REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université de Mohamed El-Bachir El-Ibrahimi - Bordj Bou Arreridj

Faculté des Sciences et de la technologie

Département d'Electronique

Mémoire

Présenté pour obtenir

LE DIPLOME DE MASTER

FILIERE : Télécommunications

Spécialité : Systèmes des Télécommunications

Par

- **BOURENNANE FATIMA**
- **BORDJI YAMINA DALIA**

Intitulé

Techniques de Cyber sécurité de Smart-Building à la base des technologies IoT/M2M

La date de soutenance : 29/06/2022

Devant le Jury composé de :

Nom & Prénom	*Grade*	*Qualité*	*Etablissement*
M. ASBAI Nassim	*MCA*	*Président*	*Univ-BBA*
M. AIDEL Salih	*Pr*	*Encadreur*	*Univ-BBA*
Mlle. DJEHAICHE Rania	*Doctorante*	*Co_Encadreur*	*Univ-BBA*
M. BENDIB Sara	*MCA*	*Examinateur*	*Univ-BBA*

Année Universitaire 2021/2022

Remerciements

En préambule ce mémoire nous remercions et glorifions ALLAH le tout puissant et miséricordieux pour la santé, le courage, la volonté, la force et patience qu'il nous a donné durant toute la période d'étude.

Nous tenons à remercier vivement notre encadreur Monsieur le Professeur 'AIDEL Salih' d'avoir accepté de nous guider tout le long de ce travail, et pour sa grande disponibilité, sa patience, ainsi que pour la générosité avec laquelle il a su partager ses connaissances et conseils.

Nos remerciements la plus respectueuse s'adressent à notre Co-encadreur Mlle 'DJEHAICHE Rania' pour ses conseils judicieux, et pour ses précieuses remarques et son soutien.

Nous tenons à citer dans ces remerciements les membres du jury qui ont bien voulu examiner et juger notre travail.

Nous exprimons également notre remerciement, pour nos parents, nos familles, nos enseignants et collègues à l'Université de Mohamed El-Bachir El-Ibrahimi et spécialement nos collègues de la promotion master 2 systèmes des télécommunications.

Et tous ceux qui ont collaboré de près ou de loin à la réussite de ce travail trouvent à travers ces quelques lignes l'expression de notre profonde gratitude pour leur soutien et leurs encouragements de tous les instants. On vous en remercie chaleureusement.

Dédicace

Je dédie ce mémoire

A ceux qui me sont chers, A ceux qui ont toujours cru en moi, A ceux qui m'ont encouragée

A mes chers parents : Aucune dédicace ne pourrait être assez éloquente pour exprimer ce que vous méritez pour tous vos sacrifices qu'elle n'a jamais cessé de me donner.

A toute ma famille (BORDJI, SEDIRI, ZEKHNINE) : ma source d'espoir et de motivation.

A mon fiancé Mehdi symbole de courage et de volonté

A mes chers frères Akrem et Massinissa. Mes adorables sœurs : Ines, Tina et Imen

A mes oncles, mes tantes, mes cousins et mes cousines.

A ma collègue Fatima, A tout le corps enseignant, administratif, toute la Promotion master 2 systèmes des télécommunications 2021/2022

DALIA

Dédicace

Je dédie ce modeste travail

A mes très chers parents

A mon très cher frère

A mes très chères sœurs

A mes amis de la promo

A tous ceux que j'aime et qui m'aiment

FATIMA

Abstract

The aim of this work is to study a security system of a house. The heart of this system is Arduino board in which it is responsible for intelligence and decision to control the peripherals of our communicating house. The human being sometimes has real difficulties, to carry out the activities of the daily life in an autonomous way. Many initiatives have introduced home automation and smart homes as a possible solution for avoiding security risks. However, very few of these achevements have focused on designing an intelligent system to allow people to model a home automation environment. This is doing by intelligent sensors for reading temperature, humidity, ventilation and possible gas leaks. Other implementation are for the detection of occupant movement or intrusion into the house. The communication between the various sensors and the central element is doing by wireless components, using a control interface that has been defining particularly for this home called the GSM module for remote control by sending SMS to the telephone.

Key words: M2M, IOT, smart home, 4G, 5G, mobile communications, smart building, cybersecurity, cyberattaque.

Résumé

Ce travail aborde l'étude et la réalisation d'un système de sécurité d'une maison. Le cœur de
Ce système est une carte Arduino, elle fonctionne comme un élément central responsable de l'intelligence et la prise de décision pour contrôler les périphériques de notre maison communicante. L'être humain éprouvent parfaits de réelles difficultés, à effectuer les activités de la vie quotidienne de manière autonome. De nombreuses initiatives ont introduit la domotique et les habitats intelligents comme une solution possible pour le but d'éviter les risques lié à la sécurité. Cependant, très peu de ces réalisations se sont intéressées à la conception d'un système intelligent pour permettre aux personnes de modéliser un environnement domotique. Cela se fait par des capteurs intelligents pour la lecture de température, l'humidité, la ventilation et d'éventuelles fuites de gaz, un Autre est implémenté pour la détection de mouvement des occupants ou une intrusion dans la maison. La communication entre les différents capteurs et l'élément centrale est assurée par des composants sans fils, en exploitant une interface de contrôle qu'nous avons défini particulièrement pour ce domicile à savoir le module GSM afin de commander à distance par l'envoie des SMS au téléphone.

