الجـــــــــــــــــــمـهـوريـــــة الجـــــــــــــزائـريـة الديمـــــــقـراطيـة الـشـــــــــعبيـة

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التـــــــــــــــــــــــــــعـليـم العـــــــالي و البـــــــــحث العـــــلـمـــي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جـــــــــــــامعة أبي بكـــر بـلـقـايد– تـلمســـــــــــــان –

Université Aboubakr Belkaïd– Tlemcen –
Faculté de TECHNOLOGIE

MEMOIRE

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

En : Télécommunication

Spécialité : Réseaux et télécommunications

Par : Asmae RABHI

Sujet

Plateforme de Sécurité Légère pour IdO

(Cas d'Etude : Hôtel Intelligent)

Soutenu publiquement, le 19 / 09 / 2020, devant le jury composé de :

M. H.ZERROUKI	Docteur	Univ. Tlemcen	Président
M. M. FEHAM	Professeur	Univ. Tlemcen	Directeur de mémoire
M. S-M. SENOUCI	Professeur	DRIVE	Co-Directeur de mémoire
M. D.MOUSSAOUI	Docteur	Univ.Tlemcen	Examinateur

Remerciements

Je tiens tout d’abord à remercier tous les enseignants du département de Télécommunication qui m’ont fait découvrir de nouvelles disciplines ainsi que tout le personnel administratif et je leur adresse mes sincères reconnaissances.

Je remercie également les membres du jury qui vont évaluer ce mémoire, grâce à leur générosité, les manquements de ce travail seront rectifiés ce qui me permettra de m’améliorer.

Je souhaite remercier aussi mon encadreur, monsieur Mohammed FEHAM pour ses remarques pertinentes.

Je ne sais comment exprimer ma gratitude à mon rapporteur monsieur Sidi Mohammed SENOUCI, le directeur du Laboratoire Drive pour son soutien, ses précieux conseils et surtout sa patience.

Je remercie enfin, monsieur Ayoub MESSOUS et madame Maissa DAMMAK pour leur aide et leur disponibilité lors de la réalisation de ce mémoire.

Dédicaces

A mes chers parents SOUMICHA et BENAMAR

Tous les mots du monde ne sauraient exprimer la profonde gratitude que je vous témoigne. Je vous rends hommage par ce modeste travail et j'espère pouvoir répondre aux espoirs que vous avez fondés en moi. Que dieu tout puissant vous garde et vous procure santé, bonheur et longue vie.

A mon frère MOHAMMED et mes sœur IMENE et MAWAHIB

Que l'amour et la fraternité nous unissent à jamais

A mes grands-parents FATNA et MOHAMMED

Que dieu vous protège et vous procure une longue vie pleine de bonheur

A la mémoire de ma grand-mère FATEMA et mon grand-père ABDESSALAM

Que DIEU tout puissant vous accorde sa clémence et sa miséricorde.

A mon oncle SIDI MOHAMMED, sa charmante femme AMMARIA et ses adorables enfants : RAYANE, LYNA, NASSIM et MYRIAM

A mes tantes, mes oncles et leurs familles

Avec l'amour que je vous porte, je vous souhaite beaucoup de bonheur dans votre vie.

A mes cousins : SAAD, ABOUBAKR, AMINE, FATIMA, ABDESSALEM, ISMAIL, SORIA et MOUNIA qui font partie de es personnes rares par leur gentillesse. Vous partagez toujours une partie de ma vie et de mon cœur. Que DIEU vous procure le bonheur que vous méritez.

A ma meilleure amie ACHOUAK, ma chère amie CHAIMAA et mes camarades SOUMIA.Z, SOUMIA.R et ABDERRAHMANE

Merci pour votre amour et votre amitié. Vous étiez toujours là pour me soutenir, m'aider et m'écouter. Que DIEU vous protège et vous procure joie et bonheur et que notre amitié reste à jamais

Résumé

L'Internet des objets (IoT) est considéré comme l'un des paradigmes les plus marquants, les plus passionnants et les plus révolutionnaires qui a le pouvoir de changer efficacement la façon dont nous interagissons avec notre environnement. L'IdO permet à une grande variété d'appareils intelligents dotés de différentes capacités de calcul, de détection et d'actionnement de communiquer de manière transparente et sans faille sur l'internet. Il permet d'offrir une qualité de vie meilleure.

Dans ce travail, nous avons mis une analyse de l'état de l'art qui portera sur les aspects de sécurité, de confidentialité et le respect de la vie privée liés à l'écosystème de l'Internet des objets. Nous avons analysé les risques et les vulnérabilités liés à un scénario spécifique (serrure connectée dans un *Smart Hotel*). Nous avons conçu une architecture pour le contrôle d'accès basé sur le contexte avec des stratégies de sécurité spécifiques afin de fournir des clés numériques/Tokens pour donner et retirer l'accès aux ressources numériques et physiques dans le cadre de l'Internet des objets (IoT). Nous avons Implémenté un scénario de démonstration en se basant sur une architecture trois-tiers objets-serveur-utilisateurs et dont le but est de sécuriser l'échange et le partage de clés.

Mots-clés : Internet des objets, sécurité des réseaux informatique, protection de la vie privée, contrôle d'accès, Infrastructure à clé publique (PKI).

Abstract

The Internet of Things (IoT) is considered one of the most striking, exciting and revolutionary paradigms that has the power to effectively change the way we interact with our environment. The IoT enables a wide variety of intelligent devices with different computing, sensing and actuating capabilities to communicate and transparently over the Internet. It enables a better quality of life.

In this work, we have put an analysis of the state of the art that will focus on the security, privacy and confidentiality aspects related to the ecosystem of the Internet of Things. We analyzed the risks and vulnerabilities related to a specific scenario (lock connected in a Smart Hotel). We designed an architecture for context-based access control with specific security strategies to provide digital keys/tokens to give and remove access to digital and physical resources in the context of the Internet of Things (IoT). We have implemented a demonstration

scenario based on a three-tiers object-server-user architecture for secure key exchange and sharing.

Keywords: Internet of Things, computer network security, privacy, access control, Public Key Infrastructure (PKI).

ملخص

تعتبر إنترنت الأشياء من أهم الاختراعات المميزة لهذا العصر. لقد شكلت قفزة نوعية و ثورية في عالم التكنولوجيا الحديثة لأنها غيرت، و إلى الأفضل، الطريقة التي نتفاعل بها مع محيطنا. تسمح إنترنت الأشياء لعدد كبير من الأجهزة الذكية الممكنة .من الحساب و الكشف و التشغيل بالتواصل على الإنترنت بطريقة سلسة. كما أنها توفر نوعية حياة أفضل

في هذا البحث ، وضعنا تحليلاً متطورًا للتعامل مع جوانب الأمن والسرية والخصوصية المتعلقة بالنظام البيئي لإنترنت الأشياء. قمنا بتحليل المخاطر ونقاط الضعف المرتبطة بحالة معينة (قفل متصل في فندق ذكي). لقد قمنا بتصميم بنية من اجل التحكم في الدخول مع إجراءات أمنية محددة من أجل توفير مفاتيح رقمية / رموز لمنح و رفض الوصول إلى الموارد الرقمية و المادية في إطار إنترنت الأشياء. لقد قمنا بتطبيق عرض توضيحي يعتمد على مخطط ثلاثي: جهاز-خادم-مستخدم، والغرض .منها هو تأمين تبادل المفاتيح ومشاركتها

كلمات المفاتيح: إنترنت الأشياء، أمان شبكة الكمبيوتر، الخصوصية، نظام مراقبة الدخول، البنية التحتية للمفتاح العام

Table des matières

Liste des figures

CHAPITRE I

CHAPITRE II

CHAPITRE III

CHAPITRE IV

Liste des tableaux

CHAPITRE I

CHAPITRE II

CHAPITRE II

CHAPITRE IV

Abréviations

DRIVE : le Département de Recherche en Ingénierie des Véhicules pour l'Environnement.

IdO : Internet des Objet.

IoT : Internet of Things.

PKI : (Publique Key Infrastructure), Infrastructure à clé publique.

WiFi : (Wireless Fidelity), fidélité sans fil.

MCU : (Micro Controller Units)

ATMEL : advanced technology for memory and logic

ARM : Advanced Risk Machine

CPU : Central Processing Unit

GPU : Graphics Processing Unit

IP : Internet Protocol

STI : Système de Transport Intelligent

GPS : (Global Positioning System), Système mondial de positionnement

OBU : Onboard Unit

WPAN : (wireless personal area network), réseau personnel sans fil

WLAN : (wireless Local area network), réseau local sans fil

WMAN : (wireless Metropolitan area network), réseau metropolitain sans fil

WWAN : (wireless Wide area network), réseau étendu sans fil

GSM : (Global System for Mobile Communications), Système Global pour les Communications Mobiles

GPRS : (General Packet Radio Service), Service général de radio par paquets

UMTS : (Universal Mobile Telecommunications System), Système universel de télécommunications mobiles

OSI : (Open Systems Interconnection), Interconnexion des systèmes ouverts

O-QPSK : Quadrature Phase Shift Keying

BPSK : Binary Phase-Shift Keying

APS : Application Support Sublayer

AF : Application Framework

SSP : Security Service Provider

ZDO : ZigBee Device Object

ZC : ZigBee Coordinateur

ZR : ZigBee Router

ZED : Zigbee End Device

RF : Radio Frequency

LE : Low Energy

MAC : Mandatory Access Control

DAC : Discretionary access control

RBAC : Role-Based Access Control

ORBAC : Organization-Based Access Control

CA : Certificate Authority

XOR : (Exclusive or), fonction OU exclusif.

DoS : Denial of Service

RFID : (Radio Frequency Identification), Identification radiofréquence.

RAM : (Random-access memory), mémoire à accès non séquentiel.

ROM : (Read Only Memory), mémoire morte.

EEPROM : (Electrically Erasable Programmable Read-Only Memory) mémoire en lecture seule programmable et électriquement effaçable.

IEEE : (Institute of Electrical and Electronics Engineers), Institut d'ingénieurs en électricité et électronique.

BLE : (Bluetooth low energy), Bluetooth basse énergie.

NFC : (Near field Communication), Communication en champ proche.

PIN : (Personal Identification Number), nombre d'identification personnel.

PARFAIT : (Personal dAta pRotection FrAmework for IoT), titre projet qui rentre dans le cadre ITEA.

ITEA : est un programme transnational de recherche, développement et innovation (R & D & I) dans le domaine de l'innovation logicielle.

TBLUA : (Token Based Light User Authentification), Authentification des utilisateurs légers basée sur des jetons.

LED : (Light-emitting diode), diode électroluminescente.

IDE : (Integrated Development environment), Environnement de développement.

INTRODUCTION GENERALE

« Il fait -2° dehors, prenez votre manteau » dit mon nouveau dressing intelligent. Certes cette phrase parait un peu futuriste quand-même mais grâce au développement technologique, l'idée peut se concrétiser puisqu'il existe déjà des dressings intelligents qui lavent, sèchent et repassent le linge grâce à une application mobile (*Samsung AirDresser*[1]). Les recherches avaient depuis plusieurs années marqué leurs intérêts pour des objets intelligents et qui ont la possibilité aussi de communiquer.

La notion de communication est au cœur des intérêts de plusieurs chercheurs et devenue donc centrale dans tous les domaines aujourd'hui et en particulier, L'Internet des objets – IdO (*Internet of Things - IoT*). C'est dans ce contexte que j'ai été conduite à associer mon stage à ces nouvelles technologies.

Quand on parle de l'Internet des objets, on parle d'un ensemble de dispositifs interconnectés entre eux permettant de relier le monde virtuel avec le monde physique. L'appellation désigne un nombre croissant d'objets connectés à l'Internet permettant ainsi une communication entre nos biens dits physiques et leurs existences numériques. Ces formes de connexions permettent de rassembler de nouvelles masses de données sur le réseau et donc, de nouvelles connaissances et formes de savoirs. Cette communication entre les différents dispositifs est réalisée en utilisant un réseau de communication sans fil tel que WiFi, NFC ou ZigBee.

De la télé intelligente à la voiture connectée, nos loisirs, nos déplacements sont facilités par ces nouveaux outils qui augmentent grandement notre confort. Certes ces objets connectés simplifient la vie quotidienne mais ils ne sont pas sans défauts. Les risques sont bel et bien présents et menacent différentes parties des systèmes composants l'IdO. Ils peuvent ainsi ciblent les appareils connectés ou même la communication entre ces derniers. Ainsi, il faut bien mettre en place des mécanismes de sécurité pour avoir un système à la fois efficace et sécurisé.

La sécurité est un facteur vital dans la communication des objets connectés. Pour garantir et établir une communication authentique, il est nécessaire de mettre en place des protocoles de communication puissants qui permettent aux objets connectés d'échanger les données en toute sécurité en tenant compte de leur hétérogénéité. Pour assurer tous les aspects de la sécurité (la confidentialité, la préservation de la vie privée des utilisateurs et la garantie de la protection des données, des réseaux, des applications, etc.), il est important de mettre une connexion sécurisée

[1] https://www.senioractu.com/Samsung-Airdresser-le-dressing-lavant-du-futur_a22419.html

entre les objets c'est-à-dire il faut que la sécurité physique et la cyber sécurité soient omniprésentes.

L'authentification et le contrôle d'accès sont l'un des principaux mécanismes de sécurité qui permettent de garantir la confidentialité, l'intégrité et bien d'autres aspects dans le système IdO.

Les objectifs du travail réalisé pendant ce stage sont premièrement d'analyser les risques et les vulnérabilités d'un cas d'usage particulier qui est le cas d'un hôtel intelligent puis d'implémenter une plateforme de sécurité légère pour l'IdO basée sur le contrôle d'accès pour ce cas d'usage.

Ce travail est structuré en deux parties :

- La partie théorique : nous étudierons le contexte ainsi que l'état de l'art de la sécurité de l'Internet des objets ;
- La partie pratique : nous analyserons l'implémentation du système et analyserons sa vulnérabilité en prenant en compte un cas d'usage particulier qui est l'hôtel intelligent.

Ce mémoire est organisé comme suit : dans le premier chapitre, nous présenterons une vue générale sur l'internet des objets, son architecture et ses domaines d'application. Nous présenterons également les réseaux de communication sans fil et nous définirons quelques protocoles utilisés. Dans le deuxième chapitre, nous entamerons la partie dédiée à la sécurité de l'IdO et la protection de la vie privée où nous évoquerons les aspects principaux pour assurer la sécurité tels que le contrôle d'accès, l'authentification, etc. Dans le troisième chapitre, nous expliquerons la conception de notre système basé sur le contrôle d'accès et nous présenterons les exigences nécessaires pour sa mise en œuvre. Ensuite, nous effectuerons une analyse des risques et des vulnérabilités. Dans le quatrième chapitre, nous détaillerons l'implémentation de notre système sur une mini maquette d'hôtel intelligent composée d'une application mobile permettant de donner l'accès ou pas à un utilisateur en toute sécurité.

CHAPITRE I : Internet des Objets

1. Introduction

L'Internet des objets (IdO, en anglais IoT pour *Internet of Things*) est actuellement une des technologies évolutionnaires où le nombre d'objets connectés en perpétuelle augmentation chaque année. Ce concept désigne des objets physiques connectés qui possèdent leur propre identité numérique et qui sont capables de communiquer entre eux ou avec une infrastructure et génèrent des quantités de données. Ce réseau crée un lien entre le monde physique et le monde virtuel.

Ce premier chapitre sera structuré en 4 parties, dans la première partie nous commencerons par définir les objets connectés ainsi que nous donnerons des exemples de cartes les plus utilisées dans un système IdO.

Dans la deuxième partie, nous présenterons l'architecture de l'IdO la plus élémentaire ainsi que les opérations qu'un objet connecté peut effectuer.

Dans la troisième partie, nous présenterons quelques domaines d'applications de l'internet des objets : maison intelligente, ville intelligente, soins de santé intelligents et les systèmes de transport intelligents.

Enfin, la quatrième partie sera consacrée à la connectivité sans fil pour les systèmes IdO où nous rappelons et comparons quelques technologies de réseaux sans fil.

2. Objets connectés

Un objet connecté est un dispositif physique ayant la capacité de se connecter à Internet pour améliorer ses compétences et donc il permet de l'enrichir en termes de fonctionnalité. Il est équipé de capteurs ou d'une puce qui lui permettent d'augmenter son utilisation initiale pour offrir de meilleures possibilités et de nouveaux services.

Par exemple un objet tel qu'une montre ou une serrure est capable de communiquer avec un Smartphone ou un ordinateur, il peut être connecté à l'aide d'un réseau sans fil qui lui permet de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu (Wifi, Bluetooth, réseaux de téléphonie mobile,…), et qui le branche à un réseau local ou à internet.

Un objet connecté est équipé de :

- Capteurs (capteurs de proximité, de mouvements, accéléromètre, luxmètre,… etc.) qui collectent les informations sur l'environnement, c'est-à-dire les données qui sont reçues ou produites, stockées ou transmises.

- Unité de calcul pour exécuter les algorithmes capables d'analyser et traiter les données.

- Dispositif de communication et de transmission.

Quelle unité de calcul : microcontrôleur ou microprocesseur ?

Microcontrôleur : Un microcontrôleur ou MCU (Micro Controller Units) est un circuit intégré numérique (il ne comprend que des 0 et des 1) c'est-à-dire un ordinateur intégré dans une puce électronique qui regroupe les unités principales d'un ordinateur : mémoire morte et mémoire vive, processeur, unités périphériques et interfaces d'entrées-sorties. Les microcontrôleurs servent à enregistrer les données, gérer des capteurs, communiquer avec d'autres microcontrôleurs, etc. Ils existent dans plusieurs domaines tels que l'automobiles, les systèmes de surveillance, appareils médicaux, les appareils domestiques (fours à micro-ondes, les machines à laver,... etc.).

Carte Arduino : Arduino est un microcontrôleur qui donne la possibilité de combiner la performance de la programmation et l'électronique, c'est la base de programmation, le langage utilisé est le Arduino C. La carte Arduino est une carte électronique open source donc c'est une

plate-forme électronique qui se base sur du matériel et des logiciels. Au milieu de chaque carte se situe un microcontrôleur ATMEL. Il y a plusieurs cartes Arduino (Arduino Uno, Arduino nano et Arduino méga), chacune ayant ses propres caractéristiques. Ces cartes peuvent être différentes selon la puissance du microcontrôleur, la consommation et la taille de la carte (voir figure 1 pour Arduino Uno). Les cartes Arduino peuvent lire les entrées (lumière sur un capteur, doigt sur un bouton ou message Twitter) et en faire une sortie : activer un moteur, allumer une LED, publier quelque chose en ligne. Pour cela, l'utilisation du langage de programmation Arduino est le logiciel Arduino (IDE) [2].

Microcontrôleur : ATMEGA328P.
Fréquence : 16 MHz
Mémoire flash : 32 KB
Entrées/sorties digitales : 14 pins.
Pins analogiques : 6 pins.
Pin UART : 2 pins.
Pin PWM : 6 pins.
La tension de fonctionnement : 5v.
EEPROM : 1 KB.
Dimensions **:** 74 x 53 x 15 mm

Figure 1 : Carte Arduino Uno [2]

Microprocesseur : Un microprocesseur est un circuit intégré complexe caractérisé par une très grande intégration et doté des facultés d'interprétation et d'exécution des instructions d'un programme. Il est chargé d'organiser les tâches précisées par le programme et d'assurer leur exécution. Il doit aussi prendre en compte les informations extérieures au système et assurer leur traitement. C'est le cerveau du système. Un microprocesseur est construit autour de deux éléments principaux : une unité de commande et une unité de traitement, associés à des registres chargées de stocker les différentes informations à traiter. Ces trois éléments sont reliés entre eux par des bus interne permettant les échanges d'informations. [3]

Raspberry PI : Le Raspberry PI est un micro-ordinateur équipé d'un microprocesseur ARM, et un système d'exploitation libre de type GNU/Linux et des logiciels compatibles, il est très utilisé dans les applications domotiques [4]. Le Raspberry PI est un nano ordinateur de la taille d'une carte de crédit que l'on peut brancher à un écran et utiliser comme un ordinateur

standard (voir figure 2 pour *Raspberry Pi 3 Model B*). Il est capable de faire tout ce que vous attendez d'un ordinateur de bureau : naviguer sur Internet, lire des vidéos hautes définitions, créer des feuilles de calcul, traiter des textes et jouer à des jeux [5]. Sa petite taille, et son prix intéressant font du lui un produit idéal pour tester différentes choses, et notamment la création d'un serveur Web chez soi. Évidemment, pour sa taille il ne faut pas s'attendre à des performances incroyables, mais pour mettre en ligne des projets à montrer au client ou expérimenter avec linux c'est largement suffisant [6].

CPU : quadricoeur ARM Cortex-A53 1.2 GHz (Broadcom BCM2837)
GPU (Processeur graphique) : Dual Core VideoCore IV, Multimedia Co-Processor
Mémoire RAM : 1 Go
Usb : 4 ports USB 2.0
Sorties audio : HDMI et stéréo jack 3,5 mm
Sorties vidéo : HDMI
Support pour cartes **:** micro-SD
Source d'alimentation : 5v
Dimensions : 88 x 58 mm

Figure 2: Raspberry Pi 3 Model B [5]

3. Architecture de l'Internet des objets

Comme indiqué dans l'introduction de ce chapitre, IoT est l'abréviation de Internet of Things ou en français l'Internet des Objets, c'est la nouvelle révolution de l'internet qui permet de relier le monde physique au monde virtuel.

IEEE Communications Magazine le définit comme un "cadre dans lequel tous les objets ont une représentation et une présence sur Internet. Plus spécifiquement, l'internet des objets vise à proposer de nouveaux services et applications permettant de relier le monde virtuel au monde physique, dans lesquels les communications de machine à machine (M2M) représentent la base communication qui permet les interactions entre objets et les applications dans le cloud. [7]

Comme illustré dans la figure suivante, l'évolution rapide de l'IoT a élargi la capacité de communication et la rendu plus facile en autorisant aux personnes de se connecter avec n'importe quoi et n'importe qui, de n'importe où à n'importe quel moment à travers des objets connectés qui font la collecte et le partage des données.

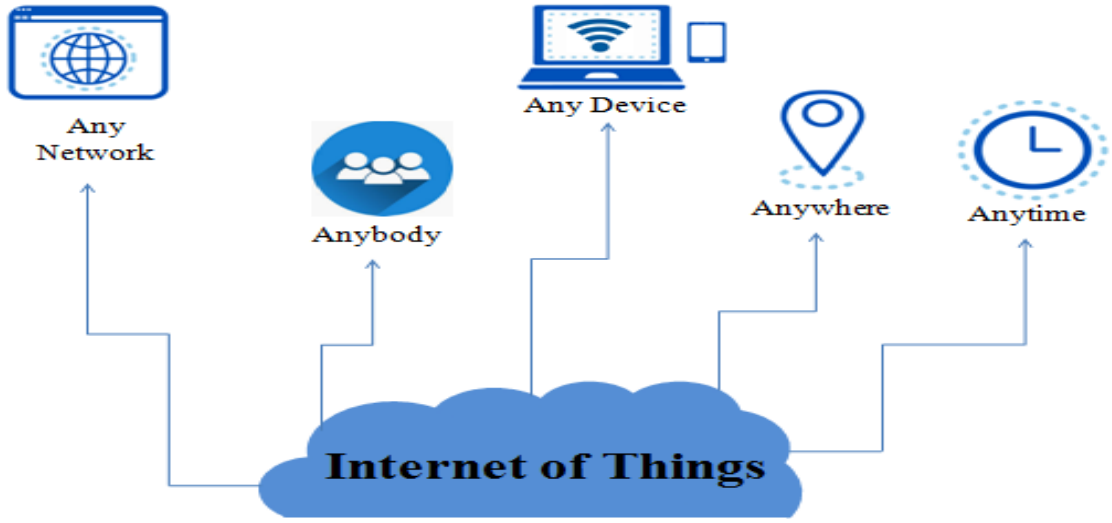

Figure 3 : Concept de l'internet des objets

Il n'y a pas de consensus unique sur l'architecture de l'IoT, qui est universellement acceptée. Plusieurs architectures ont été proposées par différents chercheurs.

