


République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université AMO de Bouira

Faculté des Sciences et des Sciences Appliquées

Département d'Informatique

Exposé

Module : Cloud

Spécialité : *Génie des Systèmes Infrmatiques*

Thème

Internet Of Things

Encadré par

— Dr :Mahfoud Z

Réalisé par

— BOUREKBA Iman

— MERROUCHE Sarah

2019/2020

Table des matières

Table des figures

Introduction générale

Introduction génrale.

Internet est un réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés. L'ensemble utilise un même protocole de communication : TCP/IP (Transmission Control Protocol / Internet Protocol).

Internet propose trois types de services fondamentaux : le courrier électronique (e-mail) ; le Web (les pages avec liens et contenus multimédia de ses sites Web) ; l'échange de fichiers par FTP (File Transfer Protocol).

Le réseau Internet sert également, et de plus en plus, aux communications téléphoniques et à la transmission de vidéos et d'audio en direct (ou streaming), c'est-à-dire à la manière d'un téléviseur ou d'un récepteur radio. L'internet a évolué avec le temps ce qui Entraînant l'émergence de nouvelles technologies. Dans ce travail on va présenter quelques aspects de la nouvelle technologie internet of things, notre travail est divisé comme suit :

— Chapitre 1 : Ce chapitre est consacré à la présentation des concepts liés à notre thème « Internet of things ». Nous commençons le chapitre par une petite définition de l'internet of things en général, puis ces caractéristiques, et enfin on va parler sur son architecture.
— Chapitre 2 :Dans ce chapitre on va présenter le coté de sécurité, vulnérabilité et menace de l'internet of things.
— Chapitre 3 :Dans ce chapitre on va parler sur l'application des IoTs en donnent quelque exemple et enfin sur le Challenge et future direction.

Chapitre 1

premier chapitre

1.1 Introduction

Ce chapitre est consacré à la présentation des concepts liés à notre thème « Internet of things ». Nous commençons le chapitre par une petite définition de l'internet of things en général, puis ces caractéristiques, et enfin on va parler sur son architecture.

1.2 Définition

Selon l'Union internationale des télécommunications, l'Internet des objets ou internet of things (IoT) en anglais 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.

D'un point de vue technique, 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.[1]

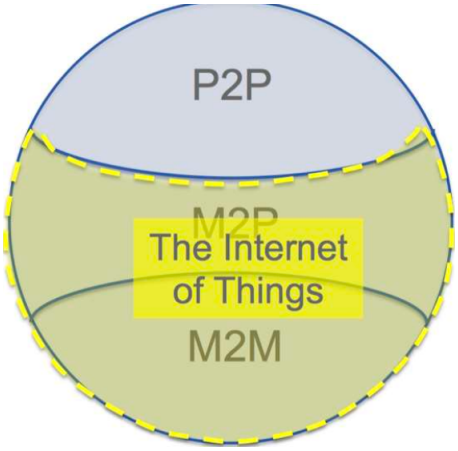

FIGURE 1.1 – Internet of things.[2]

1.3 Caractéristique

— Interconnectivité : en ce qui concerne l'IoT, tout peut être interconnecté avec l'information et la communication mondiales Infrastructure.

— Services liés aux objets : l'IoT est capable de fournir services liés aux choses dans les contraintes des choses, telles que protection de la vie privée et cohérence sémantique entre physique les choses et leurs objets virtuels associés. Afin de fournir services liés aux choses dans les contraintes des choses, technologies dans le monde physique et le monde de l'information changement.

— Hétérogénéité : les appareils de l'IoT sont hétérogènes comme basé sur différentes plates-formes matérielles et réseaux. Ils peuvent interagir avec d'autres appareils ou plates-formes de services via différents réseaux.

— Changements dynamiques : l'état des appareils change dynamiquement, par exemple, dormir et se réveiller, connecté et / ou déconnecté en tant que ainsi que le contexte des appareils, y compris l'emplacement et la vitesse. De plus, le nombre d'appareils peut changer dynamiquement.

— Échelle énorme : le nombre d'appareils qui doivent être gérés et qui communiquent entre eux seront au moins un ordre de grandeur plus grand que les appareils connectés au Internet actuel.

La gestion des données sera encore plus critique générés et leur interprétation à des fins d'application. Cela concerne la sémantique des données, ainsi que les données efficaces manipulation.