Les mots clés : M2M, IOT, smart home, 4G, 5G, mobile communications, smart building, cybersecurity, cyberattaque.

ملخص

يهدف هذا العمل الى دراسة وتحقيق نظام أمان للمنزل. باستخدام لوحةاردوينو .قلب هذا النظام هو لوحة Arduino، فهو يعمل كعنصر اساسي مسؤول عن السيطرة على الطرفية للمبنى الخاص بنا. يواجه الانسان احيانا صعوبة كبيرة في القيام بأنشطة الحياة اليومية بشكل مستقل. انجزت العديد من المبادرات للتشغيل الآلي للمباني والمنازل الذكية كحل ممكن بغرض تجنب المخاطر الأمنية. ومع ذلك ، كان عدد قليل جدًا من هذه الإنجازات مهتمًا بتصميم نظام ذكي يسمح للأشخاص بتصميم بيئة أتمتة منزلية. يتم ذلك عن طريق مستشعرات ذكية لقراءة درجة الحرارة والرطوبة والتهوية والتسرب المحتمل للغاز ، و آخرى للكشف عن اي حركة أو التسلل إلى المنزل.و هي تعمل مع وحدة GSM للتحكم عن بعد عن طريق ارسال الرسائل القصيرة للهاتف الذكي.

الكلمات المفتاحية: M2M، IOT ، المنزل الذكي ، 4 G، 5G ، اتصالات الهاتف المحمول ، المباني الذكية ، الأمن السيبراني ، التكاثر الإلكتروني.

Liste des acronymes

2G : 2éme Génération de téléphonie mobile.

3G : 3éme Génération de téléphonie mobile.

4G : 4éme Génération de téléphonie mobile.

5G : 5éme Génération de téléphonie mobile.

APT : Aux menaces persistantes avancée.

BDF : Bourennane Bordji Dalia Fatima.

6LoWPAN : réseaux personnels sans fil de faible puissance.

BLE : Bluetooth basse énergie.

CoAP : Protocole d'application contraint.

DMZ : Demilitarized zone.

DOS: Déni of service.

DDos: Deni de service distrubué

DRDOS: Distributed reflection Denial of service.

GPS: Global positioning system.

GND: Ground (mass).

GSM: Global System For Mobile.

GPRS: General Packet Radio Service.

IDE: Interated Developement Environment.

IDO: Internet des objets.

IDS: Systéme de detections d'intrusions

IEEE: Institute of Electrical and Electronics Engineers.

IoT: Internet of Things.

IP: Internet Protocol.

IPV6: Internet Protocol version 6.

IPS: In-plane switching.

LCD: Liquid Crystal Display.

LED: Lighting emitting Diode.

LoRaWAN : Le réseau étendu à longue portée.

LPWAN: Low-Power Wide Area Network.

LTE: Long Term Evolution.

M2M: Machine to machine.

MQTT: Message Queuing Telemetry Transport.

NFC: Near field communication.

NTIC: Nouvelles technologiesde de l'information et de la communication.

RFID: Radio Frequency Identification.

TCP: Transmission Control Protocol.

SIM: Subscriber Identity Module.

SMS: Short Message Service.

UDP: User Datagram Protocol.

UMTS: Universal Mobile Telecommunications System.

USB: Universal Serial Bus.

V: Volt.

WAN: Wide area network.

WIFI: Wireless fidelity.

WIMAX: Worldwide Interoperability for Microwave Access.

WLAN: Wireless Local Area Network.

WMAN: Wireless Metropolitan Area Network.

WPAN: Wireless Personal Area Network.

WWAN: Wireless Wide Area Network.

WSN: Wireless Sensor Networks.

Z-Wave: Zensys Wave.

SOMMAIRE

LISTE DES FIGURES

LISTE DES TABLEAUX

Introduction générale

Le cyber sécurité des smart buildings fait l'objet d'une attention accrue en raison du nombre toujours croissant de dispositifs IoT en réseau et de la convergence de la sécurité OT et IT.

Les smart buildings résidentiels, commerciaux ou publics d'aujourd'hui sont de plus en plus intelligents : plus confortables, plus économes en énergie et plus autonomes.

Les smart buildings dans lesquels nous vivons et travaillons reposent sur des sous-systèmes de contrôle physique interconnectés et mis en réseau, tels que des appareils de chauffage et de climatisation, des ascenseurs, des détecteurs de fumée, des alarmes, des systèmes de contrôle d'accès et de vidéosurveillance, etc.