L'architecture la plus élémentaire est une architecture à trois couches, comme indiqué dans la figure 4, à savoir les couches perception, réseau et application. [8]

La couche perception : La couche physique a des capteurs pour détecter et recueillir des informations sur l'environnement. Il détecte certains paramètres physiques ou identifie d'autres objets intelligents dans l'environnement.

La couche réseau : elle est responsable de la connexion à d'autres objets intelligents, périphériques réseau et serveurs. Ses fonctionnalités sont également utilisées pour transmettre et traiter les données des capteurs.

La couche application : elle est chargée de fournir des services spécifiques à l'application pour l'utilisateur. Elle définit diverses applications dans lesquelles l'Internet des objets peut être déployé.

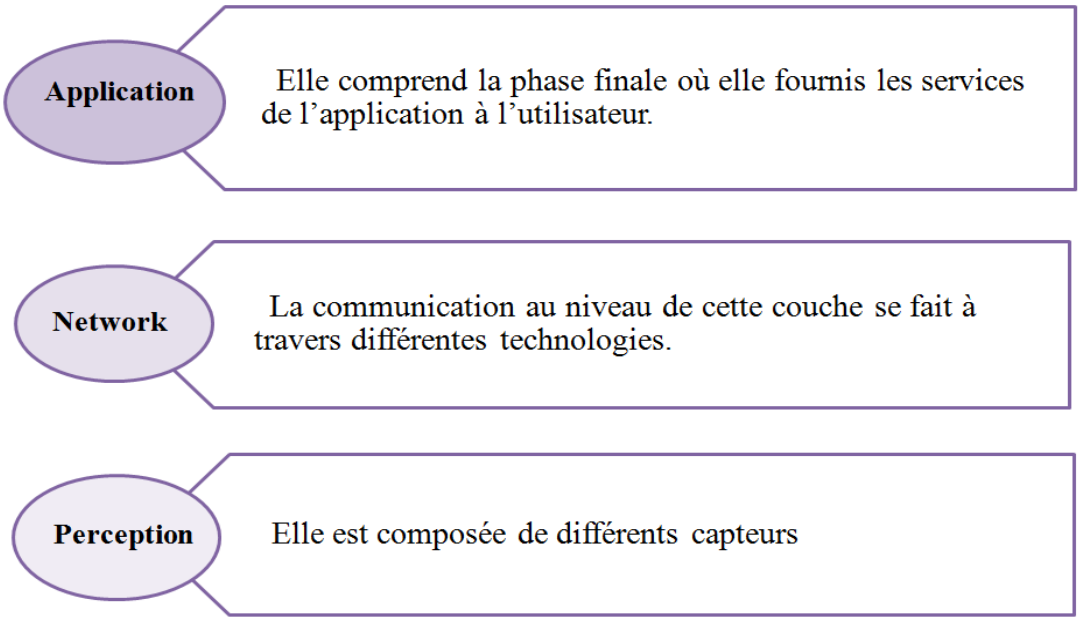

Figure 4 : Les différentes couches de l'IoT

Comme nous l'avons vu précédemment, les objets connectés sont des dispositifs qui nous permettent de faire plusieurs opérations : la collecte, le stockage, transmission et traitement des informations ou autrement dit les données. Ces objets sont divisés en deux catégories : objets passifs (Puce RFID : faible capacité de stockage) et les objets actifs (Capteurs: plus grande capacité de stockage).

Chaque processus a un rôle différent et spécifique (figure 5) :

- **Capter** : l'action de transformer une grandeur physique analogique en un signal numérique.

- **Concentrer** : permet d'interfacer un réseau spécialisé d'objet à un réseau IP standard (ex. Wifi) ou des dispositifs grand public. [9]

- **Stocker** : qualifie le fait d'agréger des données brutes, produites en temps réel, arrivant de façon non prédictible. [9]

- **Présenter** : indique la capacité de restituer les informations de façon compréhensible par l'Homme, tout en lui offrant un moyen d'agir et/ou d'interagir. [9]

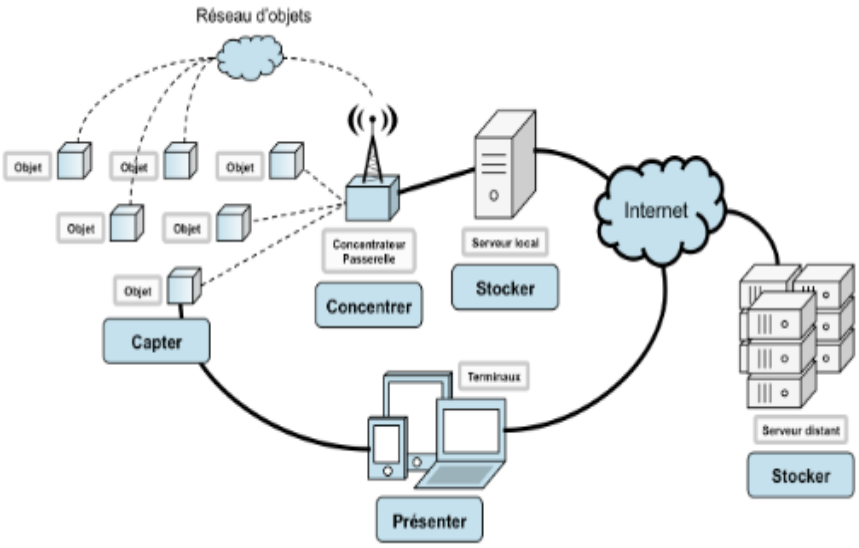

Figure 5 : Architecture de l'IoT [9]

Deux autres processus n'apparaissent pas sur le schéma, car ils sont à la fois transverses et omniprésents :

Le traitement des données est un processus qui peut intervenir à tous les niveaux de la chaîne, depuis la capture de l'information jusqu'à sa restitution. Une stratégie pertinente et commune quand on parle d'Internet des objets, consiste à stocker l'information dans sa forme intégrale. On collecte de manière exhaustive, « big data », sans préjuger des traitements qu'on fera subir aux données. Cette stratégie est possible aujourd'hui grâce à des architectures distribuées type NoSQL, capables d'emmagasiner de grandes quantités d'information tout en offrant la possibilité de réaliser des traitements complexes en leur sein [9].

La transmission des données est un processus qui intervient à tous les niveaux de la chaîne. Deux réseaux supportent les transmissions ; le réseau local de concentration (ZigBee, Zwave, etc.) et le réseau WAN [9].

4. Domaines d'application

Les systèmes IoT ont une énorme possibilité qui affecte et améliore plusieurs applications. Comme illustré dans la figure 6, ils sont utilisés dans de nombreux domaines différents tels que les maisons intelligentes, les villes intelligentes, la santé, les systèmes de transport et plusieurs autres domaines.

Chaque appareil IoT peut fournir de nombreux services pour promouvoir un environnement intuitif. Le paradigme IoT intègre des fonctionnalités de détection, de communication, de mise en réseau, d'identification et d'informatique pour permettre aux services omniprésents d'accéder aux données des appareils intelligents à tout moment et n'importe où [10].

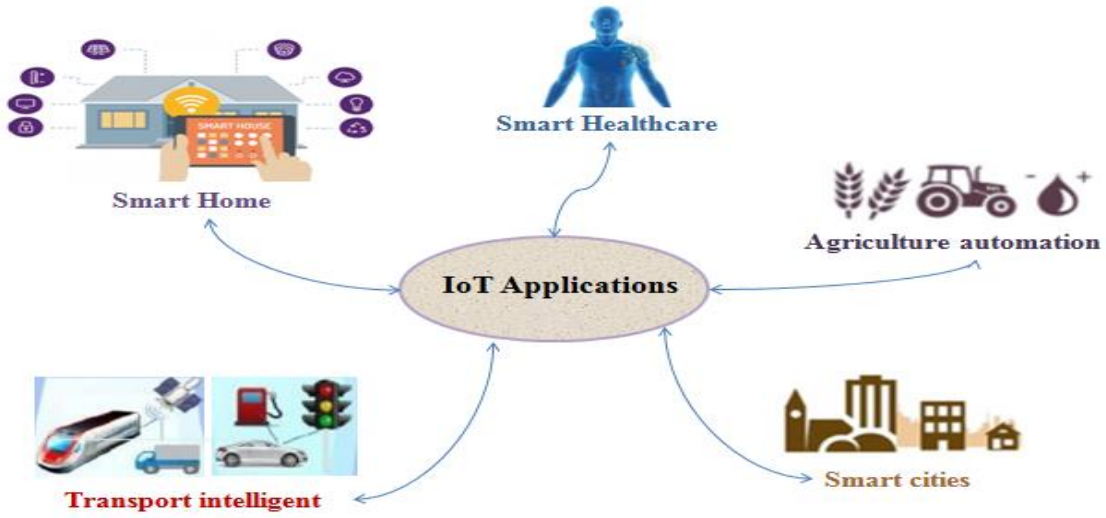

Figure 6 : Domaine d'applications de l'IoT

4.1.Smart home

L'IoT permet de connecter les différents appareils d'une maison (télévision, chauffage, climatiseur, éclairage, …) à un réseau et de les gérer et les contrôler à distance pour améliorer le confort de tous les jours et faciliter la vie. Ainsi, l'objectif d'une maison intelligente est d'avoir une vie plus sécurisée, surveillée tout le temps ce qui permet de détecter une intrusion, un cambriolage, ou un incendie.

En fait, de nombreux capteurs et actionneurs sont déployés pour suivre la consommation des services publics, surveiller et piloter à distance les appareils et les systèmes domestiques [11].

4.2.Smart city ou ville intelligente

C'est un paradigme émergent qui vise à améliorer le partage d'informations et coordination. Il vise également l'amélioration de la qualité de service aux citoyens [12].

Une ville intelligente permet de mettre en place une infrastructure de gestion (eau, énergie, information et télécommunications, transports, services d'urgence, équipements publics,

bâtiments, gestion et tri des déchets, …). De même, une ville intelligente est communicante, adaptable, durable, efficace, respectueuse de l'environnement et finalement automatisée pour améliorer la qualité de vie de ses habitants. [13]

4.3. Smart healthcare ou santé intelligente

Les soins de santé intelligents permettent de suivre la condition du patient, de la contrôler et de la surveiller à distance où ils seront équipés des dispositifs qui effectuent ce contrôle, ces dispositifs médicaux intelligents ont pour rôle de recueillir et d'analyser les informations sur les activités des patients et sur la santé tel que la température du corps, la pression de sang, l'activité respiratoire…etc. Les informations collectées seront par la suite regroupées et transmises aux prestataires et spécialistes médicaux pour prendre les bonnes mesures au bon moment.

Fournir des informations sur l'état d'un patient rend le processus plus efficace et rend les gens beaucoup plus satisfaits. [13]

4.4. Les systèmes de transport intelligent (STI)

Les systèmes de transport intelligents (STI) représentent une nouvelle technologie pour améliorer les performances et la sécurité des transports. Ce sont des applications qui détectent les informations et gèrent la communication du système. Les STI servent à réduire le taux d'accidents, améliorer la gestion de trafic, contrôler la vitesse et minimiser l'impact sur l'environnement.

Les STI permettent donc aux utilisateurs d'être mieux informés et de rendre l'utilisation des réseaux de transport plus sûre, plus coordonnée et plus intelligente. [14]

Les STI se composent de quatre composants principaux, à savoir **le sous-système du véhicule** qui utilise le GPS, le lecteur RFID, l'unité embarquée (OBU) et la communication ; **le sous-système de station** qui représente l'équipement routier ; **le centre de surveillance des STI**; et le **sous-système de sécurité** [15].

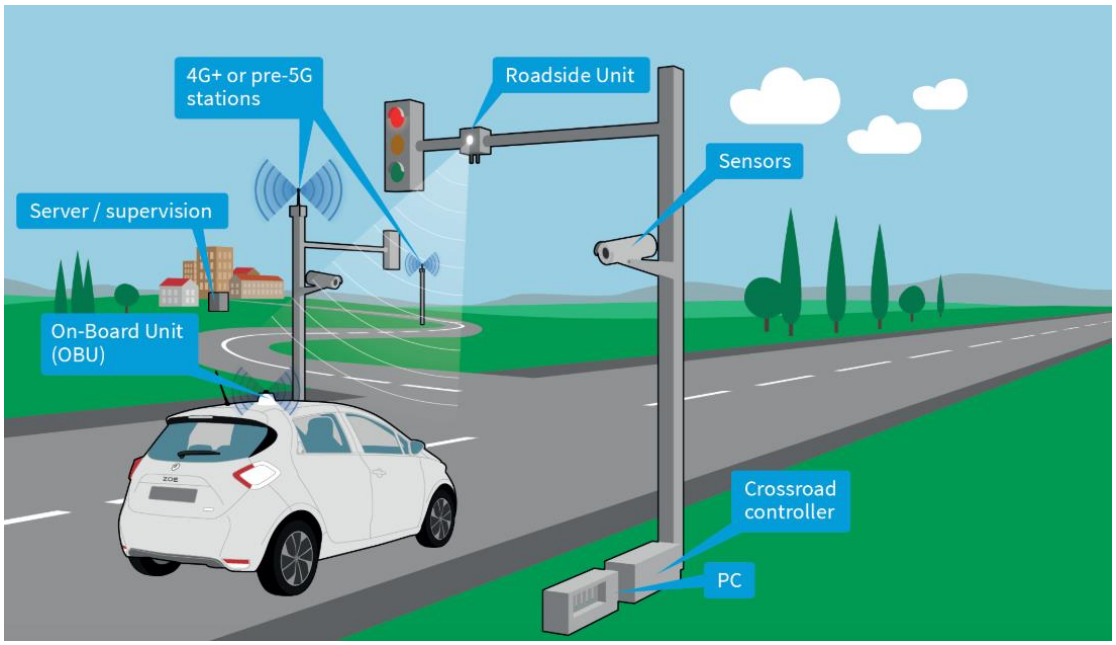

Figure 7: Système de transport intelligent [16]

5. Connectivité sans fil pour l'IDO

Beaucoup d'objets peuvent se connecter et devenir intelligents grâce à l'IdO. De ce fait, il est possible d'affirmer que l'IdO améliore plusieurs aspects de la vie quotidienne en échangeant les informations, il suffit d'avoir une connectivité sans fil

5.1. Qu'est-ce qu'un réseau sans fil ?

Un réseau de communication sans fil est une méthode de transmission des données, c'est un ensemble de dispositifs qui communiquent entre eux sans avoir besoin d'utiliser des liaisons filaires c'est-à-dire des câbles réseaux tel qu'un câble coaxial, paire torsadée, fibre optique...etc. Ces réseaux sans fil ont donné aux utilisateurs la possibilité de se connecter en se déplaçant à n'importe quel endroit mais dans un périmètre géographique plus ou moins étendu.

Au lieu des câbles réseaux, les réseaux de communication sans fil sont basés sur des liaisons des ondes radio (radioélectriques). Ils ont plusieurs caractéristiques telles que la fréquence de fonctionnement, la portée, la consommation énergétique, la topologie qui signifie l'organisation du réseau (étoile, anneau, maillé...), le coût de mise en place, le débit mais en ce qui concerne les objets connectés ils transmettent peu de données.

Selon la couverture géographique on distingue 4 types de réseaux (figure 8) :

- **Réseaux personnels sans fil (WPAN) :** les réseaux avec une faible portée c'est-à-dire une couverture d'une dizaine de mètres (~10m). Ils servent à mettre en contact les équipements personnels (téléphone portable, caméra, imprimante…). Il existe différentes technologies pour le WPAN tels que Bluetooth, Zigbee, …

- **Réseaux locaux sans fil (WLAN) :** les réseaux privés qui sont administrés par des entreprises qui couvrent une centaine de mètres (de 10 m jusqu'à 1 Km), les technologies employées sont Ethernet, WIFI…etc.

- **Réseaux métropolitains sans fil (WMAN) :** les réseaux qui regroupent plusieurs réseaux LAN c'est-à-dire une ville avec une portée de 4 à 10 kilomètres, la technologie basée sur WMAN est Wimax (IEEE 802.16).

- **Réseaux étendus sans fil (WWAN) :** les réseaux qui interconnectent les WLAN et les WMAN avec une couverture de centaine ou de milliers de km (un pays ou un groupe de pays). Ces technologies sont GSM, GPRS, UMTS…

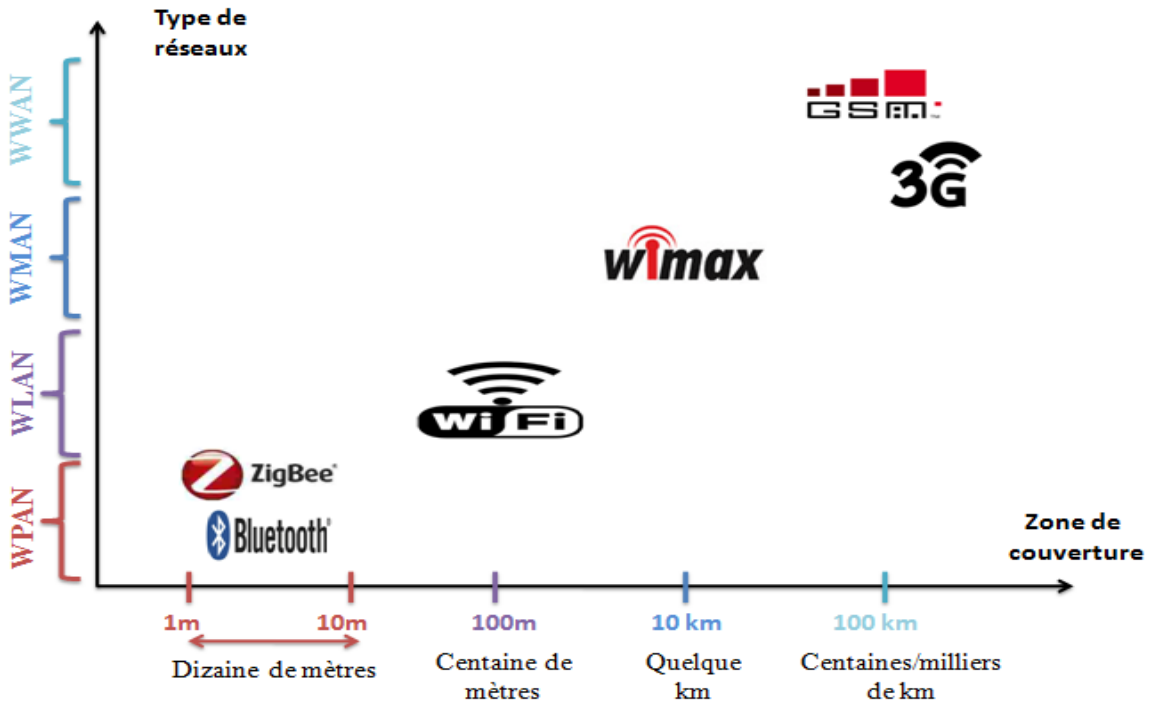

Figure 8 : Couverture des réseaux sans fil

5.2. Technologies de communication sans fil

L'IdO utilise une grande variété de technologies chacune de ces technologies est basée sur différents protocoles de communication, il est donc nécessaire de choisir la norme la plus appropriée c'est-à-dire la meilleure technologie pour les objets connectés. Nous allons citer quelques types de ces technologies, à savoir ZigBee, NFC, Bluetooth et Wifi.

5.2.1. Technologie ZigBee

5.2.1.1. Définition

La technologie ZigBee (ou IEEE 802.15.4) est une norme de communication sans fil WPAN, souvent utilisée pour les applications domestiques. Parmi ses caractéristiques, elle a une très faible consommation d'énergie, moins chère et aussi un protocole beaucoup plus simple, ce qui en fait un produit qui convient très bien à l'intégration dans des appareils électroniques de petite taille. Grâce à ce type de protocole de communication, les appareils des maisons intelligents pourront maintenant communiquer et se connecter de manière plus simple, mais à des distances plus ou moins limitées, permettant ainsi d'améliorer le confort de la vie quotidienne et d'avoir une vie plus sécurisée.

La communication entre les équipements ZigBee repose sur la définition des profils qui se décomposent en deux types : privés et publics. Chaque profil public possède un identifiant (ID). Quelques exemples de profils publics : ZigBee Smart Energy (SE) pour la gestion de l'énergie; ZigBee Personal Home & Hospital Care (PHHC) pour le suivi des patients, équipements de santé, fitness; ZigBee Home Automation (HA) pour le contrôle de la maison, domotique [17].

5.2.1.2. Pile protocolaire de ZigBee

L'OSI (Open Systems Interconnection) a proposé une structure en couche classique, cette pile de protocoles ZigBee est divisée en quatre couches essentielles (figure 9). Les deux couches inférieures de la pile ZigBee - la couche physique (PHY) et la couche de contrôle d'accès (MAC)- sont toutes les deux définies par la norme IEEE 802.15.4, alors que l'autre partie de la pile - la couche réseau (NWK) et la couche d'application (APL) - est définie par la spécification ZigBee.

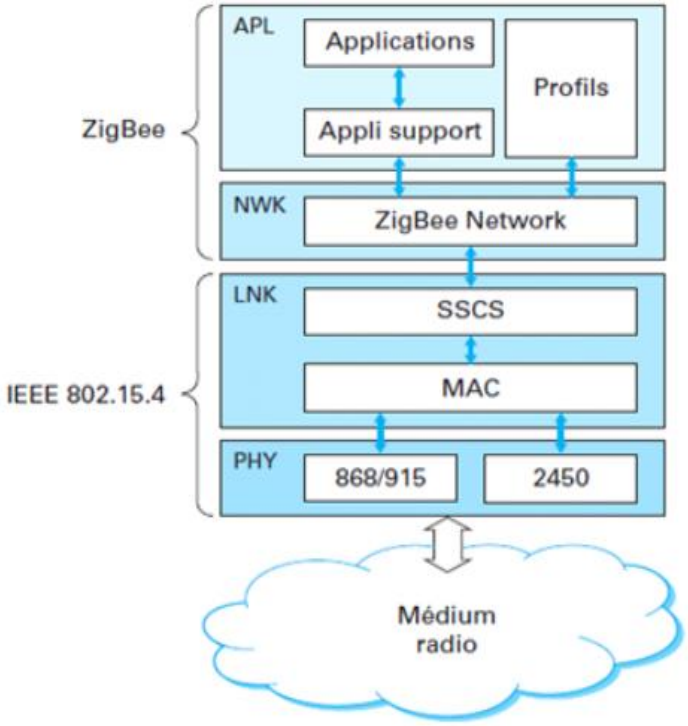

Figure 9 : Pile du protocole ZigBee [18]

La couche physique (PHY) : Permet l'activation de l'interface radio et ainsi sa désactivation, la détection d'énergie (lumière, température, …), l'émission et la réception des données. Elle utilise 3 bandes de fréquences :

- 2.4 GHz avec un débit de 250Kbits/s qui utilise la modulation par décalage de phase orthogonale en quadrature (O-QPSK).

- 915 MHz avec un débit de 40 Kbits/s qui utilise la modulation par décalage de phase binaire (BPSK).

- 868 MHz avec un débit de 20Kbits/s qui utilise aussi la modulation par décalage de phase binaire (BPSK).

La couche de contrôle d'accès (MAC) : Permet de contrôler le mécanisme d'accès au support c'est-à-dire le dialogue du réseau de transmission ou de réception, d'assurer l'intégrité des données, elle permet également de supporter les associations et les dissociations au réseau. Elle a deux types d'accès au réseau :

- Le mode non coordonné (CSMA/CA) : propose moins d'innovations que les autres technologies sans fil. Dans ce cas, la transmission s'effectue dès que l'appareil reçoit le canal.

