République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.MIRA - Béjaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle
En vue de l'obtention du diplôme Master Professionnel en Informatique
Spécialité : Administration et Sécurité des Réseaux

Thème

Conception d'un réseau de communication pour une maison intelligente en utilisant la technique d'internet des objets.

Réalisé par :

M^{elle} **KARA Nadjah**

Membres du jury :

Président : M^{r} **SAADI Mustapha**

Examinateur : M^{r} **SALHI Nadir**

Examinatrice : M^{me} **BACHIRI L.**

Encadreur : M^{r} **TOUAZI Djoudi**

Année universitaire : 2016/2017

Remerciements

Tout d'abord, je remercie Dieu le tout-puissant qui m'a donné le courage,la force et la volonté pour mener ce travail.

Un grand merci pour ma famille,à mes chers amis qui ont toujours été présents et fidèles.

A mon encadreur Mr. TOUAZI Djoudi pour tout le temps qu'il m'aconsacré, pour ces précieux conseils et pour tout son aide et son appui durant la réalisation

Aussi à tout les enseignants et employés du département Informatique à qui je doit mon avancement.

Enfin, nous tenons aussi à remercier également tous les membres de jury pour avoir accepté d'évaluer mon travail.

Dédicaces

Je tiens à dédier ce modeste travail à ma mère, ma tante et ma grand-mère.

mes chers oncles : MOKRANI Ibrahim, Madjid, Rabia, El Hamid et Said pour qui je prie Dieu de leurs accorder santé et longue vie.

A ma chère sœur NYNA pour son soutien tout au long de mes études.

A mes adorables cousins : Mohamed Cherif AMRAOUI et AbdEllali MOKRANI.

A mes chers amies : Hassiba, les sœurs Chemmache et Serina.

A mes chers amis : Fouad, Massinissa et Jonas.

Et à la personne qui m'a aidée de prés et de loin.

Liste des abréviations

IoT	**I**nternet **o**f **T**hings
IoE	**I**nternet **o**f **E**verything
RFID	**R**adio **F**requency **ID**entification)
IP	**I**nternet **P**rotocol)
SDN	**S**oftware-**D**efined **N**etworking
IdO	**I**nternet **d**es **O**bjets
URL	**U**niform **R**esource **L**ocator
TCP	**T**ransfert **C**ontrol **P**rotocol
WSN	**W**irless **S**ensor **N**etwork
GPS	**G**lobal **P**ositioning **S**ystem),
HTTP	**H**yper **T**ext **T**ransfert **P**rotocoe
NFC	**N**ear **F**ield **C**ommunication
BLE	**B**luetooth
GSM	**G**lobal **S**ystem for **M**obile
LPWAN	**L**ow **P**ower **W**ide **A**rea **N**et-work
H2T	**H**umain-**to**-**T**hing
T2T	**T**hing-**to**-**T**hing
M2M	**M**achine-**to**-**M**achine
LAN	**L**ocal **A**rea **N**etwork
WLAN	**W**irless **L**ocal **A**rea **N**etwork
FAI	**F**ournisseur d'**A**ccès **I**nternet

Table des matières

Table des figures

Liste des tableaux

Introdution Générale

Internet a évolué de telles manières que nous n'aurions jamais pu imaginer. Au tout début, les progrès ont eu lieu lentement. Aujourd'hui, l'innovation et la communication se produisent à un rythme effréné.

L'Internet des objets (IoT), comprenant des objets de tous les jours tels que les lumières, les caméras, les capteurs de mouvement, les interrupteurs et Appareils.Il est annoncé pour apporter la prochaine vague de propagation d'Internet. Les foyers, les entreprises, les campus et les villes sont attendusÊtre équipé de milliers de périphériques IoT "intelligents" qui peuvent interagir de manière autonome et être à distanceSurveillé / contrôlé.

Dans mon projet de fin d'études je vais donner une vue ensemble sur l'IoT. Le premier chapitre sera consacré à des généralités sur l'internet des objets. Le deuxième chapitre intitulé "Le réseau domistique dans une maison intelligente" dans lequel je vais appliquer l'internet des objets dans une maison personnelle. Enfin, le dernier chapitre se portera sur la simulation d'une architecture de réseau de communication des objets intelligents à l'interieur de la maison.

Chapitre 1

Introduction à l'internet des objets

1.1 Introduction

L'IoT, qui est une nouvelle vague de l'Internet, est en réalité une partie naissante de l'Internet du futur, appelé l'Internet de tous les objets ou IoE (Internet of Everything), qui vise à interconnecter les gens, les données et tous les objets, de telle sorte qu'il y ait une fusion entre le monde réel (physique) et le monde numérique (virtuel) ; les objets du monde physique vont être incorporés dans le monde virtuel de l'Internet. Cela fait appel à de nouvelles tendances et innovations que ce soit sur le plan architecture de communications ou sur le plan présentation et exploitation des services.

Ce chapitre est consacré à introduire l'Internet des objets et les aspects qui s'y rapportent.

1.2 Historique de l'Internet des objets

Dans cette section, nous citons les évènements les plus marquants sur le chemin de la concrétisation de l'IoT. Le concept d'un réseau de dispositifs intelligents a été évoqué pour la première fois en 1982, avec le premier appareil connecté à Internet à l'Université Carnegie Melon capable de signaler à son inventaire si les boissons nouvellement chargées sont bien froides. Ainsi, en 1991, Mark Weiser a introduit l'informatique omniprésente à travers son papier intitulé : "L'ordinateur du 21ème siècle " et a présenté d'avance la vision contemporaine de l'Internet des objets. Ensuite, en 1998, l'informatique ubiquitaire a commencé d'attiré l'attention par

le fait qu'elle permettrait l'incorporation flexible et efficace de l'informatique dans la vie quotidienne. Après, en 2000 la société LG annonce son premier réfrigérateur intelligent connecté à Internet. De plus, la technologie RFID (Radio FrequencyIDentification) qui est l'une des technologies constitutionnelles de l'IoT, a commencé à être massivement déployée vers les années 2003 et 2004. D'autre part, une initiative très intéressante a été prise en 2008 ; un groupe de recherche appelé IPSo Alliance s'est consacré à promouvoir l'utilisation du protocole IP (Internet Protocol) pour les réseaux d'objets miniatures intelligents.[1]

De nombreux travaux de recherches ont été succédés et se sont tous concentrés autour de la réalisation, dans les meilleures conditions, de la vision de l'Internet des objets et la mener à sa maturité en dépit de tous les défis soulevés. Cela avec la considération des progrès technologiques continus dans le marché des dispositifs intelligents et dans le domaine de technologies de télécommunication (comme : le cloudcomputing, le concept du SDN (Software-Defined Networking), etc...).[1]

1.3 Définition de l'internet des objets

L'Internet of Things (IoT) est " un réseau qui relie et combine les objets avec l'Internet, en suivant les protocoles qui assurent leurs communication et échange d'informations à travers une variété de dispositifs. ". [2]

L'IoT peut se définir aussi comme étant " un réseau de réseaux qui permet, via des systèmes d'identification électroniques normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi, de pouvoir récupérer, stocker, transférer et traiter les données sans discontinuité entre les mondes physiques et virtuels. " [3].

1.3.1 Conceptuellement : l'apparition d'identités nouvelles pour les objets

Certains définissent l'IdO comme des " objets ayant des identités et des personnalités virtuelles, opérant dans des espaces intelligents et utilisant des interfaces intelligentes pour se connecter et communiquer au sein de contextes d'usages variés ". D'autres font l'hypothèse que l'IdO 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'IdO, personnifient les objets en leur attribuant intelligence et capacité de communiquer. Elles ne reflètent pas encore la dimension concrète liée aux usages de l'IdO. [6]

1.3.2 Techniquement : une extension du nommage et convergence des identifiants

Techniquement, l'IdO 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 et des éléments physiques . Mais l'identification est directe grâce à l'utilisation d'un système d'identification électronique (puces RFID, processeur et communication Bluetooth etc.) 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.[7]

1.4 De l'IdO vers l'internet de tout (IoE)

D'après la société Cisco, la convergence entre les réseaux des personnes, des processus, des données et des objets, l'IdO va vers l'internet of Everything (IoE), ou " Internet du Tout connecté "(figure 1). C'est un Internet multidimensionnel qui combine les champs de l'IdO et du Big data.

FIGURE 1.1 – IoE (Internet of Everything)

Personnes : Connexion des personnes de manière plus pertinente et avec davantage de valeur.

Processus : Fournir la bonne information à la bonne personne (ou à la machine) au bon moment.
Données : S'appuyer sur les données pour faire ressortir les informations les plus utiles à la prise de décision.
Objets : Dispositifs physiques et objets connectés à l'Internet pour une prise de décision intelligente.

1.5 La nouvelle dimension pour l'Internet

Avec l'avènement de l'Internet des objets, la connexion Internet acquiert une troisième dimension ; en plus de la possibilité de se connecter n'importe quand et n'importe où, il est désormais possible d'être connecté avec n'importe quel objet. De plus, les objets connectés sont identifiés de façon unique et sont capable de récolter des informations environnementales (liées aux changements des paramètres de l'environnement, comme la température) ou comportementales (issues des variations d'état de l'objet lui-même ou des objets contextuels), de les traiter et de les communiquer sur Internet. D'où vient leur appellation par objets intelligents.

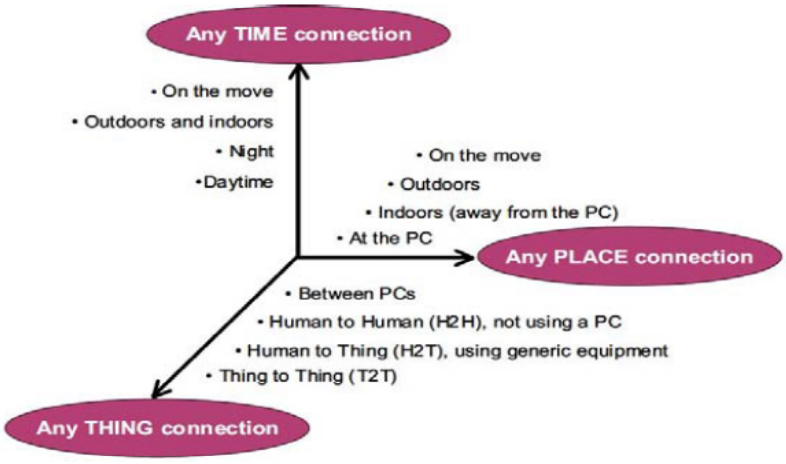

FIGURE 1.2 – Une nouvelle dimension pour l'IdO

CisCo prévoit que d'ici quelques années, spécifiquement en 2020, l'Internet des objets sera une réalité et le nombre d'objets connectés dépassera les 50 milliards [6]. A ce stade, il est nécessaire de noter que les données massives générées par un nombre immense d'objets intelligents connectés présente, partiellement, une source de la charge globale de données qualifiées de BigDatasur Internet [7]. On distingue

différents types de dispositifs connectés à l'IoT, ou qui font connecter d'autres objets à Internet, dont on cite principalement :

1.6 Technologies fondatrices de l'IoT

L'Internet of Things (IoT) permet l'interconnexion des différents objets intelligents via l'Internet. Ainsi, pour son fonctionnement, plusieurs systèmes technologiques sont nécessaires. Citons quelques exemples de ces technologies.

L'IoT désigne diverses solutions techniques (RFID, TCP/IP, technologies mobiles, etc.) qui permettent d'identifier des objets, capter, stocker, traiter, et transférer des données dans les environnements physiques, mais aussi entre des contextes physiques et des univers virtuels. [3]

En effet, bien qu'il existe plusieurs technologies utilisées dans le fonctionnement de l'IoT, nous mettons l'accent seulement sur quelques-unes qui sont, selon Han et Zhanghang, les technologies clés de l'IoT. Ces technologies sont les suivantes : RFID et WSN et sont définies ci-dessous.

1.6.1 RFID (Radio FrequenctIDentification)

Un système RFID [4] est composé d'un ou plusieurs lecteurs et d'un ensemble d'étiquettes (appelée aussi tags, marqueurs, identifiants ou transpondeurs) à micropuissances. Les étiquettes sont des dispositifs minuscules équipées d'une puce contenant des informations et une antenne pour la communication radio. Elles sont placées sur les éléments que l'on veut identifier d'une manière unique ou tracer. Les étiquettes peuvent avoir différentes formes (figure 1.7) et peuvent être passives ou actives. Les étiquettes actives sont équipées d'une batterie, elles diffusent des signaux automatiquement et d'une façon autonome, tandis que les étiquettes passives ne disposent d'aucune source d'énergie et attendent à ce qu'un signal électromagnétique leur arrive et munit de l'énergie pour pouvoir envoyer leurs propres signaux. Les étiquettes passives sont plus déployées que celles qui sont actives car leur usage est beaucoup plus flexible avec un coût nettement réduit (comparé au coût relatif aux étiquettes actives qui est nettement élevé). Une autre spécificité pas moins importante dans les étiquettes passives qui est la durée de vie. Par le fait d'être passive, la durée de

vie de l'étiquette est importante (elle reste valable tant qu'elle garde son bon état), ce qui n'est pas le cas pour une étiquette active où la durée de vie est restreinte (s'achève avec l'épuisement de la batterie).

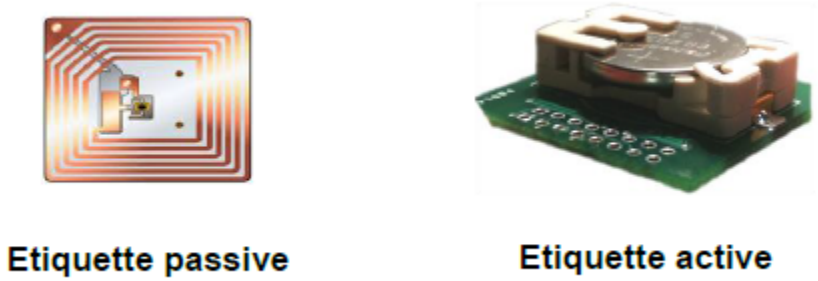

FIGURE 1.3 – Les étiquettes RFID

Le processus d'identification se réalise à travers un scénario bien déterminé. En effet, le lecteur active les étiquettes qui passent devant lui en leur envoyant un signal électromagnétique puissant. Les étiquettent s'active et réagissent en répondant par un signal transportant les identités. Contrairement aux systèmes d'identification par codes barre qui exigent que le lecteur et le code barre soient exactement opposés et très proches l'un de l'autre, dans un système RFID, il suffit juste que le lecteur et l'étiquette soient l'un dans la portée de communication de l'autre pour que l'interaction puisse avoir lieu. La portée de communication radio (appelée aussi la distance de lecture) dans un système RFID dépend du type de tag (passif ou actif) et de la gamme de fréquences utilisée. Par exemple, la portée avec les étiquettes actives est plus importante qu'avec celles qui sont passives.

Dans le contexte de l'Internet des objets, les objets intelligents ont besoin d'être identifiés de façon unique. A partir de là, l'adoption de la technologie RFID s'est avérée nécessaire.

1.6.2 Les réseaux de capteurs sans fil

Les RCSFs se composent généralement d'un grand nombre de nœuds capteurs minuscules, stationnaires ou mobiles, souvent déployés aléatoirement dans un champ de captage. Ce dernier est généralement un milieu hostile, isolé ou difficile à contrôler,

où la mission d'un nœud capteur consiste à chaque fois, de récolter, d'une façon autonome, des informations précises depuis l'environnement de déploiement. Suivant le type du nœud capteur, la donnée captée peut être la température, l'humidité, la pression, la lumière ou autres. les nœuds capteurs dans un RCSF communiquent entre eux via des liens radio pour l'acheminement des données collectées à un nœud considéré comme "point de collecte", appelé station de base ou puits. Cette dernière peut être connectée à une machine puissante, appelée gestionnaire des tâches, via Internet ou par satellite. En outre, le réseau peut être configuré de telle sorte que l'utilisateur puisse adresser ses requêtes aux capteurs en précisant l'information requise, et en ciblant les nœuds capteurs qui devraient s'y intéresser

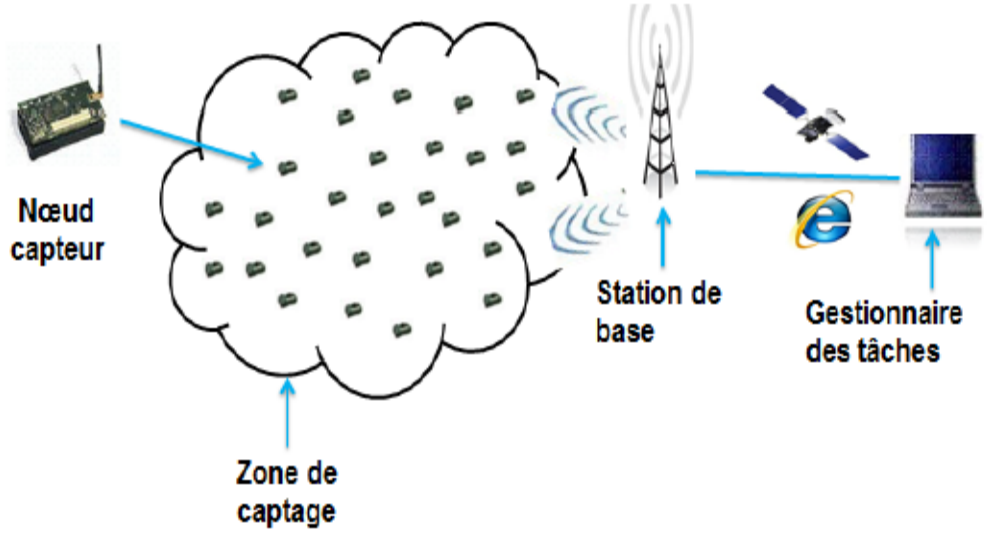

FIGURE 1.4 – Architecture de communication d'un réseau de capteur sans fil.

Les RCSFs jouent un rôle très intéressant dans l'Internet des objets. En effet, les capteurs permettent la représentation des caractéristiques dynamiques (température, humidité, pression, mouvements, ...) des objets et des endroits du monde réel dans le monde virtuel représenté par le réseau Internet global. Ainsi, avec l'incorporation des réseaux de capteurs dans l'Internet, Les capteurs deviennent des serveurs (fournisseurs de services) dans ce que l'on désigne par le web des objets (dit WoT pour Web of Things) [20].

Ainsi, les services (applications) des RCSFs se rajoutent à l'ensemble des services et applications de l'Internet de futur qui réunira une variété de réseaux fortement hétérogènes (que ça soit sur le plan matériel ou logiciel), soumis à des contraintes

différentes et qui sont déployés pour diverses applications, afin d'en avoir un monde réel très sophistiqué.

En plus de ces deux technologies principales (RFID et RCSFs), on trouve également d'autres technologies qui contribuent à la concrétisation du principe de l'Internet des objets. On parle alors des systèmes embarqués et la nanotechnologie (rétrécissement et incorporation des capteurs et autres dispositifs miniatures dans les objets à faire connecter à Internet), comme montré dans la figure suivante.

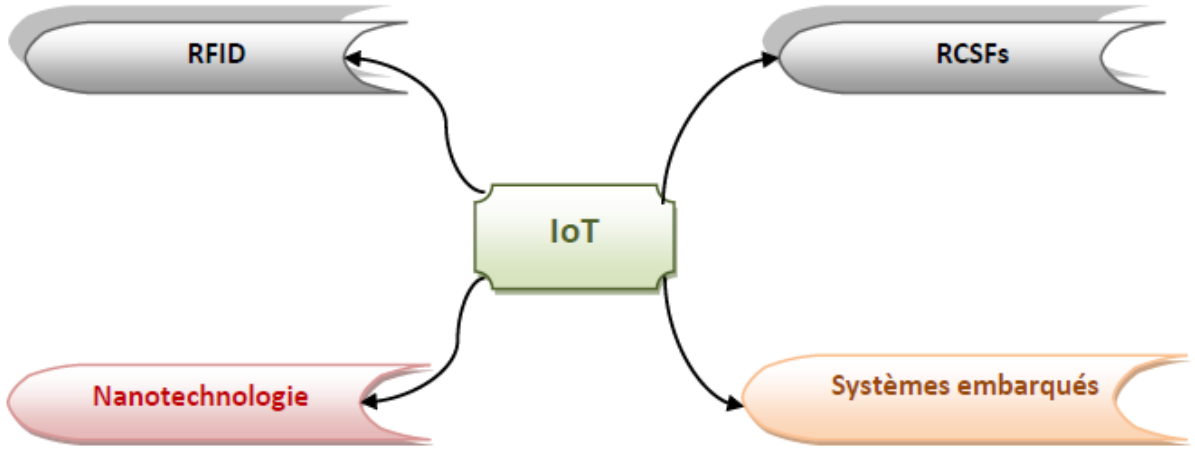

FIGURE 1.5 – Technologies fondatrices de l'Internet des objets.