Cependant, cette interconnexion transparente des dispositifs IoT rend les bâtiments intelligents de plus en plus vulnérables et susceptibles de subir des cyberattaques aux conséquences coûteuses et destructrices.

De plus en plus de « smart buildings » sont aujourd'hui construits. Ils offrent plus de confort et sont également plus économes et respectueux de l'environnement (gestion optimale de la température, de la ventilation, de l'éclairage…). Ces bâtiments promettent également d'être plus sûrs grâce à des systèmes d'alarmes, de détection d'intrusion, de vidéosurveillance, ou encore de contrôles d'accès.

- **Chapitre I :** présentation des technologies M2M/ IOT leur titre est : Concepts fondamentaux des Réseaux IOT/M2M.
- **Chapitre II :** Le Smart Building à l'ère de la cyber sécurité fait la présentation des smart buildings, da la cyber sécurité, cyber menace, cyber attaque et de la cyber défense.

- **Chapitre III :** C'est la partie pratique de notre projet qui nous a permis de et de proposer la Conception d'une solution de sécurité pour smart building.

CHAPITRE I

Concepts fondamentaux des Réseaux IOT/M2M

I.1 Introduction

L'internet des objets (IoT) et le machine to machine (M2M) sont considérés comme l'un des paradigmes les plus passionnants et les plus révolutionnaires qui ont le pouvoir de changer efficacement la façon dont nous interagissons avec notre environnement.

L'IoT et le M2M permettent à une grande variété de dispositifs intelligents dotés de différentes capacités de calcul, de détection et d'actionnement de communiquer de manière transparente sur l'internet. Il permet une meilleure qualité de vie.

Dans ce chapitre nous présentons les concepts fondamentaux de la communication M2M /IoT, la définition, l'architecture, le fonctionnement, Domaine d'applications dans cette communication. Et au aussi on va voir la différence entre le M2M et la technologie suivante qui est l'Internet des objets (IoT).

I.2 La communication M2M

I.2.1. Définition

La communication de machine à machine est un échange d'informations qui implique des machines ou des dispositifs automatisés communiquant sur un réseau sans intervention humaine ou avec une intervention humaine minimale. [1]

Le M2M comprend des technologies telles que les capteurs mobiles intelligents, les appareils mobiles et les processeurs intégrés qui permettent une interaction à distance avec un serveur ou un appareil. La communication M2M est une technologie prometteuse qui suscite l'intérêt des opérateurs de réseaux mobiles, des entreprises M2M, des fournisseurs d'équipements et, bien sûr, des organismes de recherche. Cependant, l'un des problèmes les plus importants des communications M2M est la congestion. [2]La congestion se produit lorsque la demande dépasse la capacité, affecte toutes les parties du réseau, à la fois la radio et le réseau central, et a un impact sur le plan de données et le plan de contrôle de l'utilisateur.

Pour résoudre cette congestion, les organisations et les chercheurs travaillent sur des solutions depuis quelques années. [3]

I.2.2. L'architecture de la communication M2M

Les appareils M2M peuvent se connecter à la plateforme de service M2M directement via une connexion réseau étendu (WAN) (par exemple, cellulaire 3G/4G) ou une passerelle M2M (point d'agrégation). La passerelle M2M collecte et traite les données des périphériques M2M plus simples et gère-leur configuration/fonctionnement. [4]

Le système M2M est divisé en trois domaines principaux :

1. Le domaine de réseau M2M (ou domaine de dispositif M2M) ;
2. Le domaine de plateforme de service M2M ;
3. Le domaine utilisateur/administrateur.

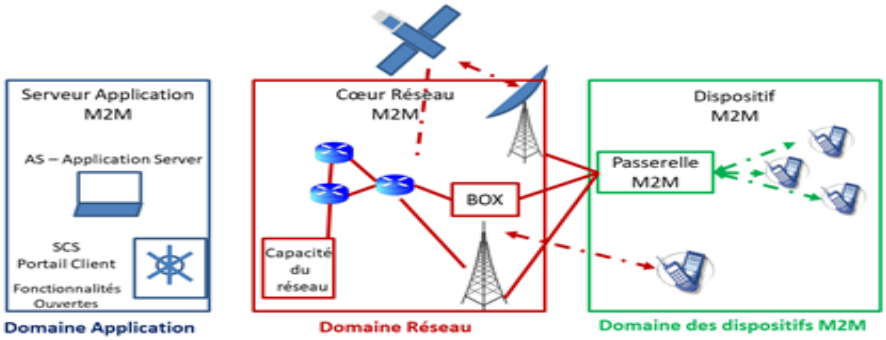

Figure 1: L'architecture fonctionnelle du M2M

I.2.3.La structure du réseau M2M

Dans le schéma de communication M2M, un grand nombre de dispositifs sont nécessaires pour communiquer avec la station de base (BS). Ces schémas se caractérisent par leur simplicité, leur flexibilité et leur faible coût. En outre, les chercheurs ont introduit le mécanisme d'accès multiple par répartition dans le temps pour éliminer les problèmes de collision dans les systèmes à contention. Ainsi, des schémas MAC hybrides, qui contiennent les avantages des protocoles MAC à contention et à réservation, ont été proposés.