- Le mode coordonné (beacon mode) : fournit un aperçu des applications intéressantes pour mettre en place la qualité de service ainsi que pour synchroniser la transmission des différents nœuds. Les trames de balises (BEACON) sont transmises de façon périodique par le coordinateur.

La couche réseau (NWK) : Elle est responsable de plusieurs opérations dans un réseau, notamment l'association et la dissociation de tous les nœuds du réseau, ce qui signifie qu'elle fournit des mécanismes permettant de constituer un réseau pour le joindre ou le quitter. Elle permet également la maintenance des routes; elle assure le transfert d'informations et la communication entre les nœuds du système, elle a pour rôle aussi d'identifier les routes entre les différents équipements connectés et de découvrir le voisinage du réseau. Elle prend aussi la responsabilité de l'adressage, l'acheminement et la sécurité des paquets.

La couche d'application (APL) : La couche application a pour but de rendre compatible les différents dispositifs proposés par des fabricants différents [19]. Elle est associée à plusieurs éléments :

- La couche interface APS (Application Support Sublayer) : assure l'interface entre la couche de réseau et la couche d'application à travers un ensemble de services [17]. Elle gère le transfert entre les périphériques et gère la sécurité au niveau de l'application [19]
- Le support d'application AF (Application Framework) : accueille les différents profils d'application. Elle propose également des API pour les développeurs [17]
- Le module SSP (Security Service Provider) : s'occupe de fournir des services de sécurité aux couches NWK et APS [17]
- Le module ZDO (ZigBee Device Object) : définit le rôle du dispositif (coordinateur, …), gère les associations et découvre les périphériques du réseau [19]

5.2.1.3. Caractéristiques de la technologie

Il existe trois éléments dans une topologie de réseau ZigBee: le coordinateur ZigBee (ZC) qui se charge de créer et de contrôler le réseau, le routeur ZigBee (ZR) qui a la possibilité d'être associer au ZC et aux autres ZR et il s'occupe de la transmission de l'information obtenue afin

d'étendre le réseau, et enfin le Terminal ZigBee (ZED). Ce dernier doit d'abord être associé au ZC ou à un ZR. Il ne s'agit que d'un composant final du réseau, car il n'accepte aucune association ou participation à l'acheminement des messages.

La couche réseau du protocole ZigBee prend en charge 3 topologies différentes : la topologie en étoile où les données échangées passent par le coordinateur qui gère les équipements qui ne communiquent qu'avec lui, la topologie maillée où chaque routeur est relié à différents chemins pour transmettre les paquets de données de ses voisins et la topologie en arbre où les messages sont contrôlés et les données sont transmises par des routeurs à l'aide d'un routage hiérarchique.

Le niveau de sécurité offert par l'architecture de sécurité ZigBee dépend de la protection des clés symétriques, des mécanismes de protection utilisés, ainsi que de la bonne mise en œuvre des mécanismes cryptographiques et des politiques de sécurité. ZigBee utilise certains éléments de sécurité de la norme *802.15.4*. Il étend les fonctionnalités de cette norme en utilisant des clés de chiffrement AES d'une taille de 128 bits [17].

5.2.2. Technologie NFC

5.2.2.1. Définition

La NFC (Near Field Communication) est une technologie de communication sans fil (WPAN) qui se fait entre deux dispositifs électriques : un lecteur et un terminal mobile. Cette technologie permet d'échanger les informations et de transmettre les données d'un appareil à un autre dans une distance limitée et proche (moins de 10 cm). L'une de ses caractéristiques est que les données échangées sont envoyées très rapidement. Le NFC a de nombreuses applications qui permettent de réaliser des paiements ou un accès à des informations précises à 'l'aide d'un tag NFC.

La technologie NFC est basée sur un champ de radiofréquences (RF) avec une fréquence de base de 13,56 MHz. Le champ RF généré par un dispositif de forum NFC pour communiquer avec une balise de forum NFC a trois rôles :

- Le transfert de l'alimentation du périphérique Forum NFC au tag Forum NFC.
- L'envoi des informations à une étiquette de forum NFC par le périphérique NFC en modulant le signal de champ RF (modulation du signal).

- La réception des informations d'un tag Forum NFC par Le périphérique NFC en détectant la modulation de la charge générée par le tag Forum NFC (modulation de charge).

5.2.2.2. Modes de communication

Les modes de fonctionnement de NFC se répartissent en trois catégories :

- **Mode émulation de carte** : permet d'utiliser un appareil muni du NFC comme d'une carte sans contact. Couplé à un Smartphone, le NFC se met en relation avec la carte SIM, où peuvent être stockées des données chiffrées [20].Il peut être positionné dans les portes des bouches de métro ou dans une borne de paiement. Ainsi, les utilisations sont nombreuses : paiement mobile, titres de transport, coupons, billets, … [21]

Figure 10 : Mode émulation de la carte [22]

- **Mode lecteur** : permet de transformer le terminal mobile en lecteur de « tags » (étiquettes électroniques), ce qui permet d'obtenir des informations ou de lancer une application de manière automatique sur les téléphones. Ces tags NFC permettent de connaître la traçabilité d'un produit alimentaire, l'empreinte écologique d'un jouet ou encore le temps d'attente pour le prochain bus dans un abribus équipé. [20]

Figure 11 : Mode lecture [22]

- **Mode pair à pair (P2P)** : permet d'échanger des informations entre deux périphériques équipés du NFC, par exemple transférer des photos, des vidéos ou des textes d'un appareil à un autre en ayant seulement à les rapprocher l'un de l'autre [20].

Figure 12 : Mode P2P [22]

5.2.3. Technologie Bluetooth

Le Bluetooth (ou IEEE 802.15.1) est une technologie de communication sans fil (WPAN) à courte portée dont les principales caractéristiques sont la faible puissance d'émission, la robustesse et le faible coût. Il permet de connecter différents appareils (téléphones mobiles, ordinateurs ou équipements audio) à un ou plusieurs hôtes. Les systèmes de technologie sans fil Bluetooth se divisent en deux types : Le mode classique qui offre des débits élevés mais une forte consommation d'énergie et Le mode Low Energy (LE) avec une consommation d'énergie faible.

5.2.4. Technologie Wifi

Le Wifi (ou IEEE 802.11) est un réseau de communication sans fil (WLAN) qui relie de nombreux appareils informatiques tels qu'un modem internet, ordinateur portable ou fixe, Smartphone ou n'importe quel périphérique avec une liaison haut débit par des ondes radio pour transmettre des données entre eux. La technologie Wifi divise en plusieurs catégories, les normes les plus courantes sont IEEE 802.11 a, b, g, n, ac, la norme IEEE 802.11 ad et la norme IEEE 802.11 ah pour les objets connectés.

5.3. Comparaison de ces technologies

Chaque protocole de communication a ses propres caractéristiques; de ce fait, les caractéristiques différentes des quatre réseaux les rendent appropriés pour des situations particulières Le tableau suivant est un tableau récapitulatif comparant les quatre principaux protocoles d'Internet des objets:

	ZigBee IEEE 802.15.4	NFC	Bluetooth IEEE802.1.5.1	Wifi IEEE 802.11
Topologie	maillée	P2P	P2P	Etoile
Technologie principale	WPAN	WPAN	WPAN	WLAN
Portés	100m	< 10cm	10-100m	100-300m
Fréquence	868MHz-2.4GHz	13.56MHz	2.4GHz	2.4GHz-5GHz
Débit	20Kb/s-250Kb/s	424Kb/s	1Mb/s	54Mb/s
Consommation d'énergie	Faible 	Très faible 	Faible 	Elevée 

Tableau 1 : Comparaison de quelques technologies de communication pour l'IdO

6. Conclusion

Ce premier chapitre était consacré à la présentation générale de l'internet des objets. Il est composé de plusieurs parties où nous avons définis son architecture et quelques types d'applications. Nous avons cité les technologies de communication les plus utilisés dans l'internet des objets ainsi que leur mode de fonctionnement.

Le chapitre suivant sera dédié au concept lié à la sécurité et à la vie privée, où nous allons définir différentes techniques de sécurité. Nous évoquons ainsi la classification des attaques tout en définissant quelques unes.

CHAPITRE II : Sécurité et vie privée dans l'Internet des objets

1. Introduction

L'IdO est aujourd'hui utilisé dans plusieurs secteurs et sa sécurité est liée aux nombres des objets connectés qui augmentent.

C'est l'évolution d'un réseau d'ordinateurs interconnectés vers un réseau d'objets interconnectés. Pour permettre à ce réseau d'atteindre son potentiel, plusieurs aspects doivent être étudiés et nécessitent de résoudre un certain nombre de problématiques [18]

Ce deuxième chapitre sera réparti en quatre sections. Dans la première section, nous définirons le terme de sécurité dans l'internet des objets et la protection de la vie privée. Ensuite, nous nous intéressons à la sécurité des communications dans les différentes couches de l'architecture IdO.

Dans la deuxième section, nous définirons un concept important qui est celui du contrôle d'accès. Puis, nous citerons quelques catégories de contrôle d'accès.

Dans la troisième section, nous présenterons un système de sécurité léger pour l'IdO. Nous définirons et expliquerons les aspects suivants : l'infrastructure à clé publique, le token et l'authentification légère basée sur les tokens.

Enfin, la quatrième section sera dédiée à la classification des attaques selon les couches de l'architecture de l'IdO. Puis, nous définirons quelques attaques qui se sont avérées intéressantes par la suite.

2. Définition

2.1. La sécurité de l'Internet des objets

L'IoT est plus susceptible d'être attaqué que l'Internet puisque des milliards d'appareils produiront et consommeront des services. La sécurité représente un élément essentiel pour permettre l'adoption généralisée des technologies et des applications de l'IoT. Sans garantie en termes de confidentialité et d'authenticité, les parties prenantes concernées seront peu susceptibles d'adopter des solutions IoT à grande échelle [23].

La sécurité informatique consiste à protéger les réseaux et les données collectées et stockées dans les systèmes informatiques (ressources matérielles et logicielles) contre les attaques malveillantes et les accès non autorisés. Le système IoT doit garantir plusieurs aspects :

- **La confidentialité :** la confidentialité des données est un des aspects fondamentaux de la gestion des données au sein d'un système d'information. Des mesures de tous types peuvent être établies afin d'assurer que les données soient vues par les personnes autorisées [24] en utilisant le chiffrement par clés ou la cryptographie des données.

- **L'authentification :** L'authentification peut être définie comme le processus de prouver une identité revendiquée. La confidentialité, l'intégrité des données, et la répudiation dépendent tous de l'authentification appropriée. Un système sans cette fonctionnalité ne peut pas fournir les objectifs de sécurité mentionnée de manière satisfaisante [25].

- **L'intégrité :** L'intégrité est un autre aspect de la gestion des données. Il s'agit ici de s'assurer par divers moyens que les données ne soient pas altérées au cours de leur acheminement [24].

- **La non-répudiation :** La non-répudiation joue un rôle majeur également dans la sécurité. L'objectif est d'empêcher toute personne de dénier le fait d'avoir effectué certaines actions, donc de pouvoir consulter un historique complet des actions faites avec un horodatage précis. Cet aspect de la sécurité a un impact évident sur la disponibilité, puisqu'il s'applique aussi sur la possibilité d'une erreur humaine qui aurait pour conséquence une interruption de service [24].

- **La disponibilité :** La disponibilité des données a pour but de maintenir en condition opérationnelle tous les équipements et les logiciels qui composent l'infrastructure informatique d'une société [24].

Afin de fournir et d'assurer chacun des services énumérés ci-dessus, différents mécanismes de sécurité doivent être mis en place. Le tableau suivant montre quelques mécanismes associés à chaque service.

Principes de sécurité	Mécanismes de sécurité
Confidentialité	Les mécanismes cryptographiques symétriques/asymétriques (AES, RSA, …)
Authentification	Le code d'authentification de message et le chiffrement
Intégrité	Les fonctions de hachage (md5, SHA, …) et les signatures numériques
Non répudiation	Les signatures numériques
Disponibilité	Le contrôle d'accès

Tableau 2 : La relation entre les services et les mécanismes de sécurité

2.2. Protection de la vie privée

Les capteurs connectés à Internet et reliés à notre propre environnement collectent des informations privées tels que l'état de santé et la localisation géographique.

L'accès direct par les objets connectés aux informations personnelles des individus et des organisations soulève des problématiques de protection de la vie privée. L'IoT doit fournir la protection des données privées transmises à travers Internet, de manière à ce qu'un trafic capturé n'expose pas le contenu de ces données. Pour cette raison, des mécanismes pour l'anonymat de données, le pseudonyme et la non-traçabilité doivent être utilisés pour garantir à la fois la protection des données privées ainsi que la protection des entités elles-mêmes [26].

2.3. Sécurité des communications dans l'IoT

L'architecture IoT repose sur trois couches (physique, réseau et application). Selon son fonctionnement, chaque couche peut être exposée à plusieurs problèmes de sécurité. Les

dispositifs et les services intelligents sont sensibles à différentes attaques et menaces de sécurité qui peuvent perturber et détruire les fonctionnalités du réseau.

2.3.1. La couche physique

Étant donné que l'objectif principal de la couche de perception dans l'IoT est de collecter des données, les défis de sécurité dans cette couche impliquent la falsification des données recueillies et la destruction des appareils de détection. Plus précisément, trois grands problèmes de sécurité se posent dans cette couche. Le premier problème est lié à la puissance des signaux sans fil. Comme les nœuds IoT communiquent via des réseaux sans fil, les communications sont vulnérables aux perturbations des ondes. En fait, un adversaire peut envoyer un signal de bruit pour interférer avec les informations échangées entre les nœuds de capteur. Le second problème, c'est le déploiement en extérieur des nœuds de capteurs qui les expose à des attaques matérielles au cours desquelles un attaquant peut altérer les composants physiques du dispositif. Enfin, la nature dynamique de la topologie du réseau et les ressources limitées des dispositifs IoT en termes de communication, de calcul et de stockage les rendent vulnérables à de nombreuses menaces et attaques [27].

2.3.2. La couche réseau

Puisque l'objectif principal de la couche réseau de l'IdO est de transmettre les données collectées, les problèmes de sécurité dans cette couche sont liés à la disponibilité des ressources du réseau [28]. En outre, la caractéristique de la communication M2M introduite par le réseau de l'IdO impose un problème de sécurité de compatibilité. L'hétérogénéité des composants du réseau rend la réutilisation des protocoles de réseau actuels inadéquate dans l'environnement IoT. Les mécanismes d'accès à distance et l'échange de données sensibles sur le canal sans fil augmentent la probabilité des attaques. Plus précisément, les attaquants peuvent exploiter l'interconnexion entre les dispositifs IdO pour divulguer des informations privées et mettre en évidence des activités criminelles [29].

2.3.3. La couche application

Pour répondre aux besoins des utilisateurs, la couche application met à disposition des services intelligents de haute qualité. En effet, les différentes applications nécessitent des exigences de sécurité différentes.

À ce niveau, la protection de la vie privée est la question la plus délicate qui doit être traitée de manière adéquate, car les applications IdO collectent en permanence nos informations privées, partout et à tout moment. En effet, ces applications peuvent même surveiller notre vie quotidienne et toute fuite d'informations peut entraîner des incidents de sécurité coûteux. Par exemple, l'accès non autorisé à des données sensibles peut facilement causer des dommages au système en interdisant l'accès aux services IdO [30].

3. Contrôle d'accès

La conception d'un système informatique et la sécurité réseau reposent sur plusieurs mécanismes qui permettent d'assurer les services de confidentialité, d'authentification, … L'un des fondements de la sécurité informatique est le contrôle d'accès.

3.1. Définition

Le contrôle d'accès est une méthode de la sécurité utilisée pour déterminer l'autorisation des utilisateurs ou des programmes à voir ou à utiliser les ressources d'un environnement informatique. Le contrôle d'accès est le fait de prouver l'identité et te montrer ce que l'on sait tel qu'un mot de passe ou un code, le contrôle se fait par un gardien à la porte qui contrôle les entrées et les sorties.

Le contrôle d'accès est divisé en deux types :

- Physique : un dispositif qui permet un accès limité à des lieux (bâtiments, salles, …) et aux matériels informatiques.
- Logique : ce type restreint le nombre d'utilisateurs et les connexions aux réseaux informatiques, aux fichiers système et aux données.

3.2. Catégories principales de contrôle d'accès

Le contrôle d'accès est divisé en quatre catégories principales :

- **Contrôle d'accès obligatoire (MAC) :** Le contrôle d'accès obligatoire permet d'imposer une politique de sécurité centralisée, appliquée à tous les sujets et les objets d'un système. Contrairement au DAC, le MAC ne permet pas à chaque sujet de définir ses propres règles. C'est usuellement l'administrateur du système qui configure ou modifie la

politique de sécurité du système, ce qui doit par ailleurs être autorisé par cette même politique [31].

- **Contrôle d'accès discrétionnaire (DAC) :** Le contrôle d'accès discrétionnaire permet à un sujet d'appliquer sa propre politique de sécurité sur ses objets. C'est le contrôle d'accès classiquement utilisé dans les systèmes de type UNIX comme GNU/Linux. L'administrateur du système peut généralement outrepasser les accès des autres utilisateurs. Il n'est cependant pas responsable de la bonne configuration du contrôle mis en place par les autres utilisateurs [31].

- **Contrôle d'accès en fonction des rôles (RBAC) :** Le contrôle d'accès basé sur des rôles est un modèle de sécurité qui arbitre l'accès à des ressources via des structures abstraites appelées rôles. Un rôle permet d'associer un sujet à un ensemble de droits. Une décision d'accès est prise en fonction du rôle qu'un sujet joue. Un sujet peut être autorisé à changer de rôle parmi une liste de rôles permis. Le principe est que le sujet se place dans le rôle correspondant à la tâche qu'il souhaite effectuer, et bénéficie ainsi des droits appropriés. Cette approche simplifie particulièrement la gestion des accès pour un nombre important de sujets et d'objets [31].

- **Contrôle d'accès organisationnel (ORBAC) :** Les approches actuelles du contrôle d'accès reposent sur les trois entités (sujet, action, objet). Le contrôle d'accès organisationnel permet au concepteur de politique de définir une politique de sécurité indépendamment de la mise en œuvre. La méthode choisie pour atteindre cet objectif est l'introduction d'un niveau abstrait. Les sujets sont résumés en rôles, un rôle est un ensemble de sujets auxquels s'applique la même règle de sécurité. De même, une activité est un ensemble d'actions auxquelles la même règle de sécurité s'applique. Une vue est un ensemble d'objets auxquels la même règle de sécurité s'applique. ORBAC est sensible au contexte, de sorte que la stratégie peut être exprimée de manière dynamique. De plus, OrBAC possède des concepts de hiérarchie (organisation, rôle, activité, vue, contexte) et de séparation [32].

3.3. Identifiants de connexion

Les systèmes de contrôle d'accès gèrent l'identification des autorisations, l'authentification, l'approbation des accès et la responsabilité des entités grâce à des identifiants de connexion,

notamment des mots de passe, des codes PIN, des analyses biométriques et des clés physiques ou électroniques.

4. Système de sécurité légère pour IdO

4.1. L'infrastructure à clé publique

Une infrastructure à clé publique ICP (ou en anglais Public Key Infrastructure PKI) est un ensemble de technologies. Il s'agit de solutions techniques basées sur la cryptographie à clé public permettant de réaliser des échanges sécurisés. C'est une méthode qui permet de garantir la confidentialité, l'authentification, l'intégrité et la non-répudiation. Lors des échanges, elle assure la protection des données de toute modification et des identités. Elle garantie la gestion des certificats, la vérification des entités, … Elle a pour rôle aussi de générer les clés privée et publique et de les révoquer en cas de perte.

La PKI a pour rôle de délivrer les certificats numériques. Ces derniers permettent d'entreprendre des opérations cryptographiques asymétriques telles que le chiffrement et la signature numérique [33].

Un certificat numérique est une donnée publique qu'on retrouve dans le quotidien sous deux familles : le certificat de signature pour signer ou authentifier des documents et le certificat de chiffrement pour déchiffrer le contenu chiffré des messages [33].

Chiffrement asymétrique

Le chiffrement asymétrique tel que RSA utilise deux clés : la clé publique pour chiffrer les messages qui est partagée à plusieurs utilisateurs et la clé privée qui sert à déchiffrer les messages. La clé privée reste confidentielle. Ainsi les messages chiffrés avec une clé publique ne peuvent être déchiffrés que par la clé privée.

Signature

Une signature numérique est une valeur calculée à l'aide d'un algorithme cryptographique et liée aux données de telle sorte que les destinataires des données puissent utiliser la signature numérique pour vérifier que les données n'ont pas été altérées et/ou qu'elles proviennent du signataire du message, assurant ainsi l'intégrité et l'authentification du message [34].

Organisation d'une PKI :

Elle sert à vérifier l'identité, comme présenté sur la figure 13, elle est composée d'une :

- **Autorité de certification :** La CA est chargée de délivrer et gérer les certificats. En effet, elle génère des certificats à clés publiques et assure l'intégrité et l'authenticité des informations contenues en les signant avec sa clé privée. Pour émettre des certificats, elle doit recevoir, au préalable, les requêtes de certification contenant la clé publique de l'entité qui le sollicite [35].

- **Autorité d'enregistrement :** Elle joue le rôle d'intermédiaire entre l'utilisateur et la CA et dépend de cette dernière. Elle a comme responsabilité de vérifier tout ce qui concerne l'utilisateur, son identité, la concordance entre clés privées/publiques, de certifier et d'assurer qu'il possède les droits nécessaires pour demander des certificats. En résumé, cette autorité a pour tâche de gérer les requêtes de certificat qu'elle reçoit des différentes entités et de concevoir les paires de clés qui leur sont spécifiques [35].

- **Autorité de dépôt :** La publication est un service qui répertorie les différents certificats à clés publiques émis par la CA afin de les rendre disponibles aux éventuels futurs utilisateurs, c'est pourquoi on se réfère communément à lui par le terme de dépôt [35]. Donc elle permet de stocker les certificats numériques, de gérer l'état des certificats et de prendre en compte leur révocation.

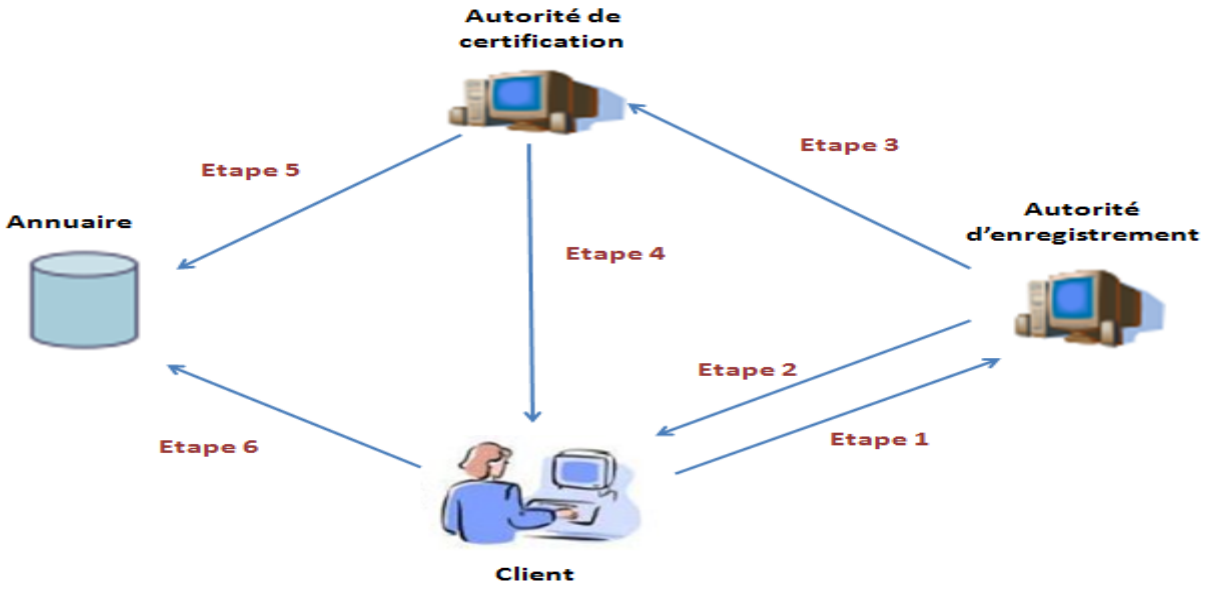

Figure 13 : Fonctionnement d'une PKI

Etape 1 : Identification de l'utilisateur, il fait une demande d'un certificat numérique.

