الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة البليدة 1
Université de BLIDA 1

كلية العلوم
Faculté des Sciences

قسم الإعلام الآلي
Département d'Informatique

Mémoire de Fin d'Etudes

En vue d'obtention du diplôme de Master

Option : Sécurité des Systèmes d'Information

Plateforme de Sécurité Légère pour IdO

(Cas d'Etude : Hôtel Intelligent)

Réalisé par : Mehdi Nacer KERKAR

Travail proposé et réalisé avec :

Promotrice :	Pr. N. BOUSTIA	(USDB)
Encadreur :	Pr. S-M. SENOUCI	(DRIVE)
Co-Encadreur :	Dr. A M. MESSOUS	(DRIVE)
Présidente :	Dr. S. AROUSSI	(USDB)
Examinatrice :	Dr. ARKAM	(USDB)

2018/2019

Dédicaces

À mes très chers parents

Je vous dois ce que je suis aujourd'hui, grâce à votre amour, votre patience et vos innombrables sacrifices.

Que ce modeste travail, soit pour vous une petite compensation et reconnaissance pour tout ce que vous avez fait.

Que Dieu, vous préserve et vous procure santé et longue vie afin que je puisse à mon tour vous combler.

À mes très chers frères et sœur

Aucune dédicace ne pourrait exprimer assez profondément ce que je ressens envers vous.

Je vous dirais tout simplement, un grand merci, je vous aime.

À mes très chers ami(e)s

En témoignage de l'amitié sincère qui je lis et les bons moments passés ensemble.

Je vous dédie ce travail en vous souhaitons un avenir radieux et plein de réussites.

Remerciement

Tout d'abord, nous remercions DIEU tout puissant de nous avoir donné la patience, la santé et la volonté pour achever ce travail.

Louange à « Allah » qui m'a guidé sur le droit chemin tout au long du travail et nous a inspiré les bons pas et les justes reflexes. Sans sa miséricorde, ce travail n'aura pas abouti.

Un remerciement spécial à mes parents et à tous les membres de ma famille pour leurs soutiens et encouragements tout au long.

J'aimerais adresser un merci à ma promotrice madame N. Boustia. Qui a su rendre mon projet possible et également apporter plus un soutien moral que physique.

A ce titre, je tiens à remercier vivement mes encadreur monsieur S-M. Senouci et monsieur A.Messous de l'occasion qu'ils mon offerte au Laboratoire Drive de me permettre de réaliser mon stage, un autre merci pour leurs conseils et leurs suivis durant la réalisation de mon projet.

Enfin, je remercie l'ensemble des personnes rencontré dans Laboratoire Drive pour les conseils qu'ils ont pu me prodiguer au cours de ce stage.

Je remercie l'équipe du labo Esubalew, Maissa, Martine, Régice, Anthony, Widdad,

A la fin de ce travail, nous tenons à remercier tous ceux qui ont contribués de près ou de loin à la réalisation de ce mémoire.

Résumé

L'Internet des objets (IdO) est un concept basé sur l'idée que tous nos objets de la vie quotidienne seront un jour connectés à Internet. En quelques années seulement depuis son apparition, il a été adopté dans divers secteurs grâce à son potentiel. Cependant, sa forte intégration soulève encore plusieurs questions et se heurte à de nombreux défis. L'un des principaux défis est "comment garantir la confidentialité et établir une sécurité solide pour cette nouvelle technologie".

Dans ce travail, nous avons mis en évidence les concepts clés pour l'environnement IdO, ainsi que les besoins et les défis en matière de sécurité IdO. Nous avons étudié certains schémas de déploiement de clés de sécurité fournissant des services d'authentification et de sécurité. Nous avons également identifié certains moyens de communication et méthodes de contrôle d'accès utilisés pour élire des utilisateurs légitimes parmi plusieurs, afin de prendre des décisions dans un système informatique. Notre proposition repose sur un protocole léger d'authentification basé sur des tokens pour la sécurité du réseau.

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 a concept based on the idea that all our daily life objects will be one day connected to the internet. In just a few years since its appearance, it has been adopted in various sectors thanks to its potential. However, its high integration still raises several questions and faces numerous challenges. One of the main challenges is "how to ensure privacy and establish robust security for this new technology".

In this work, we have highlighted the key concepts for IoT environment, as well as the needs and challenges for IoT security. We have studied some schemes for security key deployment that provide authentication and security services. We have also identified some means of communication and access control methods that are used to elect legitimate users among several, in order to make decisions in a IT system. Our proposal relies on a lightweight token-based authentication protocol for network security.

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

ملخص

إن انترنت الأشياء هو مفهوم قائم على فكرة أن جميع الأشياء حياتنا اليومية ستكون متصلة بالإنترنت في يوم من الأيام. في بضع سنوات فقط منذ ظهوره، تم اعتماده في مختلف القطاعات بفضل إمكاناته. ومع ذلك، لا يزال تكاملها العالي يثير العديد من الأسئلة ويواجه العديد من التحديات. أحد التحديات الرئيسية هي "كيفية ضمان الخصوصية وإنشاء أمان قوي لهذه التكنولوجيا الجديدة."

في هذا العمل، أبرزنا المفاهيم الأساسية لبيئة إنترنت الأشياء، وكذلك الاحتياجات والتحديات الخاصة بأمن إنترنت الأشياء. لقد درسنا بعض المخططات لنشر مفتاح الأمان التي توفر خدمات المصادقة والأمان. لقد حددنا أيضًا بعض وسائل الاتصال والتحكم في الوصول التي يتم استخدامها لانتخاب مستخدمين شرعيين بين العديد، من أجل اتخاذ القرارات في نظام تكنولوجيا المعلومات .يستند اقتراحنا إلى بروتوكول مصادقة خفيف الوزن يستند إلى رموز خاصة بأمان الشبكة.

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

Table des matières

Table des figures

Tables des tableaux

Liste des abréviations

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

ISAT : l'Institut Supérieur de l'Automobile et des Transports.

IdO : Internet des Objet.

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

I2C : (Inter-Integrated Circuit), Circuit inter-intégré.

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.

RFID : (Radio Frequency Identification), Identification radiofréquence.

E0 : est une solution cryptographique utilisé par le Bluetooth.

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.

OTPROM : (one-time programmable read-only memory) Mémoire morte programmable.

UVPROM : (Ultra Violet Programmable Read Only Memory)

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.

NIC : (The National Intelligence Council), Conseil national du renseignement.

ITU : (International Telecommunication Union), Union Télégraphique Internationale.

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

XOR : (Exclusive or), fonction OU exclusif.

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

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

INTRODUCTION GENERALE

L'Internet des objets (IdO) est considéré comme un concept qui a touché plusieurs acteurs et a acquis une plus grande reconnaissance en raison de la grande hétérogénéité de son matériel et de ses technologies. L'objectif est de permettre aux objets d'être connectés à tout moment, n'importe où, avec tout et n'importe qui (autre objets, serveur …) idéalement en utilisant n'importe quel réseau et n'importe quel service. C'est par le biais de connexions sans fil que les objets sont capables d'interagir les uns avec les autres pour créer de nouveaux services.

De nos jours, les appareils connectés à Internet connaissent une croissance exponentielle. Ainsi, un besoin d'accessibilité s'est installé au sein des utilisateurs, tout en gardant un axe sur la protection des données de la vie privée. La sécurité de l'utilisateur est le centre d'intérêts. Des solutions cryptographiques existent pour assurer ces services. Cependant, ces solutions ne seraient-elles pas inefficaces voire inapplicables à des objets ayant de fortes contraintes de ressources ?

Beaucoup de questions se posent sur l'adaptation de telles approches à un réseau IdO comportant potentiellement des milliards d'objets. Un challenge difficile serait de concevoir des protocoles de gestion de clés à la fois adaptables, robustes et résilients. Quels modèles de confiance conviendraient à cet écosystème complexe et fragile ? Ces questions deviennent encore plus pertinentes quand on sait que ces besoins peuvent évoluer dans le temps selon le contexte.

Dans ce contexte, plus les objets acquièrent de l'autonomie, plus les problèmes liés à la vie privée s'accentuent. La traçabilité des actions des objets, ainsi devenus autonomes, doit être soigneusement considérée.

En effet, la forte intégration de l'IdO au monde physique accroît le contrôle sur ce monde, mais le rend vulnérable aux actions potentiellement risquées des objets qui le contrôlent. Ainsi, émerge la question de gestion des crédentités dans l'IdO. Une gestion qui permet à la fois d'instaurer des politiques de sécurité claires, adaptatives selon le contexte et d'établir les responsabilités des faits et des actions sur l'environnement physique des objets. La taille de l'IdO est un autre challenge pour la sécurité [1].

Dans le cadre de notre projet, qui se déroule au sein du laboratoire Drive à l'ISAT. Nous adoptons la technologie d'IdO pour créer, fusionner à la fois des logiciels et du matériel connectés pour développer une plateforme de sécurité légère pour IdO.

Le but de notre projet est d'analyser les risques et les vulnérabilités, de concevoir un schéma de contrôle d'accès contextuel léger. Afin, d'implémenter un scénario utilisant une application Android pour accéder en toute sécurité à un appareil IdO. Dans notre cas une porte intelligente sera parfaite pour démontré une sécurité autonome, s'appuyant sur un mode de communication faible en consommation d'énergie.

Ce document se présentera sous forme de trois chapitres.

- Chapitre 1 : une étude bibliographique sur l'IdO, puis une analyse qui portera sur les aspects de sécurité, de confidentialité lié à l'IdO.
- Chapitre 2 : la conception d'une architecture pour le contrôle d'accès basé sur le contexte avec des stratégies de sécurité afin de fournir des clés numérique/Tokens pour donner/retirer l'accès aux ressources numériques/physiques dans le cadre de l'IdO.
- Chapitre 3 : l'implémentation d'un scénario de démonstration utilisant une application de téléphone Android pour accéder en toute sécurité à un périphérique IdO intelligent.

Contexte du projet

Ce travail a été développé dans le contexte du cadre du projet PARFAIT qui est de développer une plateforme sécurisée pour protéger les données personnelles contenues dans les applications gérant des objets connectés. Un autre objectif de ce projet est de réduire la complexité des démarches nécessaires pour intégrer et déployer des services dans les objets connectés.

Le projet PARFAIT est intimement lié au projet du même nom déposé dans le cadre d'ITEA3 dont le résumé est disponible sur le lien suivant : https://itea3.org/project/parfait.html.

Problématique

L'émergence de l'Internet des Objets (IdO- Internet of Things) comme nouveau paradigme mène vers une vie de plus en plus connectée. Des milliers d'appareils, de personnes et, éventuellement, de services devraient être interconnectés et seraient amenés à échanger des données et d'informations utiles. Bien que ce nouveau paradigme continue à créer de nouvelles opportunités, l'IdO présente également des défis fondamentaux liés à la sécurité, à la confidentialité et le respect de la vie privée. Pour établir des connexions sécurisées entre des personnes, des objets et des services, la sécurité doit être omniprésente. La sécurité physique et la cyber sécurité doivent travailler en collaboration pour protéger les réseaux, les applications, les appareils, les données et les utilisateurs, qui sont les éléments essentiels de l'IdO. A cause de l'augmentation du nombre d'appareils connectés, l'émergence du Big Data et de l'automatisation, les données exploitées par les systèmes d'information doivent être traitées de manière aussi sécurisée que possible.

Dans ce contexte, ce stage de fin d'étude portera sur l'analyse de la sécurité dans le domaine de l'IdO dont le but est de fournir une vue d'ensemble sur les concepts, les techniques, les applications, ainsi que les principaux axes de recherche dans ce domaine. En effet, la gestion et le déploiement des politiques de contrôle d'accès (*Access Contrôle Policies*) se reposent sur des architectures standardisées et fiables. Néanmoins, ces architectures peinent encore et présentent des limitations pour la prise en charge de l'évolution et le changement éventuel du contexte dans la gestion du contrôle d'accès. Le contrôle d'accès selon le contexte (*Context-sensitive Access Contrôle*) permet de prendre des décisions concernant les permissions d'accès en prenant en considération des changements d'états liés à l'environnement de l'utilisateur ou à l'objet physique (lieu, situation, niveau de confiance ou réputation des entités environnantes, etc.).

Objectifs de recherche

L'objectif principal de ce travail est de développer une preuve pour validé l'approche pour un schéma de sécurité allégée, mettant en œuvre un protocole pour le contrôle d'accès en se basant sur le concept de *Tokens*.

Ce travail repose principalement sur l'intégration d'un article de recherche « Token-Based Lightweight Authentication to Secure IdO Networks » qui est un travail de thèse théorique [0]. Mon travail sera en partie, pratique et implémentation à ce modèle de solution proposé.

CHAPITRE I : Internet des Objets

1. Introduction

Internet des objets doit être conçu pour un usage facile masquant la complexité technologique sous-jacente, et une manipulation en toute quiétude empêchant les menaces et risques potentiels. Dans l'IdO, tout objet est potentiellement connecté à Internet et capable de communiquer avec d'autres objets. Ceci engendre de nouveaux risques liés notamment à la confidentialité, l'authenticité et l'intégrité des données échangées entre les objets.

Quels modèles de confiance conviendraient à cet écosystème complexe et fragile ? Des questions deviennent encore plus pertinentes quand on sait que ces besoins peuvent évoluer dans le temps selon le contexte.

Parmi ces besoins des usagers, on peut citer le respect de la vie privée qui doit être protégée pour éviter l'identification et la localisation non autorisée. Comment s'assurer que les objets de la sphère privée, dotés de capacités à percevoir et à agir, respectent scrupuleusement ces exigences ?

Ce premier chapitre est divisé en trois sections. Dans la première section, nous présenterons et définirons l'Internet des objets (IdO) et exposerons les composants majeurs de chaque couche qui composent la pile IdO. Ensuite, nous soulignerons différents systèmes embarqués et leurs composants.

La deuxième section qui portera sur l'analyse des différentes technologies de communication basse consommation utilisé dedans. En outre, nous définirons un protocole d'application d'IdO utilisé pour garantir communication entre Internet et les réseaux sans fil basse consommation.

Enfin, la troisième section portera sur l'aspect la sécurité du système, vulnérabilités et menaces potentielles qui entourent l'internet des objets. Puis, nous nous concentrerons sur le plus important aspect qui est le contrôle d'accès, qui est censé étendre la sécurité sur toute l'architecture proposée. De plus, nous présenterons certaines évolutions prospectives de la sécurité de l'internet des objets, systèmes de sécurité léger. Enfin, nous soulignerons la partie utilisateur et mettons en évidence les principales caractéristiques qui lui sont associées.

2. Internet des Objets

L'Internet des objets est une nouvelle révolution de l'Internet. En effet, les objets obtiennent l'intelligence en prenant des décisions liées au contexte grâce à leur capacité à communiquer des informations sur eux. En outre, ils peuvent accéder à des informations qui ont été recueillies par d'autres objets, ou être éléments de services complexes. Cette révolution est associée à l'apparition du cloud et la conversion d'Internet vers IPV6 avec une quasi capacité d'adressage illimitée.

Avec l'IdO, la communication est étendue via Internet à toutes les choses qui nous entourent. L'Internet des objets a pour but de permettre aux objets d'être connectés à tout moment, en tout lieu, avec n'importe quoi et n'importe qui utilisant idéalement n'importe quel réseau et n'importe quel service.

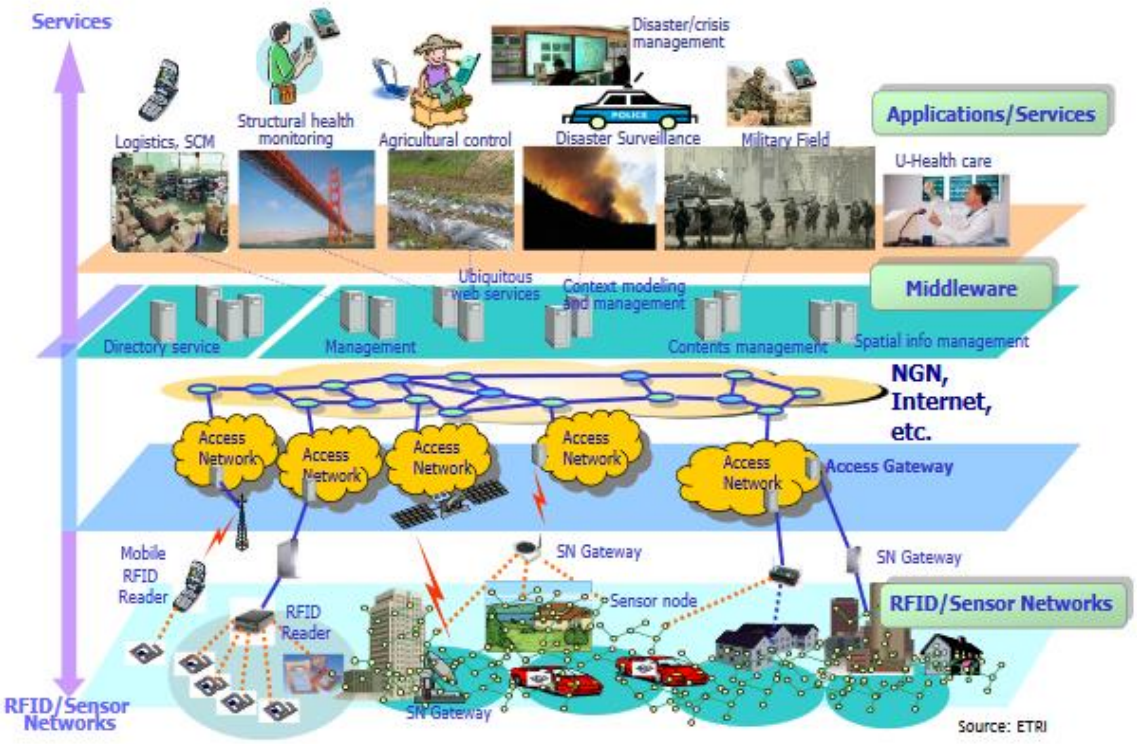


Figure 1 Structure de l'internet des objets [2]

IEEE Communications Magazine définit l'Internet des objets 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. [2]

2.1. Architecture et pile d'IdO

Afin de définir conceptuellement l'IdO, nous présentons un modèle fonctionnel à cinq couches qui inclut périphériques, connectivité, applications, plates-formes et services (Figure 2)

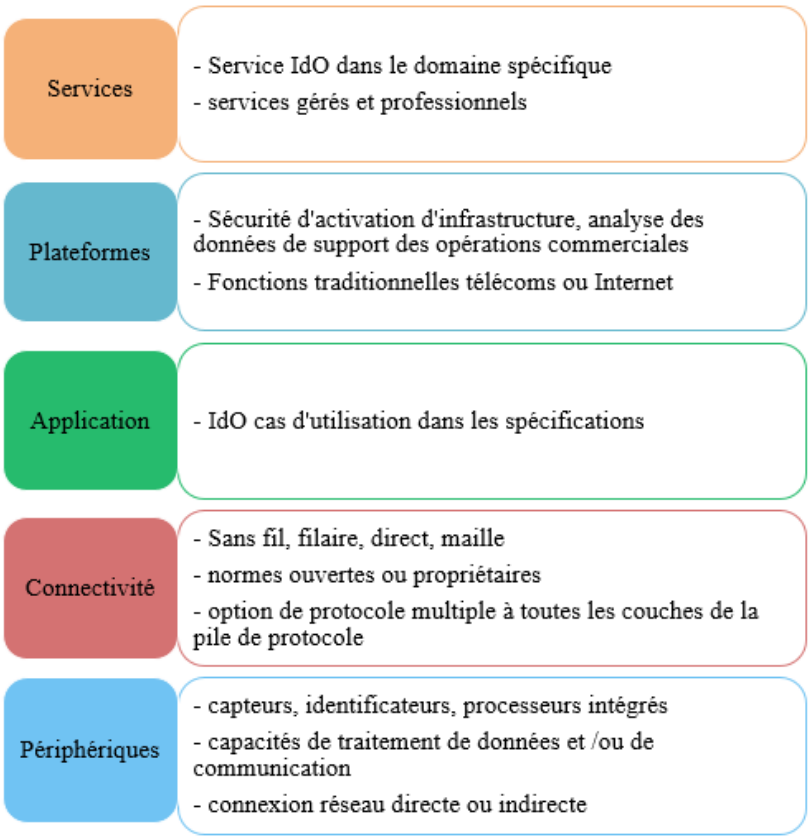


Figure 2 Pile IdO [2]

Voyons donc un peu plus en détail les aspects mentionnés :

a) **Périphériques :** contient des capteurs, des identificateurs et des passerelles qui sont des types de périphériques IdO. Utilisé pour collecter et transmettre des informations. Les appareils sont conçus et déployés pour répondre au besoin de cas d'utilisation de l'application.

b) **Connectivité :** concerne tous les appareils pouvant se connecter directement au réseau ou indirectement via un autre périphérique similaire ou une passerelle prenant en charge plusieurs périphériques. La connectivité peut être établie via plusieurs supports physiques tels que le cuivre, les fibres optiques ou en direct à travers un certain nombre de technologies sans fil.

c) **Les applications** : définissent le cas d'utilisation de chaque appareil et contiennent toutes les fonctions essentielles. Nécessaires aux fins prévues, y compris les architectures matérielle et logicielle.

d) **Les plateformes :** sont requise par les appareils et la connectivité pour fournir un service. Elles sont utilisées pour gérer et contrôler les appareils.

e) **Les services** : référencent les services IdO au client final.

Comme nous l'avons expliqué dans pile IdO, la communication d'IdO est étendue à tous les utilisateurs via Internet, toutes choses qui nous entourent. Cette communication peut se faire par l'intermédiaire d'un certain nombre de technologies sans fil. Ainsi, dans la sous-section suivante, nous illustrerons l'objet intelligent puis ses technologies de communication. [2] [3]

2.2. Qu’est-ce qu’un Système embarqué

Un système embarqué est un système électronique et informatique autonome, qui ne possède pas d’entrées/sorties standards (clavier, souris, ... etc). Il est généralement produit pour résoudre un problème bien précis, pour exécuter une tâche bien définie [4]. Un système embarqué est considéré comme un système mixte constitué d’une partie matérielle et une partie logicielle, il interagit avec l’environnement auquel il appartient [5].

2.3. Système embarqué

2.3.1. Composants

Un microcontrôleur peut être vu comme un ordinateur situé dans un circuit intégré unique qui est dédié à l'exécution d'une tâche ou à l'exécution d'une application spécifique. Il contient les éléments suivants : de la mémoire, des périphériques d'entrée / sortie programmables et processeur. Les microcontrôleurs sont principalement conçus pour des applications embarquées et sont fortement utilisés dans les appareils électroniques à commande automatique tels que les téléphones portables, les appareils photo, les fours à micro-ondes, les machines à laver, etc. [6].

Le microcontrôleur est composé principalement de quatre parties [6] :

- Un **microprocesseur**, qui va prendre en charge la partie traitement des informations et envoyer des ordres. Il est lui-même composé d'une unité arithmétique et logique(UAL) et d'un bus de données. C'est donc lui qui va exécuter le programme embarqué dans le microcontrôleur.

- **Une mémoire de données** (RAM ou EEPROM) dans laquelle seront entreposées les données temporaires nécessaires aux calculs. C'est en fait la mémoire de travail qui est donc volatile.

- **Une mémoire programmable** (ROM), qui va contenir les instructions du programme pilotant l'application à laquelle le microcontrôleur est dédié. Il s'agit ici d'une mémoire non volatile puisque le programme à exécuter est à priori toujours le même. Il existe différents types de mémoires programmables que l'on utilisera selon l'application. Notamment :

    - OTPROM : programmable une seule fois mais ne coute pas très cher.

    - UVPROM : on peut la ré-effacé plusieurs fois grâce aux ultraviolets.

    - EEPROM : on peut la ré-effacé plusieurs fois de façon électrique comme les mémoires flash.

2.3.2. Arduino

Arduino est une plate-forme électronique à code source ouvert basée sur du matériel et des logiciels faciles à utiliser. 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 ce faire, l’utilisation du langage de programmation Arduino et le logiciel Arduino (IDE).

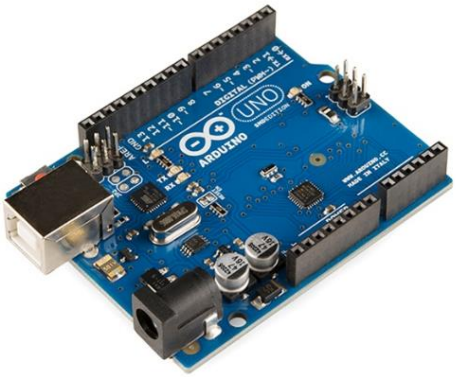


Figure 3 Arduino UNO [7]

Au fil des ans, Arduino a été le cerveau de milliers de projets, allant des objets du quotidien aux instruments scientifiques complexes. Une communauté mondiale de décideurs - étudiants, amateurs, artistes, programmeurs et professionnels - s'est rassemblée autour de cette plate-forme open source. Leurs contributions ont permis d'accumuler une quantité incroyable de connaissances accessibles qui peuvent être d'une grande aide pour les novices et les experts. [7]

2.3.3. Raspberry Pi

Le Raspberry Pi est un ordinateur de la taille d'une carte de crédit et pouvant être connecté à un écran d'ordinateur ou à un téléviseur. Il utilise un clavier et une souris standard. C'est un petit appareil capable qui permet aux personnes de tous âges d'explorer l'informatique et d'apprendre à programmer dans des langages tels que Scratch et Python. Il est capable de faire tout ce que vous attendez d'un ordinateur de bureau : naviguer sur Internet, lire des vidéos haute définition, créer des feuilles de calcul, traiter des textes et jouer à des jeux.