1.7 Architecture de l'Internet des objets

De point de vue architectural, on peut dire que l'Internet des objets est organisée en trois couches principales [6] : la couche de perception de donnée, la couche réseau et troisièmement la couche application. La figure ci-dessous illustre telle organisation.

1.7.1 La couche perception

La couche perception, au niveau bas dans la hiérarchie, est responsable de la capture de données, ainsi que leur identification dans leur environnement. Cette couche comprend ainsi le matériel nécessaire pour parvenir à la collection de données contextuelles des objets connectés, à savoir les capteurs, les étiquettes RFID, caméras, GPS (Global Positioning System), etc.

1.7.2 La couche réseau

Cette couche se charge de la transmission fiable des données générées dans la couche perception ainsi que l'assurance de la connectivité inter-objets connectés et entre objets intelligents et les autres hôtes de l'Internet. D'autre part, il est prévu que les données issues de la couche perception soient énormes car le nombre d'objets connectés à Internet ne cesse d'augmenter à grands pas. De ce fait, il s'est avéré nécessaire de mettre en place des mécanismes et des équipements de stockage et de traitement massif de ces données sur Internet, à faible coût. Cela est bel et bien garanti par les services cloud [8] qui assurent une gestion élastique des ressources de mémorisation et de traitement sur les géants centres de données résidant sur Internet et qui sont en mesure d'absorber efficacement la charge de données générée du côté de l'Internet des objets. à ce stade, il est important de noter que le cloud utilise un concept récent dénommé SDN (Software Defined Networking) qui vise une méthode de gestion abstraite basée sur le découplage des fonctionnalités décisionnelles et opérationnelles des équipements réseau, en vue de pouvoir déployer les tâches de contrôle sur des plateformes beaucoup plus performantes que les commutateurs classiques. Cela va réduire davantage la latence réseau et rendre possible l'automatisation de la gestion du large ensemble de serveurs sur le cloud et leur auto-configuration.

1.7.3 La couche application

Quant à elle, la couche application définit les profiles des services intelligents et les mécanismes de gestion de données de différents types, provenant de différentes sources (différents types d'objets). L'architecture peut être étendue à une quatrième couche dite la couche middleware [9] entre la couche application et les deux autres couches. Cette couche sert pour une interface entre la couche matérielle et les applications. Elle comprend des fonctionnalités assez compliquées permettant la gestion des dispositifs, et traite aussi l'agrégation, l'analyse et le filtrage de données et le contrôle d'accès aux services. La couche middleware permet également la dissimulation de la complexité des mécanismes de fonctionnement du réseau et rend plus facile le développement des applications par les concepteurs.

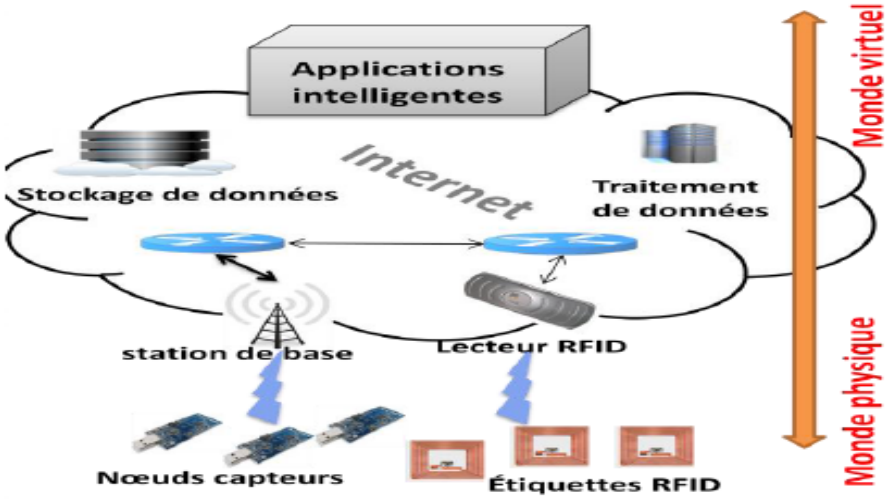

FIGURE 1.6 – Architecture de l'internet des objets.

1.8 Les objets d'identification

Codes barre, marqueurs RFID et autres dispositifs miniaturisés qui servent à l'identification et la traçabilité des objets sur lesquels ils sont collé pouvant être collés sur les objets d'usage courant (ex. vêtements, marchandises, livres, véhicules, etc.). Ce type de dispositifs nécessite qu'il y ait un lecteurpour récupérer leurs données qui seront par la suite téléchargées sur un serveur et deviennent alors accessibles via le système d'information d'une organisation ou directement sur Internet.

1.8.1 Les capteurs

Les capteurs dans l'IoT permettent de récolter des informations contextuelles concernant les objets dans lesquels ils sont intégrés, ou les environnements sur lesquels ils sont déployés. Les capteurs communiquent les informations collectées sur Internet d'une manière directe ou indirecte, tout dépend du modèle adopté pour l'intégration des réseaux de capteurs à l'internet.

1.8.2 Les drones

Un drone désigne un aéronef miniature sans pilote, pouvant porter des charges utiles, communiquer et exécuter des commandes en toute flexibilité. Les drones sont utilisés dans des applications civiles aussi bien que dans des applications militaires pour accomplir des missions bien déterminées. On entend parler de l'efficacité de

l'utilisation des drones dans le domaine commercial pour par exemple, les livraisons à domicile des commandes faites sur Internet. Aussi, des opérations de sauvetage, d'exploration et de surveillance sont réalisables par les drones dans le contexte des applications militaires. Bien que la technologie (ou bien son prototype) des drones en elle-même existait depuis bien longtemps, son exploitation idéale dans différentes applications demeure modeste. Récemment, les drones sont élus pour faire une importante part de l'Internet du futur, soit en tant que objets intelligents terminaux rapportant des données de contrôle, soit en tant que routeurs particuliers (mobiles et volants) de données entre les parties connectées à Internet. Comparés aux capteurs qui sont le plus souvent stationnaires ou dans certains cas mobiles mais dans tous les cas, manquent de l'aspect aérien, un drone parvient très efficacement à donner une vision aérienne sur l'état de la zone à contrôler même dans les zones isolée et/ou inaccessibles (là où il est difficile d'installer une infrastructure terrestre avec des points d'accès et des stations de base).

1.8.3 Smartphones et tablettes électroniques

Les smartphones et les tablettes qui sont déjà connectés à Internet par le biais de diverses technologies (Wi-Fi, 3G, 4G) permettent aux utilisateurs de communiquer à distances avec les autres types d'objets connectés dans l'IoT. Les objets intelligents peuvent rapporter en temps réel l'état actuel aux utilisateurs via Internet. Dans ce cas, les utilisateurs reçoivent des e-mails ou simplement des messages d'alertes sur leurs Smartphones ou tablettes, tout dépend de l'application. Il est meme possible que les utilisateurs supervisent ou ordonnent leurs objets connectés, à distance, via leurs smartphones ou tablettes. La figure ci-dessous présente les principaux types d'objets dans l'IoT.

FIGURE 1.7 – Typologie des objets dans l'IoT.

1.9 Cycle de vie d'un objet connecté dans l'IoT

Dans l'IoT, les objets intelligents passent par trois étapes : la phase préparatoire (bootstrapping, la phase opérationnelle et la phase de maintenance [5].

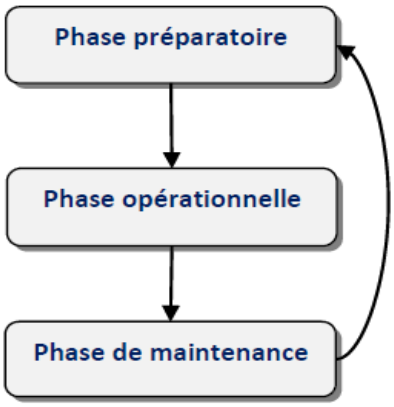

FIGURE 1.8 – Cycle de vie de l'objet.

La phase préparatoire (bootstrapping) : déploiement des objets (capteurs, tags), leurconfiguration avec les informations nécessaires, par exemple les identificateurs, les clés desécurité, etc.

La phase opérationnelle : dans la phase opérationnelle, l'objet connecté se met à réaliser sa mission qui diffère d'une application à une autre.

La phase de maintenance : effectuer des mises à jours, régler les problèmes en faisant d'éventuelles réparations des objets en cas de défaillances par exemple.

Il est même possible de remplacer carrément des objets et redémarrer à nouveau à partir de la phase préparatoire.

1.10 Fonctionnement de l'IoT

Les objets connectés se multiplient et se diversifient tant sur le marché grand public que professionnel. Ceci a engendré un nouveau besoin : celui de créer des interactions entre ces objets, au delà de leurs constructeurs ou secteurs d'activités, afin d'apporter de nouveaux services et casser ainsi les silos. Automatiser certaines tâches de la vie quotidienne (e.g., dans la domotique) ou professionnelle (e.g., dans l'industrie, le transport, la santé) deviendra ainsi possible. Les plateformes IoT ont vocation à connecter ces objets hétérogènes et les faire communiquer entre eux.

Comme introduit au début, l'écosystème IoT est assez complexe, car il intègre plusieurs technologies et domaines de compétences. Un système IoT englobe, généralement, à la fois du hardware, des protocoles de communication, du software, du cloud et du mobile. Ainsi, un projet IoT nécessite d'avoir une équipe pluridisciplinaire.

On peut décomposer un système IoT en 4 fonctionnalités distinctes comme le montre la figure ci-dessous :

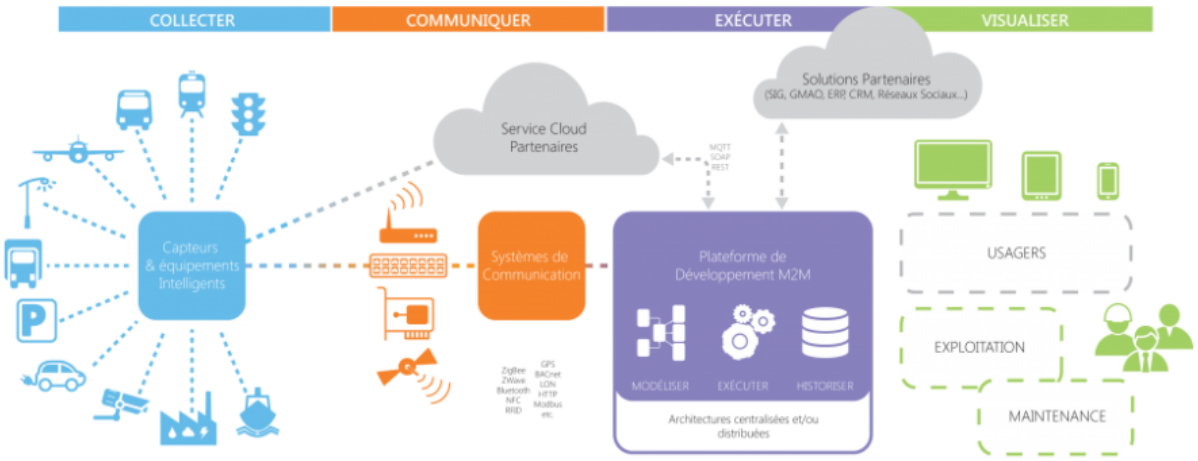

FIGURE 1.9 – décomposition d' un système IoT en 4 fonctionnalités

1.10.1 Collecter /Actionner

A cette étape, on est au niveau de l'objet connecté. On parle de capteurs qui permettent de faire des mesures de l'environnement physique (ex : température, humidité, bruit) et des actionneurs qui peuvent agir sur l'environnement (ex : des moteurs pour fermer ou ouvrir une porte). Certains objets peuvent être dotés de capacités électroniques, informatiques et réseaux qui leur permettent de se connecter directement au réseau Internet. Mais généralement, ayant des contraintes matérielles et logicielles (autonomie limité, capacité de traitement limité, pas de stack réseau, etc), les objets implémentent des protocoles de communication à basse énergie / bas débit et communiquent avec le réseau internet à travers une passerelle " gateway ".

1.10.2 Communiquer

C'est l'étape qui permet l'envoi des données depuis le réseau local vers le cloud. On parle essentiellement des protocoles pour transporter la donnée et on peut en distinguer deux modèles : Le modèle Publish / Subscribe avec des protocoles de type MQTT et le modèle REST avec des protocoles comme HTTP ou encore CoAP.

1.10.3 Executer

C'est l'étape de stockage et de traitement de la donnée. À cette étape on parle souvent de " Plate-forme IoT " qui est souvent une solution cloud capable de connecter plusieurs objets connectés, stocker leurs données, les traiter, les analyser et les exposer à travers différentes applications. Les plateformes IoT permettent aussi de faire communiquer de objets hétérogènes. Ces plateformes se multiplient de nos jours (Amazon, Google, Microsoft, etc.) et on parle même de " guerre des plateformes IoT".

1.10.4 Visualiser

C'est l'étape qui permet d'exposer les services des objets connectés à travers différentes applications dédiées. Un utilisateur, à travers une application mobile, peut par exemple communiquer avec ses objets en consultant leurs données ou en envoyant des actions vers ses objets.

1.11 Communication à l'aide des réseaux

Une des caractéristiques de l'IoT aujourd'hui est la diversité et l'hétérogénéité des réseaux existants. Nous distinguerons trois grandes familles en se basant sur la portée et la consommation énergétique des réseaux :

1.11.1 ReseauLAN(Local Area Network)

Ce sont des réseaux courte portée (entre 1 m et 100 m) et peu consommateurs d'énergie. Ces réseaux sont très utilisés comme boucles locales par les objets connectés du grand public (à l'image des box domotiques pour le smart home ou les bracelets connectés pour le smart health). On peut citer par exemple NFC, RFID, BLE et Zigbee.

1.11.2 Réseaux cellulaires

Ce sont des réseaux longue portée (de quelques kilomètres en ville à 30 km en zone rurale) et consommateurs d'énergie. À l'image des réseaux GSM, 2G, 3G ou 4G, ils permettent le transport de grands volumes de données (vidéos, images, etc.) et ont une bonne couverture au niveau national et international.

1.11.3 Les réseaux LPWAN (Low Power Wide Area Network)

Un réseau émergent dédié à l'IoT fait son essor depuis quelques années, il est encore peu connu, mais derrière lui se cache des technologies plus médiatisées tels que LoRaWan et SigFox. Cette technologie permet d'émettre et recevoir des messages de très petites tailles, sur de très longues portées (de 5km à 40km), avec pour avantage majeur que les composants utilisés pour émettre ces messages sont très peu couteux et très peu énergivores (il est donc possible avec une simple batterie, d'émettre quelques messages par jours pendant 10 ans).

1.12 Paradigmes de communication

En plus des communications humain à humain qui ont régné sur l'Internet classique, de nouveaux styles d'interactions émergent avec l'apparition de l'Internet des

objets comme le montre la figure ci-dessous qui illustre ces interactions inter objets connectés et entre l'humain et le(s) objet(s) dans l'IoT.

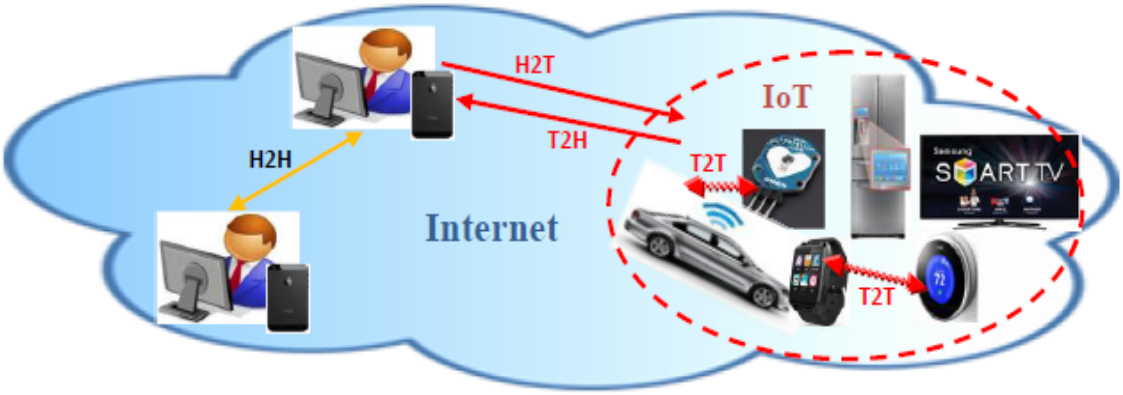

FIGURE 1.10 – L'émergence de nouveaux paradigmes de communication dans l'Internet du futur.

1.12.1 Les communications humain-à-objet

L'utilisateur peut interroger des objets connectés à Internet à tout moment via son smartphone (ou autre dispositif connecté). Les communications humain-à-objet (dite aussi H2T pour Human-to-Thing) [10] sont très fréquentes dans certaines applications de l'Internet des objets (voir section 9) comme est le cas d'une application médicale ou de l'automatisation des maisons. Tel type d'interactions est caractérisé par une forte hétérogénéité matérielle et technologique car du côté de l'utilisateur on utilise généralement des équipements beaucoup plus puissants (ordinateur portable, Smartphone ou tablette) que les capteurs contraints du côté de l'objet sollicité dans l'IoT. Cependant, l'hétérogénéité dans toutes ses formes doit être traitée efficacement.

1.12.2 Les communications objet-à-objet

Les communications objet-à-objet (ou T2T pour Thing-to-Thing) sont appelées également machine-à-machine ou M2M (Machine-to-Machine) [11]. Cela désigne des communications automatiques et autonomes inter-machines sans l'intervention humaine. En fait, les interactions inter-objets intelligents dans l'IoT sont souvent homogènes, du moins au niveau des contraintes où on trouve des capteurs qui peuvent

utiliser différentes technologies de transmission mais qui observent les mêmes limitations en termes de ressources et qui ont les mêmes vulnérabilités.

1.13 Le traitement de la donnée IoT

Il y a dix ans, le volume des données qui était généré en un an l'est aujourd'hui en une semaine. Cela représente plus de 20 exaoctets de données produites chaque semaine. Au fur et à mesure de la connexion de nouveaux périphériques à Internet, le volume de données continue à croître exponentiellement. Ces données collectées sont stockées dans des data center qui est une installation qui fournit les services nécessaires à l'hébergement des plus grands environnements informatiques qui existent à l'heure actuelle. Sa fonction principale est de permettre la continuité des activités en assurant la disponibilité des services informatiques [200].

D'une manière générale, les données sont considérées comme des informations collectées avec le temps la valeur de l'IoT réside principalement dans l'exploitation des données issues de différents capteurs. Mais avant d'extraire de la valeur de ces données, les entreprises doivent d'abord réussir la phase d'intégration de ces nouvelles sources avec les données existantes et les connecter à leurs applications internes afin de pouvoir par exemple déclencher des actions en temps réel.

1.13.1 Le model client serveur

Depuis la création d'Internet, la méthode principale utilisée par les entreprises pour le traitement des données a été le modèle client-serveur. Envisagez la manière selon laquelle les organisations peuvent implémenter des serveurs de fichiers. Les utilisateurs finaux appartenant à une organisation peuvent stocker un nombre quelconque de fichiers et de documents sur le serveur de fichiers, tout en permettant aux périphériques finaux de conserver de la mémoire et de la puissance de traitement pour les applications locales. Le stockage des fichiers sur un serveur de fichiers central permet aux autres utilisateurs de l'organisation d'accéder facilement à ces fichiers, d'où une collaboration plus efficace et un meilleur partage des informations. Enfin, la présence de services centralisés (comme les serveurs de fichiers) permet également aux organisations d'implémenter une sécurité centralisée ainsi que des procédures de sauvegarde destinées à assurer la protection de ces ressources.

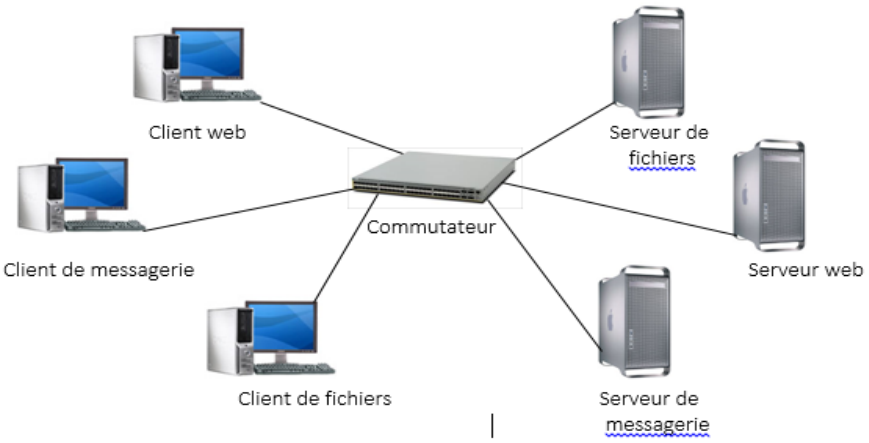

FIGURE 1.11 – le model client serveur

Avec la croissance d'Internet et l'augmentation du nombre d'utilisateurs mobiles, le modèle client-serveur n'est pas toujours la solution la plus efficace. De plus en plus d'individus se connectant à partir de distances toujours plus éloignées, l'utilisation d'un serveur centralisé peut ne pas être optimale.

