PERIPHERIQUES BLUETOOTH 26
6. INDUSTRIE 4.0 27

CHAPITRE 2: DEVELOPPEMENT DES OBJETS CONNECTES

I. LES INFRASTRUCTURES DE CONNECTIVITE 29

1. FOISONNEMENT DE TECHNOLOGIES 29
   1.1. Des Réseaux Non Opérés A Portée Locale Ou Ultra Locale 30
   1.2. Réseaux opérés au déploiement étendu 32
   1.3. Réseaux filaires 34
2. ELARGISSEMENT DE LA GAMME DES BESOINS 35

II. LES RESSOURCES RARES 35

1. AUTORISATION D'UTILISATION DES FREQUENCES 35
   1.1. Les fréquences libres (bandes ISM) 35
   1.2. Fréquences soumises à une autorisation individuelle 36
2. DISPONIBILITE DES FREQUENCES 37
3. MULTIPLICITE DES MODES D'ADRESSAGE 39

1.1. RESEAUX CELLULAIRES 39
1.2. Réseaux LPWAN 40
1.3. Identifiants RFID et NFC 40
1.4. Adressage IP 40
III. OUVERTURE AU SEIN DES IOT 41
1. L'ENJEU DE L'OUVERTURE ET DE L'INTEROPERABILITE 41
2. UNE COURSE AUX STANDARDS AU NIVEAU DES COUCHES BASSES 43
3. UNE AUTRE COURSE AUX STANDARDS AU NIVEAU DES COUCHES 44
4. DES ENJEUX DE FLUIDITE 44
CHAPITRE 3: EXPOSITION DES SYSTEMES D'OBJETS CONNECTES
I. VULNERABILITE 46
1. ÉCHELLE DE L'INTERNET DES OBJETS 46
2. HETEROGENEITE DE L'INTERNET DES OBJETS 48
3. INFLUENCE DU MONDE PHYSIQUE SUR L'INTERNET DES OBJETS 50
4. SECURITE ET VIE PRIVEE 52
II. LES ATTAQUES 54
1.1. Les attaques contre les objets connectes eux-mêmes 54
1.2. Les attaques réalisées au travers des objets connectes 55
1.3. Les attaques contre les réseaux et protocoles de communication de l'iot 56
2. LES FUTURES CYBERATTAQUES 57
CHAPITRE 4: METHODES DE SECURISATION D'UNE INFRASTRUCTURE IoT
I. MECANISMES DE DEFENSES ASSOCIES AUX IOT 60
1. MECANISMES TECHNIQUES 60
1.1. La sécurité physique de l'objet 61
1.5. Les protocoles de communication 61
1.6. Sécurité applicative et système 62
2. LA LABELLISATION 63
II. METHODES DE SECURISATION D'UNE INFRASTRUCTURE IOT 64
1. COTE FABRICANT/INTEGRATEUR DE MATERIEL IOT 64
2. COTE DEVELOPPEUR DE SOLUTIONS IOT 64
3. COTE RESPONSABLE DU DEPLOIEMENT DE SOLUTIONS IOT 65
4. COTE OPERATEUR DE SOLUTIONS IOT 65
CHAPITRE 5: DEVELOPPEMENT D'UN SYSTEME IOT SUR PROTEUS 8.7

I. FONCTIONNEMENT DE L'IoT BUILDER 68
II. ENONCE DU PROJET 69
III. DETALS DU PROJET 69
IV. CONCLUSION 81
BIBLIOGRAPHIE 82

RESUME

L’expression "internet des objets " a été inventée par Kevin Ashton; elle peut être définie comme étant une interconnexion d'objets physiques ou virtuels.
Ce système doit impérativement intégrer ces différents composants: le capteur, la connectivité, le traitement de l'information et une interface d'utilisation.
Ainsi, il y a deux architecture qu'on pourrait utiliser: celle ayant comme passerelle un smartphone et celle utilisant une antenne relai.

Du côté matériel la plateforme utilisée par l'IoT est le System-on-chip qui se trouve être une puce ou on met le programme qui gère les données reçues par le capteur.

Pour la transmission de ces données on utilise soit les réseaux longue portée (lora, sigfox, les réseaux cellulaires), les réseaux courte portée (bluetooth, zigbee, NFC, Z-Wave etc.) ou les réseaux filaire; ce qui nous fait comprendre qu'il y'a un foisonnement de technologie avec les IoT.

De ce fait, pour permettre à l'utilisateur d'être plus à l'aise il nous faudrait une certaine ouverture et une certaine interopérabilité entre les systèmes, c'est à dire pour n’importe quel objet connecté il ne doit pas y avoir un changement de technologie qui serait assez contraignant vu du côté de l'utilisateur.

Cependant, face à l'augmentation considérable du nombre d'objet connecté, on note une certaine vulnérabilité vis à vis de l'adressage des objets, vis à vis de l’hétérogénéité du système qui empêche les objets d’interagir en toutes circonstances, mais aussi vis à vis des paramètres physiques qui peuvent interférer sur les informations à transmettre.

Il faudrait également savoir qu'avec la collecte et le partage de données, l'IoT se trouvent être très vulnérable aux attaques soient liées à l'objet physique ou au réseau qui est le support de transfert des données.
Il devient alors vital d'essayer de trouver des moyens pour faire face à ces attaques; sur ce on doit déjà protéger physiquement l'objet et utiliser des protocoles sécurisés.
Par ailleurs, une conception de système de gestion de la variation de température est mise en place pour plus de compréhension sur le fonctionnement des systèmes IoT.

INTRODUCTION

L'Internet des objets est une révolution technologique de l'information et de la communication. Il décrit un monde composé d'équipements intelligents organisés en réseau pouvant être connectés entre eux mais aussi avec l'environnement extérieur. Cette évolution technologique génère de nouvelles formes de communication entre les objets du monde réel qui sont capables de percevoir et de partager des informations précises.

Ainsi Les objets connectés (Internet of Things ou IoT) peuvent donner l'impression de vivre dans un monde futuriste en nous donnant l'opportunité de mettre en place de nouvelles façons d'interagir avec les objets ; ce que l'internet tout seul ne permettait pas de faire car n'allant pas au-delà du monde électronique.

Beaucoup de secteurs seront touchés par cette avancée technologique, et le but principal sera de facilité nos moindre taches, de nous faire gagner énormément de temps mais également nous faire vivre dans un confort féerique.

Cependant c'est bien beau de s'arrêter juste sur l'aspect avantage des objets connectés, ce qui est loin d'être réaliste. Dès lors qu'on parle d'internet il est logique de penser aux données, et celles-ci vont être plus sensibles que jamais car étant directement recueillies de notre quotidien. De ce fait avec l'internet des objets la sécurité des données va devenir vitale.

C'est ainsi que dans notre étude nous allons essayer de remonter vers l'histoire des objets connectés pour avoir une compréhension plus assise sur celle-ci et c'est ce qui va constituer notre premier chapitre.

Dans le deuxième chapitre nous allons voir les différentes technologies qui peuvent être utilisées pour mettre en place une solution d'objets connectés.

Le troisième chapitre va nous conscientiser sur la fragilité d'une solution d'objets connectés, qui se trouve être une banque de données sensibles.

Toute fois des solutions ne vont pas manquer pour mettre en sécurité toutes ses informations confidentielles et c'est ce qui va nous servir de chapitre quatre.

CHAPITRE 1 : GÉNÉRALITÉ SUR LES OBJETS CONNECTÉS

I. HISTORIQUE DES OBJETS CONNECTES

Certains analystes font remonter l'histoire des objets connectés au XIXe siècle, époque de l'invention du télégraphe, le premier appareil électronique de radio-communication. L'homme a toujours alimenté de nombreuses réflexions sur les voies de communication entre eux et les objets.

En 1901, le célèbre inventeur et ingénieur Nikola Tesla (1856-1943), auquel l'entreprise automobile du même nom a voulu rendre hommage, pense un système de collecte de données, qu'il pourrait coder et qui diffuserait l'information à un dispositif tenu à la main, l'équivalent d'Internet sur les smartphones aujourd'hui. En 1926, il imagine « un monde où les habitants seraient reliés par des installations de communication sans fil. ». Ce sont les innovations autour de la problématique du partage de données qui sont la clé de voûte des rêves du « tout connecté ».

L'évolution de l'Internet des Objets est corrélée à celle d'Internet. Il faut ainsi attendre la fin du XXe siècle et l'invention du World Wide Web par Sir Tim Berners-Lee, l'Internet universel utilisé à présent, pour que la voie s'ouvre un peu plus à la réalisation d'objets connectés, dont les premiers, relatifs à la domotique, apparaissent alors.

En effet, l'histoire des objets connectés débute véritablement en 1999 lorsque Kevin Ashton, pionnier de la technologie RFID (Radio Frequency Identification: Technologie d'identification automatique), invente l'expression "***Internet des objets***". Cette même année, le concept naît aux États-Unis et particulièrement au MIT (*Massachusetts Institute of Technology*). Ce laboratoire est dédié à la création d'objets connectés à l'aide de l'identification par radiofréquence et les réseaux de capteurs sans fil.

L'Internet des objets (IoT) est apparu à l'issue de la mécanisation et de la standardisation, appliquée à l'automatisation du traitement du document et de l'information sur support matériel puis numérique. Il s'est rapidement diffusé avec la mondialisation. Peu à peu, les objets ont été modifiés (avec des puces RFID par exemple) ou conçus pour « parler le protocole IP », devenant des « objets connectés» reliés à des serveurs capables de communiquer entre eux.

Il faut tout d'abord connaître **Rafi Haladjian**, l'homme qui a créé en juin 1994 le premier opérateur internet en France : FranceNet, cédé à British Telecom en 2001.

Il se lance ensuite dans le monde de l'internet des objets et fonde la société Ozone, puis Violet qui a pour baseline « Let all things be connected ».Violet lancera le premier objet connecté **:** **la lampe DAL** en 2003.

Cette lampe wifi c'est vendue à une cinquantaine d'exemplaires à 790€ unité. La lampe est composée principalement de 9 voyants qui s'illuminent de différentes couleurs en fonction des "*événements*", d'un micro (a priori) et de capteurs de toucher. Elle propose différents services comme la météo, la pollution, des alertes google ou encore des "envois de messages de couleurs" par sms ou email (via un service dédié, la lampe ne reçoit pas les SMS directement).



FIGURE 1: Lampe DAL

Un peu plus tard, **en 2005** cette société lancera le **Nabaztag,** qui devint l'icône des objets connectés. Ce lapin connecté en hi-fi peut alors déjà lire des mails à haute voix, émettre des signaux visuels et diffuser de la musique. L'objet est aujourd'hui commercialisé sous le nom de **Karotz**.



FIGURE 2: Karotz

C’est néanmoins en 2007 que le phénomène des IoT a pris de l’ampleur, avec la démocratisation des Smartphones et la sortie du premier iPhone par Apple.
Nous vivons actuellement une rupture forte, telle une troisième révolution industrielle. Celle nous permettant de connecter Internet au moindre objet de notre quotidien. Ces objets génèrent un nombre de données exceptionnel, dont les perspectives d’exploitation apparaissent, sur le long terme, sans limite. Le sujet des datas est donc délicat et suscite des questions éthiques de l’ordre de la préservation de la vie privée.

II. DEFINITION

1. QU’EST-CE-QU’UN OBJET

Dans l'Internet des objets, un « objet » peut être une personne équipée d'un pacemaker, un animal de ferme qui porte une puce (transpondeur), une voiture qui embarque des capteurs pour alerter le conducteur lorsque la pression des pneumatiques est trop faible, ou encore tout objet naturel ou fabriqué par l'être humain auquel peuvent être attribuées une adresse IP et la capacité de transférer des données sur un réseau.

En effet on peut donc dire que les objets, les animaux et les personnes se voient attribuer des identifiants uniques, ainsi que la capacité de transférer des données sur un réseau sans nécessiter aucune interaction humain-à-humain ou humain-à-machine.

2. QU’EST-CE-QUE L’INTERNET DES OBJETS

D’après l’Union Internationale des Télécommunications : “ l’**I**nternet **d**es **O**bjets (**IoT**) est une infrastructure mondiale pour la société de l’information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l’information et de la communication interopérables existantes ou en évolution”.

En réalité, la définition de ce qu'est l'Internet des objets n'est pas figée. Elle recoupe des dimensions d'ordres conceptuel et technique.

- **D'un point de vue conceptuel:**

L’internet des objets caractérise des objets physiques connectés ayant leur propre identité numérique et capables de communiquer les uns avec les autres. Ce réseau crée en quelque sorte une passerelle entre le monde physique et le monde virtuel.

Certains définissent l'IoT comme des « objets ayant des identités et des personnalités virtuelles, opérant dans des espaces intelligents et utilisant des interfaces intelligentes pour se connecter et communiquer au sein de contextes d'usages variés ». D'autres font l'hypothèse que l'IoT représente une révolution car il permet de connecter les gens et les objets n'importe où, n'importe quand, par n'importe qui. Ces définitions, qui mettent l'accent sur la dimension ubiquitaire de l'IoT, personnifient les objets en leur attribuant intelligence et capacité de communiquer. Elles ne reflètent pas encore la dimension concrète liée aux usages de l'IoT.

- **D'un point de vue technique :**

Techniquement, l'IoT est une extension du système de nommage internet et traduit une convergence des identifiants numériques au sens où il est possible d'identifier de manière unifiée des éléments d'information numérique (adresses URL de sites web par exemple) et des éléments physiques.

Mais l'identification est directe grâce à l'utilisation d'un système d'identification électronique. Il n'y a pas besoin de saisir manuellement le code de l'objet. Le réseau s'étend jusqu'à lui et permet ainsi de créer une forme de passerelle entre les mondes physique et virtuel.

En résumé on peut dire que l'IoT consiste en l'identification numérique directe et normalisée (adresse IP, protocoles smtp, http...) d'un objet physique grâce à un système de communication sans fil qui peut être une puce RFID, Bluetooth ou Wi-Fi.

3. LES QUATRE POINTS FONDAMENTAUX DE L'IOT

Le système complet d'un objet connecté intègre quatre composants distincts :

-Des capteurs

-Une connectivité

-Un traitement de l'information

-Une interface utilisateur

- **Les capteurs**

Tout d'abord, les capteurs récoltent les données de leur environnement. Cela peut être une simple lecture de niveau de bruit comme une lecture complète d'un flux photo ou vidéo.

On utilise des capteurs, car ils peuvent souvent être regroupés ou faire partie d'un appareil qui fait beaucoup plus que juste sentir son environnement. Par exemple, votre téléphone est un

appareil qui possède plusieurs capteurs : caméra, accéléromètre, GPS, etc…), mais votre téléphone n'est pas juste un capteur.

Dans tous les cas, qu'il s'agisse d'un capteur autonome ou un appareil, la première étape est toujours la même : quelque chose capte les informations de son environnement.

- **Connectivité**

Ensuite, l'information est envoyée dans le cloud, mais elle a besoin d'un moyen d'y parvenir.Les capteurs/appareils peuvent être connectés au cloud au travers d'une variété de méthodes incluant : réseau cellulaire, satellites, WIFI, Bluetooth, les réseaux LPWAN (Low-Power Wide-Area Network) ou une connectivité directe à internet via ethernet.

Chaque option possède son lot de contrainte que ce soit en consommation d'énergie ou en bande passante. Choisir la meilleure connectivité dépend des fonctionnalités et de l'application de l'objet connecté. Au final, toutes les options offrent le même résultat : envoyer les informations dans le cloud.

- **Traitement de l'information**

Une fois l'information dans le cloud, des logiciels réalisent un traitement sur ces dernières.
Le traitement peut être très simple, comme vérifier si la température lu est comprise dans une fourchette acceptable définie précédemment. Il se peut que le traitement soit également très complexe, comme identifier un objet particulier au travers d'une vidéo lue par un ordinateur. Cette application est utilisée pour identifier des intrus dans une maison.
Mais finalement, que se passe-t-il si la température est trop haute ou trop basse ? Ou qu'il y a un intrus dans la maison ? C'est à ce moment que l'utilisateur entre en jeu.

- **Interface utilisateur**

L'information est tout d'abord rendue utile et lisible pour l'utilisateur final. Elle peut prendre vie sous forme d'alerte à l'utilisateur (email, sms, notification, etc…). Un SMS est envoyé à l'utilisateur lorsqu'un intrus est détecté dans la maison, par exemple.

Aussi, les utilisateurs disposent souvent d'une interface qui leur permet de vérifier de manière proactive dans le système. Par exemple, notre utilisateur va pouvoir voir un flux vidéo de l'intérieur de sa maison sur une application mobile ou une page web.

En fonction du champ d'application de l'objet connecté, le flux d'information n'est pas toujours un envoi à sens unique. L'utilisateur peut aussi être en mesure de déclencher une action

sur le système. Par exemple, l'utilisateur peut ajuster la température de la chambre froide lorsqu'il décèle une vague de chaleur grâce aux capteurs, directement depuis son téléphone.

D'autres actions sont déclenchées automatiquement. Ainsi, l'utilisateur peut sur certains systèmes créer des scripts qui se déclencheront grâce à des règles prédéfinies. Ainsi, au lieu de vous alerter directement, le système de l'objet connecté pourra alerter directement les autorités compétentes.

En résumé un système d'objet connecté est composé de capteurs ou d'appareils qui "dialogue" avec le cloud au travers d'une certaine connectivité. Une fois l'information relayée sur le cloud, des logiciels la transforme et la traite et peuvent éventuellement décider d'agir en conséquence du résultat obtenu.

Si une interaction utilisateur est requise ou s'il veut simplement se connecter au système, une interface utilisateur lui permet d'agir en fonction. Tous les ajustements ou actions qu'un utilisateur fait sur son interface sont ensuite envoyé dans la direction opposée via le système : depuis l'interface utilisateur, vers le cloud, et finalement vers les capteurs/appareils pour effectuer un changement.

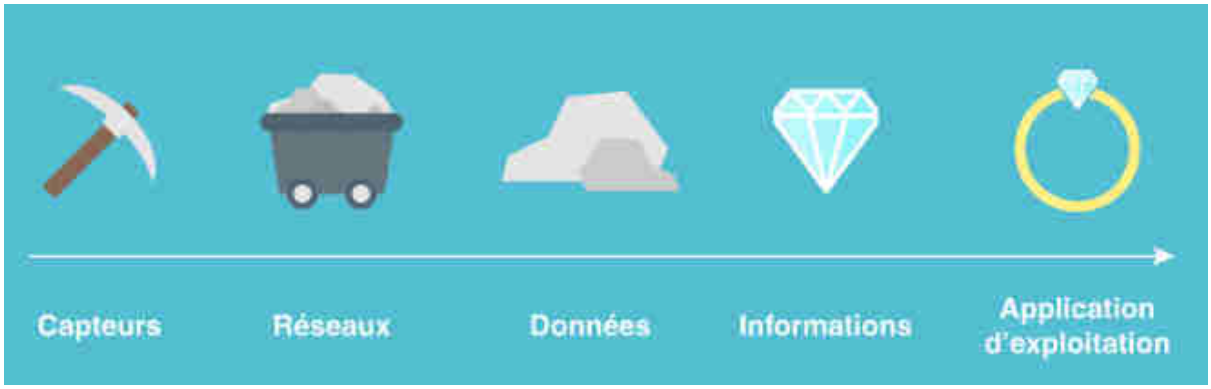


FIGURE 3: Système IoT

III. ECOSYSTEME DES OBJETS CONNECTES

1. INFRASTRUCTURE D'UNE SOLUTION CONNECTEE

L'infrastructure d'une solution connectée peut être perçue comme l'ensemble des ressources nécessaires au fonctionnement du service associé à l'objet connecté. Elle comprend en général l'objet connecté, disposant d'une interface de communication courte ou longue distance, une passerelle de communication, (fréquemment un smartphone ou une passerelle d'un opérateur

de communication), un service d'appui (tel qu'un serveur hébergé dans un Cloud), et souvent une application dédiée pour l'utilisateur (de type application mobile, portail Web, etc.).

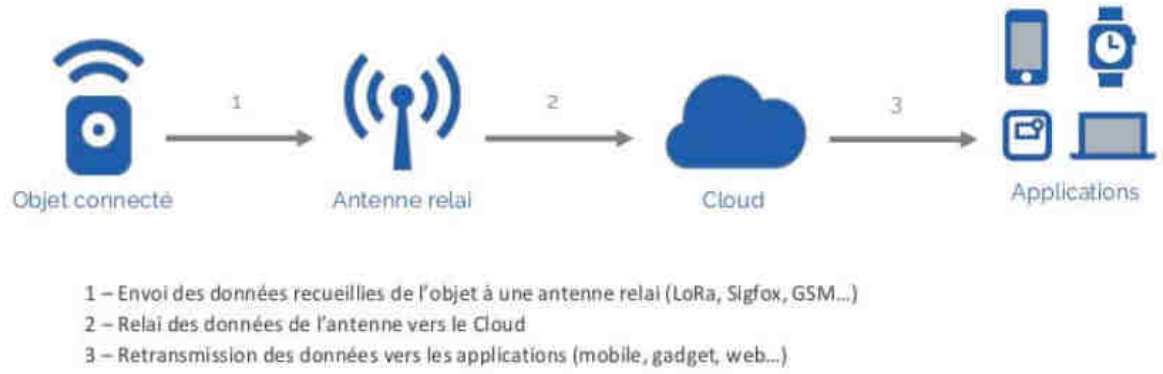


FIGURE 4 :1er exemple d'architecture d'une solution connectée



FIGURE 5 : 2eme exemple d'architecture d'une solution connectée

2. PLATEFORMES MATERIELLES

La grande majorité des objets connectés reposent sur une plateforme ou un agrégat de plateformes matérielles. Ces dernières se présentaient il y a quelques années sous forme de modules électroniques plus ou moins encombrants, fournissant les fonctionnalités nécessaires à l'équipement. Ces modules ont depuis évolué vers une puce électronique tout-en-un : le System-on-Chip ou SoC. Ces composants intégrés sont petits, réalisent tout un ensemble de tâches spécifiques et contiennent tout le nécessaire à leur fonctionnement : de la mémoire programmable, un micro-processeur ainsi que des circuits internes spécialisés.