Figure 4 Raspberry Pi 3 Model B [8]

De plus, le Raspberry Pi a la capacité d'interagir avec le monde extérieur et a été utilisé dans un large éventail de projets de créateurs numériques, allant des machines à musique aux détecteurs de parents, en passant par les stations météo et les cabanes à oiseaux avec des caméras infrarouges. [8]

2.4. Comparaison

Dans l'ensemble des systèmes embarqués, les deux systèmes Raspberry Pi et Arduino sont les plus pratique à utiliser. Donc voilà une comparaison simple :

Raspberry Pi	Arduino
Ordinateur, utilise un système d'exploitation, pas de temps réel	Microcontrôleur, pas de système d'exploitation, temps réel
Versatile (ordinateur)	Spécialisé (fait comparativement peu de chose, mais les fait bien)
Autonome	Semi-autonome : a besoin d'un ordinateur pour le programmer
Quelques entrées/sorties numérique (8 par défaut), aucun analogique	Beaucoup d'E/S numérique (14 à 54), beaucoup d'entrées analogique (6 à 16)
Sortie audio, vidéo, E/S USB, connecteurs spécialisé écran/caméra, réseau.id	Possibilités d'extension via des cartes filles
Communauté importante	Communauté importante

Tableau 1 Comparaison Raspberry Pi / Arduino [9]

Au final, même s'ils semblent concurrents, les deux produits ne répondent pas aux mêmes besoins, et peuvent être complémentaires. Nous passons aux technologies de communication entre les objets.

3. Technologies réseau pour l'IdO

Un système intelligent aide non seulement à développer la qualité de vie, mais il contribue aussi à diminuer la consommation d'énergie. Un réseau local de communication exhaustif offre des fonctions de surveillance et de contrôle des objets, pour mieux échanger l'information avec l'utilité d'électricité. Afin de construire un réseau local pour réaliser ces fonctions, l'un des principaux problèmes qu'il faudra résoudre est la communication dans le réseau local et entre celui-ci et le réseau public.

Plusieurs technologies de communication peuvent être choisies, par exemple, Wi-Fi et Ethernet sont les plus populaires présentement ; d'ailleurs, il existe des technologies émergentes qui sont plus appropriées au petit réseau : ZigBee, Z-Wave. Chaque protocole comporte des avantages et des inconvénients ; ainsi il faut s'assurer de bien choisir une technologie de communication qui favorise à l'interopérabilité et la fiabilité, qui assiste notre système afin de compléter ses missions efficacement. Toutes les technologies de communication peuvent être classées en deux catégories : filaire (câblée) et sans-fil.

3.1. Réseau sans fil basse consommation

Par conséquent, cette section introduit les technologies sans fil.

- IEEE 802.15.4 a mis au point un système à faible coût, faible consommation d'énergie, faible complexité, standard de communication bas à moyen au niveau de la liaison et des couches physiques pour dispositifs aux ressources limitées. [10]
- Le1 Wi-Fi, aussi orthographié wifi2 est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11 (ISO/CEI 8802-11). Un réseau Wi-Fi permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, modem Internet, etc.) au sein d'un réseau informatique afin de permettre la transmission de données entre eux. [11]
- Bluetooth est un système de communication à courte portée destiné à remplacer les câbles connectant des appareils électroniques portables ou fixes. Les principales caractéristiques de la technologie sans fil Bluetooth sont la robustesse, une faible consommation d'énergie et un faible coût. La technologie de base est définie et gérée par le groupe d'intérêt spécial Bluetooth (SIG) dans la « spécification de base », qui sert de structure uniforme pour que les périphériques puissent interagir. [12]

  Il existe deux types de systèmes de technologie sans fil Bluetooth :

  - Taux de base (BR) (Bluetooth classique) : norme sans fil introduite dans la spécification Bluetooth depuis 1.0.
  - Bluetooth Low Energy (BLE) : norme sans fil à faible consommation développée avec la version 4.0 de la spécification.
- La technologie ultra large bande (UWB) est une technologie émergente dans le domaine de l'IdO qui transmet des signaux sur une grande plage de fréquences. UWB, en plus de ses capacités de communication, peut permettre une haute gamme de précision des dispositifs dans les applications IdO. [2]
- Zigbee est une spécification basée sur IEEE 802.15.4 pour une suite de protocoles de communication de haut niveau, utilisée pour créer des réseaux personnels avec de petites radios numériques à faible puissance, telles que la domotique, la collecte de données sur les dispositifs médicaux et autres. Besoins en bande passante réduite, conçus pour les petits projets nécessitant une connexion sans fil. Par conséquent, Zigbee est un réseau ad hoc sans fil à faible consommation d'énergie, à faible débit de données et à proximité étroite (par exemple, une zone personnelle). [13]
- RFID / NFC propose diverses normes pour offrir des solutions sans contact. Les cartes à Proximité ne peuvent être lues qu'à partir de 10 cm, elle est conforme à la norme ISO 14443 et

également la base de la norme NFC. Étiquettes RFID ou étiquettes de voisinage dédiées à l'identification des objets a une distance de lecture pouvant atteindre 7 à 8 mètres. [2]

- Z-Wave est une technologie de communication fiable, à faible puissance, à un coût peu élevé, qui vise la communication à courte distance, particulièrement à l'application de contrôle à distance dans une résidence. Grâce à la pile de protocole légère et au format des trames à compression, Z-Wave a une consommation extrêmement faible d'énergie ; la topologie Mesh permet aux appareils de s'échanger l'information ; puisque Z-Wave n'est pas conçu pour transférer une grande quantité de données, sa bande et portée lui permettent de fonctionner très faible puissance ; Z-Wave a moins de possibilité d'interférence avec les autres dispositifs sans-fil [14]

3.2. Comparaison

La conception et les exigences de notre système conduisent à une considération spécifique quant aux technologies de communication. Ils ont leurs propres caractéristiques et avantages, qui conviennent à divers scénarios. Une comparaison de ces technologies est abordée dans cette section, afin d'aider le consommateur à faire des choix judicieux quant à la mise en place du système.

	NFC / RFID	Bluetooth	Z-Wave	ZigBee
Standard/Protocol	ISO 13157	IEEE 802.1.5.1	Z-Wave	ZigBee
Fréquence	13,56MHz	2,4GHz	908M/ 860MHz	868MHz/ 915MHz/ 2,4GHz
Débit de donnée	424Kbps	1Mbps	40Kbps	20Kbps/ 40Kbps/ 250Kbps
Portés	<20 cm	100m	30m	10-100m
Topologie	/	Etoile	Maillé	Maillé/Etoile
Consommation d'énergie	faible	faible	faible	faible
Sécurité	Pas avec RFID	chiffrement E0 par flot	AES-128	AES-128
Nœuds	/	8	232	6500

Table 1 Comparaison des technologies de communication [15]

En résumé, les différentes caractéristiques des quatre réseaux les rendent appropriés selon diverses situations. Dans notre cas, l'objectif de recherche est la mise en place des technologies de communication approprié. Selon les performances des technologies qui ont été abordées ci-dessus, ZigBee pourrait être le meilleur choix pour le contrôle et la surveillance dans le système, car il est relativement facile à implanter et à développer ; la faible consommation d ' énergie convient aux dispositifs avec une source de batterie ; d'ailleurs, il soutient une grande quantité de nœuds.

Pour la technologie utilisée sur mobile, NFC et Bluetooth sont deux technologies de communication relativement courte portée disponibles sur les téléphones mobiles. La technologie NFC fonctionne à des vitesses plus faibles que Bluetooth, le point fort est qu'elle a une portée beaucoup courte qui rendra difficile les attaques physiques, et consomme beaucoup moins d'énergie et ne nécessite pas d'appairage. [37]

Dans ce document, nous nous concentrons sur la technologie ZigBee qui vise à réduire le coût de consommation de l'objet connecté et le NFC qui vise à faciliter les accès du client.

3.3. ZigBee

3.3.1. Définition du ZigBee

ZigBee est une technologie de réseau sans fil développée par ZigBee Alliance pour les applications à faible débit de données et à courte portée. La pile ZigBee protocole est composée de quatre couches principales : la couche physique (PHY), la couche de contrôle d'accès (MAC), la couche réseau (NWK) et la couche application (APL). De plus, ZigBee fournit des fonctionnalités de sécurité sur plusieurs niveaux (Fig. 5). Les deux couches inférieures de la pile ZigBee protocole sont définies par la norme IEEE 802.15.4, tandis que le reste de la pile est défini par la spécification ZigBee.

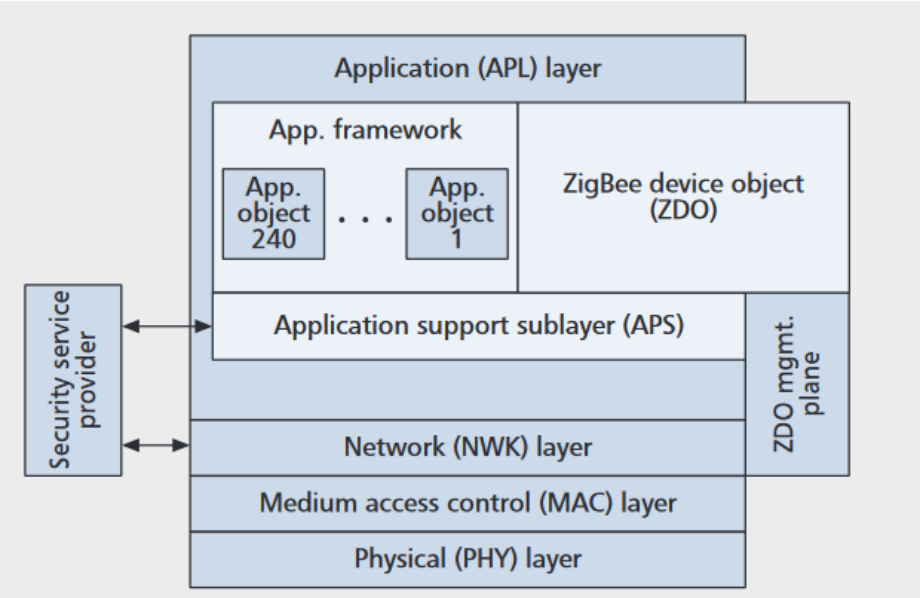


Figure 5 La structure du protocole ZigBee [21]

Les débits de données sont respectivement de 20 kb / s, 40 kb / s et 250 kb / s. La modulation par décalage de phase binaire (BPSK) est utilisée dans les deux premières bandes et la modulation par décalage de phase orthogonale en quadrature (O-QPSK) est utilisée pour les signaux à 2,4 GHz. Ces mécanismes de communication sont combinés avec le spectre étalé à séquence directe (DSSS). [16]

La couche ZigBee NWK prend spécifiquement en charge l'adressage et le routage pour les topologies arborescentes et maillées. La topologie de l'arborescence, qui convient à la collecte de données, est enracinée au niveau du coordinateur ZigBee. Ce schéma comprend un mécanisme d'attribution d'adresses, ce qui facilite également la transmission de données multiples. Dans une topologie maillée, les routes sont créées à la demande et gérées à l'aide d'un ensemble de mécanismes basés sur le protocole de routage ad hoc sur vecteur de distance (AODV). Cette solution est utilisée pour un trafic arbitraire de point à point. La solution ZigBee PRO propose également un routage multiple pour la communication entre plusieurs périphériques et un contrôleur central ou un nœud récepteur. Ce nœud peut répondre aux périphériques à l'aide de routage source. Seuls les coordinateurs ZigBee et les routeurs participent aux opérations de routage. [17] [18]

3.3.2. ZigBee 3.0

Zigbee 3.0 augmente le choix et la flexibilité offerts aux utilisateurs et aux développeurs, et garantit que les produits et les services fonctionneront ensemble grâce à la normalisation à tous les niveaux de la pile. La solution Zigbee 3.0 inclut des tests, une certification, une stratégie de marque et un support marketing facilitant le développement et la vente de produits et solutions interopérables. Il ouvre des

opportunités de croissance tout en favorisant l'innovation pour permettre de nouvelles fonctionnalités à la maison, au travail et sur la route.

Zigbee 3.0 est basé sur Zigbee PRO, qui améliore la norme IEEE 802.15.4 en ajoutant des couches de réseau maillé et de sécurité, ainsi qu'un cadre applicatif, pour devenir une solution Zigbee empilable, de faible puissance, certifiée et interopérable. [19]

3.3.3. Caractéristiques du protocole ZigBee

Les trois premières couches (PHY, MAC, et NWK) s'occupent de la création et de l'entretien du réseau, elles garantissent théoriquement le débit de transmission de données jusqu'à 250kbps. La couche d'application est responsable de la communication entre les dispositifs, par exemple, pour envoyer une commande ou demander une information. Le réseau de ZigBee supporte différentes topologies, le réseau en étoile, en pair à pair, et maillé. Trois types de nœuds peuvent exister dans un réseau ZigBee :

1) Coordinateur, qui s'occupe de la création et du contrôle de réseau. Les informations des autres nœuds (adresse, données recueillies ...) sont stockées et échangées par le coordinateur ;

2) Routeur, le routeur est capable de se connecter au coordinateur et aux autres routeurs, ainsi qu'aux appareils. Il sert à transmettre les informations reçues afin d'étendre le réseau. Par rapport au coordinateur, le routeur n'a pas la capacité de créer un réseau et leurs principales fonctions sont similaires.

3) Le périphérique terminal ZigBee Ce dernier est normalement un périphérique simple. Avec des capacités très faibles de transmission de données au capteur, c'est-à-dire un appareil qui doit se connecter soit avec le coordinateur soit avec routeur [20], [21]

3.3.4. Architecture de sécurité

Zigbee utilise des AES avec des clés 128 bits pour mettre en œuvre ses mécanismes de sécurité. Une clé peut être associée soit à un réseau, utilisable à la fois par les couches Zigbee et la sous-couche MAC, soit à une liaison, acquise par pré-installation, accord ou transport. L'établissement des clés de liaison est basé sur une clé principale qui contrôle la correspondance des clés de liaison. Enfin, au moins, la clé principale initiale doit être obtenue via un support sécurisé (transport ou pré-installation), car la sécurité de l'ensemble du réseau en dépend.

La distribution de clés est l'une des fonctions de sécurité les plus importantes du réseau. Un réseau sécurisé désignera un périphérique spécial auquel les autres périphériques font confiance pour la distribution des clés de sécurité : le centre de confiance.

Idéalement, l'adresse de confiance du centre et la clé principale initiale seront préchargées sur les appareils. Si une vulnérabilité momentanée est autorisée, elle sera envoyée comme décrit ci-dessus. Les applications types ne nécessitant pas de sécurité particulière utilisent une clé réseau fournie par le centre de confiance (via le canal initialement non sécurisé) pour communiquer. [22] [23]

3.4. Technologie NFC

La communication en champ proche NFC (Near Field Communication) est une technologie de communication sans contact basée sur un champ de radiofréquence (RF) utilisant une fréquence de base de 13,56 MHz. La technologie NFC est parfaitement conçue pour échanger des données entre deux appareils par un simple geste tactile.

Le champ RF généré par un dispositif de forum NFC pour communiquer avec une balise de forum NFC a trois tâches :

- Pour transférer l'alimentation du périphérique Forum NFC au tag Forum NFC. Par conséquent, les tags de forum NFC n'ont pas besoin de piles ni d'autres sources d'alimentation pour fonctionner car le champ RF fournit l'énergie nécessaire à la communication. Cette technologie est également idéale pour les petits périphériques IdO faisant office de balise de forum NFC, car aucune alimentation supplémentaire n'est nécessaire pour la communication NFC.
  Pour la charge sans fil, l'objectif principal de la technologie NFC est de transférer l'énergie, ce qui étend la communication. Dans ce cas, la communication NFC est utilisée pour réguler le transfert de puissance. Lorsque le mode de charge sans fil est activé, il est possible d'augmenter l'intensité du champ RF, permettant ainsi un transfert de puissance allant jusqu'à 1 W.

- Le périphérique NFC envoie des informations à une étiquette de forum NFC en modulant le signal de champ RF (modulation du signal).

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

Figure 6 Démarche NFC [31]

La technologie NFC est conçue pour une distance de fonctionnement de quelques centimètres. Il est donc plus difficile pour les attaquants d'enregistrer la communication entre un périphérique Forum NFC et une étiquette de forum NFC par rapport à d'autres technologies sans fil permettant une distance de travail de plusieurs mètres. De plus, l'utilisateur du dispositif de forum NFC détermine par le geste de geste quelle entité doit avoir lieu la communication NFC, ce qui rend plus difficile la connexion de l'attaquant. Par conséquent, le niveau de sécurité de la communication NFC est par défaut supérieur à celui des autres protocoles de communication sans fil. De plus, le forum NFC a ajouté la communication d'égal à égal, qui permet de chiffrer toutes les données échangées afin d'éviter qu'un espion puisse interpréter une communication enregistrée. [24]

3.4.1. Le format Background

NDEF est le standard d’échange pour une carte NFC pouvant contenir 4096 bytes données. Grâce à cette norme, les appareils dotés de la technologie NFC peuvent lire rapidement le contenu de la balise NFC. Les informations contenues dans le tag NFC n’ont pas besoin d’être complexe, mais un segment de site Web ou un numéro de téléphone suffira à transmettre les informations aux utilisateurs. Pour la technologie NFC, il suffit aux utilisateurs de « contacter » le mobile avec le tag NFC pour lire directement les informations contenues dans le tag. C'est relativement pratique. L’application de la technologie NFC peut être divisée en " Mode de réglage de scénario ", "Lecture et édition de balises NFC" et "Transmission de données". En outre, la technologie NFC permet au mobile de transmettre directement des fichiers mutuellement. Les mobiles n'ont besoin que de démarrer la fonction de détection NFC pour transmettre ses données à un autre mobile NFC, ce qui simplifie considérablement le processus de correspondance complexe dans le passé et rend la transmission de données entre véhicules plus pratique.

4. Sécurité et vie privée dans l'IdO

4.1. L'internet des Objets : vulnérabilités et menaces

« The National Intelligence Council (NIC) » considère que les avancées technologiques combinées à une forte demande des marchés encourageraient une adoption et un déploiement à large échelle de l'IdO. Néanmoins, la plus grande crainte est que les objets du quotidien deviennent des risques potentiels d'attaque de sécurité. Pire encore, la pénétration à large échelle de l'IdO diffuserait ces menaces d'une façon beaucoup plus large que l'Internet d'aujourd'hui [25].

4.1.1 Amplification des menaces sur les données et les réseaux

L'omniprésence des objets communicants dépourvus de protection physique et de surveillance, les rendent une proie facile aux attaques matérielles et logicielles. Ces objets peuvent être volés, corrompus et contrefaits. Sans mesures particulières, les données stockées sur ces dispositifs seraient alors accessibles, y compris des données cryptographiques qui permettraient d'accéder à d'autres données sensibles ou jouer des rôles sensibles dans les systèmes complexes les hébergeant. Par ailleurs, les transmissions sans fil, sont à leur tour une proie facile à l'écoute et au déni de service (« jamming » [26] [27]). Il existe aujourd'hui des solutions cryptographiques pour assurer des services de confidentialité, de contrôle d'intégrité, d'authentification, de non-répudiation, etc. mais beaucoup reste à faire pour rendre ces algorithmes efficaces et performants sur des dispositifs embarqués de plus en plus miniaturisés. Le CERP-IdO cite dans [28] quelques problématiques amplifiées par la nature des objets embarqués miniaturisés. On cite notamment : l'hétérogénéité et la mobilité des objets qui rajoutent une couche de complexité aux problèmes de sécurité.

4.1.2 Menaces sur la vie privée

Tous les pronostics envisagent le développement d'un informatique personnel avec potentiellement des dizaines d'objets par personne y compris dans leur sphère privée et intime. Ces objets de l'espace personnel sont géolocalisables, peuvent communiquer avec d'autres objets à travers des réseaux spontanés, peuvent écouter ce que dit la personne, peuvent filmer la personne et/ou son environnement, et peuvent même enregistrer son rythme cardiaque, son rythme respiratoire, la température de son corps, et sa cinématique ! Des questions légitimes se posent sur le devenir de cette masse de données personnelles et parfois intimes. Sans régulation stricte, une protection accrue de la vie privée, un degré élevé de contrôle des objets par les usagers, l'adoption de l'IdO serait un échec. L'ITU dans son rapport sur l'Internet des Objets [29] a pointé du doigt ces menaces potentielles. Elle conclue que la protection de la vie privée ne doit pas se limiter à des solutions technologiques, mais doit comprendre des mesures juridiques, une régulation du marché et des considérations socio-éthique.

4.1.3. Menaces sur les données et les réseaux

Le manque de surveillance et de protection physique des objets communicants peut engendres des attaques potentielles portées sur le matérielle telles que le vol, la corruption ou la contrefaçon de ces derniers pour récupération des données qui sont stockées sur ces dispositifs ou pour interrompre le bon fonctionnement des réseaux ou les systèmes complexes les hébergent. De plus, les transmissions sans fil sont réputées par leur forte vulnérabilité aux attaques de l'écoute passive et de déni de service. Les solutions cryptographiques existantes aujourd'hui ne sont pas adéquates pour tenir faces à ces problèmes cités à cause de la limitation de ressources des objets communicants, de ce fait, l'adaptation de ces dernières ou la conception de nouveaux modèles est une nécessité afin d'assurer les services de sécurité [1].

4.1.4. Menaces sur les systèmes et l'environnement physique des objets

Des objets malicieux connectés à un réseau ou intégrés dans un système complexe peuvent causer un dysfonctionnement quelconque, un déni de service ou autres types d'attaques à l'intégrité des données et les informations sensibles du système, ou pire encore prendre le contrôle du système en causant des importants dégâts [30].

4.1.5. La sécurité

Définition des objectifs de la sécurité

La sécurité informatique d'une manière générale consiste à assurer que les ressources matérielles et logicielles d'une organisation sont uniquement dans le cadre prévu. Elle vise à assurer plusieurs objectifs, dont les cinq principaux sont : l'authentification, confidentialité, l'intégrité, la disponibilité et la non-répudiation [30], [31].

a) 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 pouvait pas fournir les objectifs de sécurité mentionnée de manière satisfaisante [32].

b) Confidentialité

Ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données [32].

c) Intégrité

L'intégrité peut être vue comme un ensemble de mesures garantissant la protection des données contre les modifications et les altérations non autorisées. L'objectif des attaques sur l'intégrité est de changer, D'ajouter ou supprimer des informations ou des ressources [32].

d) Disponibilité

La disponibilité est un service réseau qui donne une assurance aux entités autorisées d'accéder aux ressources réseaux avec une qualité de service adéquate. L'objectif des attaques sur la disponibilité est rendre le système inexploitable ou inutilisable [32].

e) Non-répudiation

Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire, c'est-à-dire les correspondants ne pourront pas nier ni l'envoi ou ni la réception du message [32], [31].

4.2. Contrôle d’accès

Généralement, la sécurité informatique vise trois principaux objectifs : l’intégrité, la confidentialité et la disponibilité des données. L’intégrité permet de déterminer si les données n’ont pas été altérées que ce soit de manière accidentelle ou intentionnelle. La confidentialité consiste à assurer que seules les personnes autorisées aient accès aux ressources protégés. La disponibilité permet de garantir l’accès aux informations et services. Pour assurer la sécurité informatique, plusieurs techniques sont employées dont le contrôle d’accès.

4.2.1. Définition

Le contrôle d'accès logique est un système de contrôle d'accès à un système d'information. Il est souvent couplé avec le contrôle d’accès physique et permet de restreindre le nombre d’utilisateurs du système d’information.

4.2. Modèles

Depuis les années 1960 le modèle du contrôle d'accès a évolué dû à des besoins initiaux dans les domaines aussi bien militaires que civils. Le domaine militaire nécessite un contrôle d’accès dû principalement aux nombreuses données confidentielles qu'il peut contenir. Le domaine civil quant à lui se limite au contrôle des intégrités.

A partir des années 1970, beaucoup de modèles de contrôle d’accès ont été mis en place. Parmi eux les modèles DAC, MAC, ABAC et OrBAC.

a) Contrôle d’accès discrétionnaire (DAC)

Le contrôle d’accès discrétionnaire est une Stratégie de contrôle d'accès appliquée à tous les sujets et objets d'un système d'information, spécifiant à un sujet à qui l'accès à l'information a été autorisé peut effectuer une ou plusieurs des opérations suivantes: (i) transmettre l'information à d'autres sujets ou objets ; (ii) accorder ses privilèges à d'autres sujets ; (iii) modifier les attributs de sécurité sur des sujets, objets, systèmes d'information ou composants du système; (iv) choisir les attributs de sécurité à associer aux objets nouvellement créés ou révisés; ou (v) modifier les règles régissant le contrôle d'accès. [38] [33]

b) Contrôle d’accès obligatoire (MAC)

Le contrôle d'accès obligatoire est une méthode permettant de limiter l'accès aux ressources en fonction de la sensibilité des informations contenues dans la ressource et de l'autorisation donnée à l'utilisateur d'accéder aux informations avec ce niveau de sensibilité.