1.13.2 Le cloud computing

Dans le cas du cloud computing, les données sont synchronisées sur plusieurs serveurs, de telle sorte que les serveurs situés dans un data center mettent à jour les mêmes informations que ceux qui sont situés à un autre emplacement. Les organisations peuvent tout simplement s'abonner à différents services au sein du Cloud. Les organisations individuelles ne sont ainsi plus responsables de la gestion des mises à jour, de la sécurité et des sauvegardes des applications. Ces tâches incombent dorénavant à l'organisation qui offre le service de Cloud.

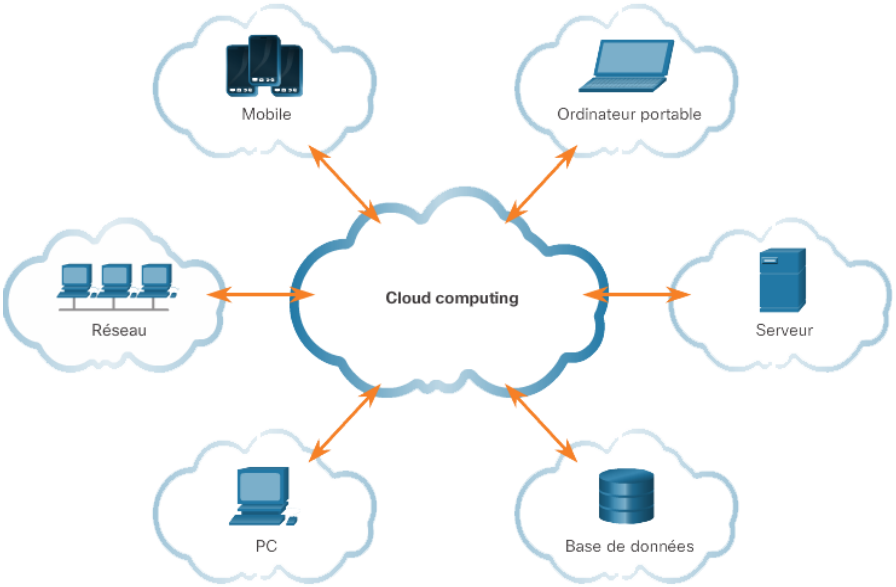

FIGURE 1.12 – Le cloud computing

Le cloud computing a permis de résoudre de nombreux problèmes du modèle client-serveur traditionnel. Il se peut toutefois que le cloudcomputing ne soit pas la meilleure solution dans le cas d'applications sensibles aux retards et qui nécessitent des réponses immédiates et locales.

1.13.3 Le fog computing

L'émergence de l'IoT requiert la prise en charge de la mobilité ainsi qu'une distribution géographique, en plus de la reconnaissance de l'emplacement et de délais minimum. Les périphériques utilisés au sein de l'IoT auront besoin de données en temps réel ainsi que de mécanismes de qualité de service. L'IoT englobe un nombre pratiquement illimité de périphériques compatibles IP, capables de contrôler ou de mesurer pratiquement n'importe quoi. Toutefois, la seule chose que ces périphériques ont en commun est qu'ils sont répartis partout sur le globe.

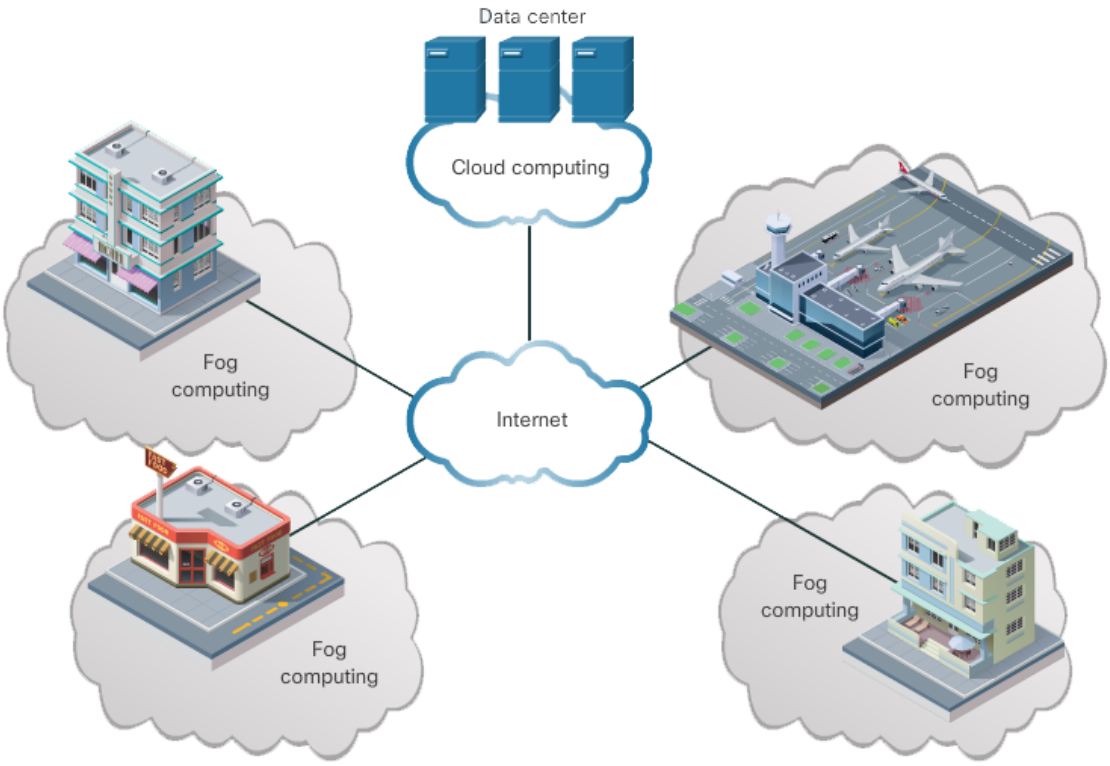

FIGURE 1.13 – Le fog computing

L'un des plus grands défis que cela représente est la création de liaisons entre ces périphériques et les data centers au niveau desquels les données peuvent être analysées, comme le montre la figure. En effet, ces périphériques peuvent générer des quantités considérables de données. Par exemple, en seulement 30 minutes un moteur d'avion à réaction peut produire 10 téraoctets de données relatives à ses performances et à son fonctionnement. Il serait inefficace d'envoyer toutes les données issues des périphériques IoT dans le Cloud pour analyse, puis de retransférer les décisions vers la périphérie. En revanche, une partie du travail d'analyse devrait avoir lieu à la périphérie elle-même, par exemple sur des routeurs de qualité industrielle, conçus pour fonctionner sur site.

Le fogcomputing crée une infrastructure informatique distribuée, plus proche de la périphérie du réseau et exécutant des tâches simples qui nécessitent une réponse rapide. Cette technologie permet de diminuer la charge liée à l'administration des données sur les réseaux. Elle améliore la résilience en permettant aux périphériques IoT de continuer à fonctionner en cas de perte de connexion réseau. Elle améliore également la sécurité en permettant d'éviter de devoir transporter les données sen-

sibles au-delà de la périphérie du réseau.

1.14 Les domaines d'application de l'Internet des objets

Nous constatons que le concept de l'Internet of Things (IoT) est en pleine explosion vu que nous avons de plus en plus besoin dans la vie quotidienne d'objets intelligents capables de rendre l'atteinte de nos objectifs plus facile. Ainsi, les domaines d'applications de l'IoT peuvent être variés.

Plusieurs domaines d'application sont touchés par l'IoT. Dans leur article, Gubbiet al. [6] ont classé les applications en quatre domaines : 1) le domaine personnel, 2) le domaine du transport, 3) l'environnement et 4) l'infrastructure et les services publics. Comme le schéma ci-dessous le montre, on trouve alors l'IoT dans notre vie personnelle quotidienne et également dans les services publics offerts par le gouvernement.

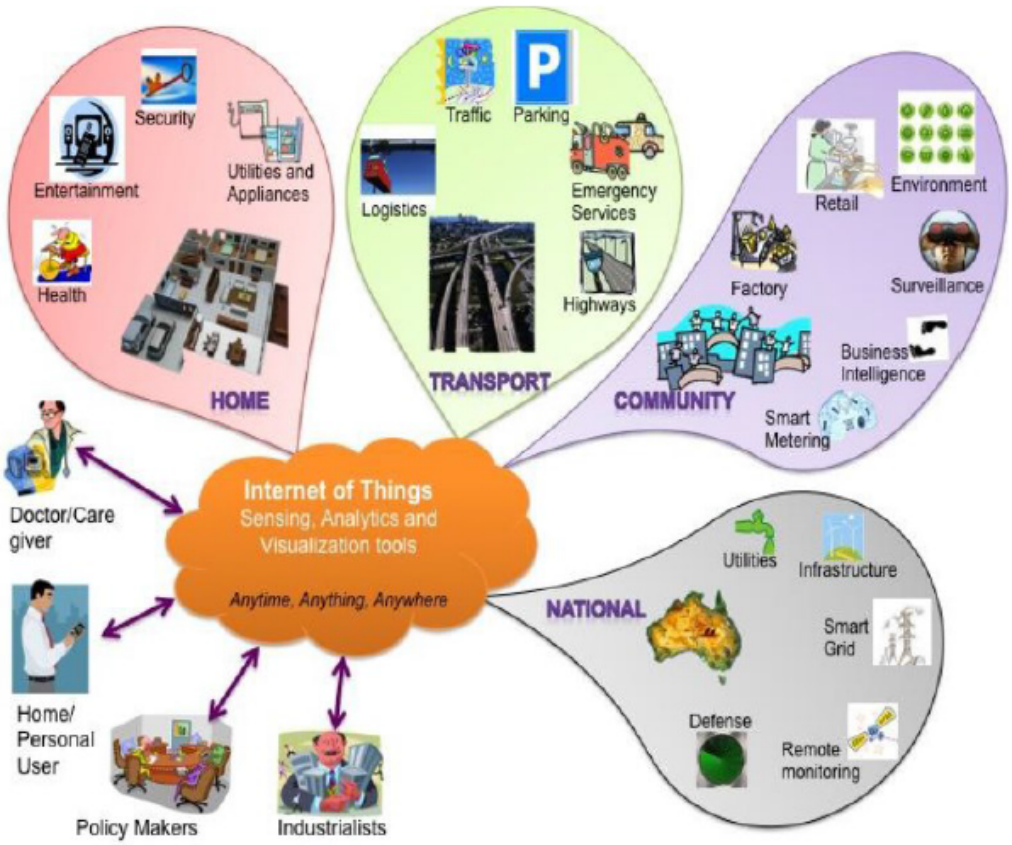

FIGURE 1.14 – Les domaines d'Internet of Things [26]

Nous pouvons affirmer que l'Internet peut être connecté à n'importe quel objet. Ainsi, les domaines d'applications de l'IoT sont multiples. On cite, à titre d'exemples, l'industrie, la santé, l'éducation et la recherche. Cependant, il sera possible dans le futur de trouver le concept de l'IoT n'importe où, n'importe quand et à la disposition de tout le monde.

Dans notre travaille on se focalise sur la maison du futur(comme on verra dans les chapitres à venir)qui contient des objets connecté à Internet accessible à distance par ses propriétaires via des Smartphones, tablette ou ordinateurs connectés

1.15 Les enjeux de l'Internet des objets

Bien que l'Internet des objets soit un concept qui est à la fois avantageux et prometteur, et qui pourra apporter des solutions efficaces des problèmes du suivi et de télésurveillance dans différents domaines. En contrepartie, l'IoT soulève certaines

questions décisives, étroitement liées à sa maturité et son acceptabilité. On cite ci-dessous les enjeux les plus marquants :

La sécurité : la sécurité des personnes, des communications, des données, des services, des réseaux et des équipements était et continue à être un problème sévère observé par l'internet courant. aujourd'hui avec la naissance de l'IoT, l'amplitude du problème va prendre un autre ordre de gravité. Des milliers d'objets contraints connectés en permanence à internet et intégrés dans toute sorte d'objets dans notre vie quotidienne, vont porter le risque d'être ciblés par les menaces classique de l'Internet. Il est même possible que de nouvelles générations d'attaques apparaissent. Donc, les objets intelligents dans l'IoT, la transmission et le stockage de leurs données sur Internet devraient être sécurisés.D'autre part, l'IoT peut lui-même menacer la sécurité des individus ou des institutions. L'armée chinoise proscrit les officiers et les soldats de porter des objets connectés (comme les montres et les lunettes connectées à Internet) et considère leur utilisation comme une violation de la réglementation sur le secret dans les casernes [12].

La protection de la vie privée des utilisateurs : un grand nombre de capteurs connectés à Internet et intégrés dans des objets d'usage quotidien révèlent nos habitudes notre état de santé notre localisation géographique et autres types d'informations qui nous sont privées. Il devra absolument y avoir des mécanismes robustes qui peuvent assurer la confidentialité des données que l'utilisateur qualifie être sensibles. Les utilisateurs devraient également pouvoir savoir qui accède quelles données (concernant les utilisateurs) sur Internet et pour quelle raison.

Les limitations de ressources : les capteurs et les tags RFID sont très limités en ressources de calculs, de stockage mémoire et d'énergie. A cet effet, les solutions (protocoles de communications ou de sécurité, technologies de transmission, etc.) destinées à l'Internet des objets doivent prendre en considération telles contraintes et limitations. ? L'hétérogénéité : des dispositifs de divers types ayant des capacités variées et appartenant à des réseaux de différentes natures, vont intégrer l'Internet en utilisant différentes technologies de communication (filaire, sans fil, satellitaire, ...). Avec toutes ces formes d'hétérogénéités matérielles et technologiques, il serait primordial de mettre en place des mécanismes bien avertis qui soient capables d'en cacher et gérer.

L'interopérabilité : c'est parmi les plus grands défis de la réalisation de l'Internet des objets. L'interopérabilité c'est, en réalité, la cohabitation des dispositifs, des systèmes et des mécanismes disjoints et la possibilité de les faire coopérer et interagir en toute flexibilité. Une tendance récente tend vers la standardisation et l'unification des systèmes et protocoles opérationnels dans l'IoT et de les présenter en open source (à accès libre). Ceci afin de faciliter la collaboration entre objets connectés, ainsi que le couplage avec les entités externes se trouvant sur Internet.

La virtualisation : plusieurs capteurs connectés peuvent représenter un seul capteur virtuel qui rapporte une mesure virtuelle résultant de l'agrégation de plusieurs états secondaires. Parexemple un capteur virtuel qui nous dit si l'état de santé du patient est bon ou non. Cette information n'est qu'une combinaison de plusieurs informations fournies par plusieurs capteurs médicaux réels incorporés dans le corps du patient. Ainsi, un model générique de virtualisation des objets connectés à l'IoT, nommé VoT (Virtualization of Things) [13] permet une représentation abstraite des objets et l'accumulation des données qui en proviennent, depuis différents endroits, pour faciliter leur contrôle.

La transparence : l'objectif de l'informatique transparente est de rendre les systèmes informatiques des boites noires transparentes à travers des communications sans fil, automatiques et invisibles ne nécessitant pas l'interaction avec les utilisateurs. La transparence est la base de l'informatique pervasive qui est à son tour un facteur essentiel dans l'Internet des objets.

Le nombre croissant d'objets connectés : il est prévu que le nombre d'objets intelligents qui vont peupler l'Internet du futur franchira les millions, voir les milliards. Avec cela, l'adoption de nouveaux mécanismes qui supportent efficacement l'évolutivité continue dans le nombre d'objets connectés, est vivement recommandée.

La mobilité : un nombre immense d'objets connectés à Internet en tant que partie de l'Internet des objets, seront le plus souvent mobiles. De ce fait, des solutions flexibles de gestion de la mobilité doivent être mises en place pour permettre à tels objets d'accomplir leurs missions efficacement indépendamment de la fréquence et la vitesse de la mobilité.

La qualité de service des communications : suivant que l'application est critique ou non, les communications inter objets connectés dan l'IoT et entre ces derniers et les hôtes ordinaires de l'internet, peuvent exiger ou non un minimum de qualité de service en termes de délais, débits, fiabilité, etc.

1.16 Conclusion

L'Internet des objets en tant qu'une évolution de l'Internet actuel permet une amélioration considérable de notre mode de vie et la façon dont les objets intelligents dans notre entourage interagissent entre eux et avec leurs utilisateurs de telle sorte que nos activités, nos biens, notre état de santé, nos dépenses,... puissent être contrôlés efficacement et d'une manière ubiquitaire. Dans ce chapitre, nous avons discuté principalement le fonctionnement, les technologies de base,le stockage de données dans l'IoT ainsi que les applications en vedette de l'IoT. Nous avons aussi mis en évidence les contraintes liées au déploiement de l'IoT et qui devraient être soigneusement traitées pour atteindre les objectifs prédéfinis.

Dans le chapitre qui suit nous entamons la connectivité des objets intelligents dans une maison connectée.

Chapitre 2

Le réseau domistique dans une maison intelligente

2.1 Introduction

L'Internet of Things (IoT) vise à connecter ce qui ne l'est pas encore. Il permet aux objets, qui n'étaient historiquement pas connectés, d'être accessibles par Internet. Avec 50 milliards de périphériques à connecter d'ici 2020, le globe lui-même deviendra un véritable " système nerveux ", capable de détecter et de traiter des quantités sans cesse croissantes de données. L'Internet of Everything peut améliorer la qualité de vie des gens, où qu'ils se trouvent, en tirant parti de ces objets connectés ainsi que des données générées, tout en intégrant de nouveaux processus permettant aux individus de prendre de meilleures décisions et d'offrir de meilleurs services.

Nous on s'intéresse à la connexion des objets à l'intérieur de l'habitat humain et à la façon dont ils se communiquent entre eux pour créer un environnement compatible au besoin personnel de l'être humain, donc quels sont les objets connectés, comment et a quoi ils sont connectés, leurs langage de programmation et Comment la connexion d'objets influence-t-elle notre vie personnelle ?