Récemment, Intel a lancé son SoC Edison, un système complet un peu plus grand qu'un timbre-poste, intégrant les technologies Bluetooth 4.0, WiFi et 40 entrées/sorties programmables, avec pour objectif de fournir un SoC facilitant le prototypage et la mise sur le marché.

Il existe un grand nombre de System-on-Chip, la plupart spécialisés dans différents protocoles de communication : Bluetooth Smart, WiFi, ZigBee, RFID, protocoles propriétaires tels que ceux utilisés dans les souris et claviers sans fil, et même des puces intégrant des émetteurs LoRa et Sigfox. La mémoire intégrée permet d'y insérer un micrologiciel mettant en œuvre la logique métier, et pouvant même interagir avec des composants externes supplémentaires grâce à des ports d'entrée/sortie. Les plus populaires sont notamment ceux reposant sur des architectures de processeurs reconnues et renommées, telles que la famille de processeurs ARM Cortex, MIPS ou encore Intel 8051.

3. MICROLOGICIELS ET SYSTEMES D'EXPLOITATION

La couche logicielle d'un équipement connecté varie selon les plateformes matérielles. Certains SoC spécialisés, tels quelques-uns de ceux conçus par Texas Instruments ou Marvell par exemple, se contentent d'exécuter une application composée d'un programme unique. Ce logiciel (ou micrologiciel) ne constitue pas un système d'exploitation. Il est au contraire spécialisé et dédié à un ensemble de tâches bien définies.

4. INFRASTRUCTURES DE COMMUNICATIONS

Il existe deux grandes catégories de réseaux qui permettent de transmettre des informations entre plusieurs objets connectés avec une consommation maîtrisée et minimale d'énergie : les réseaux longue portée (Low-Power Wide-Area Network, LPWAN) et les réseaux à courte portée. Au sein de chacune de ces catégories, plusieurs réseaux concurrentiels existent.

Les réseaux longue portée sont capables de faire transiter des données d'un équipement à un autre ou à destination d'un service d'appui sur Internet sur de vastes distances (de l'ordre du kilomètre). Dans cette catégorie, on trouve tout d'abord les technologies cellulaires qui sont fournis par les opérateurs de télécommunication et qui ont comme avantage de transférer d'importantes quantités de données. Ils sont en revanche plus gourmands en énergie que les autres réseaux longue portée, tels que LoRa ou Sigfox qui sont réputés peu énergivores.

Les réseaux à courte portée permettent de transférer des données sur de faibles distances, ainsi ils sont beaucoup utilisés dans la domotique.

Un bracelet connecté n'est jamais très loin du téléphone avec lequel il échange ses données. Parmi ces réseaux on retrouve notamment le protocole Bluetooth Low Energy (BLE), principalement destiné aux objets connectés pour lesquels le besoin énergétique est faible ; le MQTT qui est particulièrement adapté pour l'utilisation d'une très faible bande passante; ou encore Z-Wave et ZigBee, deux protocoles de communication dédiés à la domotique.

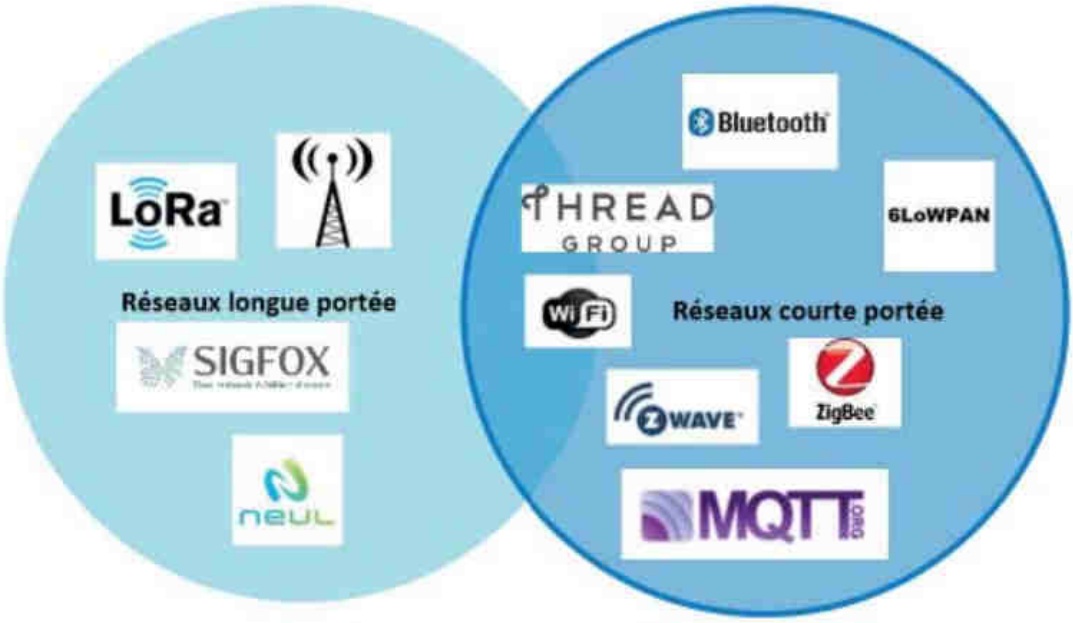


FIGURE 6: les différents types de réseaux dans l'internet des objets

IV. QUELQUES APPLICATIONS DE L'INTERNET DES OBJETS

1. LA DOMOTIQUE

La domotique ou maison connectée, représente les usages de l'Internet des Objets dans une maison.

Grâce à la domotique, les tâches quotidiennes sont maintenant automatisées donc simplifiées.

Les entreprises pionnières telles que Nest, Netatmo ou encore Sense ont créés des écosystèmes d'objets communicants qui permettent de centraliser le contrôle des différents systèmes de votre maison.

En vous équipant de leurs produits, vous pourrez optimiser votre consommation d'eau et d'énergie, sécuriser votre maison et déclencher vos appareils à distance (chauffage, garage, machine à laver).



FIGURE 7: illustration de la domotique

2. LA SMART CITY

La smart city a pour but d'améliorer la qualité de vies des habitants en utilisant les nouvelles technologies pour accroitre l'efficacité des services.

Plusieurs villes dans le monde sont déjà équipées de capteurs de stationnement, d'éclairages intelligents etc.

On peut citer comme exemple le boulevard Victor Hugo à Nice qui est équipé de plus de 200 capteurs qui permettent de collecter des données centralisées sur une plateforme Cisco. Les usages sont divers :

- Etre informé en temps réels des places de parking disponibles
- Réguler l'intensité des éclairages en fonction des mouvements détectés
- Maitriser les pics de pollution
- Alerter les services concernés sur le niveau de remplissage des conteneurs.

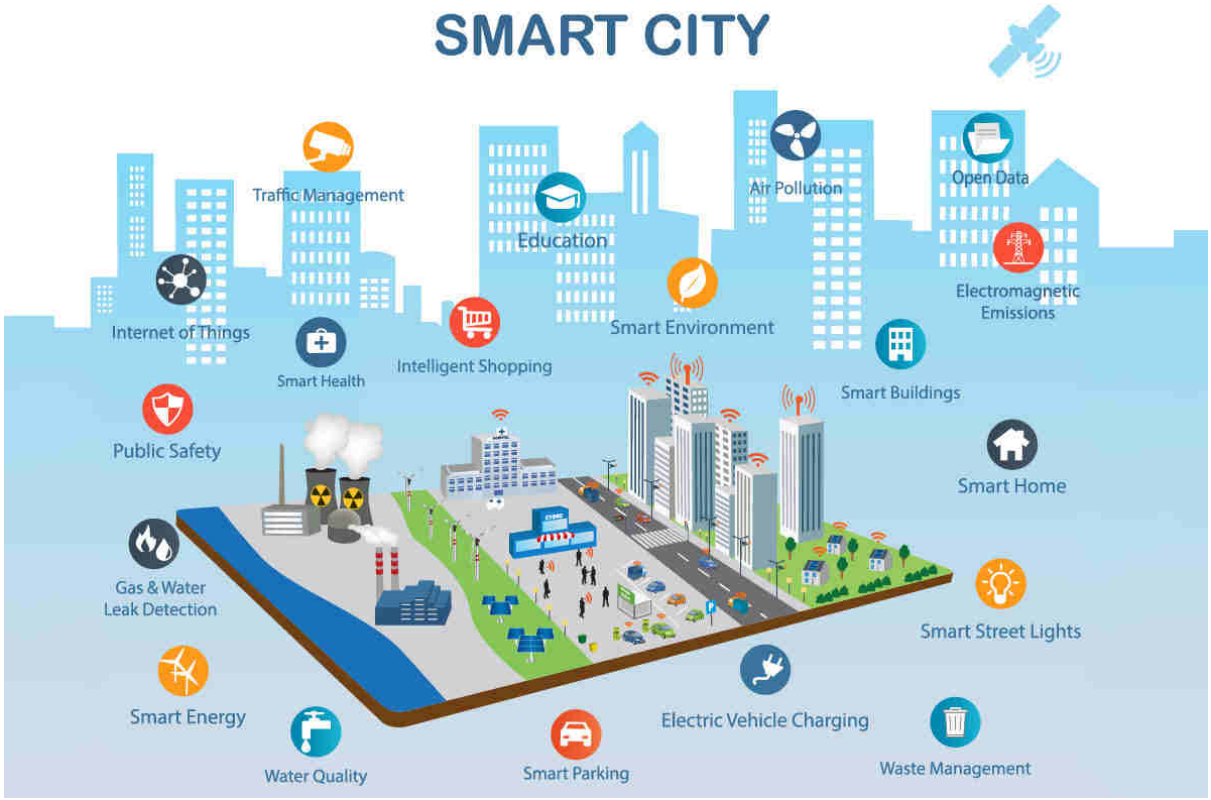


FIGURE 8: illustration d'une smart city

3. AUTOMOBILE 4.0

La conduite d'une automobile a toujours été un lieu de convergence très forte entre la sécurité, le confort et le plaisir.
L'internet des Objets est en train de modifier profondément l'industrie automobile en proposant des fonctions inédites aux utilisateurs.

La voiture de demain dépasse sa fonction utilitaire pour augmenter l'expérience utilisateur du client. Elle devient connectée, intelligente et autonome : c'est l'***automobile 4.0***.

Les centaines de capteurs intégrés dans les véhicules produiront des données exploitées par les entreprises pour améliorer l'expérience utilisateur : votre véhicule sera en mesure de vous soumettre des publicités et du contenu adaptés. Les assurances sont les premières à profiter des appareils de ***tracking*** en proposant des offres préférentielles suivant la conduite de l'usager.

Ces données pourront également être partagées avec d'autres véhicules : votre voiture pourra changer votre itinéraire si un « mauvais » conducteur est sur votre route.
Autonome, votre voiture pourra faire vos courses ou aller récupérer vos enfants à l'école.



FIGURE 9: voiture connectée

Les bénéfices et opportunités de l'IoT dans l'industrie automobile sont considérables. A terme, cela permettrait une réduction des accidents et une fluidification du trafic, une gestion des émissions de CO^2 et de nouvelles expériences marketing et commerciales.

4. E-SANTE

Suivez et analysez votre santé via des applications et des objets connectés en Bluetooth Smart. Les nouvelles technologies améliorent les procédés médicaux complexes en les rendant à la fois plus simples et plus fiables. Le Bluetooth permet ainsi de développer des applications facilitant l'analyse et le suivi médical du patient.

Les médecins peuvent désormais suivre un patient à distance et réagir en temps réel s'il y a une urgence. A terme, l'utilisation de ces nouveaux outils permettra la détection précoce d'éventuelles maladies et l'accroissement de l'efficacité des traitements proposés aux patients suivant l'historique des données fournies aux médecins.

Les trackers et applications Bluetooth Smart sont également très plébiscités chez les sportifs : bracelets connectés et montres connectées dominent le marché des objets connectés sport et fitness en se présentant comme de véritables coachs mobiles. Souvent reliés à une application mobile, ces objets transmettent et interprètent diverses données (nombre de pas effectués, vitesse de marche, mouvements etc.) et conseillent ses utilisateurs sur leurs objectifs et les moyens de les atteindre.

Ces objets connectés ont déjà conquis de nombreux sportifs professionnels (natation, tennis, football, golf…).



FIGURE 10: illustration de l'e-santé

5. PC ET PERIPHERIQUES BLUETOOTH

L'ère de la portabilité participe à la croissance des périphériques *Bluetooth.*

Grâce au succès des tablettes et des laptops, le marché des périphériques *Bluetooth* est en hausse. Ils permettent aux utilisateurs de se déplacer avec leur ordinateur sans décroitre leur productivité grâce à des claviers slim sans fils, des souris *Bluetooth* etc.

Les appareils musicaux (casques, écouteurs, enceintes) ou encore les imprimantes bluetooth augmentent l'expérience utilisateur en lui donnant la liberté de se déplacer sans être bloqué par les fils.



FIGURE 11: laptop et périphériques bluethooth

6. INDUSTRIE 4.0

Grâce aux objets connectés entre eux, l'industrie pourra créer des applications lui permettant de nombreuses économies.

Selon une étude, l'industrie investira entre 4 et 11 milliards de dollars dans l'Internet des Objets (IoT) d'ici 2025 : c'est le début de l'***industrie 4.0***, ou ***IIoT***.

L'Internet des objets est une vraie révolution, que ce soit dans la vie de tous les jours ou en situation professionnelle. Appliqué au secteur industriel, l'IoT permettra d'optimiser le processus logistique des entreprises ou encore d'optimiser la consommation d'énergie afin de réduire les coûts et les risques.

Grâce à un *beacon* (boitier munis de capteurs) déposés sur un emballage ou dans un camion, nous serons en mesure de tracer les déplacements des objets et d'analyser s'ils ont subis des chocs ou des températures extrêmes.

L'une des applications les plus développée de l'industrie 4.0 est la maintenance prédictive. Ce terme désigne la capacité de prévoir et d'anticiper les pannes ou toutes autres défaillances grâce à l'Internet des Objets.

A l'aide de capteurs disposés sur les équipements, les entreprises seront en mesure de réviser ces équipements dans leurs conditions réelles d'utilisation. En analysant les données récoltées par ces capteurs, les équipes de maintenance pourront déterminer les facteurs de probabilité d'un défaut, prévoir les pannes ou encore prévoir l'entretien des machines. Cela permet de ne

mobiliser les équipes de maintenance que lorsque l'intervention est nécessaire, et donc de réduire les coûts liés à la maintenance.

Donc nous comprenons l'industrie 4.0 comme une transformation numérique de la production par la convergence et l'application des technologies numériques (industrielles)

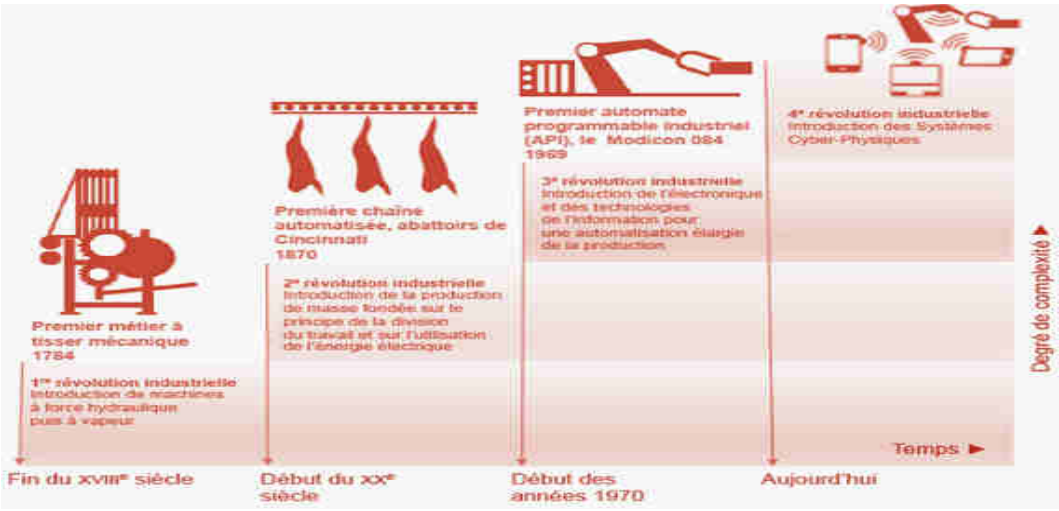


FIGURE 12: industrie 4.0

En gros nous pouvons dire qu'avec le système SoC déployer une solution est devenu moins encombrant; avec un large choix sur la technologie de connectivité.

Et les applications illustrées au-dessus nous montre la place que vient d'occuper l'IoT dans nos vie.

CHAPITRE 2 : DEVELOPPEMENT DES OBJETS CONNECTES

Le développement de l'internet des objets s'appuie sur l'accès à des réseaux d'objets de natures hétérogènes. Toute la variété des technologies de communication est mise à contribution pour répondre aux multiples usages attachés à ces objets.

On peut relever en particulier le besoin accru en mobilité et en couverture pour des objets peu consommateurs en énergie, qui a favorisé le développement de nouvelles technologies de connectivité, qui permettent à leur tour de nouveaux usages.

I. LES INFRASTRUCTURES DE CONNECTIVITE

1. FOISONNEMENT DE TECHNOLOGIES

Si certains objets fixes peuvent être connectés par des réseaux filaires, la croissance de l'internet des objets devrait majoritairement être portée par l'utilisation de technologies sans fil et mobiles.

Les technologies de connectivité sans fil sont nombreuses et variées, et l'usage de l'une ou l'autre est souvent avant tout décidé par la portée du réseau envisagé. Certains cas d'usage nécessitent également l'association de technologies sans fil et filaires pour relier les équipements à des réseaux privés étendus ou à Internet.

Un point saillant des développements technologiques actuels autour de l'internet des objets a trait au bouleversement de la dichotomie classique dans le monde des fréquences entre, d'une part, des technologies à courte portée opérant en bande « libre », souvent foisonnantes et déployées par l'utilisateur lui-même et, d'autre part, des technologies à grande portée opérant en bande de fréquence soumise à autorisation préalable (« sous licence »), déployées par un nombre réduit d'opérateurs.

Le développement de réseaux à bas débit et longue portée, en bandes libres, entraîne ainsi une pullulation d'initiatives.

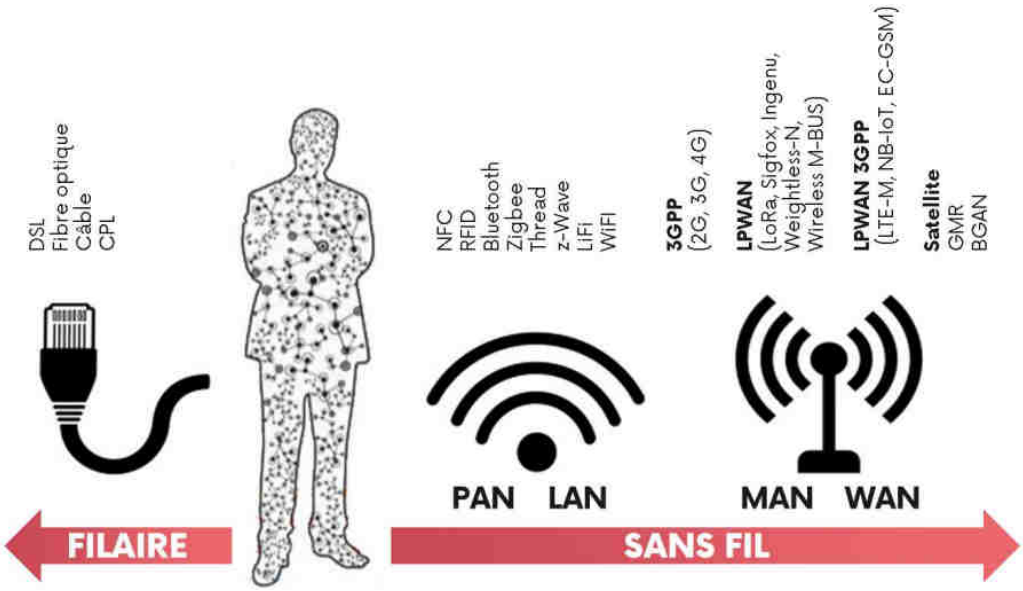


FIGURE 13: technologies de connectivité

1.1. Des Réseaux Non Opérés A Portée Locale Ou Ultra Locale

Pour les usages sans fil à courte distance, de type PAN (Personal Area Network) ou LAN (Local Area Network) on a les technologies suivantes :

- **Bluetooth:** s'étant imposée dans le secteur de l'informatique et dans différents marchés de produits de consommation, la technologie Bluetooth est un acteur incontournable pour les télécoms de courte portée. Elle devrait apporter une contribution majeure pour les produits portables notamment, facilitant encore une fois la connexion à l'IoT même par l'intermédiaire d'un smartphone. La nouvelle technologie ***Bluetooth Low-Energy*** (BLE), qui répond désormais au nom de Bluetooth Smart, est un protocole important pour les applications IoT. Offrant une portée similaire à celle du Bluetooth, elle a été conçue pour réduire considérablement la consommation d'énergie électrique.
- **Zigbee:** cette technologie de réseau sans fil cible les applications nécessitant des échanges de données relativement peu fréquents à de faibles vitesses de transmission sur un espace restreint.

  Associant fonctionnement à faible consommation, robustesse et grande évolutivité, ce protocole présente d'importants avantages dans les systèmes complexes. Il n'est également pas cher et facile à implémenter pour les fabricants d'objets connectés.
- **Thread:** c'est un tout nouveau protocole de réseau IPv6 basé sur IP, destiné à l'environnement domotique.

Il s'agit ici de créer un réseau propre aux objets communicants, capable de trouver de nouvelles routes d'accès si sur un nœud il y a un composant indisponible.

La technologie Thread comble une lacune importante dans l'écosystème de l'IoT en fournissant la première solution de l'industrie du maillage réseau, basée sur des standards, de faible consommation, qui permet aux appareils domestiques connectés, alimentés par batterie, de disposer d'une connectivité Internet fiable.