— Sécurité : à mesure que nous tirons profit de l'IoT, nous ne devons pas oublier sur la sécurité. En tant que créateurs et destinataires de l'IoT, nous doit concevoir pour la sécurité. Cela comprend la sécurité de nos personnels donnés et la sécurité de notre bien-être physique. Sécuriser les points de terminaison, les réseaux et les données se déplaçant à travers tout cela signifie créer un paradigme de sécurité qui évoluera.

— Connectivité : la connectivité permet l'accessibilité au réseau et compatibilité. L'accessibilité se connecte à un réseau pendant la compatibilité offre la capacité commune de consommer et produire des données. [3]

1.4 Architecture et standardisation

L'IoT ne doit pas être considéré comme un concept utopique. En réalité, il sera fondé sur plusieurs technologies habilitantes tels que la RFID, la communication en champ proche (NFC : Near Field Communication), les capteurs et actionneurs sans fil, les communications machine-à-machine (M2M), l'ultralarge bande ou 3/4G, IPv6, 6LowPANet RPL, etc. qui devraient tous jouer un rôle important dans le développement de l'IoT. L'IoT voit ses racines remonter aux technologies M2M (Machine-to-Machine) pour le contrôle de processus de production à distance. Cette technologie a évolué vers le concept d'Internet des Objets depuis l'apparition d'IP sur réseaux mobiles cellulaires durant les années 2000. L'ETSI préconise une évolution du paradigme M2M vers l'internet des objets. Cet organisme de normalisation propose une architecture à base de trois domaines comme illustré sur la Figure 1.2 : le domaine du réseau d'objets, le domaine du réseau cœur d'accès, et le domaine des applications M2M et applications clientes.

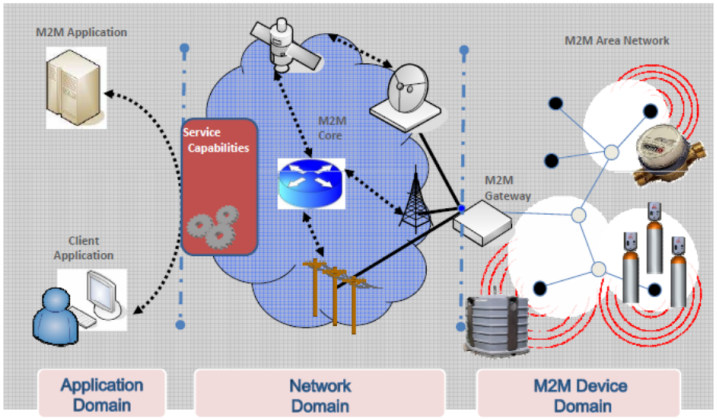

FIGURE 1.2 – Architecture simple pour l'interconnexion d'objets.[4]

Cette architecture permet une coexistence des différentes technologies actuelles et futures qui entrent dans le paysage de développement de l'Internet des objets comme l'illustre la Figure 1.3 :

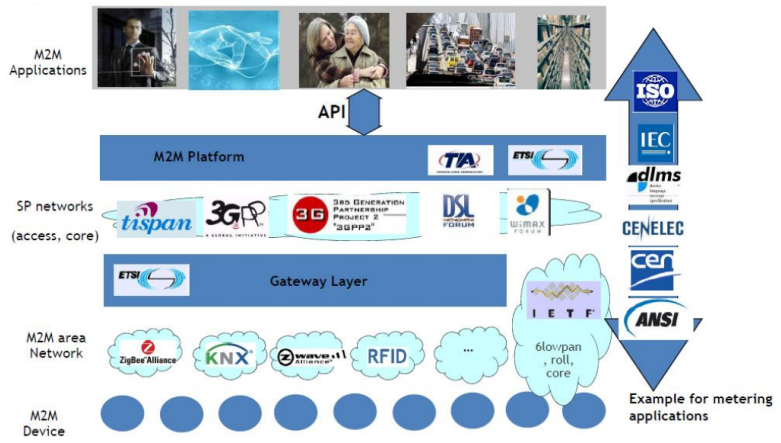

FIGURE 1.3 – Paysage de standardisation M2M.[4]

— Dans le domaine du réseau d'objets, on retrouve les différentes technologies d'interconnexion des objets (M2M, RFID, IEEE802.15.4, IETF-6LowPAN, IETF-RPL, etc.), et des passerelles vers les réseaux cœurs de transport.

— Dans le domaine du réseau cœur, on retrouve les différentes technologies de réseaux de transport et d'accès comme xDSL, WiMax, WLAN, 3/4G, etc.

— et dans le domaine des applications M2M et applications clientes on retrouve les plateformes M2M, les middlewares et API des applications M2M, processus métiers exploitant l'internet des objets, etc.[4]

1.5 Conclusion

Dans ce chapitre, on a illustré les aspects principaux de l'internet of things pour donner une vue globale. Dans le prochain chapitre, on va compléter cette étude en parlent sur le coté de sécurité.