2.2 Le réseau domestique

Le réseau domestique est généralement un LAN avec des périphériques qui se connectent au routeur domestique. Souvent, le routeur possède également des fonctionnalités sans fil. Dans cet exemple, le LAN fournit un accès LAN sans fil (WLAN).[16]

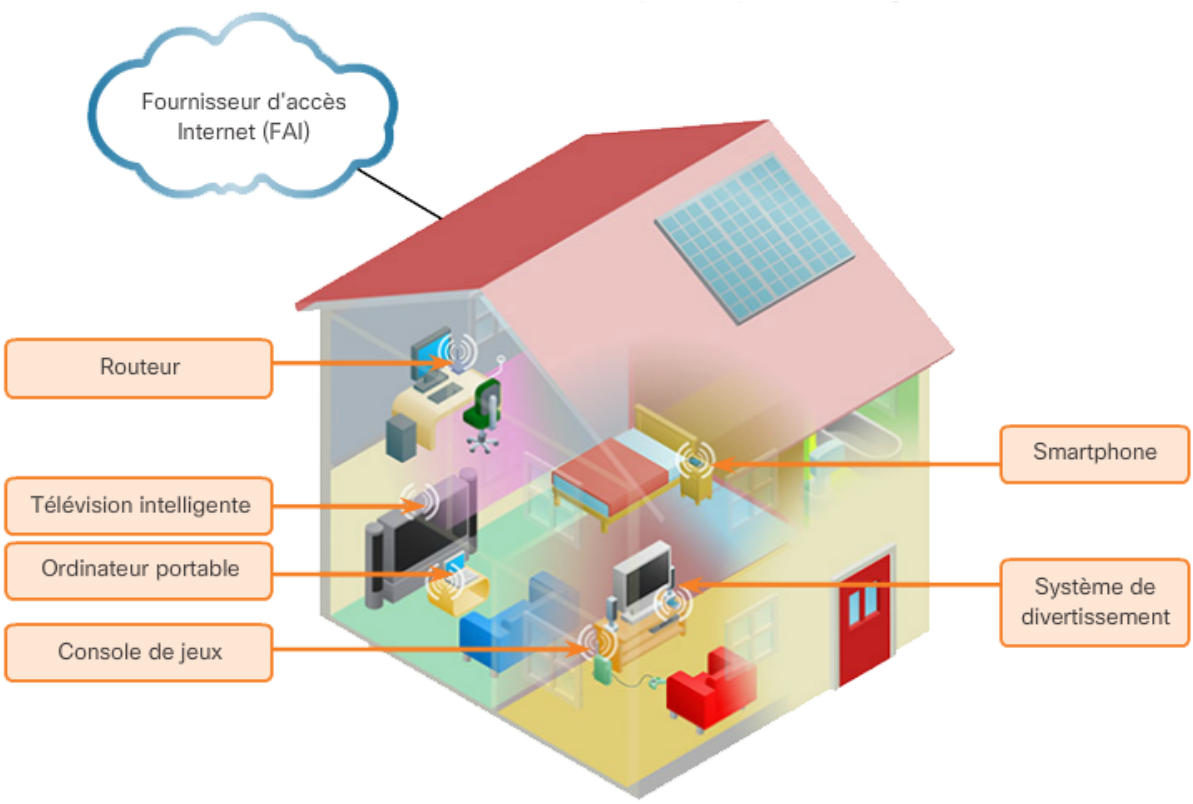

FIGURE 2.1 – Réseau local sans fil (WLAN) domestique

La Figure ci-dessus illustre un WLAN domestique classique avec une connexion à Internet établie par le biais d'un fournisseur d'accès Internet (FAI). Les périphériques et les connexions du FAI ne sont pas visibles pour un client domestique, mais ils sont toutefois critiques pour la connectivité à Internet.[16]

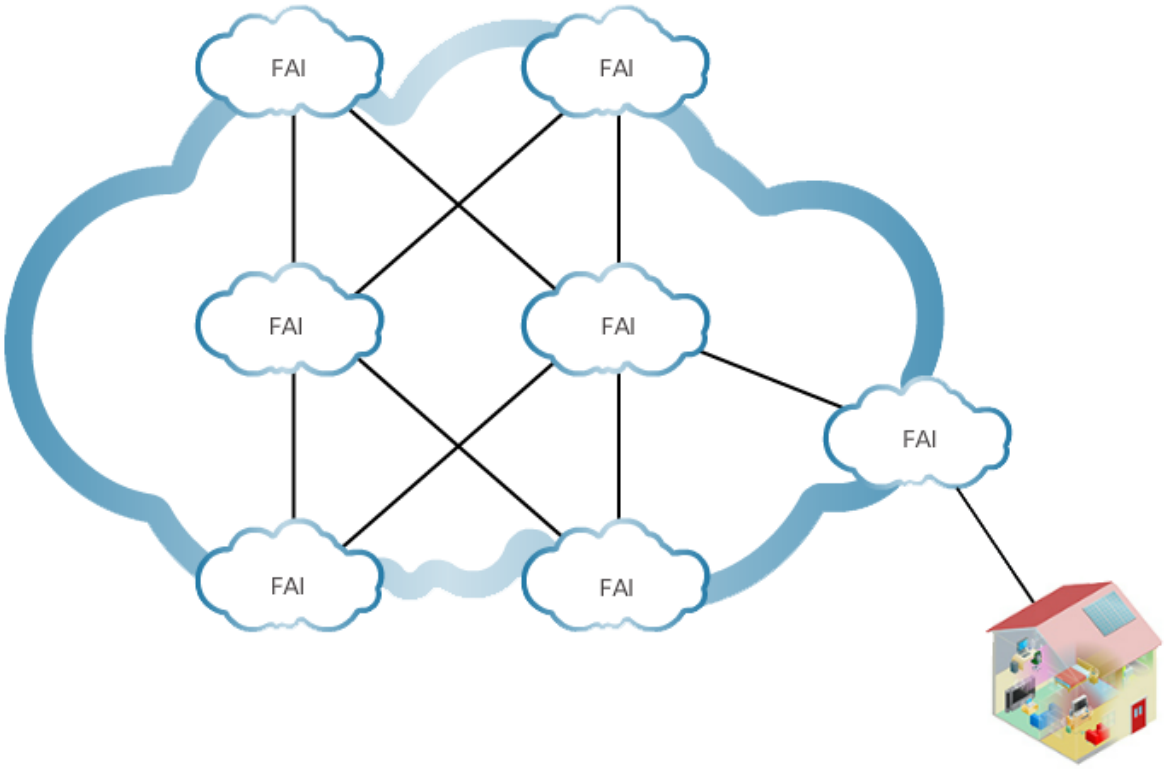

FIGURE 2.2 – Une inerconexion de plusieurs FAI

comme le montre la Figure ci-dessus, Le FAI local se connecte à d'autres FAI, autorisant ainsi l'accès aux sites Web et aux contenus du monde entier. Ces FAI se connectent les uns aux autres à l'aide de diverses technologies, par exemple des technologies WAN Toutefois, le type de connexion M2M est un type de connexion réseau unique pour l'IoT.[16]

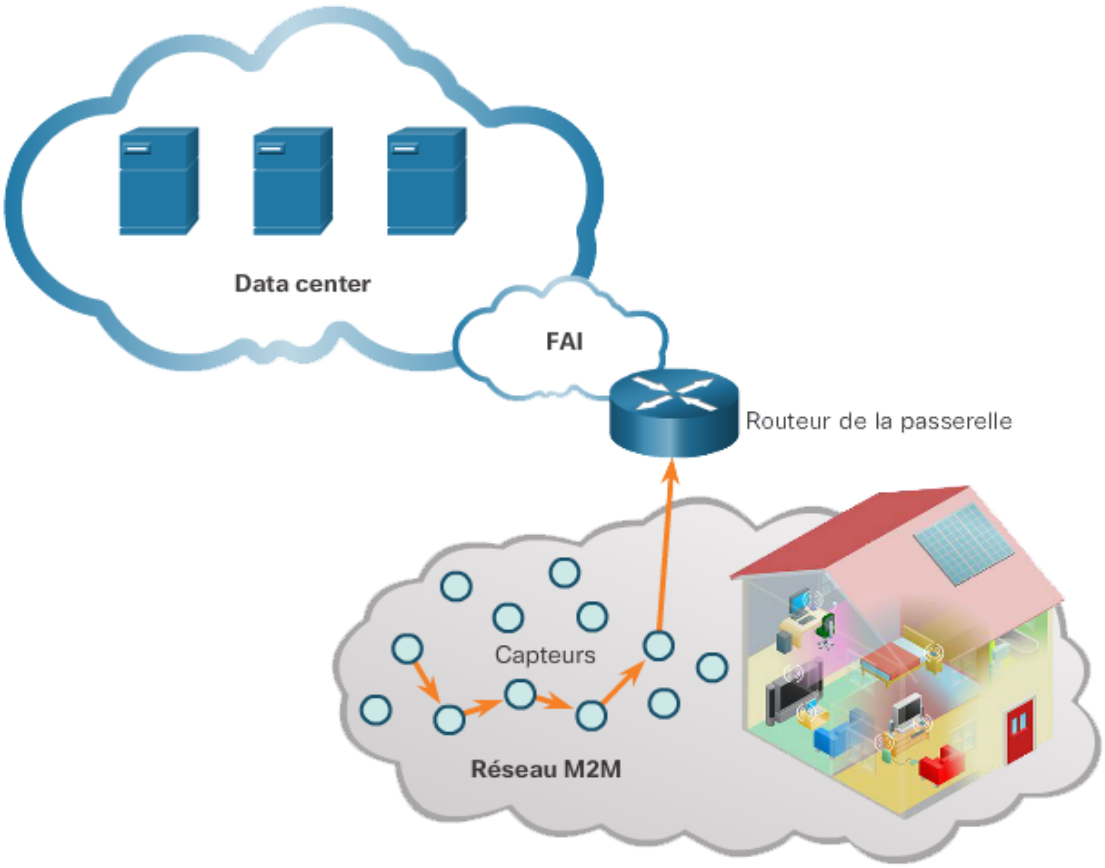

FIGURE 2.3 – Communication de capteurs

La Figure 3 montre une série de capteurs d'alarmes d'incendie ou de systèmes domestiques de sécurité, capables de communiquer les uns avec les autres et d'envoyer des données vers un environnement serveur dans le Cloud par l'intermédiaire du routeur de la passerelle (routeur domestique). Les données peuvent s'accumuler et être analysées à cet endroit.

2.3 Connexion au réseau domestique

Lorsque deux périphériques communiquent entre eux sur un réseau, ils doivent tout d'abord se mettre d'accord sur un ensemble donné de règles prédéterminées ou protocoles. Les protocoles se réfèrent aux règles de communication utilisées par les périphériques et qui sont spécifiques aux caractéristiques de la conversation.

2.3.1 Suite de protocoles

Les suites de protocoles réseau décrivent des processus tels que :

- Le format ou la structure du message.
- La méthode selon laquelle des périphériques réseau partagent des informations sur des chemins avec d'autres réseaux.
- Le mode et le moment de transmission des messages d'erreur et des messages systèmes entre les périphériques.
- L'établissement et la fin des sessions de transfert de données.

L'une des suites de protocoles réseau les plus courantes est TCP/IP (Transmission Control Protocol/Internet Protocol). Tous les périphériques qui communiquent sur Internet doivent utiliser la suite de protocoles TCP/IP. En particulier, ils doivent tous utiliser le protocole IP de la couche Internet de la pile, celui-ci leur permettant d'envoyer et de recevoir des données sur Internet[17].

Les objets qui sont compatibles IP, ce qui signifie que la suite de protocoles TCP/IP doit être installée, auront la capacité de transférer des données directement sur Internet[18].

2.3.2 Technologies de communication

La couche inférieure du modèle TCP/IP est la couche d'accès réseau. La couche d'accès réseau contient les protocoles que les périphériques doivent utiliser lorsqu'ils transfèrent des données sur le réseau. Au niveau de cette couche d'accès réseau, les périphériques peuvent être connectés au réseau de l'une des deux manières suivantes : filaire ou sans fil.

2.3.2.1 Technologies filaire

Le protocole filaire le plus couramment utilisé est le protocole Ethernet. Ethernet utilise une suite de protocoles qui permet aux périphériques réseau de communiquer entre eux par le biais d'une connexion LAN filaire. Un LAN Ethernet permet de connecter des périphériques en utilisant de nombreux types de câbles différents :

Cablecoaxial : Un câble coaxial est composé d'un fil entouré d'un matériau isolant, puis d'un blindage conducteur. La plupart des câbles coaxiaux sont également recouverts d'une gaine isolante externe.

Cable à paire torsadée : La catégorie 5 est la plus communément utilisée pour le câblage des réseaux locaux. Le câble se compose de 4 paires de fils qui sont torsadées afin de réduire les interférences électriques.

Ethernet sur courant porteur : Il est possible d'utiliser le réseau électrique d'une habitation pour connecter des appareils au LAN Ethernet.

2.3.2.2 Technologies sans fil

Il existe également divers protocoles de communication sans fil de faible portée pour les objets qui ne sont pas compatible IP et les besoins en énergie sont extrêmement faibles, afin de leur permettre d'envoyer des informations sur le réseau. Dans certains cas, ces protocoles ne sont pas compatibles IP et doivent transférer des informations à un périphérique compatible IP connecté, comme un contrôleur ou une passerelle.nous citerons :

Bluetooth : Le protocole Bluetooth est généralement utilisé entre des appareils situés l'un à proximité de l'autre.

NFC (Near Field Communication) : c'est une norme de communication entre des objets très proches, généralement à quelques centimètres l'un de l'autre. Par exemple, la NFC est utilisée dans les points de vente entre une balise RFID et le lecteur.

ZigBee : ZigBee est une autre suite de protocoles 802.15 qui repose sur le jumelage entre une source et une destination spécifiées. Citons par exemple un capteur de porte et un système de sécurité qui envoie une alerte lors de l'ouverture de la porte.

2.4 Les périphériques finaux du réseau domestique

les gens utilisent chaque jour de plus en plus des périphériques mobiles pour communiquer entre eux et effectuer des tâches quotidiennes par le moyen d'ordinateurs, d'ordinateurs portables, de smartphones, de tablettes,À l'avenir, le grand public pourrait bénéficier de ces technologies où de nombreux objets présents dans la maison seront également connectés à Internet et il sera par conséquent possible de les contrôler et de les configurer à distance.

FIGURE 2.4 – quelques exemples d'objets à connecter

Les périphériques qui ne sont pas traditionnellement connectés au réseau nécessitent des capteurs, des actionneurs et des contrôleurs.

2.4.1 Les capteurs

Un capteur est un objet pouvant être utilisé pour mesurer une propriété physique et convertir les informations recueillies en un signal électrique ou optique. Il existe par exemple des capteurs de chaleur, de poids, de déplacement, de pression et d'humidité.

Les capteurs sont généralement livrés avec des instructions spécifiques préprogrammées ; toutefois, certains capteurs peuvent être configurés de manière à modifier leur degré de sensibilité ou leur fréquence de rétroaction. Le paramètre de sensibilité du capteur est une mesure de la variation du résultat de celui-ci lorsque la quantité mesurée varie. Par exemple, un détecteur de mouvement peut être calibré pour détecter le déplacement de personnes, mais pas celui d'animaux domestiques. Un contrôleur, pouvant inclure une interface utilisateur graphique, est utilisé pour modifier les pa-

ramètres du capteur, localement ou à distance.

FIGURE 2.5 – Les différents capteurs

2.4.2 Les actionneurs

Un actionneur est un simple moteur qui peut être utilisé pour déplacer ou commander un mécanisme ou un système, sur la base d'un ensemble spécifique d'instructions. Les actionneurs sont capables d'effectuer une fonction physique.

Quel que soit le mode selon lequel l'actionneur provoque le mouvement à réaliser, sa fonction de base est de recevoir un signal, puis d'exécuter une action prédéfinie en fonction de ce signal. Les actionneurs ne sont généralement pas capables de traiter des données. En revanche, le résultat de l'action exécutée par l'actionneur se base sur le signal reçu. L'action effectuée par l'actionneur est généralement provoquée par un signal issu du contrôleur.

2.4.3 Les contrôleurs

Il existe deux types de controleurs :

Controleurs non compatible IP : Les capteurs collectent des données et transfèrent ces informations aux contrôleurs. Le contrôleur peut transmettre toute information collectée à partir des capteurs vers les autres périphériques situés dans le Fog, comme le montre la figure.

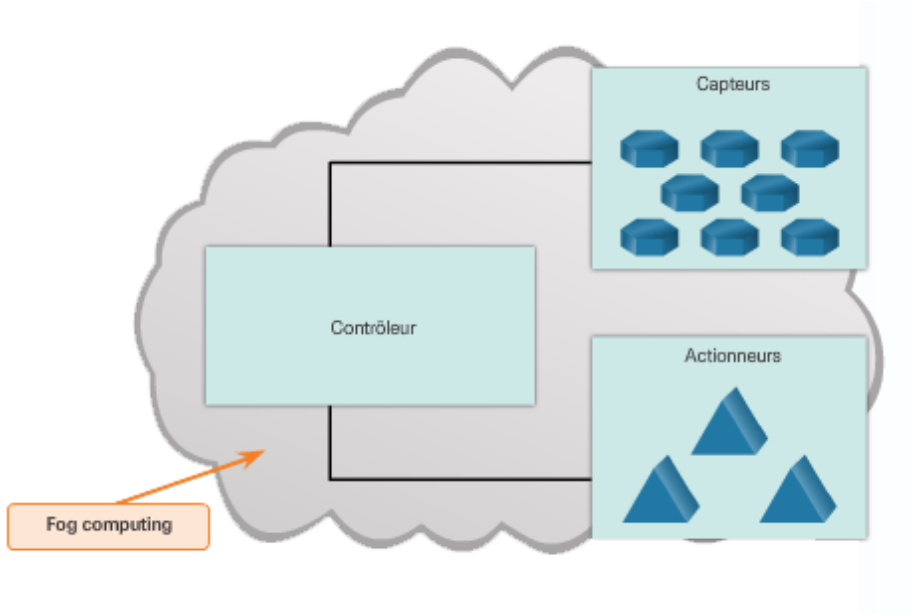

FIGURE 2.6 – contrôleurs non compatible IP

Contrôleurs compatibles IP : Le contrôleur transfère les informations sur un réseau IP, les individus étant autorisés à accéder au contrôleur à distance. En plus de transférer des informations de base dans une configuration M2M, certains contrôleurs sont également capables de réaliser des opérations plus complexes. Certains contrôleurs peuvent ainsi rassembler les informations issues de plusieurs capteurs ou effectuer une analyse de base des données reçues.

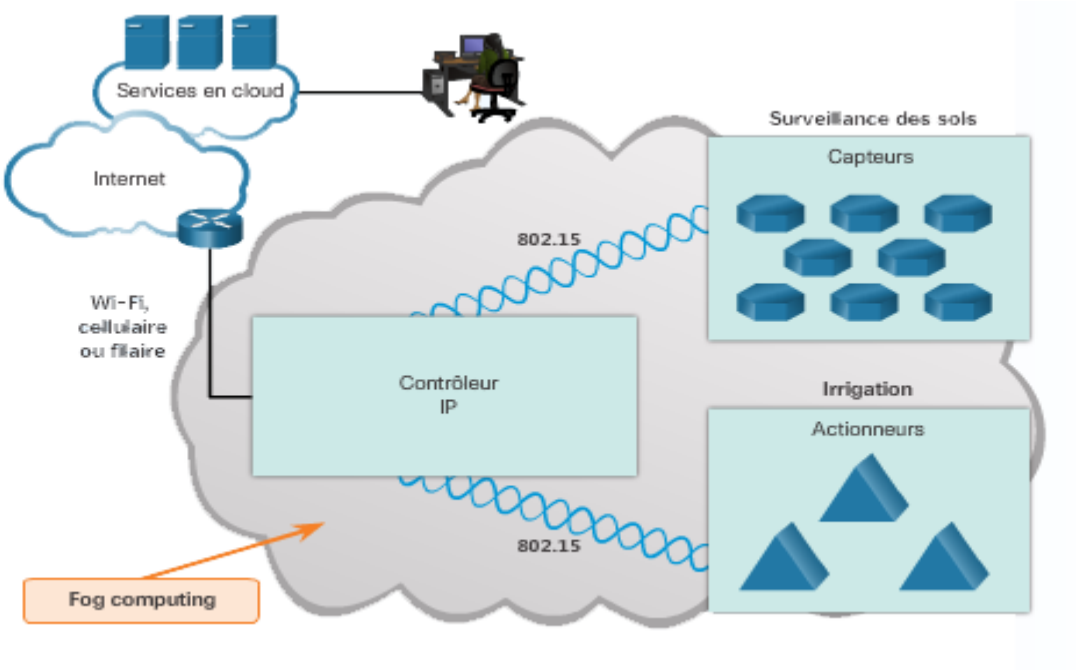

FIGURE 2.7 – contrôleurs compatible IP.

Dans ce scénario, le contrôleur collecte les informations en provenance des capteurs en utilisant le protocole ZigBee 802.15. Le contrôleur rassemble les informations reçues, puis transfère les données à la passerelle au moyen de la suite de protocoles TCP/IP.

SBC(single board computer) : est un type de contrôleurs que nous allons utiliser pour communiquer les données collectées dans notre maison intelligente pour interconnecter les objets qui ne sont pas compatibles IP.C'est un ordinateur sur une puce utilisée pour contrôler les appareils électroniques connectées à ces port el il est programmables de façon a prendre décision en fonction de données transmises.

Capteurs et actionneurs compatibles IP : Certains capteurs et actionneurs prennent en charge TCP/IP, ce qui permet de se passer de contrôleur.

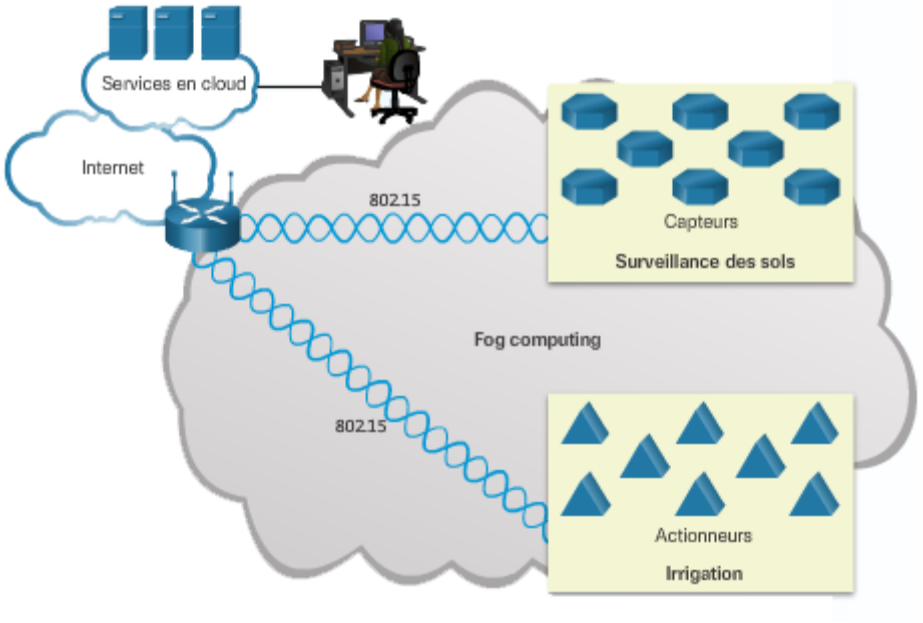

FIGURE 2.8 – capteurs et actionneurs compatible IP

La figure montre des capteurs et des actionneurs connectés directement au Cloud, par l'intermédiaire d'une passerelle. Dans cet exemple, la passerelle exécute la fonction de routage nécessaire pour permettre aux périphériques compatibles IP de se connecter à Internet. Les données générées par ces périphériques peuvent être transportées vers un serveur régional ou mondial en vue d'être analysées et traitées ultérieurement.