Etape 2 : RA génère et envoie la clé privé au client.

Etape 3 : RA génère et envoie la clé publique au CA (transmet la demande de certificat à CA).

Etape 4 : L'envoi de certificat signé.

Etape 5 : Publication du certificat.

Etape 6 : Le client peut accéder aux certificats et à la liste de révocation.

4.2. Token

L'un des principes de sécurisation des données est le Token de sécurité (ou en français jeton), c'est une méthode pour la gestion des accès et des identités permettant de fournir une authentification pour une période de temps précise en assurant l'authentification mutuelle entre les parties communicantes. Ce Token est irréversible et généré aléatoirement. C'est un lien fort qui établit un lien de confiance entre les périphériques intelligents et les clients. Le Token a un niveau de sécurité très élevé, Il permet de limiter les risques et de protéger les données sensibles.

On peut distinguer plusieurs types de Token de sécurité : token X509 (certificat), token XML (Token personnalisés), Username Token (un nom d'utilisateur)… etc.

Le token se comporte souvent de la même manière en un processus de cycle de vie. Le processus comprend une étape d'enregistrement de l'identité de l'utilisateur, qui passe par un cycle qui commence par la production du token, sa distribution et son usage. Dans le cas où il y a un renouvellement d'identité il revient à l'étape de production [32]. Le cycle de vie de token se termine par sa suppression.

4.3. Authentification des utilisateurs légers basée sur les Tokens (TBLUA)

Les tokens ont été introduits en tant que solution efficace pour créer un lien fort entre les utilisateurs qui ont demandé la réservation et le périphérique intelligent. En même temps, l'authentification par token réduit le risque des facteurs d'authentification volés. Les tokens étant protégés contre abus, ils ne nécessitent pas beaucoup plus d'effort de l'utilisateur qu'un mécanisme basé sur un mot de passe. L'authentification utilisateur à périphérique est fondamentale. Cependant, la plupart des périphériques IdO sont soumis à des contraintes de ressources. Les dispositifs ont besoin de transmettre des données détectées périodiquement. Par

conséquent, il est nécessaire que les objets intelligents adoptent un protocole d'authentification léger pour réduire leur consommation d'énergie lorsqu'un dispositif vise à s'authentifier et à transmettre des données à son pair ciblé. De même, les appareils IdO communiquent via des canaux de communication non sécurisés et les utilisateurs illégaux (attaquants) peuvent casser la sécurité et également avoir accès au réseau dispositif intelligent. De plus, en compromettant une clé secrète, un attaquant peut déduire toute clé de session précédente qui représente une menace sérieuse [36]

L'authentification légère basée sur les Token a de nombreux avantages : d'une part, elle offre plus de sécurité puisqu'elle utilise la technique de token qui permet l'accès à une ressource précise pour une durée prédéfinie. D'autre part, ce protocole n'utilise que des opérations de calcul légère (fonctions de hachage et XOR) donc les coûts de calcul seront réduits et l'énergie sera économisée.

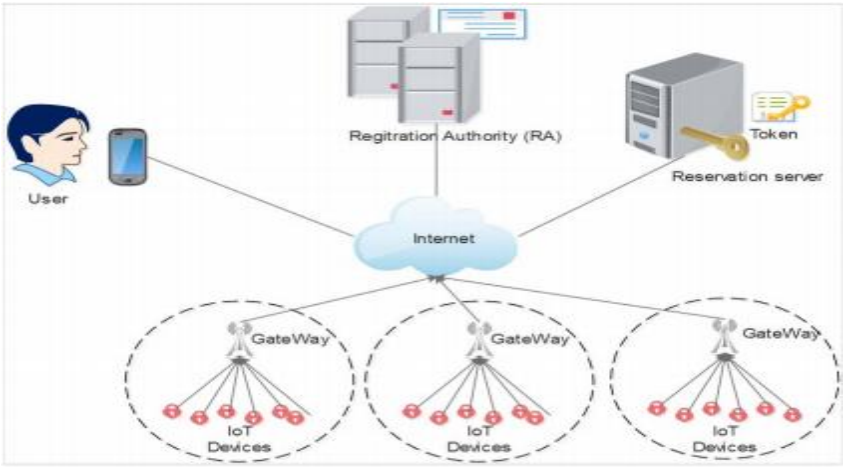

Figure 14 : Réseau TBLUA [35]

Pour avoir une transmission sécurisée, le protocole TBLUA comprend plusieurs étapes (la figure 14 présente le réseau TBLUA) : d'abord, l'enregistrement des appareils intelligents et des Gateway. Ensuite, la réservation des clients puis la distribution des Token. Enfin, la connexion et l'authentification.

5. Attaques dans les systèmes IoT

5.1. Classification des attaques

Les systèmes IoT sont vulnérables à différents attaques, ces dernières peuvent menacer les systèmes en visant la communication entre les équipements ou les équipements eux-mêmes. Le tableau suivant présente une classification des attaques selon les différentes couches IoT :

Couche physique	Couche réseau	Couche application
− DoS attack − Replay attack − Node jamming − Side channel attack − Social Engineering	− DoS attack − Man-in-the-middle attack − Sinkhole attack − Sybil attack − Spoofing attack − Traffic analysis − Eavesdropping	− Phishing attack − DoS attack − Software vulnerabilities

Tableau 3 : Classification des attaques selon les couches IdO

Dans ce qui suit, on donne la définition de plusieurs attaques qui s'avèrent intéressantes dans le cas qu'on va étudier par la suite.

5.1.1. Attaques au niveau Communication

- **Man in the middle :** l'attaquant de l'homme du milieu espionne de manière illégale la communication et la déforme parfois, violant la confidentialité en s'assurant que l'échange semble tout à fait normal. Cette attaque s'appuie sur les protocoles de communication

- **Advanced Persistent threats (APTs) :** Les APT, des opérations à long terme dont le but est de pouvoir infiltrer et exfiltrer un maximum de données utiles par l'utilisation de logiciels malveillants et sans se faire repérer.

- **Vol de session (Hijacking) :** un attaquant prétend d'être un des deux hôtes en s'intervenir entre eux pendant la communication.

- **Traffic analysis :** L'interception et l'examinassions des paquets du trafic réseau pour obtenir des informations et évaluer les volumes d'information même si les messages sont crypté.

- **Eavesdropping :** L'acte d'intercepter les communications entre deux points et de voler les informations. Cette attaque se fait quand le canal de communication est non sécurisé c'est-à-dire un manque de cryptage.

- **Data tampering :** L'acte de modifier, manipuler et détruire les données par des canaux non autorisés. Cela est dû au manque de hachage qui rend les paquets de données transmit sans protection.

- **Replay attack :** cette attaque se produit lorsqu'un pirate détecte une communication réseau sécurisée ou une transmission de données, l'intercepte, puis la transmet comme si c'était la leur.

5.1.2. Attaques au niveau Application mobile

- **Social engineering :** l'attaquant interagit avec le réseau IoT en manipulant les utilisateurs pour obtenir des informations privées.

- **Sniffing :** les attaquants peuvent intercepter et lire les informations des utilisateurs en utilisant des applications ou des matériels.

- **IP Spoofing :** Une entité qui prend l'identité d'une autre, une technique consistant à remplacer l'adresse IP de l'expéditeur IP par l'adresse IP d'une autre machine.

- **Impersonation attack :** Une attaque par usurpation d'identité est une attaque dans laquelle un adversaire réussit à assumer l'identité d'une des parties légitimes dans un système ou dans un protocole de communication [37].

- **Brute force :** c'est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles [38].

5.1.3. Attaques au niveau Serveur

- **Ransomware :** c'est un type de logiciel malveillant qui bloque l'accès à un système informatique ou à des données, généralement en les cryptant, jusqu'à ce que la victime paie une redevance à l'agresseur [39].

- **Data flooding :** l'attaquant injecte une quantité illimitée de paquets de données inutiles dans le réseau dans le but de le surchargés [40]

- **Denial of Service :** Un attaquant peut bombarder un réseau IoT avec plus de données de trafic qu'il peut gérer, ce qui peut entraîner une attaque par déni de service réussie [41].

5.2. Types d'attaques

Il existe plusieurs types d'attaques qui visent la sécurité des systèmes IoT. Ces menaces sont classées en deux types : passive et active

- **Attaque Passive :** L'attaquant se met en écoute non autorisée, en surveillant simplement la transmission ou la collecte d'informations**,** elle est difficile à détecter car elle n'implique aucune modification dans les données [42]. Cette attaque impacte la confidentialité de système.
- **Attaque Active :** l'attaquant tente de modifier l'information ou crée un faux message. La prévention de ces attaques est assez difficile en raison d'un large éventail de vulnérabilités physiques, de réseaux et de logiciels [42]. Cette attaque impacte l'intégrité et la disponibilité des systèmes.

6. Conclusion

Dans ce deuxième chapitre, nous avons défini la sécurité et la vie privée dans l'internet des objets. Nous avons également examiné le principe du contrôle d'accès. Ensuite, nous avons étudié d'autres techniques de sécurité ; le token et le protocole TBLUA.

Dans le chapitre suivant, nous allons introduire le cas qu'on va étudier « l'hôtel intelligent » et les exigences essentielles pour mettre en œuvre le système de sécurité légère ainsi que sa conception. Nous ferons ainsi une analyse des risques et des vulnérabilités spécifiques à notre système.

CHAPITRE III : Conception d’une solution de sécurité pour un hôtel intelligent

1. Introduction

Les systèmes IoT nécessitent plusieurs exigences de sécurité telles que l'authentification ou le contrôle d'accès qui donnent à une entité l'autorisation d'accéder aux ressources demandées, qu'elles soient physiques ou logiques. L'accès physique est défini par l'accès à un bâtiment, à une salle ou dans notre cas l'accès à une chambre d'hôtel.

Dans ce troisième chapitre, nous allons présenter les exigences nécessaires à respecter et nous expliquerons la manière dont notre système de sécurité légère est mis en œuvre dans le domaine de l'IoT et plus particulièrement pour le cas d'usage étudié qui est l'hôtel intelligent (smart hotel en anglais).

Ce chapitre est divisé en trois grandes parties :

- Dans la première partie, nous présenterons le cas d'étude de notre système IoT qui est l'hôtel intelligent.

- Dans la deuxième partie, nous présenterons l'architecture fonctionnelle de notre système en décrivant les entités composant ce système et comment chaque entité collabore avec les autres.

- Dans la troisième partie, nous présenterons le tableau de l'analyse des risques et des vulnérabilités de notre système.

2. Présentation du cas d'usage d'hôtel intelligent

2.1. Présentation générale

Le but de l'étude est de réaliser un schéma de sécurité légère en mettant en place une architecture fiable. Nous avons donc conçu un système de contrôle d'accès qui se base sur le concept des clés numériques (Token ou même jeton) qui permettent d'offrir l'accès ou de le supprimer à un utilisateur.

Notre étude porte sur le cas d'usage d'hôtel intelligent où le client peut faire une réservation en utilisant une application Android et il aura l'accès à la porte intelligente de l'hôtel en toute

sécurité. Ce travail rentre dans le cadre d'un projet Européen plus large qui est le projet ITEA PARFAIT [43].

Figure 15 : Système PARFAIT Pi-Bank [43]

Dans notre système, on utilise un distributeur de token Pi-Bank (figure 15). Le Token d'identification est envoyé par le système de réservation à la Pi-Bank. Ensuite, la porte intelligente demande le token à la Pi-Bank qui par la suite envoie ce dernier à la porte intelligente et au client. Enfin, on rapproche le Smartphone à la porte, via une communication NFC par exemple, qui va vérifier le token d'identification et annonce à la Pi-Bank son utilisation.

2.2. Les défis

L'un des principaux défis des systèmes IoT est d'avoir une équivalence entre la sécurité et l'efficacité des systèmes.

Pour harmoniser ces deux aspects présentés sur la figure 16, il est nécessaire de mettre en place des exigences différentes. Au niveau de sécurité, les mesures de sécurité telles que le contrôle d'accès ou l'utilisation d'un token sont destinées à assurer la confidentialité du système et à le rendre résistant à plusieurs attaques. Au niveau de l'efficacité du système, il est important d'avoir une authentification légère, un calcul et une communication minimums.

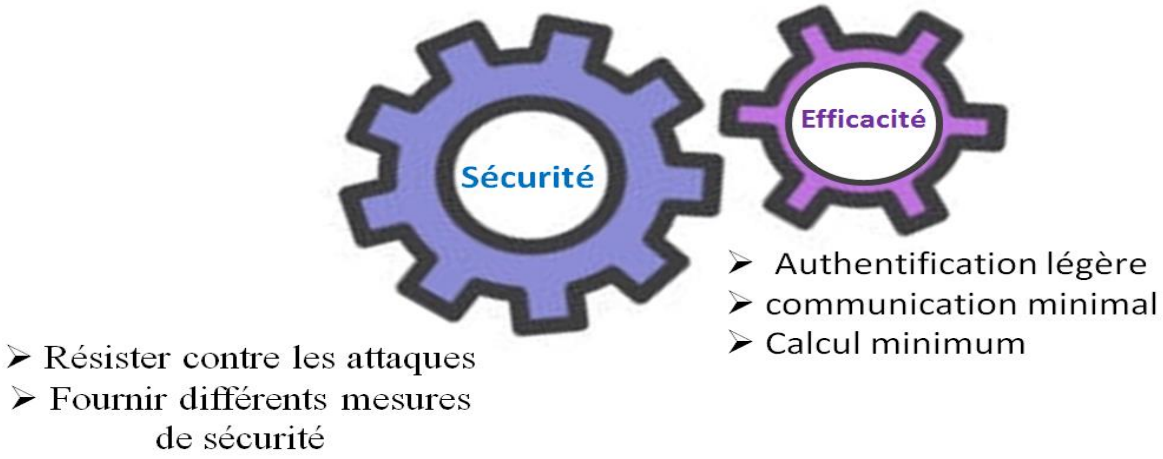

Figure 16 : Challenge entre la sécurité et l'efficacité

3. Architecture et Conception du système

3.1. Architecture générale

Notre système représente un hôtel intelligent (figure 17), il est composé de :

- L'objet connecté serrure intelligente
- L'objet connecté Smartphone
- Serveur qui établit le lien entre ces objets.

Les utilisateurs de ce système sont des clients qui cherchent à faire une réservation à l'hôtel et avec un accès facile en utilisant leurs Smartphones. Ils pourront également contrôler d'autres fonctionnalités de la chambre d'hôtel (Température, lumière, …).

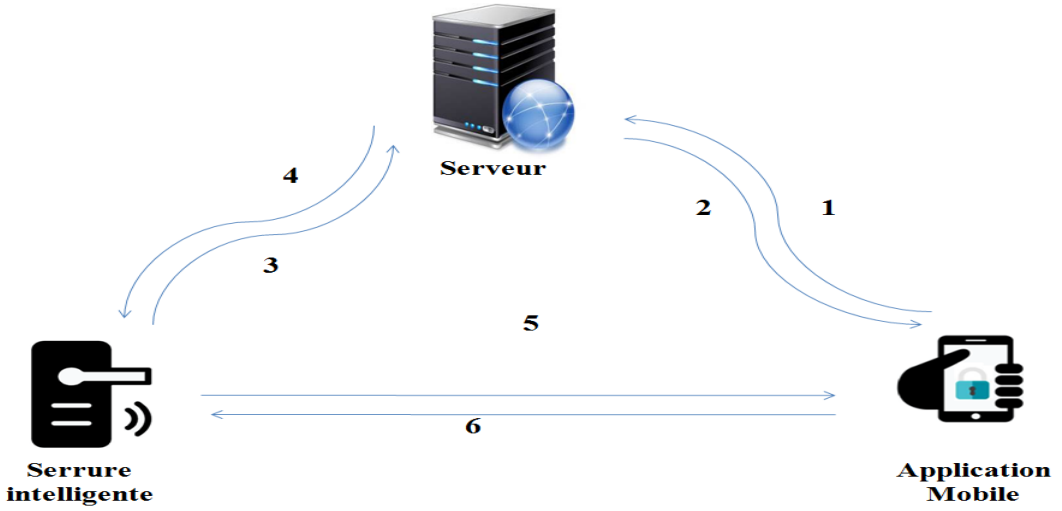

Figure 17 : Architecture de notre système

1 → Le client s'enregistre et demande une réservation

2 → Le serveur génère un token et l'envoie au client

3 → Le serveur envoie la liste d'accès à la serrure

4 → La serrure envoie le log

5 → Le client demande l'accès à la serrure

6 → La serrure envoie l'autorisation au client

3.2. Critères et analyse de système

Notre système cherche à assurer plusieurs exigences : la sécurité et l'efficacité du système sont le point les plus essentielles. Pour cela, nous devons garantir l'authentification des utilisateurs, le transfert sécurisé des données entre les entités de système, le contrôle des objets connectés, …

Pour réaliser notre système, nous avons eu besoin de plusieurs dispositifs physiques et des différents logiciels que nous listons ci-après :

Matériels requis

- Smartphone : pour la partie réservation et accès à la chambre d'hôtel
- Réseaux wifi : pour avoir une relation entre l'application mobile et le serveur.
- Serveur machine (Windows) : pour convertir les données de internet à ZigBee.
- Connectivité Xbee : pour avoir une connexion entre le serveur et la porte.
- Carte Arduino Mega : pour le développement de programme d'hôtel intelligent.
- Deux LED : pour montrer l'accès autorisé/refusé à la porte.
- Petite porte en bois : pour être commandé par le Smartphone.
- Capteur NFC : pour lire les tentatives d'accès à la porte.
- Batteries : pour alimenter l'Arduino et la gâche électrique.
- Fils de connexion : pour relier les différents composants électriques.
- Gâche électrique : pour le verrouillage et le déverrouillage de la porte à distance.

3.3. Les entités composant notre système

Le serveur dans notre cas joue le rôle de passerelle entre la serrure intelligente et l'utilisateur. La figure suivante montre un système plus détaillé où on indique comment chaque entité est reliée à l'autre. Le serveur est fusionné au routeur, il communique avec la porte en utilisant la

communication à faible consommation (ZigBee) et avec l'utilisateur en utilisant un réseau internet.

D'une manière générale, l'utilisateur aura accès aux données par son téléphone intelligent alors que l'administrateur contrôlera ces données via le serveur.

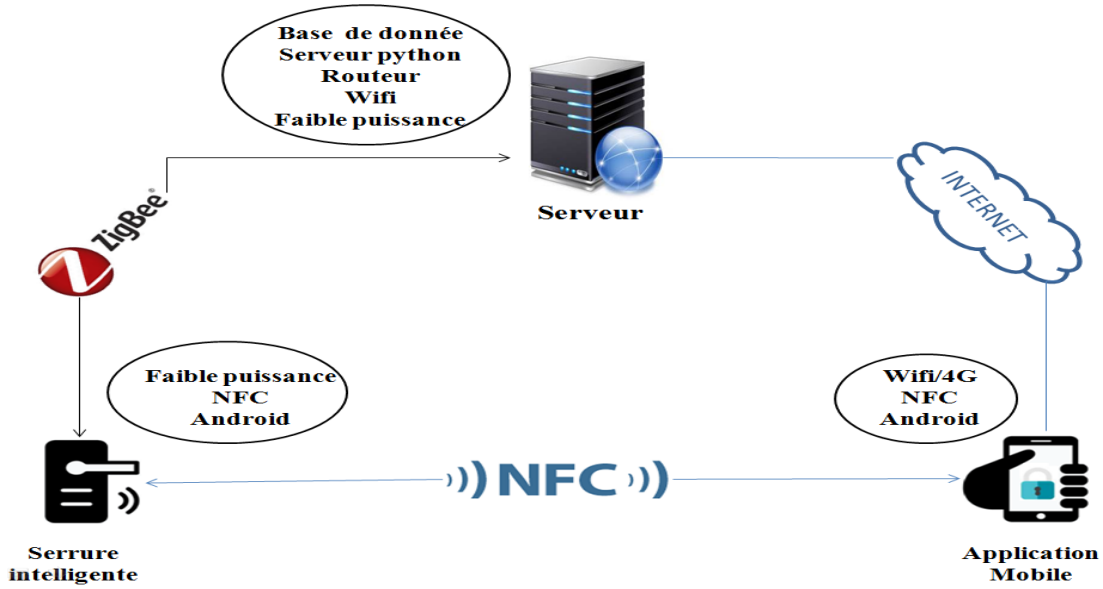

Figure 18 : Conception de système détaillé

3.3.1. Serveur

Notre serveur joue un rôle différent avec les deux autres parties du système (Serrure et Smartphone). Il communique avec l'utilisateur via un réseau internet pour l'interception des demandes et avec la serrure intelligente via un protocole ZigBee.

Le serveur a besoin de deux ports, un pour la réception des données et l'autre pour l'envoi des données.

Code d'accès = hash md5 (la clé + le PIN).

- **<u>Communication avec l'utilisateur :</u>**

  ➔ Le serveur se met en communication avec l'utilisateur avec un réseau internet.

  ➔ Il intercepte les requêtes envoyées par l'utilisateur.

  ➔ Il analyse et traite les données reçues c'est-à-dire les informations de la réservation.

➔ Il génère le token aléatoirement.

➔ Il stocke les informations dans une base de données.

➔ Il envoie la validation à l'utilisateur.

➔ Les données à ce niveau sont cryptées et décryptées à chaque transmission avec un algorithme AES.

- **Communication avec la serrure intelligente :**

➔ Le serveur se met en communication avec la serrure intelligente via un protocole ZigBee.

➔ Il intercepte les données envoyées par la serrure intelligente.

➔ Il analyse les données c'est-à-dire les tentatives d'accès sur la serrure.

➔ Il stocke les informations dans une base de données

➔ Enfin, il envoie le token.

3.3.2. Application mobile

L'application mobile de l'utilisateur lui permet de faire les deux fonctions principales de système en choisissant un des deux boutons présentés sur la première partie de la figure. L'utilisateur pourra faire :

- La réservation de la chambre en choisissant une date précise (date de début et date de fin) et un numéro de chambre.
- L'accès à la chambre en entrant le code PIN.

Figure 19 : Schéma de l'application mobile

3.3.3. Porte

La porte comporte une serrure intelligente qui est un matériel électronique qui fait partie de l'IoT. Elle permet aux utilisateurs d'accéder à leur maison ou dans notre cas à la chambre d'hôtel intelligent sans avoir besoin des clés mais en utilisant leurs téléphones intelligents. La figure suivante montre le schéma représentatif de la porte et la zone qui comporte le système de matériel électronique (capteur NFC… etc.).