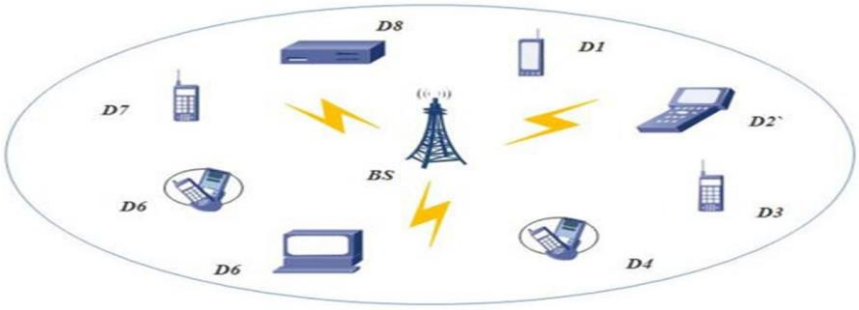

Figure 2: Structure de réseau M2M

Les auteurs ont introduit un protocole MAC hybride pour prendre en charge le trafic vidéo sur les réseaux sans fil. Ils ont étudié les performances avec des schémas MAC basés sur la contention, sur la planification et hybrides. En outre, certaines normes existantes, telles qu'IEEE 802.15.3 et IEEE 802.11ad, ont été adoptées pour les protocoles MAC hybrides afin d'améliorer le débit du réseau. [5,6]

Architecture de trame dans le domaine temporel pour MAC hybride :

Le fonctionnement du réseau M2M s'effectue trame par trame. Chaque trame est composée de quatre parties, à savoir NP, CP, AP et TP, comme le montre la figure. Chaque région sera expliquée en détail comme suit :

- **Période de notification** : Dans cette période, tous les dispositifs reçoivent un message de notification de la part de la BS pour connaître le début de la trame. Après avoir reçu ce message, seuls les dispositifs actifs seront prêts à faire face pendant le CP.
- **Période de validité** : Pendant cette période, les dispositifs qui ont des paquets de données à envoyer sont censés réserver un créneau de transmission dans le TP.

  De nombreux schémas de contention peuvent être utilisés pendant cette période, tels que CSMA, NP-CSMA, P-CSMA, S-ALOHA, etc. Le dispositif doit envoyer un message de demande de transmission REQ à la station de base. La contention n'est considérée comme réussie que lorsqu'il n'y a pas de collision. Par conséquent, la station de base réserve un intervalle de temps valide dans le PT pour ce dispositif. Enfin, la station de base enverra un message à tous les nœuds ayant réussi, avec le numéro de l'intervalle de temps réservé dans le PT. A la réception du message ACK qui inclut le nombre de créneaux horaires alloués, le dispositif cessera d'envoyer un message REQ.
- **Période d'annonce** : Une fois le challenge terminé, la BS commence à diffuser le message d'annonce à tous les numéros de dispositifs.
- **Période de transmission** : Pendant la période de transmission, seuls les dispositifs ayant réussi envoient leurs paquets selon le mécanisme TDMA. Dans ce cas, chaque dispositif réussi se voit attribuer un créneau fixe pour envoyer ses propres paquets jusqu'à ce qu'il ait terminé. Ensuite, son emplacement TDMA sera libéré pour les autres. [5,6]

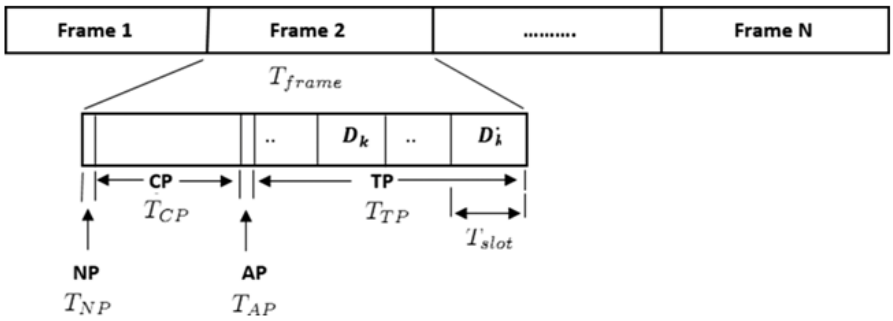

Figure 3: Structure temporelle du schéma MAC hybride

I.2.4. La topologie de la communication M2M

Certaines technologies M2M traitent le scénario où la communication se fait localement entre deux ou plusieurs dispositifs, mais dans le scénario le plus courant, la communication se fait entre des dispositifs situés à distance sur le terrain et un serveur central. Une variante de cette topologie comprend également une passerelle M2M, qui concentre le trafic entre de nombreux dispositifs et le serveur central. La passerelle peut également traduire les protocoles si nécessaire. La topologie de communication M2M est illustrée à la figure 4.