2.5 Les périphériques d'infrastructure

Les périphériques d'infrastructure sont principalement responsables du déplacement des données entre les périphériques des contrôleurs et autres périphériques finaux, comme le montre la figure.

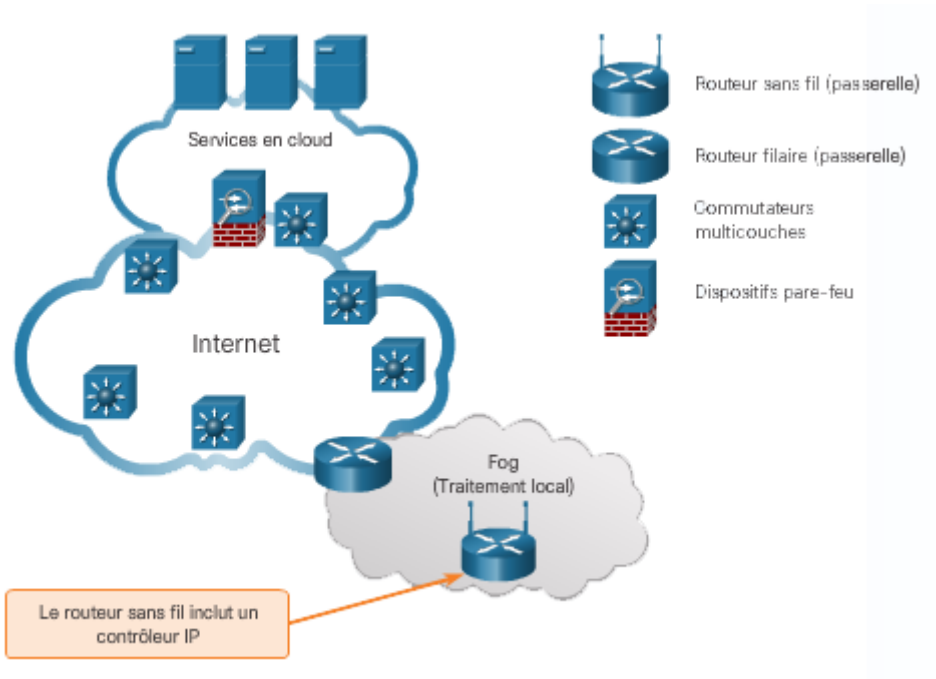

FIGURE 2.9 – périphériques d'infrastructure

Les périphériques d'infrastructure fournissent un certain nombre de services, par exemple :

- Connectivité filaire et connectivité sans fil.
- Qualité de la file d'attente des services (par exemple, les données voix avant les données vidéo).
- Disponibilité élevée.
- Transfert sécurisé.

Les périphériques d'infrastructure connectent les périphériques finaux individuels au réseau et ils peuvent connecter plusieurs réseaux individuels pour former un inter-réseau. La gestion des données lors de leur passage à travers le réseau est l'un des rôles principaux des périphériques d'infrastructure ou intermédiaires. Ces périphériques utilisent l'adresse du périphérique final de destination, ainsi que les informations concernant les interconnexions réseau, pour déterminer le chemin que doivent emprunter les messages à travers le réseau.

2.6 Programmation des objets

Comme discuté dans la section précédente, les capteurs et actionneurs sont utilisés abondamment dans l'IoT. Les capteurs mesurent une propriété physique et

transfèrent cette information sur le réseau. Comment les capteurs savent-ils quelles informations ils doivent capturer ou avec quel contrôleur ils doivent communiquer ?

Il faut indiquer aux capteurs quelles informations ils doivent capturer et où ils doivent envoyer les données. Un contrôleur doit être programmé à l'aide d'un ensemble d'instructions afin de pouvoir recevoir ces données et de déterminer s'il doit les traiter et les envoyer vers un autre périphérique.

Pour cela nous avons utilisé deux différents type de langage de programmation que nous citons ci-dessous :

Langage C : le langage C est un langage de programmation informatique très populaire. Des systèmes d'exploitation entiers ont ainsi été écrits en C. Même s'il a été initialement développé entre 1969 et 1973, l'évolution de ce langage de programmation vers la version C++ orientée objet, puis vers la version C, fait qu'il reste aujourd'hui très moderne.

JavaScript : désigne un langage informatique, et plus précisément un langage de script orienté objet. On le retrouve principalement dans les pages web.Créé en 1995 par Brendan Eich, en même temps que la technologie Java, le langage JavaScript se distingue des langages serveurs par le fait que l'exécution des tâches est opérée par le navigateur lui-même, sur l'ordinateur de l'utilisateur, et non sur le site Web. Il s'active donc sur le poste client plutôt que du côté serveur.

Python : un langage de script de haut niveau, structuré et open source. Il est multi-paradigme et multi-usage. Développé à l'origine par Guido van Rossum en 1989, il est, comme la plupart des applications et outils open source, maintenu par une équipe de développeurs un peu partout dans le monde.

2.7 Les avantages de l'Internet des objets

Nous avons cité dispersement dans différentes parties du présent chapitre quelques avantages de l'Internet des objets. Dans cette section, nous résumons les principaux avantages de l'IoT.

- Accès ubiquitaire à l'information pour un monde plus intelligent et un mode vie sophistiqué et confortable.

- Amélioration de la qualité de service et de la télésurveillance dans différents domaines d'applications, à savoir le domaine industriel, médical, etc.
- Améliorer la productivité et l'expérience-client : les objets connectés envoient des rapports à leurs constructeurs indiquant les préférences et les habitudes des clients aidant davantage les entreprises à agir de manière proactive et adaptée qui satisfait la demande et les exigences de la clientèle.
- Le gain du temps est un autre avantage de l'IoT. Les déplacements inutiles sont dès lors remplacés par une simple navigation sur le web pour commander des produits, contrôler l'état des objets et/ou endroits connectés.
- Dans certaines applications, l'IoT nous permet même de rationaliser nos dépenses et faire des économies car on ne consomme qu'en cas de besoin, que ça soit pour les achats ou la consommation énergétique (nécessaire pour l'éclairage ou la climatisation) ou autre.
- Possibilité d'exploitation des ressources géantes de l'Internet pour le stockage et le traitement des données écoulées de l'IoT.

2.8 Conclusion

Dans ce chapitre, nous avons expliqué que Pour que l'IoT fonctionne, il faut que tous les périphériques qui font partie de la solution IoT recherchée soient interconnectés, de manière à pouvoir communiquer. Il existe deux types de connexions de périphériques, à savoir les connexions filaires et les connexions sans fil. Les périphériques qui ne sont pas traditionnellement connectés au réseau nécessitent des capteurs, des RFID et des contrôleurs.

Mais comment programmer ces objets et comment les configurer d'une façon à ce que tous les objets soient interconnectés entre tout en cohérence et soumissent à exécuter les requetés de changement d'état envoyées par le propriétaire de la maison ?

Dans le chapitre qui suit, nous allons entamer l'étape de l'analyse et la simulation d'un réseau de communication des objets interconnectés à l'interieur de la maison intelligente.

Chapitre 3

Analyse et simulation

3.1 Introduction

Ce chapitre sera consacré à la description des étapes fondamentales de la conception et la réalisation du système d'information par l'identification des différents acteurs qui interagissent avec le système sous forme d'un diagramme de contexte. Par la suite, la description des cas d'utilisation et la présentation du diagramme global de ces derniers, qui décrit les scénarios nominaux de chaque acteur ainsi que les diagrammes de séquence qui représentent les interactions entre l'acteur et les objets. Pour conclure, nous présentons des captures qui illustrent la configuration et la programmation.

3.2 Etude préliminaire

3.2.1 Identification des acteurs

Un acteur représente un rôle joué par une entité externe (utilisateur humain, dispositifs matériels ou autre système) qui interagit directement avec le système étudié. Un acteur peut consulter et/ou modifier directement l'état du système, en émettant et/ou en recevant des messages susceptibles d'être porteurs de données.[21]

L'acteur humain qui interagisse avec notre système est le propriétaire de la maison.

3.2.2 Diagramme de contexte du système

Dans la figure ci-dessous, seront illustrés les différents acteurs qui interagissent avec le système à réaliser.

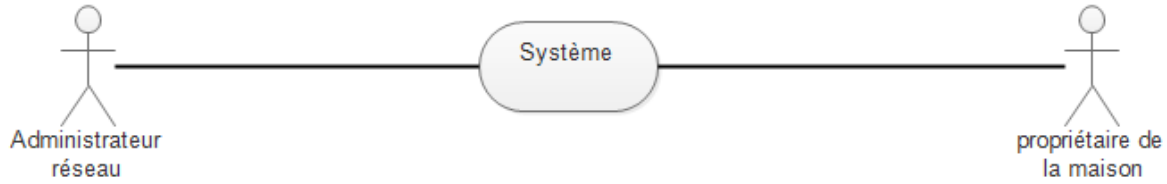

FIGURE 3.1 – Diagramme de contexte du système.

3.3 Etude des besoins fonctionnels

3.3.1 Identification des cas d'utilisation

Un cas d'utilisation décrit sous la forme d'action et de réaction, le comportement du système étudié du point de vue des utilisateurs. Il définit les limites du système et ses relations avec son environnement. [21]

L'ensemble des cas d'utilisations du système à développer sont définis dans le tableau suivant :

TABLE 3.1 – Les cas d'utilisatoin

Acteur	**Cas d'utilisation**
Administrateur réseau	Programmer un nouvel objet. Modifier le fonctionnement d'un objet existant.
Propriétaire de la maison	S'authentifier. Verification de l'état de l'objet . Activer un objet. Desactiver un objet.

3.3.2 Diagramme de cas d'utilisation global

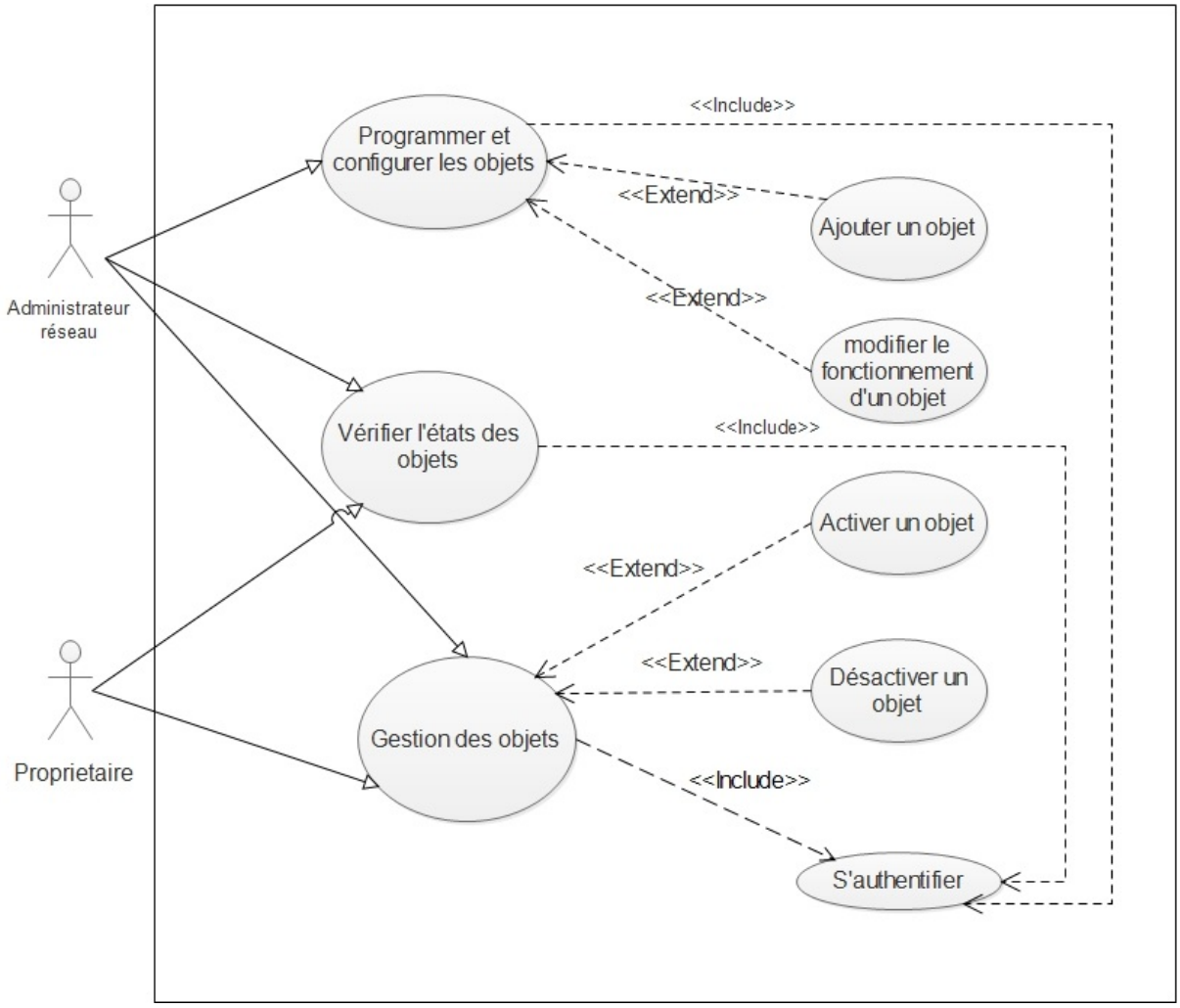

FIGURE 3.2 – Diagramme de cas d'utilisation global.

À chaque cas d'utilisation doit être associée un diagramme de cas d'utilisation des interactions entre l'acteur et le système et les actions que le système doit réaliser en vue de produire les résultats attendus par l'acteur.

Nous allons nous intéresser à quelques-uns des scénarios sous la forme d'échanges d'évènements entre l'acteur et le système.

3.3.2.1 Diagramme de séquence du cas d'utilisation " S'authentifier "

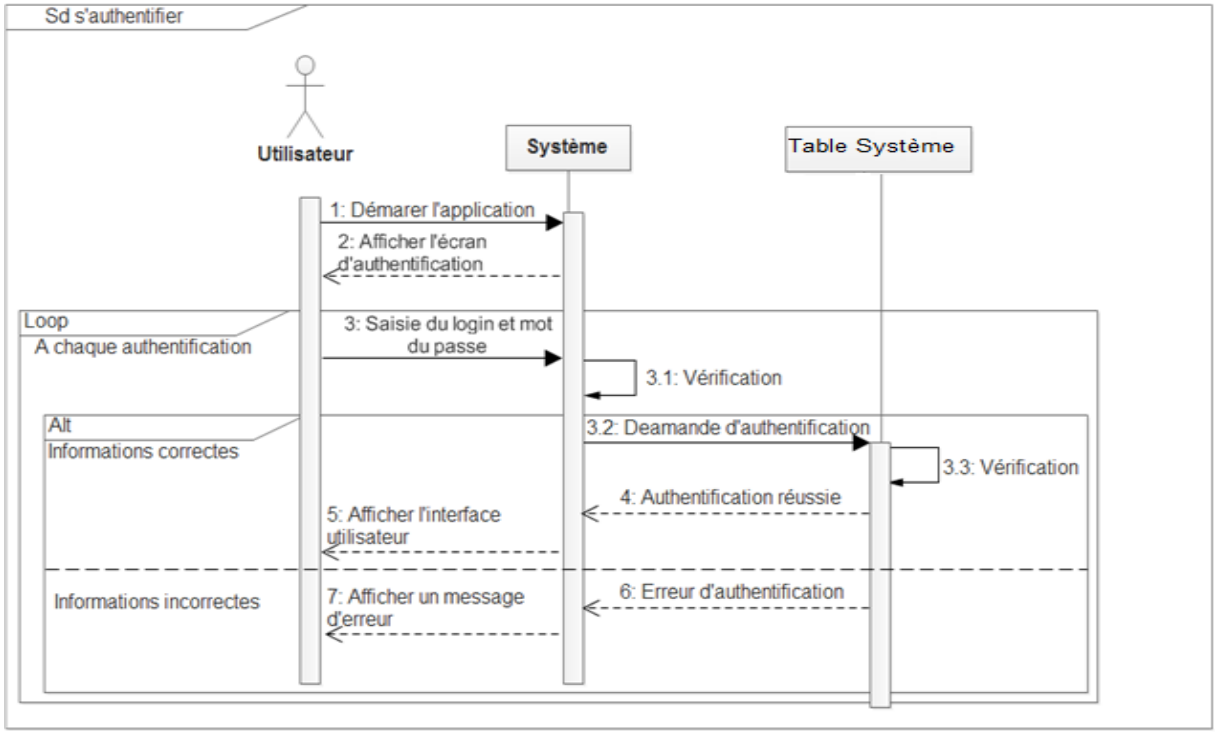

FIGURE 3.3 – Diagramme de séquence du cas d'utilisation " S'authentifier "

3.3.2.2 Diagramme de séquence du cas d'utilisation " Programmer un nouveau objet "

.

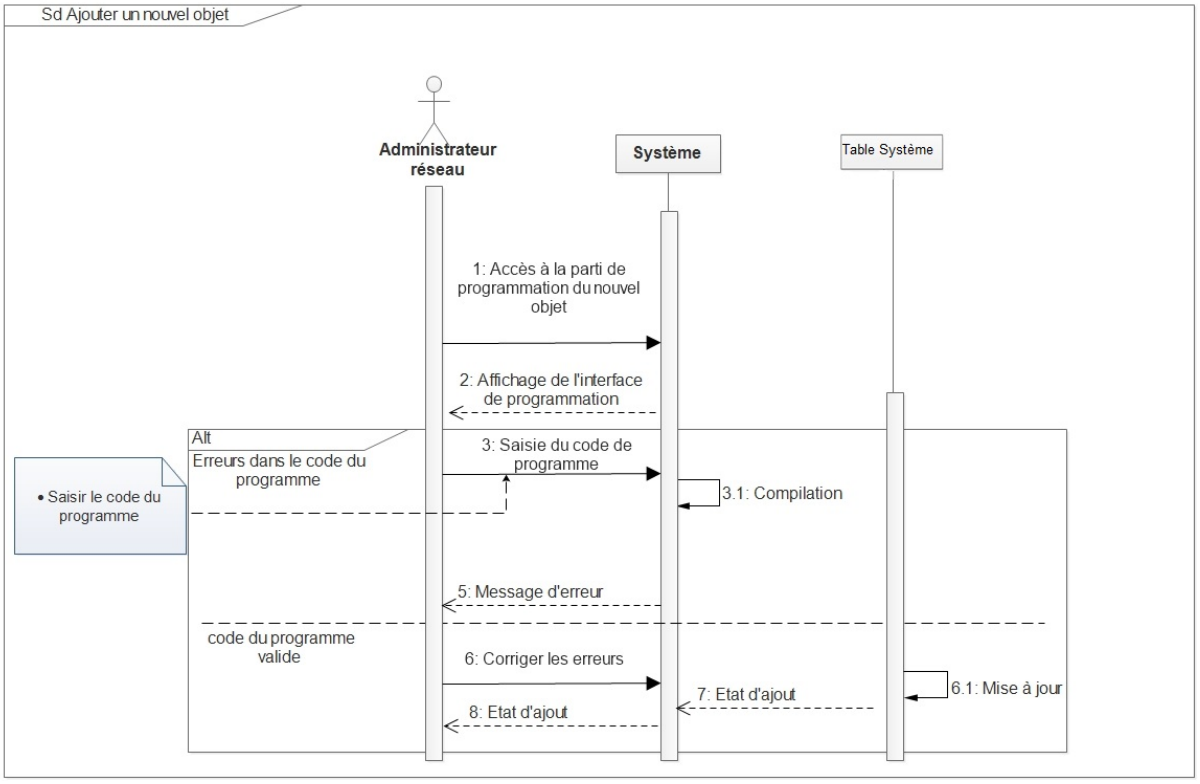

FIGURE 3.4 – Diagramme de séquence du cas d'utilisation " Programmer un nouveau objet "

3.4 Simulation

Pour la réalisation d'un réseau de communication pour une maison intelligente nous allons nous servir de du logiciel Cisco Packet Tracer version 7.