Chapitre 2

deuxième chapitre

2.1 Introduction

Dans ce chapitre on va présenter le coté de sécurité, vulnérabilité et menace de l'internet of things.

2.2 Vulnérabilité et menace

≪The National Intelligence Council(NIC)≫ américain considère que les avancées technologiques combinées à une forte demande des marchés encourageraient une adoption et un déploiement à large échelle de l'IoT. Néanmoins, la plus grande crainte est que les objets du quotidien deviennent des risques potentiels d'attaque de sécurité. Pire encore, la pénétration à large échelle de l'IoT diffuserait ces menaces d'une façon beaucoup plus large que l'Internet d'aujourd'hui.

En effet, l'ubiquité de l'IoT amplifiera les menaces classiques de sécurité qui pèsent sur les données et les réseaux. Mais en plus, le rapprochement du monde physique et du monde virtuel à travers l'IoT ouvre la voie à de nouvelles menaces qui pèseront directement sur l'intégrité des objets eux-mêmes, les infrastructures et processus (monde physique), et la vie privée des personnes.

2.2.1 Amplification des menaces sur les données et les réseaux

L'omniprésence des objets communicants dépourvus de protection physique et de surveillance, les rendent une proie facile aux attaques matérielles et logicielles. Ces objets peuvent être volés, corrompus et contrefaits. Sans mesures particulières, les données stockées sur ces dispositifs seraient alors accessibles, y compris des données cryptographiques qui permettraient d'accéder à d'autres données sensibles ou jouer des rôles sensibles dans les systèmes complexes les hébergeant.

Par ailleurs, les transmissions sans fil, sont à leur tour une proie facile à l'écoute et au dénie de service (≪jamming≫).Il existe aujourd'hui des solutions cryptographiques pour assurer des services de confidentialité, de contrôle d'intégrité, d'authentification, de non-répudiation, etc. mais beaucoup reste à faire pour rendre ces algorithmes efficaces et performants sur des dispositifs embarqués de plus en plus miniaturisés.

Le CERP-IoT cite dans quelques problématiques amplifiées par la nature des objets embarqués miniaturisés. On cite notamment : l'hétérogénéité et la mobilité des objets qui rajoutent une couche de complexité aux problèmes de sécurité.

2.2.2 Menaces sur la vie privée

Tous les pronostics envisagent le développement d'une informatique ambiante avec potentiellement des dizaines d'objets par personne y compris dans leur sphère privée et intime. Ces objets de l'espace personnel sont géo-localisables, peuvent communiquer avec d'autres objets à travers des réseaux spontanés, peuvent écouter ce que dit la personne, peuvent filmer la personne et/ou son environnement, et peuvent même enregistrer son rythme cardiaque, son rythme respiratoire, la température de son corps, et sa cinématique ! Des questions légitimes se posent sur le devenir de cette masse de données personnelles et parfois intimes.

Sans régulation stricte, une protection accrue de la privacy, un degré élevé de contrôle des objets par les usagers, l'adoption de l'IoT serait un échec.

L'ITU dans son rapport sur l'Internet des Objets a pointé du doigt ces menaces potentielles.

Elle conclue que la protection de la privacy ne doit pas se limiter à des solutions technologiques, mais doit comprendre des mesures juridiques, une régulation du marché et des considérations socio-éthiques

2.2.3 Menaces sur les systèmes et l'environnement physique des objets

L'IoT fera partie intégrante du monde physique et des systèmes complexes. En conséquence, un disfonctionnement quelconque, un déni de service, ou un comportement byzantin des objets n'entravera plus uniquement l'intégrité du monde virtuel (composé de données et d'informations), mais directement les processus sous leur contrôle en causant des dommages collatéraux importants.

De ce point de vue, l'IoT pourrait constituer un véhicule privilégié pour les hackers amateurs de sensations fortes et la menace terroriste ! Par exemple, il est rapporté qu'en 2010 le ver StuxNet avait infecté des dizaines de milliers de stations Siemens SCADA.

Ces systèmes étaient utilisés en majorité dans des entreprises de services et de fabrication et même des stations nucléaires ! StuxNet avait montré alors qu'il était relativement simple de causer des dommages catastrophiques à un réseau de contrôle industriel.

En 2009, une équipe de recherche d'IOActiveavait démontré l'existence de failles de sécurité dans des dispositifs utilisés dans des «smart grids» pour le contrôle de distribution de l'énergie.