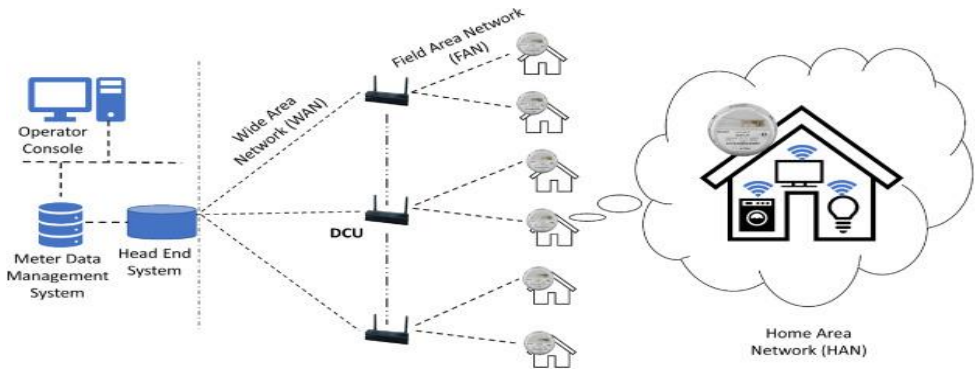

Figure 4: Topologie de communication M2M

Un réseau M2M typique se compose des blocs suivants :

- Réseau longue portée (WAN) ;
- Réseau de terrain (FAN), Réseau de quartier (NAN) ;
- Réseau local domestique (HAN) et Réseau local (LAN).

A) WAN/FAN : Dans ces normes, cellulaire M2M la technologie utilisant 2G/3G/4G/5G joue un rôle important.

B) HAN/NAN/LAN : Pour effectuer le rôle de surveillance, ils sont des capteurs et actionneurs sans fil à grande échelle installés dans un réseau M2M standard.

Ces capteurs jouent un rôle important dans la réalisation de différentes fonctionnalités disponibles dans le réseau M2M [7].

I.3 L'internet des objets (IoT)

Le terme "Internet des objets" (IoT) représente un mécanisme de communication entre des millions de dispositifs. Dans l'IoT, les objets physiques, les objets virtuels et les dispositifs informatiques sont connectés les uns aux autres, ce qui permet à ces dispositifs d'accéder à divers services et de les contrôler à distance [8]. L'IoT désigne l'informatique qui se fond dans notre quotidien pour nous simplifier la vie. Cependant, certaines des informations possédées par les objets sont confidentielles, ce qui pose des problèmes de sécurité pour les individus et les entreprises. Dans cette section, nous présentons la définition de l'IoT, ses domaines d'application, son fonctionnement, son architecture et ses étapes de mise en œuvre.

I.3.1. Définition

L'internet des objets ou ‘Internet of things’ en anglais est "un réseau qui connecte et combine des objets avec l'internet, en suivant des protocoles qui assurent leur communication et l'échange d'informations à travers une variété de dispositifs". [9]

L'IoT peut également être défini comme "un réseau de réseaux qui permet, par l'intermédiaire de systèmes d'identification électronique normalisés et unifiés, et de dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi, de pouvoir récupérer, stocker, transférer et traiter des données de manière transparente entre les mondes physique et virtuel". [10]

Il existe plusieurs définitions du concept d'IoT, mais la définition la plus pertinente pour notre travail de recherche est celle proposée par Weill et Souissi qui ont défini l'IoT comme : " une extension de l'Internet actuel à tout objet pouvant communiquer directement ou indirectement avec des équipements électroniques eux-mêmes connectés à l’Internet. Cette nouvelle dimension de l'Internet s'accompagne de forts enjeux technologiques, économiques et sociaux, notamment avec les grandes économies qui pourraient être réalisées par l'ajout de

Technologies favorisant la normalisation de ce nouveau domaine, notamment en matière de communication, tout en assurant la protection des droits et libertés individuels «. [7,11]

I.3.2. L’architecture du réseau IoT

- **L’architecture de l’IoT à trois couches**

L'architecture IoT typique comporte trois couches : perception, réseau et application, comme le montre la figure 5. [12]