La sensibilité de la ressource sera définie à l'aide d'une étiquette de sécurité. L'étiquette de sécurité est composée d'un niveau de sécurité et de zéro ou plusieurs catégories de sécurité. Le niveau de sécurité indique un niveau ou une classification hiérarchique des informations (restreint, confidentiel ou interne, par exemple). La catégorie de sécurité définit la catégorie ou le groupe auquel les informations appartiennent (telles que le projet A ou le projet B). Les utilisateurs ne peuvent accéder qu'aux informations d'une ressource à laquelle leurs étiquettes de sécurité leur donnent droit. Si l'étiquette de sécurité de l'utilisateur ne dispose pas de suffisamment d'autorité, l'utilisateur ne peut pas accéder aux informations de la ressource. [34]

c) Contrôle d'accès basé sur les attributs (ABAC)

ACL et RBAC sont à certains égards des cas particuliers d’ABAC en termes d’attributs utilisés. Les ACL travaillent sur l'attribut « identité ». RBAC travaille sur l'attribut de "rôle". La principale différence avec ABAC est le concept de stratégies qui expriment un ensemble de règles booléennes complexes pouvant évaluer de nombreux attributs [35] [36]

d) Contrôle d'accès organisationnel (ORBAC)

En matière de sécurité informatique, le contrôle d'accès basé sur l'organisation (OrBAC) est un modèle de contrôle d'accès présenté pour la première fois en 2003. Les approches actuelles du contrôle d'accès reposent sur les trois entités (sujet, action, objet) permettant de contrôler l'accès à la stratégie. Le sujet a la permission de réaliser une action sur un objet.

OrBAC 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.
- Et 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. [37]

4.3. Système de sécurité légère pour IdO

4.3.1. L'infrastructure à clé publique (PKI)

L'infrastructure à clé publique (ICP) est un mécanisme efficace pour établir la confiance et assurer la confidentialité, l'intégrité et l'authenticité de partenaires afin de sécuriser les transactions sur Internet. Technologie de sécurité complète, stratégies et relations définies utilisant la cryptographie et des normes pour permettre aux utilisateurs :

- De s'identifier (authentifier) eux-mêmes sur les services réseau, les stratégies d'accès et les uns des autres afin de prouver leur source et leur origine; c'est-à-dire que les ressources ne sont mises à la disposition que des personnes autorisées à y accéder;
- Signer numériquement des documents électroniques, des courriels et d'autres données pour fournir des autorisations et prouver l'intégrité ;
- Cryptez les courriels, données et autres documents pour empêcher tout accès non autorisé et assurer la confidentialité.
- Les praticiens de la sécurité décrivent les services ci-dessus comme étant la CIA, c'est-à-dire la confidentialité, l'intégrité et la disponibilité. [38]

a) Technique

Une infrastructure à clé publique utilise des mécanismes de signature et certifie des clés publiques qui permettent de chiffrer et de signer des messages ainsi que des flux de données, afin d'assurer la confidentialité, l'authentification, l'intégrité et la non-répudiation.

Une infrastructure PKI fournit donc quatre services principaux :

- Fabrication de bi-clés.
- Certification de clé publique et publication de certificats.
- Révocation de certificats.
- Gestion la fonction de certification.

- Signature

Dans la signature il se trouve une bi-clé : une clé (privé) pour la création de signature et une clé (publique) pour la vérification de signature, pour signer un message voici comment se passe :

1) À l'aide de la clé privée de signature de l'expéditeur, une empreinte connue sous le nom "message digest" est générée par hachage en utilisant l'algorithme SHA-1 ou MD5, le plus utilisé étant SHA-1. Cette empreinte est ensuite cryptée avec cette clé privée de signature.

2) On joint au message l'empreinte et le certificat contenant la clé publique de signature.

3) Le destinataire vérifie la validité du certificat et sa non révocation dans l'annuaire.

4) Le destinataire transforme l'empreinte grâce la clé publique de signature ainsi validée. Cette opération permet de s'assurer de l'identité de l'expéditeur.

5) Ensuite le destinataire génère une empreinte à partir de message reçu en utilisant le même algorithme de hachage. Si les deux empreintes sont identiques, cela signifie que le message n'a pas été modifié.

   Donc la signature vérifie bien l'intégrité du message ainsi que l'identité de l'expéditeur.

Exemples d'algorithme de signature : RSA, DSA

- Chiffrement

Il y a deux types de chiffrement possible :

- **Chiffrement à clé secrète (symétrique) :**

  L'émetteur utilise une clé pour chiffrer le message et le destinataire utilise la même clé (le même algorithme mais en sens inverse) pour déchiffrer le message.

- **Chiffrement à clé publique (asymétrique) :**

  Un message chiffré avec une clé publique donnée ne peut être déchiffré qu'avec la clé privée correspondante.

  Par exemple si A souhaite envoyer un message chiffré à B, il le chiffrera en utilisant la clé publique de B (qui peut être publié dans l'annuaire). La seule personne qui déchiffre le message est le détenteur de la clé privée de B.

Exemples d'algorithme de chiffrement :

- Symétrique : DES ; AES
- Asymétrique : RSA

a) Organisation d'une PKI

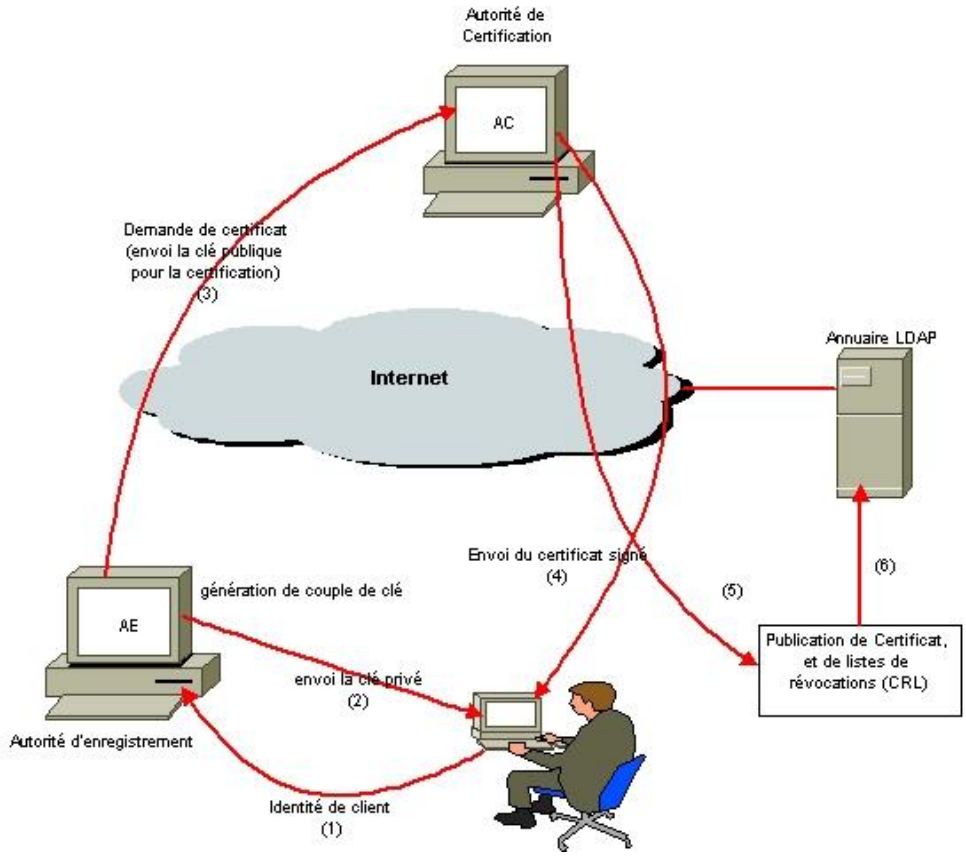


Figure 7 Organisation d'une PKI [39]

Après qu'un utilisateur se soit identifié à l'autorité AE, l'AE lui envoie la clé privée et envoie la clé publique à l'autorité de certification CA. Pour que ce lui la, puisse envoyer le certificat signé à l'utilisateur et mettre à jour la liste de révocation CRL sur l'annuaire.

b) La technologie PKI / CA

La technologie PKI / CA basée sur les certificats numériques crypte et décrypte la transmission d'informations sur le réseau, les signatures numériques et la vérification de signatures. Cela permet également de garantir que les informations n'ont pas été falsifiées au cours de la transmission, à moins que l'émetteur et le destinataire eux-mêmes ne soient volés par d'autres personnes. L'expéditeur confirme l'identité du destinataire par le biais de certificats numériques, mais également pour s'assurer que l'expéditeur ne peut pas refuser ses propres messages envoyés. Par conséquent, nous pouvons envisager d'utiliser le principe de la technologie PKI qui est largement utilisée sur Internet pour protéger la sécurité des transmissions de l'information et certification dans l'Internet des objets. [39]

4.3.2. Token de sécurité

Un token de sécurité est un type d'informations d'identification qui contient des informations relatives au sujet de l'identité. Un token est décrit comme "un ensemble de revendications". "revendication" fait référence à certains biens que le sujet concerné prétend avoir, par exemple un nom ou un rôle. Il existe différents types de token de sécurité : tokens X509 (certificat), Username Tokens (un nom d'utilisateur), token XML (Token personnalisés), tickets Kerberos ... Chacun de ces token peut être ajouté à une socket et envoyé à un noeud final, où le token peut être utilisé pour prouver l'identité d'un utilisateur. D'autres parties de la socket peuvent faire référence au token en utilisant une référence token. Les tokens peuvent également être envoyés sous forme de données cryptées.

Comparés les uns aux autres, les types de tokens contiennent différents types d'informations. Un nom d'utilisateur (avec un mot de passe) peut être utilisé à des fins d'authentification dans plusieurs types de services. Un certificat peut être utilisé pour vérifier une identité ou une signature. La clé publique du certificat peut être utilisée pour chiffrer un message. Un token peut contenir des informations plus spécifiques. Ces informations peuvent être personnelles (nom, profession, adresse, etc.) ou techniques (droits d'accès ou rôle). Par conséquent, le token peut être utilisé pour transporter des informations sur un sujet, ou les informations peuvent être utilisées dans un contexte approprié. Cependant, grâce à des extensions, un certificat peut être créé pour contenir des faits similaires. [40]

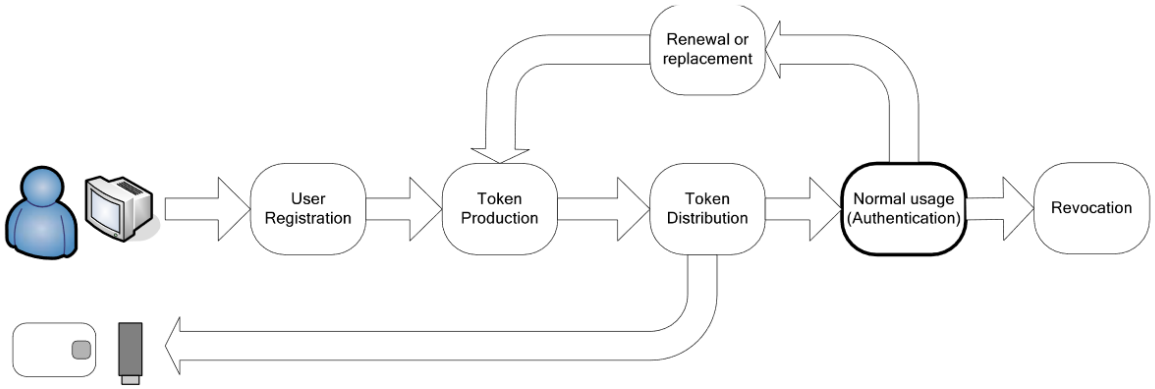


Figure 8 Processus du cycle de vie d'un token [46]

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 un cycle qui commence par la production du token, ça distribution et son usage. Ensuite le cas où il y a un renouvèlement d'identité qui revient à l'étape de production, ou en fin de cycle de vie avec suppression.

4.3.3. Authentification légère basée sur des Tokens pour la sécurité réseaux IdO

La prolifération de l'Internet des objets dépense dans de nombreux aspects de notre style de vie, la prochaine frontière est l'environnement de l'industrie numérique (par exemple, ville intelligente, hôtel intelligent, bureau intelligent). Bien que l'avenir de l'industrie intelligente soit beaucoup plus prometteur, il faut relever les défis techniques pour atteindre commodité et sécurité. Plus précisément, alléger à l'utilisateur l'authentification pour le système de réservation a été un problème critique en raison de la communication entre l'utilisateur et les appareils intelligents qui est limité dans le temps. La raison est que les utilisateurs peuvent vouloir réserver une liste d'appareils intelligents pour établir des communications pour une période de temps. Pour cela, il est important d'authentifier la légitimité d'un utilisateur pour un intervalle de temps prédéfinie. Dans ce contexte, les tokens ont été introduits en tant que solution efficace pour créer un lien fort entre les utilisateurs qui a 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, et il ne nécessite pas beaucoup plus d'effort de l'utilisateur qu'un mécanisme basé sur un mot de passe. [0]

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 canaux de communication non sécurisés et les utilisateurs illégaux (attaquant) 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.

Les points fort du protocole TBLUA (Token Based Light User Authentification) :

- Génère une couche de sécurité supplémentaire d'authentification en adoptant la technique du token qui donne accès à une ressource spécifique pour période de temps prédéfinie.
- Réduit les coûts de calcul et économise de l'énergie pour authentifier les appareils lors de la session d'authentification, en utilisant uniquement des opérations de calcul légères telles comme XOR et fonction de hachage.
- Est conçu pour résister aux plus populaire attaques et assure les propriétés de sécurité.

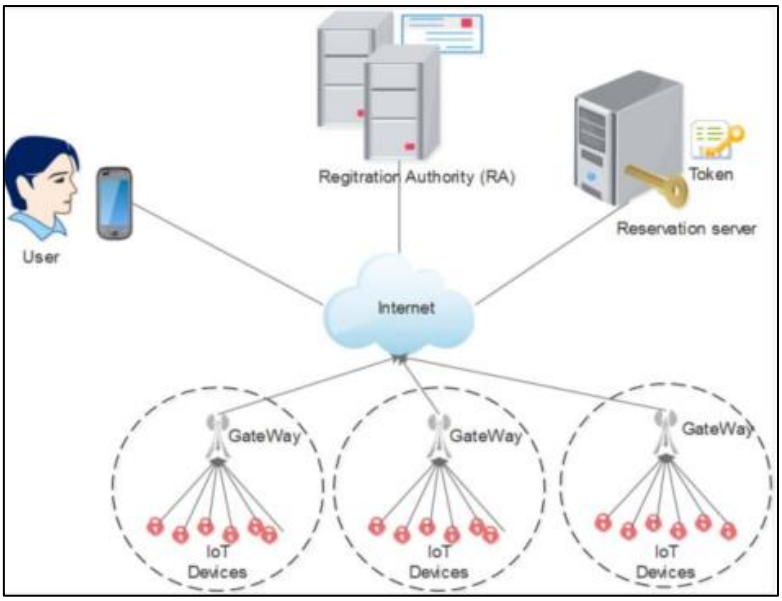


Figure 9 Model de réseaux [0]

a) Modèle de réseau et de menace

Nous présentons le modèle de réseau qui est illustré à la Fig. 9. Notre modèle est composé de l'utilisateur final (U) qui doit s'inscrire à la réservation de confiance Serveur (RS) pour communiquer avec Smart Devices (SD). (RS) est responsable de la génération des jetons de réservation pour (U) et la distribution de l'autorité d'enregistrement (RA). Ce dernier est responsable de l'enregistrement de tous les appareils intelligents et passerelle (GW) en toute sécurité. De plus, nous supposons que tous les appareils hétérogènes sont synchronisés avec leurs horloges et convenir d'un délai de transmission maximal (ΔT) pour protéger nos schémas contre les attaques par rejeu. Deux parties communicantes (U, SD) interagissent sur un canal non sécurisé et ils ne sont pas considéré comme digne de confiance. Un adversaire (A), peut écoutez les messages échangés et modifiés ou supprimés les messages pendant la transmission. De plus, (SD) ne sont pas sur et donc, ils peuvent être physiquement compromis par (A). De plus, le téléphone intelligent (SP) de l'utilisateur peut être perdu / volé par (A). Par conséquent, (A) peut extraire des données sensibles. Néanmoins, nous supposons que le (GW) dans le schéma proposé est un nœud de confiance et n'est pas compromis en aucune circonstance ; sinon, le réseau est compromis. En outre, (RA) et (RS) sont des serveurs fiables et ne peuvent pas être compromit par un adversaire. [0]

b) Etapes de du protocole TBLUA

TBLUA se compose de plusieurs étapes d'authentification et protocole de négociation de clé pour sécuriser les données transmis après une réservation réussie.

Le protocole d'authentification comprend quatre phases suivantes :

(i) Enregistrement de périphérique intelligent et de GW hors ligne.

(ii) La réservation de l'utilisateur.

(iii) Répartition des Tokens entre GW et dispositifs intelligent.

(iv) Connexion et authentification.

4.4. Aspect Utilisateur

La technologie a pour vocation première de simplifier la vie de l'homme. A priori, elle est à son service. Pourtant, depuis la nuit des temps, l'homme entretient avec elle un rapport ambigu. Fasciné par les progrès et la modernité qu'elle symbolise, effrayé par ses possibles dérives. « La technologie a un caractère magique. Tant qu'il n'y a pas eu d'expérience, ils projettent sur elle des scénarios du futur, des scénarios de science-fiction », analyse Christophe Rebours, fondateur de l'agence de 'processus de design'. Et si plus personne ne souhaite revenir à l'âge de pierre, un temps d'adaptions mutuelle est nécessaire pour que l'homme retrouve le sentiment de dominer la technologie.

Les téléphones intelligents sont l'une des tendances les plus récentes de la nouvelle ère informatique. Les smartphones se caractérisent par le fait qu'ils possèdent deux fonctionnalités essentielles ; être multimodal, conscient de son emplacement et disposer d'une plate-forme de développement. La multi modalité a pour objectif essentiel de maintenir le périphérique connecté en permanence grâce à une combinaison de connexions différentes. Ces fonctionnalités permettent à l'appareil de basculer entre la 4G, le Wi-Fi et Bluetooth en fonction du contexte et de la situation. Les smartphones deviennent également plus puissants que les téléphones mobiles précédents. Les derniers téléphones intelligents utilisent un processeur de haute technologie. En raison de cette installation informatique de grande puissance, c'est pourquoi le choix du développement d'une application mobile a été un choix essentiel à notre système pour garantir la portabilité et la facilité d'utilisation, car comme décrit ci-dessus, le téléphone portable est un quotidien à l'homme. Il reste que ces appareils restent non fiable à cent pour cent. [41]

5. Conclusion

Dans ce premier chapitre, nous avons définis l'IdO, parlé de l'architecture de l'IdO, cité ses technologies, ses composantes et quelques protocoles de fonctionnement, cité les axes de recherche et décrit en détail dans cette partie les menaces et les vulnérabilités relatives à son déploiement. Ainsi, nous avons étudié le concept contrôle d'accès afin de pouvoir limiter les vulnérabilités. L'introduction de diffèrent technique de sécurité. Enfin, Survolé l'interaction avec l'utilisateur.

Le prochain chapitre portera sur l'analyse des besoins nécessaires pour la mise en œuvre d'un système de sécurité léger pour IdO. Dans ce chapitre, nous allons passer à la phase de conception qui consiste à élaborer l'architecture du système.

CHAPITRE II : ANALYSE ET CONCEPTION

1. Introduction

Actuellement, le problème de contrôle d'accès est très important dans plusieurs applications, le contrôle d'accès physique consiste à vérifier si une entité demande d'accéder aux droits nécessaires pour le faire. Les protocoles de vérification d'identité qui permettent l'accès s'appellent les protocoles d'authentification.

Au cours de ce deuxième Chapitre, nous allons expliquer l'essentiel de notre travail. Nous allons expliquer en détail les besoins nécessaires pour la mise en œuvre de notre système de Sécurité Léger.

Ce chapitre est divisé en trois parties, la première sera consacrée à la présentation, notre cas d'étude, les démarche à suivre et les objectifs à atteindre. Ensuite, la deuxième partie, qui est la vision générale de notre système, l'analyse des besoins du système, les principaux acteurs et les cas d'utilisation. Enfin, la troisième partie porteras sur une conception spécifique de chaque entité et comment ses entités communique entre eux.

2. Hôtel intelligent cas d'étude

Notre principal objectif est la conception d'un schéma/architecture pour le contrôle d'accès basé sur le contexte avec des stratégies de sécurité spécifiques afin de fournir des clés numérique/Tokens pour donner/retirer l'accès aux ressources numériques/physiques dans le cadre de l'Internet des objets (IdO). En partant de notre cadre hôtel intelligent le choix a été fait, une porte intelligente démontrerait bien l'accès physique. Et donc atteindre une implémentation réaliste d'un scénario démontrant l'utilisation d'une application Android pour accéder en toute sécurité à l'objet qui est notre porte d'hôtel intelligente.

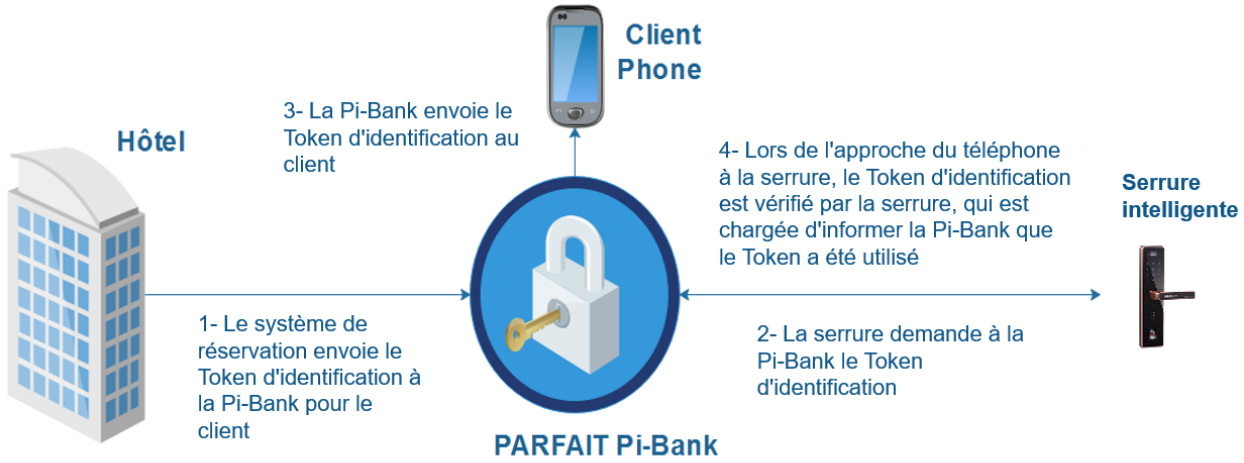


Figure 10 Système PARFAIT Pi-Bank

Le système de gestion des tokens est en fait notre Pi-Bank, Distributeur de token ou précisément le fournisseur d'accès. Le système de réservation de l'hôtel envoie le token d'identification à la Pi-Bank pour le client. Par la suite le verrou demande à la Pi-Bank un token d'identification, la Pi-Bank envoie le token d'identification au client et à la serrure intelligente. Enfin lors de l'approche du téléphone vers la serrure, le token d'identification est vérifié par la serrure, qui est chargée d'informer la Pi-Bank que le token a été utilisé.

2.1. Présentation de la démarche

2.1.1. Cycle semi-itératif

Le cycle semi itératif est une méthode de gestion de projet qui peut être considérait comme une évolution du cycle itératif classique. On distingue deux types de modèle dans un cycle semi-itératif :

- Top down (de haut en bas) : une approche dite descendante fait référence à un style de développement dans lequel une application est construite en commençant par une description très large de ce que l'application est supposée faire, elle est ensuite décomposée en plusieurs spécifications de plus en plus précises et ce jusqu'à atteindre les détails les plus fins.
- Bottom Up (de bas en haut) : une approche dite ascendante contrairement à une approche descendante va elle se baser sur des fonctionnalités très précises que l'on va assembler au fur et à mesure pour venir créer des modules et enfin arrivé à une application très complexe.

En effet, cette méthode Agile est basée sur des phases courtes et itératives. Voici un schéma illustrant ce cycle :

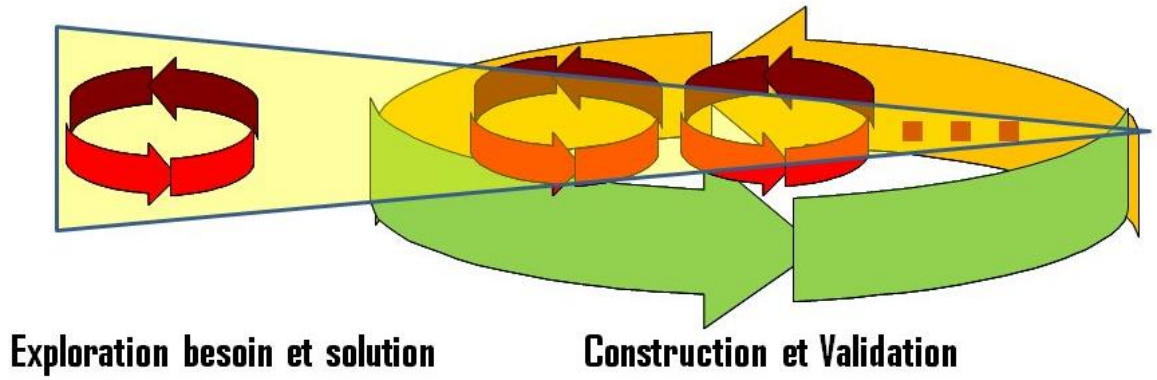


Figure 11 Méthode agile 'Cycle semi-itératif' [42]

Dans le cycle semi-itératif l'on va utiliser la méthode dite 'Top down' lors des phases d'expressions du besoin et de spécification, ce qui va permettre au début d'avoir une belle idée d'ensemble de ce que sera le projet et au fur et à mesure de l'avancement de ces deux étapes d'arriver à des spécifications très précises qui correspondent parfaitement aux besoins du client. Pour ce qui est des autres phases du cycle l'on va choisir la méthode dite 'Bottom Up', car elle apporte de gros avantages en termes de développement et de maintenance ce qui permettra d'aboutir à une solution qui répond aux attentes du client et qui pourra facilement évoluer dans le temps.