- **Wi-Fi**: Compte tenu de l'omniprésence du Wi-Fi dans l'environnement domotique au sein de réseaux locaux, la connectivité Wi-Fi s'impose souvent comme le choix évident pour beaucoup de développeurs. Elle permet le transfert de données rapide et la possibilité de gérer de grandes quantités de données c'est pour cela qu'il est très énergivore.

  Fonctionnant en bidirectionnel, il permet de mettre facilement à jour les appareils.
- **Z-Wave :** elle est une technologie télécoms RF à faible consommation, principalement conçue pour la domotique.

  C'est un réseau maillé, c'est-à-dire que chaque appareil connecté au système est émetteur de données mais peut aussi relayer celles qui sont émises par ses voisins. Cela permet d'élargir sa portée.

  Cette technologie offre une totale résistance aux interférences causées par le Wi-Fi et les autres technologies sans fil dans la plage 2,4 GHz, telles que le Bluetooth ou ZigBee. Elle utilise un protocole plus simple que d'autres technologies, offrant un développement plus rapide et plus facile.

  Le Z-Wave n'est par ailleurs pas aussi universel que le Wifi. Tous les appareils de la maison ne pourront pas forcément communiquer avec un objet connecté via cette technologie.
- **NFC:** Les protocoles **Near Field Communication (NFC)** sont fondés sur la technologie d'identification par radio fréquence RFID (Radio frequency identification). Les objets équipés d'une puce électronique RFID possèdent une « étiquette » et sont automatiquement identifiés par radio fréquence lorsqu'ils se trouvent à proximité d'un équipement appelé interrogateur.

  Le protocole NFC est un standard de communication radiofréquence sans contact à très courte distance, de l'ordre de quelques centimètres, permettant une communication simple entre deux équipements électroniques. Il est par exemple utilisé dans de

nombreuses entreprises pour les badges d'accès aux locaux, ou comme support d'un abonnement à un réseau de transport en commun.

	Courte portée			Moyenne portée		
Technologie	NFC	Bluetooth	Zigbee	Z-Wave	Wi-Fi	BLE
Portée moyenne (en intérieur)	<10 cm	10 m	10 m	50 m	50 m	50 m
Débit (Mbit/s)	1.10^{-3}	1.10^{-3}	1.10^{-2}	1.10^{-2}	1.10^{2}	1.10^{-1}
Autonomie	Mois	Jours	Années	Années	Jours	Mois
Fréquence	2,4 GHz	2,4 GHz	2,4 GHz 868 MHz	868 MHz	2,4 GHz 5 GHz	2,4 GHz
Usages	Téléphonie Cartes de paiement	Périphériques informatiques et multimédia	Domotique		Navigation internet Transferts conséquents de données	Périphériques informatiques et multimédia

TABLEAU 1: caractérisques des réseaux PAN et WAN

Toutes ces technologies fonctionnant en bandes « libres », se démarquent particulièrement. Une grande partie des usages de l'internet des objets seront diffusés par le biais de telles technologies de connectivité, et en premier lieu ceux destinés au grand public, dont on constate d'ores et déjà la multiplication.

La plupart de ces réseaux locaux, notamment chez les particuliers, sont non opérés. C'est généralement l'utilisateur qui fait l'acquisition des équipements réseau (routeurs reliés à un box internet par exemple) et devient responsable de la configuration et du bon fonctionnement du réseau local. Ces réseaux permettent une mobilité très limitée, quoique parfaitement adaptée à un usage domestique ou individuel.

En revanche, ces technologies susmentionnées, principalement orientées LAN et PAN, n'offrent pas de connectivité étendue à l'échelle nationale ou internationale, par opposition aux réseaux MAN (Metropolitan Area Network) ou WAN (Wide Area Network).

1.2.Réseaux opérés au déploiement étendu

Parmi les technologies sans fil déployées sur de grandes distances, de type MAN ou WAN, on peut retenir principalement :

- **Les réseaux cellulaires classiques (3GPP)**

Pour assurer la mise en œuvre et l'exploitation de ces réseaux à grande échelle, le recours à un opérateur est le plus souvent nécessaire. On parle alors de ***réseaux opérés***, dont font notamment partie les réseaux mobiles cellulaires historiques, presque exclusivement déployés avec des technologies 3GPP (2G, 3G et 4G) et dont la plupart sont déployés sur des fréquences sous autorisation exclusive.

Les acteurs du 3GPP travaillent par ailleurs à la standardisation de la 5G qui cherche à prendre en compte, dès sa création, tous les besoins de l'internet des objets (densité, consommation énergétique, coût des terminaux…).

- **Les réseaux de type LPWAN**

À cet égard, certains besoins nouveaux de l'internet des objets, plutôt antagonistes à la course aux performances qui a longtemps animé le développement des réseaux mobiles, ont entrainé l'émergence de nouvelles technologies de connectivité mobile. Celles-ci permettent d'atteindre des coûts de terminaux très bas et de très faibles consommations énergétiques et sont souvent regroupées sous le terme LPWAN (Low Power Wide Area Network). Parmi les technologies qui se distinguent au niveau mondial dans ce domaine on a :

- **Sigfox** (créé par l'entreprise du même nom): pour ce modèle l'opérateur assure une couverture internationale en s'appuyant sur des déploiements propres ou sur des partenariats avec des opérateurs locaux (nationaux).

C'est un réseau de communication radio sans fil à bas débit et à basse fréquence (***868MHz***), d'une portée moyenne de 10 kilomètres en milieu urbain et de 30 à 50 kilomètres en milieu rural.

Ce réseau convient à des appareils à basse consommation, dotés ainsi d'une grande autonomie, qui transfèrent une faible quantité de données.

- **LoRaWAN**: c'est un protocole de communication développé coopérativement par de nombreux acteurs au sein de la LoRa Alliance. Ce modèle, ouvert à la coexistence de plusieurs opérateurs membres de l'alliance sur une même zone géographique, amène naturellement au développement d'un standard interopérable, permettant aux objets LoRa de fonctionner sur les divers réseaux déployés internationalement.

Ce protocole de communication radio (fréquence ***868MHz***) à très basse consommation, permet de transmettre des données en petite quantité, à des distances de 2 à 5 kilomètres en ville et jusqu'à 45 kilomètres en milieu urbain. À l'instar de Sigfox, il s'agit d'un dispositif qui

convient particulièrement aux équipements peu énergivores n'émettant que périodiquement, notamment les capteurs.

En particulier, les réseaux LPWAN autorisant une alimentation sur batterie, permettent de surmonter les cas de coupure électrique c'est-à-dire qu'ils peuvent être une solution pour la redondance. Ces performances font de la connexion de secours l'un des marchés privilégiés des services de connectivité LPWAN : un objet peut être connecté grâce à un réseau fixe ou mobile « haut débit » en tant que connexion principale et basculer sur une connexion LPWAN de secours afin de prendre le relais en cas de défaillance.

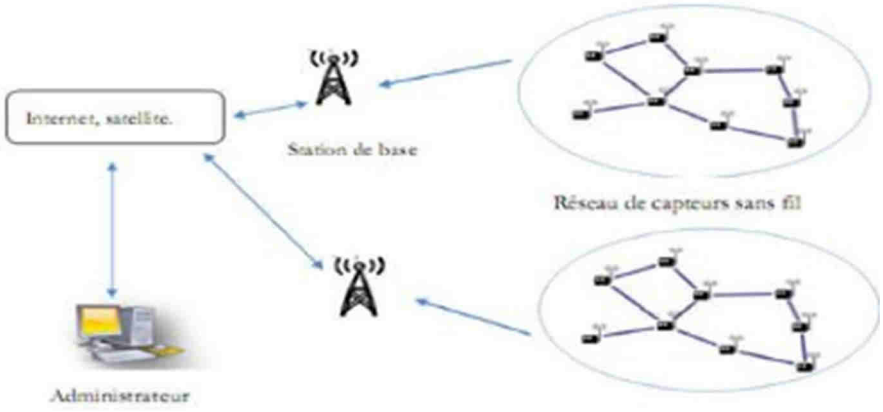


FIGURE 14: Réseau LPWAN

- **Les solutions de types satellite**

En ce qui concerne les technologies satellites, les opérateurs et équipementiers collaborent au sein de l'ETSI (l'institut européen des normes de télécommunication) à l'adaptation des normes de réseaux terrestres aux contraintes des systèmes satellitaires, notamment les normes relatives à la 2G, 3G, 4G et la future 5G. Ces travaux devraient faciliter l'intégration des technologies satellites et la convergence satellite-terrestre.

Par ailleurs, on peut noter l'intérêt de ces technologies dans le but d'étendre la couverture aux zones les plus reculées (mer, désert) et aux zones blanches, non couvertes par un réseau opéré ou à celles pour lesquelles il n'est pas possible de disposer d'accord d'itinérance (zones de conflits).

1.3.Réseaux filaires

De nombreux objets fixes sont connectés aux réseaux filaires des opérateurs traditionnels. Le réseau de cuivre, la fibre optique et le câble coaxial sont couramment utilisés, en particulier pour tous les usages nécessitant de forts besoins en débit (caméras de vidéosurveillance,

supports publicitaires vidéo, etc.) ou des latences faibles et maitrisées (machines-outils, téléchirurgie, etc.).

2. ELARGISSEMENT DE LA GAMME DES BESOINS

Les besoins des réseaux en termes de couverture et de qualité sont renouvelés par le déploiement massif d'objets connectés. En effet, l'économie de l'internet des objets, pour ce qui concerne les besoins nécessitant des réseaux à large couverture, ne se développera qu'à la condition que les réseaux soient disponibles sur une large partie des territoires.

Par ailleurs, les opérateurs sont tenus d'assurer la résilience c'est à dire la capacité d'un système à surmonter une crise déclenchée par un incident critique de leur propre réseau pour répondre aux besoins de leurs utilisateurs, qui peuvent souhaiter assurer la résilience de leur système de connectivité à travers une redondance inter-technologies (multi-sourcing) ou une haute disponibilité intra-technologie (multi-roaming).

Avec le besoin accru de mobilité et de couverture, les acteurs ont saisi l'enjeu d'une couverture étendue, continentale, nécessaire à la création d'un marché suffisamment vaste, afin de générer des économies d'échelle et permettre la baisse des prix des terminaux et de la connectivité. Par ailleurs, cette couverture transnationale sera un impératif pour certains usages, tels que le véhicule connecté ou le suivi de marchandises.

II. LES RESSOURCES RARES

La fourniture de solutions de connectivité identifiées précédemment mobilise souvent deux types de ressources : des fréquences et des adresses. Ces ressources, considérées comme rares, le sont d'autant plus que la croissance envisagée pour le nombre d'objet connectés est extrêmement importante.

1. AUTORISATION D'UTILISATION DES FREQUENCES

1.1. Les fréquences libres (bandes ISM)

Utilisées par exemple pour des réseaux LPWAN par Sigfox, les acteurs de l'Alliance LoRa. Pour ces fréquences, aucune autorisation individuelle préalable n'est nécessaire et leur utilisation n'est pas soumise au paiement de redevances. Des contraintes techniques afférentes à ces bandes doivent être respectées ; leur objectif est d'assurer la coexistence entre tous les utilisateurs.

Malgré l'existence de ces règles d'usage, il faut toutefois souligner qu'il existe une probabilité, faible, mais non nulle, que des brouillages surviennent dans la mesure où d'autres peuvent utiliser la même fréquence. Un certain nombre de ces bandes de fréquences, dont les conditions techniques d'utilisation sont fixées par l'Arcep, sont utilisées par les dispositifs de faible puissance, comme les appareils utilisant le Wi-Fi, mais également par l'internet des objets, notamment les bandes :

Pays	Bandes de fréquences
Etats-Unis *FCC*	2,400 – 2,485 GHz
Europe *ETSI*	2,400 – 2,4835 GHz
Japon *MKK*	2,471 – 2,497 GHz
France *ART*	2,4465 – 2,4835 GHz

TABLEAU 2 : bande ISM

1.2.Fréquences soumises à une autorisation individuelle

En ce qui concerne ces fréquences, le processus d'autorisation permet de s'assurer que deux personnes n'utilisent pas la même fréquence au même endroit. Hormis les cas d'usage sans autorisation ou d'usage d'un équipement non conforme, il n'existe donc, en théorie, jamais de brouillages. L'usage de ces fréquences est, sauf cas exceptionnel, soumis au paiement de redevances.

Les technologies d'accès GSM, UMTS et LTE, utilisées par les réseaux mobiles ouverts au public, permettent déjà des applications pour l'internet des objets.
Cependant le choix de l'utilisation d'une bande de fréquences plutôt qu'une autre dépend, en plus du régime d'autorisation de la bande et donc de la simplicité d'accès à la ressource, des exigences opérationnelles :

- Volume des données à transmettre et échanger ;
- Communication ininterrompue ou utilisation intermittente ;
- Communications en temps réel (par exemple, pour des applications de contrôle/commande) ou communications retardées (par exemple, pour de la collecte d'informations) ;
- Utilisation de bande passante (hauts ou faibles débits de données) ;
- Couverture (usages de proximité ou avec couverture étendue, à l'intérieur ou à l'extérieur des bâtiments) ;

- Consommation énergétique.

Ainsi, en fonction de leur modèle d'affaire ou des usages anticipés, les acteurs auront tendance à se tourner soit vers des bandes libres, soit vers des bandes attribuées à titre exclusif (notamment en s'appuyant sur les réseaux des opérateurs mobiles grand public).

Il faut également souligner que des modes d'autorisation hybrides peuvent exister, par exemple en autorisant plusieurs personnes dans la même bande de fréquences : cela réduit les risques de brouillage en contrôlant le nombre d'utilisateurs, tout en permettant de s'exonérer des contraintes liées à l'usage exclusif par un unique titulaire.

Par ailleurs, les auditions ont mis en avant que l'usage de fréquences « libres » présente pour certains acteurs, souvent les plus petits, un moyen de tester des modèles économiques à moindre coût, en comparaison de l'usage de bandes soumises à autorisations individuelles.

2. DISPONIBILITE DES FREQUENCES

À court terme, les fréquences disponibles ne semblent pas être un frein au déploiement de l'internet des objets et de multiples options sont déjà disponibles.

Les perspectives de croissance, qui annoncent un internet des objets reliant, d'ici 2020, plus de 50 milliards d'objets, imposent néanmoins une démarche d'anticipation.

Pour les fréquences libres : Une croissance importante des applications et des usages sur une certaine bande de fréquences peut contraindre le fonctionnement d'une application ou le service rendu à l'utilisateur final. En conséquence, il importe de répondre aux demandes d'accès aux fréquences soulevées par les nouvelles applications et formulées par l'industrie.

Par ailleurs, il ressort des auditions que la qualité d'utilisation de ces bandes peut être perturbée par des brouillages, notamment dus au non-respect des normes harmonisées ou des conditions d'utilisation des fréquences en vigueur par certains équipements.

En outre, les règles d'utilisation conçues pour des usages définis pourraient nécessiter des adaptations aux nouveaux besoins de l'internet des objets.

En effet, les conditions techniques d'utilisation des bandes de fréquences libres peuvent être relativement restrictives afin de permettre l'utilisation non coordonnée de très nombreux

systèmes. Elles peuvent parfois être limitées à une application spécifique afin de réduire les risques de brouillage.

En revanche, l'augmentation exponentielle de la densité d'objet prévue par toutes les études pourrait justifier l'identification de nouvelles ressources harmonisées en tenant compte de nouveaux scénarios de déploiements et conditions d'utilisation, par exemple de l'augmentation des niveaux de puissance et des taux d'utilisation, pour accompagner la croissance du secteur.

L'harmonisation des fréquences au niveau mondial est une condition importante, notamment pour les acteurs qui visent un déploiement international. En effet, la croissance des industriels sur la scène internationale dépend en partie de leur capacité à réaliser des économies d'échelles afin d'offrir des solutions technologiques à bas coût en s'appuyant sur des systèmes utilisant les mêmes fréquences.

À ce sujet, les bandes de fréquences 863 – 870 MHz, 870 – 876 MHz et 915 – 921 MHz ont été identifiées au niveau européen pour plusieurs applications de faible puissance (RFID, smart cities, alarmes….).

Pour les fréquences soumises à une autorisation individuelle : Les auditions n'ont pas fait ressortir de demande spécifique en vue de l'attribution de nouvelles bandes soumises à autorisation individuelle.

Les acteurs qui se sont exprimés, en particulier les opérateurs mobiles, qui disposent déjà de telles fréquences, sont avant tout en attente de l'arrivée des standards EC-GSM, LTE-M et NB-IoT, qui devraient fonctionner dans les bandes aujourd'hui attribuées, et à terme de la 5G qui fait d'ores et déjà l'objet de travaux visant la mise à disposition de nouvelles bandes de fréquences ou l'adaptation des conditions techniques dans les bandes actuellement harmonisées pour les réseaux mobiles.

En revanche, dans les bandes 900 MHz et 1800 MHz, les dispositions d'harmonisation sont liées aux conditions spécifiques de coexistence entre systèmes GSM, UMTS, LTE et WiMAX. Ainsi des travaux visant à évaluer la compatibilité de ces cadres réglementaires avec les solutions envisagées pour l'Internet des objets dans ces bandes ont été engagé.

3. MULTIPLICITE DES MODES D'ADRESSAGE

Dans un contexte où plusieurs milliards d'objets ont vocation à se connecter, la rareté des ressources d'adressage fait partie des enjeux majeurs. Plusieurs systèmes sont utilisés pour identifier les objets connectés dans les réseaux :

- **Identifiants ouverts** : numéros de téléphone mobiles, identifiants de cartes SIM, adresses IP (dans leurs variantes IPv4 ou IPv6), adresses MAC, identifiants OID (Object IDentifiers)…..
- **Identifiants propriétaires** : formats non standardisés.

Le principal enjeu est d'éviter la pénurie d'identifiants ouverts face à un volume d'objets connectés toujours croissant. Il peut être également nécessaire de définir une meilleure articulation entre l'échelle mondiale du marché des objets connectés et la gestion nationale de certaines ressources de numérotation.

Par ailleurs, les problématiques liées aux modes d'adressage rejoignent celles liées à la fluidité et à l'interopérabilité.

1.1. RESEAUX CELLULAIRES

S'agissant des réseaux mobiles : les normes 3GPP (GSM / UMTS / LTE) prévoient qu'à chaque ligne mobile soit affecté un numéro de téléphone mobile MS-ISDN.

Ces numéros MS-ISDN sont également utilisés pour identifier les objets connectés dans le système d'information de l'opérateur de réseau mobile.

Cependant, l'objet communique généralement avec l'application métier par le biais de protocoles de communications informatiques tels que l'IP, situé sur une couche réseau supérieure.

Toutefois, les protocoles de communication voix et SMS, utilisant le numéro MS-ISDN comme identifiant d'adressage, sont utilisés dans le cadre de certaines applications spécifiques, ou pour « réveiller » les machines (qui opèrent la plupart du temps en mode veille pour optimiser leur autonomie) afin d'initier un échange de données.

Ces numéros MS-ISDN sont attribués par l'Arcep aux opérateurs, qui les affectent ensuite aux abonnés.

1.2.Réseaux LPWAN

S'agissant des réseaux LPWAN, il n'existe à ce jour aucun plan de numérotation standardisé et unifié. Ces réseaux utilisent des identifiants privés, aux formats propriétaires, pour identifier les capteurs. Si cela ne semble pas devoir poser de problème dans l'immédiat, l'identification pourrait devenir un enjeu de standardisation à long terme.

1.3.Identifiants RFID et NFC

De nombreux objets disposent aujourd'hui d'un identifiant par le biais des technologies RFID ou NFC. Celui-ci est constitué de plusieurs sous-identifiants, intégrés dans la mémoire de la puce électronique dès sa fabrication. Etant donnée la multiplicité des objets utilisant RFID et NFC, l'unicité de l'identifiant est un enjeu crucial.

Ainsi, une autorité d'enregistrement actuellement l'ISO assure la cohérence d'ensemble et attribue des codes à une pluralité d'organismes, qui gèrent la mise à disposition de certaines sous-familles d'identifiants auprès des utilisateurs.

1.4.Adressage IP

Une partie des objets nécessitent d'être directement accessibles sur le réseau Internet et doivent disposer d'adresses IP publiques (une adresse par objet ou par réseau d'objets); ce qui accroisse ainsi la demande en ressources IP.

Au niveau mondial, la gestion des adresses IP est assurée par l'Internet Corporation for Assigned Names and Numbers (l'ICANN).

L'ICANN partage les adresses IP en blocs, entre les différents registres régionaux comme le RIPE NCC (Réseaux IP Européens -Network Coordination Centre pour l'Europe et le Moyen-Orient), lesquels se chargent de les attribuer localement.

Le 14 septembre 2012, le RIPE NCC a annoncé le début de la distribution des adresses issues du dernier bloc d'adresses IPv4 (version du protocole définie en 1981) dont il dispose, alertant ainsi contre un risque de pénurie et appelant à la nécessaire migration vers le nouveau système d'adressage IPv6.

La version 6 du protocole IP, qui a été finalisée en 1998 par l'IETF, permettra d'identifier directement l'ensemble des objets connectés à l'Internet à travers le monde sans risque de pénurie, grâce à l'utilisation d'adresses plus longues offrant un espace d'adressage quasi illimité.

III. OUVERTURE AU SEIN DES IOT

Pour que les objets connectés s'organisent en réseau, et répondent à la promesse que porte l'expression « internet des objets », il sera nécessaire que des formes plus ou moins larges d'interopérabilité existent entre les objets, qui peuvent se mettre en place à différents niveaux. Les auditions ont permis de distinguer deux grands niveaux d'interopérabilité :

- l'interopérabilité au niveau des couches basses, c'est-à-dire de l'acheminement de l'information ;

- l'interopérabilité au niveau de couches hautes correspondant au dialogue applicatif, pour le traitement des données.