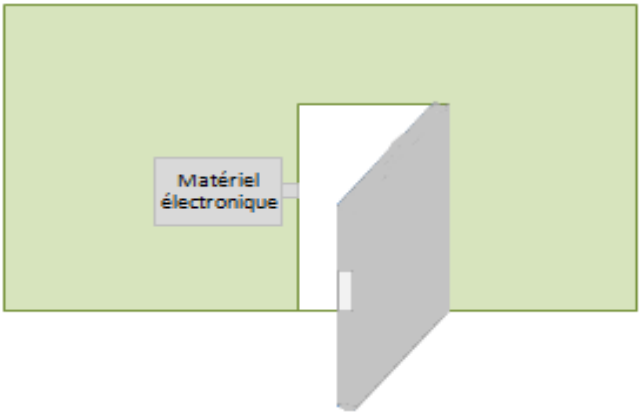

Figure 20 : Schéma représentatif de la porte

Matériels électroniques de la porte :

Figure 21 : Arduino Mega 2560 rev3 [32]

Figure 22 : PN532 NFC reader [32]

Figure 23 : XBee S2 [32]

Figure 24 : XBee to USB adapter [32]

Figure 25 : CYTRON XBee Shield for Arduino [32]

Figure 26 : Motor Shield Relay MD10 [32]

Figure 27 : Gâche électrique [32]

Figure 28 : Support à pile [32]

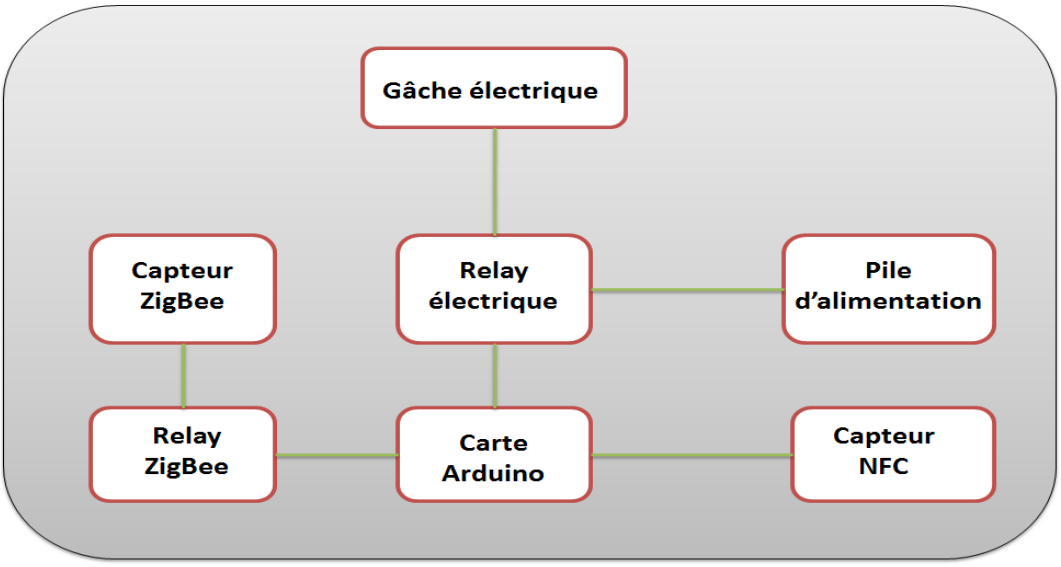

Figure 29 : Schéma électronique de la porte

La figure ci-dessus nous présente la relation entre les composants électroniques de la porte. La carte Arduino est reliée au :

- capteur NFC
- capteur ZigBee grâce au relay ZigBee
- relay électrique qui permet l'alimentation de la gâche électrique et de la carte Arduino aussi

3.4. Diagramme de cas d'utilisation

Un diagramme de Cas d'Utilisation montre l'interaction entre le système et les entités externes au système. Ces entités externes sont désignées comme acteurs. Les acteurs représentent des rôles qui peuvent inclure des utilisateurs humains, du matériel externe ou d'autres systèmes [44].

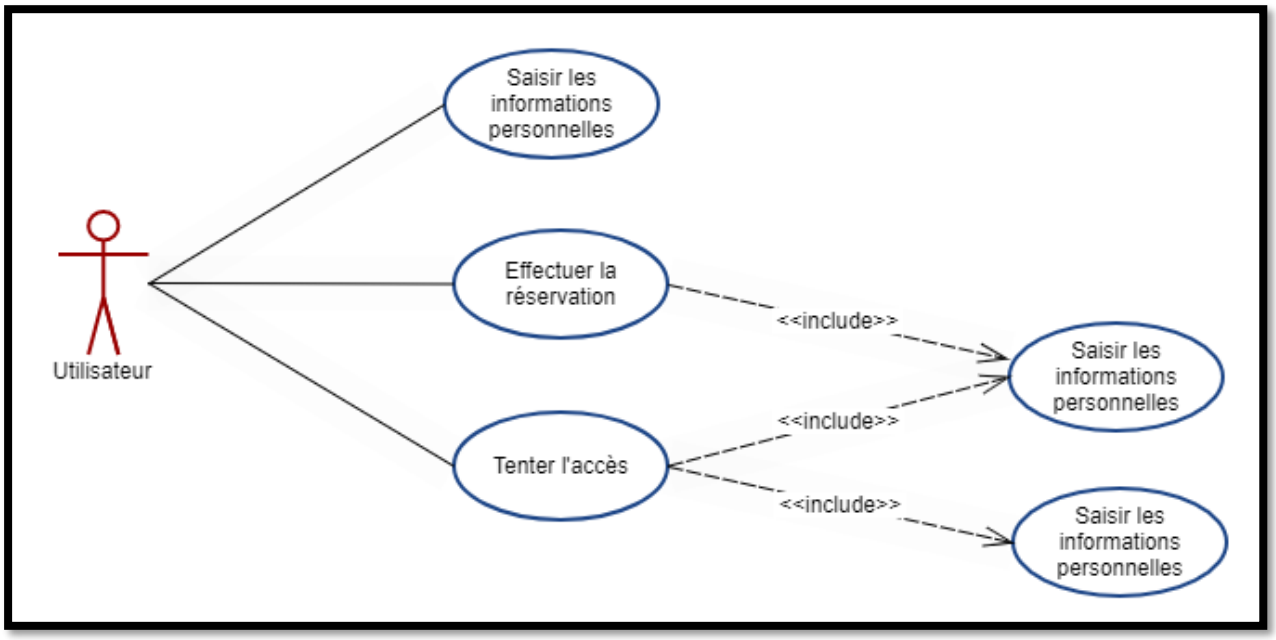

Figure 30 : Diagramme de cas d'utilisation.

Notre système (représenté par un diagramme de cas d'utilisation sur la figure 30) donne la possibilité à des clients de réserver des chambres d'hôtel avec une date précise, lors de la réservation, le client reçoit un token qui lui permet d'accéder à la chambre en utilisant son téléphone intelligent à travers la serrure intelligente. Cette action se fait en rapprochant le Smartphone équipé d'un NFC à la porte intelligente équipée aussi d'un capteur NFC. Le lecteur compare la clé numérique et le PIN de téléphone mobile avec la clé numérique et le PIN de la porte.

3.5. Diagramme de classes

Le diagramme de classes montre les blocs de construction de tout système orienté-objet. Les diagrammes de classes représentent une vue statique du modèle ou une partie du modèle, en décrivant les attributs et les comportements qu'il a [45].

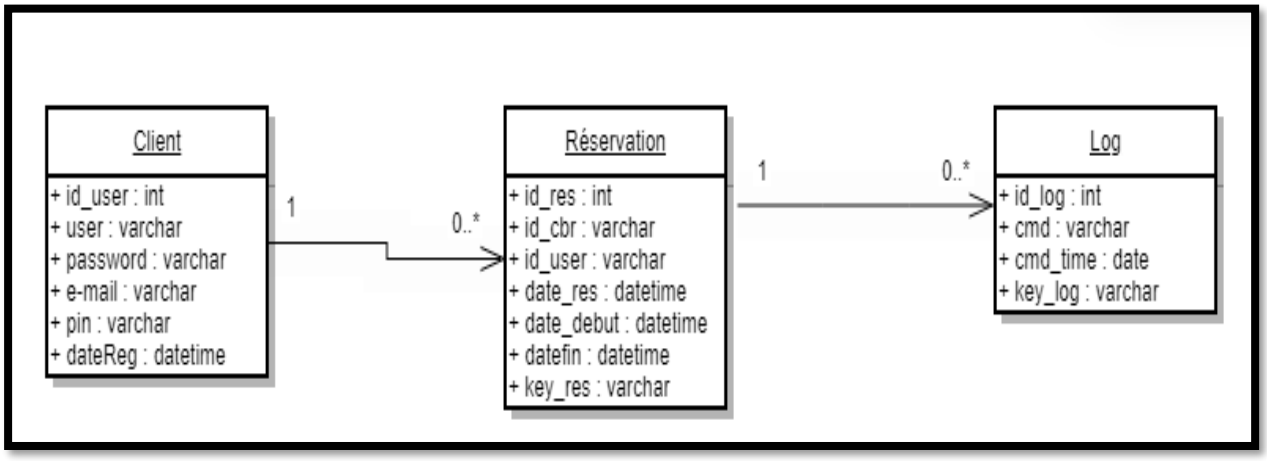

Figure 31 : Diagramme de classes.

La figure 31 représente le diagramme de classe de notre système - hôtel intelligent -, elle est composée de trois tables :

- La table client pour représenter les clients enregistrés c'est-à-dire qui veulent faire des réservations dans l'hôtel intelligent.
- La table réservation pour représenter les réservations des clients
- La table log pour représenter les tentatives d'accès

3.6. Diagramme d'activité

Un diagramme d'activité fournit une vue du comportement d'un système en décrivant la séquence d'actions d'un processus. Les diagrammes d'activité sont similaires aux organigrammes de traitement de l'information, car ils montrent les flux entre les actions dans une activité [46].

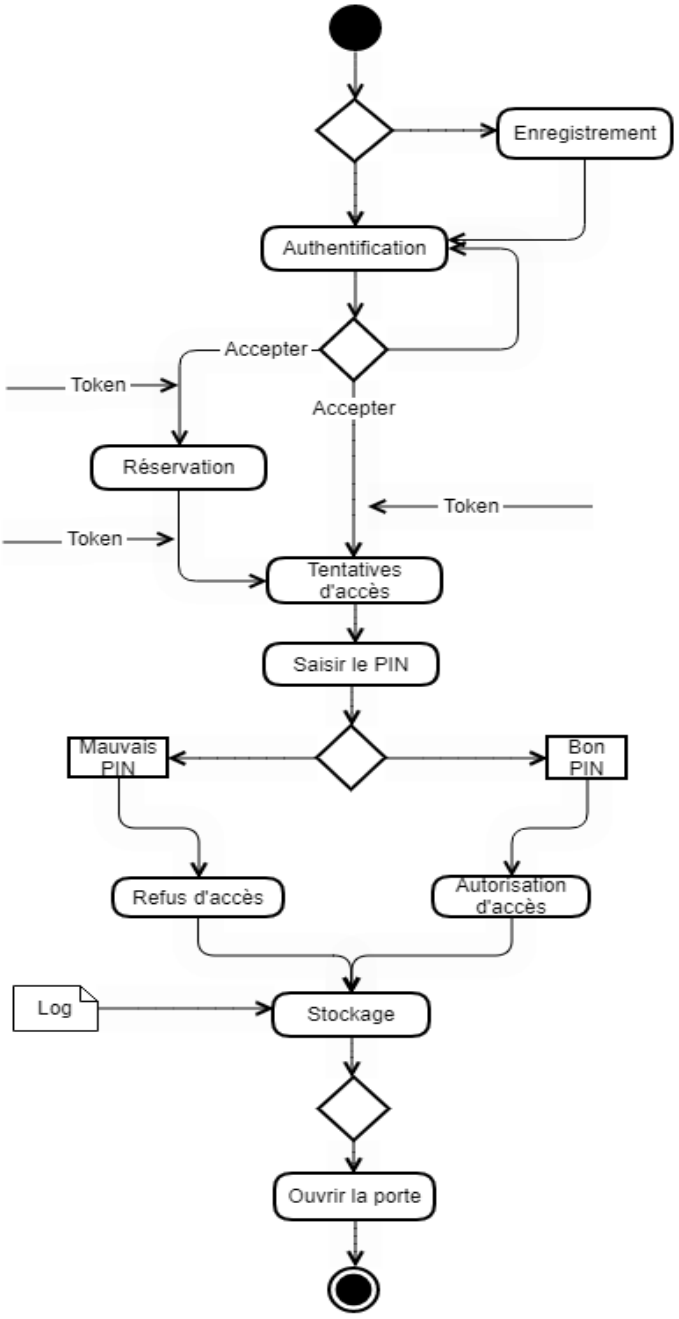

Figure 32 : Diagramme d'activité

Le diagramme d'activité (figure 32) montre les étapes pour avoir accès à la chambre d'hôtel intelligent. L'utilisateur doit s'enregistrer et s'authentifier auprès du serveur pour pouvoir faire la réservation avec une date précise. Après avoir reçu le Token, l'utilisateur pourra donc tenter l'accès à la porte en entrant le code PIN. Si le token et le PIN sont justes, l'accès est autorisé, sinon l'accès est refusé. Dans les deux cas, les informations d'accès seront stockées dans la table log de serveur. L'utilisateur pourra donc ouvrir la porte.

3.7. Diagramme de séquence

Le diagramme de séquence fait partie des diagrammes comportementaux (dynamiques) et plus précisément des diagrammes d'interactions. Il permet de représenter des échanges entre les différents objets et acteurs du système en fonction du temps [47].

Dans ce qui suit, nous allons présenter un diagramme de séquence générale de notre cas d'hôtel intelligent ainsi que des diagrammes de séquence pour expliquer les échanges entre les entités du système (Serveur-Application mobile-Porte).

3.7.1. Séquence générale

Il faut commencer par la mise en place de serveur qui est en communication avec le client et avec la serrure intelligente (La figure 33 représente le diagramme de séquence générale du système).

- Le client envoie ses informations au serveur (enregistrement) et fait la réservation avec une date précise.
- Le serveur enregistre la demande du client puis il génère un token.
- Le serveur envoie le token à la serrure intelligente et au client.
- Le client demande l'accès.

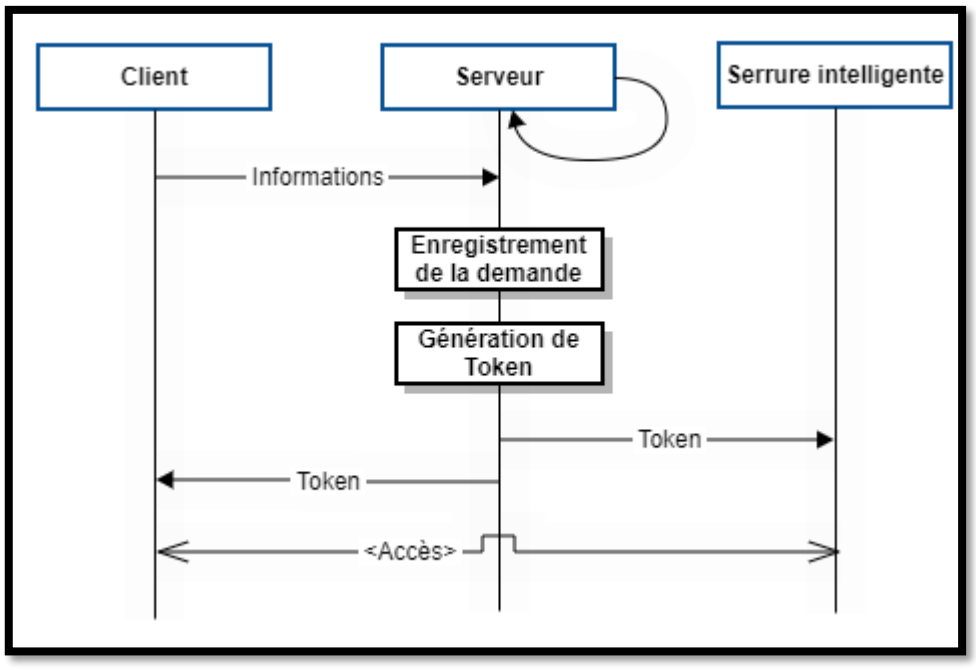

Figure 33 : Diagramme de séquence générale

3.7.2. Serveur-application mobile

Il faut commencer par l'enregistrement et l'installation de l'application mobile (la figure 34) représente le diagramme de séquence serveur-application mobile).

- Le client fait une demande d'enregistrement auprès du serveur.
- Le serveur envoie sa validation au client.
- Le serveur envoie le PIN à l'utilisateur.
- Le client peut maintenant faire une réservation à la chambre avec une date précise.
- Le serveur génère et envoie de la clé d'accès au client.

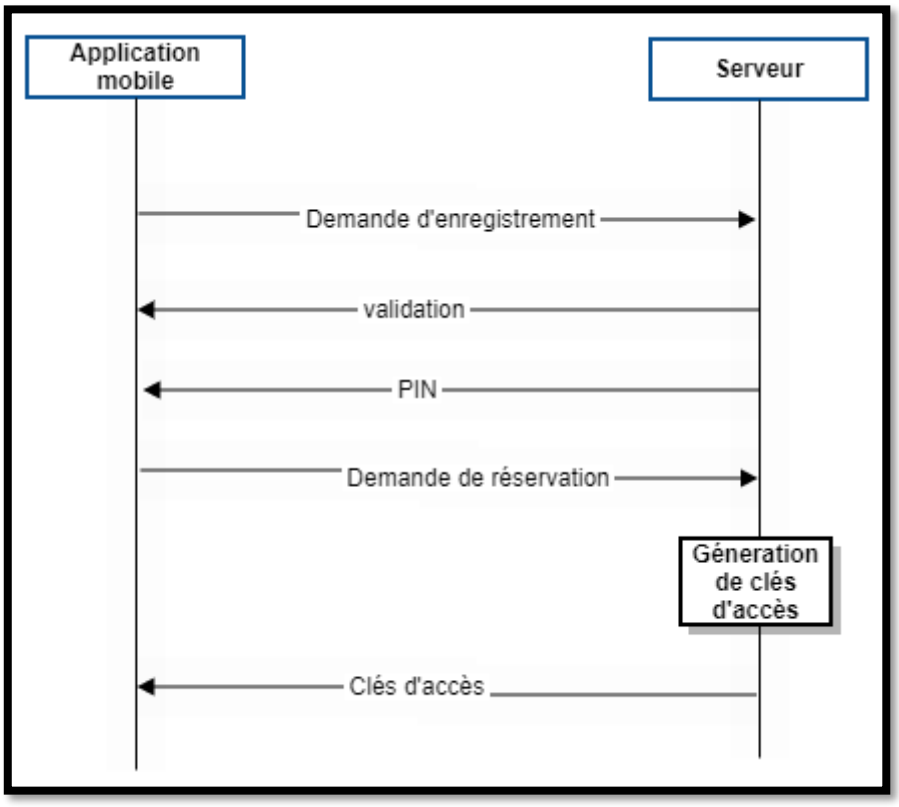

Figure 34 : Diagramme de séquence Serveur-Application mobile

3.7.3. Porte-serveur

Il faut commencer par l'installation de la porte intelligente et l'initialisation de l'objet. Pour permettre une communication entre le serveur et la porte, il faut mettre un protocole ZigBee. Les étapes suivantes vont être échangées après la réservation du client (la figure 35 représente le diagramme de séquence porte-serveur)

- La porte envoie un ID au serveur.
- Le serveur génère un nombre aléatoire, puis il l'envoie à la porte.
- La porte envoie le nombre aléatoire haché au serveur
- Le serveur compare le nombre haché reçu avec le nombre qui l'a haché lui-même.
- Si les nombres sont authentiques, le serveur envoie le code d'accès à la porte intelligente via un canal sécurisé.

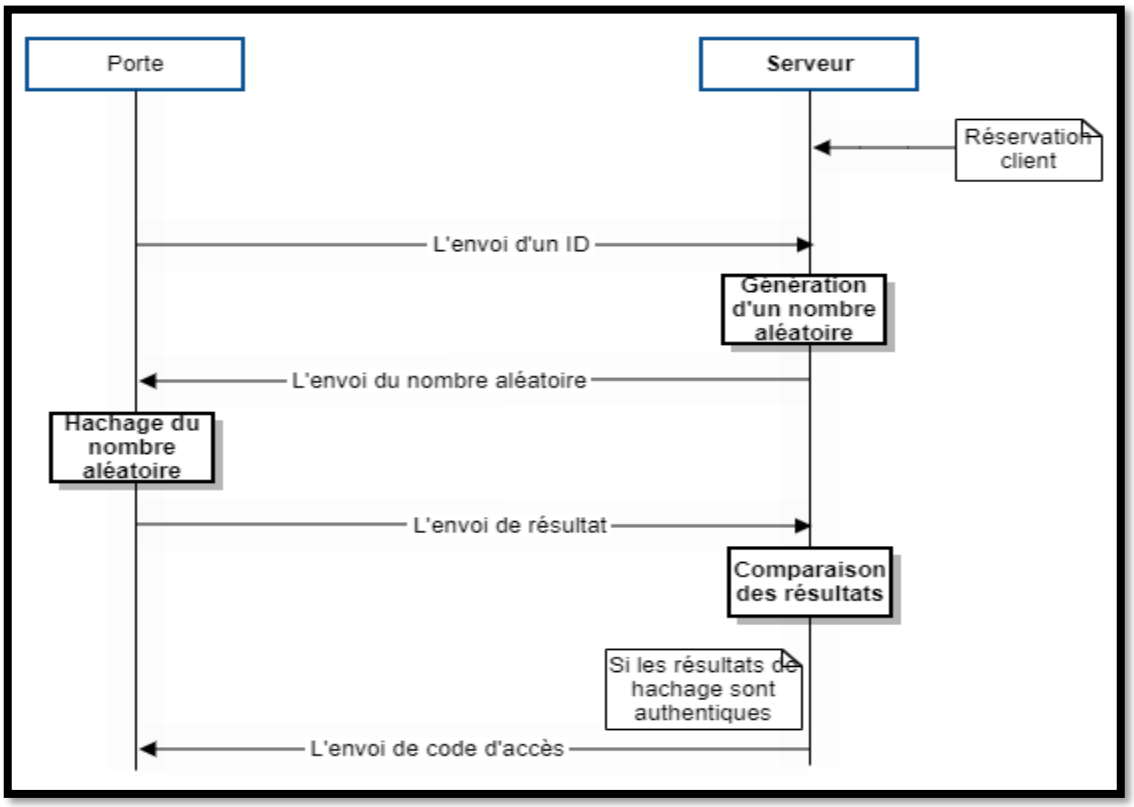

Figure 35 : Diagramme de séquence porte-serveur

3.7.4. Porte-application mobile

La dernière étape est entre le client et la serrure intelligente présenté par un diagramme de séquence sur la figure 36.

- L'utilisateur commence par s'identifier sur son téléphone.
- Il place son Smartphone à proximité du lecteur NFC donc il demande l'accès
- La porte demande le PIN.
- La porte compare son code d'accès avec celui de l'utilisateur :
  - ➔ Accès autorisé si le PIN est juste.
  - ➔ Accès refusé si le PIN est faux.

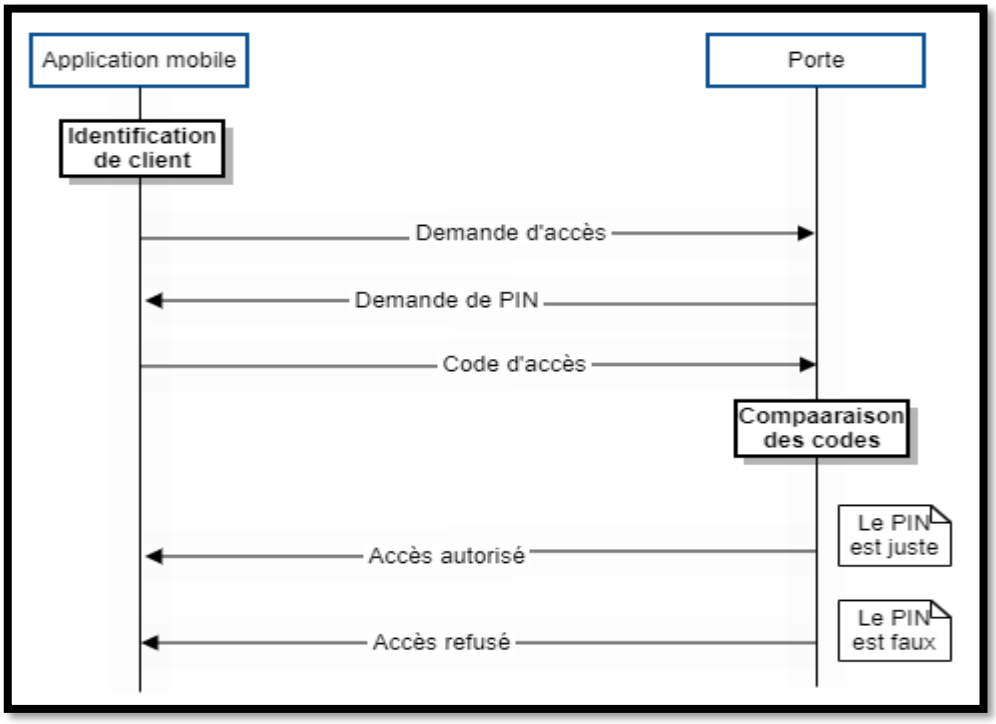

Figure 36 : Diagramme de séquence Porte- Application mobile

3.8.Application web

L'application web est conçue pour l'administrateur de l'hôtel où il aura accès aux données c'est-à-dire il pourra gérer les réservations et toutes les informations concernant son hôtel.