Pour rappel le cycle de vie semi-itératif reprend les étapes principales de développement du cycle itératif : [48]

a) L'expression des besoins :

On commence un cycle semi-itératif pas l'étape de l'expression des besoins, c'est durant cette étape que le client ou le commanditaire du projet va préciser ses besoins pour le projet à réaliser.

b) Les spécifications :

La seconde étape du projet est l'étape durant laquelle l'on rédige les spécifications techniques du projet en cours de développement, cette étape a pour but de retranscrire les besoins exprimés par le client ou le commanditaire du projet en langage technique que les développeurs pourront exploiter lors de la réalisation du code, c'est aussi durant cette étape que l'on va choisir les solutions techniques pour la réalisation du projet, les technologies à mettre en place et les langages à utiliser lors des développements à venir.

c) Le développement :

La troisième étape du cycle de type semi-itératif est la phase de développement qui consiste en l'écriture du code ainsi que la mise en place d'une éventuelle infrastructure, que l'on aura définie avant dans l'étape des spécifications.

d) La validation :

La quatrième étape de ce cycle est la phase de validation, cette phase va permettre de dire si le développement réalisé dans l'étape précédente correspond bien aux spécifications techniques ainsi qu'aux attentes du client, des tests unitaires, des tests d'intégrations ainsi que des tests fonctionnels vont être réalisés durant cette étape.

e) L'évaluation :

La cinquième étape de ce cycle est l'étape dite de l'évaluation, qui correspond à une sorte d'état d'avancement du projet pour pouvoir voire les fonctionnalités qui ont été réaliser dans les étapes précédentes et celles qui ne l'on pas était voir abandonné cela nous permettra de mettre en place le reste des fonctionnalités qui restent à développer.

f) Le déploiement :

La sixième étape du cycle de type semi-itératif est l'étape dite du déploiement, qui consiste à la mise à disposition du client ou du commanditaire des livrables qui ont été réaliser à ce jour.

Notre travail se dérouleras comme décrit ci-dessus en cycle semi itératif, une analyse des besoins sera fait avec objectif de trouver une solution, le choix des technologies te techniques utilisés, suivie des essaie de construction qui pour but d'arrivée à la mise en place d'une éventuelle infrastructure, suite à une validation et une évaluation, tout cela en répétant le cycle plusieurs fois. Nous allons démontrer cette méthode sur les sections qui suive.

2.2. Les challenges

Dans notre environnement, certains aspects ne peuvent être négligé de la part d'un client, un principe fondamental est incontournable. Comment assurer le compromis entre : la sécurité et l'efficacité du système

Figure 12 Challenges entre sécurité et efficacité

Tout cela n'est possible que quand certains points ne sont pas oubliés et bien exécuté. La sécurité informatique dépend bien de la résistance du système contre les attaque externe et interne, l'adoption de plusieurs fonctionnalités de sécurité pour pouvoir assurer la discrétion du système dans tout son contexte. L'efficacité du système est un point essentiel qui a pour challenges, le calcule rapide et une communication légère.

3. Conception de l'architecture

C'est durant cette étape que le client du projet va préciser ses besoins pour le projet à réaliser.

3.1. Identification du système

L'acteur principal de notre système est un client qui cherche un hébergement avec une facilité d'accès qui pourra tout faire avec son téléphone intelligent. Ainsi, il peut bénéficier des fonctionnalités offertes par notre système. Notre système sera composé d'objets connectés et du gestionnaire d'objets qui est un serveur.

Voici donc le schéma représentatif du système :

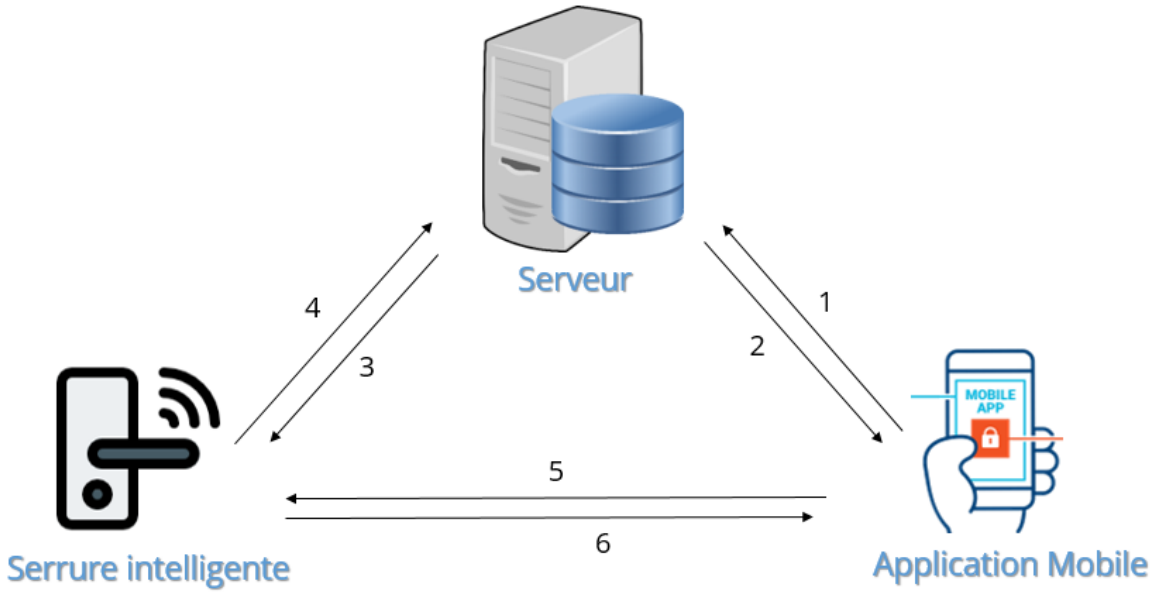


Figure 13 Schéma représentatif de notre système

1- Demande de réservation
2- Envoie du token
3- Envoie list d'accès
4- Envoie Log
5- Demande d'accès
6- Envoie d'autorisation

3.2. Analyse des besoins du système

3.2.1. Identification des exigences fonctionnelles

Les exigences fonctionnelles sont les services offerts par notre système. Ainsi, ils décrivent le comportement de notre système qui peut être classé en des exigences principales :

a) Assurer l'authentification des différents utilisateurs du système.
b) L'opérationnalité des trois entités.
c) Permettre le transfert de données entre les trois entités.
d) Transfert sécurisé.
e) Contrôler, à distance, les objets connectés.
f) Gestion des comptes des utilisateurs.
g) Stockage des données.

3.2.2. Identification des exigences non-fonctionnelles

- La sécurité du système.
- L'efficacité du système.
- Une IHM mobile ergonomique simple.
- Un indicateur de tentative d'accès externe à la porte.

3.3. Vision générale de la solution proposée

La solution à développer adopte un mécanisme de contrôle d'accès sur deux types d'aspects complémentaires : physique et logiciel. Les règles régissant, l'aboutissement et l'échouement seront expliquées par la suite. L'approche est basée également sur la génération de Tokens et la prise en compte d'authenticité de l'utilisateur. Cette application se veut une application client/serveur dont le développement est sous mobile et desktop. Une telle solution nécessite les composants matériels et logiciels suivant :

3.3.1. Besoins matériels

- Microcontrôleeur : Carte Arduino Mega avec alimentation USB.
- Deux Module de connectivité Xbee avec shield Xbee et shield USB.
- Capteur : NFC pour la lecture de la carte à puce.
- Deux LED.
- Fils de connexion.
- Résistances.
- Batterie.
- Gâche électrique.
- Porte miniature en bois.
- Smart phone.
- Serveur Machine sous Windows.
- Réseaux wifi / point d'accès.

3.3.2. Besoins Logiciels

- Arduino IDE.
- XCTU ou Putty.
- Android studio.
- WAMPP.
- BDD MySQL.

3.4. Spécification des fonctionnalités du système

3.4.1. La vue statique du système d'IdO

Identification des acteurs : nous distinguons les acteurs suivants :

- **Administrateur** : Son rôle est de gérer le système. Il possède tous les privilèges d'accès. Il a la possibilité d'utiliser toutes les fonctionnalités du système.
- **Utilisateur** : Il représente un client commun. Cet acteur a des restrictions d'accès au système qui se limite par la consultation de ces données.

3.5. Digramme de cas d'utilisation

Après avoir identifié les exigences majeures garanties par notre système, il est important de les représenter avec des diagrammes de cas d'utilisation. En fait, un diagramme de cas d'utilisation est une technique de modélisation logicielle détermine les fonctionnalités à implémenter dans le système. En outre, il est utilisé pour exprimer les besoins de chaque acteur qui n'a pas de compétences techniques approfondies.

3.5.1. Diagramme de cas d'utilisation global

Notre système doit atteindre son objectif principal tout en respectant les exigences, sans oublier les exigences utilisateurs (non-fonctionnel).

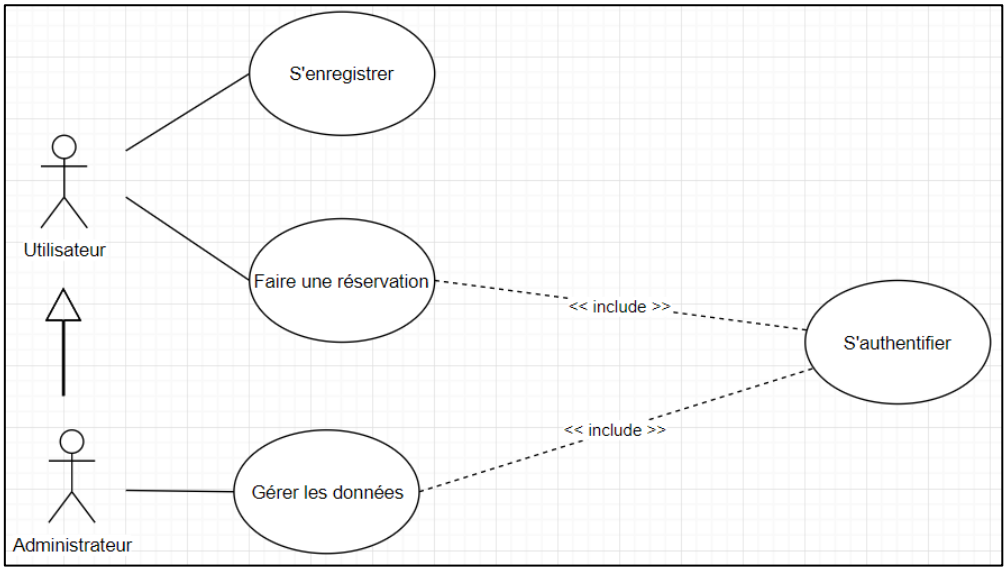


Figure 14 Diagramme de cas général

Notre système offre une caractéristique principale qui consiste à réserver des chambres par le client qui par la suite accédera à la chambre grâce à la serrure intelligente. Ainsi cette action est satisfaite d'une manière qu'une seule réservation est faite pour une date précise, l'utilisateur recevras le token. Il se contentera de rapprocher son appareil mobile à la serrure intelligente de façon que lecteur puisse lire la clé numérique ajouté d'un PIN. Alors que l'administrateur a pour but de gérer les informations du système. Nous présenterons les différentes entités dans les parties suivantes.

3.5.2. Diagramme de cas d'utilisation faire une réservation

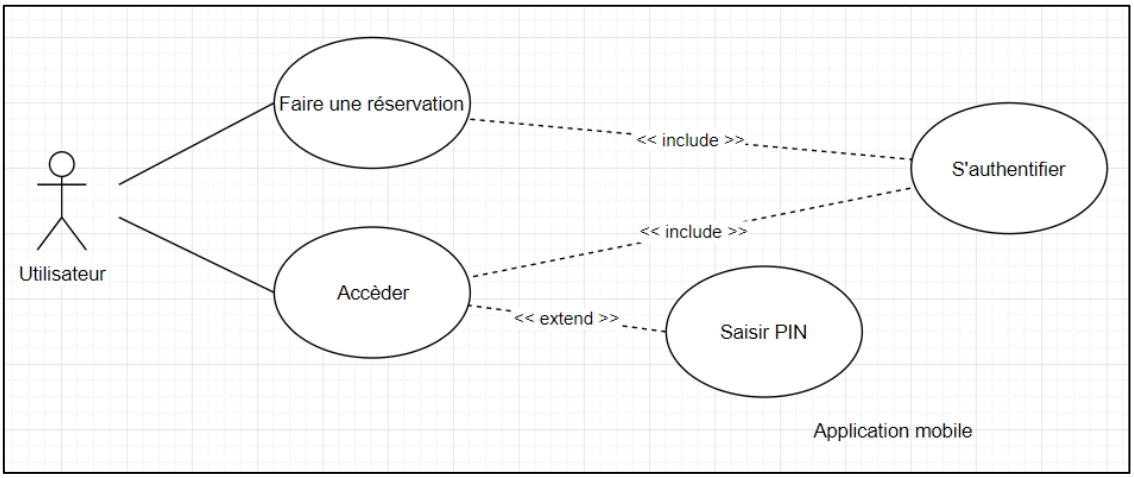


Figure 15 Diagramme de cas faire une réservation

Description textuelle

Cas d'utilisation : faire une réservation

Cas d'utilisation	**Faire une réservation**
Acteurs principaux	utilisateur
Objectif	L'utilisateur peut utiliser l'application mobile pour : – Faire une réservation. – Simuler la carte d'accès
Pré conditions	– La porte connectée est placée et installé dans son environnement. – Connexion wifi. – L'activation du NFC du smartphone. – Lancer l'application. – S'authentifier. – Saisir les informations

Table 2 Faire une réservation

3.5.3. Diagramme de cas d'utilisation gestion des données

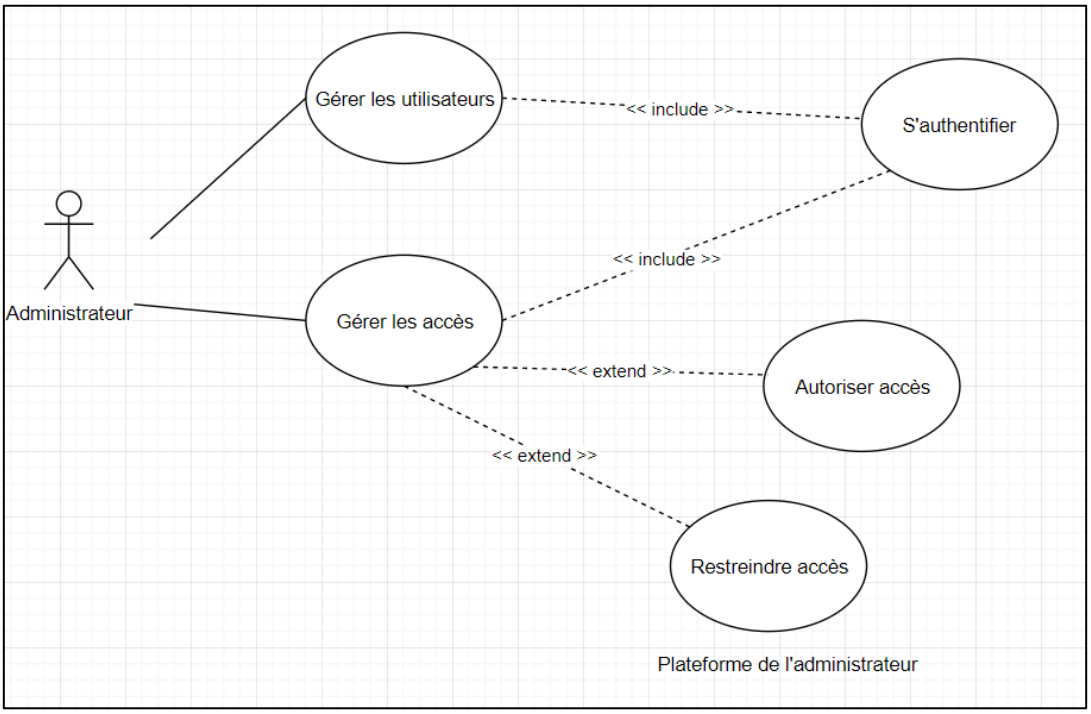


Figure 16 Diagramme de cas gestion des données

Description textuelle

Cas d'utilisation : gestion des données

Cas d'utilisation	**Gestion des données**
Acteurs principaux	administrateur
Objectif	– L'administrateur a le droit de gérer le stockage des données. – Gestion des utilisateurs. – Gestion des accès. – Gestion des chambres.
Pré conditions	– L'objet connecté est bien placé et bien installé dans son environnement. – L'accès au réseau internet. – L'application serveur fonctionne très bien et toujours en écoute. – Lancer l'application serveur. – S'authentifier.

Table 3 Gestion des données

3.6. Diagramme de classe de conception du système

Après avoir réalisé les diagrammes de cas d'utilisation, il est essentiel de représenter maintenant les diagrammes de classe. En fait, un diagramme de classe est une technique de modélisation logicielle détermine concept du système conçu. En outre, il est utilisé pour couvrir l'architecture à implémenter dans le système. [55]

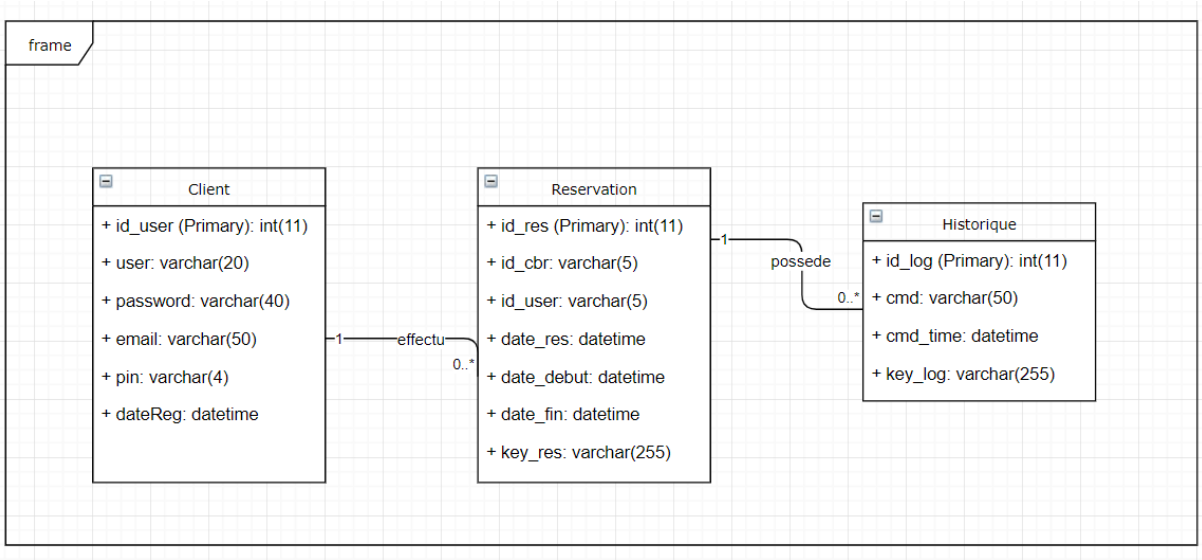


Figure 17 Diagramme de classe système

Classe	**Description**
Client	Représente les clients souhaitant faire des réservations.
Réservation	Représente les réservations faites par les clients.
Log	Représente toutes les tentatives d'accès à la porte intelligente.

Table 4 Description diagramme de classe

Le système contient trois tables, client, réservation et log ; car pour un système complet 'Hôtel' cela est insuffisant. La table client stockera tout individu s'enregistrant sur la plateforme pour utiliser notre service, les réservations sont le point majeur du système, le log est tout fait enregistré, en cas de non répudiation.

3.7. Diagramme d’activité (Accès porte intelligente)

Le diagramme d'activités est composé d’actions et de transitions entre ces actions. Il permet d’exprimer le déroulement et le flot de contrôle interne d’un cas d’utilisation en décrivant le séquencement des activités et leur coordination. [55]

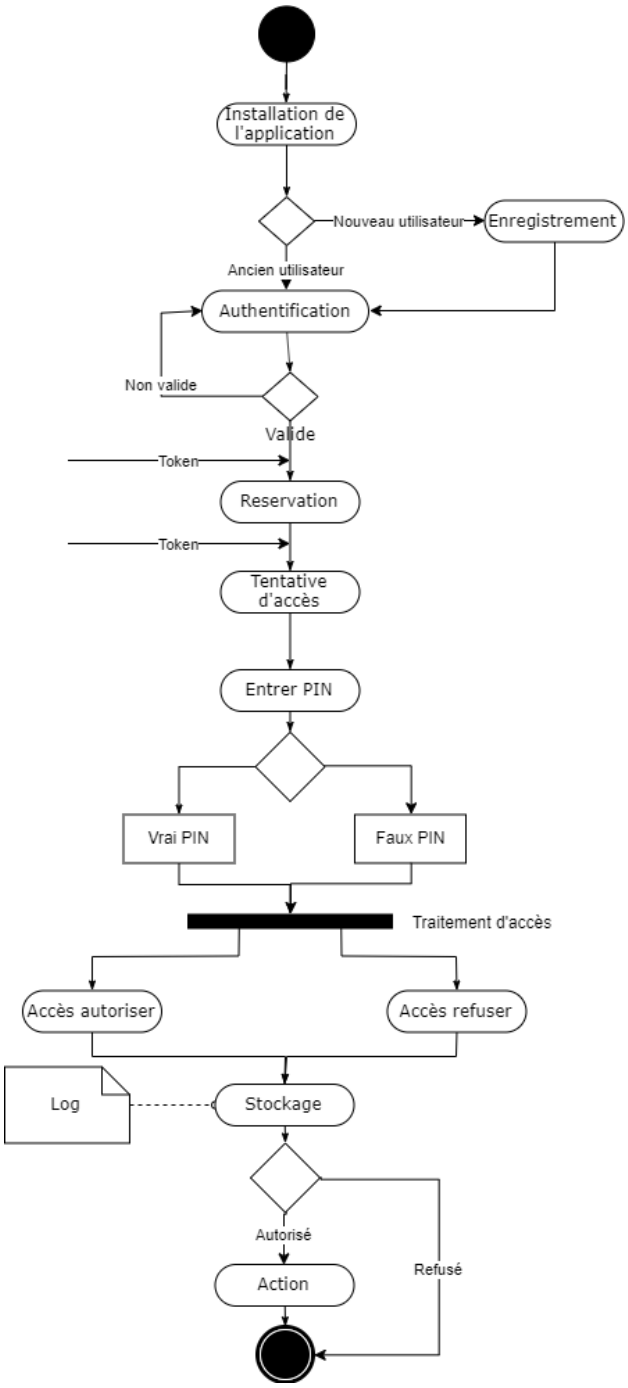


Figure 18 Diagramme d'activité accès porte connecté

Tout commence par l’installation de l’application mobile, l’enregistrement de l’utilisateur s’il est nouveau. Des tentatives d’accès prennent suite à une réservation, Après avoir reçu le token et entrée le pin, le smartphone se rapproche de la porte intelligente plus précisément du lecteur NFC. La tentative d’accès pourra emprunter deux chemins possibles, une autorisation d’accès si le token et le pin sont juste. Alors qu’un refus d’accès si l’un des deux est faux, Un log pour chaque tentative seras envoyé au serveur puis stocké, puis suite à l’action de l’utilisateur d’ouvrir la porte et d’entrée.