1. L'ENJEU DE L'OUVERTURE ET DE L'INTEROPERABILITE

Les implications du degré d'ouverture des systèmes ont déjà fait l'objet d'analyses économiques dans le cadre de marchés présentant une innovation forte et des économies de réseau importantes.

L'Autorité de la concurrence estimait ainsi, dans son rapport intitulé « analyse économique des systèmes ouverts et fermés » que les avantages et les inconvénients d'un système ouvert, par rapport à un système fermé, devaient être appréciés au cas par cas.

D'abord, elle a relevé que l'ouverture comme la fermeture d'un système pouvaient être favorables à la concurrence : quand la première vise à promouvoir la concurrence au sein d'un système, la seconde encourage la concurrence entre systèmes.

Ensuite, elle a souligné que l'ouverture favorisait la compatibilité entre systèmes, ce qui augmente le bien-être des utilisateurs et maximise les effets de réseau ; elle a également noté que la fermeture, au contraire, permettait d'encourager l'innovation en évitant la standardisation. Ces analyses peuvent donc s'appliquer à l'internet des objets.

On a une diversité de solutions de connectivité qui démontre une innovation forte et s'accompagne de l'émergence de nombreux acteurs, mais pourrait être remise en cause avec la maturité du marché.
Le développement du marché conduit ainsi à la question de son juste degré d'ouverture, qui peut se poser à différents niveaux (objets/capteurs, données, connectivité, adresses et protocoles, etc.).

L'ouverture peut se mesurer à l'une des possibilités d'interopérabilité et des conditions de fluidité en général.

La question de l'interopérabilité est celle de la compatibilité entre les objets et entre les applications. L'interopérabilité se traduit par deux effets économiques :

- d'une part, l'interopérabilité favorise la fluidité du marché, condition nécessaire au plein exercice de la concurrence, puisqu'elle laisse aux utilisateurs le choix des solutions de l'internet des objets sans contrainte de changement de technologies, donc de fournisseurs.
- d'autre part, elle permet aux utilisateurs d'enrichir la gamme et le volume d'objets connectables à leurs propres objets. Cela permet d'enrichir les offres et de faire émerger de nouveaux usages. Ainsi, l'interopérabilité est a priori de nature à améliorer le bien-être des utilisateurs.

Néanmoins, l'interopérabilité peut créer des contraintes et des interdépendances pour les fabricants, peut limiter les facultés de différenciation et d'innovation. Alors que le marché est encore émergent, forcer l'interopérabilité risquerait de freiner, voire d'empêcher, l'innovation et cela limiterait les possibilités de monétisation pour les acteurs innovants qui seraient moins en mesure de retenir leurs clients.

Dans le contexte spécifique de l'internet des objets, imposer une interopérabilité totale et générale pourrait également avoir un impact physique sur les objets, alors qu'il existe déjà d'importantes contraintes technologiques pour les fabricants, telles que la taille, la mémoire, l'autonomie et la consommation.

À très court terme, l'interopérabilité ne semble pas le premier enjeu pour les fabricants ; les solutions technologiques ne sont pas encore matures, les usages restent souvent locaux, limités sur le plan géographique ou au sein d'une entité unique.
Les nombreux fabricants ont ainsi tendance à développer leurs objets indépendamment les uns des autres.

Pour les utilisateurs, l'interopérabilité n'est pas une priorité à court terme, en particulier pour certains industriels et quelques collectivités territoriales qui testent encore à petite échelle les solutions qui leur sont proposées et ont une certaine capacité à y incorporer par la suite une étape d'intégration, avant d'envisager un déploiement massif.

En revanche, les acteurs de l'internet des objets ont conscience qu'à moyen terme, tout objet connecté sera valorisé en fonction de sa capacité à communiquer avec un écosystème.

Par exemple, dans le cas de la maison connectée, il conviendra d'éviter aux particuliers de faire face à une multitude de modalités de connectivité en leur proposant des objets parlant la même langue pour leur éviter des coûts d'apprentissage et des dépenses supplémentaires pour le contrôle de leurs équipements. Il faudra que les collectivités, à la tête d'une multitude d'objets connectés, puissent rationaliser leurs parcs pour diminuer les coûts et croiser les données collectées.

Dans le cas des véhicules connectés, il sera crucial que les véhicules communiquent entre eux et avec les territoires connectés qu'ils seront amenés à traverser. Le manque d'interopérabilité pourra alors se révéler comme un frein au déploiement de l'internet des objets. Certains acteurs s'inquiètent déjà du fait que ce manque pourrait conduire à un fractionnement du marché.

Par ailleurs, le manque de visibilité sur les démarches d'interopérabilité pourrait également entrainer, à terme, un certain attentisme pour le lancement de services à grande échelle

2. UNE COURSE AUX STANDARDS AU NIVEAU DES COUCHES BASSES

Au niveau des couches basses, on peut identifier deux sujets d'interopérabilité : sur les protocoles de communication d'une part, et sur l'adressage des objets d'autre part. L'heure n'est pas encore à l'interopérabilité en termes de protocoles de communication : la recherche de très bas coûts pour les modules de connectivité impose une simplicité qui ne permet que difficilement, une connectivité multi-protocoles.

Toutefois, certains acteurs s'organisent pour promouvoir des standards à l'échelle mondiale.

Ainsi, les acteurs de la LoRa Alliance visent une forme d'interopérabilité entre les réseaux des opérateurs adhérents.

De leur côté, les membres de la Wi-Fi Alliance, déjà active à l'échelle mondiale, proposent le standard HaLow pour répondre aux besoins de l'internet des objets contraints par une faible consommation énergétique.

De même, les membres de la ZigBee Alliance développent un standard commun sur le protocole de communication et ont créé un partenariat avec le consortium Thread afin d'assurer une forme d'interopérabilité allant jusqu'aux couches hautes.

Sigfox, quant à lui, contrôle seul le déploiement de son standard propriétaire et gère l'alliance SNO (Sigfox Network Operators) qui octroie des accords de déploiement localement exclusifs à ses opérateurs membres.

Les exploitants de réseaux mobiles pour leur part, s'appuient sur les standards 3GPP, qui permettent une forte interopérabilité puisque les terminaux seront nativement compatibles avec les réseaux de tous les opérateurs respectant ces standards.

3. UNE AUTRE COURSE AUX STANDARDS AU NIVEAU DES COUCHES HAUTES

Si l'interopérabilité parait difficile à organiser au niveau des couches basses, certains acteurs semblent se positionner sur les couches hautes pour structurer le marché au niveau applicatif. Ces pratiques s'opèrent selon deux modalités, via une gouvernance collective ou autour d'un acteur unique.

Dans le premier cas, un standard est porté par une alliance. Ainsi, le consortium AllSeen, comprenant entre autres plusieurs acteurs travaille à développer des standards communs de communication via la technologie AllJoyn. Cette technologie présente de plus la caractéristique d'être mise à disposition en open source.

Dans le deuxième cas, un acteur se saisit du rôle de passerelle entre les objets. Cet acteur peut occuper une place plus ou moins incontournable auprès des fabricants d'objets. Le rôle de la passerelle peut être peu intrusif, lorsque celle-ci joue simplement un rôle de traducteur. C'est le cas par exemple de la plateforme IFTTT « If This Then That » qui a établi de nombreux partenariats afin de permettre l'interopérabilité entre les objets via le partage d'APIs (application programming interface).

4. DES ENJEUX DE FLUIDITE

Le passage d'une solution technologique à une autre, ou d'un fournisseur à un autre, fait généralement l'objet de coûts de changement, qui peuvent réduire les incitations à la migration et avoir des impacts sur la fluidité et les incitations concurrentielles sur le marché.
Les auditions ont permis d'identifier, à ce stade, trois grandes catégories de coûts de changement potentiels dans le contexte de l'internet des objets.

D'abord, de tels coûts pourraient être supportés lors du changement de fournisseur de connectivité. Il peut s'agir du coût de remplacement complet de l'objet, lorsque les technologies ne sont pas interopérables, ou du coût de changement de carte SIM dans le cas de technologies cellulaires, interopérables. En effet, le changement d'opérateur sur ces technologies impose un changement physique de cette carte SIM, ce qui engage des coûts de changement importants pour l'utilisateur.

Toutefois, il se développe des technologies permettant la reprogrammation des cartes SIM « over the air » qui offrent la possibilité de modifier à distance, sans intervention physique sur la flotte de terminaux, le contenu de la carte SIM pour remplacer notamment les clés de sécurité et l'IMSI d'un opérateur par ceux d'un autre. Cette solution semble permettre de limiter, en partie, le verrouillage des utilisateurs vis-à-vis de leurs fournisseurs de connectivités, dans le cas de réseaux cellulaires. Leur bon développement, dans des conditions efficaces et ouvertes à tous les fournisseurs de connectivité cellulaire, constitue un enjeu d'actualité.

Ensuite, des coûts de changement pourraient être dus au manque de transparence sur le marché, compte tenu de la faible comparabilité des informations disponibles, en termes de couverture et de qualité de service, concernant les différents réseaux déployés. L'hétérogénéité observée, par exemple, au niveau de la définition des indicateurs peut nuire à la lisibilité des performances de chaque fournisseur et limite la volonté des utilisateurs à changer de fournisseur.

Enfin, les modalités de portabilité des données ou des contenus pourraient également engendrer des coûts de changement pour les utilisateurs, si le changement de système implique la perte, totale ou partielle, ou du moins la modification, des données des utilisateurs. Les évolutions à venir du cadre juridique national et européen devraient faciliter la portabilité des données personnelles fournies par les utilisateurs en leur permettant de pouvoir les récupérer dans un format structuré, couramment utilisé et lisible par machine.

CHAPITRE 3 : EXPOSITION DES SYSTEMES D'OBJETS CONNECTES

Pour permettre à l'Internet des objets d'atteindre son plein potentiel et concrétiser les scénarios qui en découlent, plusieurs aspects doivent être étudiés. En effet, les concepts prometteurs imaginés par la communauté scientifique nécessitent de résoudre un certain nombre de problématiques : grande échelle, hétérogénéité, impact du monde physique (grands flux continus de données, variabilité de l'environnement), sécurité des biens et des personnes, et respect de la vie privée des utilisateurs.

I. VULNERABILITE

1. ÉCHELLE DE L'INTERNET DES OBJETS

Il paraît raisonnable, en ce qui concerne le réseau de communication global proprement dit, de considérer le réseau Internet comme un candidat prometteur.

En effet, celui-ci est déjà massivement déployé à l'échelle mondiale et interconnecte plusieurs milliards de machines diverses et variées. En cela, Internet est le plus grand réseau connu jamais déployé, et paraît donc une bonne base pour l'Internet des objets.

Par ailleurs, on estime qu'aujourd'hui une portion non négligeable des connexions sur Internet se font déjà entre objets connectés, et que ceux-ci sont au nombre de 15 milliards environ. D'après la progression actuelle, ce nombre pourrait augmenter et atteindre jusqu'à 100 milliards d'objets d'ici 2020, avec un trafic Internet global qui se compterait en zettaoctets (10^{21}octets).

Les différents problèmes liés à l'échelle de l'Internet des objets sont relatifs à l'adressage et l'identification des objets, que l'on espère cependant résoudre au moyen de technologies existantes :

- Le protocole IPv6 pour l'adressage des objets.
- Les codes de produits électroniques (electronic code product, ou EPC), les identifiants universels uniques (universally unique identifie, ou UUID) pour l'identification unique des objets.

Toutefois, au-delà du simple adressage, d'autres problématiques se posent quant à la gestion de l'identité des objets et la découverte de ces derniers. De manière générale, le processus de découverte permet aux machines de prendre connaissance de l'existence d'autres machines,

soit en émettant un message à destination de toutes les machines accessibles directement sans routage (découverte locale), soit en contactant un annuaire externe, c'est-à-dire une base de données stockant les identités d'objets.

Découvrir les objets est fondamental dans le cadre de certains scénarios de l'Internet des objets, typiquement lorsque ce dernier utilise des capteurs qui ne sont pas explicitement connus au préalable.

Aussi, grâce à l'infrastructure de découverte, il doit être possible de :

- récupérer et mettre à jour l'identité d'un objet à partir de son adresse ou de son identifiant ;
- récupérer les adresses des objets dont l'identité satisfait certaines contraintes.

La première opération s'apparente à ce que nous connaissons aujourd'hui avec les systèmes de noms de domaine (domain name system, ou DNS) du réseau Internet : un annuaire hiérarchique permettant de retrouver l'adresse IP d'une machine à partir de son nom d'hôte. De la même façon, le concept de système de noms d'objet (object name system, ou ONS) peut être introduit pour retrouver l'identité d'un objet à partir de son adresse ou de son identifiant.

Si un ONS conçu sur le modèle du DNS paraît envisageable à l'échelle de l'Internet des objets, l'opération inverse consistant à retrouver les adresses des objets à partir de leurs caractéristiques est cependant plus complexe.

En effet, certains paramètres de l'identité peuvent changer au cours du temps, le plus courant étant la position, ce qui complexifie la synchronisation dans le cas d'un ONS inverse distribué. Toutefois, à une telle échelle, une approche centralisée est difficilement envisageable étant donné la quantité d'identités à stocker.
En plus d'avoir un impact sur la découverte, l'échelle de l'Internet des objets complexifie l'accès et la collecte des informations produites par les objets.
Par exemple, si l'on considère un scénario consistant à analyser la pollution d'une ville, l'ensemble des capteurs disponibles pourrait être très grand, car comprenant les capteurs fixes installés pour la ville et les éventuels capteurs mis à disposition par les citoyens. Accéder séparément à chaque capteur pour y récupérer un flux de mesures conduirait à gaspiller inutilement les ressources énergétiques des capteurs et à saturer les canaux de communication.

Par ailleurs, le problème est démultiplié lorsque la taille des données augmente, comme c'est le cas pour les systèmes publics de vidéosurveillance. Ces grands volumes de données, issus

d'un grand nombre de sources différentes, posent un problème en ce qui concerne leur analyse (filtrage, agrégation, recherche, etc.) et leur stockage, et requièrent des approches et des techniques spécifiques de traitement continu en temps réel.

2. HETEROGENEITE DE L'INTERNET DES OBJETS

Conformément aux usages pour lesquels ils ont été conçus, les propriétés et les capacités des objets varient significativement, contribuant à faire de l'Internet des objets un écosystème certes riche, mais aussi hétérogène, les effets de cette hétérogénéité sont :

- **Hétérogénéité fonctionnelle**

Les objets possèdent des capacités spécifiques (statique ou mobile, alimenté en continu ou par une batterie, ressources matérielles, capteurs etc.) et à chacune d'elle correspond des contraintes particulières (connectivité intermittente, durée de vie, tâches réalisables, etc.).

Différentes approches et techniques doivent être considérées pour gérer les objets en fonction de leurs contraintes et de leurs différences propres.

- **Hétérogénéité technique**

Les technologies matérielles et logicielles utilisées pour construire les objets sont multiples et compromettent l'idéal de collaboration autonome entre objets. De plus, le développement d'applications est complexifié, nécessitant des développeurs des connaissances spécifiques sur le fonctionnement de chaque objet.

Aux caractéristiques des objets correspondent des contraintes qui conditionnent la façon dont ces objets sont utilisés et interagissent avec leur environnement. Par exemple, les objets mobiles sont plus susceptibles de souffrir d'une connectivité intermittente que les objets statiques, les objets alimentés par une batterie sont limités par leur durée de vie et les objets possédant de faibles ressources matérielles sont restreints à des tâches simples. De la même façon, les objets embarquent différents capteurs et actionneurs conformément à leurs fonctions, ce qui a un impact direct sur leurs aptitudes à mesurer et à influer sur leur environnement.

Sachant que dans l'Internet des objets les différents objets sont interconnectés et collaborent dynamiquement entre eux, cette hétérogénéité fonctionnelle doit être prise en compte. De manière générale, les objets devraient pouvoir interagir en toutes circonstances, quelles que soient les contraintes posées par leurs caractéristiques et leur environnement.

En plus d'être hétérogène au niveau fonctionnel, l'Internet des objets est directement affecté par la diversité des composants matériels et logiciels utilisés pour construire les objets.

En effet, en fonction des constructeurs, les objets n'utilisent pas les mêmes systèmes d'exploitation, ne possèdent pas les mêmes interfaces de communication et ne respectent pas les mêmes formats de données, ce qui conduit à une hétérogénéité technique significative. Si un effort de standardisation est mené par différents organismes, de nombreuses technologies propriétaires restent couramment utilisées.

En outre, les différentes façons de programmer les systèmes complexifient le développement d'applications à grande échelle en obligeant les développeurs à posséder des connaissances sur le fonctionnement des objets de chaque constructeur.

Concernant l'autonomie des objets, les multiples interfaces de communication et protocoles utilisés, lorsque ceux-ci sont incompatibles, limitent les interactions naturelles entre les appareils et contribuent à former des ilots d'objets isolés les uns des autres.

Les formats utilisés pour nommer les objets, décrire leurs identités et représenter les données que leurs capteurs produisent sont nombreux, d'où d'importantes difficultés pour deux objets d'échanger des informations « compréhensibles».

Les effets négatifs de ces deux formes d'hétérogénéité, décuplés par la grande échelle et la popularité croissante de l'Internet des objets auprès des constructeurs, peuvent être atténués en agissant sur plusieurs fronts.

Tout d'abord, pour lutter contre l'hétérogénéité technique, l'effort de standardisation technologique doit être mené à son terme, notamment au travers de la convergence des technologies dédiées aux systèmes limités en ressources vers celles du réseau Internet actuel. Ensuite, des couches d'abstraction logicielles doivent être introduites pour gérer l'hétérogénéité fonctionnelle de l'Internet des objets, couplées à l'utilisation de formats ouverts et interopérables.

Enfin, il paraît utile de rendre les objets plus autonomes, notamment en leur permettant de manipuler des connaissances grâce aux technologies de description de la sémantique. Ainsi, en raisonnant automatiquement à partir des concepts, les objets seraient plus à même de s'adapter dynamiquement à leur environnement et aux contraintes fonctionnelles et techniques, lorsque cela est possible.

3. INFLUENCE DU MONDE PHYSIQUE SUR L'INTERNET DES OBJETS

L'Internet des objets est fondamentalement influencé par les caractéristiques du monde physique et des outils qui permettent de le mesurer.

Le monde physique est un environnement qui évolue naturellement au cours du temps, d'une part parce que des objets y sont ajoutés ou retirés continuellement et, d'autre part, du fait de la mobilité des êtres humains et de certains de leurs objets. Globalement, de nombreux objets sont amenés à découvrir dynamiquement leur environnement et à communiquer de manière opportuniste avec d'autres objets, c'est-à-dire initier des échanges à un instant t avec des objets proches qui ne seront peut-être plus disponibles à l'instant t + 1.

Concrètement, la mobilité et les interactions à la volée induisent une topologie dynamique du réseau, où certains objets bougent, apparaissent et disparaissent au gré de leurs batteries, des mouvements de leurs utilisateurs et des infrastructures de communication sans fil disponibles (connectivité intermittente).

Les objets doivent donc être en mesure de s'adapter dynamiquement aux changements qui surviennent au cours du temps, aussi bien en ce qui concerne leurs propres états que leur environnement.

Aussi, conformément aux besoins exprimés par les utilisateurs, les objets devraient posséder les moyens nécessaires pour réagir dynamiquement en fonction des situations, que ce soit en collaborant avec d'autres objets ou en appliquant des techniques appropriées.

Au-delà de l'autonomie des objets, relier le monde physique au monde virtuel implique de tenir compte des particularités et des limites fondamentales des systèmes qui permettent d'interagir avec ce monde physique : les capteurs et les actionneurs. De manière générale, les capteurs produisent soit des mesures régulières d'un phénomène donné (comme les capteurs de température) soit des évènements (comme les capteurs de présence).

Ces informations sont ensuite transformées et consommées par d'autres objets, dont les actionneurs sont généralement placés en bout de chaîne.
On constate que les deux familles d'information générées par les capteurs sont dépendantes du temps :

- les mesures régulières représentent l'évolution d'un phénomène au cours du temps ;
- les évènements correspondent à un fait limité dans le temps.

Aussi, qu'il s'agisse de flux d'échantillons ou de flux d'évènements, un capteur produit des données en continu qui doivent être traitées au fur et à mesure.

En effet, il n'est pas envisageable d'attendre la fin du flux avant de commencer à effectuer des opérations, étant donné que l'on ignore quand le flux se terminera (infinité potentielle), les données produites perdent de leur intérêt au cours du temps et nous ne disposons pas forcément de l'espace de stockage nécessaire.

Contrairement aux ensembles finis de données classiques que l'on rencontre habituellement dans les bases de données (les tables) ou sur le Web (les pages), les flux de données sont produits, traités ou consommés en continu, élément après élément.

Peu d'informations sont connues à priori lorsque l'on traite un flux de données : celui-ci est potentiellement infini et son débit peut être variable, tout particulièrement dans le cas des évènements dont l'occurrence, la durée ou la taille ne sont pas forcément prédictibles.

À l'échelle de l'Internet des objets, certains flux peuvent avoir un débit très important, à tel point que les données produites ne peuvent pas être stockées dans leur intégralité. Dans un tel scénario, les nouveaux éléments produits dans le flux doivent être traités en une seule passe puis immédiatement supprimés de la mémoire.

Pour pouvoir faire face à cette contrainte, des algorithmes spécialement conçus à cet effet doivent être employés.

L'Internet des objets, du fait de son utilisation massive de capteurs, doit aussi faire face aux limites techniques de ces derniers, connus pour introduire des erreurs de mesure.

Plusieurs types d'erreurs peuvent être rencontrés, notamment :

- un bruit aléatoire (noise) qui affecte toute une série de mesures ;
- une succession de mesures identiques, dont la valeur est soit anormalement basse ou haute, soit anormalement constante.

Il est généralement impossible de prédire quand ces erreurs vont survenir et leurs causes sont difficiles à déterminer de manière spécifique : il peut s'agir de défaillances matérielles, comme un court-circuit ou un capteur endommagé, d'un effet dû au déchargement de la batterie (introduction de bruit), d'une défaillance logicielle ou d'une erreur de calibration.