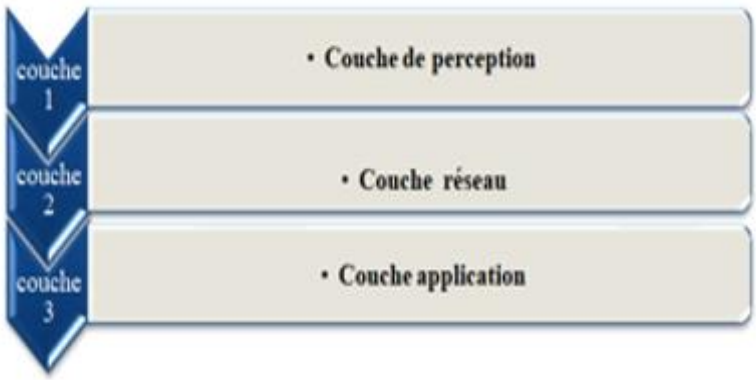

Figure 5: L'architecteur d’IoT à trios couche

1. **La couche de perception**

La couche de perception comprend différents dispositifs physiques IoT; elle est responsable de l’interaction entre les dispositifs et la collecte de données IoT. Responsable de l’interaction entre les appareils et la collecte de données IoT. La collecte de données est effectuée à l’aide de dispositifs intelligents comme des identificateurs de radiofréquence et les capteurs de cations (RFID). [12]

2. **La couche réseau**

La couche réseau traite les données collectées fournies par la couche de perception et stocke ou envoie des données à la couche applicative. C’est la couche la plus importante de l’architecture IoT car elle intègre diverses technologies de communication qui permettent la connectivité des appareils IoT. Technologies de communication largement utilisé comprennent : Zig Bee, Bluetooth LowEnergy (BLE), IPv6 sus réseaux personnels sans fil de faible puissance (6LoWPAN) et longue portée (LoRa WAN). [12]

3. **La couche application**

La couche application reçoit les données de la couche réseau et fournit les services nécessaires aux services aux utilisateurs de l'IoT. Elle prend en charge une grande variété

d'applications telles que la maison intelligente, la vente au détail intelligente, le réseau intelligent, etc.

Les protocoles d'application les plus courants sont le protocole d'application contraint (CoAP) et le transport de télémétrie par file d'attente de messages (MQTT). [12]

- **Architecture à cinq couches :**

L'architecture à trois couches définit l'idée principale de l'internet des objets, mais elle n'est pas suffisante pour la recherche sur l'internet des objets car celle-ci se concentre souvent sur des aspects plus fins de l'internet des objets. Par conséquent, de nombreuses autres architectures en couches sont proposées dans la littérature. La première est l'architecture à cinq couches, qui comprend également les couches de traitement et d'affaires. Les cinq couches sont les couches de perception, de transport, de traitement, d'application et d'entreprise (voir la figure 5). Le rôle des couches perception et application est le même que dans l'architecture à trois couches. Nous décrivons la fonction des trois autres couches. [13]

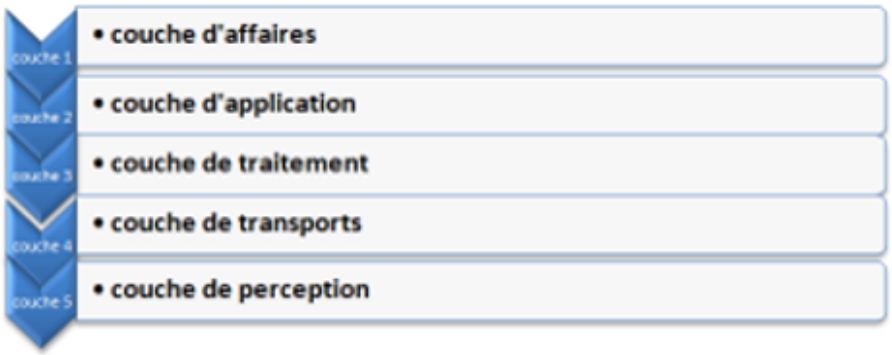

Figure 6: L'architecteur à cinq couches

1. **Couche de transport** :

Cette couche transfère les données du capteur de la couche de perception à la couche de traitement et vice versa à travers des réseaux tels que sans fil, 3G, LAN, Bluetooth, RFID, et NFC. [13]

2. **Couche de traitement** :

Cette couche est également connue sous le nom de couche de middleware. Elle stocke, analyse et traite d'énormes quantités de données qui proviennent de la couche de transport. Elle peut gérer et fournir un ensemble diversifié de services aux couches inférieures. Elle utilise de

nombreuses technologies comme les bases de données, l'informatique en Cloud et les modules de traitement des métadonnées. [13]

3. Couche d'affaires :

Cette couche gère l'ensemble du système de l'Internet des objets, y compris les applications, les modèles d'affaires et de profit, et la vie privée des utilisateurs. Le niveau opérationnel n'est pas visé par le présent document. Par conséquent, nous n'en discutons pas d'avantage. [13]

I.4 Les protocoles des réseaux IoT/M2M

Selon la couverture géographique on distingue 4 types de réseaux :

I.4.1 Les réseaux personnels sans fil (WPAN)