3.8. Diagramme de séquence

Le diagramme de séquence se compose d'objets et de flèches. Ces éléments sont organisés selon deux axes perpendiculaires : le premier axe exprime le temps, et le deuxième axe représente les instances. Le diagramme de séquence présente le déroulement d'un cas d'utilisation sous forme d'un scénario entre les acteurs et leurs interactions séquentielles par le changement des messages entre les objets, en respectant l'ordre chronologique (en fonction du temps). [55]

3.8.1. Diagramme de séquence général

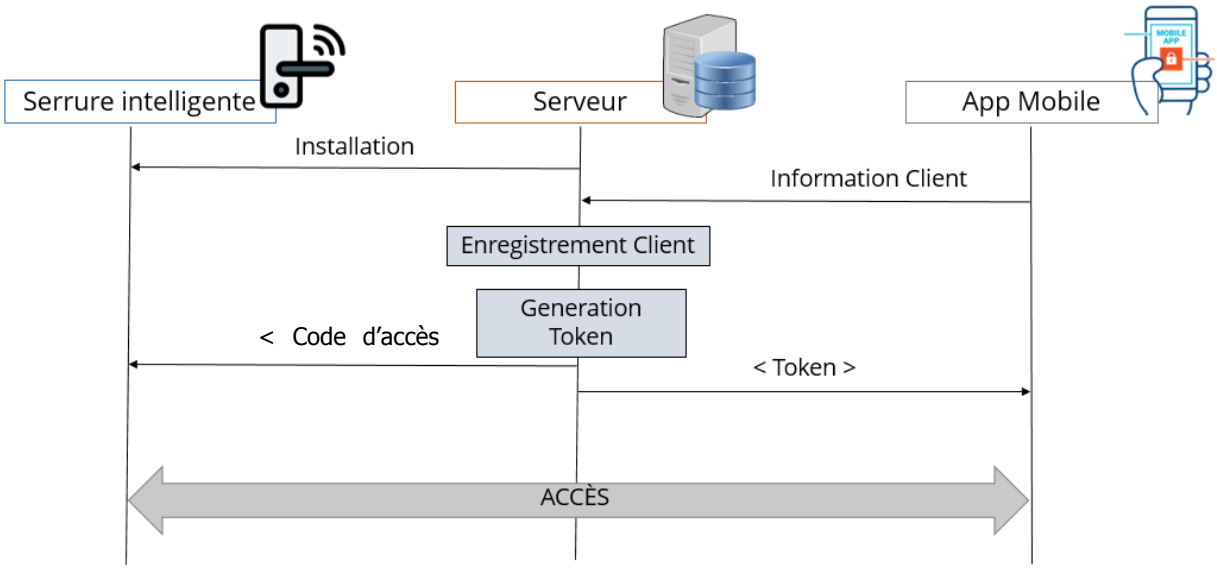
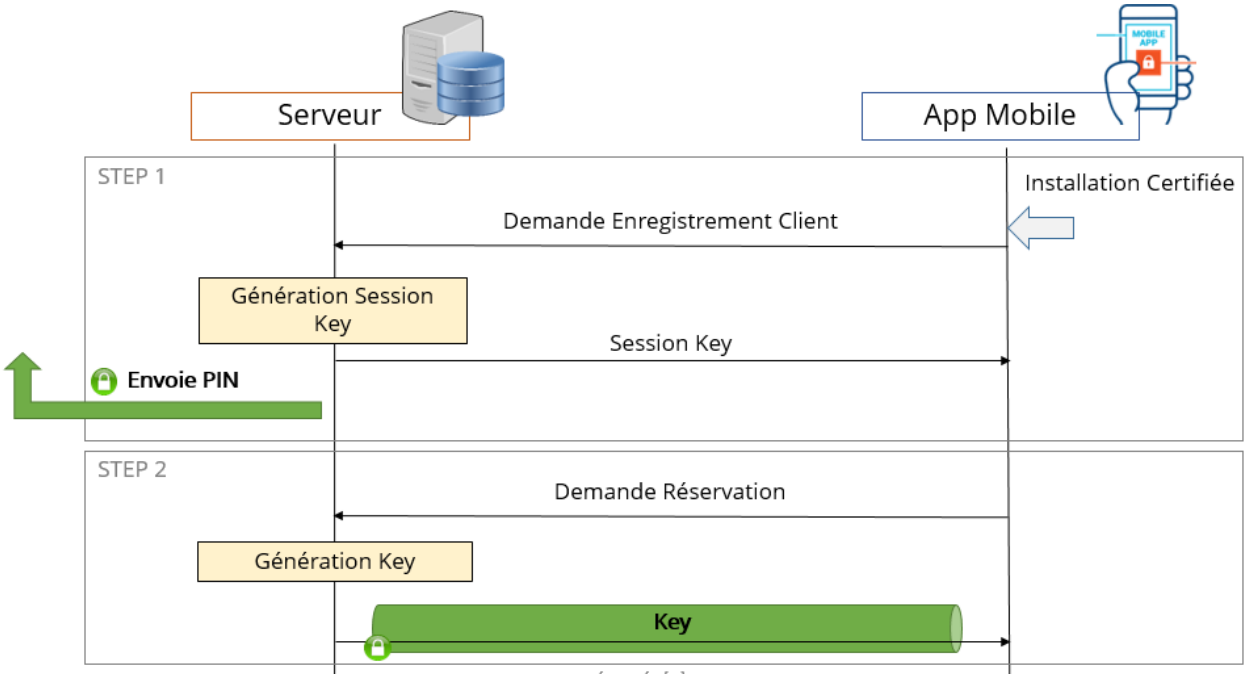


Figure 19 Diagramme de séquence général

Scénario : général

Cette phase est précédée par l'étape mise en place du serveur,

- Après l'enregistrement de l'utilisateur sur la plateforme, le client fait une réservation pour une date.
- Après l'initialisation de l'objet connecté Le système lui affiche une fiche produit, l'utilisateur envoie une requête vers le serveur.
- Enregistrement du client et de la demande, traitement puis génération du token.
- Le renvoie du token à l'utilisateur et à la porte intelligente dont il va tenter un accès.
- Dernière étape l'accès.



3.8.2. Diagramme de séquence du scénario réservation client

Figure 20 Diagramme de séquence du scénario réservation client

Scénario : réservation client

- Après avoir enregistré l'application mobile auprès d'une autorité certifiée et sur. La première étape, du client est d'installer l'application mobile certifié, le client pourra faire une demande d'enregistrement au serveur.
- Le serveur lui répondra avec une clé de session après sa génération.
- Le PIN a été envoyé préalablement à l'utilisateur via un autre canal de communication.
- Ensuite, la deuxième étape, et que l'utilisateur fait une réservation à une dates précise pour une chambre.
- Le serveur génère une clé d'accès et lui envoie via le canal sécuriser mis en place avec la clé de session.

3.8.3. Diagramme de séquence du scénario installation serrure intelligente

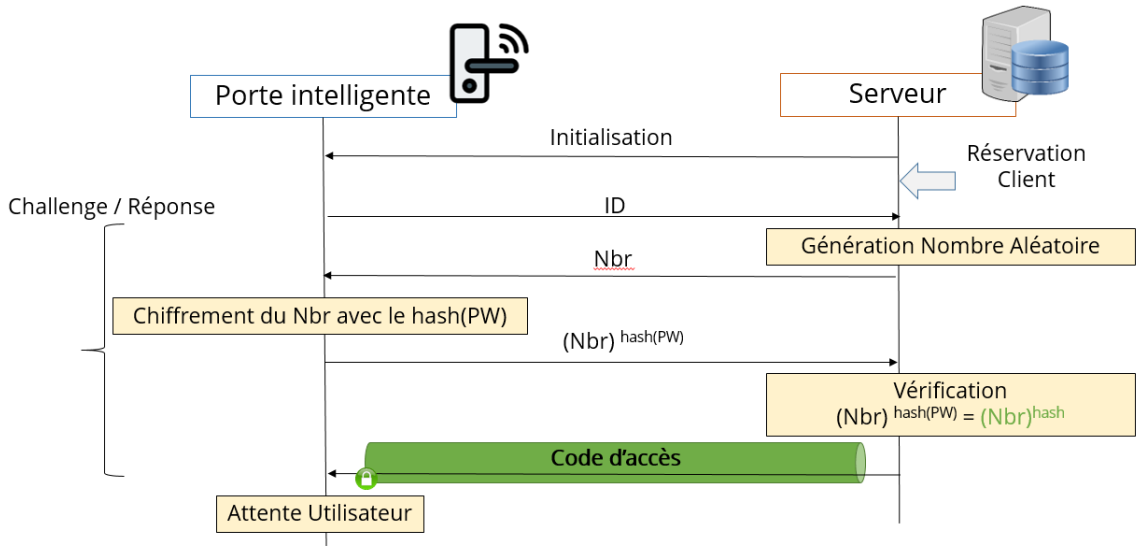


Figure 21 Diagramme de séquence du scénario coté serrure intelligente

Scénario : installation serrure intelligente

Après installation de la serrure intelligente, l'initialisation de l'objet et la réservation du client. Un protocole spécifique à Zigbee va être échangé entre les deux entité, le protocole est semblable à un challenge / réponse.

L'objet ayant un identifiant 'ID' et un mot de passe 'PW'

- L'objet envoie l'ID au serveur, le serveur génère un nombre aléatoire qui ensuite le renvoie à l'objet.
- L'objet calcule le chiffrement du nombre avec le hash du PW, et l'envoie au serveur.
- Après réception, le serveur calcule lui aussi le chiffrement du nombre avec le hash du PW qui trouve au sein de sa base de données.
- Maintenant, vérifie la valeur obtenue avec celle reçu.
- Enfin, envoie le code d'accès via un canal sécurisé à la porte intelligente qui est en attente d'accès utilisateur.

3.8.4. Diagramme de séquence du scénario accès client

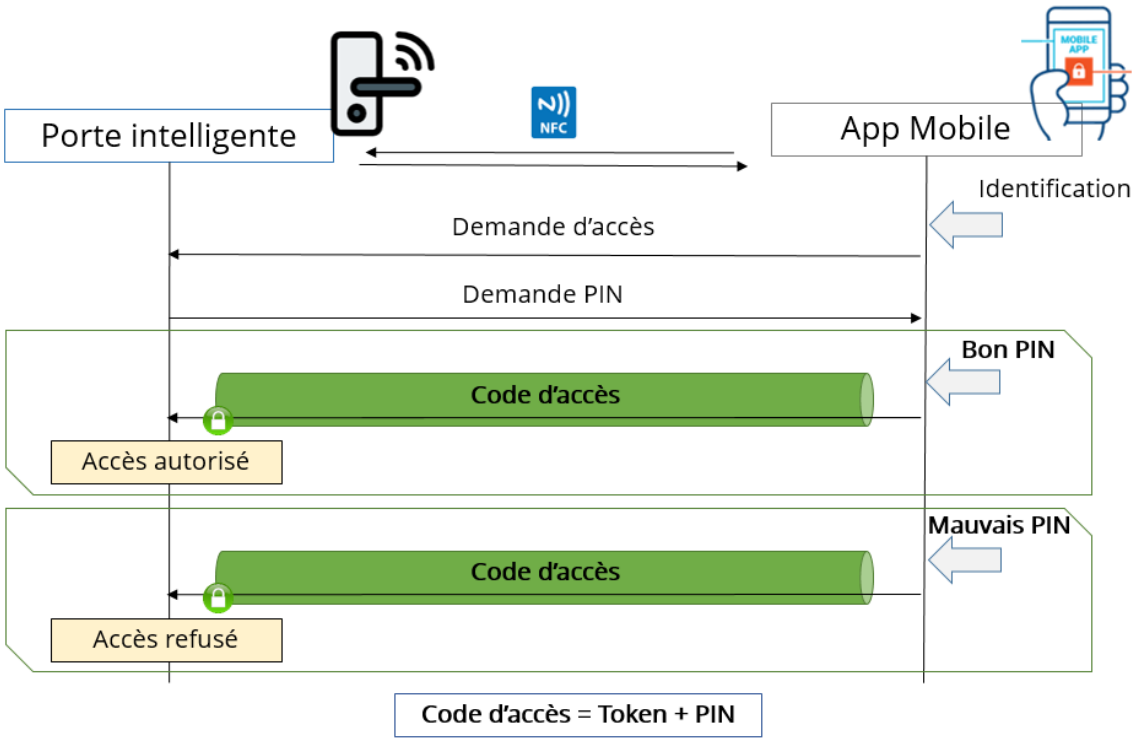


Figure 22 Diagramme de séquence du scénario accès client

Scénario : Accès client

Finalement, le dernier diagramme de séquence qui finalise aussi le travail.

- Identification de l'utilisateur sur son smartphone auparavant.
- L'utilisateur rapproche son smartphone au lecteur NFC de la porte intelligente.
- Une demande d'accès est envoyée, l'ajout du PIN au Token est nécessaire.
- Enfin, l'échange entre l'utilisateur et la porte intelligente faite,
    - Cas 1 : Bon PIN = Accès autorisé.
    - Cas 2 : Mauvais PIN = Accès refusé.

4. Les entités du système

Une conception plus détaillée du système, entité par entité simplifiera l'étape de développement et réalisation.

L'administrateur a accès aux données par le serveur, l'utilisateur par son smartphone. Le serveur local fait place à la passerelle ou routeur sur le lieu des objets connectéssa pour traduire les données depuis internet au ZigBee.

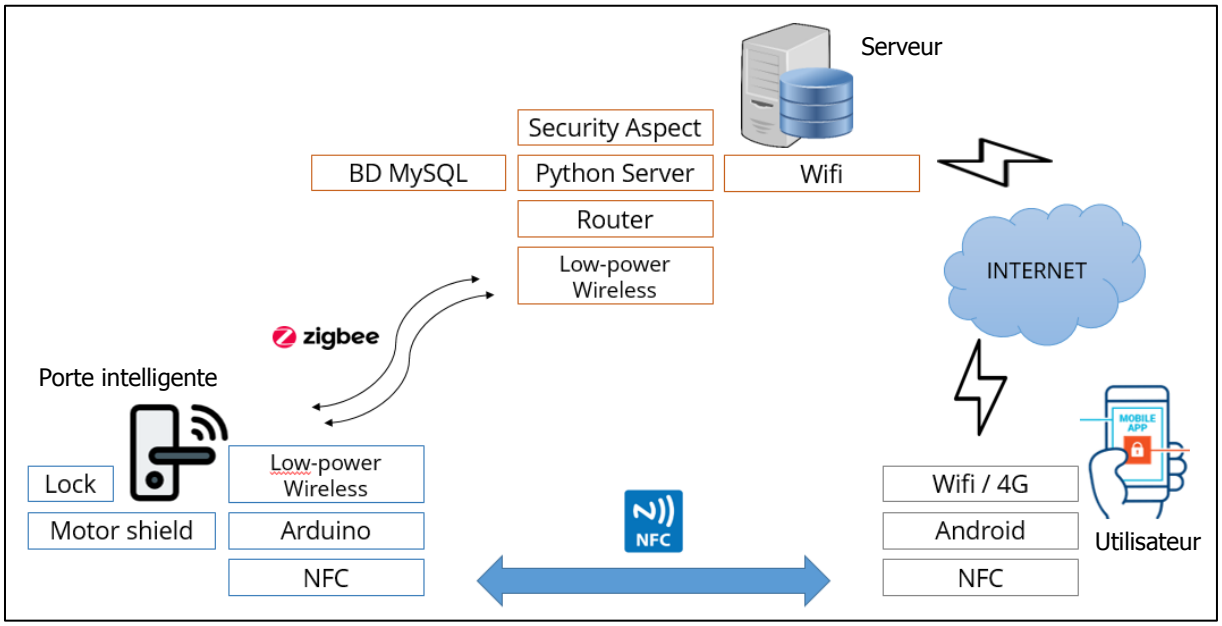


Figure 23 Structure générique détaillé

Cette figure indique les périphériques connectés sur les réseaux (internet et faible consommation), nous fusionnerons notre serveur et notre routeur sur une seul machine lors de notre démonstration.

4.1 Serveur

4.1.1. Présentation

Le serveur se compose de deux parties, la première partie donnant accès vers l'internet pour intercepter les demandes de l'utilisateur mobile, et la deuxième partie communiquant avec la porte connectée par le bien d'un moyen de communication basse consommation. Les actions possibles :

La première partie (via Internet) :

- L'interception de requêtes des utilisateurs.
- L'analyse des données reçu.
- Le traitement de ses données(réservation,).
- Génération des tokens.
- Stockage base de données.
- Enfin la réponse aux demandes.
- Le cryptage et le décryptage des données à chaque transmission (AES)

En vue de réception et d'envois de données, l'utilisation de deux ports de communication diffèrent est nécessaire.

La deuxième partie (via Zigbee) :

- L'interception des données envoyées à partir de la porte intelligente.
- L'analyse des données reçu (Activité tentative d'accès).
- Stockage base de données.
- Envoie des token.

4.1.2. Structure du code d'accès

Le code d'accès est principalement un hash MD5 composé de deux parties la clé et le pin 'md5(key, pin)'. La génération des token se fait aléatoirement.

4.2. Application mobile (utilisateur final)

4.2.1. Présentation

L'application de l'utilisateur sert à interagir avec le système donc un accès direct à la plateforme, l'utilisateur pourra principalement toucher les deux grands traits du système qui sont : faire des réservations de chambre et pouvoir accéder aux chambres sans contraintes.

4.2.2. Schéma Simplifié de l'application

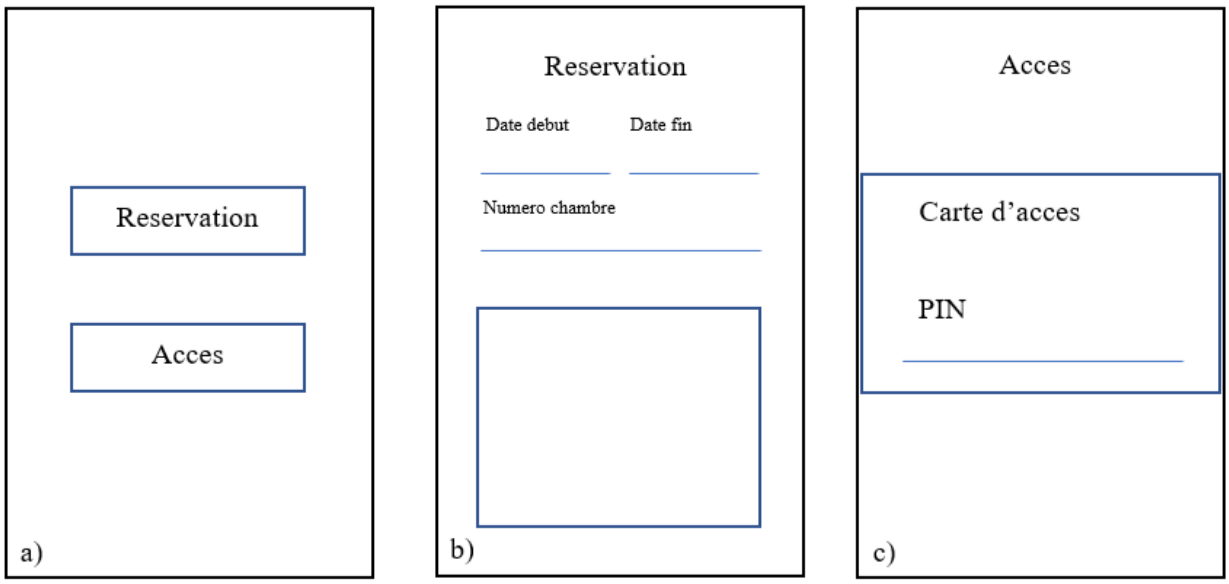


Figure 24 a) Interface principale, b) Interface de réservation, c) Interface d'accès

L'interface a) montre le menu principal à deux boutons pour se diriger à deux interfaces b) et c), l'interface b) pour la réservation avec des champs pour les informations utiles dates et chambre à réserver, le dernier champ affichera les données reçus, la deuxième interface c) pour l'accès à la porte intelligente avec un champ pour le PIN.

4.3. Porte intelligente

4.3.1. Présentation

Une porte intelligente est un dispositif de verrouillage électronique et mécanique qui s'ouvre sans fil avec l'authentification d'un utilisateur autorisé.

Dans une maison intelligente, les portes intelligentes permettent à un propriétaire d'entrer chez lui ou de fournir un accès à d'autres personnes sans nécessiter de clé traditionnelle. Au lieu de cela, l'utilisateur utilise son smartphone ou un porte-clés pour vérifier et déverrouiller mécaniquement la porte sans fil. Les serrures intelligentes sont une extension de la domotique dans la sécurité domestique. En tant qu'appareil connecté, les serrures intelligentes peuvent être considérées comme faisant partie de l'Internet des objets (IdO).

4.3.2. Schéma de la porte connectée

Après quelques dessins sur papier du model à réaliser, un schéma convenable et réaliste a été conçu.

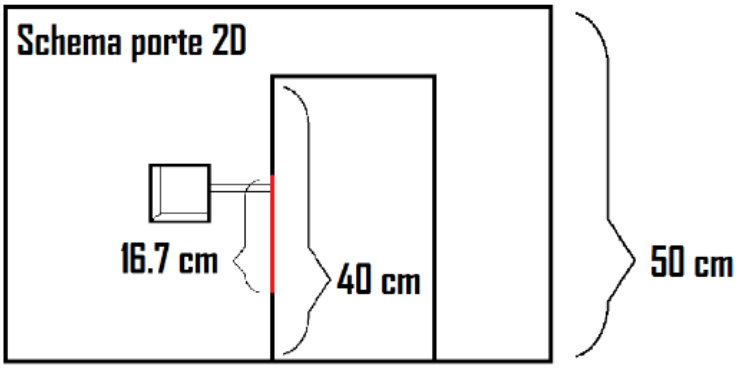


Figure 25 Schéma porte intelligente 2D

La fig. 28 montre le schéma 2D de la porte intelligente, un cadre pour la porte et un cache où se trouve le matériel électronique. Quant à la Fig.29 qui montre le schéma de la serrure sur la porte.

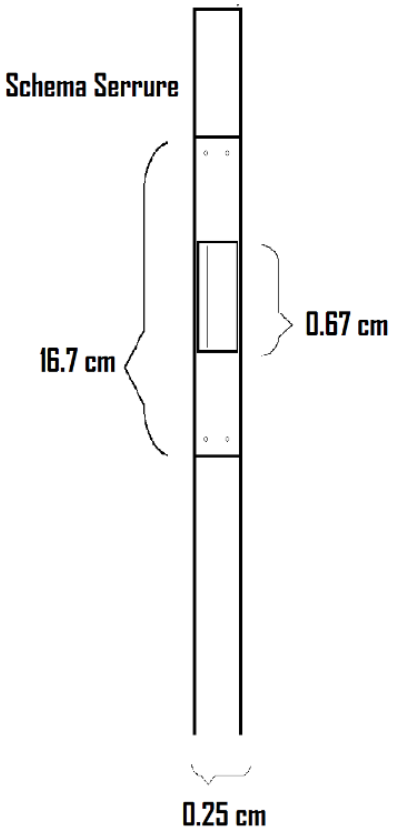


Figure 26 Schéma serrure

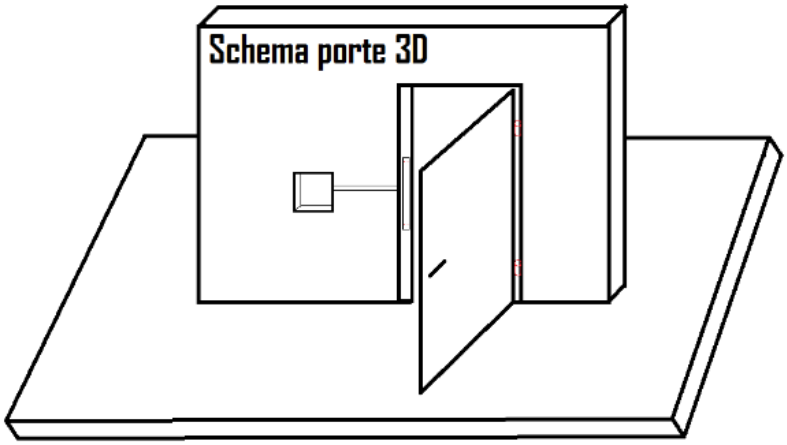


Figure 27 Schéma porte intelligente 3D

La fig. 30 montre le shéma de la porte en 3D. La simulation se fera sur une port miniature qui comporteras tout le système electronique connecté.

4.3.3. Composants matériels de la porte

- L'Arduino utilisé Mega 2560

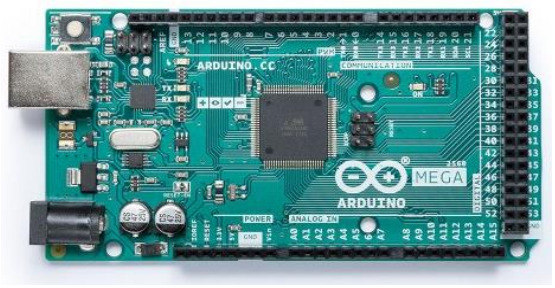


Figure 28 Arduino Mega 2560 rev3

- Un module NFC pour lire les tentatives d'accès des utilisateurs
  - Le mode I2C est utilisé avec (SDA, SCL)

Figure 29 PN532 NFC reader

- 2 XBee S2
  - Adaptateur Arduino XBee
  - Adaptateur USB XBee

Figure 30 XBee S2

Figure 31 CYTRON XBee Shield for Arduino

Figure 32 XBee to USB adapter

- Un module Relay pour gérer les tensions du lock

Figure 33 Motor Shield Relay MD10

- Lock ou gâche Électrique

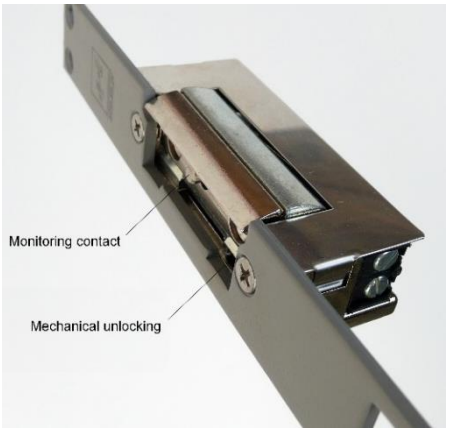


Figure 34 Gâche électrique

- Support à piles AA
  - 8 piles pour alimenter l'arduino
  - 12 piles pour alimenter le gacher via le relay

Figure 35 Support à pile

4.3.4. Schéma électronique

La serrure intelligente se composera de plusieurs entités :

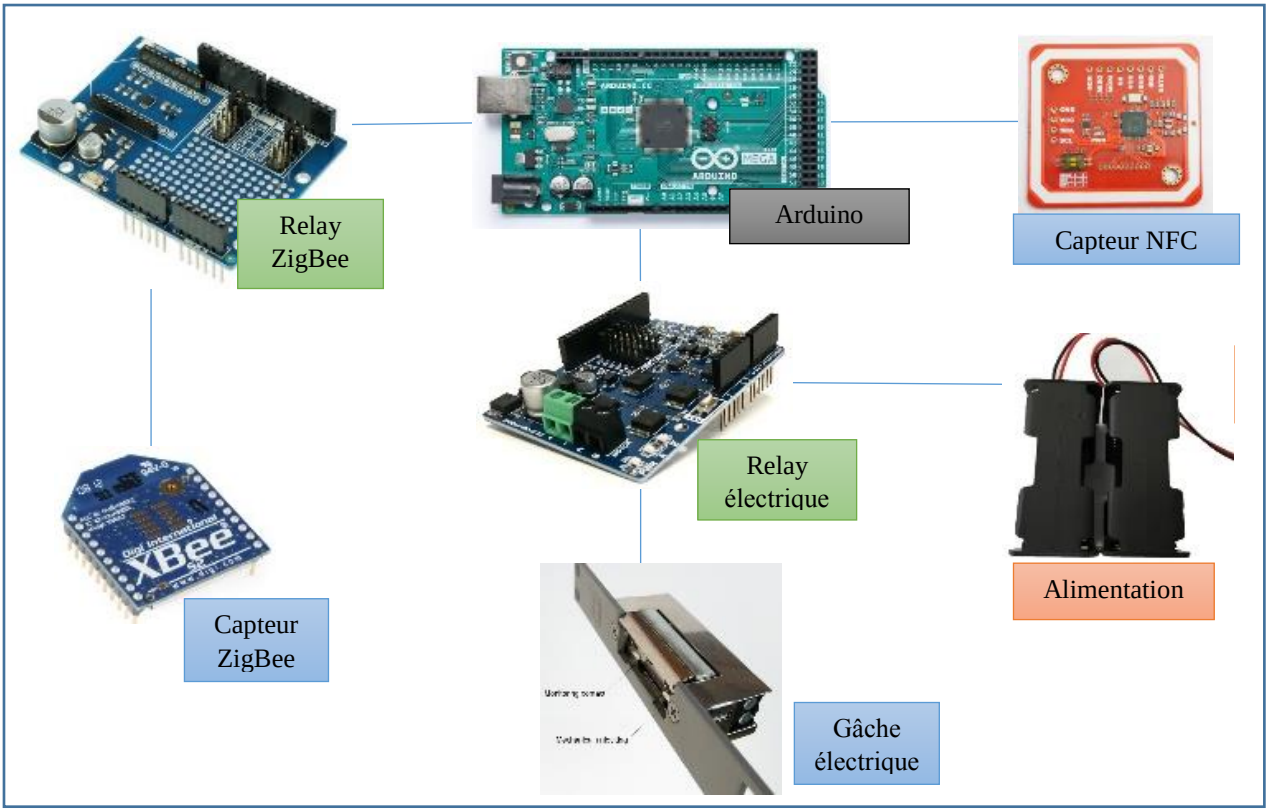


Figure 36 Schéma électronique serrure intelligente

L'Arduino est le composant cerveau du système qui est relié au capteur Zigbee grâce au relay Zigbee, puis le capteur NFC et le relay électrique qui gère d'alimenter l'Arduino et la gâche électrique.