3.4.1 Présentation de Cisco Packet Tracer version 7

Packet Tracer est un simulateur de matériel réseau Cisco, C'est un outil qui permet d'apprendre les réseaux en les simulant sans matériel.

Packet Tracer 7.0 est la version de Packet Tracer la plus récente avec des améliorations majeures et de nouvelles fonctionnalités : un nouveau commutateur et des routeurs,

SPAN / ERSPAN, un serveur amélioré à qui on a intégré le service Internet Of Everything, les capteurs et les langages programmation qui sont l'amélioration principale de cette nouvelle version.Ce qui rend le logiciel l'environnement adéquat à la réalisation de notre projet.

.

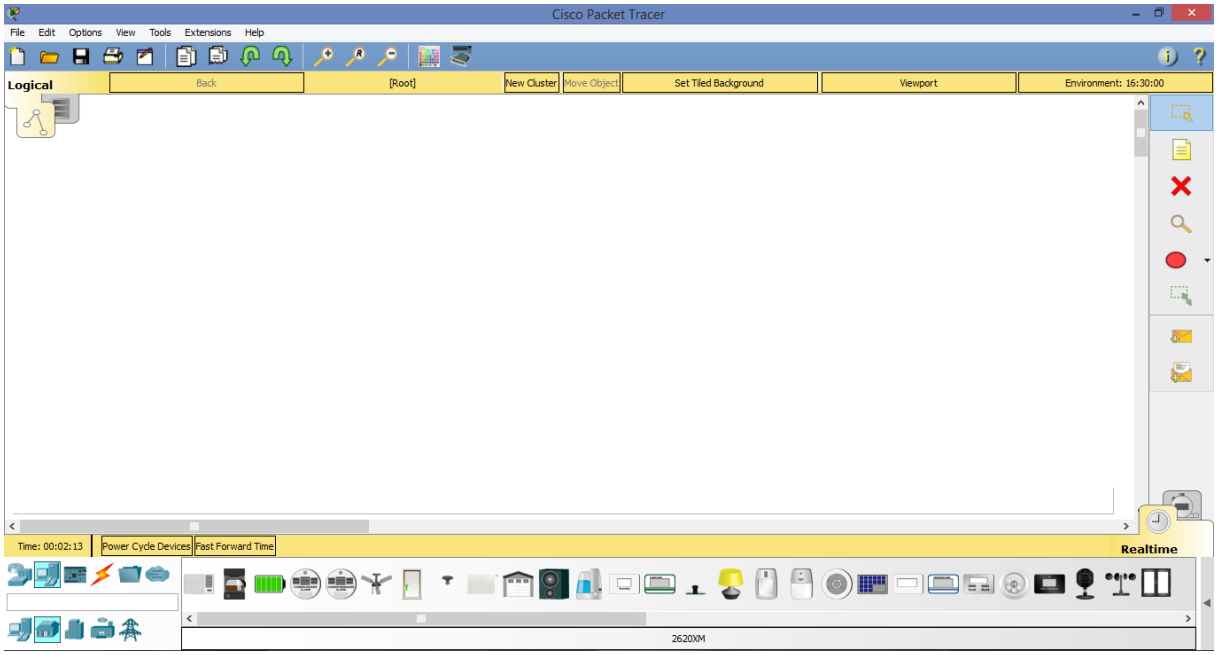

FIGURE 3.5 – Présentation de cisco packet tracer 7

3.4.1.1 Périphériques finaux dans la nouvelle version de Packet Tracer

Dans la figure ci-dessous nous avons l'option de configurer des appareilles domestique. .

FIGURE 3.6 – Les nouveaux périphériques finaux dans Packet Tracer 7.0

3.4.1.2 Capteurs programmables

Pour la raison de relier les objets de façon qu'ils interagissent l'un en dépendance de l'autre nous avons des composants que nous pouvons programmer et les relier aux

appareils. Dans la figure ci-dessous on trouve le capteur SBC que nous avons cité dans le chapitre précédent.

.

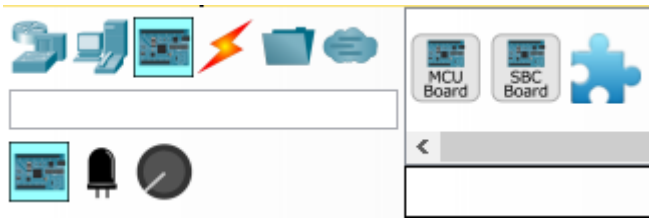

FIGURE 3.7 – Capteurs programmables

3.4.1.3 Le service IoE

Dans la figure ci-dessous on présente un serveur avec un service IoE intégré :

.

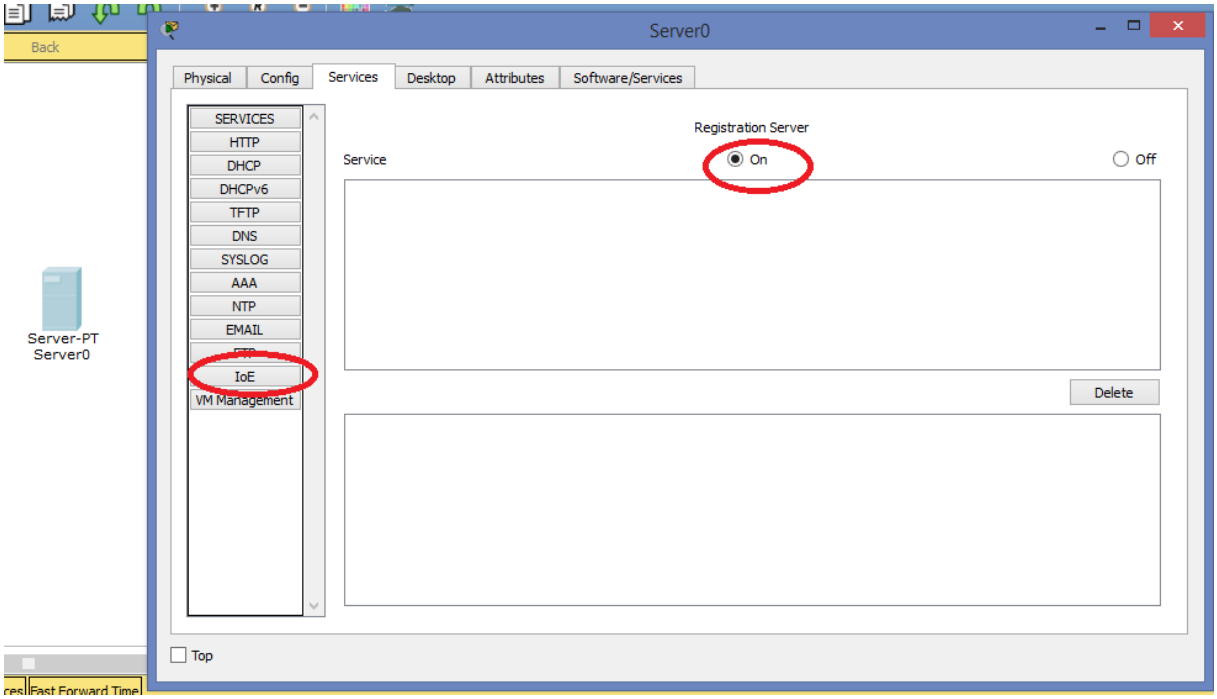

FIGURE 3.8 – Activation du service IoE dans un serveur sur packet tracer

3.4.2 Présentation de notre projet sur Packet Tracer

Notre projet consiste à implémenter un réseau de communication d'appareils dans une maison intelligente.

.

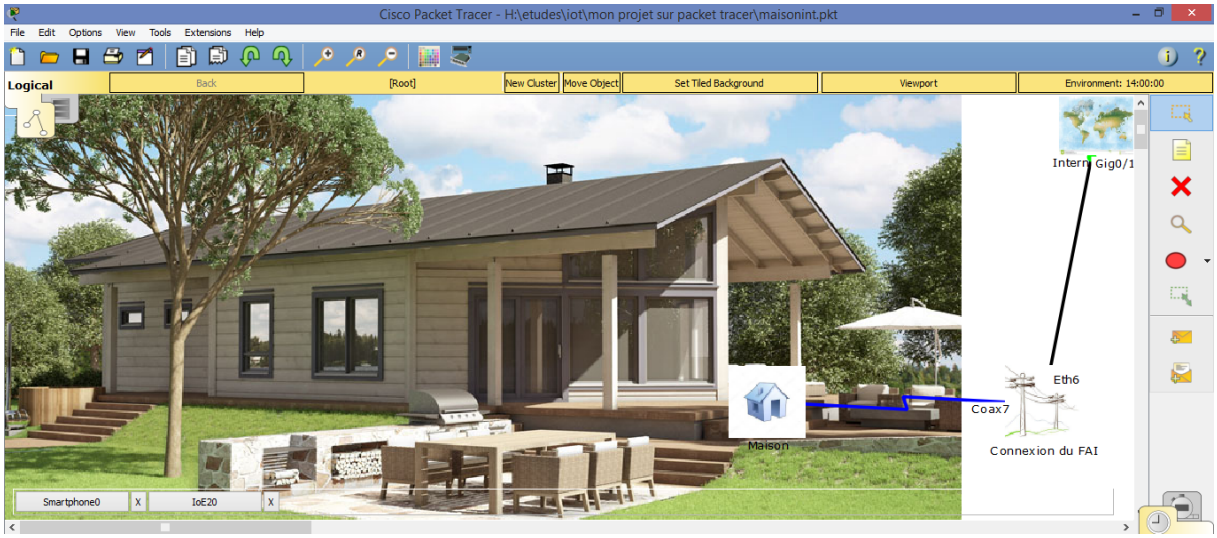

FIGURE 3.9 – vue d'ensemble de connexion de la maison intelligente au réseau extérieur

La figure ci-dessus représente une vue d'ensemble de la manière dont la maison est connecté au réseau extérieur.

La maison est connecté tout d'abord au fournisseur d'accès internet (FAI) qui est à son rôle connecté au réseau internet au quel le propriétaire de la maison pourra se connecter pour avoir accès à distance aux appareilles connectés à l'intérieur de sa maison. Comme illustré dans la figure ci-dessous : .

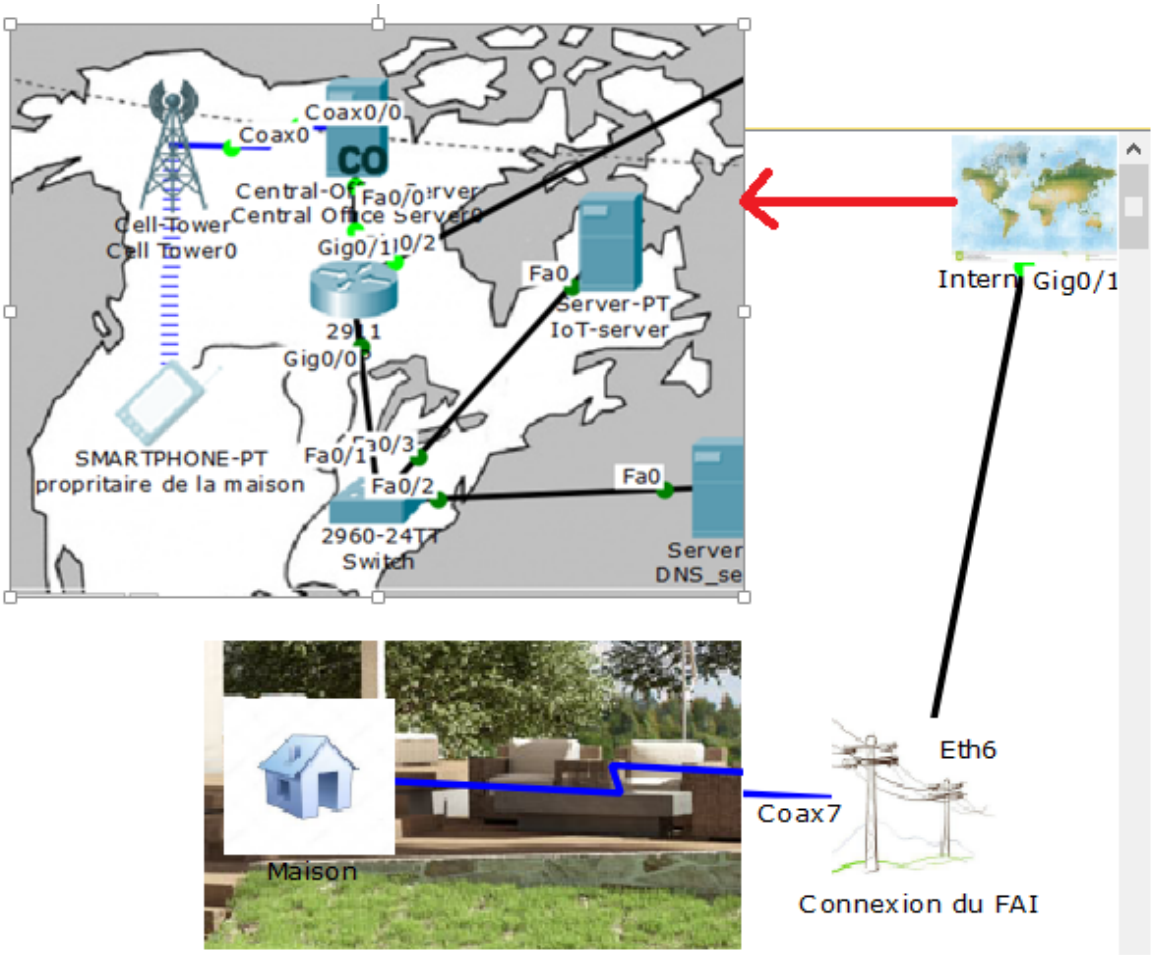

FIGURE 3.10 – Accès à distance du proprietaire à sa maison connecté

3.4.2.1 Présentation de la connexion du réseau domestique

.

FIGURE 3.11 – Connexion des objets à la passerelle

3.4.2.2 Configuration de la passerelle

.

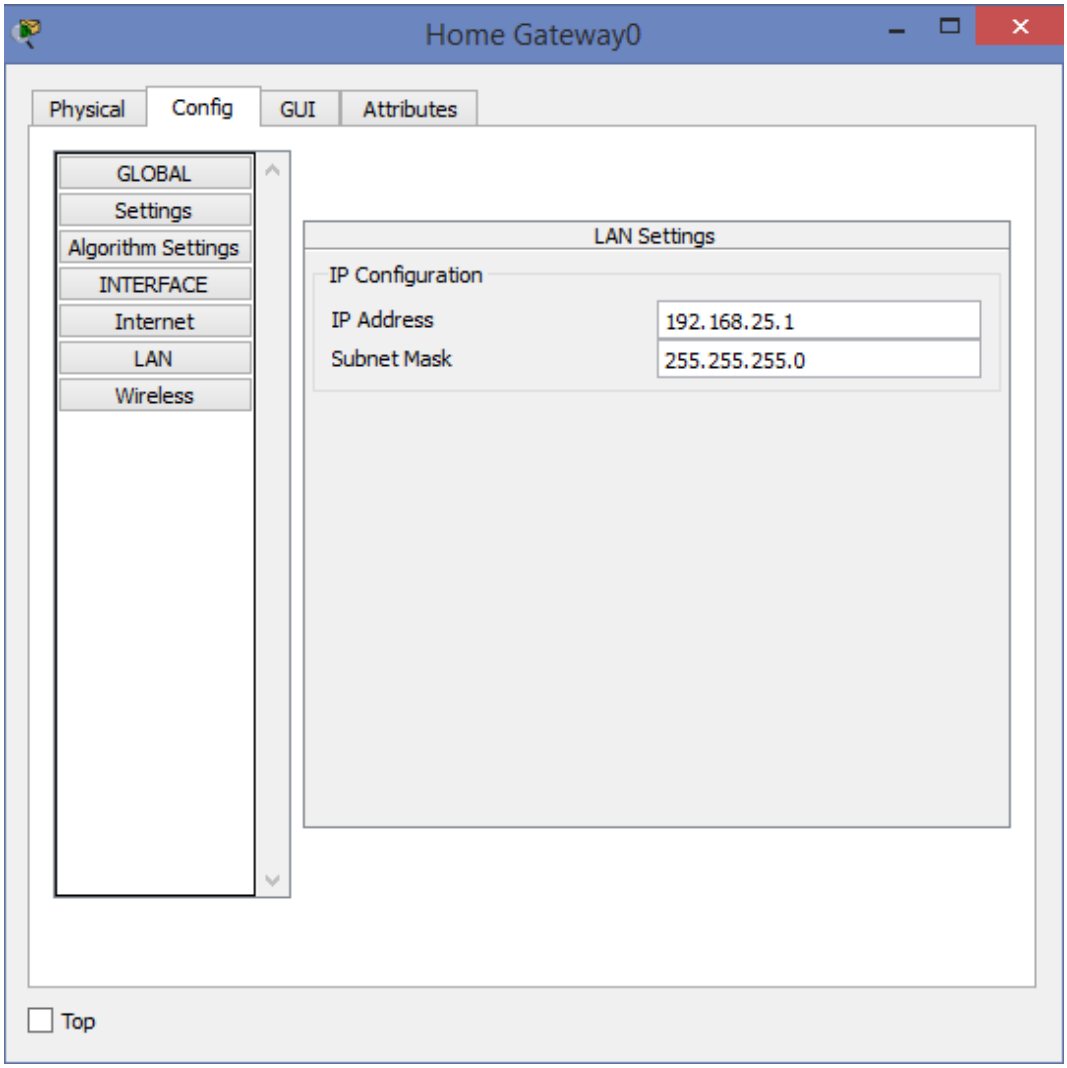

FIGURE 3.12 – introduire l'adresse IP du LAN et le masque sous réseau à la passerelle

.

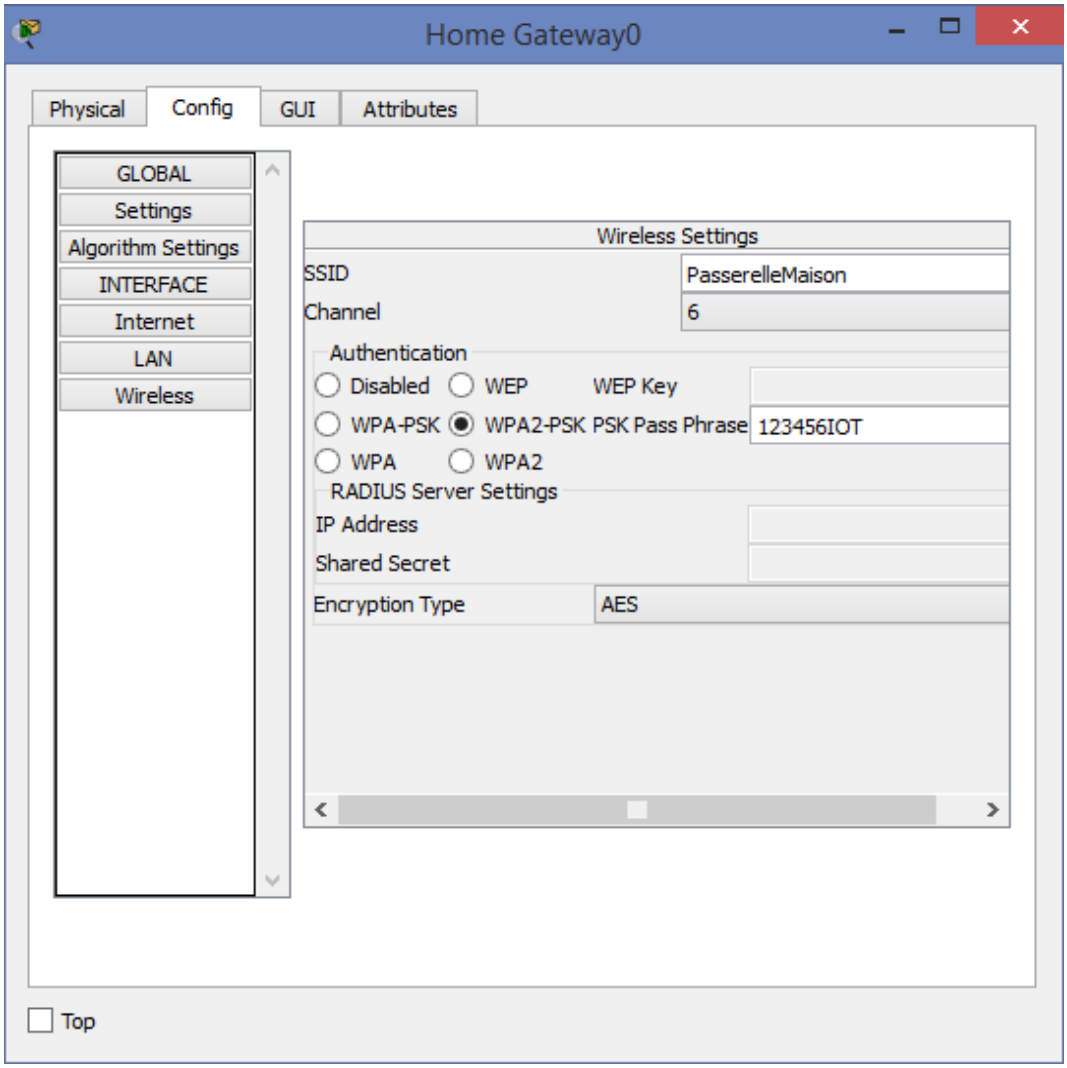

FIGURE 3.13 – Configurer le WLAN de la passerelle

3.4.2.3 Configuration de périphériques finaux

Nous n'allons pas exposer la connexion de tous les objets qui serons connectés à l'intérieur de la maison mais nous allons nous contenter du cas d'activation de la camera de surveillance en dépendance du détecteur de mouvement.