La figure suivante montre l'interface principale de l'application web.

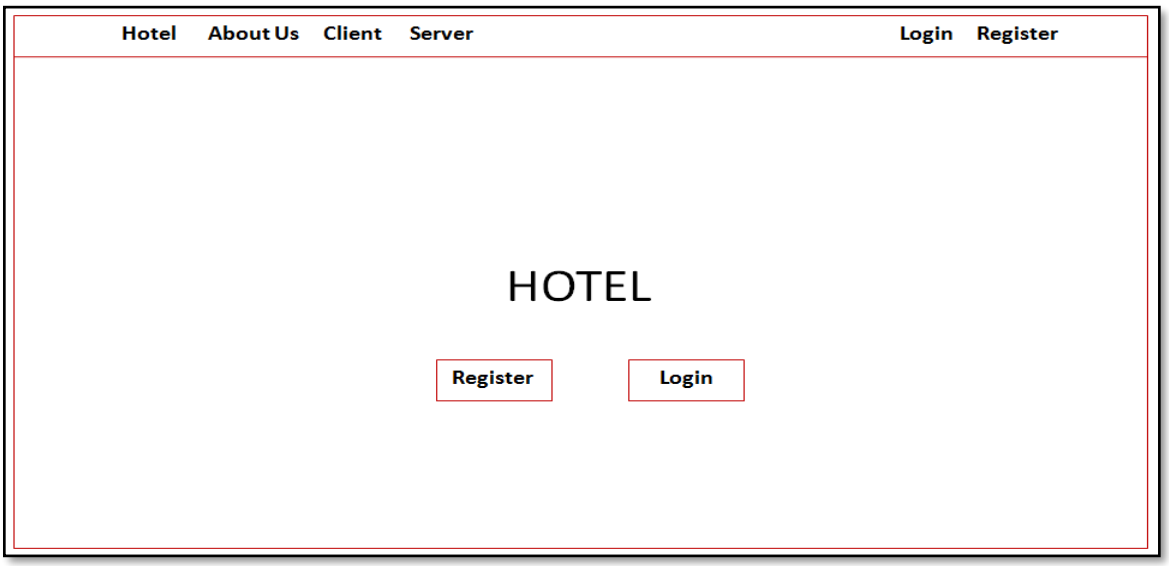

Figure 37 : Schéma principal de l'application web

La figure suivante se divise en deux parties : (a) pour s'inscrire et (b) pour s'identifier ainsi que la réinitialisation en cas de mot de passe oublié.

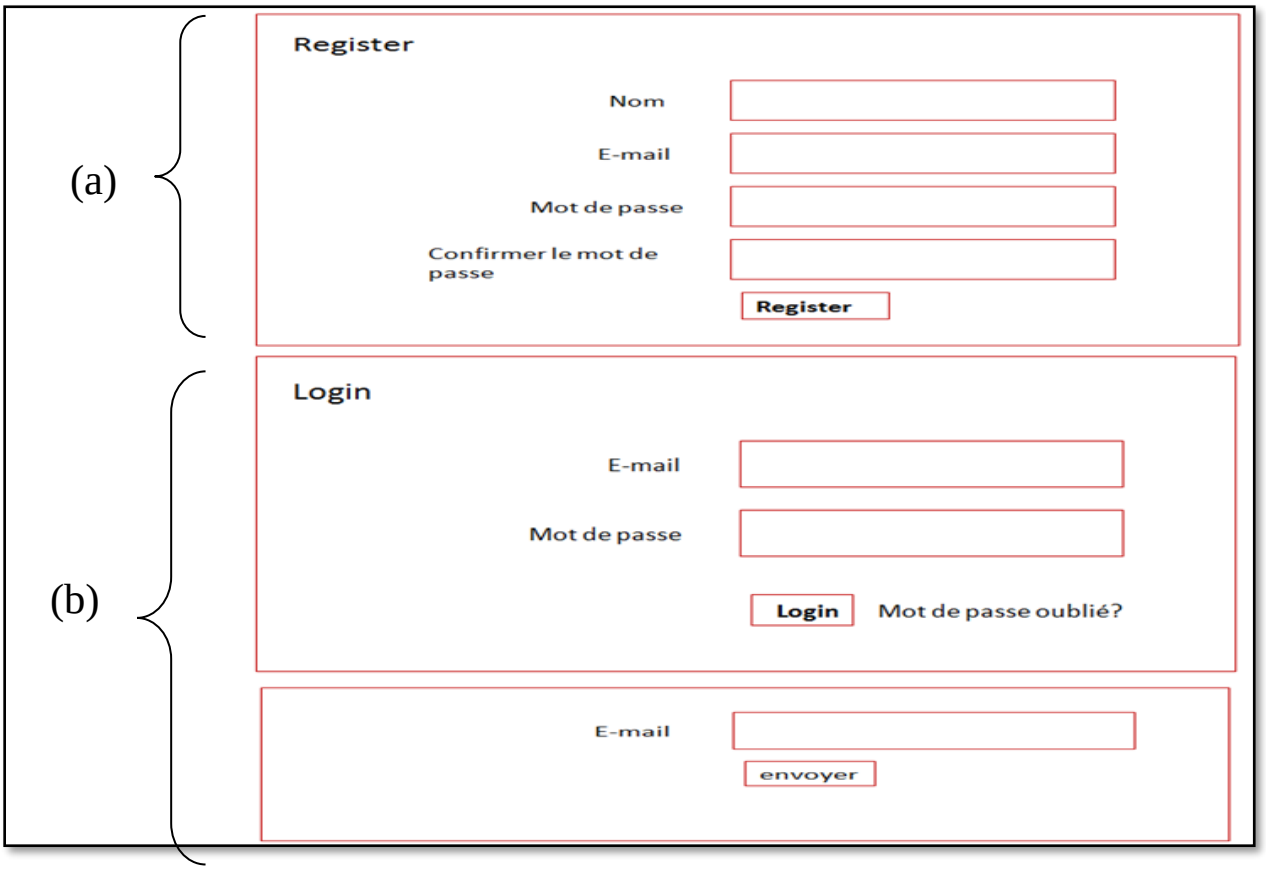

Figure 38 : Schéma Register et Login de l'application web.

4. Analyse des risques et des vulnérabilités

Le tableau suivant présente une classification des différentes attaques qui menacent notre système selon leur cible (les entités de système et la communication entre elles). Nous avons précisé les types d'attaques ainsi que leur impact sur notre système.

	Attaques	Type	Impact
Communication	Man in the middle	Active	-Vol de données et d'identité. -Perte de clients → Perte financière
	APTs	Passive	-Informations sensibles compromises (menace de la vie privée)

	Vol de session	Active	-Faire tomber le système -Injection de nouvelles failles de sécurité dans le système
	Traffic analysis	Passive	-Divulgation de l'identité des parties communicantes et le contenu de la communication
	Eavesdropping	Passive	-Perte de confidentialité des données
	Data tampering	Active	-Faille de sécurité
	Replay attack	Active	-Violation de l'intégrité du système
Application mobile	Social engineering	Passive	-Propagation des malwars(-Ransomware -Cheval de troie -Botnets) -Vol de données
	Sniffing	Passive	-Vol des informations privées -Chantage -L'obtention des noms d'utilisateur et des mots de passe -Espionnage des e-mails et des messages de chat. -Vol d'identité
	IP Spoofing	Active	-Perte d'information privée
	Impersonation attack	Active	-Divulgation d'information sensible.
Serveur	Ransomware	Active	-Perte temporaire ou permanente d'informations sensibles ou exclusives. -Pertes financières encourues pour restaurer les systèmes et les fichiers, et atteinte potentielle à la réputation de l'organisation

	Data flooding	Active	-Ressources mémoire épuisées
	DoS	Active	-Indisponibilité des services -Empêchement des utilisateurs légitimes d'utiliser un service
Porte	Brute force	Active	-Accès à des informations sensibles -Craquage des mots de passe

Tableau 4 : Analyse des risques et des vulnérabilités

5. Conclusion

Ce troisième chapitre est dédié à la présentation de notre système IoT « hôtel intelligent » où nous avons cité les besoins matériels pour l'implémentation. Nous avons aussi présenté les entités principales qui composent le système et la méthode de communication entre elles. Il est à noter que la classification des risques et des vulnérabilités était analysée dans ce chapitre.

Après avoir étudié la partie théorique de notre système, le dernier chapitre sera consacré à son implémentation.

CHAPITRE IV : Développement et mise en œuvre

1. Introduction

Après avoir décrit le système d'hôtel intelligent, ses exigences et ses principales entités dans le chapitre précédent, nous allons dans ce dernier chapitre donner les détails de son implémentation. Nous commencerons par une présentation des outils et plates formes utilisées. Nous mettrons ensuite en œuvre les différentes entités de système. Enfin, nous présenterons les tests et les résultats ainsi qu'une étude de différentes attaques qui menacent notre système.

2. Outils utilisés

Pour réaliser ce projet, nous aurons besoin de certains outils de développement et des langages de programmation

Python : Python est un langage de programmation interprété, orienté objet, de haut niveau et doté d'une sémantique dynamique. Ses structures de données intégrées de haut niveau, combinées à un typage dynamique et à une liaison dynamique, le rendent très attrayant pour le développement rapide d'applications, ainsi que pour une utilisation en tant que langage de script ou de colle pour relier des composants existants entre eux. La syntaxe de Python, simple et facile à apprendre, met l'accent sur la lisibilité et réduit donc le coût de la maintenance du programme. Python prend en charge les modules et les paquets, ce qui encourage la modularité des programmes et la réutilisation du code [48].

Arduino : Le langage Arduino est simplement un ensemble de fonctions C/C++ qui peuvent être appelées à partir du code. L'esquisse subit des modifications mineures (par exemple, la génération automatique de prototypes de fonctions) et est ensuite directement transmise à un compilateur C/C++ [49].

Android studio : Android Studio est l'environnement de développement intégré pour la plateforme Android de Google. Les versions d'Android Studio sont compatibles avec certains systèmes d'exploitation Apple, Windows et Linux. Grâce à la prise en charge de la plateforme Google Cloud et de l'intégration des applications Google, Android Studio offre aux développeurs une boîte à outils bien fournie pour la création d'applications Android ou d'autres projets, et fait partie intégrante du développement Android depuis 2013 [50].

Xampp : XAMPP est un ensemble de logiciels permettant de mettre en place facilement un serveur Web et un serveur FTP. Il s'agit d'une distribution de logiciels libres (X Apache MySQL Perl PHP) offrant une bonne souplesse d'utilisation, réputée pour son installation simple et

rapide. Ainsi, il est à la portée d'un grand nombre de personnes puisqu'il ne requiert pas de connaissances particulières et fonctionne, de plus, sur les systèmes d'exploitation les plus répandus [51].

SQLite : SQLite est un système de base de données ou une bibliothèque proposant un moteur de base de données relationnelles. Il repose sur une écriture en C, un langage de programmation impératif, et sur une accessibilité via le langage SQL (Structured Query Language). SQLite présente la particularité d'être directement intégré aux programmes et dans l'application utilisant sa bibliothèque logicielle alors que ses concurrents comme MySQL reproduisent de leur côté le schéma classique client-serveur. Avec SQLite, la base de données est intégralement stockée dans un fichier indépendant du logiciel [52].

Arduino IDE : Les créateurs de Arduino ont développé un logiciel pour que la programmation des cartes arduino soit visuelle, simple et complète à la fois. C'est ce que l'on appelle une IDE, qui signifie Integrated Development Environment ou Environnement de Développement « Intégré » en français (donc EDI). L'IDE Arduino est le logiciel qui permet de programmer les cartes Arduino. L'IDE affiche une fenêtre graphique qui contient un éditeur de texte et tous les outils nécessaires à l'activité de programmation. Vous pouvez donc saisir votre programme, l'enregistrer, le compiler, le vérifier, le transférer sur une carte arduino… [53].

PHP : Le PHP, pour Hypertext Preprocessor, désigne un langage informatique, ou un langage de script, utilisé principalement pour la conception de sites web dynamiques. Il s'agit d'un langage de programmation sous licence libre qui peut donc être utilisé par n'importe qui de façon totalement gratuite [54].

Laravel : Laravel est un framework PHP qui propose des outils pour construire une application web. Le créateur de Laravel, Taylor Otwel, a simplement regroupé les meilleures librairies pour chaque fonctionnalité nécessaire pour la création d'un site web [55].

3. Mis en ouvre

3.1.Porte

La carte arduino va être responsable de plusieurs tâches, d'une part avec la technologie ZigBee et d'autre part avec la technologie NFC.

Pour permettre la connexion entre la porte intelligente et le serveur, nous aurons besoin d'une connexion ZigBee. La figure suivante montre le montage du capteur ZigBee sur la carte Arduino.

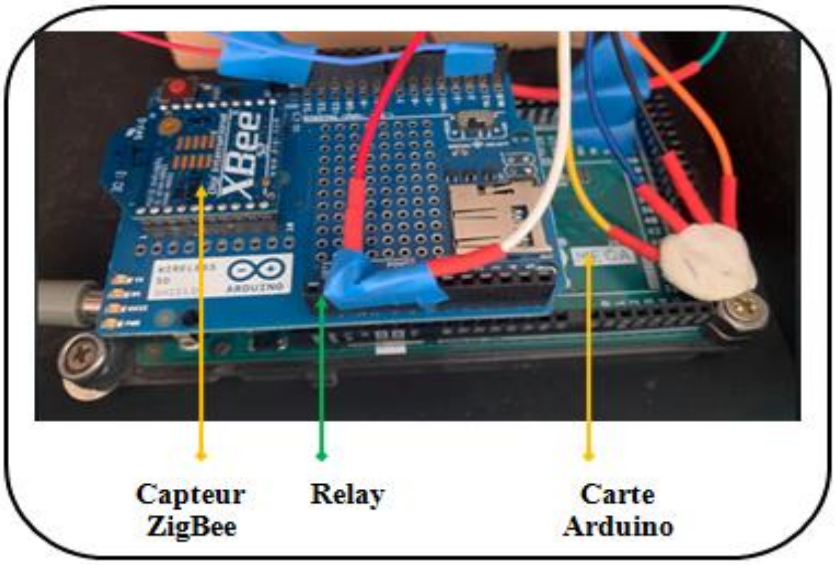

Figure 39 : Montage du capteur ZigBee avec Arduino

Ce capteur ZigBee est responsable de l'interception, la fragmentation et l'analyse des données. Pour cela, nous utilisons différentes fonctions, chacune a un rôle précis. La fonction de traitement de données permet aussi d'exécuter les commandes reçues (ajouter pour le stockage des données, afficher, supprimer, rebouter et requête invalide).

La carte Arduino sera aussi en connexion avec la technologie NFC (figure 40) qui va permettre la communication avec le Smartphone. Nous utilisons une fonction qui permet de lire les tags NFC et les attributs. Une fois le code d'accès est lu par la porte, un log sera envoyé au serveur par le biais de ZigBee.

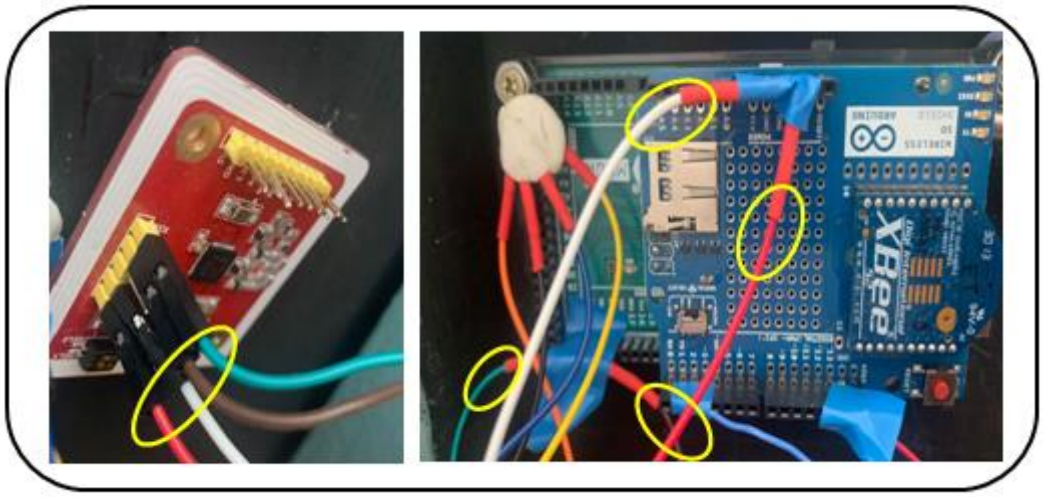

Figure 40 : Montage du capteur NFC avec Arduino

Pour le montage final de la porte intelligente (figure 41), la carte Arduino sera alimentée par 8 piles (+12V) et la gâche sera alimentée par 12 piles (+18V) via un Relay électrique

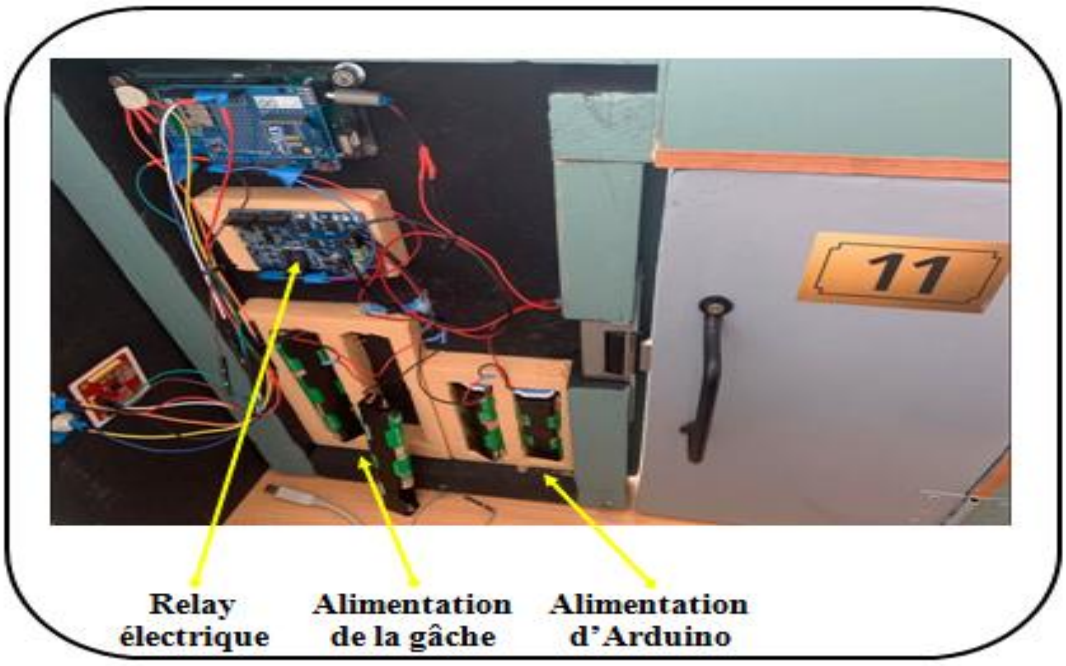

Figure 41 : Montage final de la porte

3.2.Application mobile

L'application mobile permettra à l'utilisateur de saisir les informations de réservation et d'accéder à la chambre d'hôtel. Pour cela, plusieurs fonctions ont été utilisées ; une pour l'envoi des données, une pour la réception et une qui permettra d'émuler la NFC sur le Smartphone. L'échange de données se base sur un chiffrement et un déchiffrement AES.

La figure suivante montre les trois interfaces de l'application mobile : l'interface principale, l'interface de réservation où l'utilisateur peut choisir les dates début et fin ainsi que le numéro de la chambre et l'interface d'accès en utilisant le mode d'émulation où l'utilisateur entre un code PIN et l'application va pouvoir émuler le code d'accès (PIN + token).

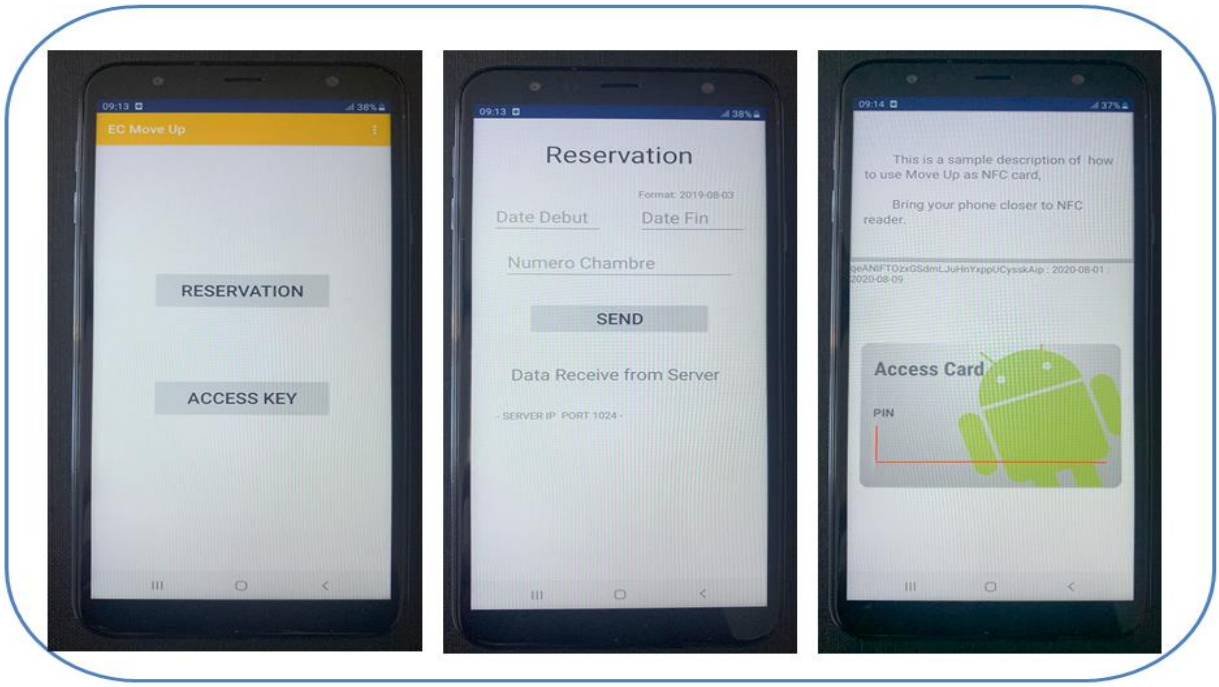

Figure 42 : Interfaces d'application mobile.

3.3.Serveur

Comme on a vu auparavant, le serveur communique avec l'utilisateur via internet et avec la porte intelligente via le réseau faible consommation ZigBee.