Ces dernières sont très répandues et peuvent corrompre les résultats de différentes manières, par exemple en introduisant un décalage constant, un gain constant ou une variation de ces deux propriétés au cours du temps.

Elles sont en outre difficiles à détecter, car l'ensemble des mesures est affecté et, de fait, conserve une certaine cohérence vis-à-vis du phénomène mesuré. Par exemple, un décalage constant sur un capteur de température ne perturberait pas la cohérence du cycle jour-nuit.

La lecture des puces RFID et la communication en champ proche, bien que n'effectuant pas de mesures à proprement parler, souffrent des mêmes perturbations et erreurs de mesure. Les lecteurs échouent régulièrement à détecter les objets à proximité (environ 30% d'échec) ou produisent des détections erratiques, par exemple sous la forme de multiples détections dans un court intervalle de temps par un ou plusieurs lecteurs.

De la même façon, les technologies de communication en champ proche (NFC) sont sujettes à de fréquentes déconnexions et un fort taux de pertes.

La détection de ces erreurs et leur correction est une tâche complexe en temps normal, mais devient critique à l'échelle de l'Internet des objets où le volume de données est tel qu'il n'est ni souhaitable ni forcément possible de les stocker pour les parcourir plusieurs fois.

En outre, l'hétérogénéité joue un rôle ici aussi, étant donné que d'une famille de capteurs à une autre les propriétés de mesure peuvent varier : précision, résolution, sensibilité, plage de mesure, temps de réponse, etc. De manière analogue, les probabilités d'occurrence de certaines erreurs vont être dépendantes des technologies de capteurs utilisées.

4. SECURITE ET VIE PRIVEE

Si l'Internet des objets introduit plusieurs cas d'utilisation prometteurs, il pose aussi plusieurs problèmes quant à la sécurité et à la vie privée.

En effet, les objets étant des entités physiques possédant les capacités nécessaires pour influer sur leur environnement, les dégâts provoqués par une attaque informatique dans un tel contexte ont un impact bien plus important que ceux causés par les intrusions, les défigurations de site, les vols de données ou les dénis de service que nous connaissons à l'heure actuelle.

Concrètement, l'Internet des objets souffre de plusieurs vulnérabilités inhérentes aux technologies utilisées. En effet, de nombreux objets possèdent des capacités matérielles

réduites, voire quasiment inexistantes, et de ce fait, ne peuvent pas directement mettre en œuvre des techniques de sécurisation modernes, ces dernières nécessitant des ressources de calcul conséquentes.

De la même façon, le coût énergétique élevé des communications sans fil complexifie les processus d'authentification des objets au travers d'infrastructures dédiées, du fait de l'échange de multiples messages entre les appareils et les serveurs d'authentification.

L'échange de clés entre les différents objets pose des problèmes similaires, aussi bien en matière de calculs (génération des clés) qu'en matière de communication (échange des clés). Pour finir, la préservation de l'intégrité des données, c'est-à-dire la garantie qu'un adversaire ne puisse pas modifier de données sans que cela soit détecté par le système, est difficile à assurer en l'absence de chiffrement fort.

Par ailleurs, les objets sont vulnérables physiquement, étant le plus souvent déployés dans un environnement sans surveillance particulière. Un attaquant pourrait, notamment, altérer leur mémoire en accédant directement à leur matériel ou aux interfaces d'entrée-sortie disponibles. En outre, l'utilisation des technologies de communication sans fil facilite d'une part la mise en place d'écoutes clandestines et, d'autre part, les attaques par déni de service en perturbant le signal radio.

Étant donné l'intégration naturelle des objets dans l'environnement, de nombreuses informations peuvent être collectées à l'insu des utilisateurs, aussi bien par le propriétaire des objets à proximité que par d'éventuels attaquants.

De manière générale, il n'est plus possible de savoir où, quand, pourquoi et par qui les données sont collectées, pas plus qu'il n'est possible de savoir combien de temps celles-ci seront conservées et qui pourra y accéder dans le futur.

Par exemple, certaines informations sensibles, telles que l'état de santé ou les comportements de conduite, pourraient être utilisées à l'insu d'un utilisateur lorsque celui-ci tenterait de contracter une police d'assurance.

De plus, dans le cadre des outils d'analyse de comportements suspects à priori, la présence d'erreurs introduites volontairement ou non serait directement et automatiquement dommageable pour les individus ciblés.

Ainsi, l'Internet des objets pose des problèmes de respect de la vie privée même pour ceux qui n'en utilisent pas les services, car la simple présence d'un individu dans l'environnement entraîne implicitement la collecte d'informations.

Couplé à l'identification unique des objets, cela rend possible la construction de profils extrêmement complets à propos des utilisateurs et des objets qu'ils possèdent ou transportent sur eux. Ces profils uniques peuvent ensuite être utilisés pour suivre les individus en temps réel et à très grande échelle, en se basant sur la détection des objets et sur les différents capteurs placés dans l'environnement.

Il faut avoir conscience que ce problème de collecte à l'insu des utilisateurs ne peut pas être résolu uniquement avec des mesures techniques. En effet, celles-ci doivent être accompagnées d'un cadre légal fort, notamment en ce qui concerne l'information des utilisateurs quant aux données collectées, les limitations légales relatives au stockage, à l'utilisation et à la redistribution de ces informations et, enfin, le droit des utilisateurs à faire rectifier ou supprimer tout ou partie des données collectées à leur sujet par un tiers.

Au-delà de la collecte à leur insu, les utilisateurs informés qui désirent bénéficier des services de l'Internet des objets doivent en outre gérer leurs données et le partage de celles-ci avec d'autres systèmes. Il est nécessaire pour les utilisateurs de pouvoir définir la façon dont leurs objets collectent des informations à leur sujet (le quoi, le où et le quand) et à qui ces informations sont diffusées, ce de la manière la plus simple et compréhensible possible.

II. LES ATTAQUES

1. CARTOGRAPHIE DES METHODES D'ATTAQUE

Les piratages d'objets connectés peuvent être classés en trois catégories définies en fonction des vulnérabilités existantes et de l'intention de l'attaquant.

1.1. Les attaques contre les objets connectes eux-mêmes

L'attaquant peut entreprendre d'attaquer directement le matériel, par exemple en piratant les composants présents sur les circuits imprimés. Cela peut impliquer de dessouder le processeur central, d'extraire les données chiffrées de la mémoire à long terme (NVRAM), d'intercepter les messages sur la mémoire vive statique (SRAM).

Côté logiciel, la compromission d'un objet connecté par un code malveillant peut entraîner son inaccessibilité pour son utilisateur, la désactivation de fonctions de sécurité voire la compromission d'autres objets connectés communiquant avec l'équipement compromis.

L'installation locale ou à distance de rançongiciels (ou logiciel de rançon qui est un logiciel malveillant qui prend en otage des données personnelles en les chiffrant et en demandant à son propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer) impactant la disponibilité des équipements et leur intégrité peut aussi permettre à des pirates d'obtenir un gain financier. Cette menace est d'autant plus importante si l'équipement est connecté à Internet ou à un ensemble d'équipements similaires et que le rançongiciel peut être installé à distance.

L'extraction de secrets propres à un équipement produit par un fabricant (mots de passe d'administration identique pour tous les équipements, clefs de chiffrement maîtresse, etc.) peut permettre de compromettre un ensemble d'équipements connectés et d'impacter à large échelle les systèmes auxquels ils sont connectés ou ont accès.

1.2.Les attaques réalisées au travers des objets connectes

Ces attaques exploitent les équipements connectés comme moyen d'accès à de plus vastes réseaux tels qu'Internet. L'équipement compromis sert ainsi de relais dans la réalisation d'une attaque de plus vaste ampleur, comme un déni de service distribué.

Une caméra connectée à Internet peut par exemple posséder une vulnérabilité permettant à un pirate d'en prendre le contrôle et d'exécuter du code malveillant. Le pirate va ainsi tenter de prendre le contrôle d'un maximum de caméras identiques accessibles sur Internet afin de les transformer en autant de machines participant à une attaque de plus vaste ampleur, sans que les propriétaires desdites caméras ne se rendent compte que leur équipement a été détourné de son usage primaire et participe à une attaque d'envergure.

De même, il est tout à fait envisageable qu'un pirate puisse se servir d'équipements connectés à Internet pour héberger des contenus malveillants ou des sites d'hameçonnage. Ce dernier cas de figure est relativement complexe à traiter, car à la différence des contenus hébergés sur des serveurs et sur lesquels des administrateurs ont accès, ces équipements connectés ne fournissent généralement pas d'accès système pour retirer les contenus malveillants.

1.3.Les attaques contre les réseaux et protocoles de communication de l'iot

Les attaques les plus classiques sont les attaques basées sur l'écoute de trafic (attaques passives) et de l'homme du milieu (attaques actives) permettant l'interception de données transmises en clair, ou chiffrées si un chiffrement est fourni nativement par le protocole de communication ou par l'application.

Dans le monde des objets connectés, il existe plusieurs protocoles permettant d'interconnecter des équipements entre eux. Ces protocoles autorisent la communication entre différents équipements à courte ou longue distance, de manière sécurisée ou non, et certains d'entre eux permettent même d'établir des réseaux d'objets connectés.

Un pirate réussissant à s'introduire dans ces réseaux peut être en mesure d'intercepter les données échangées entre divers équipements mais aussi d'attaquer d'autres équipements auxquels il n'avait pas accès initialement, grâce à cette interconnexion.

Les réseaux à longue portée conçus pour les équipements à faible consommation (LPWAN) sont particulièrement sensibles à l'interception de données ou à l'usurpation d'équipement (le fait pour un pirate de simuler un équipement réel et d'injecter des données falsifiées) ; d'autant plus que la barrière physique est quasi inexistante : la portée des équipements peut selon la technologie employée dépasser la quinzaine de kilomètres. Un pirate peut dès lors envoyer des informations erronées semblant provenir de nombreux capteurs déployés sur le territoire national, faisant croire à une avarie généralisée et provoquer une réaction inattendue d'un fournisseur d'énergie (coupures préventives d'électricité pour cause d'incident) ou une interruption de trafic dans le cas de transporteurs.

Les protocoles de communication à courte distance ne sont pas pour autant plus sécurisés : la sécurité mise en place est bien souvent rudimentaire et peut être soit cassée après une interception d'échanges faiblement sécurisés, soit contournée lors de la réalisation d'interception par une attaque de « l'homme du milieu ». Un pirate peut ainsi intercepter des identifiants d'accès à une ou plusieurs ressources critiques, ou encore des clefs dématérialisées permettant de manœuvrer une serrure connectée et de s'introduire dans une zone à accès restreint.

2. LES FUTURES CYBERATTAQUES

Face aux multiples enjeux sécuritaires que représentent l'Internet des objets, des études ont été faites sur les principales menaces de cet écosystème vulnérable. L'identification des principaux risques a permis d'élaborer plusieurs scénarios prospectifs en se basant sur l'actualité et sur des retours d'évaluation de sécurité.

- DOMOTIQUE

Le piratage d'objets connectés dans le secteur de la domotique peut avoir des conséquences beaucoup plus graves tels que le détournement d'argent ou l'intrusion physique. Plusieurs scénarios peuvent ainsi être envisagés :

Les serrures connectées sont un moyen d'accès facile à pirater en raison de leur porosité. Les configurations par défaut, les interfaces sans fils n'implémentant pas correctement la sécurité, les badges clonables ou émulables, et enfin les interfaces d'administration sont mal protégées. Ces serrures connectées « ouvrent donc la porte » aux criminels. De plus, ces serrures étant conçues pour communiquer avec des smartphones, l'utilisation d'une application spécialisée dans le crochetage de serrures numériques par les criminels facilite le procédé sans éveiller les soupçons.

- E-SANTE

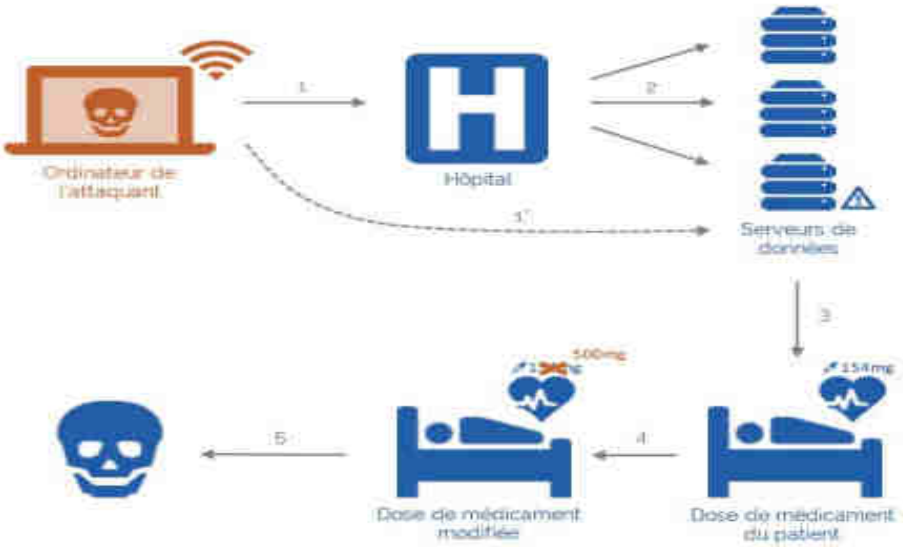


FIGURE 15: Cyberattaque contre un équipement médical connecté

1 ⟹ Intrusion d'un attaquant dans le réseau de l'hôpital

1* ⟹ Attaque directe sur les données stockées dans le Cloud

2 ⟹ Accès aux serveurs de données de l'hôpital

3 ⟹ Modification des doses de médicaments à administrées au patient λ

4 ⟹ Récupération de la nouvelle posologie par le moniteur de surveillance

5 ⟹ Administration automatique d'une dose potentiellement létale par l'appareil ou le praticien.

Le centre de télésanté fournit au médecin traitant un suivi en temps réel de ses patients. Le médecin peut modifier à distance les prescriptions et dosages opérés par les équipements de santé afin d'adapter les soins à l'état de santé du patient.

Les équipements médicaux connectés peuvent porter atteinte à la santé du patient s'ils ne sont pas correctement utilisés ou configurés.

Un attaquant pourrait rechercher sur Internet les passerelles de télésanté accessibles, et prendre le contrôle de celles-ci afin de modifier les données transmises par ces dernières aux services de télésanté, voire modifier des dosages ou des configurations d'équipements employés par le patient tels que des respirateurs ou des pompes à insuline, pouvant aboutir au décès d'un grand nombre de patients utilisant ces équipements.

- SMART CITY

Le piratage simultané des infrastructures urbaines d'une smart city aurait des conséquences catastrophiques.

La réaction à une attaque informatique sur une ville connectée serait nettement plus complexe, surtout si l'attaque informatique était menée depuis l'étranger. Plusieurs types de scénarios sont envisageables:

- Des criminels pourraient envisager de forcer l'arrêt d'une centrale électrique en attaquant son système informatique industriel, entraînant ainsi un blackout complet.
- Les pirates pourraient également lancer des cyberattaques dans le réseau informatique de l'aéroport d'une ville, de ce fait les avions seraient dans l'impossibilité de se poser ou de décoller.

- Les pirates pourraient attaquer les compteurs connectés installés chez les particuliers et dans les sociétés afin de les désactiver à distance, ce qui permettrait de réaliser des attaques très ciblées sur certaines cibles en particulier ou au contraire des attaques de grande envergure plongeant une ville entière dans le noir.

CHAPITRE 4 : METHODES DE SECURISATION D'UNE INFRASTRUCTURE IoT

Ce chapitre vise à proposer un ensemble de recommandations permettant de pallier le manque de sécurité souvent constaté dans les solutions connectées. Ces recommandations peuvent permettre aux constructeurs et à tout organisme impliqué dans le développement de l'IoT d'atteindre un bon niveau de sécurité. Cette analyse se base sur une méthodologie intuitive, c'est-à-dire des recommandations seront proposées selon leur degré de criticité. Les solutions les plus urgentes à mettre en place seront exposées en premier lieu, puis les solutions moins prioritaires mais qui sont néanmoins nécessaires au bon fonctionnement des objets connectés.

I. MECANISMES DE DEFENSES ASSOCIES AUX IOT

1. MECANISMES TECHNIQUES

La règle d'or est l'intégration de la sécurité dès le début des projets ; en plus d'être bien plus efficace, elle coûte habituellement 3 à 5 fois moins chère que d'intégrer la sécurité pendant le développement ou la recette de la solution.

Par ailleurs, la sécurité repose parfois en grande partie sur l'architecture de la solution, architecture choisie lors des phases préliminaires de conception et qui peut difficilement être changée pendant son développement.

La cryptographie joue un rôle important, puisqu'elle permet d'adresser au moins partiellement les problématiques de confidentialité, d'intégrité, de disponibilité et de non-répudiation. Des outils cryptographiques appropriés et prêts à l'emploi existent aujourd'hui pour quasiment tous les besoins de sécurité imaginables.

Plus globalement, il est vivement recommandé d'utiliser systématiquement les bonnes pratiques existantes à tous les niveaux, et d'éviter les mesures de sécurité « originales » ou «créées sur mesure ». Des composants réutilisables, fiables et éprouvés sont toujours bien plus sûrs qu'un code ou protocole créé spécialement pour la solution, et non éprouvé.

1.1.La sécurité physique de l'objet

A la différence d'une solution logicielle, aujourd'hui le plus souvent déportée sur le Cloud, la sécurité d'une solution IoT va reposer en partie sur le fait que l'utilisateur peut avoir entre ses mains un objet connecté de la solution. En particulier, l'application, le système d'exploitation et aussi le matériel sur lequel la solution repose peut être manipulé presque à volonté par l'utilisateur.

En effet les données collectées et stockées par l'objet doivent être protégées, surtout s'il s'agit de données sensibles et d'ailleurs souvent réglementées (données à caractère personnel, données de santé, données financières, …), contre les fuites ou exfiltrations, mais aussi de protéger la propriété intellectuelle du concepteur de la solution, par exemple contre la copie physique ou celle de son micrologiciel.

- ✓ Le scellement du boîtier des objets connectés : il s'agit de « verrouiller » le boîtier de l'objet par (collage, thermocollage, soudure, ...) de façon à empêcher son ouverture normale, au détriment, il est vrai de pouvoir facilement réparer l'objet. Cela permet aussi de voir si l'intégrité physique de l'objet a été atteinte au premier coup d'œil.
- ✓ Le moulage des cartes et composants électroniques dans de la résine : cela empêchera l'identification des composants utilisés, ainsi que leur analyse par mesure ou débogage.
- ✓ La désactivation des ports de débogage et de lecture mémoire des composants : pour empêcher l'analyse de leur comportement et des données traitées.
- ✓ L'utilisation de composants sécurisés pour le stockage des clés et les traitements cryptographiques : cela rend quasiment impossible l'extraction des secrets stockés dans l'objet.
- ✓ L'utilisation de clés et mots de passe tous différents dans chaque périphérique : pour éviter qu'une compromission sur un périphérique ne puisse compromettre l'intégralité du parc.
- ✓ Le chiffrement et l'offuscation du micrologiciel : même s'il s'agit de sécurité par l'obscurité, jamais efficace à long terme, cela ralentit considérablement le travail d'analyse et de rétroingénierie du micrologiciel, et donc son altération ou sa copie.

1.5.Les protocoles de communication

Le choix des protocoles de communication utilisés dans la solution IoT n'est pas anodin. En plus de contraintes liées aux capacités de l'objet (puissance de calcul, mémoire, autonomie énergétique), il doit répondre aux besoins de sécurité propres aux données manipulées et à

l'usage de la solution. Il est en effet fréquent de pouvoir écouter une communication non chiffrée ou de pouvoir usurper très facilement un objet en copiant son identifiant.

Cependant, très souvent, les protocoles de communication sont mal choisis et/ou mal implémentés. Il ne suffit pas uniquement de choisir un protocole adapté, il est aussi nécessaire d'activer ses fonctions de sécurité et les utiliser convenablement.

Il y a trois principales menaces récurrentes sur les communications : l'écoute passive, le brouillage (volontaire ou involontaire), et l'usurpation. Dès lors, nous conseillons :

- ✓ Le chiffrement des communications sensibles
- ✓ L'authentification des objets les uns avec les autres : on parle alors d'authentification mutuelle, ce qui évite les attaques de type « Man-in-the-Middle ». Habituellement, cette authentification est faite sous forme d'une procédure de paiage, ou par certificat électronique.
- ✓ L'utilisation de protocoles sécurisés d'échange de clés : le plus courant étant le protocole Diffie-Hellman, attention ce dernier nécessite auparavant d'avoir authentifié les périphériques concernés pour éviter l'interception par un tiers.
- ✓ L'utilisation de mesures anti-brouillage, comme l'étalement de spectre (« spread spectrum ») ou les sauts de fréquence (« frequency hopping » / « channel hopping »), utilisés dans certains protocoles comme Bluetooth.

Certaines de ces mesures sont implémentées de base dans les protocoles sans fil. Celles qui ne sont pas implémentées peuvent souvent l'être au niveau de la couche applicative, donc restant à la charge du développeur.

1.6.Sécurité applicative et système

Enfin, la solution connectée peut-être attaquée par son maillon applicatif, que ce soit côté client (smartphone, tablette, micrologiciel, …) ou côté serveur (passerelle, serveur sur le cloud, …). Nous recommandons à ce titre :

- ✓ Le choix et l'utilisation de briques applicatives répandues et régulièrement mises à jour.
- ✓ L'implémentation des contrôles côté serveur, car les contrôles côté client sont manipulables et contournables par un utilisateur malintentionné.
- ✓ Le filtrage et la validation de toutes les entrées, et si possible des sorties des traitements effectués. De manière générale, n'accorder aucune confiance aux données reçues par

un composant de la solution. Eviter autant que possible l'utilisation de listes noires de filtrage, elles sont rarement exhaustives, préférer systématiquement l'utilisation de listes blanches.