Cette faille permettait à un hacker potentiel de diffuser un code malicieux et de couper l'alimentation en électricité des foyers. Les menaces sur les infrastructures et l'environnement physique des objets sont bien réelles, et nécessitent des mesures préventives pour les contrarier et des solutions curatives pour les confiner et empêcher leur propagation le cas échéant.

2.3 Sécurité de l'Internet des Objets : challenges et perspectives

2.3.1 Dimensions de la sécurité de l'IoT

L'IoT est une technologie caractérisée par une forte ubiquité dans le monde physique et une omniprésence autour de ses usagers.

Les diverses applications potentielles de l'IoT, l'hétérogénéité de ses technologies habilitantes et sa forte dimension humaine et socioéconomique rendent sa sécurité un sujet difficile et complexe.

En plus des problèmes de sécurité des technologies qui le constitueront, l'IoT accentue les problèmes de sécurité des personnes qui l'utiliseront, et fait émerger de nouveaux problèmes liés à la sécurité des systèmes sous son contrôle.
la sécurité et la privacy dans l'IoT peut être abordée de trois angles complémentaires qui reflètent ses dimensions technologique, humaine et systémique.

La protection de la technologie concerne en premier lieu la sécurité des données, des communications et des infrastructures réseaux. Cette protection est nécessaire pour contrarier les attaques classiques et futures sur l'intégrité, l'authenticité et la confidentialité des données, ainsi que les attaques sur les infrastructures réseaux et leurs fonctionnalités.

La protection des personnes concernera la protection de la vie privée des usagers (≪privacy≫) qui nécessite, en plus des solutions technologiques, une régulation appropriée qui établit les responsabilités en cas de litiges. La protection des systèmes interconnectés et hébergeant les objets de l'IoT, concernera la protection des objets eux-mêmes livrés à ces systèmes et les processus qu'ils contrôleront

2.3.2 Plan d'action à court, moyen et long termes

Après analyse des travaux existants et les besoins de l'IoT en termes de sécurité, nous concluons que les développements potentiels se dérouleront autour de trois axes à court, moyen et long termes :

— Une sécurité efficace pour une informatique embarquée miniaturisée.
— Une sécurité adaptative de l'informatique mobile omniprésente.
— Une sécurité de l'internet des objets selon une approche cognitive et systémique.

Ces trois axes répondront aux besoins évolutifs de l'IoT en termes de sécurité et accompagneront son évolution vers plus d'autonomie des objets.

2.3.3 Sécurité des réseaux embarqués

Miniaturisés Durant ces dernières années, le besoin de développer des systèmes cryptographiques performants, efficaces et peu coûteux en termes de ressources (énergie, mémoire, bande passante) fut déjà ressenti.

L'avènement de l'IoT avec l'interconnexion d'un nombre potentiellement très élevé d'objets omniprésents, accentue le problème de rareté des ressources en y ajoutant une problématique d'adaptation au facteur d'échelle.

Parmi les challenges et verrous scientifiques et technologiques, les problèmes suivants occuperont une place importante dans les travaux à venir à court et long termes :
— Cryptographie efficace pour l'informatique embarquée miniaturisée
— Gestion de clés efficace et scalable pour l'Internet des Objets
— Authentification et gestion efficace de crédentités
— Protocoles sécurisés pour les environnements dynamiques à énergie et connectivité faibles

2.3.4 Sécurité de l'informatique mobile omniprésente

L'évolution d'Internet vers un IoT se fera grâce à l'intégration à des systèmes complexes des objets communicants, localisables, mobiles et dotés de facultés les rendant de plus en plus autonomes.

Cette informatique omni présente fera émerger des questions légitimes sur la privacy des usagers, et sur la variabilité et la diversité des exigences des usagers et des applications en termes de services de sécurité.

Ceci nécessite des solutions de sécurité centrées sur les utilisateurs, adaptatives avec une prise en compte du contexte.

La diversité des besoins et des exigences en termes de sécurité et privacy pourrait être abordée à travers une gestion adaptative des politiques et des profils de sécurité qui tient compte du contexte ambiant.

La protection de la privacy aura son empreinte sur le traitement des données qui devrait désormais tenir compte de cette dimension selon le contexte :

— Privacy et sécurité centrée sur l'utilisateur selon le contexte
— Gestion adaptative des profils et politiques de sécurité
— Partage sécurisé dans les environnements mobiles

2.3.5 Approche cognitive et systémique de la sécurité de l'IoT

L'Internet des objets permettra aux objets de notre environnement de devenir des participants actifs partageant l'information avec d'autres objets du réseau.