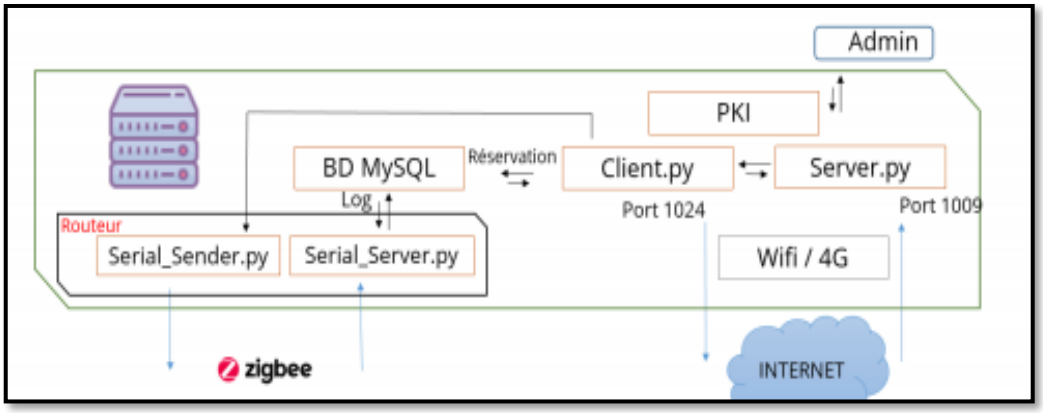

Figure 43 : Connexion serveur [32]

Étape 1 : installation du réseau LAN en connectant les deux composants sur le même réseau et en configurant les adresses IP de serveur (192.164.43.147) et de mobile (192.164.43.77). Le server.py est la partie connectée à internet qui reçoit les données de l'utilisateur, traite les données et donc la réservation, il envoie la réponse à l'utilisateur par le client et les données à l'Arduino par le serial_sender. Il permet aussi de stocker les requêtes dans la base de données.

La figure suivante montre deux tables de la base de données. La première partie la table réservation où les informations vont être stockées (date de début, date de fin, token, …) et la deuxième partie la table Log concerne le stockage de différentes fonctions, dans ce cas l'ajout de l'utilisateur est marqué par ADD.

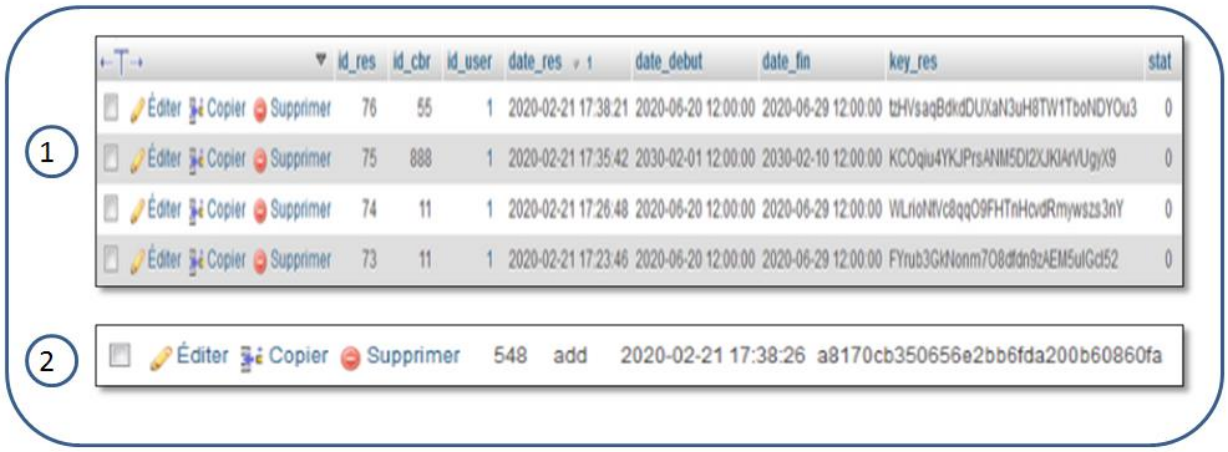

Figure 44 : Table BD Réservation et Log

Étape 2 : installation de réseau faible consommation ZigBee. A l'aide d'un logiciel X-CTU ou putty on peut configurer les cartes Xbee. Le Serial_server est la partie connectée au ZigBee qui intercepte les données reçues de la porte c'est-à-dire les tentatives d'accès et qui traite les données. Il permet aussi de stocker ces données dans la base de données.

La figure suivante montre la table Log où on enregistre les tentatives d'accès. L'autorisation de l'utilisateur est marquée par ALW alors que le refus est marqué par DNY.

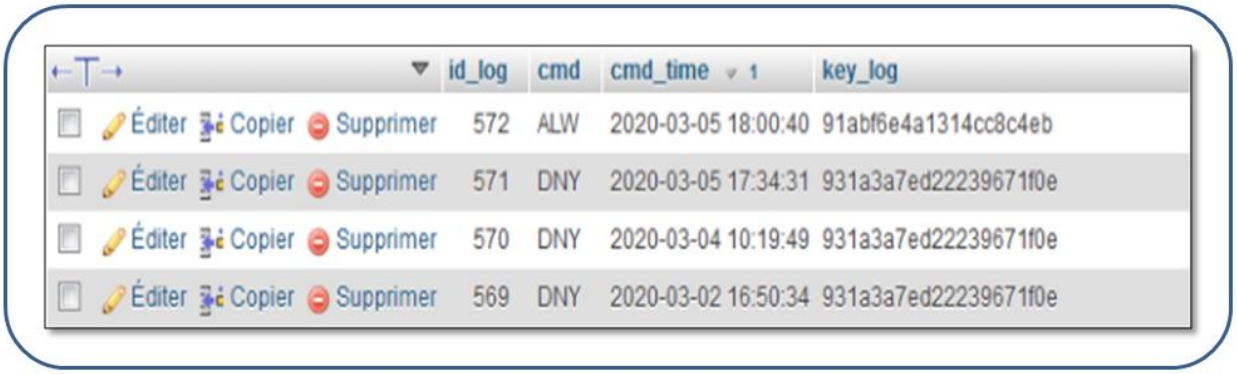

Figure 45 : Table BD Log

Il existe d'autres commandes et fonctions qui peuvent être stockées dans la table Log : ERE pour désigner les messages d'erreur, CLR pour la suppression, …

3.4.Application web

L'application web permettra à l'administrateur de s'inscrire et s'identifier comme la montre les figures suivantes :

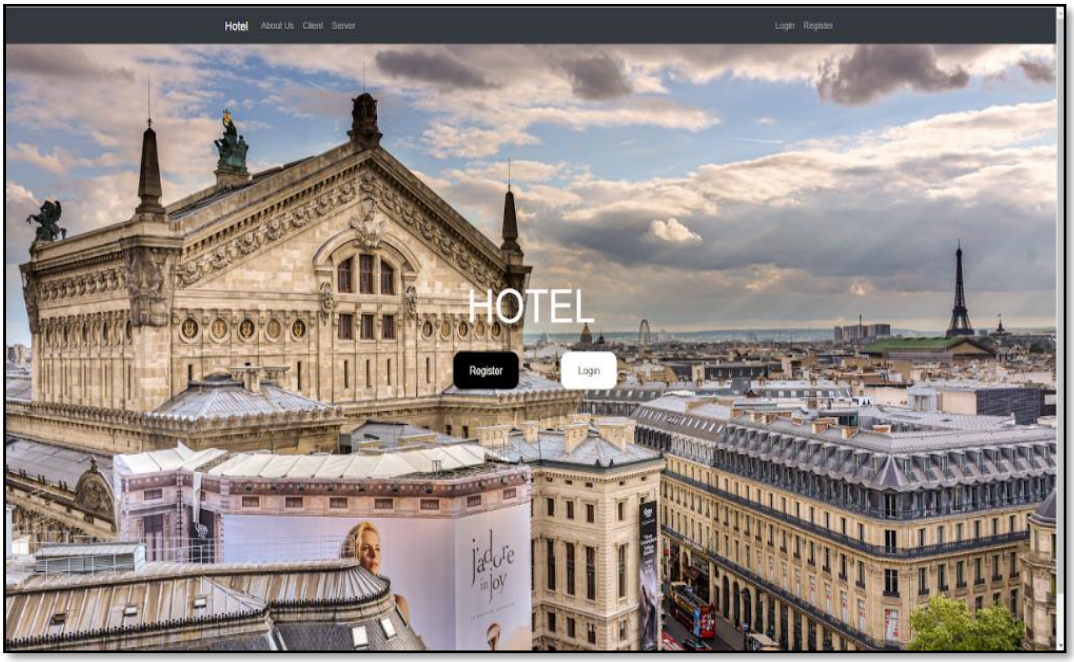

Figure 46 : Interface principale de l'application web

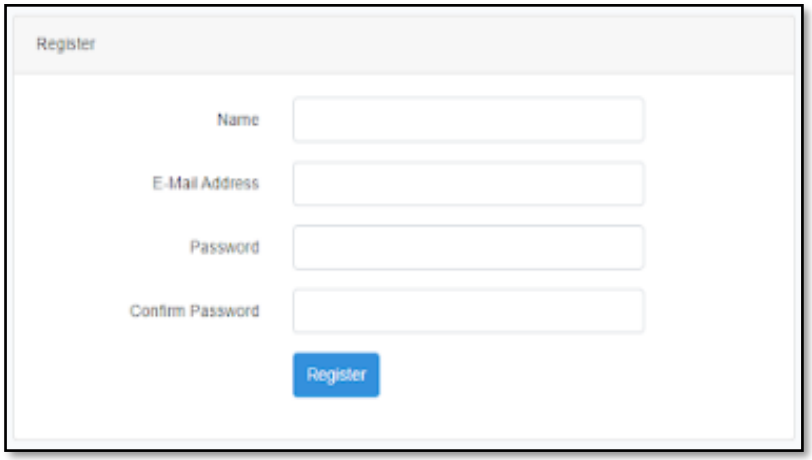

Figure 47 : Interface d'inscription « Register »

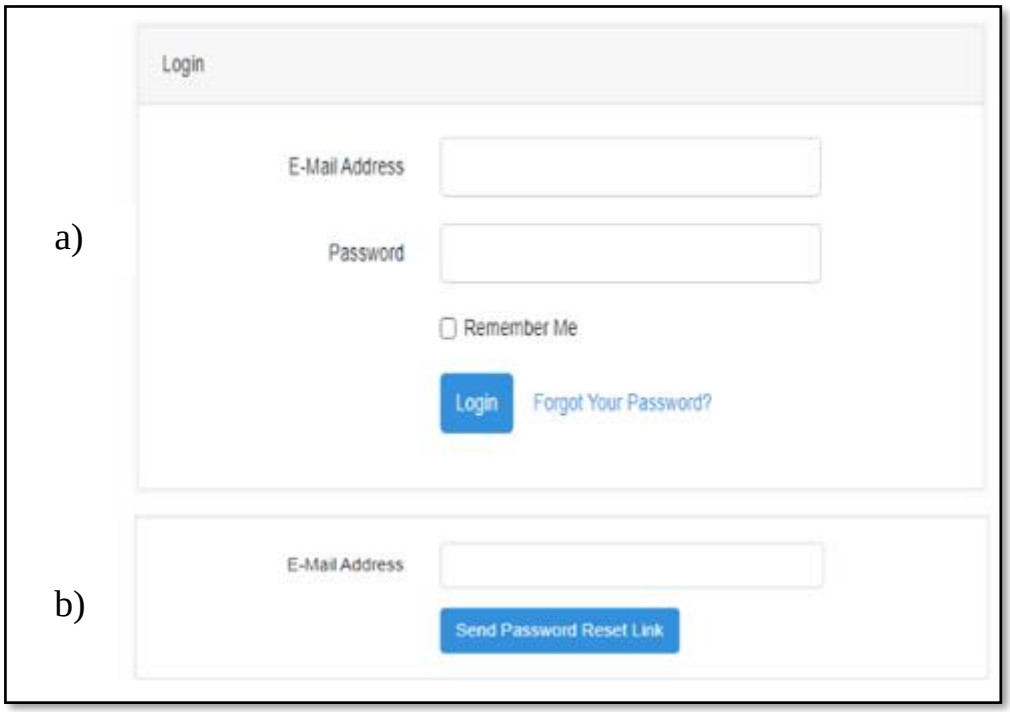

Figure 48 : Interfaces a) d'identification « Login », b) mot de passe oublié

Après être s'identifier, l'administrateur pourra lancer le serveur qui reçoit les données pour pouvoir les traiter et contrôler la réservation.

La figure suivante montre l'interface où il y a un bouton « Server » pour le lancer :

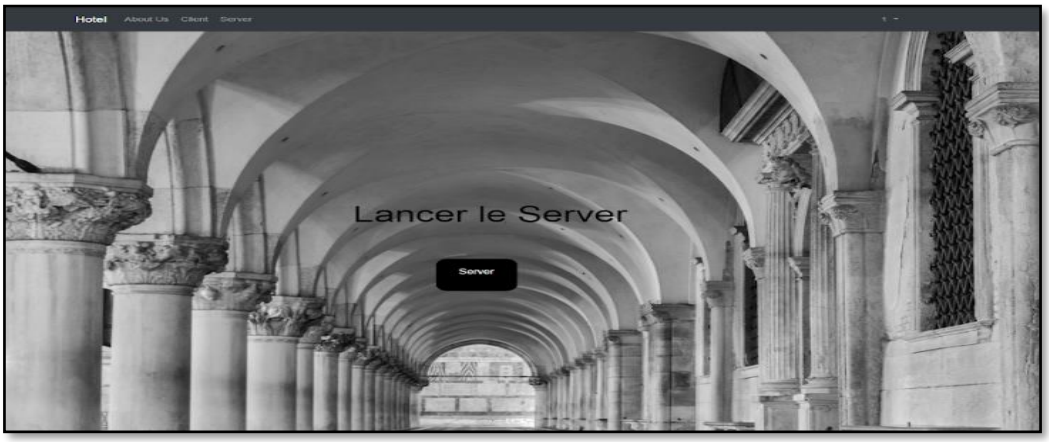

Figure 49 : Interface de lancement du Serveur

Après avoir lancé le serveur, l'utilisateur fait une réservation et tente l'accès à la chambre d'hôtel. On aura une fenêtre - présentée sur la figure 50 - qui montre la tentative d'accès avec le code d'accès à une heure et une date précise.

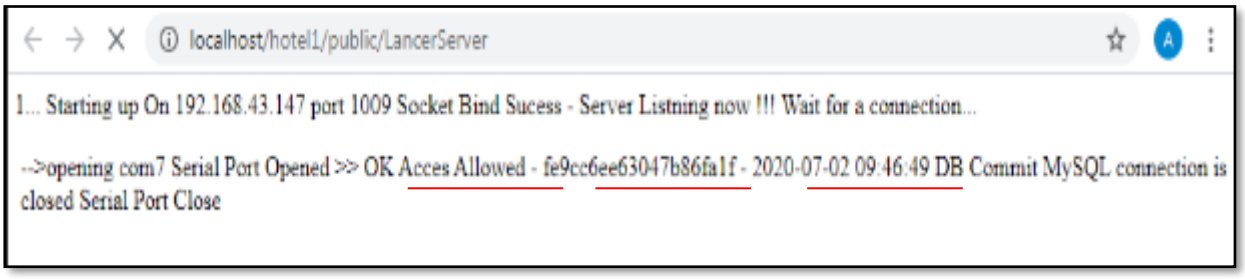

Figure 50 : Tentative d'accès sur l'application mobile

4. Tests et résultats

4.1.Réservation

Pour pouvoir faire une réservation, l'utilisateur doit se connecter avec une identité et un mot de passe. Puis, en utilisant l'application mobile il fait la réservation pour une période du temps.

Le serveur génère un token et l'envoie à l'utilisateur via un canal sécurisé, il envoie aussi le PIN via un autre canal.

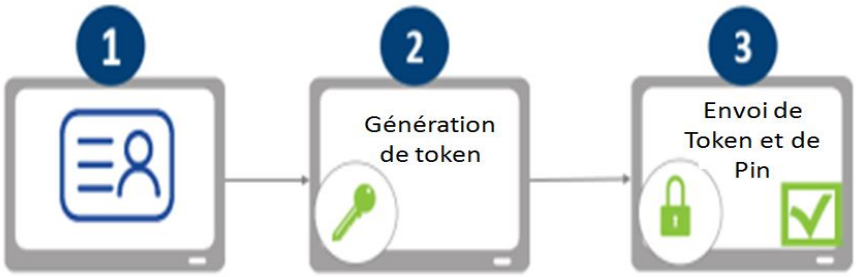

Figure 51 : Etapes de réservation.

Dans la figure suivante, nous montrons l'interface de réservation. La première partie indique l'avant réservation et la deuxième partie indique l'après réservation où on remarque les données reçues (envoyées par le serveur).

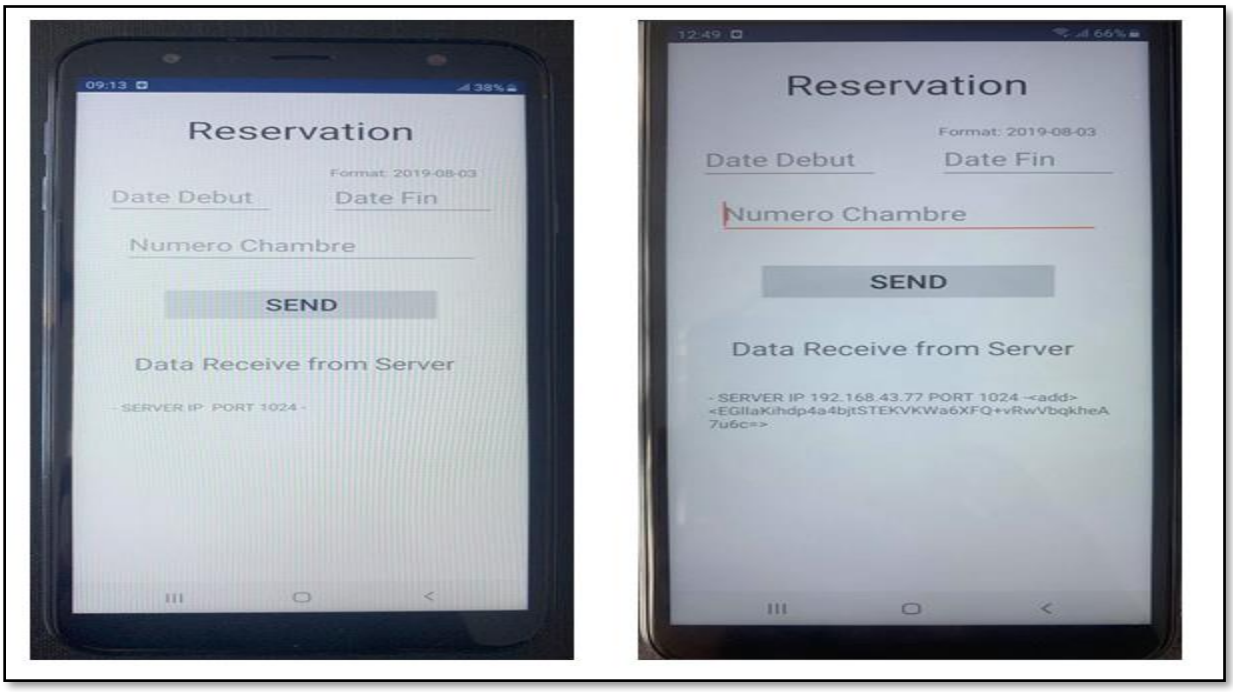

Figure 52 : Avant-Après réservation

4.2.Accès

Pour que l'utilisateur puisse avoir accès à la chambre d'hôtel, trois éléments doivent être vérifiés (figure 53) :

« Something you have » ⟶ Smartphone
« Something you know » ⟶ Code PIN
« Something you get » ⟶ Token

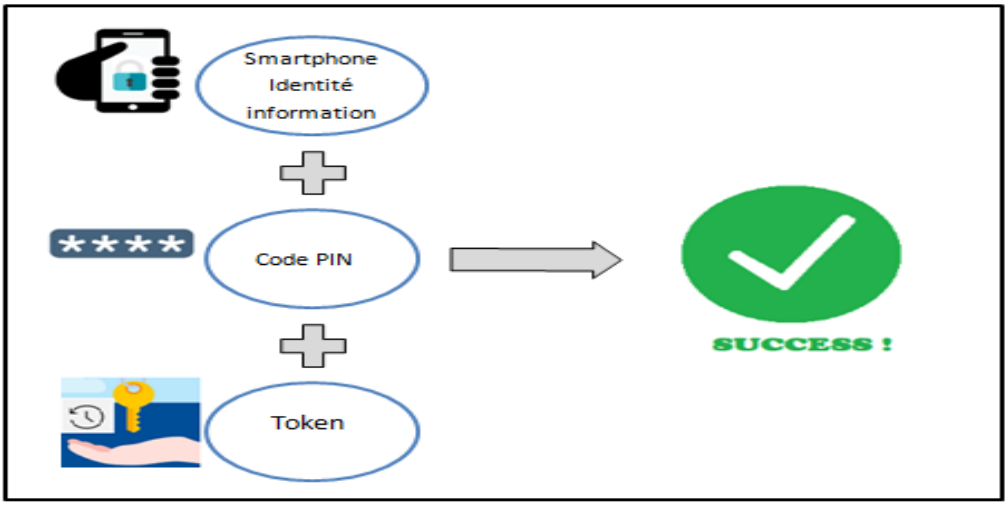

Figure 53 : Étapes d'accès.

L'utilisateur reçoit le Token (figure 54) et entre le code PIN sur son Smartphone et donc il peut tenter l'accès à la porte intelligente.

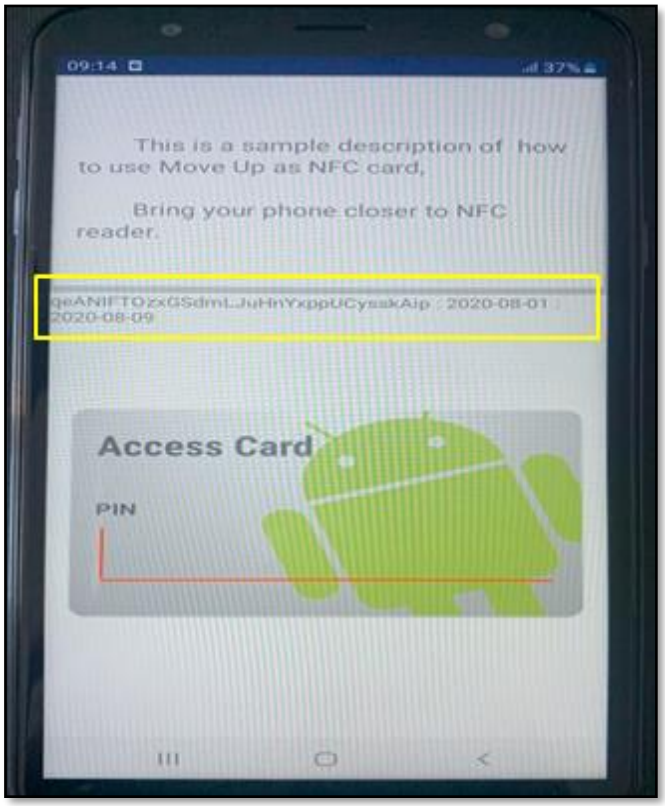

Figure 54 : Réception de Token

4.2.1. Accès garanti

L'accès à la porte intelligente est garanti si l'utilisateur a la bonne clé et utilise le bon PIN

```
>> OK Acces Allowed - e2e982f367f05a5c78d8 - 2020-07-02 09:58:38
DB Commit
MySQL connection is closed
>> NO + Received
```

Figure 55 : Accès autorisé sur le serveur

Figure 56 : Accès autorisé à la porte

4.2.2. Accès refusé

L'accès à la porte intelligente est refusé en deux cas :

- Si l'utilisateur a la bonne clé mais utilise un mauvais PIN.
- Si l'utilisateur a la mauvaise clé et le bon PIN.

```
Serial Port Opened
>> OK Acces Denied - e2e982f367f05a5c78d8 - 2020-07-02 09:58:25
DB Commit
MySQL connection is closed
```

Figure 57 : Accès refusé sur le serveur

Figure 58 : Accès refusé à la porte

4.3.Attaques résistantes

Un attaquant de type Man-in-the-Middle peut se positionner entre le serveur et la serrure et entre l'utilisateur et la serrure. Dans les deux cas, notre système résiste à ce type d'attaque :

- Serveur - Serrure intelligente : l'échange entre ces deux entités est sécurisé en utilisant le hachage MD5 qui est irréversible.