- ✓ L'application d'une sécurité en profondeur, en donnant aux utilisateurs les privilèges minimums à leur utilisation de la solution et en redondant les mécanismes de sécurité eux-mêmes.
- ✓ L'utilisation de procédures et référentiels de durcissement système sur les serveurs de la solution : suppression des comptes et services non utilisés, applications de mots de passe forts sur tous les comptes, mises à jour régulièrement appliquées, monitoring actif des accès, veille permanente sur les vulnérabilités affectant les composants de la solution connectée, sondes HIDS,...

2. LA LABELLISATION

Les évènements passés liés à l'insécurité de certains systèmes connectés ont explicité les risques financiers que peuvent engendrer une sécurité défaillante. Si les processus de sécurisation engendrent certes des frais supplémentaires, il est primordial pour les entreprises de comprendre que la négligence de cet aspect peut se révéler bien plus dangereux : c'est une question de retour sur investissement qui, s'il n'est pas forcément visible de prime abord, peut s'avérer très rentable sur le long terme.

La délivrance de label garantira la fiabilité des solutions auditées et permettra l'augmentation de la confiance du consommateur et des utilisateurs vis-à-vis de la marque et du produit.

Les organismes de labellisation devront faire passer les objets par une batterie de tests de sécurité incluant des analyses classiques en termes de sécurité des systèmes d'information mais devront aussi vérifier les paramètres propres aux écosystèmes IoT (radiofréquences, hardware, micrologiciel, etc.).

Se faisant, ces processus de labellisation auront comme objectif de maintenir un haut niveau de fiabilité en incitant les constructeurs à prendre en compte la sécurité dès la phase de conception du produit ou du service. A ce jour les principaux labels et certifications ont été créés dans le domaine de la santé connectée.

Outre le secteur de la santé, de nouveaux labels apparaissent progressivement pour récompenser les produits ou les entreprises les plus innovantes en matière de nouvelles technologies et de sécurité.

II. METHODES DE SECURISATION D'UNE INFRASTRUCTURE IOT

Cette stratégie de sécurité complète peut être développée et appliquée avec la participation active des différents acteurs impliqués dans la fabrication, le développement et le déploiement de l'infrastructure et des appareils IoT. Voici une description générale de ces acteurs.

1. COTE FABRICANT/INTEGRATEUR DE MATERIEL IOT

Il s'agit généralement de fabricants de matériels IoT déployés, d'intégrateurs qui assemblent le matériel de différents fabricants ou de fournisseurs de matériels dédiés à un déploiement IoT réalisé ou intégré par d'autres fournisseurs.

Sur ceux en voici les bonnes pratiques à respecter pour ces acteurs :

- ✓ **Concevoir le matériel selon les exigences minimales** : la conception du matériel doit répondre aux fonctionnalités minimales requises pour son fonctionnement, et rien de plus. Par exemple, des ports USB sont inclus uniquement s'ils sont nécessaires au fonctionnement de l'appareil. Les fonctionnalités supplémentaires exposent l'appareil à des vecteurs d'attaque indésirables qui doivent être évités.
- ✓ **Protéger l'appareil contre les falsifications** : intégrez un mécanisme permettant de détecter toute altération physique telle que l'ouverture du capot ou la suppression d'une partie de l'appareil. Les signaux de falsification peuvent être inclus dans le flux de données chargé sur le cloud, permettant d'informer les opérateurs de ces événements.
- ✓ **Intégrer la sécurité au matériel** : Si le coût des marchandises vendues le permet, intégrez des fonctionnalités de sécurité, telles qu'un stockage sécurisé et chiffré.
- ✓ **Sécuriser les mises à jour** : le microprogramme doit faire l'objet de mises à jour durant toute la durée de vie de l'appareil. Prévoyez des chemins d'accès sécurisés pour les mises à jour et un chiffrement garanti des versions du microprogramme. L'appareil sera ainsi sécurisé pendant et après les mises à jour.

2. COTE DEVELOPPEUR DE SOLUTIONS IOT

Ce développeur peut faire partie d'une équipe interne ou être un intégrateur système spécialisé dans cette activité. Le développeur de solutions IoT peut développer différents composants de la solution IoT de bout en bout, intégrer une variété de composants du commerce ou open source ou adopter des solutions préconfigurées moyennant une légère adaptation.

Voici les bonnes pratiques pour les développeurs de solutions IoT:

- ✓ **Respecter la méthodologie de développement de logiciels sécurisés**: le développement de logiciels sécurisés requiert une réflexion de bout en bout sur la sécurité, depuis le lancement du projet jusqu'à son implémentation, aux tests et au déploiement.

  Les choix des plateformes, des langages et des outils sont influencés par cette méthodologie.
- ✓ **Choisir des logiciels open source avec précaution**: les logiciels open source permettent de développer des solutions rapidement. Quand on choisit des logiciels open source, on doit tenir compte du niveau d'activité de la communauté vis-à-vis de chaque composant open source.

  Avec une communauté active, les logiciels bénéficient d'un vaste soutien, et les problèmes sont identifiés et traités. Ce n'est nécessairement pas le cas d'un projet logiciel open source obscur et inactif : les problèmes ne sont probablement pas identifiés.

3. COTE RESPONSABLE DU DEPLOIEMENT DE SOLUTIONS IOT

Une fois développée, une solution IoT doit être déployée sur le terrain. Ce processus implique le déploiement du matériel, l'interconnexion des appareils et le déploiement des solutions sur les appareils ou dans le cloud.

Voici les bonnes pratiques pour les responsables du déploiement de solutions IoT:

- ✓ **Déployer le matériel de façon sécurisée**: les déploiements IoT peuvent nécessiter un déploiement du matériel dans des lieux non sécurisés, par exemple dans des espaces publics ou des régions non supervisées. Dans ce cas, assurez-vous que le déploiement matériel est protégé contre les falsifications, autant que faire se peut. Si le matériel est doté de ports, vérifiez qu'ils sont correctement protégés. De nombreux vecteurs d'attaque peuvent les utiliser comme point d'entrée.
- ✓ **Protéger les clés d'authentification** : lors du déploiement, chaque appareil requiert des ID et les clés d'authentification associées générées par le service cloud. Protégez physiquement ces clés, même après le déploiement. Une clé compromise pourrait être utilisée par un appareil malveillant pour usurper l'identité d'un appareil existant.

4. COTE OPERATEUR DE SOLUTIONS IOT

Voici les bonnes pratiques pour les opérateurs de solutions IoT :

- ✓ **Garder le système à jour** : vérifiez que les systèmes d'exploitation et tous les pilotes des appareils sont au niveau des dernières versions.
- ✓ **Protéger le système contre les activités malveillantes**: installez les dernières fonctionnalités de protection antivirus et anti-programme malveillant sur le système d'exploitation de chaque appareil, quand celui-ci le permet. Cette pratique peut contribuer à atténuer la plupart des menaces externes. Vous pouvez protéger la plupart des systèmes d'exploitation contre les menaces en prenant les mesures appropriées.
- ✓ **Effectuer des audits fréquemment** : il est essentiel de rechercher les problèmes de sécurité au sein de l'infrastructure IoT pour traiter les incidents de sécurité. La plupart des systèmes d'exploitation offrent une journalisation des événements intégrée. Examinez les journaux fréquemment pour vous assurer qu'aucune violation de sécurité n'a été détectée. Les informations d'audit peuvent être envoyées sous la forme d'un flux de télémétrie au service cloud, où elles peuvent être analysées.
- ✓ **Protéger physiquement l'infrastructure IoT** : les attaques de sécurité les plus menaçantes pour l'infrastructure IoT sont lancées par le biais d'un accès physique aux appareils. Une pratique de sécurité essentielle consiste à protéger les appareils contre l'utilisation malveillante des ports USB et d'autres modes d'accès physiques. Pour détecter toute violation, vous devez notamment journaliser l'accès physique, comme l'utilisation des ports USB.
- ✓ **Protéger les informations d'identification cloud** : les informations d'identification cloud utilisées pour configurer et exploiter un déploiement IoT constituent peut-être le moyen le plus simple d'accéder à un système IoT et de le compromettre. Protégez les informations d'identification en modifiant fréquemment le mot de passe et en évitant de les utiliser sur des machines publiques.

Les fonctionnalités des différents appareils IoT peuvent varier. Certains appareils peuvent être des ordinateurs exécutant des systèmes d'exploitation courants, tandis que d'autres peuvent exécuter des systèmes d'exploitation très légers. Les bonnes pratiques en matière de sécurité décrites précédemment peuvent s'appliquer à ces appareils selon différents degrés.

Il se peut que les fabricants de ces appareils établissent leurs propres bonnes pratiques en matière de sécurité et de déploiement. Le cas échéant, elles doivent être observées également. Certains appareils existants et limités n'ont peut-être pas été conçus spécifiquement pour un déploiement IoT. Il se peut qu'ils ne soient pas en mesure de chiffrer les données, de se

connecter à Internet ou d'assurer un audit avancé. Dans ce cas, une passerelle de champ moderne et sécurisée peut agréger les données des appareils existants et offrir la sécurité requise pour connecter ces appareils à Internet. Les passerelles de champ peuvent assurer l'authentification sécurisée, la négociation de sessions chiffrées, la réception des commandes du cloud et beaucoup d'autres fonctionnalités de sécurité.

CHAPITRE 5: DEVELOPPEMENT D'UN SYSTEME IOT SUR PROTEUS 8.7

Proteus est un logicielle destiné à l'électronique ; il est composé de quatre modules : ISIS (éditeur de schéma électronique), ARES (qui permet la création de circuit imprimé), PROSPICE (simulateur de comportement des composant d'un schéma) et VSM (qui est un simulateur de code)

Il a été développé par la société ***Labcenter Electronics*** dans l'optique de simplifier les développements de la conception à la production des systèmes électroniques.

Sa version ***8.7*** intègre la notion d'IoT avec **l'IoT builder.**

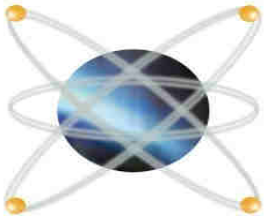


FIGURE 16: logo Proteus

I. FONCTIONNEMENT DE L'IoT BUILDER

Proteus IoT Builder pour Arduino permet de développer rapidement et facilement des applications IoT, de les simuler et de les déployer sur un smartphone ou une tablette connectée à une Arduino Yun !

Une carte Arduino Yun est une carte arduino qui possède quelques fonctionnalités avancées pour réaliser des prototypes d'objets connectés. Ainsi elle a le pouvoir de faire communiquer les capteurs directement avec un réseau local ou internet, qu'il soit filaire ou wifi. Elle simplifie considérablement la communication distante, via internet, entre un ordinateur et des capteurs.

Donc on peut dire que mettre en place une solution d'iot sera à la portée de tout un chacun; c'est maintenant la figure suivante qui va nous détailler le fonctionnement de l'iot builder.

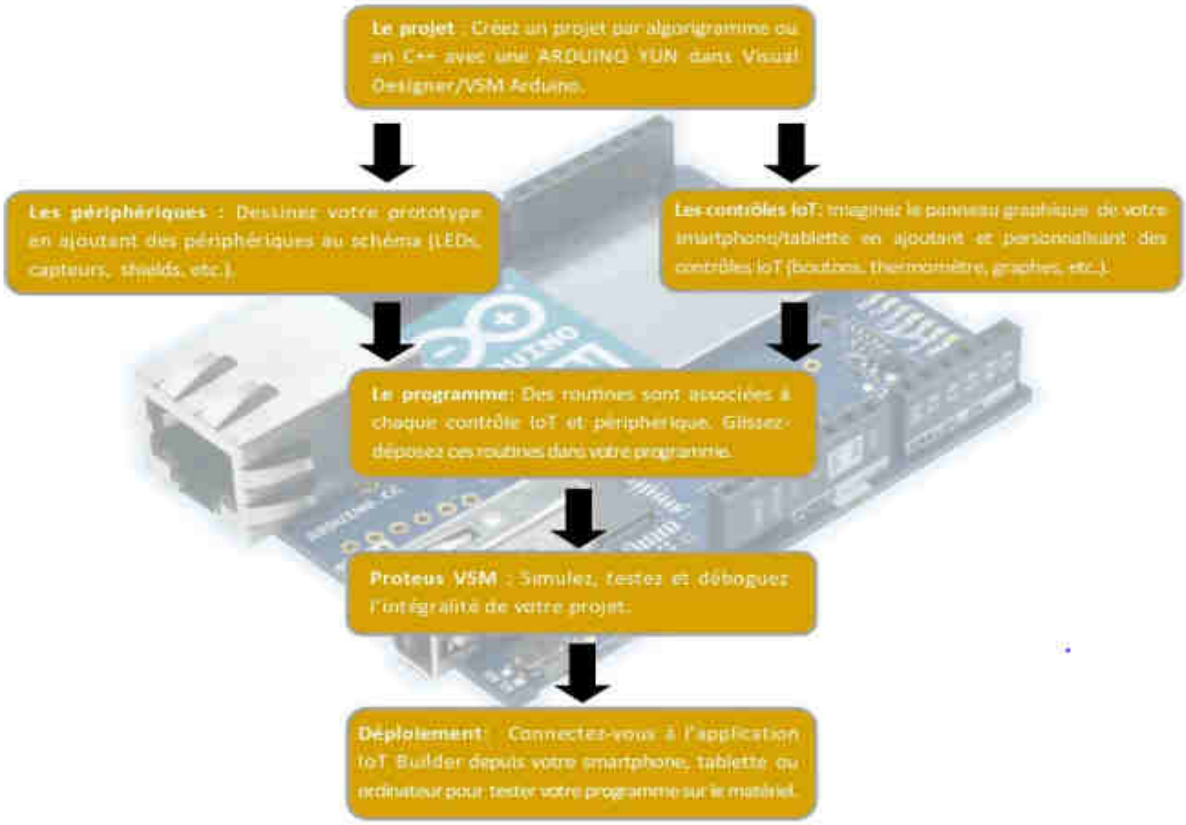


FIGURE 17:fonctionnement de l'IoT builder

II. ENONCE DU PROJET

Sur ce projet on aura à concevoir un système qui permettrait de visualiser et de pouvoir contrôler à partir de son smartphone les variations de température qui seront enregistrés par un capteur de températur. On utilisera donc une application qui porte le nom de 'IoT controller'.

Toute la conception se fera sur le module ***visual designer*** qui est implémenté sur proteus pour permettre la conception et la simulation des systèmes arduino par algorigramme. Ce qui veut dire qu'on ne va pas programmer mais utiliser seulement des blocs d'algorigramme.

Ce module dispose de plusieurs périphériques qui sont automatiquement reliés à la carte une fois choisis. Ainsi chaque périphérique est associé à des méthodes et des fonctions qui permettent de faciliter l'utilisation des blocs.

III. DETALS DU PROJET

En lançant proteus on a la page d'accueil et pour créer un projet il suffit juste de cliquer sur l'onglet 'New Project'.

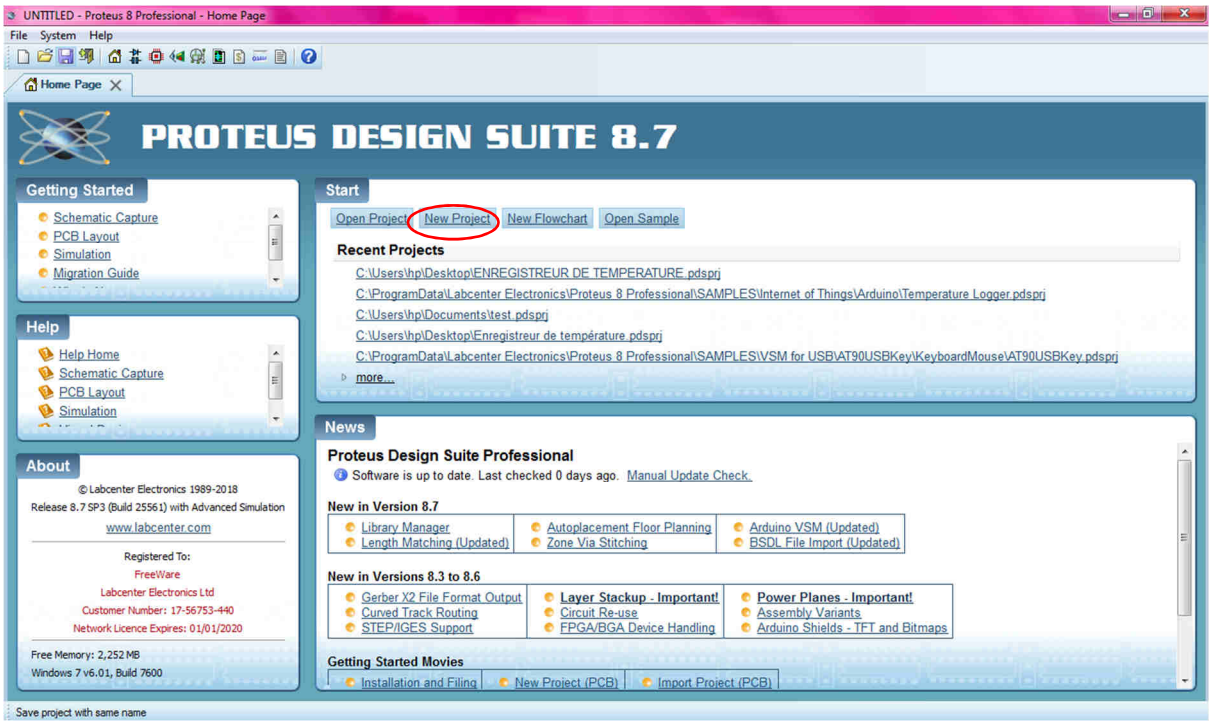


FIGURE 18: Interface d'acueil de proteus

De ce faite on aura la fenêtre ci-dessous qui nous donne la possibilité de nommer notre projet et de spécifier le chemin à suivre pour l'enregistrement.

Si tout est bien choisi on doit juste cliquer sur Next pour continuer.

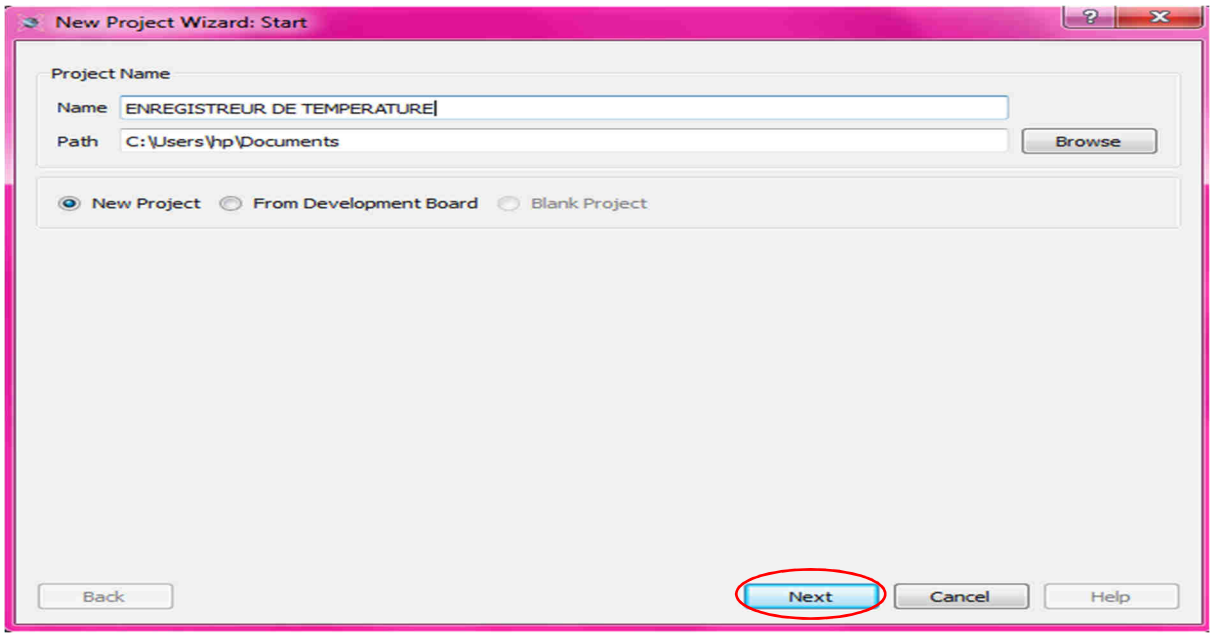


FIGURE 19: fenêtre d'enregistrement du nom du projet

En bas on a la page à laquelle on doit accéder :

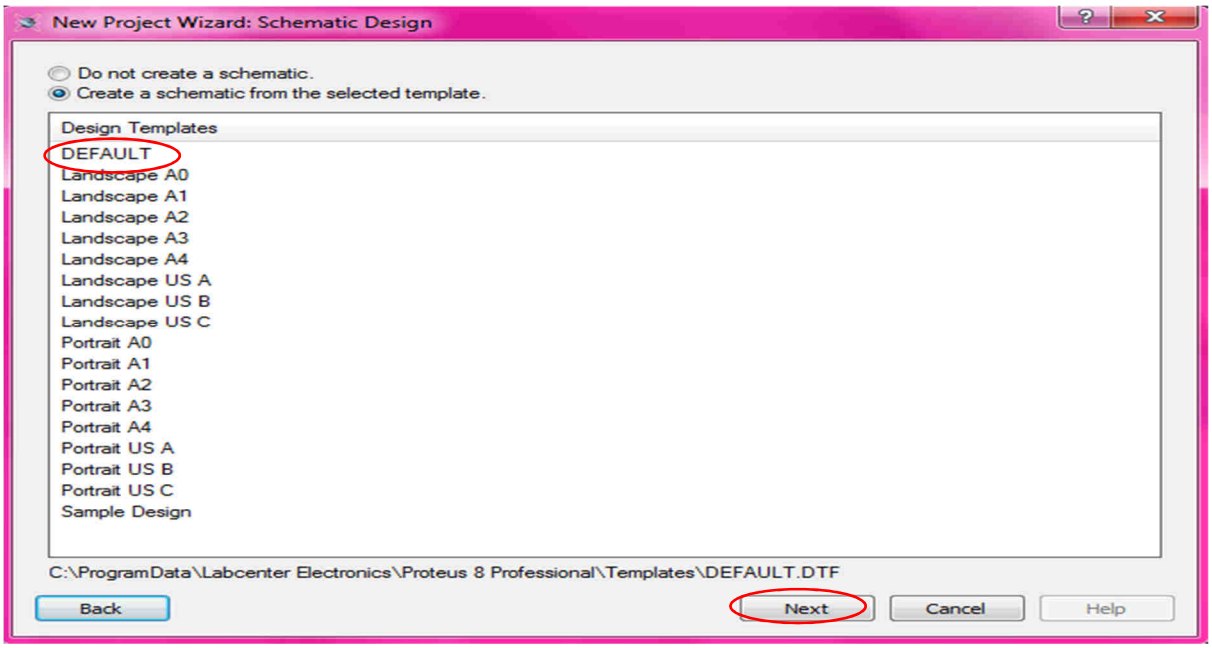


FIGURE 20: fenêtre pour le choix du design de schematic

Ici il faudrait cocher « create a schematic from the selected template » qui veut juste dire "Créer un schéma à partir du gabarit choisi".