Configuration et programmation du détecteur de mouvement

.

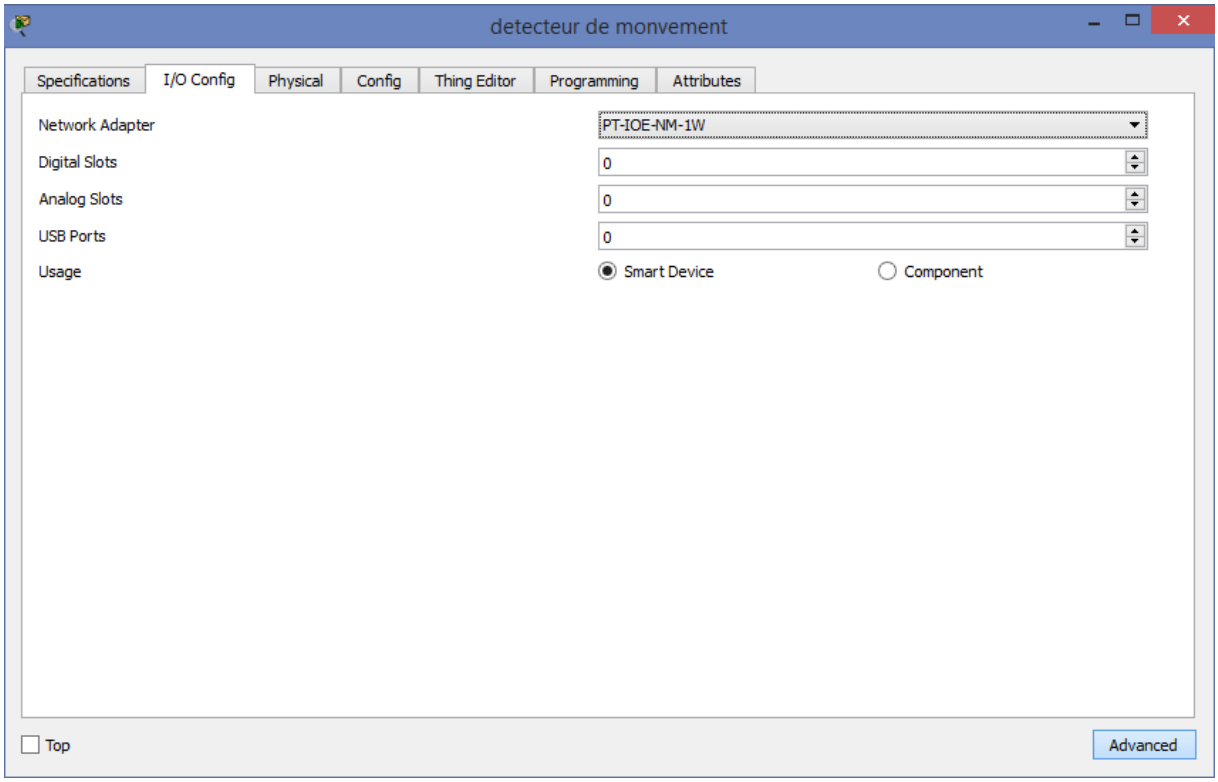

FIGURE 3.14 – Sélectionner la carte Wifi pour la connexion sans fil du détecteur de mouvement

.

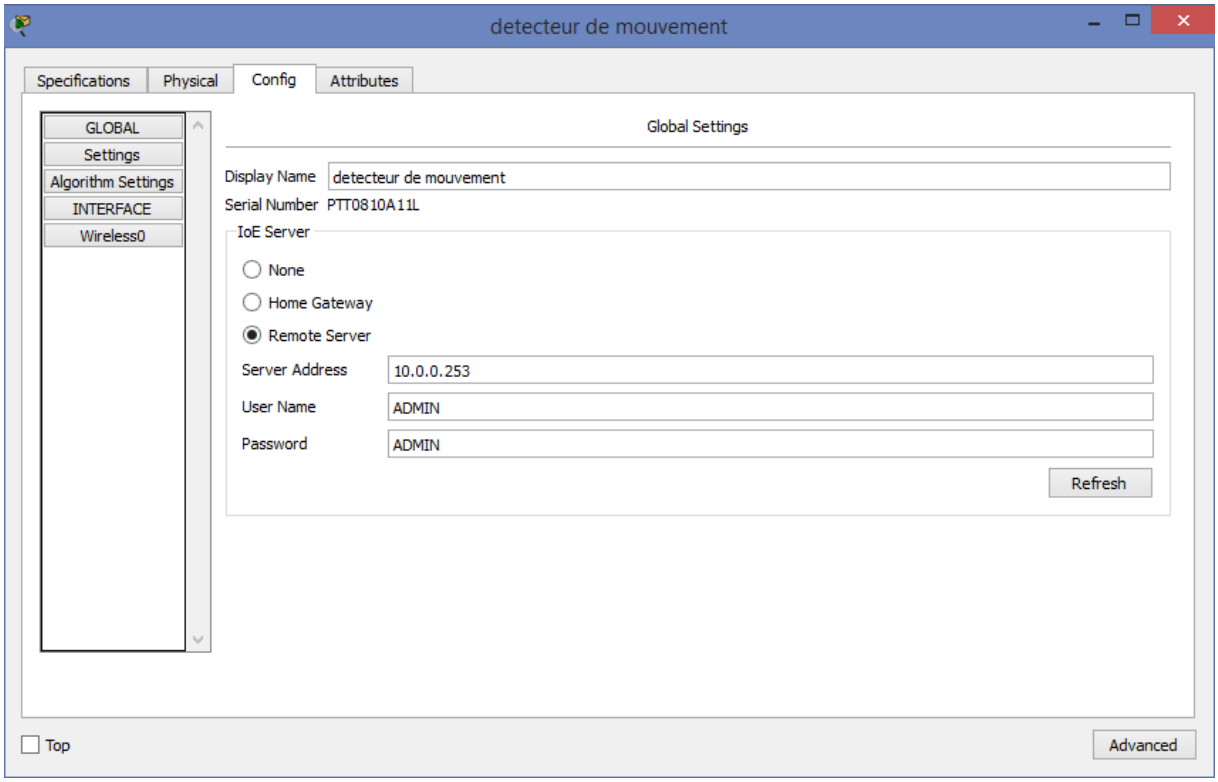

FIGURE 3.15 – Enregistrer le détecteur de mouvement dans le serveur IoE

.

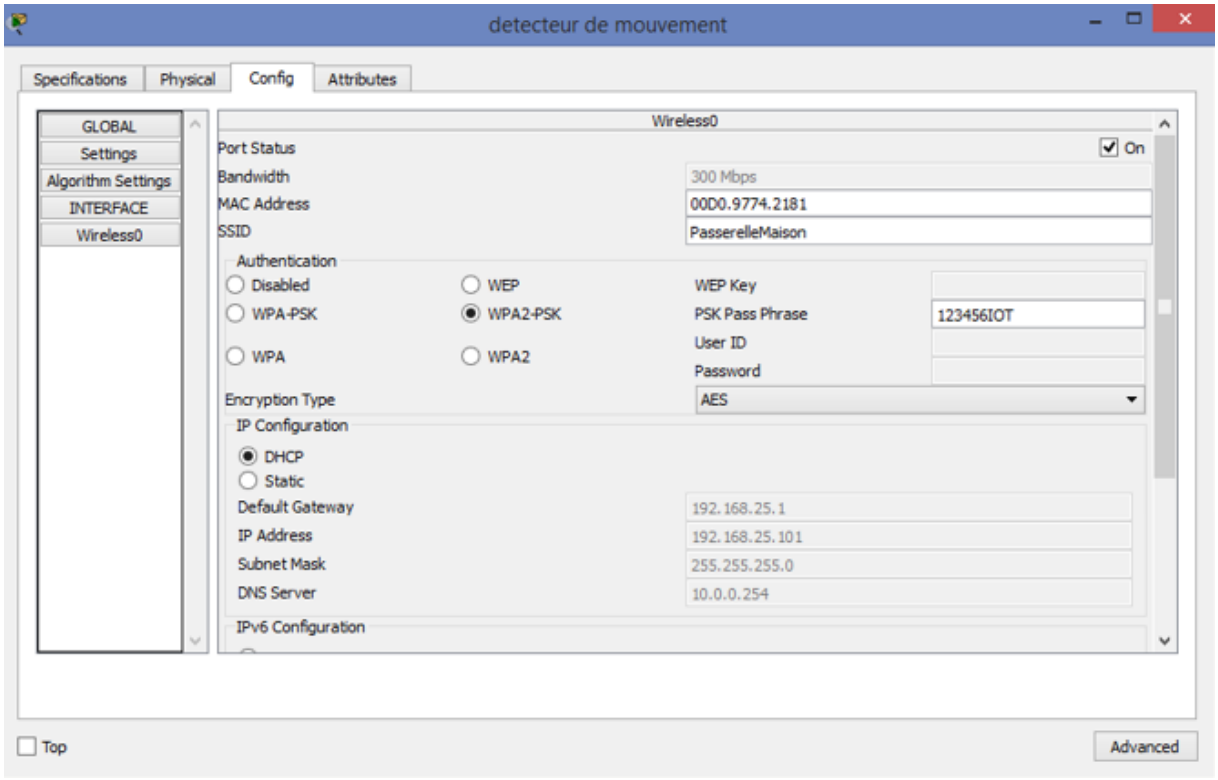

FIGURE 3.16 – Connexion du détecteur de mouvement au réseau sans fil de la passerelle et activation du DHCP

Configuration et programmation du détecteur de la Webcam

.

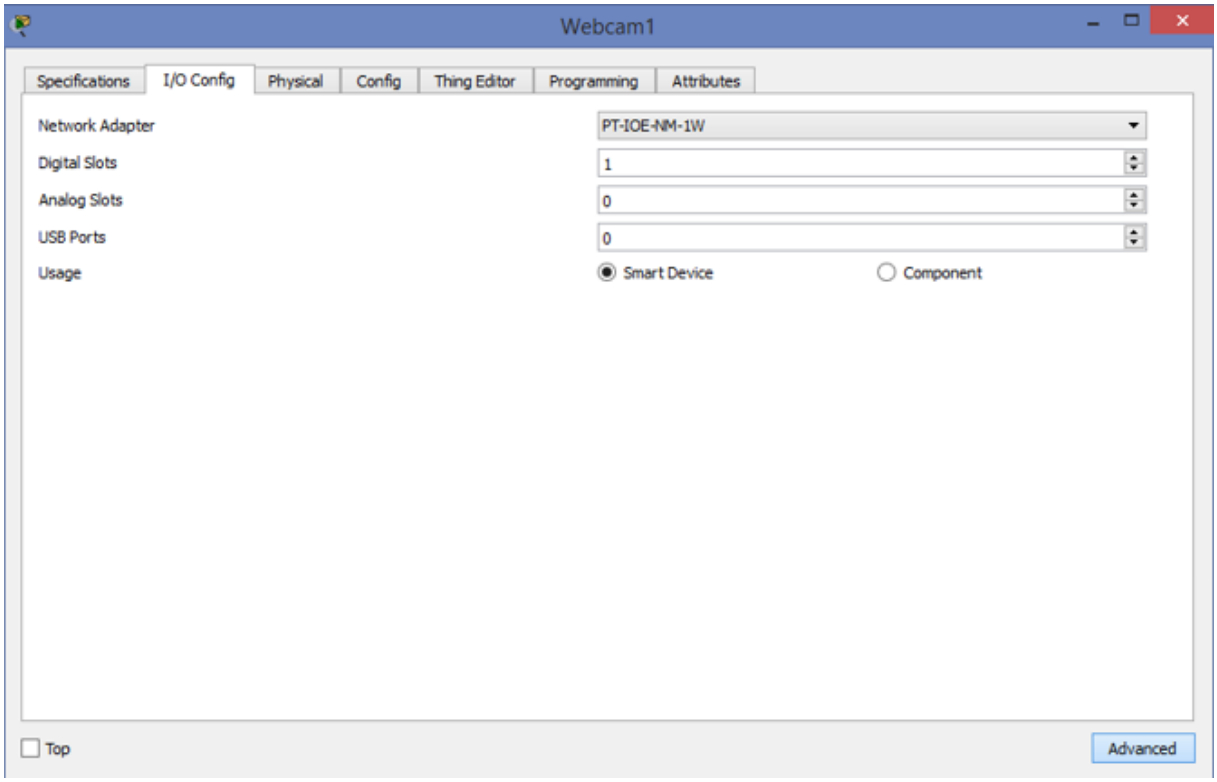

FIGURE 3.17 – Sélectionner la carte Wifi pour la connexion sans fil de la webcam

.

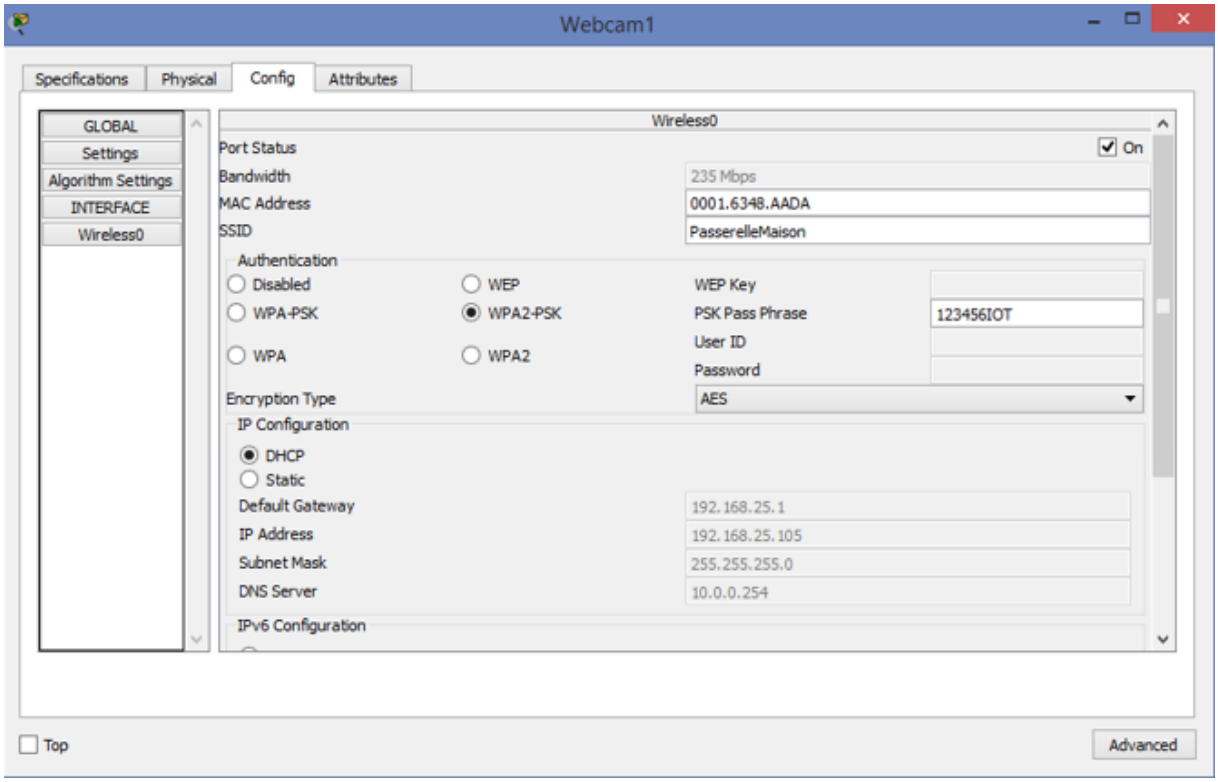

FIGURE 3.18 – Connexion de la webcam au réseau sans fil de la passerelle et activation du DHCP

.

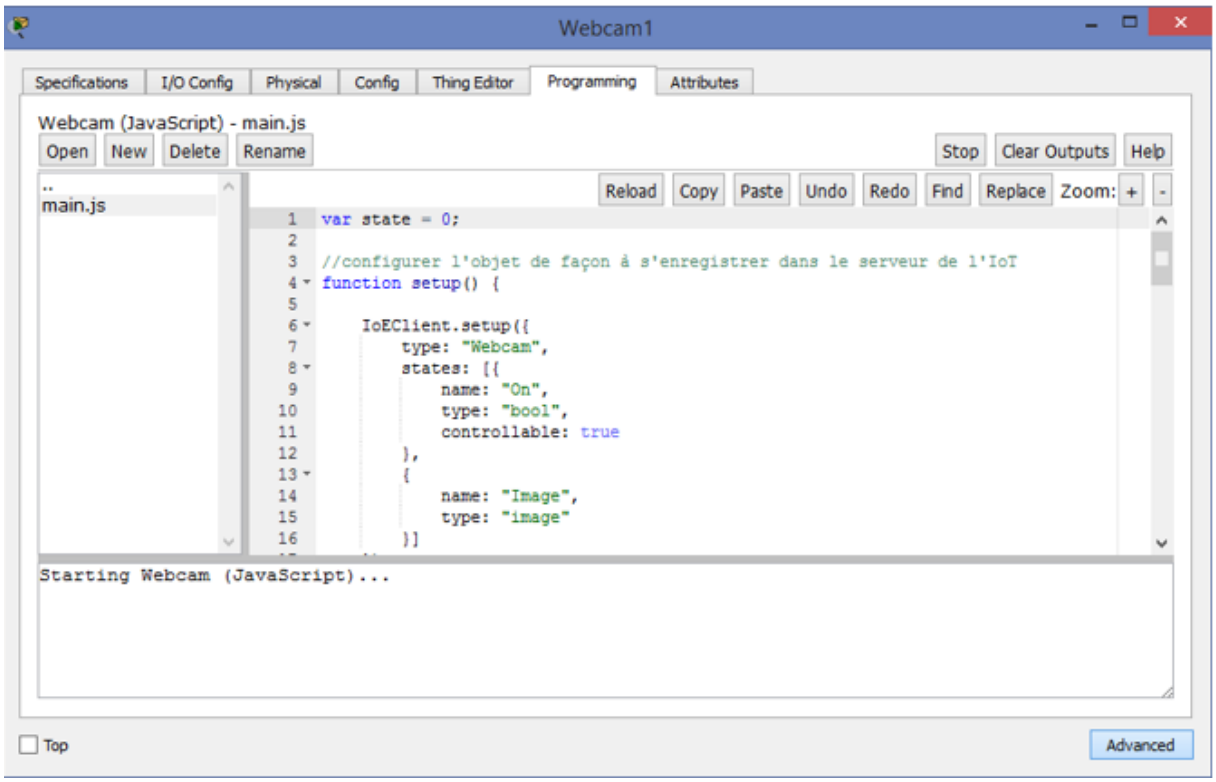

FIGURE 3.19 – Programmation de la webcam

.