- Application mobile – Serrure : en utilisant la technologie NFC, l'attaquant ne peut pas intercepter la communication car la distance entre la serrure intelligente et l'utilisateur est très courte (quelques centimètres).

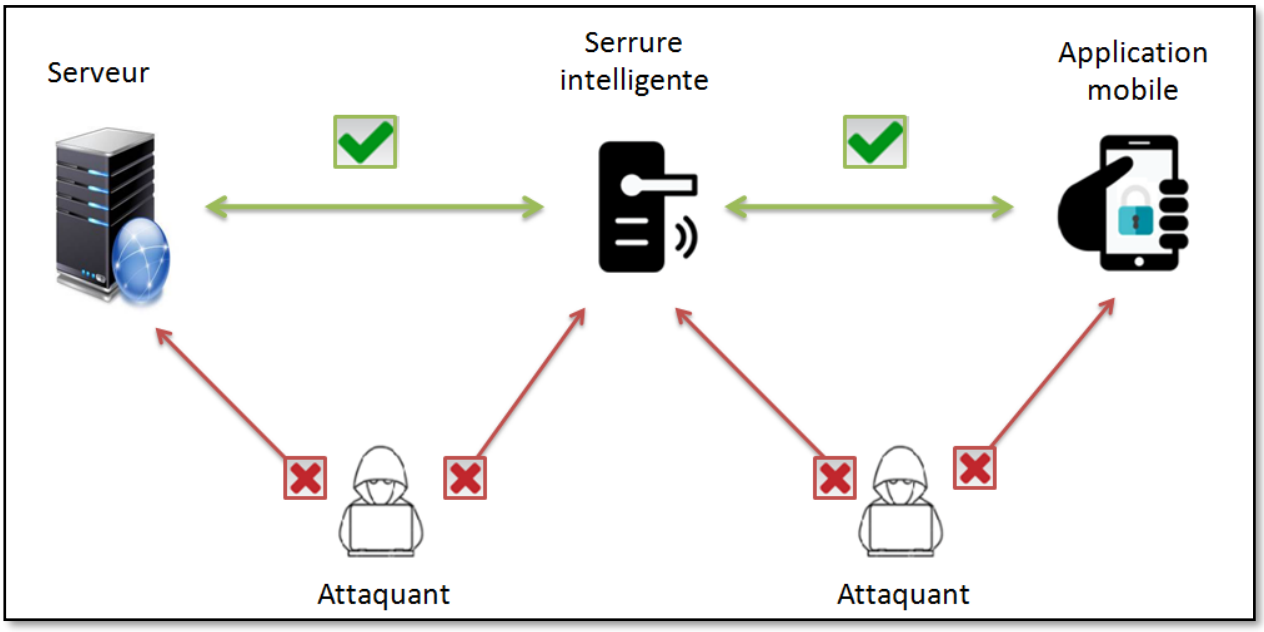

Figure 59 : Attaque Man-in-the-Middle

L'attaquant de type *Eavesdropping* se met entre le serveur et l'application mobile pour pouvoir intercepter la communication et avoir des informations sur la vie privée des utilisateurs et donc perte de confidentialité. Dans notre cas, le système résiste à ce type d'attaque car les informations entre ces deux entités sont échangées dans un canal sécurisé (authentification, cryptage,…).

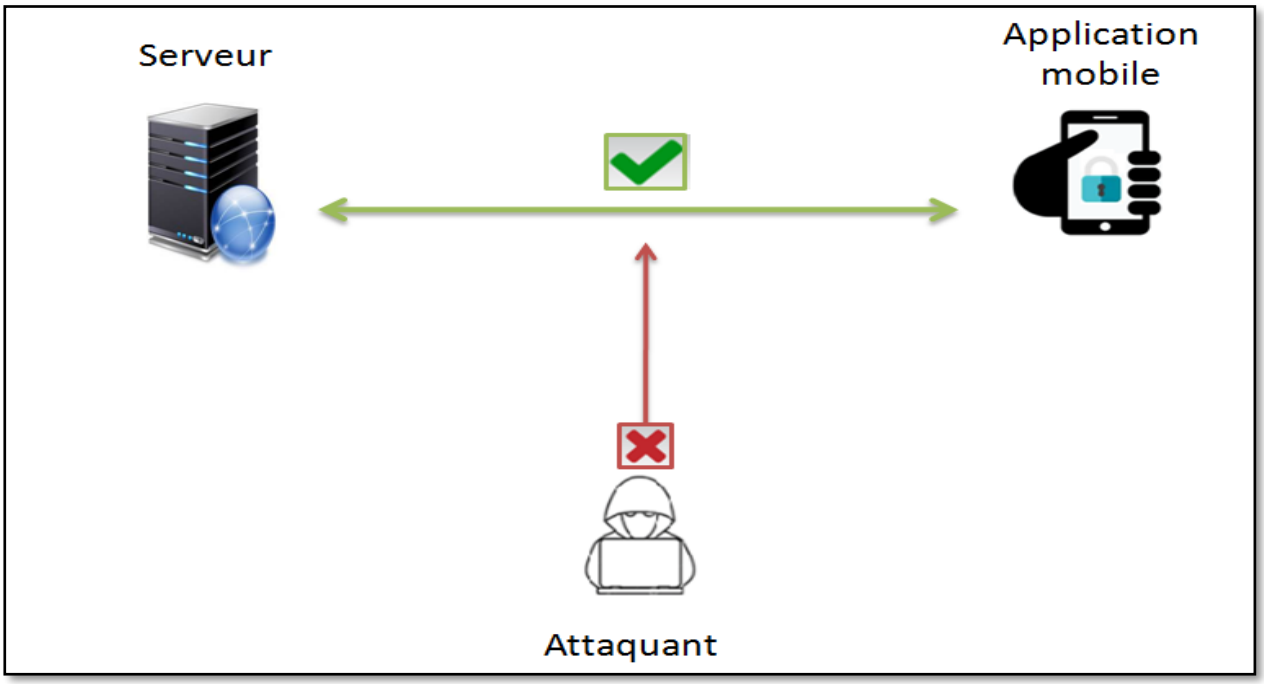

Figure 60 : Attaque Eavesdropping.

L'attaquant de brute force vise la serrure intelligente pour trouver le mot de passe ou une clé en essayant plusieurs tentatives. Dans notre cas, le système résiste à ce type d'attaque car nous avons limité l'envoi de PIN à trois essais dans une période de temps.

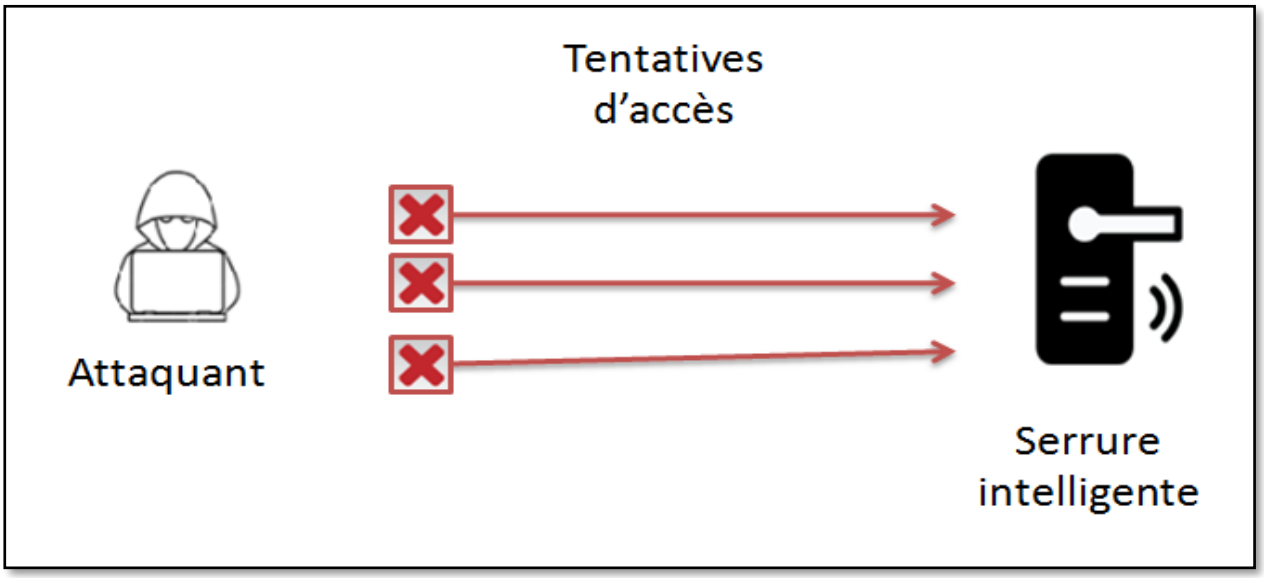

Figure 61 : Attaque brute force

Un attaquant d'usurpation d'identité vise l'application mobile en volant l'identité de l'utilisateur. L'attaquant peut également perdre son téléphone ; dans ce cas, notre système résiste car l'attaquant ne dispose pas du code PIN parce qu'il a été envoyé via un autre moyen de communication.

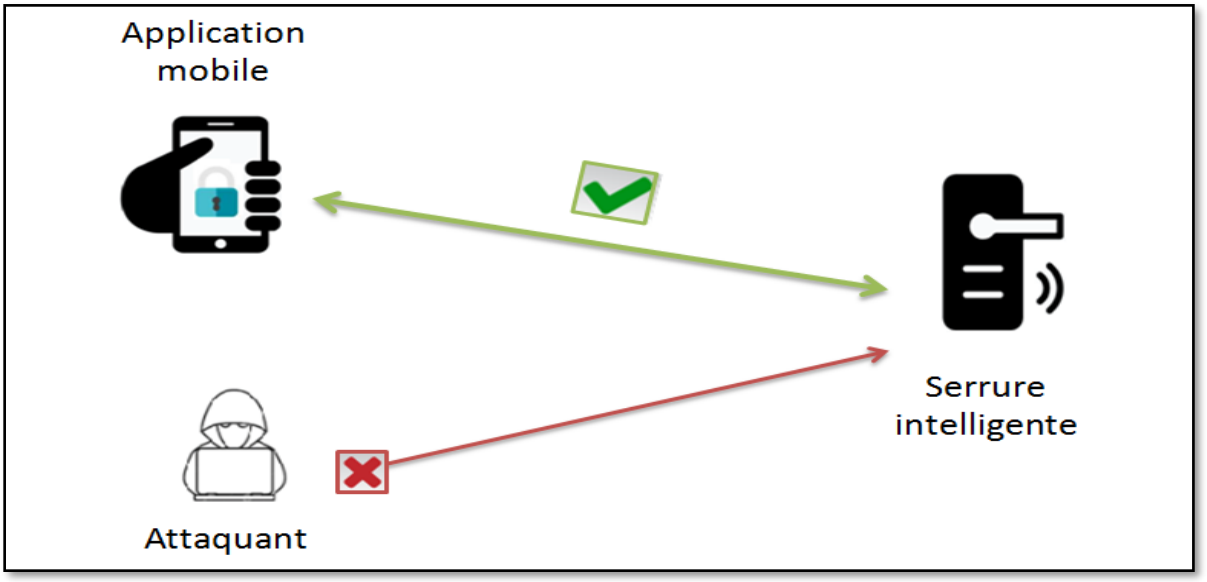

Figure 62 : Attaque d'usurpation d'identité.

Le tableau suivant montre les contre mesures de chaque attaque ainsi que si notre système résiste ou pas.

	Attaques	Contremesure	Notre système
Communication	Man in the middle	-Utilisation de hachage MD5 côté serveur porte. -Utilisation de protocole challenge/réponse.	Résiste
	APTs	-Maintenir à jour ses systèmes -Sensibiliser les utilisateurs -Utilisation de hachage MD5. -L'authentification pour assurer l'intégrité de chaque entité de système.	Résiste
	Vol de session	-Utilisation de protocole challenge/réponse.	Résiste

		-Utilisation des token de size 32 crypté	
	Traffic analysis	-Envoi de faux paquet c'est à dire envoyer un flux continu de messages (surveillance régulière du réseau) -Utiliser des identités temporaires	Ne résiste pas
	Eavesdropping	-Canal sécurisé → les informations échangées seront protégés par plusieurs type (authentification, cryptage...)	Résiste
	Data tampering	-Pare-feu -Signatures numériques -Contrôles d'accès	Ne résiste pas
	Replay attack	-Etablir une clé de session -utiliser des timestamps (associer une date et une heure au paquet envoyer) sur tous les messages. Cela empêche les pirates de renvoyer des messages envoyés	Ne résiste pas
Application mobile	Social engineering	-Sensibilisation de la clientèle.	Résiste
	Sniffing	-Utilisation de cryptage AES pour l'envoie des informations au serveur.	Résiste
	IP Spoofing	-Protéger l'adresse IP des clients en utilisant un réseau sécurisé -Protéger les données (authentification, chiffrement, droits d'accès) -Pare-feu	Résiste
	Impersonation attack	-Mettre en place un système d'échange sécurisé. -Echange de clé privée	Résiste
Serveur	Ransomware	-Avoir toujours un backup des informations	Ne résiste pas
	Data flooding	-Il faut changer dans le code, pour ajouter des limitations	Ne résiste pas

		pour nombre de réservation de même adresse IP dans une période du temps.	
	DoS	-Pare Feu -Un serveur backup	Ne résiste pas
Porte	Brute force	-Ajouter des limitations dans le code pour que quelqu'un n'aura pas le droit d'envoyer plus de 3 PIN dans une période du temps	Résiste

Tableau 5 : Classification d'attaques avec les contremesures

5. Conclusion

Ce dernier chapitre nous a permis d'évaluer et de tester les performances de notre de sécurité légère. En ce qui concerne les attaques qui peuvent menacer la communication de notre système ou ses entités, elles sont multiples et nous avons donc montré que notre système de sécurité résiste à certaines d'entre elles.

Conclusion générale

A la fin de cette recherche, nous pouvons constater que la communication se fait à travers plusieurs moyens et l'IdO est devenue un élément crucial qui correspond aux besoins d'aujourd'hui. Malgré ses nombreux avantages (surtout la facilité de l'échange et de la transmission des informations entre les objets connectés) qui sont indéniables, nous avons aussi confirmé, au cours de notre étude, le souci de départ, celui de la sécurité de ces réseaux (ou plutôt le manque de sécurité !). Malheureusement, l'augmentation des appareils intelligents entraîne l'augmentation des risques liés à l'atteinte à la vie privée des individus et des sociétés.

Chacun a sa perspective concernant l'IdO selon le cas étudié. Dans notre cas, l'hôtel intelligent, nous avons dans un premier temps approfondi nos recherches autour du concepts IdO. Puis, nous avons présenté les exigences essentielles de la sécurité dans l'IdO. Nous avons par la suite mis en œuvre un protocole de contrôle d'accès basé sur le token qui nous a permis de réaliser un système de sécurité légère. L'objectif de notre travail était donc de présenter le côté intelligent des objets connectés, d'analyser la sécurité du système et son efficacité en tenant compte du respect de la vie privée.

Notre système résiste à différentes attaques mais il est toujours menacé par d'autres (DoS, Replay attaque, Traffic analysis, etc.). Donc, il peut être amélioré au niveau de sécurité avec une autre forte authentification ou d'autres aspects de sécurité. Il peut également avoir une plateforme qui gère plusieurs utilisateurs et objets. Pendant cette étude, j'ai eu la chance de m'initier à plusieurs méthodes d'amélioration du système de sécurité. Une vision générale de tout le travail qui a été faite du chapitre théorique jusqu'à l'analyse des résultats obtenus permet d'approuver l'hypothèse principale qui dit que jusqu'à maintenant, il n'y a aucun système sécurisé à 100%. Bien entendu cette insécurité n'est pas de la même intensité dans tous les objets connectés. Ceci dit, ce travail m'a permis de consolider certaines connaissances théoriques que j'ai acquises à l'université. Elle m'a donnée aussi l'espoir d'atteindre un jour un meilleur degré de sécurité sur les réseaux.

Références bibliographique

[1] https://www.senioractu.com/Samsung-Airdresser-le-dressing-lavant-du-futur_a22419.html consulté juillet 2020

[2] https://www.arduino.cc/en/guide/introduction consulté avril 2020

[3] T.Dumartin "Architecture des ordinateurs'', Note de cours, 2004-2005

[4] YAHI, Amina, and Loubna KOURI. Contrôle et suivi d'une maison intelligente via internet. Diss. Université Akli Mouhand Oulhadj-Bouira, 2018.

[5] https://www.raspberrypi.org/help/what- is-a-raspberry-pi/ consulté avril 2020

[6] https://www.grafikart.fr/blog/raspberry-pi-utilisation consulté avril 2020

[7] M. DAMMAK "Smart Bracelet supporting Bluetooth 4.2 and communicating over IPv6", SupCom et HEPIA, 20-120, 2016

[8] P. Sethi and S. R. Sarangi "Internet of Things: Architectures, Protocols, and Applications'', Journal of Electrical and Computer Engineering, vol.2017.

[9] https://blog.octo.com/modeles-architectures-internet-des-objets/ , consulté Avril 2020

[10] A. ARFAOUI "Context-Aware and Adaptive Security Solutions for the Internet of Things'', université de Bourgogne, 15, 2019

[11] D. J. Cook, A. S. Crandall, B. L. Thomas, and N. C. Krishnan, "CASAS: A smart home in a box," Computer, vol. 46, no. 7, pp. 62–69, Jul. 2013

[12] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for Smart Cities," in IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22-32, Feb. 2014

[13] El Mouaatamid, O., Lahmer, M., & Belkasmi, "Internet of Things Security: Layered classification of attacks and possible Countermeasures'', electronic journal of information technology (9), 2016

[14] https://en.wikipedia.org/wiki/Intelligent_transportation_system , consulté mai 2020

[15] Y. Leng and L. Zhao, "Novel design of intelligent internet-of-vehicles management system based on cloudcomputing and Internet-of-Things,'' Proceedings of 2011 International

Conference on Electronic & Mechanical Engineering and Information Technology, Harbin, 2011, pp. 3190-3193

[16] https://www.irt-systemx.fr/projets/eva/ , consulté juillet 2020

[17] https://connect.ed-diamond.com/MISC/MISC-086/Tout-tout-tout-vous-saurez-tout-sur-le-ZigBee , consulté mai 2020

[18] T.FETTIOUNE, N.MAIZIA and S. AISSANI, “Gestion de clés dans l'Internet des Objets. ’’ Diss. Université Abderrahmane Mira-Bejaia, 2018.

[19] http://www.mede.fr/tp/TP_pdf/zigbee.pdf consulté mai 2020

[20] https://www.echosdunet.net/dossiers/technologie-nfc#technologie-nfc-un-bluetooth-ameliore consulté juin 2020

[21] https://www.frandroid.com/comment-faire/comment-fonctionne-la-technologie/237303_lenfc-2 consulté juin 2020

[22] https://nfc-forum.org/what-is-nfc/about-the-technology/ consulté juin 2020

[23] N.MAKHLOUFI, R.ACHOUR, A.BOUKERRAM, “Authentificaiton Dans L’iot’’ Diss. Université abderrahmane mira Béjaia, 2017.

[24] https://www.supinfo.com/articles/single/2961-principes-fondamentaux-securite-informatique consulté juin 2020

[25] NIST SP 800-53 Rev. 4 under Discretionary Access Contrôle, “https://doi.org/10.6028/NIST.SP.800-53r4 ”

[26] S.EL JAOUHARI, A.BOUABDALLAH and J.M.BONNIN “La sécurité des objets connectés.’’ MISC: multi-system & internet security cookbook 88 (2016): 54-59.

[27] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of internet of things (IoT)," Perception, vol. 111, no. 7, pp. 1-6, 2015.

[28] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan. “Internet of things (iot) security: Current status, challenges and prospective measures”. 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), December 2015.

[29] R. P. Padhy, M. R. Patra, and S. C. Satapathy, “Cloud computing: security issues and research challenges,” International Journal of Computer Science and Information Technology & Security (IJCSITS), vol.21, no.2, pp. 136–146, Dec.2011.

[30] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483-2495, Aug. 2018

[31] M. SALAÜN “Intégration de l’utilisateur au contrôle d’accès: du processus cloisonné à l’interface homme-machine de confiance.’’ Diss. Evry, Institut national des télécommunications, 2018.

[32] M.N.KERKAR, S.M.SENOUCI “Plateforme de Sécurité Légère pour IdO (Cas d’Etude : Hôtel Intelligent),’’ université de Bourgogne, 2019

[33] https://www.certeurope.fr/blog/quest-ce-quune-pki-ou-infrastructure-a-cles-publiques/ consulté juin 2020

[34] Standard, O. A. S. I. S. "Web Services Security: SOAP Message Security Version 1.1." (2012).

[35] S.DIOP, “Une infrastructure à clés publiques (PKI) pour sécuriser les messages dans un réseau V2G. ’’ Diss. Université du Québec à Trois-Rivières, 2018

[36] M. Dammak 1 , O. R. Merad Boudia , M.A.Messous 1 , S-M. Senouci 1 , C.Gransart ‘Token-Based Lightweight Authentication to Secure IoT Networks’, 2019, p 1-4

[37] https://link.springer.com/referenceworkentry/10.1007%2F0-387-23483-7_196 , consulté juin 2020

[38] https://fr.wikipedia.org/wiki/Attaque_par_force_brute , consulté avril 2020

[39] https://www.proofpoint.com/us/threat-reference/ransomware , consulté avril 2020

[40] https://www.sciencedirect.com/topics/computer-science/flooding-attack , consulté avril 2020

[41] I.ANDREA, C.CHRYSOSTOMOU, G.HADJICHRISTOFI, “Internet of Things: Security vulnerabilities and challenges. ’’ 2015 IEEE Symposium on Computers and Communication (ISCC). IEEE, 2015.

[42] https://waytolearnx.com/2018/07/difference-entre-attaque-active-et-attaque-passive.html consulté juin 2020

[43] M.N.KERKAR, M.DEMMAK, S.M.SENOUCI, M.A.MESSOUS, “Lightweight Security Platform for IoT: Smart hotel use case ’’, DRIVE Lab, Univ. Bourgogne Franche Comté, 2019

[44] https://www.sparxsystems.fr/resources/uml2_tutorial/uml2_usecasediagram.html consulté juin 2020

[45] https://www.sparxsystems.fr/resources/uml2_tutorial/uml2_classdiagram.html , consulté juin 2020

[46]https://www.ibm.com/support/knowledgecenter/fr/SS5JSH_9.5.0/com.ibm.xtools.modeler.doc/topics/cactd.html , consulté juin 2020

[47] http://remy-manu.no-ip.biz/UML/Cours/coursUML5.pdf consulté juin 2020

[48] https://www.python.org/doc/essays/blurb/ , consulté juin 2020

[49] https://www.arduino.cc/en/main/FAQ , consulté juin 2020

[50] https://www.techopedia.com/definition/33631/android-studio , consulté juin 2020

[51] https://desgeeksetdeslettres.com/web/xampp-plateforme-pour-heberger-son-propre-site-web, consulté juin 2020

[52] https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203607-sqlite-definition/ , consulté juin 2020

[53] https://www.positron-libre.com/electronique/arduino/arduino.php , consulté juin 2020

[54] https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203597-php-hypertext-preprocessor-definition/ , consulté juin 2020

[55] https://www.supinfo.com/articles/single/5637-presentation-framework-laravel , consulté juin 2020