Dans la partie "Design Templates", vous pouvez choisir entre :

- Default : Page vierge sans gabarit
- landscape : Page en mode paysage avec gabarit
- Portrait : page en mode portrait avec gabarit

Ensuite on clique sur l'onglet "Next " pour accéder à la page ci-dessous

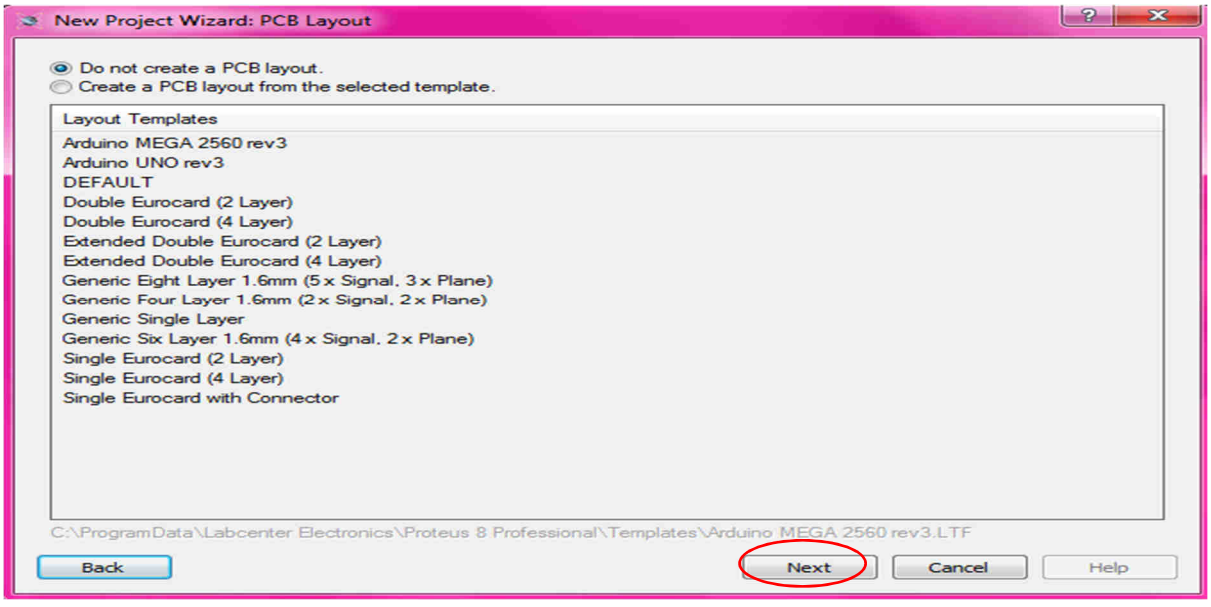


FIGURE 21: fenetre pour le choix de la création de PCB

Sur cette page on va cocher « do not create a PCB layout » et aller sur « Next » puisque dans le projet on ne va pas créer des circuits imprimés.

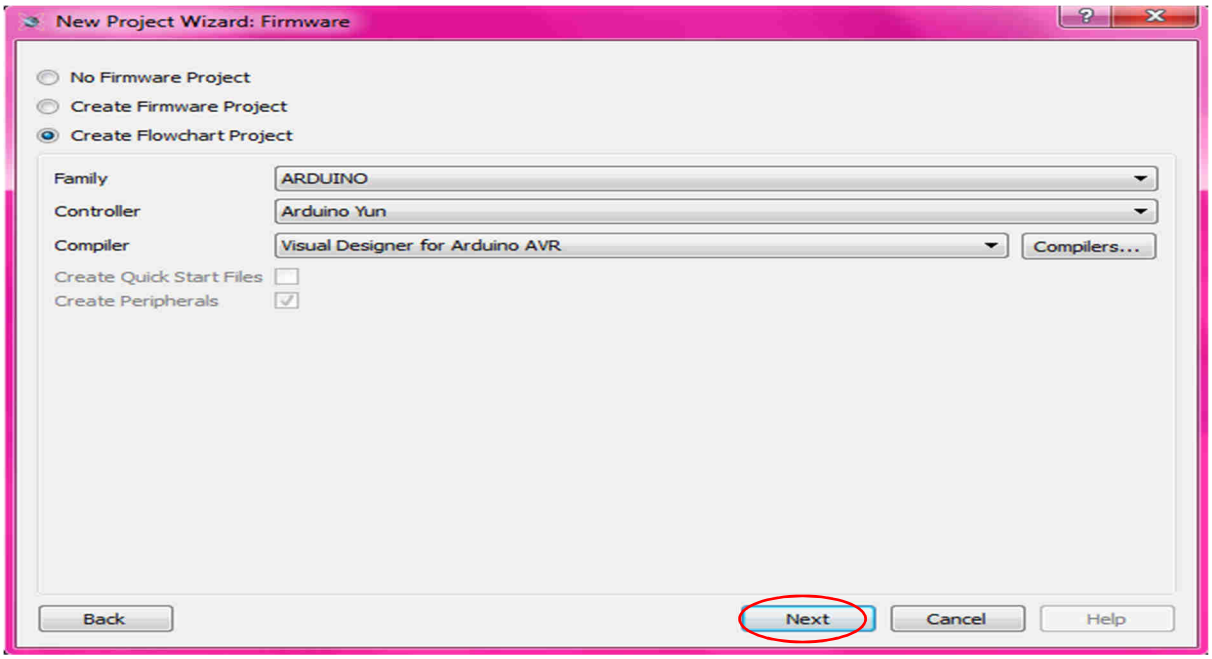


FIGURE 22 : fenêtre pour le choix de la carte et de la manière de coder

Ici on a le choix entre :

-no firmware project (aucune page de programmation)

-create firmware project: une page nous donnant accès aux codes source sera créée, ce qui veut dire qu'au préalable on a une maitrise des codes de programmation.

-create flowchart project: qui sera notre choix car c'est ici qu'on va avoir les blocs d'algorigramme déjà crées ; et notre controller sera l'Arduino Yun.

En cliquant sur « Next » on va avoir le résumé des différents choix qu'on a fait.

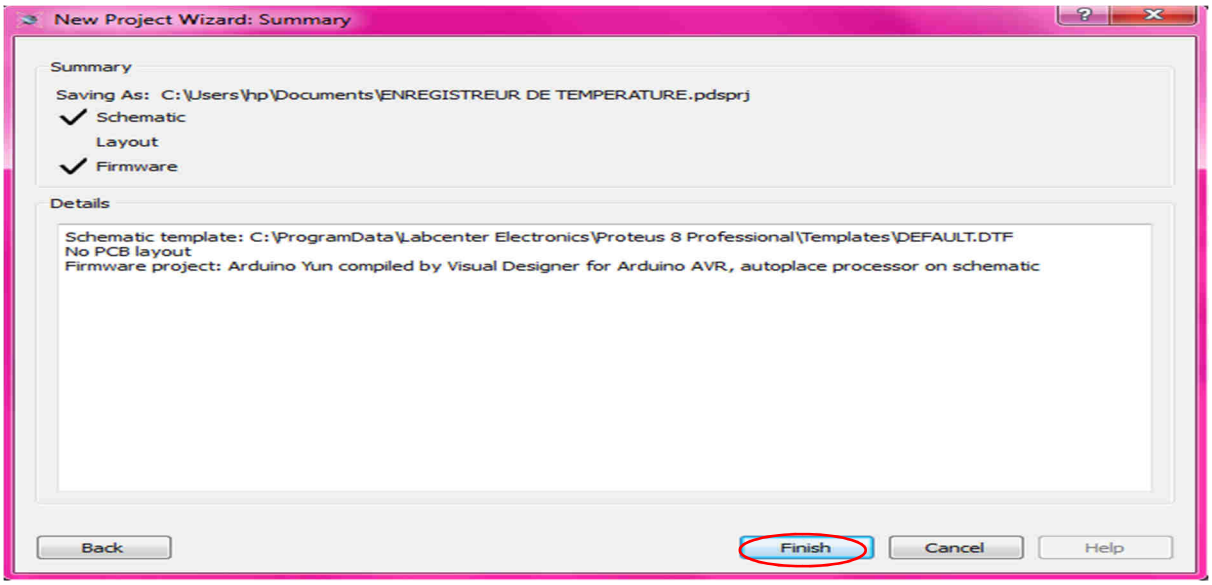


FIGURE 23: fenêtre de résumé des choix effectués

Et pour terminer on doit cliquer sur « Finish ».

Après création on aura deux onglets, l'un portera le nom de « Schematic Capture » et on va y retrouver la carte arduino yun.

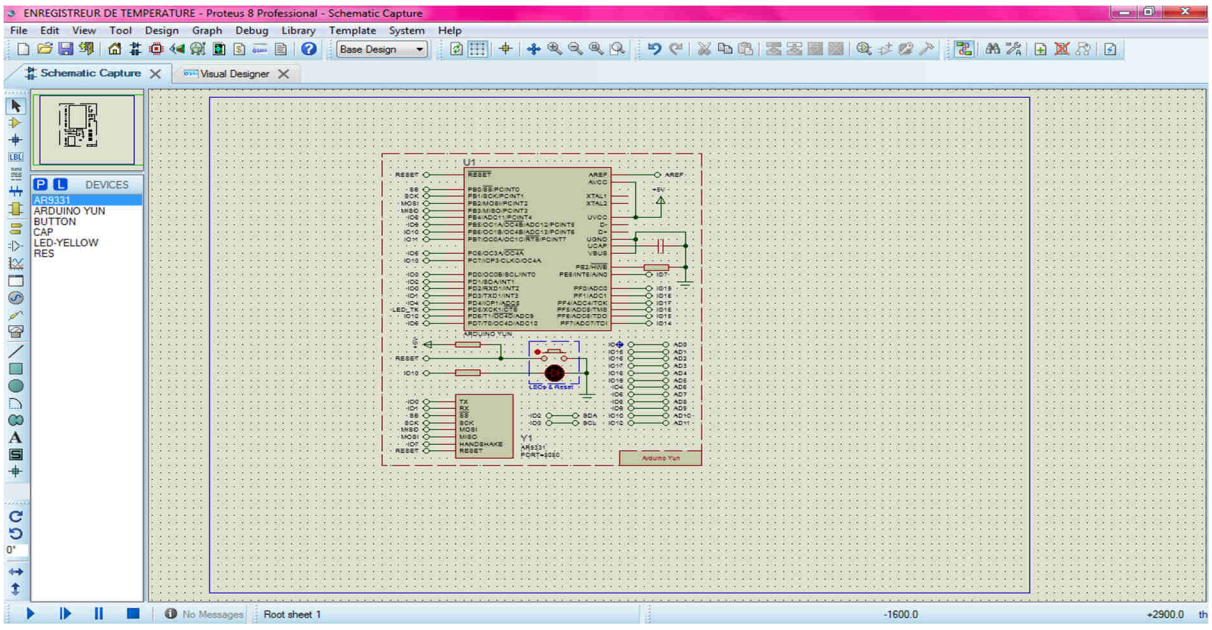


FIGURE 24: fenêtre du « schematic capture »

L'autre onglet sera le « Visual Designer » qui nous montre déjà le bloc **LOOP** (un bout de code, une instruction permettant de répéter en partie ou tout un programme) et **SETUP** (utilisé pour initialiser les variables et qui n'est exécutée qu'une seule fois, après chaque mise sous tension ou reset de la carte Arduino).

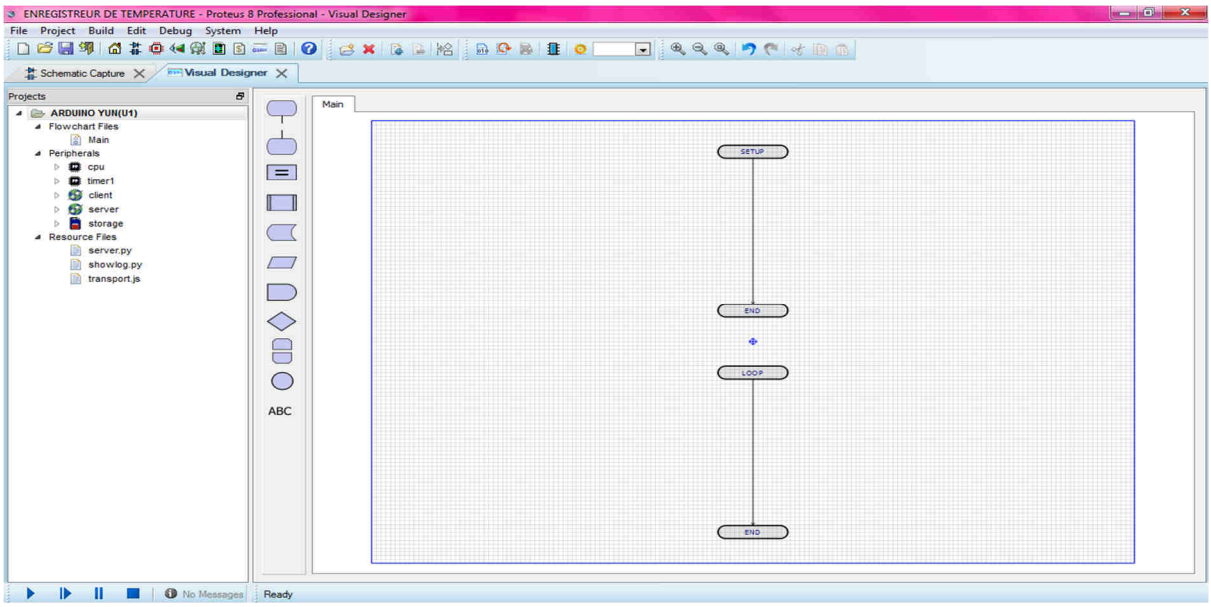


FIGURE 25: fenetre du « visual designer »

Sur ce à partir de « visual desingner » on va ajouter un périphérique qui sera notre capteur de température (composé d'une thermistance et d'un connecteur grove) en faisant clique-droit sur le dossier 'arduino yun' et en choisissant 'add peripheral'.

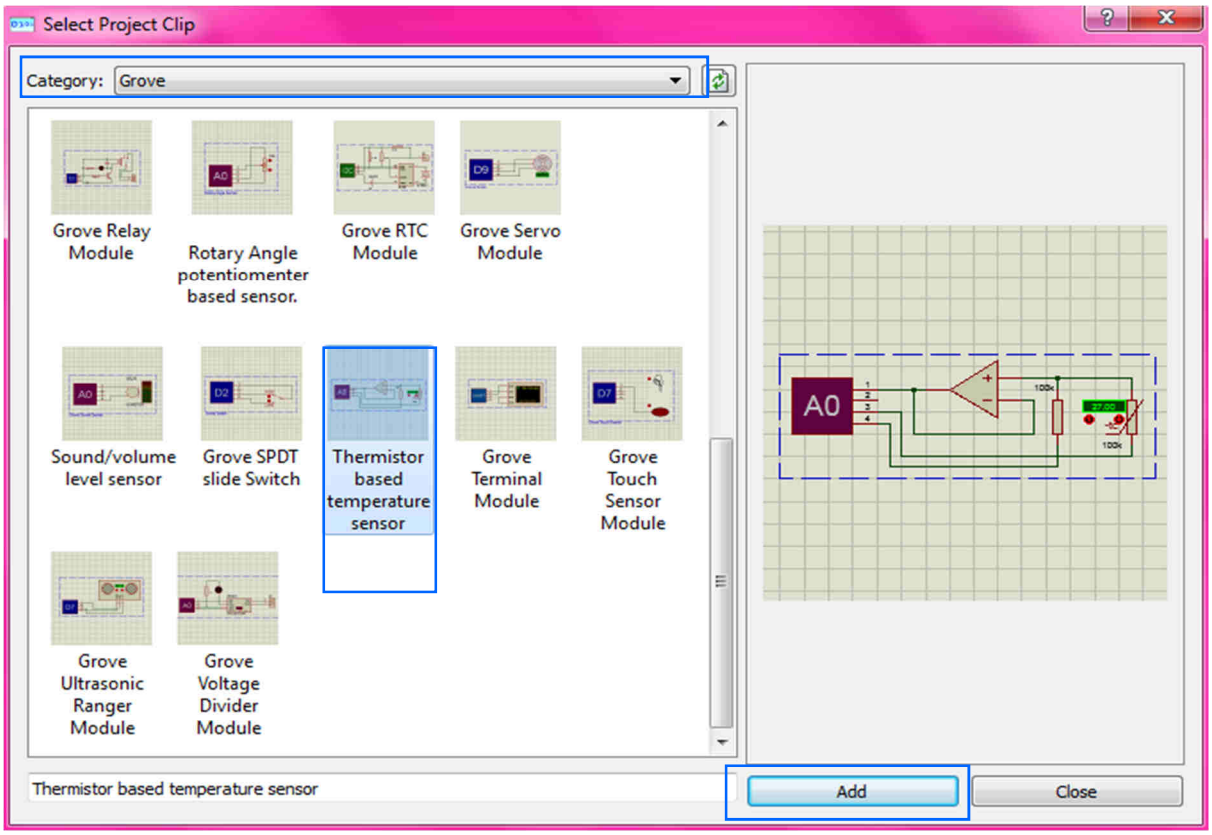


FIGURE 26: fenêtre des périphériques

Les carrés bleus représentent les choix que nous avons eu à faire.

De ce fait sur la page « schematic capture » on aura notre module grove et notre carte arduyino yun.

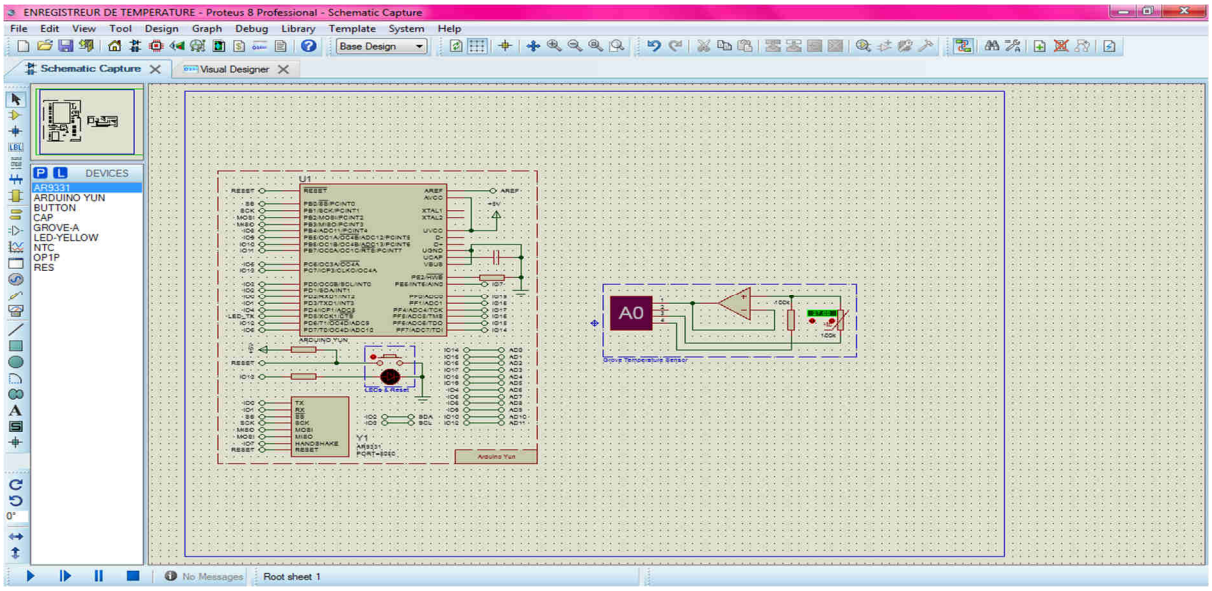


FIGURE 27 : fenêtre de "schematic capture "avec le périphérique

Maintenant on retourne sur ‘visual designer’ pour ajouter les différents ‘IoT controls’ qui permettront de contrôler les variations de température.

Donc on aura quatre boutons (un pour faire un reset et trois autres pour choisir le temps de variation c’est-à-dire en minute, heure ou jour), un thermomètre, un repére et un panneau de control où on va placer les différente ‘Iot controls’.

On fera clique-droit sur ‘arduino yun’ et choisir ‘add IoT Control’.