Ces objets seront capables de reconnaître des événements et des changements dans leur environnement et pourront capter et réagir d'une façon assez autonome sans intervention humaine.

En effet, l'informatique évolue d'un réseau de calculateurs qui traitent des données, vers des réseaux de plus en plus «intelligents» dotés de capacités de captage, de perception et reconnaissance, d'action et réaction, et continuera à évoluer vers plus d'autonomie.

L'intégration des objets dans la commande de systèmes complexes et le monde physique, rend la sécurité de l'IoT très difficile à appréhender d'une façon analytique.

Nous croyons qu'une approche systémique de la sécurité est plus appropriée pour l'IoT.

Une approche systémique qui permettra de tenir compte de la complexité intrinsèque des systèmes qu'interconnectent l'IoT.

— Modèles de confiance pour les «clouds d'objets»

— Auto-immunité des objets.

— Identification.

— Responsabilité. [4]

2.4 Conclusion

Dans ce chapitre, on a parlé sur les vulnérabilités et les menaces de l'internet of things surtout sur la vie privée ainsi que la sécurité.
Dans le prochain chapitre on va donner quelques exemples de l'application de l'IoT

Chapitre 3

Troisième chapitre

3.1 Introduction

Dans ce chapitre on va parler sur l'application des IoTs en donnent quelque exemple et enfin sur le Challenge et future direction.

3.2 Applications des IOTs

Une enquête réalisée par le projet IoT-I en 2010 a identifié des scénarios d'application IoTs qui sont regroupés en 14 domaines à savoir ; Transport, smart home, smart city, mode de vie, commerce de détail, agriculture, smart factory, chaîne d'approvisionnement, urgence, soins de santé, interaction avec les utilisateurs, culture et tourisme, environnement et énergie. Cette enquête était basée sur 270 réponses de 31 pays et les scénarios les plus intéressants étaient les suivants : smart home, smart city, transports et soins de santé .Dans ce travail, l'accent sera brièvement mis sur les applications de l'IoT dans le domaine médical (santé soins) , smart home ,et système de sécurité communautaire intelligent (smart city).

3.2.1 IoT dans les applications médicales

En raison de la croissance démographique, de l'urbanisation rurale, de la baisse du taux de natalité, du vieillissement de la population, de la croissance économique et de l'utilisation sociale déséquilibrée des ressources, certains problèmes sociaux sont apparus dans le domaine des soins de santé.

— Le niveau de gestion de la santé et l'incapacité de répondre à l'urgence est un problème social pressant.

— Il y a une grave pénurie de personnel médical, d'établissements institutionnels en particulier dans les zones rurales, de manque d'installations médicales, de faible niveau de traitement, d'un système de santé inadéquat

— Le système de prévention des maladies imparfaites ne peut pas répondre aux exigences de la stratégie nationale pour protéger la santé des citoyens, devenant ainsi un lourd fardeau pour l'économie, les individus, les familles et l'État.

— Capacité inadéquate de prévention des maladies et de détection précoce. Pour résoudre ces problèmes, la plate-forme de surveillance et de gestion à distance des informations sur les soins de santé (RMMP-HI) peut assurer la surveillance et la gestion de ces maladies liées au mode de vie afin d'atteindre l'objectif de prévention et de détection précoce.

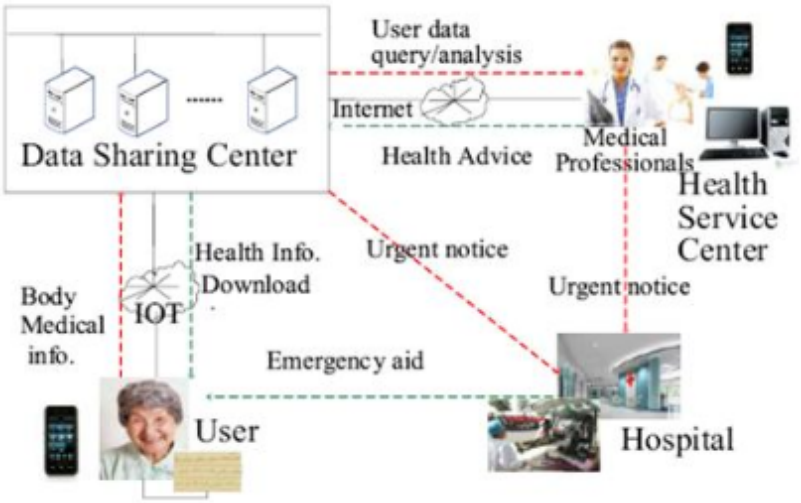

FIGURE 3.1 – Le framework de service de la santé

[6]