5. Conclusion

La conception est une étape très importante qui précède l'implémentation de tout système. Ce chapitre a été consacré à l'analyse et la spécification des besoins de notre système. Nous avons proposé une architecture matérielle et logicielle. Nous avons opté et défini trois grandes entités où nous déploierons notre proposition, et ce, afin de tester notre solution dans un environnement réel. Après des choix qui ont été fait, technologie utilisé, méthode de communication, architecture et modèle un certain équilibre s'est installé entre l'efficacité et la sécurité.

Dans le prochain chapitre nous allons décrire les outils permettant la réalisation de notre système et un aperçu sur les fonctionnalités réalisées.

CHAPITRE III : DEVELOPPEMENT ET MISE EN ŒUVRE

1. Introduction

Après avoir réalisé la conception appropriée à notre projet, nous allons dans ce chapitre décrire le processus de réalisation de notre système. Ceci en spécifiant l'environnement de développement, ainsi qu'une présentation de quelques algorithmes importants décrivant leur mécanisme. Puis, les tests et validation et enfin l'évaluation et le déploiement. Mais avant tout, voici un aperçu de l'achèvement du travail grâce un diagramme de Gantt.

Diagramme de Gantt

Intitulé du projet : Platform de sécurité légère pour l'Internet des objets — **Etat d'avencement 80%** — **1/8/19**

Date : 12/02/2019 au 13/07/2019

	Détail des tâches	FEVRIER		MARS				AVRIL				MAI				JUIN				JUILLET			
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22
1	**Etat de l'art**																						
1.1	Equipement electronique / Composants	X	X	X			X	X															
1.2	Previous Project / Control d'acces			X																			
1.3	Architecture / Gestion IoT		X					X	X	X											X		
1.4	Analyse des Riques et Vulnérabilités																					X	X
2	**Design / Conception**																						
2.1	Architecture global	X	X	X			X	X	X														
2.2	Details sur la partie control d'acces									X	X	X											
2.3	Echange / protocole (Maissa)														X		X	X	X	X			
3	**Implementation / Validation**																						
3.1	Approfondire les connaisances sur Arduino (Xbee / NFC)	X	X					X															
3.2	Realisation du Serveur Plateforme					X	X							X	X								
3.3	Realisation de l'application mobile			X	X					X	X	X											
3.4	Realisation de la relation (App Mobile - SL)										X	X	X										
3.5	Realisation de la relation (Serveur - SL)						X	X	X														
3.6	Realisation de la relation (App Mobile - Serveur)														X	X	X						
3.7	Finaliser le Smart Lock concept																	X	X				
3.8	Ajout du service PKI													X		X	X						
3.9	Tests / Validation																	X	X	X			
4	**Rapport**																						
4.1	Etude Etat de l'art	X	X	X	X			X						X	X						X	X	X
4.2	Diagramme de Classe 'UML'				X	X		X		X										X	X	X	
4.3	Graphe/Schema/Test de Validation		X				X		X				X	X						X	X		
4.5	Finalisation du rapport				X				X												X	X	X

Figure 37 Diagramme de Gantt achevé

2. Outils et plates-formes

Cette partie concerne la présentation des outils, du langage de programmation et des plates-formes utilisées dans ce projet :

2.1 Java

Java est un langage de programmation et une plate-forme informatique créés par Sun Microsystèmes en 1995. C'est la technologie sous-jacente qui permet l'exécution de programmes à la pointe de la technologie, notamment des utilitaires, des jeux et des applications professionnelles. Java est utilisé sur plus de 850 millions d'ordinateurs de bureau et sur un milliard d'appareils dans le monde, y compris des appareils mobiles et des systèmes de diffusion de télévision. [43]

2.2. C Arduino

Le langage de programmation Arduino est un langage simplifié à partir du langage de programmation C / C ++ basé sur ce que Arduino appelle des "esquisses", qui utilisent des structures de programmation, des variables et des fonctions de base. Celles-ci sont ensuite converties en un programme C ++. D'autres projets de prototypage électronique open-source, tels que Wiring and Processing, fournissent les bases de la technologie Arduino. [44]

2.3. Python

Python est un langage de programmation interprété orienté objet, qui a gagné en popularité en raison de sa syntaxe et de sa lisibilité. Python est relativement facile à apprendre et à transporter, ce qui signifie que ses instructions peuvent être interprétées sous plusieurs systèmes d'exploitation, notamment les systèmes UNIX, Mac OS, MS-DOS, OS / 2 et diverses versions de Microsoft Windows 98. Python a été créé par Guido van Rossum, un ancien résident des Pays-Bas. Le code source est librement disponible et ouvert pour modification et réutilisation. Python a un nombre important d'utilisateurs. [45]

2.4. Android Studio

C'est un environnement de développement pour développer des applications Android. Il est basé sur IntelliJ IDEA. (IntelliJ IDEA est un IDE commercial Java développé par JetBrains). Android Studio vous permet principalement de modifier des fichiers Java et des fichiers de configuration pour une application Android. Entre autres choses, il offre des outils pour gérer le développement d'applications multilingues et vous permet de visualiser simultanément la disposition des écrans sur des écrans de différentes résolutions. [46]

2.5. SQLite

SQLite est une biblIdOhèque écrite en langage C qui offre un moteur de base de données relationnelle accessible par le langage SQL. Il implémente une grande partie des propriétés standard et ACID de SQL-92. Sa particularité n'est pas de reproduire le schéma habituel client-serveur mais d'être directement intégré dans les programmes. Toute la base de données (déclarations, tables, index et données) est stockée dans un fichier indépendant de la plate-forme. C'est le moteur de base de données le plus utilisé au monde. Grâce à son utilisation dans de nombreux logiciels grand public tels que Firefox, Skype, Google Gears, il est également très populaire sur les systèmes embarqués, en particulier sur les smartphones et tablettes les plus modernes. Les systèmes d'exploitation mobiles IOS, Android et Symbian l'utilisent également comme système de base de données intégré. [47]

2.6. Arduino IDE

Le logiciel Arduino Open Source (IDE) facilite l'écriture de code et son téléchargement sur le tableau. Il fonctionne sous Windows, Mac OS X et Linux. L'environnement est écrit en Java et est basé sur d'autres logiciels à code source ouvert. Ce logiciel peut être utilisé avec n'importe quelle carte Arduino. [48]

2.7. WAMPP

XAMPP est l'environnement de développement PHP le plus populaire, C'est une distribution Apache totalement gratuite et facile à installer, contenant MariaDB, PHP et Perl. Le paquet open source XAMPP a été configuré pour être incroyablement facile à installer et à utiliser. [49]

2.8. XCTU

XCTU est une application multiplate-forme gratuite conçue pour permettre aux développeurs d'interagir avec les modules Digi RF via une interface graphique simple à utiliser. Il comprend de nouveaux outils qui facilitent la configuration, la configuration et le test des modules XBee® RF. XCTU inclut tous les outils dont un développeur a besoin pour devenir rapidement opérationnel avec XBee. Des fonctionnalités uniques telles que la vue graphique du réseau, qui représente graphiquement le réseau XBee ainsi que la puissance du signal de chaque connexion, et le générateur de trames API XBee, qui aide intuitivement à construire et à interpréter les trames API pour XBees utilisées en mode API, permettent de développer sur la plate-forme XBee plus facile que jamais. [50]

2.9. Putty

PuTTY est un client SSH et Telnet, développé à l'origine par Simon Tatham pour la plate-forme Windows. C'est un logiciel open source disponible avec code source, développé et soutenu par un groupe de volontaires. [51]

3. Description du système mis en œuvre

Dans cette section, nous allons décrire et expliquer la méthodqologie de la plupart des fonctionnalités importantes. Dans notre solution, nous avons divisé les stratégies en 3 entités différents, une porte intelligente, une application mobile et un Serveur.

3.1. Porte intelligente

Avant tout, une porte intelligente est un dispositif de verrouillage électronique et mécanique qui s'ouvre sans fil avec l'authentification d'un utilisateur autorisé.

La porte intelligente aura des besoins primaires pour pouvoir accéder aux exigences principales.

- Montage de la porte intelligente avec tous ses capteurs.
- Interception des tokens d'accès à partir du serveur.
- Authentification des clients.
- Donne accès au utilisateurs légitime.
- L'envoie des tentatives d'accès (autorisé ou pas), passe d'accès et heure où la tentative a été faite.

Comme nous l'avons dit précédemment, utilisant une carte Arduino, nous allons développer en C Arduino sur l'IDE dédié. Le développement commence avec la partie principale setup qui initialise les output (pinMode), les périphériques de connectivités : le port serial (choix d'une vitesse de communication) avec lequel va communiquer par la technologie Zigbee et l'initialisation de la technologie NFC communicant avec le smartphone. Puis, la boucle qui exécute les fonctions primaires, la lecture Zigbee et NFC, le traitement des données. Tout cela se présente sur la carte Arduino. Les fonctionnalités suivantes présentent la connectivité de l'Arduino.

3.1.1. Partie Zigbee

Le capteur Zigbee intercepte les données puis les fragmente et les analyse, pour pouvoir répondre par la suite au serveur.

La fonction 'recvWithStartEndMakers()' reçoit les données à partir de 'Serial.available()', reconnait le début et la fin de la socket, donc peu lire la socket convenablement. La fonction 'parseData()' sert à la fragmentation des données de façon à ce que les données puissent être traitées par la suite. La fonction suivante 'functionToDo()' traite les données, puis exécute les commandes reçues (ADD, ITR, CLR, RBT, IVD) respectivement (ajouter, afficher, supprimer, rebouter, requête invalide).

ADD utilise la fonction 'eeprom_store()' pour stocker les données utiles à la porte intelligente. ITR utilise 'eeprom_iteration(X,Y)' qui itère les données depuis la case mémoire X jusqu'à Y. CLR utilise 'eeprom_clear()' qui supprime toutes données sur la mémoire EEPROM.

Le montage du capteur Zigbee sur l'Arduino a)Relay de connectivité Zigbee, b) capteur Zigbee.

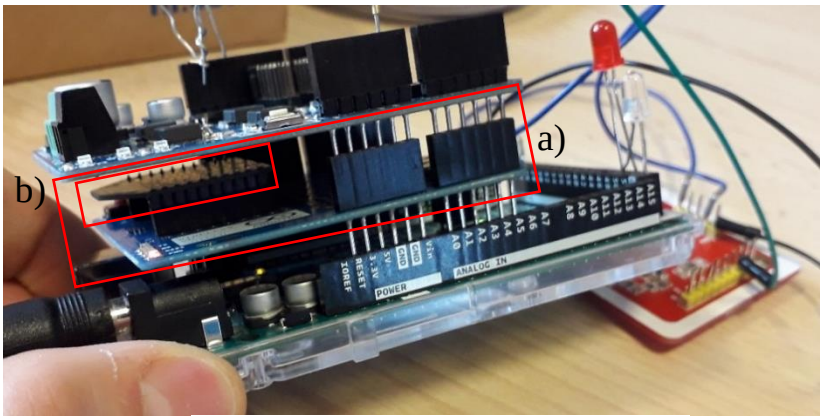


Figure 38 Relay Xbee et capteur Zigbee

3.1.2. Partie NFC

Après l'installation de la partie Zigbee, nous passons à la partie NFC, la fonction lecture 'fct_lecture' est une fonction qui va pouvoir lire les tag NFC. En utilisant 'selectApdu', les attributs : 'CLA' la classe d'instruction, 'INS' l'instruction, 'P1, P2' les paramètres de l'instruction, 'L'la taille de la donnée, 'Data' la donnée, 'Le' la taille maximum que peu atteindre la réponse. Si la donnée lue correspond à un code d'accès valide, une ouverture de la porte et un log est envoyé au serveur grâce au Zigbee sinon un log seulement est envoyé.

Il existe différents tags, par leur taille, format d'encodage. Nous avons commencé en utilisant des simples tag RFID. Après plusieurs tentatives de lecture et d'écriture sur un tag. Nous passons à la lecture de puce NFC de smart phone. Avec précedement un montage du capteur nfc avec l'arduino.

Figure 39 Tag RFID

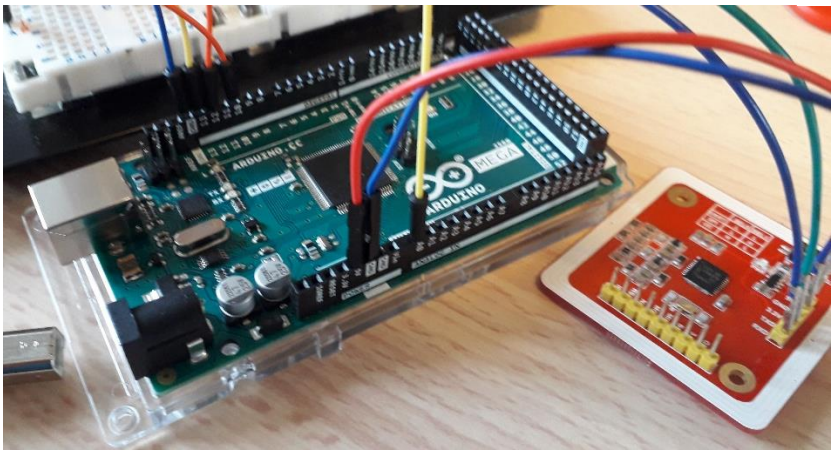


Figure 40 Arduino et capteur NFC

3.1.3. Model de porte

Après la conception de la porte, nous passons au montage de la porte à l'aide d'un technicien. Le découpage du bois, le soudage des fils d'alimentation, et les coups de peinture ont été fait, et enfin, le montage de la gâche.

Figure 41 Montage serrure

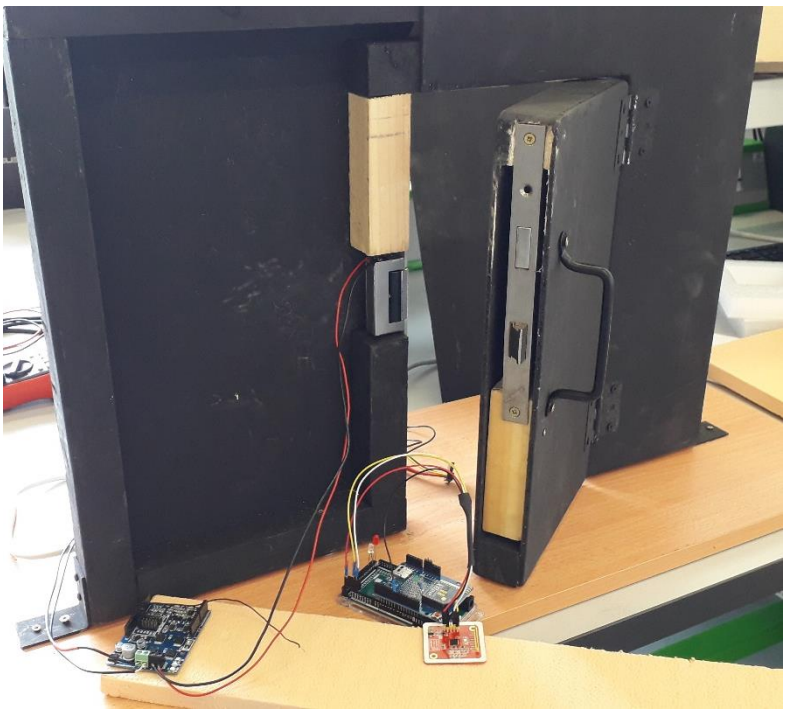


Figure 42 Montage de la porte connecté 1

La décision s'est porté sur le choix de l'alimentation apparente, avec une alimentation d'ordinateur ou des piles pour que ce soit portatif. Après plusieurs tests avec une alimentation apparente plus facile à implémenter. Nous décidons de calculer pour une alimentation non-apparente avec des accumulateurs dû à l'ampérage élevé.

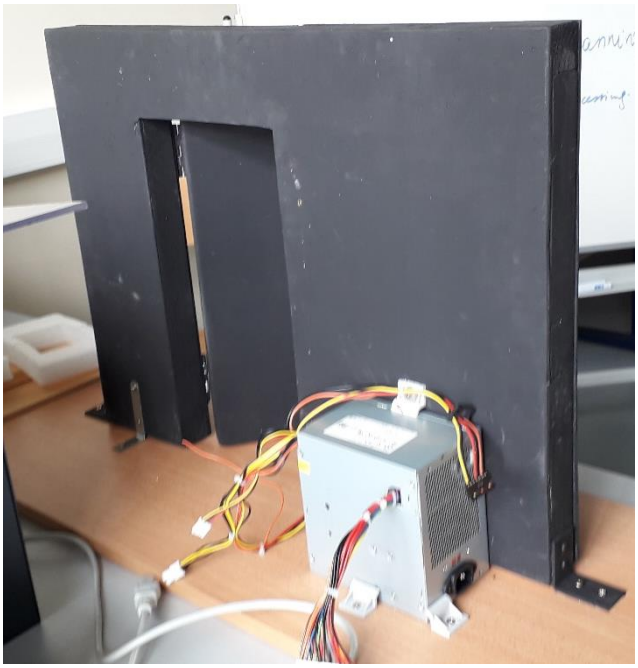


Figure 43 montage alimentation apparent

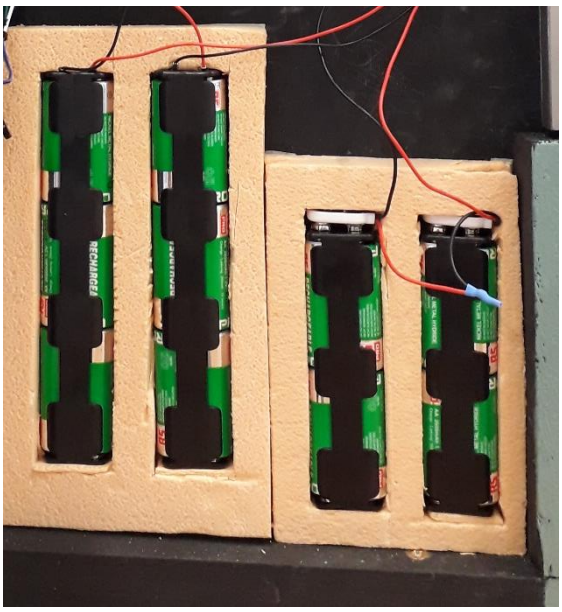


Figure 44 montage alimentation non-apparent

Le calcul d'alimentation est simple, 12V pour la gâche et 5V pour l'Arduino grâce à l'alimentation apparente qui est une alimentation d'ordinateur fixe car il se trouve que cette sortie existe déjà. Par contre pour la non-apparente ci-dessous.

a) Alimentation Arduino

D'après la documentation du constructeur, si on utilise la prise jack pour alimenter la carte, il faut entre + 7 V et + 12 V. Sachant qu'à 6V, la tension en sortie du régulateur ne sera pas suffisante pour alimenter le microcontrôleur. Donc avec 8 piles, nous avons +12V le maximum. Avec 12 V nous pouvons tolérer une décharge pour chaque pile jusqu'à 0.875 V (pour obtenir 7 V). Étant donné que les accumulateurs ont une bonne tenue en tension en décharge, cela nous assure une bonne longévité de fonctionnement avant recharge des piles.

Ce montage est nécessaire pour rendre le système portatif et fonctionnel sur la durée. En réalité, ce montage permet de faire fonctionner la carte Arduino.

b) Alimentation la gâche

Nous avons fait un montage expérimental. L'idée était que même déchargée à 1 V (pour un accumulateur 1.5V), le pack d'accumulateurs puisse actionner l'électro aimant de la gâche. La gâche supportait +18 V, et alimenter toujours jusqu'à +12V.

Sans oublier le Relay électrique régulateur de tension qui ouvre et ferme le circuit alimentant la gâche.

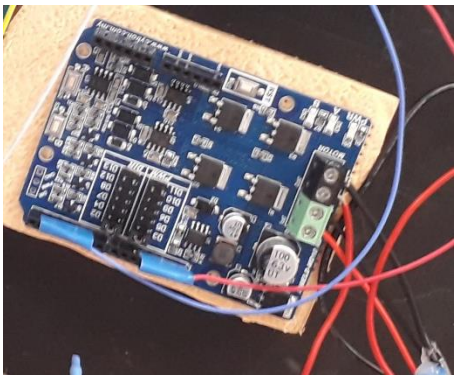


Figure 45 Relay électrique

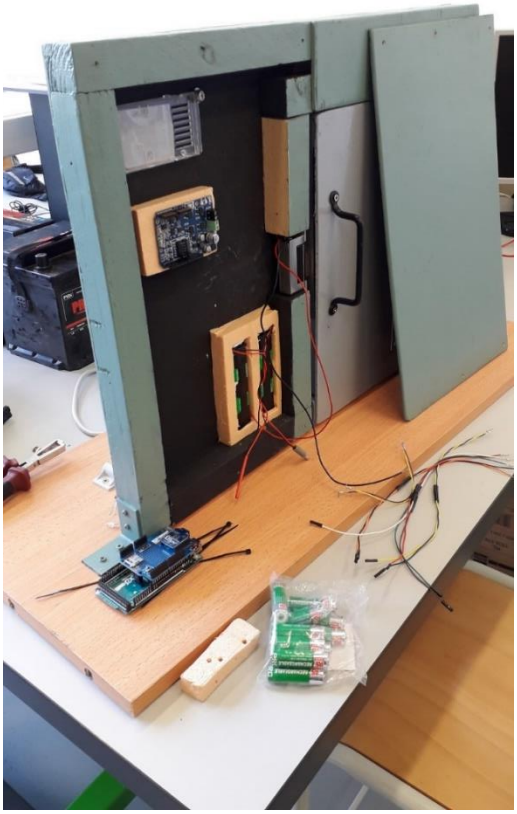


Figure 46 Montage des composants dans la porte intelligente

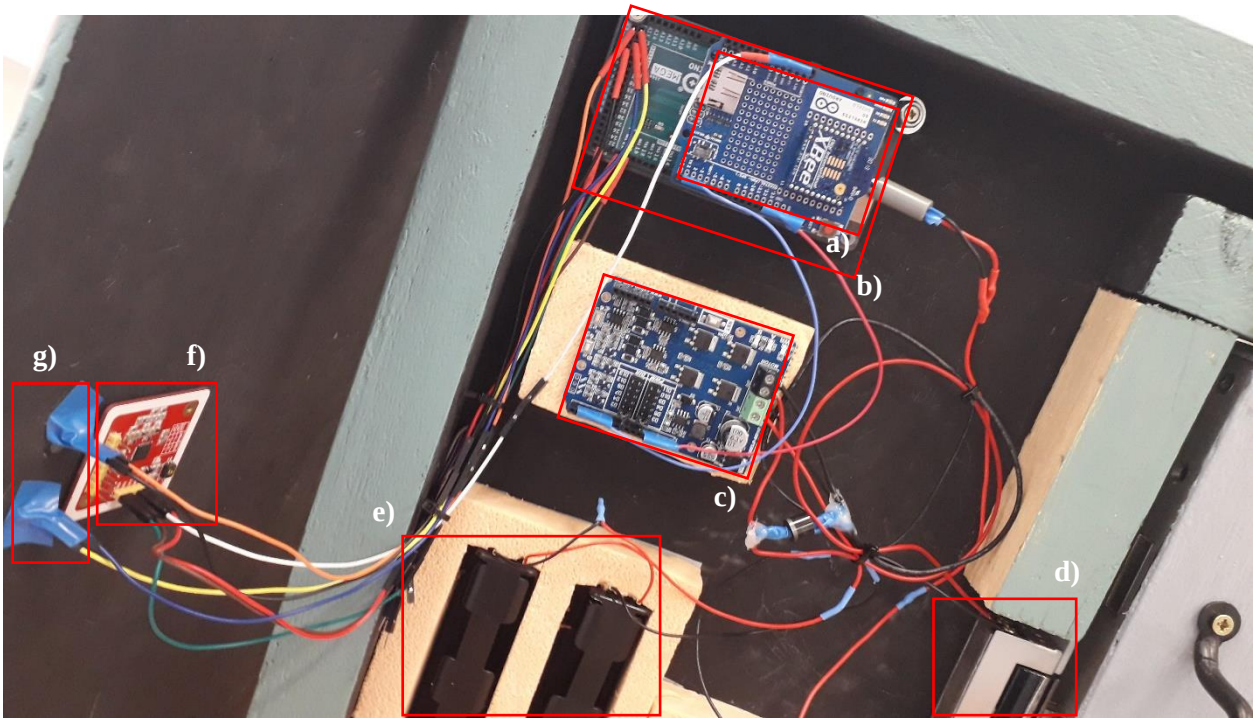


Figure 47 Montage des modules de connexion

Dans cette figure a) Relay Zigbee, b) Arduino Mega, c) Relay électrique d) gâche électrique, e) support piles pour l'alimentation, f) Capteur NFC, g) Leds rouge et vert.