- **Bluetooth (IEEE 802.15.1) :** Le Bluetooth est une technologie de communication sans fil à court portée dont les principales caractéristiques sont une faible puissance de transmission, la robustesse et le faible coût. Elle permet de connecter différents appareils (téléphones cellulaires, ordinateurs ou équipements audio) à un ou plusieurs hôtes. Les systèmes de technologie sans fil Bluetooth peuvent être divisés en deux types : Le mode classique qui offre des débits de données élevés mais une forte consommation d'énergie et le mode Low-Energy (LE) avec une faible consommation d'énergie faible consommation d'énergie.
- **ZigBee (IEEE 802.15.4) :** ZigBee est une norme de communication sans fil WPAN, parmi ses caractéristiques, il a une très faible consommation d'énergie, moins cher et aussi un protocole beaucoup plus simple, ce qui le rend très approprié pour l'intégration dans les petits appareils électroniques. Avec ce type de protocole de communication, les appareils de la maison intelligente pourront désormais communiquer et se connecter de manière plus simple, mais à des distances plus ou moins limitées. [14]

- **NFC :** Near Field Communication (NFC) est une technologie de communication sans fil (WPAN) qui se fait entre deux appareils électriques : un lecteur et un terminal mobile. Cette technologie permet d'échanger des informations et de transmettre des données d'un appareil à un autre dans une distance limitée et proche (moins de 10 cm). L'une de ses caractéristiques est que les données échangées sont envoyées très rapidement. La technologie NFC repose sur un champ de radiofréquences (RF) dont la fréquence de base est de 13,56 MHz. [19]

- **RFID :** Il s'agit d'une technologie qui permet de stocker et de récupérer des informations à distance grâce à une étiquette qui émet des ondes radio. Il s'agit d'une technologie automatique qui code des données numériques dans une " étiquette " RFID, apposée sur un produit, et qui permet à un dispositif à ondes radio de la lire à distance.

I.4.2 Réseaux locaux sans fil (WLAN)

Réseaux locaux sans fil (WLAN) : sont les réseaux privés qui sont administrés par les entreprises et qui couvrent une centaine de mètres (de 10 m à 1 Km), les technologies utilisées sont Ethernet, Wi-Fi.

- **Wi-Fi (IEEE 802.11)** : Le Wi-Fi est un réseau de communication sans fil (WLAN) qui permet de connecter de nombreux appareils informatiques tels qu'un modem Internet, un ordinateur portable ou de bureau, un smartphone ou tout autre appareil. Il permet aux utilisateurs de surfer sur Internet à grande vitesse lorsqu'ils sont connectés à un point d'accès (AP) ou en mode ad hoc. La technologie Wifi est divisée en plusieurs catégories, les normes les plus courantes sont IEEE 802.11 a/ b/ g, la norme IEEE 802.11 ad et la norme IEEE 802.11 ah pour les objets connectés.

I.4.3 Réseaux métropolitains sans fil (WMAN)

Les réseaux qui regroupent plusieurs réseaux LAN c'est-à-dire une ville avec une portée de 4 à 10 kilomètres, la technologie basée sur WMAN est WiMax (IEEE 802.16). [14]

I.4.4 Réseaux étendus sans fil (WWAN)

Les réseaux qui interconnectent les WLAN et les WMAN avec une couverture de centaine ou de milliers de km (un pays ou un groupe de pays). Ces technologies sont GSM, GPRS, UMTS, LTE. [14]

- **GSM (2G) :** Au cours de cette période, toutes les communications sans fil étaient centrées sur la voix. [15]
- **GPRS (2.5G)** Les communications sans fil sont principalement destinées à la voix à haute capacité avec un service de données limité. Le système CDMA utilisant une bande passante de 1,25 MHz a été adopté aux États-Unis.

- **UMTS (3G) :** Pour cette génération, la plate-forme de communication sans fil est dotée de capacités de transmission de la voix et des données ; la 3G est le premier système doté d'une norme internationale publiée par l'UIT. 3G utilise le WCDMA avec une largeur de bande de 5 MHz, il fonctionne à la fois en duplex par répartition en fréquence (FDD) et en duplex par répartition dans le temps (TDD). [16]

Ainsi, en passant des systèmes 2G aux systèmes 3G, on est passé de systèmes centrés sur la voix à des systèmes centrés sur les données. [15]

- **LTE (4G) :** La 4G est un système de transmission de données et de voix à haut débit. Développée après le WiMax, cette technologie est similaire au WiMax. Notez que la bande passante des deux systèmes est de 20 MHz.
- **5G** : commencent actuellement à être mis en œuvre et visent à être 100 fois plus rapides que les réseaux 4G actuels. Les réseaux 5G offriront des débits de données allant jusqu'à 10 Gbps, une faible latence (en millisecondes) et une plus grande fiabilité. Imaginez qu'un film HD puisse être téléchargé en quelques secondes seulement. Cette technologie peut prendre en charge de nombreux appareils compatibles avec l'Internet des objets (IoT) et des véhicules intelligents, comme le montre la figure 3. Une technologie d'accès sans fil efficace, capable d'augmenter le débit sans augmenter la bande passante ou densifier la cellule, est essentielle pour répondre aux exigences permanentes de la 5G. Certains des avantages significatifs de la 5G sont les suivants :
  - **Le débit de données** : Le réseau 5G fournirait un débit de données allant jusqu'à 10 Gbps, ce qui est presque cent fois mieux que les réseaux 4G.
  - **Latence** : le réseau 5G offre une latence aussi faible que 1 ms, contre 10 ms pour les réseaux 4G.
  - **Signalisation efficace** : Les réseaux 5G fournissent une signalisation efficace pour la connectivité IoT et la communication M2M.
  - **Expérience utilisateur** : La 5G améliore la réalité augmentée, la réalité virtuelle et l'intelligence artificielle.