Indépendamment des restrictions de localisation, de temps et d'état d'activité de l'utilisateur, RMMP-HI peut collecter des informations médicales sur le corps humain en temps opportun grâce à une variété de capteurs médicaux du corps chargés dans le corps humain ou l'espace environnant et extraire des informations utiles par cryptage, stockage, comparaison des données analyse et traitement. Lorsqu'une apparence anormale est constatée,

les utilisateurs sont invités à prendre un traitement précoce ; cela permet une détection et une prévention précoces. Grâce à une surveillance en temps réel, lorsque l'utilisateur se trouve dans des agences d'urgence ou des autorités compétentes, ce qui améliore le traitement médical d'urgence et la capacité de réponse. En outre, il est également efficace d'établir des dossiers nationaux de gestion de la santé, de fournir une base de prévention et de prise de décision pour les maladies liées au mode de vie, les maladies épidémiques et régionales par le biais de la surveillance, de la comparaison de l'analyse et du traitement des informations sur les soins de santé du groupe associé. De cette façon, les capacités de prévention des maladies, de détection précoce et de traitement précoce sont considérablement améliorées. Les capteurs Body médical peuvent s'enregistrer et supprimer, constituant automatiquement le Medical Body Area Network (MBAN). Comme montre la figure précédente, le module de capteur de communication sans fil à courte portée transmettra des informations médicales humaines au téléphone mobile 3G ou à la passerelle domestique. Ces informations médicales sont téléchargées en temps opportun vers le centre de stockage et de traitement des données. Ensuite, les conseils de santé importants seront renvoyés au patient, aux membres de la famille des patients ou aux institutions médicales après le traitement analytique du système expert ou l'inspection du personnel médical professionnel dans le centre de services de santé. Dans l'état d'urgence, un avis de premiers soins est délivré à l'établissement médical par le centre de santé pour fournir des services d'urgence aux patients.

3.2.2 IoT dans Smart Home

De nos jours, les maisons intelligentes deviennent de plus en plus rentables et intellectualisées avec des progrès continus et une réduction des coûts dans les technologies de communication, les technologies de l'information et l'électronique, qui connecte Internet avec des appareils et des capteurs de tous les jours pour connecter des objets virtuels et physiques via les données développement des capacités de capture et de communication.

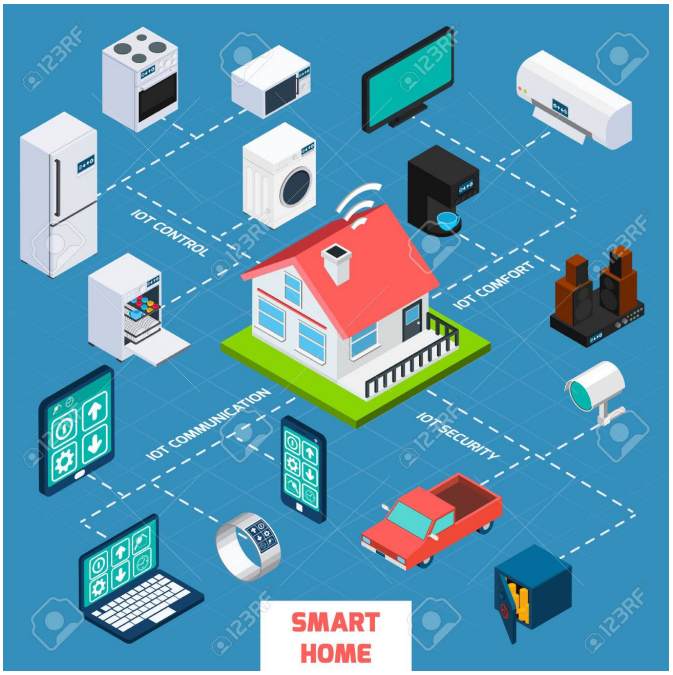

FIGURE 3.2 – IoT smart home

[5]