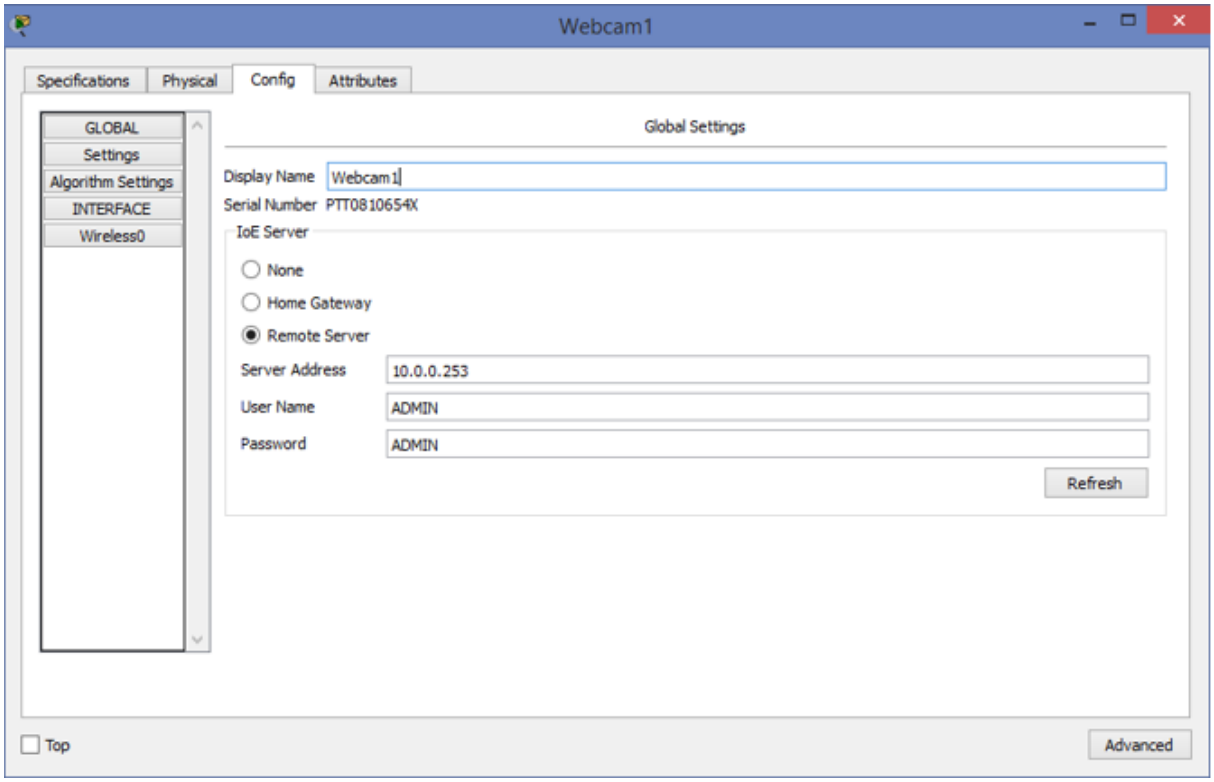

FIGURE 3.20 – Enregistrer le détecteur de mouvement dans le serveur IoE

3.4.2.4 Configurer l'interaction entre le détecteur de mouvement et la webcam

Authentification

.

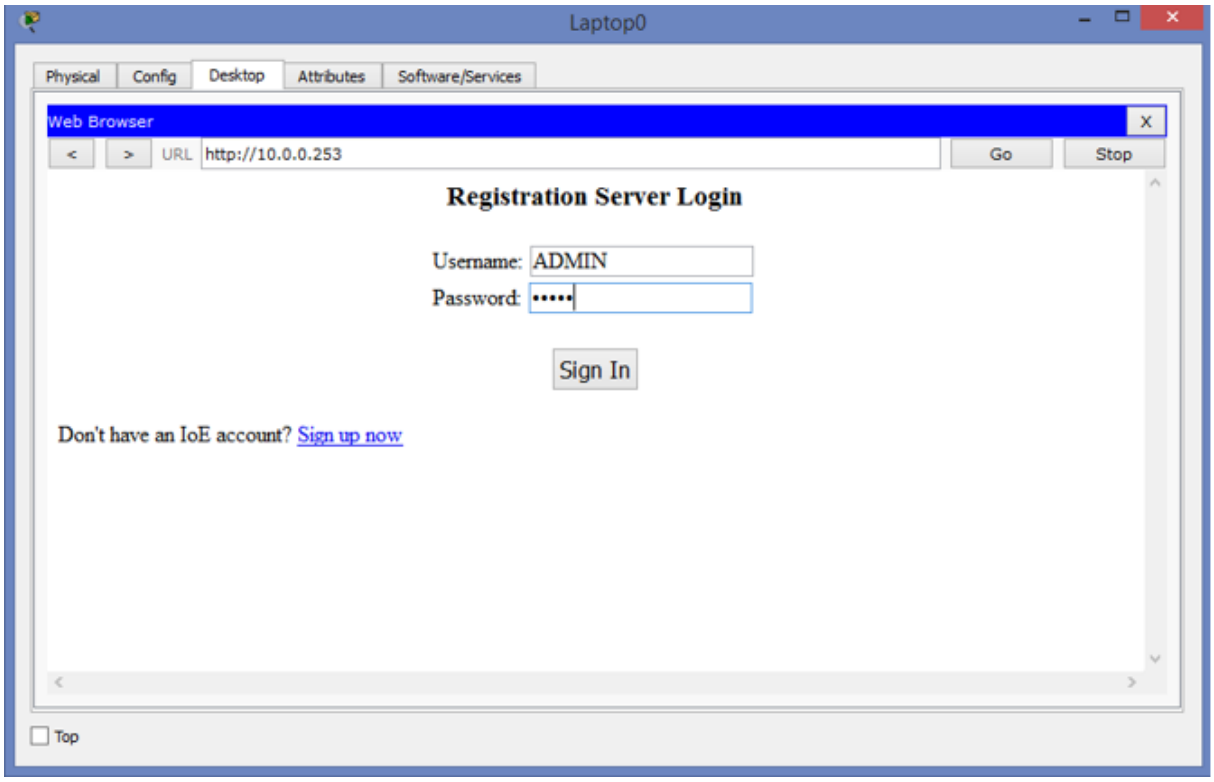

FIGURE 3.21 – Authentification

Apres que l'administrateur s'est authentifié, la liste des objets connectés à l'intérieur du réseau de la maison s'affiche.

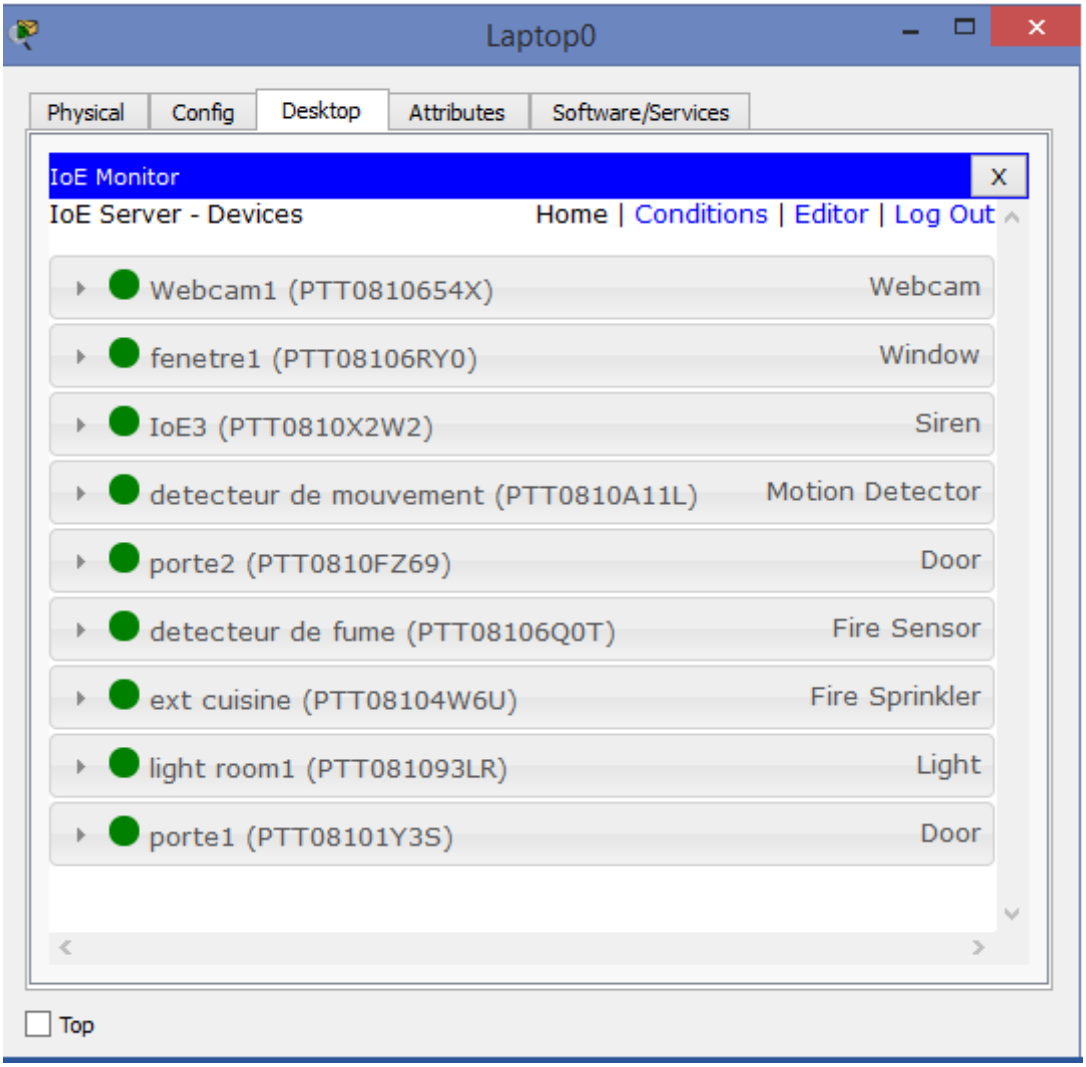

FIGURE 3.22 – Liste des objets connectés

Et c'est dans la partie condition que l'administrateur pourra ajouter les conditions sur le fonctionnement des objets.

Configurer l'activation de la webcam en fonction du détecteur de mouvement

.

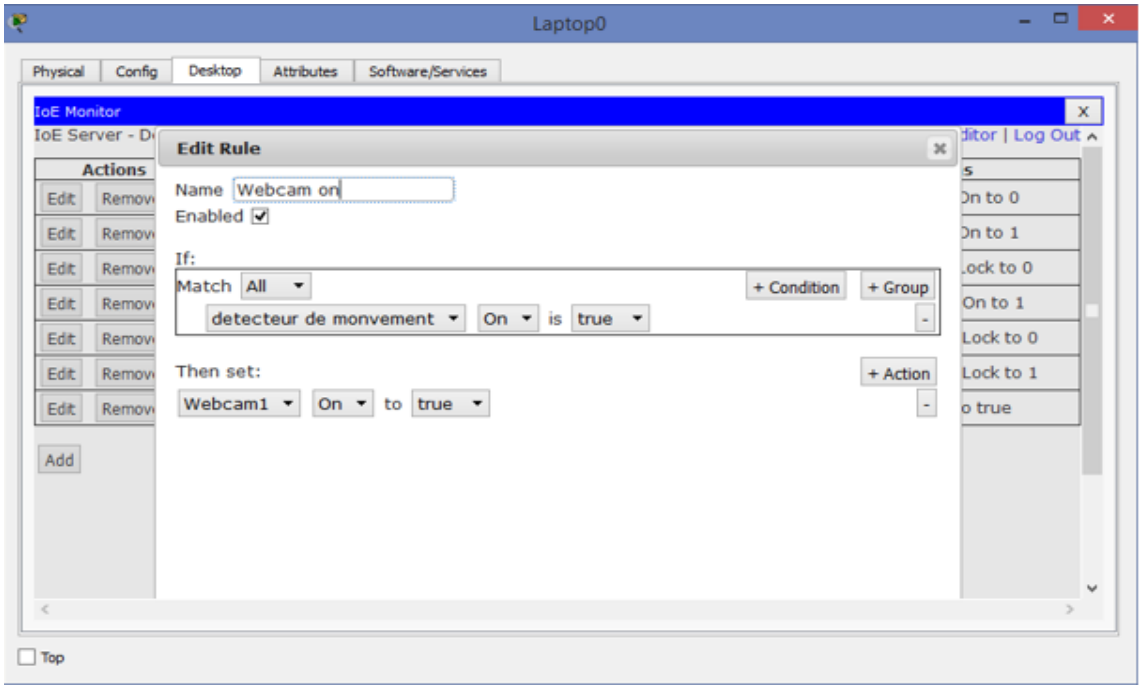

FIGURE 3.23 – Condition pour l'activation de la webcam

.

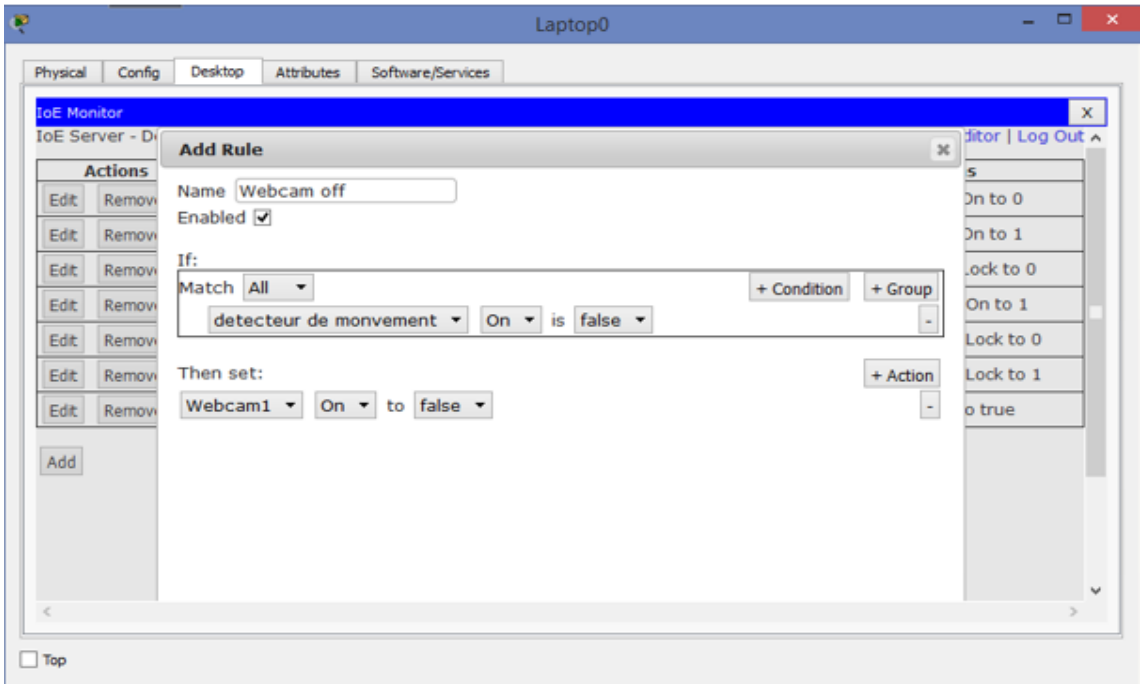

FIGURE 3.24 – Condition pour la désactivation de la webcam

3.5 Conclusion

La connexion des périphériques domestique à internet a pour objectif l'accessibilité à distance à la vérification, l'activation, la désactivation de leurs états et plusieurs autres fonctionnalités.La simulation de réseau d'une maison intelligente nécessite des ressources matériels et logiciels spécifiques.

Dans ce chapitre nous avons présenté d'une partie quelques diagrammes UML tels que : le diagramme de cas d'utilisation et diagramme de séquence, et d'une autre partie un exemple de simulation d'un réseau de communication d'objets connectés dans une maison dont nous avons illustré la configuration et la programmation de quelques appareils.

Conclusion Générale

Nous sommes parvenus, par le biais de ce projet, à mettre en marche un réseau de communication dans une maison intelligente qui permet l'accès à distance aux périphériques connectés à ce réseau au sein du réseau domestique.

La réalisation de notre travail s'est déroulée en trois étapes hiérarchisées logiquement comme suite : la première étape consiste à faire une recherche d'une manière générale sur l'internet des objets et comprendre le concept pour en déduire les domaines d'applications de ce dernier. Le deuxième chapitre qui est l'implémentation de l'internet des objets dans une maison pour arriver à la dernière étape qui consiste en la conjuration et la mise en œuvre de notre réseaux de communication des objets connectés à l'intérieur de la maison.

La mise en œuvre de ce réseau de communication nous a permis de conclure plusieurs points bénéfiques pour le propriétaire et les objets de la maison en question, en effet : notre serveur assure le stockage de données collectés par les objets connectés dans des data centre accessibles via le Web, la surveillance et l'analyse de ces données permet à l'utilisateur de gérer ses appareils d'une manière adéquate à son mode de vie.

Bibliographie

[**1**] A. Hakin, A. Gokhale, P. Berthou, D. C. Schmidt, T. Gayraud, Software-Defined Networking : Challenges and research opportunities for Future Internet, Computer Networks, (2014).

[**2**] M. Han and H. Zhang, "Business intelligence architecture based on internet of things " Journal of Theoretical Applied Information Technology, 2013.

[**3**] P.-J. Benghozi, S. Bureau, F. Massit-Folléa, C. Waroquiers, and S. Davidson, L'internet des objets : quels enjeux pour l'Europe, Éd. de la Maison des sciences de l'homme éd., 2009.

[**4**] X. Jia, Q. Feng, T. Fan, Q. Lei, RFID technology and its applications in Internet of Things (IoT), 2nd International Conference on Consumer Electronics, (CECNet), Yichang, 21-23 April 2012.

[**5**] D. E Vans,The Internet of things : how the next evolution of the internet is changing every thing, Cisco Internet Business Solutions Group (IBSG), 2011.

[**6**] L. Atzori, A. Lera, G. Morabioto, The Internet of Things : a survey, Computer Networks (2010).

[**7**] D. Miorandi, S. Sicari, F. De-Pellegrini, I. Chlamtac, Internet of things : Vision, applications and research challenges, Ad Hoc Networks (2012).

[**8**] G. Aceto , A. Botta , W. Donato , A. Pescapè Cloud monitoring : A survey, Computer Networks (2013).

[**9**] J. Granjal , E. Monteiro, J. Sá Silva, Security in the integration of low-power Wireless Sensor Networks with the Internet : A survey, Ad Hoc Networks (2015).

[**10**] O. Garcia-Morchon, S. Keoh, S. Kumar, R. Hummen, R. Struik,

Security Considerations in the IP-based Internet of Things, draft-garcia-core-security-04, 2012.

[**11**] S. Severi, F. Sottile, G. Abreu, C. Pastrone, M2M technologies, Enablers for a pervasive Internet of Things, 2014 European Conference on networks and communications.

[**12**] BOYD D., CTAWFORD K., Critical Question for Big Data, 2014

[**13**] L. Haiyan, L. Yanyan, X. Zenggang, Y. Zhen, and T. Kun, "Study and Application of Urban Flood Risk Map Information Management System Based on SOA,",2012.

[**15**] Institut Montaigne, "Big data et objets connectés Faire de la France un champion de la révolution numérique", Rapport Avril 2015.

[**16**] G. Aceto , A. Botta , W. Donato , A. Pescapè, Cloud monitoring : A survey, Computer Networks (2013)

[**17**] ABERER, K., AND HAUSWIRTH, M, Middleware support for the internet of things. 2012.

[**18**] Cisco Research Center Requests for Proposals (RFPs).Fog computing, ecosystem, architecture and applications. 2014.

[**19**] J. D. Pessemier, "Une réflexion sur " L'internet des Objets " (IdO) ou " Internet of Things " (IoT)," 2015.

[**20**] S. Duquennoy, G. Grimaud, J. J. Vandewalle, The Web of Things : Interconnecting Devices with High Usability and Performance, Zhejiang, 25-27 May 2009, pp. 323 – 330.

[**21**] GEORGES GARDARIN, Bases de données, Edition Eyrolles, 10 avril 2003

Résumé

L'Internet des objets (IoT) est un paradigme prometteur qui étale la connexion Internet de nos jours pour interconnecter différents types d'objets intelligents, autre que les ordinateurs et les téléphones mobiles, pour un mode de vie beaucoup plus sophistiqué.

Nous nous sommes focalisés plus précisément sur l'application de l'internet des objets dans le domaine personnel pour créer une maison intelligente qui nécessite la création d'un réseau à l'intérieur cette dernière vers qui les appareils et dispositifs seront connectés, pour cela pour cela nous nous sommes tournés vers l'environnement et l'outil CISCO Packet-Tracer 7.0. Cet outil nous a permis de simuler un réseau domestique et configurer des périphériques finaux et d'infrastructure.

Mots-clés : IoT, maison intelligente, objets intelligents, reseaux de communication.

Abstract

Internet of Things (IoT) is a promising paradigm that spreads the nowadays Internet connection to interconnect several types of smart objects, other than computers and mobile phones, for a sophisticated lifestyle.

We have focused more precisely on the application of the internet of objects in the personal domain to create a smart home that requires the creation of a network within the latter to which devices will be connected, that's why we turnedto the environment andof CISCO Packet-Tracer 7.0. This allowed us to simulate a home network and to configure end devises and infrastructure devices.

Keywords : IoT, smart home, smart devices, Communication network.