Après le changement de peinture et quelques stickers, une vue d'ensemble est présenté ci-dessous. Par la suite, quelques tests vérifiant que la connectivité Zigbee été établie et que le lecteur NFC pouvait lire.

Figure 48 Vue final de la porte intelligente

3.2. Application mobile

Avant tout, l'application mobile sert à interagir avec le système donc un accès direct à la plateforme, l'utilisateur pourra principalement toucher les deux grandes exigences système qui sont : faire des réservations de chambre et pouvoir accéder aux chambres sans contrainte.

Les exigences primaires de l'application pour pouvoir accéder aux exigences principales sont :

- Une interface, avec champs à remplir dates de réservation plus numéro de chambre.
- Un bouton qui envoie au serveur la demande de réservation.
- Un coté serveur qui intercepte une réponse du serveur.
- L'émulation de la Carte à puce NFC.
- L'ajout du PIN.

3.2.1. Code Sources

L'application mobile a été développé sur Android studio grâce au langages JAVA.

Deux fonctions de chiffrement, déchiffrement AES ont été utilisées avant envoie et après réception.

Les fonctions qui permettent le transfert de données sur le réseau internet sont :

- La fonction 'send' permet l'envoie de donnée qui utilisent des socket TCP (adresse, port).
- La fonction 'lunchServer' qui permet la réception des données avec 'serversocket'.

L'action qui permettra l'accès à la porte intelligente est la fonction qui émule la puce NFC sur smartphone, par la fonction 'processCommandApdu'.

3.2.2. Interfaces utilisateur

Les interfaces de l'application mobile sont très simples, pour une première version.

Figure 49 Interface menu principale

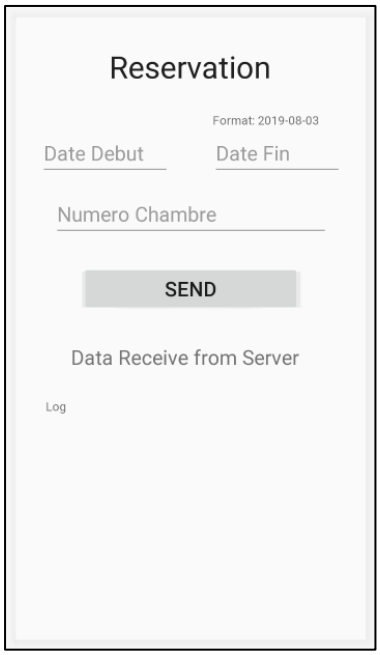


Figure 50 Interface reservation

L’interface suivante est l’interface qui permet d’accéder à la porte intelligente en utilisant l’émulation de la puce NFC. L’application émulera le code d’accès qui est le token et le pin.

Figure 52 Interface carte d'accès Android studio

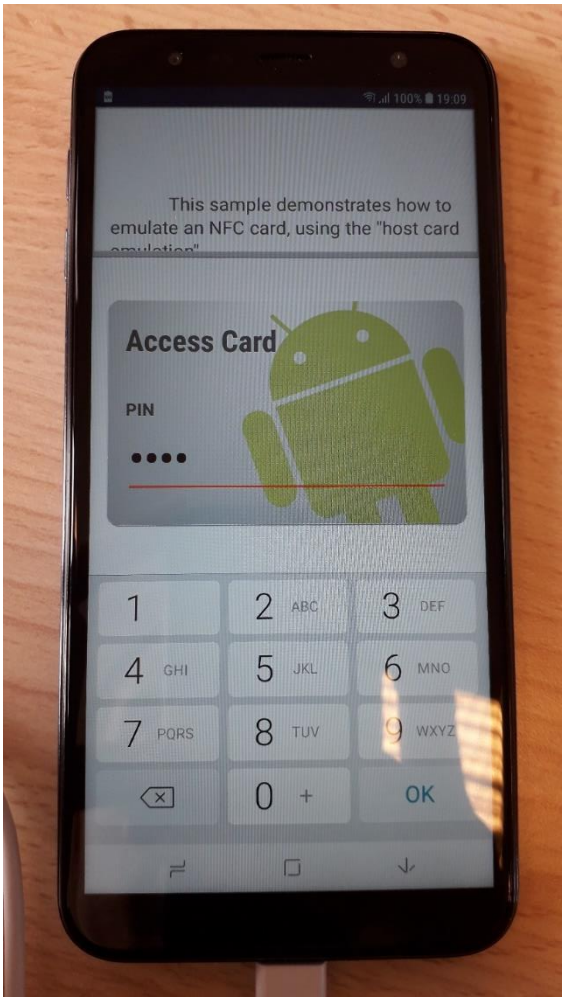


Figure 51 Interface carte d'accès sur Mobile

3.3. Serveur

3.3.1. Structure serveur

Le serveur se sépare en deux parties, partie internet et partie Zigbee, la connexion se divise comme ci-dessous.

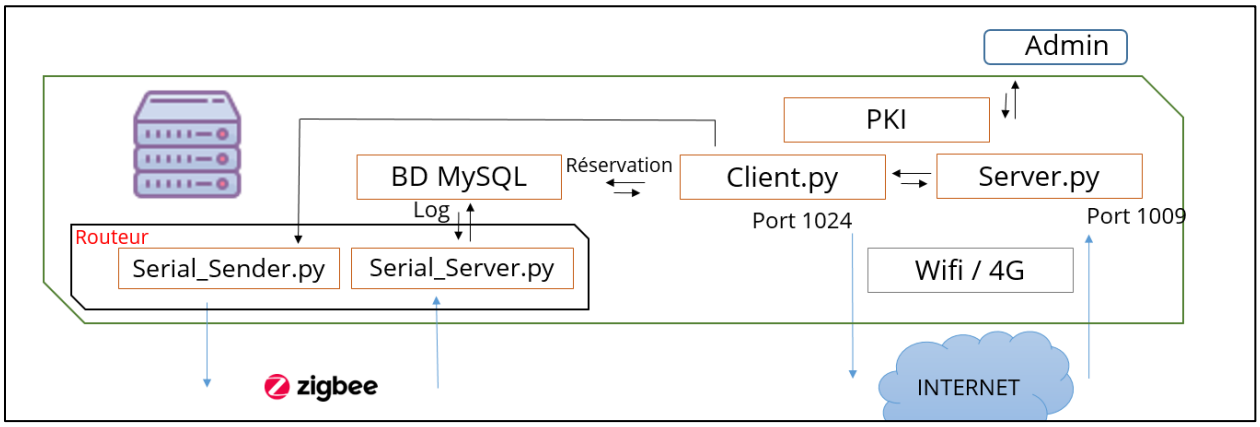


Figure 53 Connexion serveur

3.3.2. Partie Internet

Après installation du réseau LAN.

- La connexion d'un utilisateur avec 'accept', l'interception de requêtes des utilisateurs par socket TCP avec 'recvfrom()'. Suivie du déchiffrement avec l'algorithme AES du package 'Cryptodome.Cipher'.

- La fragmentation des sockets reçu en donnée, le traitement de la validité de la demande (les détails de réservation).

- La génération des tokens pour la réservation.

- Le stockage sur base de donnée (réservation, nouvelle utilisateur) avec le package 'mysql.connector' et la fonction 'cursor et execute', les données importantes se hachent avec SH1 avant de se stocker avec le package 'hashlib'.

- Enfin l'envoie d'une réponse aux demandes des utilisateurs avec la fonction send_client_Ekey qui envoie le token chiffré avec AES par socket TCP.

3.3.3. Partie Xbee

Installation du réseau faible consommation d'énergie.

- La configuration des deux cartes XBee avec (Logiciel X-CTU ou par commande avec putty)

    - a) Même ID (PAN ID) qui est l'id réseau (personal area network) et b) SC (Scan Channels) est la fréquence de transmission.
    - c) SH et SL (Serial Number High e Serial Number Low) sont les fragments d'adresses de votre capteur Zigbee.
    - d) Les adresses DH (Destination Adress High) et DL (Destination Adress Low) sont les deux fragments d'adresse du destinataire 'DH+DL', dans le cas d'une seule porte « un envoyeur, un receveur », les adresses doivent être inversées sur les deux capteurs Zigbee Cas implémenté. Dans le cas de plusieurs capteurs ce paramètre n'importe pas.

    - Broadcast Radius, SE (source endpoint) et DE (destination endpoint) pour plusieurs portes.

    - Les paramètres de sécurité (EE, EO, NK, KY) requis, sont :
        - EE : Activer ou désactiver la sécurité sur le réseau.
        - EO : Définir la politique de sécurité pour le réseau.
        - NK : Définir la clé de sécurité du réseau. S'il est défini sur 0 (valeur par défaut), le périphérique utilisera une clé de sécurité réseau aléatoire.
        - KY : définir la clé de liaison du centre de confiance pour le réseau. S'il est défini sur 0 (valeur par défaut), le périphérique utilisera une clé de sécurité réseau aléatoire.

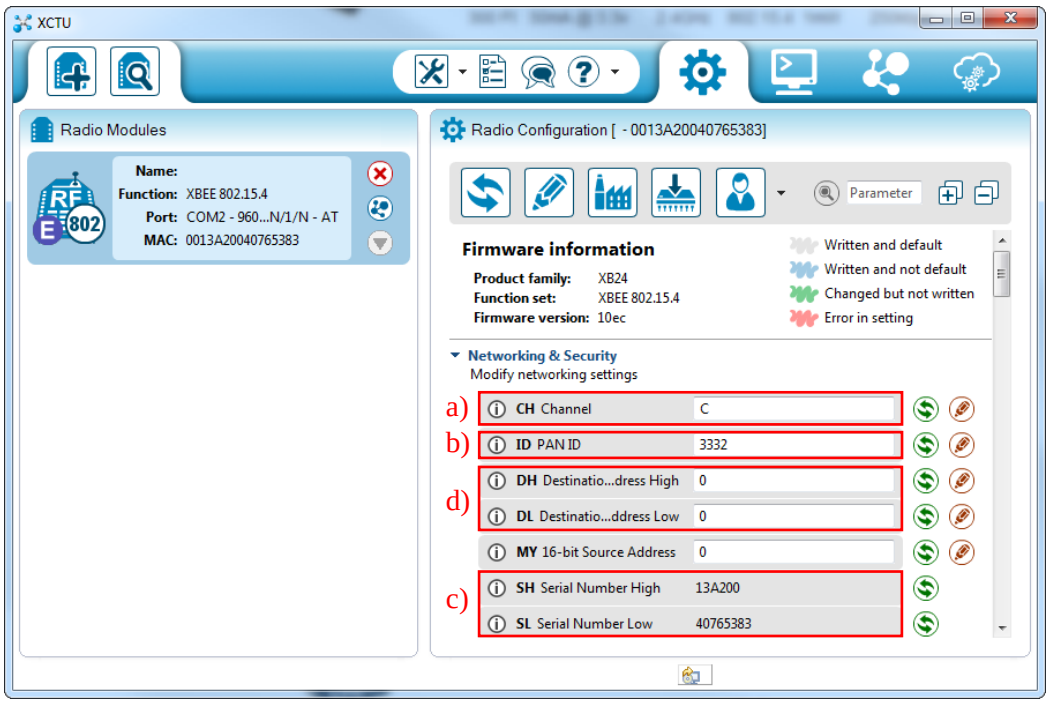


Figure 54 Logiciel XCTU config

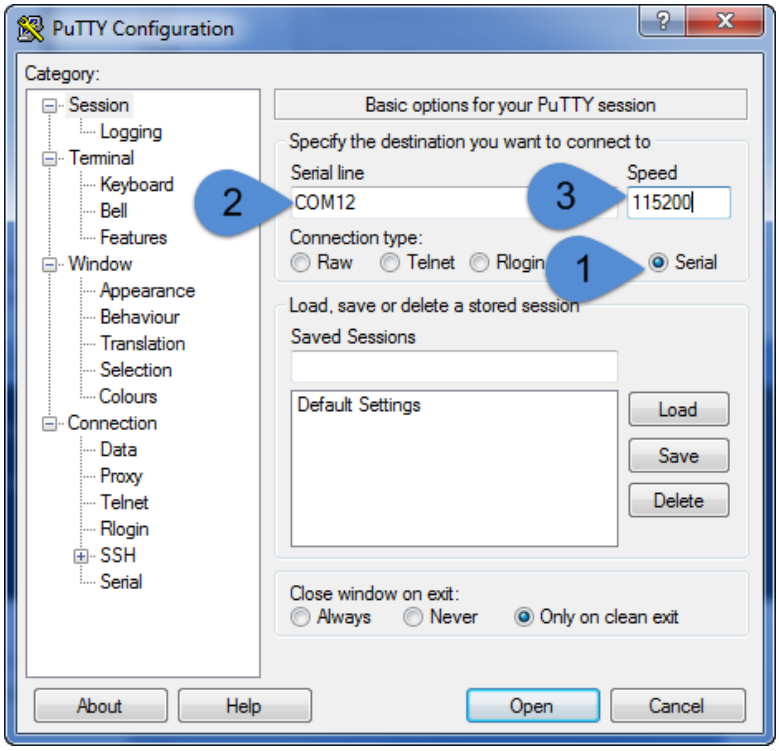


Figure 55 Logiciel Putty connexion avec Serial

1) Le choix de la connexion Serial.
2) Le choix du nom du port Serial COM.
3) Le choix de la vitesse de communication entre les ports.

Par la suite, la connexion se fait par un écran de commande, la configuration des capteurs Zigbee se fait donc par commande.

L'envoie des caractères '+++' est suivie d'une réponse du capteur par OK, et la configuration commence par l'envoie AT suivie du paramètre à changer et de l'entrée.

Exemple :	ATID 2015	réponse OK, pour modifier le PAN ID
	ATDH 13A200	réponse OK, pour le DH
	ATDL 40765383	réponse OK, pour le DL

Une réponse ERE quand la commande ne passe pas.

Après avoir fait une connexion ZigBee :

- L'interception et l'analyse des données reçues à partir de la porte intelligente (Activité tentative d'accès), l'envoie au serveur du Log.

Les commandes possibles :

  - L'allumage de la carte (RUN)
  - L'autorisation d'un utilisateur (ALW)
  - Refus d'un utilisateur (DNY)
  - Message d'erreur (ERE)

- Stockage sur base de données, Ajouter l'envoie des Tokens.

Les fonctions qui peuvent être envoyées à la carte de la serrure intelligente

  - Ajouter utilisateur (ADD)
  - Afficher les utilisateurs (ITR)
  - Supprimer tout (CLR)
  - Redémarrer la carte (RBT)

Le stockage des données dans Base de données (Log, reservation, utilisateur) voici certaines lignes des tables :

	id_log	cmd	cmd_time	key_log
Edit Copy Delete	465	DNY	2019-07-04 16:44:50	b2e373ccc130e75b9157
Edit Copy Delete	466	ALW	2019-07-04 16:45:04	93744b4ad970af56650f
Edit Copy Delete	467	clr	2019-07-04 16:45:15	0
Edit Copy Delete	468	ALW	2019-07-04 16:45:25	93744b4ad970af56650f
Edit Copy Delete	469	DNY	2019-07-04 16:45:42	93744b4ad970af56650f
Edit Copy Delete	470	add	2019-07-04 16:54:21	76dd9af5768676e990fb811555cc2563
Edit Copy Delete	471	DNY	2019-07-04 16:54:45	16ad1dab3d509702328f
Edit Copy Delete	472	ALW	2019-07-04 16:54:58	76dd9af5768676e990fb
Edit Copy Delete	473	clr	2019-07-04 16:55:09	0
Edit Copy Delete	474	ALW	2019-07-04 16:55:25	76dd9af5768676e990fb
Edit Copy Delete	475	DNY	2019-07-04 16:55:40	76dd9af5768676e990fb

Figure 56 Table de BD Log

La table Log a quatre colonnes, id du log, la commande qui a été exécuté que ça soit une tentative d'accès 'ALW' ou 'DNY', ou une commande qui modifie la liste des utilisateurs possibles 'add' et 'clr', la colonne d'après est la date à laquelle l'action a été executé, puis key_log qui est le code d'accès.

id_user	user	password	email	pin	dateReg
1	mehdi	e10adc3949ba59abbe56e057f20f883e	mehdi@fo.rt	4923	2019-06-06 20:09:22
4	esubalew	47108be5188519c2585852d5daf17b76	esubalew@fo.rt	1234	2019-06-06 18:19:10

Figure 57 Table de BD Utilisateur

La table utilisateur a cinq colonnes, nom de l'utilisateur, le hash du mot de passe, l'email, le pin puis la date d'enregistrement. Le pin a été laisser en clair pour pouvoir faire une différence avec le mot de passe mais le stockage se fait toujours haché :

id_res	id_cbr	id_user	date_res	date_debut	date_fin	key_res
67	2	1	2019-07-03 15:32:16	2019-08-04 12:00:00	2019-08-05 12:00:00	l9h1eVjdN3O4ynKMvLzpKXu3XmKKBFZY
68	2	1	2019-07-04 15:01:48	2019-08-04 12:00:00	2019-08-05 12:00:00	F6L8ZrlMVAYkb8UZouwtAbaBkC5Yulrj
69	2	1	2019-07-04 16:27:37	2019-08-04 12:00:00	2019-08-05 12:00:00	NqmkptxunB60StvXJSmqedaeraKwF4nM
70	2	1	2019-07-04 16:37:38	2019-08-04 12:00:00	2019-08-05 12:00:00	pjTmtZJk0C6omIbTjVTOI94d5GTV3hYq
71	2	1	2019-07-04 16:44:21	2019-08-04 12:00:00	2019-08-05 12:00:00	V1fmPWhJ9DQvRNWw21hHxGhtUM4KvbsS
72	2	1	2019-07-04 16:54:19	2019-08-04 12:00:00	2019-08-05 12:00:00	pXQsCrm3bT2Pjw6D8jNE0Q6hZq7qTfJx

Figure 58 Table de BD Reservation

La dernière table réservation a sept colonnes, id de réservation, id chambre et id utilisateur puis les trois dates, les dates de réservation et la date ou la demande a été envoyée, enfin, la key_res qui le token de réservation.

4. Test et confirmation

La figure ci-dessous présente l'architecture finale, nous distinguons notre utilisateur A qui est connecté sur un réseaux locaux LAN à notre machine B qui fait office de serveur, le serveur B est connecté à un réseau faible consommation de technologie Zigbee grâce à son capteur branché. La porte intelligente C à droite de la figure est elle aussi connecté au réseau Zigbee.

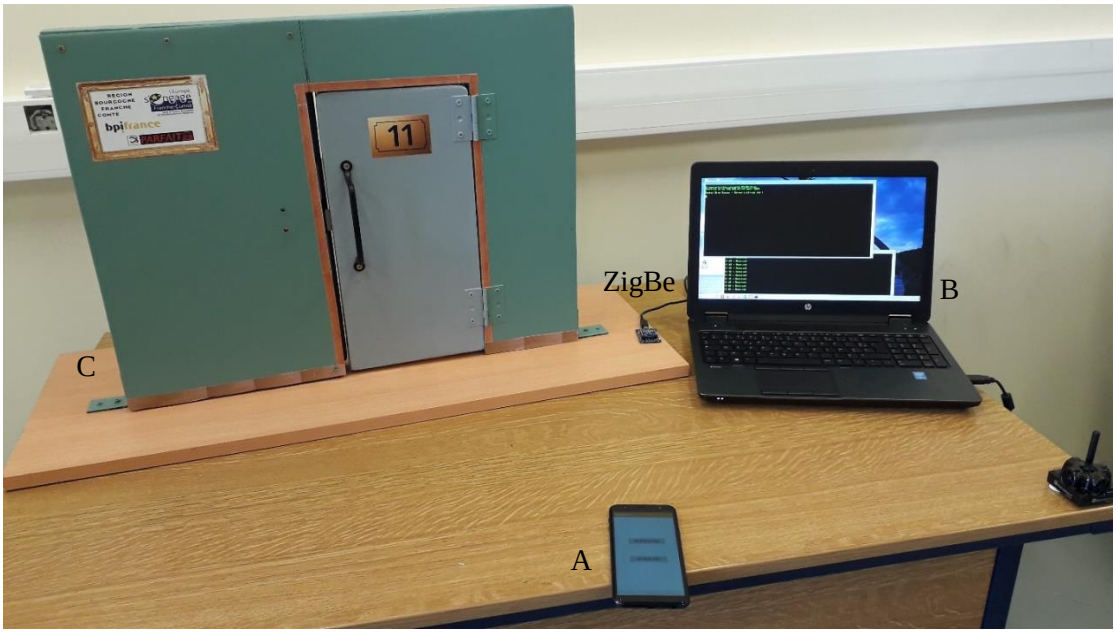


Figure 59 L'architecture final

Après que l'utilisateur soit authentifié, l'utilisateur fait une réservation qui est traité par le serveur. Si la demande est bonne, deux réponses 'token' sont envoyées, l'une à l'utilisateur pour pouvoir accéder plus tard à la porte intelligente et une autre à la porte intelligente pour pouvoir reconnaitre l'utilisateur légitime du mauvais.

Après avoir finalisé la connectivité, des tests sur chaque composant, les réservations, les tentatives d'accès, les résultats ont été ceux qu'on attendait. Nous allons présenter les démarches pour une réservation et simuler un cas réel de scénario :

4.1. Réservation chambre

La réservation se fait en trois étapes :

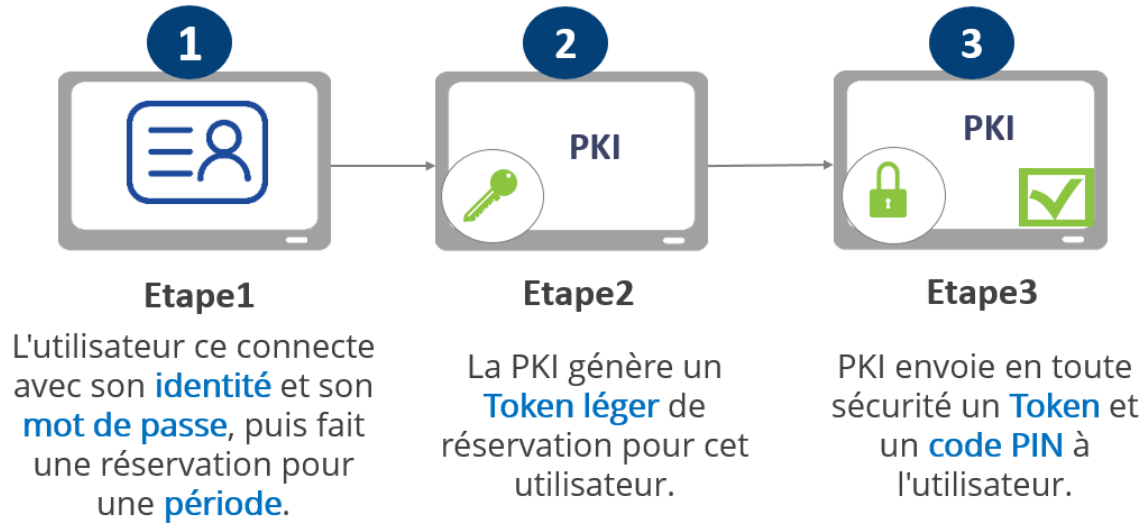


Figure 60 Etape de réservation

La réservation se compose de trois étapes, première étape l'utilisateur doit se connecter avec son identité puis remplir la période de réservation et la chambre. Par la suite la deuxième étape, le token est généré par le serveur. Troisième et dernière étape, l'utilisateur reçoit le token en toute sécurité et reçoit le pin par un autre canal de communication.

- Après avoir fait une réservation pour le 02/07/2019 au 03/07/2019

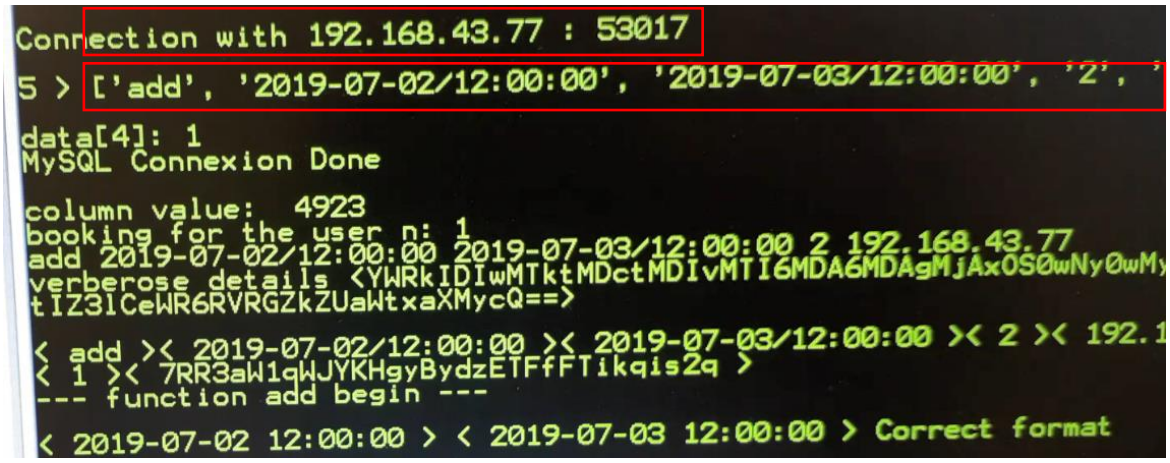


Figure 61 Serveur réceptionnant une requête client

Sur la fig. 61, nous recevons sur le serveur une connexion par client, puis une demande de réservation qui est traité par la suite.