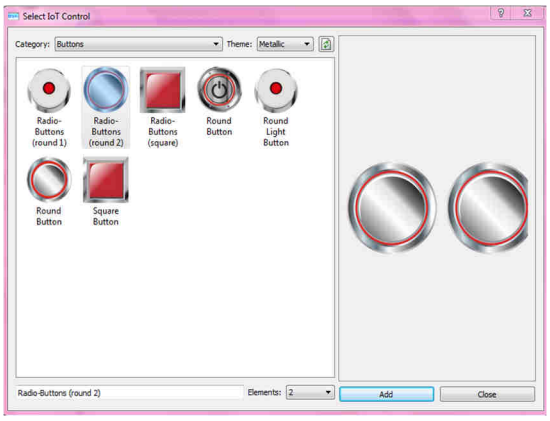


FIGURE 28: fenêtre du choix des boutons

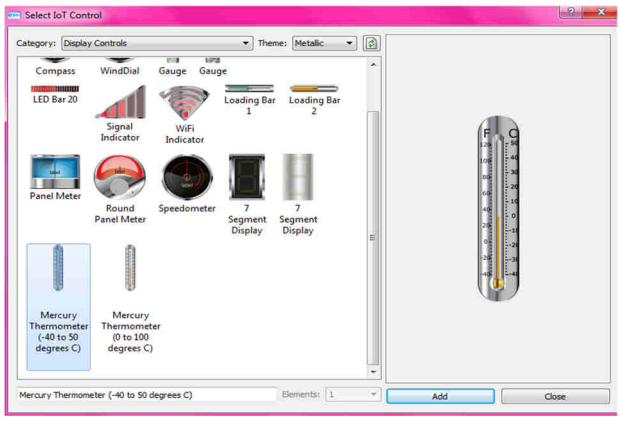
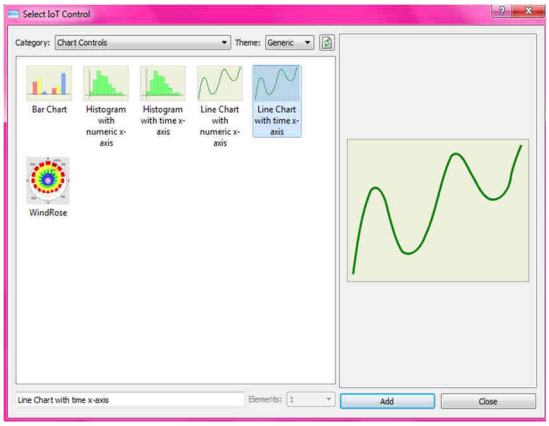
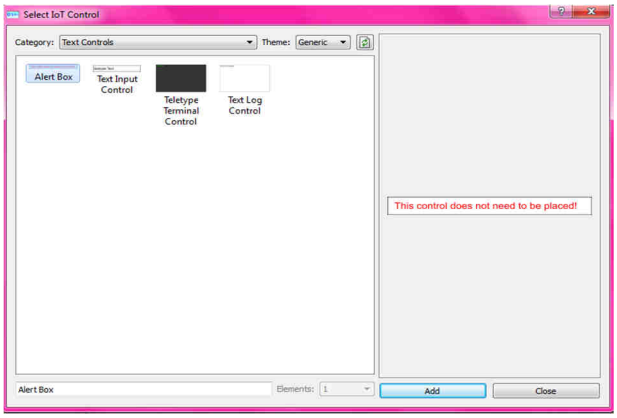


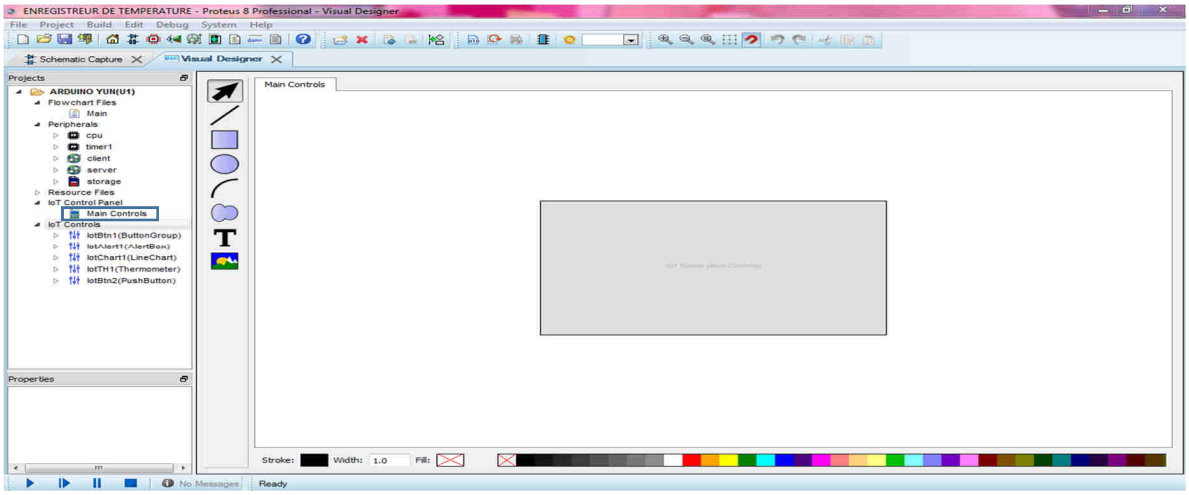
FIGURE 29: fenêtre du choix du thermomètre





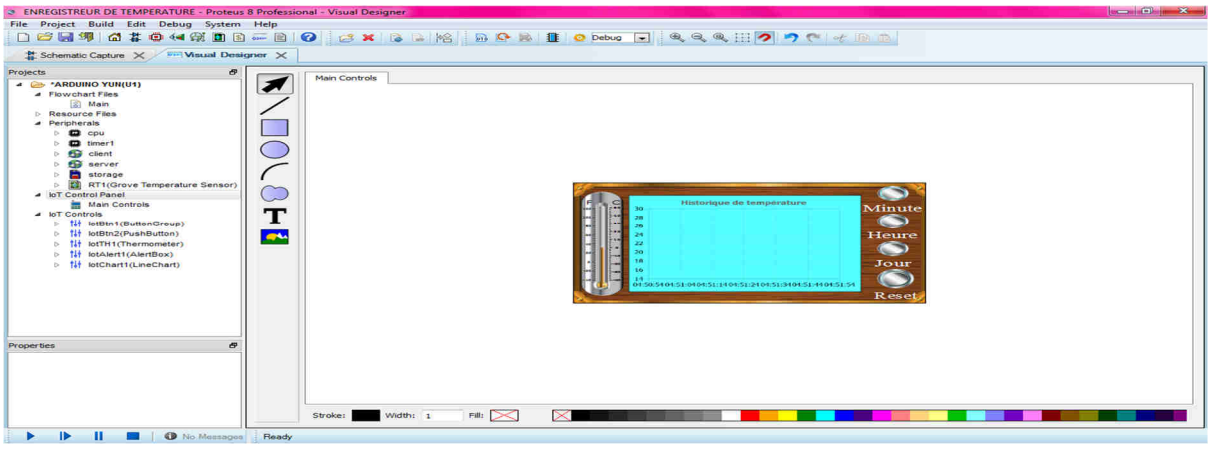
[FIGURE 30](): fenêtre du choix du repère [FIGURE 31](): fenêtre du choix du message reset

C'est sur la fenêtre suivante qu'on va glisser tous ces 'IoT control'.



[FIGURE 32](): fenêtre de 'main controls'

On aura donc:



[FIGURE 33](): fenêtre de 'main controls' avec les 'iot controls''

Apres avoir fini l'interface on va mettre les blocs d'algorigrammes en utilisasant les différents méthodes des 'IoT controls'.

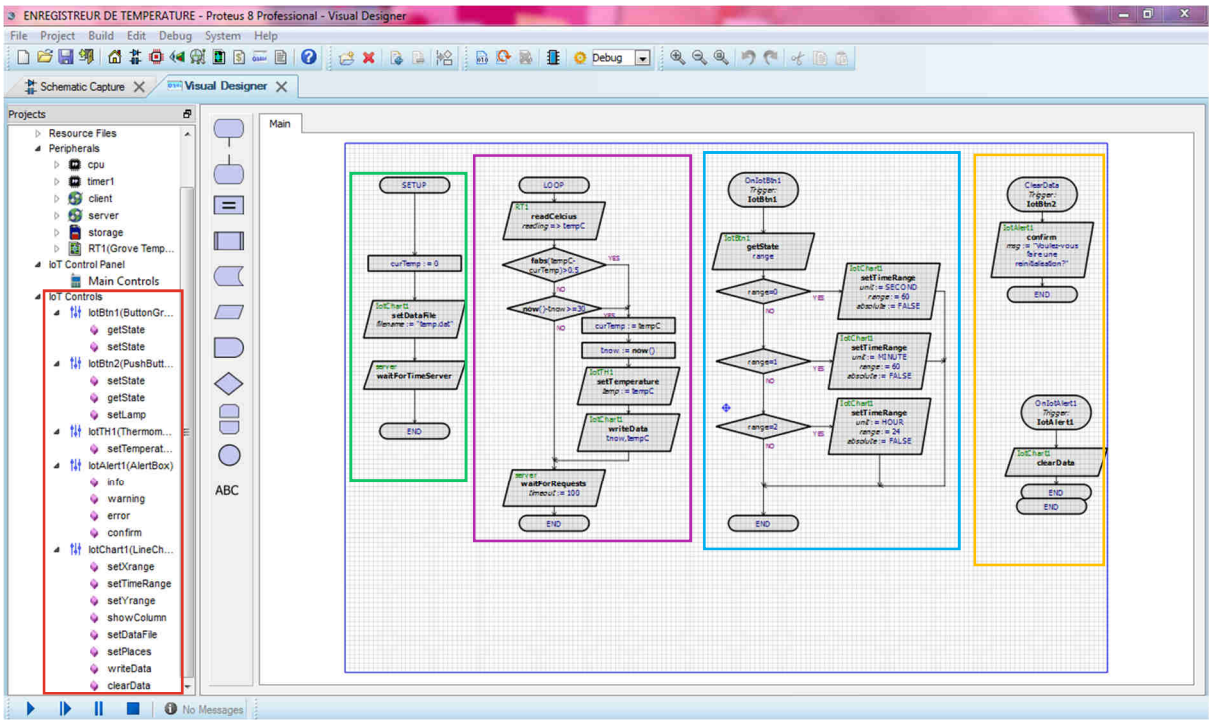


FIGURE 34: Les Algorigrammes

- Le bloc en **rouge** permet de choisir les méthodes des 'IoT Controls'
- Le bloc en **vert** permet de créer un fichier de données où seront enregistrées les températures (bloc setup).
- Le bloc en **mauve** permet d'actualiser la température periodiquement si celle-ci évolue de manière significative.
- Le bloc en **bleu** permet la gestion des trois boutons pour le contrôle du temps qu'on aurait choisi (minute, heure ou jour).
- Le bloc en **jaune** permet la gestion du bouton reset qui une fois actionné nous montre un message de confirmation ou d'annulation.

Après simulation peut avoir quatre états :

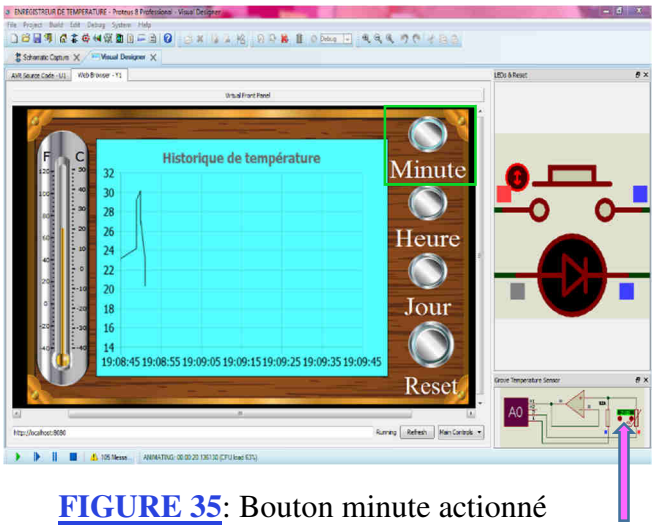


FIGURE 35: Bouton minute actionné

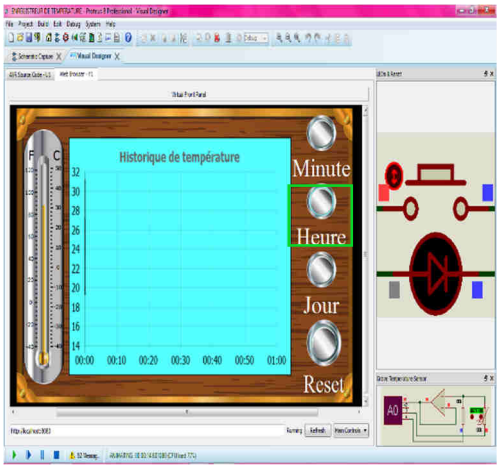


FIGURE 36: Bouton heure actionné

(Faire varier la température)

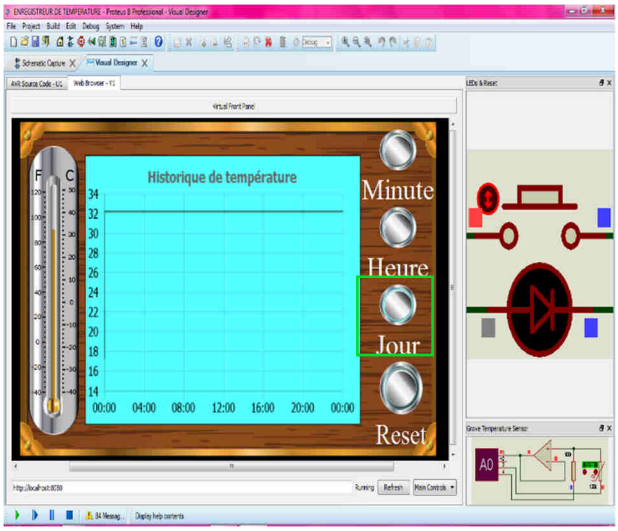


FIGURE 37: Bouton jour actionné

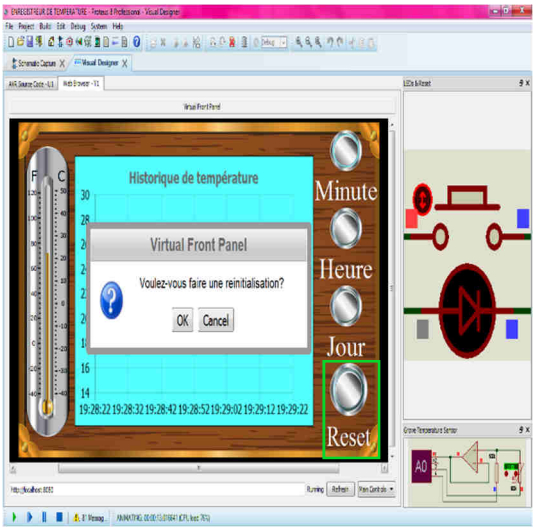


FIGURE 38: Bouton reset actionné

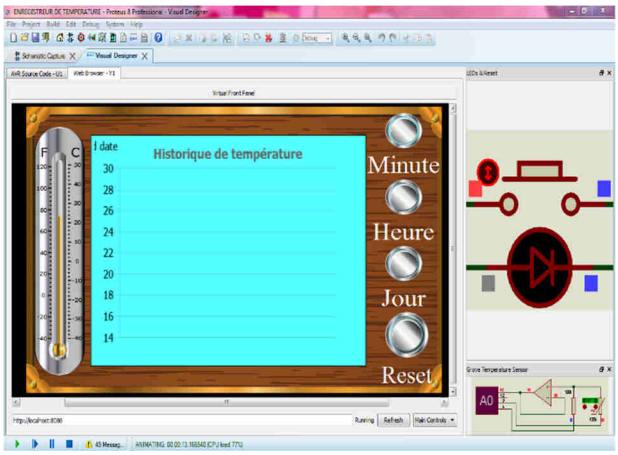
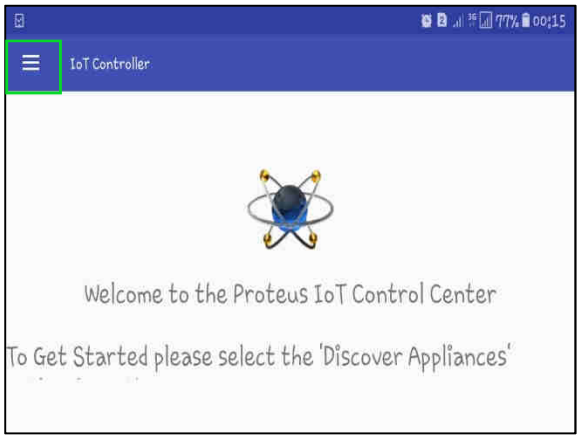


FIGURE 39: Reset effectué

Maintenant avec l'application '**IoT Controller**' il suffit juste de mettre dans le même réseau local protéus et l'application.

L'application a comme icone  et si on la lance on aura la fenêtre suivante :



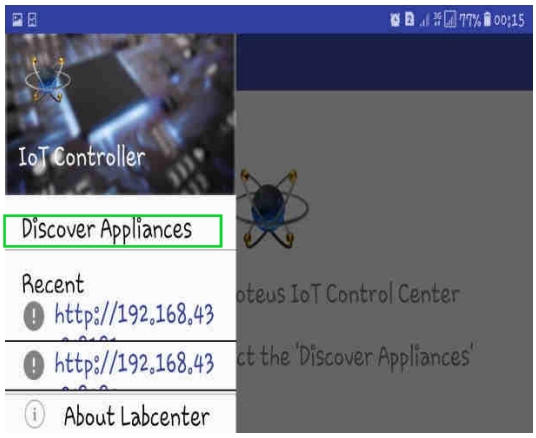


FIGURE 40: Fenêtre d'accueil de l'IoT controller **FIGURE 41**: Menu de l'IoT controller

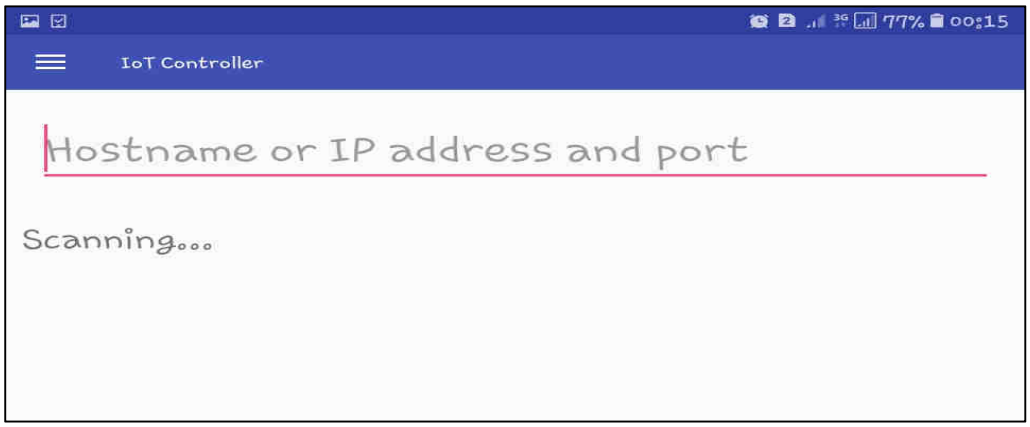


FIGURE 42: Fenêtre d'ajout d'adresse IP

En saisissant l'adresse IP de la machine et le port de la simulation on va avoir directement l'interface de simulation sur le smartphone et on va pouvoir contrôler à distance notre système.



FIGURE 43: L'interface graphique sur un smartphone

Grace à l'Iot buider de proteus et l'application IoT controller on arrive facilement à mettre en en place et à simuler une solution IoT.

IV. CONCLUSION

L'objectif de notre mémoire était d'expliciter le fonctionnement d'un système IoT en passant par les réseaux les plus utilisés, de déceler les différentes failles et d'essayer de donner les solutions qu'on pourrait appliquer à l'immédiat pour pouvoir respecter la confidentialité des données des utilisateurs finaux.

Toutefois, nous avons commencé par détailler ce sigle 'Iot' en élargissant la définition d'un objet qui n'est rien d'autre que tout ce qui peut embarquer en son sein un capteur.

Nous avons également donné les différents modèles de déploiement qui pourraient nous servir de mieux comprendre le fonctionnement et d'avoir des idées sur d'éventuels projets.
Et pour être plus claire, nous avons donné des exemples d'applications qui sont actuellement utilisés.

Par ailleurs, comme les données traitées sont d'une sensibilité très haute, nous avons fait sortir les différentes méthodes qui pourraient servir d'attaque à un mal intentionné.

Cependant, comme tout attaque doit être contrée nous avons eu a détaillé les différents mécanismes qui sont actuellement utilisés pour protéger les données.
Ce qui nous a fait comprendre la difficulté à mettre en place une sécurité à faible taux d'imperfection.

Pour finir nous avons mis en place un système IoT en utilisant le logiciel proteus et l'application IoT controller. Ce qui nous permet de manager à distance un système de variation de température.
Maintenant, il faut savoir que ce système pourrait étre déployé sur une carte arduino Yun réelle de ce fait la carte va remplacer le logiciel et les données vont transitées via un réseau wifi.

Tout ceci nous permet de constater que déployer un systéme IoT pourrait sembler facile si on ne se soucie pas de l'importance et de la sensibilité des données qui y transite.
Donc pour proposer une solution IoT il faut mettre en haut de l'échelle la sécurité des données et la facilité d'utilisation de la solution.

BIBLIOGRAPHIE

http://books.openedition.org/editionsmsh/84?lang=fr#tocfrom1n1. (s.d.).

http://www.minalogic.com/fr/actualite/des-siecles-de-reve-et-dinnovation-jusqua-liot. (s.d.).

http://www.multipower.fr/initiez-vous-a-proteus-iot-builder-pour-arduino/. (s.d.).

http://www.pearltrees.com/u/81475816-connectes-histoire-definitions#l270. (s.d.).

https://medium.com/iot-makers/les-4-fondamentaux-de-linternet-des-objets-3da39a18ae0. (s.d.).

https://www.connect-object.com/histoire-des-objets-connectes/. (s.d.).

https://www.futura-sciences.com/tech/definitions/internet-internet-objets-15158/. (s.d.).

https://www.gemalto.com/france/iot/securite-iot. (s.d.).

https://www.lemagit.fr/definition/Internet-des-objets-IoT. (s.d.).

https://www.multipower.fr/brochur/BrochureProteus.pdf. (s.d.).

https://www.welcometothejungle.co/articles/focus-sur-l-internet-of-things-iot-l-essentiel-a-savoir. (s.d.).