La lecture des compteurs à distance peut être obtenue grâce à ces systèmes de maison intelligente. Cela implique que les données relatives à l'électricité domestique, aux télécommunications, au gaz et à l'eau peuvent être envoyées automatiquement à leur entreprise de services publics correspondante pour améliorer l'efficacité des travaux. De plus, grâce aux systèmes de maison intelligente, les fenêtres, la ventilation de la maison, les portes, l'éclairage, la climatisation, etc., peuvent être contrôlés à distance. Chaque appareil électronique tel que réfrigérateur, machine à laver, four, etc., peut être manipulé par des plates-formes ou des programmes à distance. Les équipements de divertissement comme les radios et les téléviseurs peuvent être connectés à des canaux communs distants. En outre, la sécurité à domicile et les soins de santé sont également des aspects importants des maisons intelligentes. Par exemple, les dispositifs d'aide à la santé peuvent aider une personne âgée à envoyer une demande ou une alarme à un membre de la famille ou à un centre médical professionnel. Dans la conception de la maison intelligente, la maison et ses différents appareils électriques ont été équipés d'actionneurs, de capteurs. Les appareils domestiques fonctionnent dans un réseau local mais, à certaines occasions, connectés à une plate-forme de gestion à distance afin d'effectuer le traitement et collecte de données.

3.2.3 Système de sécurité communautaire intelligent (ICSS)

le système de sécurité communautaire intelligent (ICSS) contient plusieurs sous-systèmes, tels que le sous-système de gestion des véhicules (VMS), le sous-système de sécurité environnant (SSS), le système central de traitement de l'information (CIPS), le sous-système de gestion immobilière (PMS), le sous-système de prévention des incendies et des vols (FTPS), etc.

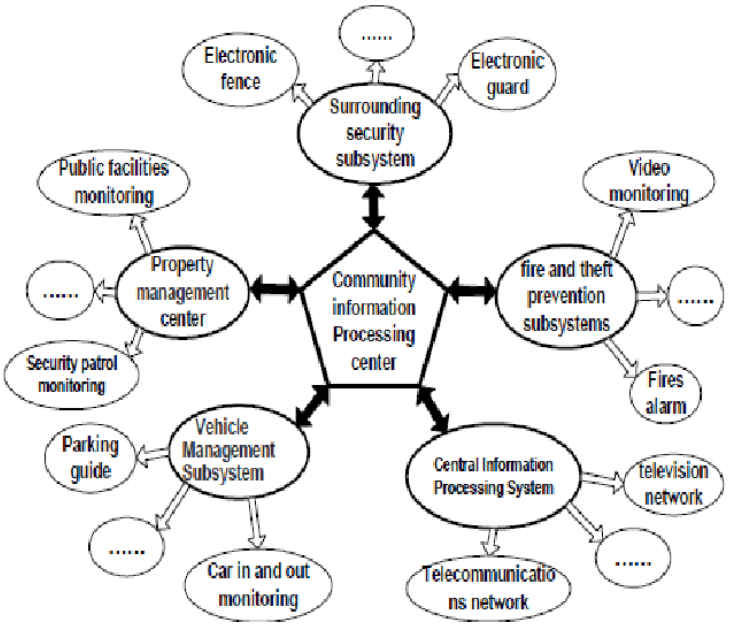

FIGURE 3.3 – Intelligent community security system (ICSS)

[4]

Grâce au sans fil, les informations de chaque sous-système sont envoyées au CIPS, ce qui implique des ajustements automatiques et des avertissements en temps opportun afin de maintenir la sécurité de la communauté.[6]

3.3 Challenge et future direction

Alors que l'avenir de l'Internet des objets est prometteur et que les attentes augmentent, d'importants défis restent à résoudre non seulement d'un point de vue technologique, mais aussi d'un point de vue commercial, où l'introduction de produits connectés soulève un certain nombre d'importants problèmes opérationnels et questions stratégiques.

Par exemple, au niveau stratégique, les dirigeants sont désormais obligés d'évaluer les opportunités et les menaces que l'émergence de l'IoT pourrait présenter pour leurs entreprises. En conséquence, les modèles commerciaux existants peuvent devoir être adaptés ou redéfinis en fonction d'un nouveau positionnement des produits dans l'Internet des objets, et même des frontières entières de l'industrie peuvent devoir être réévaluées à mesure que la concurrence commence à se déplacer et à s'étendre. Au niveau opérationnel, des défis de gestion fondamentaux sont par exemple susceptibles de survenir alors que des cultures matérielles et logicielles rigoureuses commencent à s'affronter non seulement au sein des entreprises, mais même aux premiers stades de développement de produits. Il peut être nécessaire de modifier les processus de service après-vente pour répondre aux exigences des produits connectés. De nouveaux outils marketing pourraient devenir pertinents car les produits connectés permettent une communication plus directe ou étendue avec les clients. De nouveaux principes de conception peuvent être nécessaires pour soutenir le développement d'un produit connecté, par exemple pour permettre des mises à jour ou une personnalisation continues du produit (Fleisch et al. 2014 ; Porter et Heppelmann 2014).