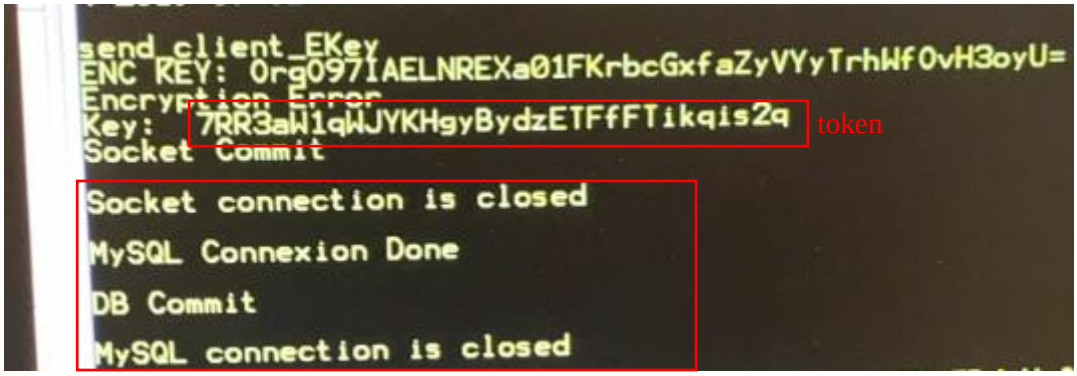


Figure 62 Serveur génération Token et cryptage

Dans la Fig. 62, la génération du Token et sa valeur chiffrée, puis l'envoie de la donnée à l'utilisateur, puis le stockage sur la base de données.

4.2. Accès chambre

L'authentification se fait avec trois informations : information (1) quelque chose que vous avez qui est votre smart phone et votre identité, information (2) quelque chose que vous savez votre code PIN et la information (3) quelque chose que vous obtenez le Token.

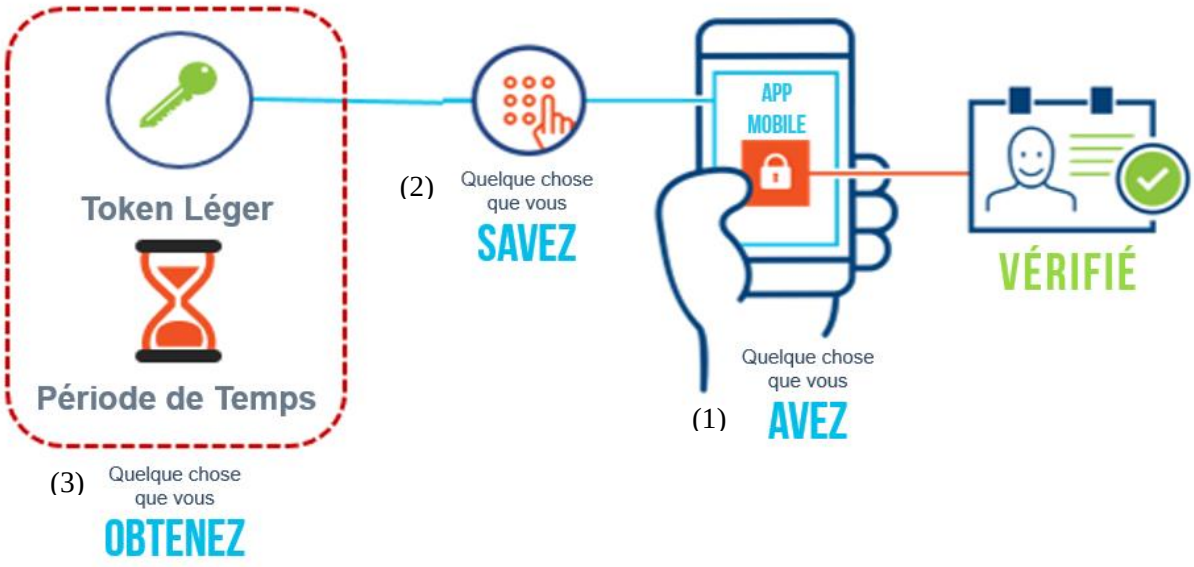


Figure 63 Etape d'accès

Ensuite Fig. 63, un écran de smart phone montrant le même token arrivée à l'utilisateur pour la même période valide.

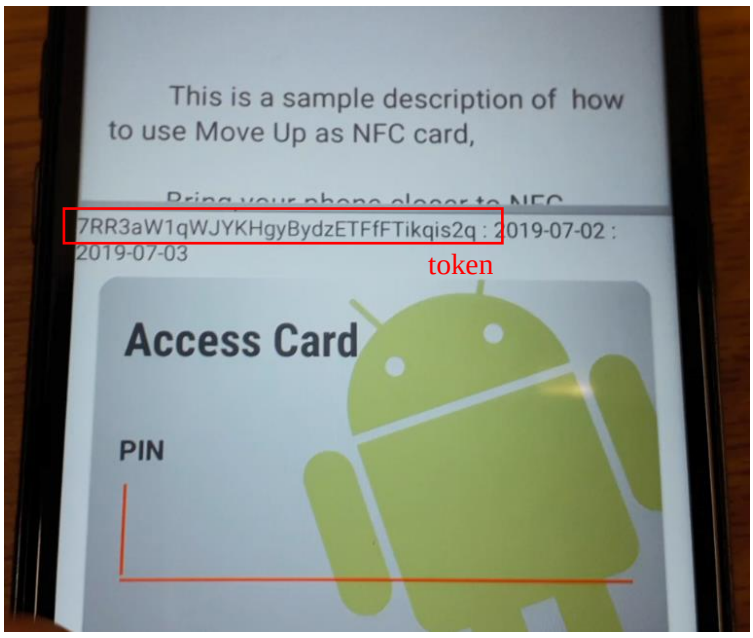


Figure 64 Smart phone réception Token

Après réception du token, l'utilisateur peut entrer son code PIN et utiliser son smartphone pour déverrouiller la porte intelligente.

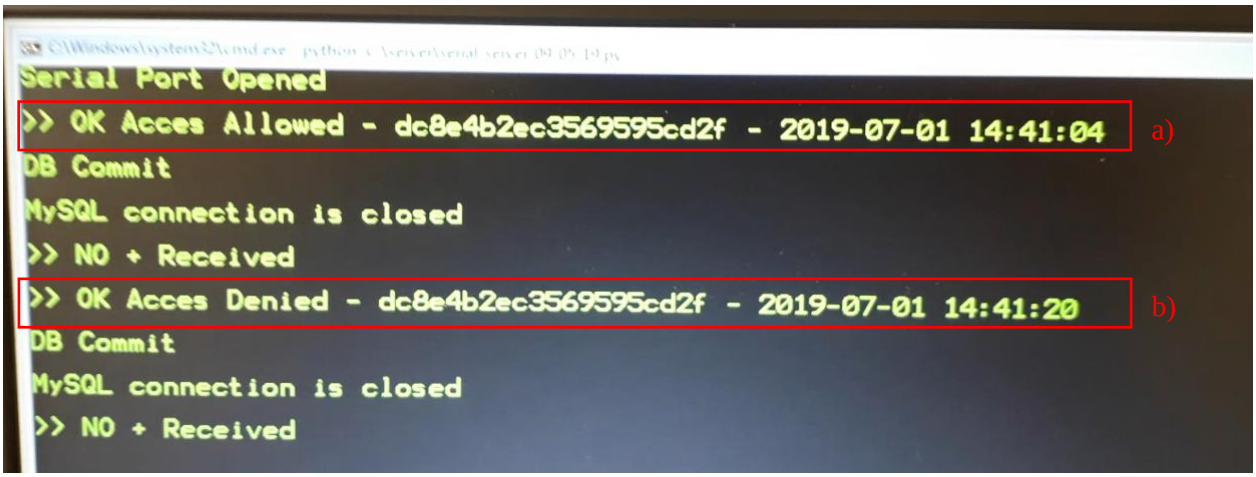


Figure 65 Serveur tentatives d'accès

La figure 65 montre le serveur interceptant les données de la porte intelligente, a) indique une tentative d'accès réussi avec le code d'accès ‘‘dc8e4b2ec3569595cd2f’’ autorisé à 14 :41 :04 puis le même passe d'accès a eu un refus d'accès au b) à 14 :41 :20, ce code d'accès est donc obsolète et ne pourra pas accéder à l'avenir, car le temps de réservation est fini.

4.3. Tentatives possibles

Notre système peut gérer plusieurs cas, aboutant ou échouant.

- Une tentative d'accès de la part d'un bon utilisateur avec une clé valide et son bon PIN obtient le droit à l'accès.

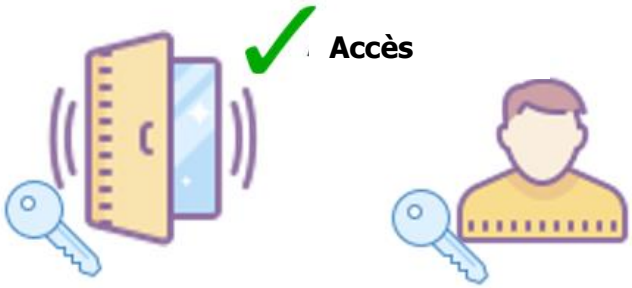


Figure 66 Accès garantie (bonne clé + bon pin)

Figure 67 Droit d'accès à la porte intelligente autorisé

- Une tentative d’accès de la part d’un utilisateur (mauvais ou bon) avec une clé valide et un mauvais PIN n’obtient pas le droit à l’accès.

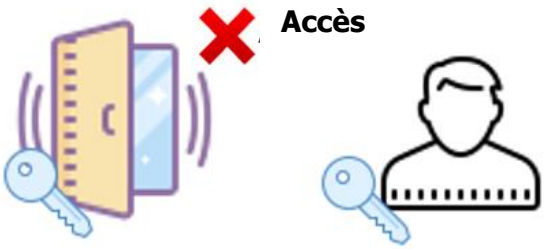


Figure 68 Accès refusé (bonne clé + mauvais pin)

- Une tentative d’accès de la part d’un bon utilisateur avec une clé valide (mais temps d’accès dépassé) et un bon PIN n’obtient pas le droit à l’accès.

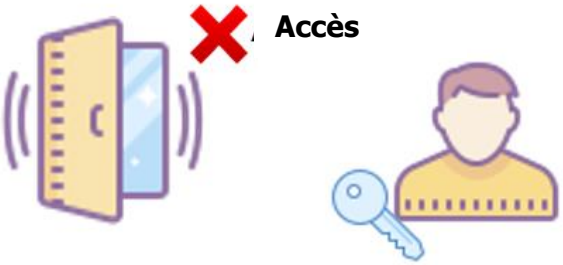


Figure 69 Accès refusé (mauvaise clé + bon pin)

Figure 70 Droit d'accès à la porte intelligente refusé

4.4. Scénario d'attaque et stratégies de défenses

Les attaques malveillantes sont inévitables, pour ça nous avons réfléchi sur plusieurs stratégies.

Lors de l'accès d'un client, il sera difficile pour un attaquant d'intercepté la communication entre ce client et la porte intelligente, Car la technologie utilisé est NFC utilise la proximité de quelques centimètres entre l'appareil mobile et la porte.

.

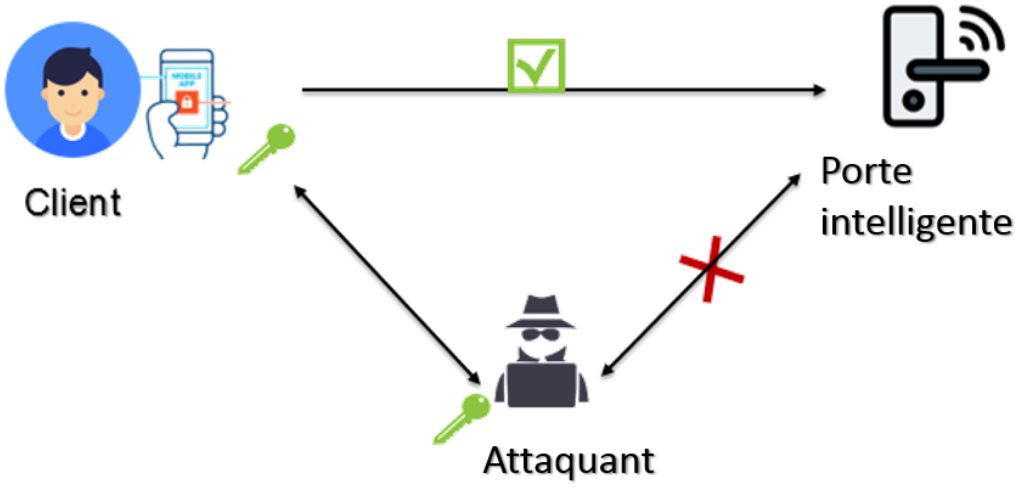


Figure 71 Accès interdit pour l'homme du milieu

Le PIN est envoyé antérieurement par un autre moyen de communication que l'application mobile tel (par sms, email).

Si l'attaquant arrive à intercepter le token, il ne peut pas accéder à la serrure intelligente de la porte car il ne connait pas le bon PIN.

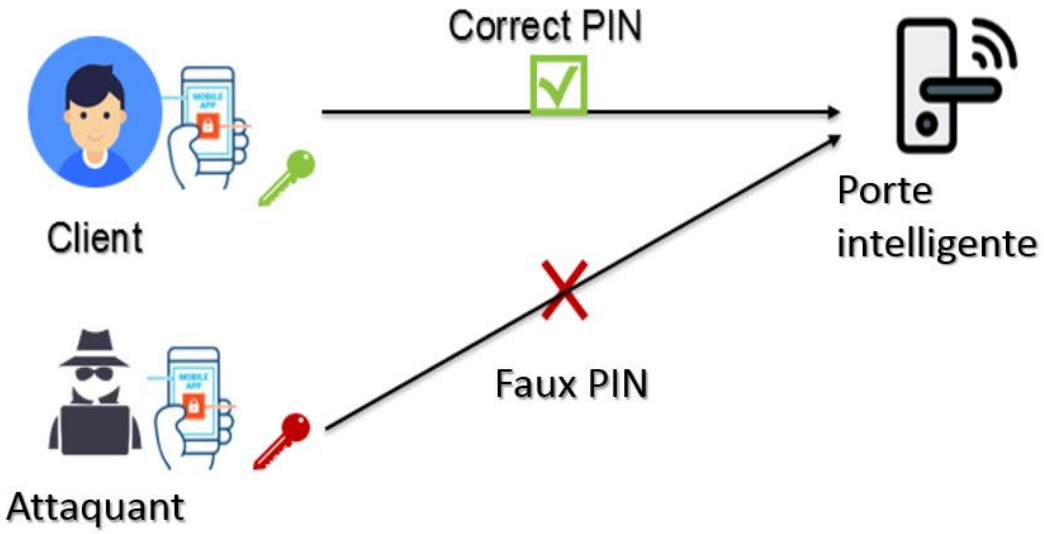


Figure 72 Accès interdit pour faux utilisateur

a) Attaque sur le token

L'attaquant ne peut pas générer le token car il est généré de manière aléatoire.

b) Attaque l'homme du milieu

L'attaquant peut écouter le Token de réservation mais celui-ci est chiffré (AES), il ne peut donc pas y accéder.

c) Attaque sur le code d'accès

L'attaquant peut avoir la code d'accès. Cependant, il est haché (MD5) et la fonction de hachage est irréversible.

d) Attaque vol du smart phone

L'attaquant ne peut pas avoir accès avec le smartphone de l'utilisateur s'il ne possède pas le code PIN.

5. Conclusion

Dans ce dernier chapitre, nous avons exposé une étude de cas, en essayant de présenter les notions essentielles relatives à l'implémentation de notre projet une plateforme de sécurité légère pour IdO. Nous avons présenté le maximum des mises en œuvre requises pour préparer notre environnement, suite au développement et à l'installation de la sécurité.

Cette solution a été un moyen de démonter l'importance et l'efficacité de l'internet des objets tout en respectant la sécurité de l'environnement.

En revanche, notre architecture n'est pas prête à être utilisée dans le cloud ou dans un environnement avec un grand nombre d'utilisateurs en raison du trafic intense qui empêcherait notre système de fonctionner efficacement, comme prévu dans un environnement à faible trafic et à faible consommation d'énergie.

CONCLUSION GENERALE

De nos jours, les objets connectés sont de plus en plus présents autour de nous. Ils ont un besoin grandissant d'accessibilité et de sécurité. En dédiant une plateforme aux objets, on permet à quiconque de se connecter facilement et d'échanger des informations avec l'objet. Le principal avantage d'une telle solution est qu'elle permet de gérer les données échangées avec les objets connectés et avoir toujours conscience des actes fait par un utilisateur.

Comme dans le cas de notre travail, nous avons mis en avant les concepts essentiels de l'IdO, ainsi que les besoins et les défis de la sécurité dans l'IdO. Nous sommes arrivées à notre objectif qui est de développer une preuve pour validé l'approche pour un schéma de sécurité allégée, mettant en œuvre un protocole pour le contrôle d'accès en se basant sur le concept de Tokens.

Dans ce travail, notre projet nous a conduit à introduire l'aspect intelligent de l'objet à la portée de tous, tout en respectant la vie privée de l'utilisateur et en renforçant sa sécurité et son environnement.

Cette étude ne s'arrêtera pas là, conception d'un système plus évolué, résistant à plus d'attaques digital (DOS …) et d'attaque physique (falsification), éventuellement la possibilité de gestion de plusieurs objets et plusieurs utilisateurs, avec un serveur de surveillances actif en temps réel, jusqu'à l'intention d'intégrer une authentification forte avec un protocole d'authentification 'blockchain'.

De plus, notre système n'a pas la capacité d'identifier automatiquement d'autre modèle d'appareil IdO en raison d'une faible compatibilité entre les différents modèles. Le travail futur est donc de créer un système capable d'identifier et de se connecter à diffèrent modèle (Autre objets).

En outre, comme dernière amélioration, il est idéal de créer une plate-forme pour contenir tous les utilisateurs d'un même groupe. Faciliter le partage de clés pour (différente période de temps), afin de permettre et de faciliter l'accès aux différents objets.

Références Bibliographiques

[0] 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'

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

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

[3] Zahoui Anissa Amel,'' Developpement D'une Chaine D'outils En Fonction Du Nouveau Standard Fondationnel Uml(Fuml)'', Universite Badji Mokhtar

[4]P.KADIONIK; Cours de l'option Systèmes embarqués; Ecole Normale Supérieure d'Electronique, Informatique et Radiocommunications de Bordeaux –ENSEIRB; 2004.

[5] Mohamed KOUDIL; Cours intitulé –Méthode de conception conjointe des systèmes embarqués; Institut national de formation et informatique; 2004.

[6] ''http://www.dsi.cnrs.fr/RMLR/textesintegraux/volume4/43-adu14-09-1990(3).htm''

[7] https://www.arduino.cc/en/guide/introduction

[8] https://www.raspberrypi.org/help/what- is-a-raspberry-pi/

[9] http://rasberryaumaoc.blogspot.com/2014/06/comparaison-arduino-raspberry-pi_23.html

[10] IEEE 802.15.2 Recommended Practice: Coexistence of WPAN with other wireless devices operating in unlicensed frequency bands

[11] "IPv6 over Low power WPAN (6lowpan)". IETF. Retrieved 10 May 2016. https://datatracker.ietf.org/wg/6lowpan/

[12] Bluetooth SIG Company Identifiers https://www.bluetooth.org/Technical/

[13] "ZigBee Specification FAQ". Zigbee Alliance. Archived from http://www.zigbee.org/Specifications/ZigBee/FAQ.aspx on 27 June 2013. Retrieved 14 June 2013.

[14] J. Cheng and T. Kunz, "A Surveyon Smart Home Networking," Carlet. Univ. Syst. Comput. Eng. Tech. Rep. SCE-09-10, 2009.

[15]" Overview and Comparison of Leading Communication Standard Technologies for Smart Home Area Networks Enabling Energy Management Systèmes," 46th Int. Univ. Power Eng. Conf, no. September, pp. 1--6,2011

[16] C. Gomez and J. Paradells, "Wireless Home Automation Networks: A Survey of Architectures and Technologies", Technical Univ of Catalonia, IEEE Communications Magazine, June 2010

[17] ZigBee Alliance, "ZigBee Home Automation PublicApplication Profile," revision 25, v. 1.0, Oct. 2007.

[18] ZigBee Alliance, "ZigBee Smart Energy Profile Specifica-tion," revision 15, Dec. 2008.

[19] ZigBee definition " https://www.zigbee.org/zigbee-for-developers/zigbee-3-0/ "

[20] G. Ferrari, P. Medagliani, S. Di Piazza, and M. Martal<'>, "Wireless sensor networks: Performance analysis in indoor scenarios," EURASIP J. Wirel. Commun. Netw., 2007.

[21] D. Han and J. Lim, "Smart home energy management système using IEEE 802.15.4 and zigbee," IEEE Trans. Consum. Electron., vol. 56, pp. 1403-1410,2010.

[22] Eugenia Gabriela NUTA NICOLSCU; Spécification et validation des systèmes hétérogènes embarqués; Thèse pour obtenir le grade de DOCTEUR de l'INPG en microélectronique; Laboratoire TIMATIMA dans le cadre de l'Ecole Doctorale EEATS; Institut national polytechnique de GRENOBLE; 2002.

[23] Security, heise. "Deepsec: ZigBee macht Smart Home zum offenen Haus", " http://heise.de/-3010287 "

[24] NFC definition "https://nfc-forum.org/what-is-nfc/about-the-technology/ "

[25][National Intelligence Council, Disruptive Civil Technologies —Six Technologies with Potential Impacts on US Interests Out to 2025—Conference Report CR 2008–07, April 2008.

[26] Y. Law, L. Van Hoesel, J. Doumen, P. Hartel, P. Havinga. Energy-Efficient Link-Layer Jamming Attacks against Three Wireless Sensor Network MAC Protocols. In Proceedings of ACM SASN, Alexandria, Virginia. November 2005.

[27] W. Xu, K. Ma, W. Trappe, Y. Zhang. Jamming sensor networks: attack and defense strategies. IEEE.Network. Volume 20, number 3. pp 41-47, May-June 2006.

[28] Cluster of European Research Projects on the Internet of Things, "Vision and Challenges for Realisingthe Internet of Things", March 2010.

[29] Babakhouya, A. and Challal, Y. and Bouabdallah, A. and Gharout, S. "Securing Distance Vector Routing Protocols for Hybrid Wireless Mesh Networks",SAR-SSI 2010

[30] Y.ait mouhoub, F.Bouchebbah . Propotion d'un modèle de confaince pour l'internet desObjets, Université A/MIRA de Bejaia . 2015

[31] CNSSI 4009-2015 (NIST SP 800-53 Rev. 4), https://www.cnss.gov/CNSS/issuances/Instructions.cfm

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

[33]"https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.2.0/com.ibm.zos.v2r2.icha700/icha700_Mandatory_access_contrôle__MAC_.htm"
[34] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone, "Guide to Attribute Based Access Contrôle (ABAC) Definition and Considerations", NIST Special Publication 800-162
[35] "SP 800-162, Guide to Attribute Based Access Contrôle (ABAC) Definition and Considerations" (PDF). NIST. 2014. Archived from the original (PDF) on 2016-03-05. Retrieved 2015-12-08. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf
[36] "OrBAC: Organization Based Access Contrôle - The official OrBAC model website". orbac.org. Archived from the original on 2017-06-10. Retrieved 11 September 2017. https://en.wikipedia.org/wiki/Organisation-based_access_contrôle
[37] AllSeen Summit 2015: IdO: Taking PKI Where No PKI Has Gone Before Presented by: Scott Rea – DigiCert Sr. PKI Architect
[38] L. Yang, P. Yu, W. Bailing, B. Xuefeng1, Y. Xinling, L. Geng, "IDO Secure Transmission Based on Integration of IBE and PKI/CA", International Journal of Contrôle and AutomationVol. 6,No. 2, April, 2013
[39] Nadalin A. et al., Web Services Security: SOAP Message Security Version 1.1.1, OA-SIS Standard, Available:http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SOAPMessageSecurity-v1.1.1.pdf Accessed: 15.10.2012
[40] Duncan de Borde, "Considerations for selection of a two-factor authentication système", Siemens Insight Consulting.
[41] https://sites.bu.edu/cmcs/2017/11/16/the-revolution-of-the-mobile-phone-and-its-revolutionary-aspects/
[42] https://www.supinfo.com/articles/single/4356--gestion-projet-methodes-predictives
[43] Java Introduction " https://www.w3schools.com/java/java_intro.asp »
[44] Arduino C definition " https://www.techopedia.com/definition/27874/arduino "
[45] Python definition " https://whatis.techtarget.com/definition/Python "
[46] Android Studio Introduction " https://developer.android.com/studio/intro/ "
[47] SQL Lite site web officiel " https://www.sqlite.org/about.html "
[48] Arduino site web officiel " https://www.arduino.cc/en/main/software "
[49] Xampp definition " https://www.apachefriends.org/index.html "
[50] XCTU definition " https://www.digi.com/products/embedded-systèmes/digi-xbee-tools/xctu "
[51] Putty site web officiel " https://www.putty.org/ "