D'un point de vue technologique, la mise en œuvre d'une application IoT nécessite l'intégration d'une gamme de technologies de l'information et de la communication sous forme matérielle et logicielle, comme décrit précédemment. Certains des défis les plus importants auxquels les innovateurs de l'IoT sont actuellement confrontés dans ce contexte concernent, par exemple, l'approvisionnement en énergie au niveau des appareils, l'identification et l'adressage, l'évolutivité d'Internet, la sécurité et la vie privée, ainsi que la normalisation et l'harmonisation (Atzori et al. 2010 ; Mattern 2013 ; Vermesan et al.2014). En ce qui concerne les plateformes IoT, un premier défi important pour les entreprises proposant des produits ou des systèmes de produits connectés résidera certainement dans le choix de la plateforme IoT, le marché respectif étant jeune et très fragmenté. Un facteur clé sera alors sans aucun doute la capacité des fournisseurs de plates-formes à construire des écosystèmes actifs autour de leurs plates-formes et à fournir un soutien professionnel et en temps opportun à leurs partenaires ainsi qu'aux communautés de développement. Et enfin, la prise en charge des normes les plus récentes et en constante évolution ainsi que l'intégration de chaînes d'outils de bout en bout adéquates, même dans le domaine des logiciels embarqués pour améliorer la productivité des développeurs, représente d'autres

défis importants dans le développement des plateformes IoT (Porter et Heppelmann 2014 ; Schuermans et Vakulenko 2014).

Pour la communauté des SI scienti ques, ces défis ouvrent des thèmes inspirants pour la recherche future, où les questions clés tournent autour de l'impact de l'innovation basée sur l'IoT sur la stratégie ainsi que sur les infrastructures informatiques de l'entreprise. Dans l'Internet des objets, la technologie numérique fait partie intégrante des formulations stratégiques. Par conséquent, les modèles reçus de gestion de l'informatique en tant que produit standardisé et d'alignement de l'informatique sur la stratégie commerciale doivent être remis en question et complétés par de nouveaux cadres, qui considèrent les technologies IoT non seulement comme une fonction de support, mais comme un élément central de la création de valeur et comme une source d'avantage compétitif. Afin de permettre la mise en œuvre de ces nouvelles stratégies d'innovation numérique, les infrastructures informatiques d'entreprise auront besoin de nouveaux principes, outils et processus de gouvernance afin de gérer, coordonner et connecter efficacement et efficacement les ressources requises au sein de et au-delà des frontières des sociétés individuelles (Yoo et al. 2010). Par conséquent, une multitude de nouvelles opportunités émergent à nouveau pour les chercheurs en SI afin de contribuer à la solution des défis du monde réel et de créer une valeur directe pour les praticiens.[7]

3.4 Conclusion

Dans ce chapitre, on a parlé sur l'application des IoTs en donnent l'exemple de smart city, smart home et smart health et enfin on a parlé sur le Challenge et future direction.

Conclusion générale et perspectives

Conclusion génrale.

Le but de ce travail est de donner une vision globale et riche sur la nouvelle technologie internet of things qui peut dans le future occupe tous les domaines dans notre vie quotidienne (médecine, agriculture, maison, ville, etc.), malgré les vulnérabilités et les menaces mais ça peut s'améliorer avec le temps pour faciliter nos vie.

Bibliographie

[1] https ://www.futura-sciences.com/tech/definitions/internet-internet-objets-15158/.consulté le 21/01/2020

[2] https ://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2017/Nov IoT/Session%201%20IntroIoTMZ-new%20template.pdf. consulté le 30/02/2020

[3] Patel, Keyur & Patel, Sunil & Scholar, P & Salazar, Carlos. (2016). Internet of Things-IOT : Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges

[4] Yacine Challal. Sécurité de l'Internet des Objets : vers une approche cognitive et systémique. Réseaux et télécommunications [cs.NI]. Université de Technologie de Compiègne, 2012. tel-00866052

[5] https ://www.123rf.com/photo_49541954_stock-vector-smart-home-iot-internet-of-things-control-comfort-and-security-isometric-flowchart-icon-poster-abstr.html

[6] J. Sathish Kumar, Dhiren R. Pate. A Survey on Internet of Things : Security and Privacy Issues. International Journal of Computer Applications (0975 –8887)Volume 90 –No 11, March 2014

[7] Wortmann, Felix & Flüchter, Kristina. (2015). Internet of Things. Business & Information Systems Engineering. 57. 221-224. 10.1007/s12599-015-0383-3.