- **Autonomie de la batterie** : la 5G offre une autonomie de près de dix ans pour les appareils IoT à faible puissance.

Figure 7: Evolution des réseaux mobiles

I.5 Les domaines d'applicationsdeM2M/IoT

Il existe une panoplie de domaines d'applications pour le paradigme IoT/M2M que ce soit dans le monde industriel ou dans la vie quotidienne. Dans cette partie on va présenter quelques domaines d'applications de l'IoT/M2M [17].

Figure 8: Les domaines d'applicationsdeM2M/IoT

I.5.1 Maison intelligente [18]

- **Appareils électroménagers intelligents** : réfrigérateurs avec écran LCD indiquant ce qui est à l'intérieur, la nourriture qui est sur le point d'expirer, les ingrédients que vous devez acheter et avec toutes les informations disponibles sur une application pour smartphone.

- **Surveillance du gaz** : informations réelles sur l'utilisation du gaz et l'état du gaz lignes

pourraient être fournies en connectant les compteurs de gaz résidentiels à Internet protocole (IP) réseau. Quant à la surveillance de l'eau, le résultat possible réduction des coûts de main-d'œuvre et d'entretien, amélioration de la précision et réduction des coûts de lecture des compteurs et, éventuellement, réduction de la consommation de gaz [19].

- **Bijoux intelligents** : Sécurité personnelle accrue grâce au port d'un bijou inséré avec la technologie compatible Bluetooth utilisé d'une manière qu'une simple poussée établit le contact avec votre smartphone, qui par le biais d'une application enverra les alarmes aux personnes sélectionnées dans votre cercle social avec les informations dont vous avez besoin aide et votre emplacement.

I.5.2 Surveillance de l'environnement intelligent

- **Pollution atmosphérique** : contrôle des émissions de CO2 des usines, pollution émise, par les voitures et les gaz toxiques produits dans les fermes [20].

- **Protection de la faune** : Colliers de suivi utilisant des modules GPS/GSM pour localiser et suivre les animaux sauvages et communiquer leurs coordonnées par SMS.

- **Réseau de stations météorologiques** : Étude des conditions météorologiques dans les champs pour prévoir la formation de glace, la pluie, la sécheresse, la neige ou les vents [21].

I.5.3 Energie intelligente

- **Réseau intelligent**: Suivi et gestion de la consommation d'énergie.

- **Installations photovoltaïques** : surveillance et optimisation des performances dans les centrales solaires.

- **Niveaux de rayonnement** : Mesure distribuée des niveaux de rayonnement dans le nucléaire l'environnement des centrales électriques pour générer des alertes de fuite. [19]

I.5.4 Bâtiment intelligent

- **Présence de liquides** : détection de liquides dans les centres de données, les entrepôts et les terrains sensibles du bâtiment pour prévenir les pannes et la corrosion.

- **Thermostat intelligent** : Thermostat qui apprend la programmation des utilisateurs

Calendrier après quelques jours, et de ce programme lui-même. Peut être utilisé avec une application pour se connecter au thermostat à partir d'un téléphone intelligent, où le contrôle, l'histoire de l'énergie, combien d'énergie est économisée et pourquoi peut être exposé.

- **Alarme incendie intelligente** : Système avec capteurs mesurant la fumée et le carbone monoxyde, donnant à la fois des alertes précoces, des alarmes hurlantes et parle la voix humaine qui dit où est la fumée ou quand les niveaux de monoxyde de carbone sont en hausse, en plus de donner un message sur le smartphone ou la tablette si la fumée ou l'alarme de CO se déclenche.

- **Systèmes de détection d'intrusion** : Détection des ouvertures de fenêtres et de portes et les violations pour prévenir les intrus.

I.5.5 Transport intelligent et mobilité

- **Paiement NFC** : Traitement des paiements en fonction de l'emplacement ou de la durée de l'activité pour les transports en commun, les gymnases, les parcs d'attractions, etc.

- **Le suivi des véhicules trafic** : Où les capteurs sur les routes peuvent permettre de détecter les embouteillages trafic, les routes polluées ou les chaussées endommagées et de proposer dynamiquement un réacheminement pour les utilisateurs finaux disposant d'un équipement de type GPS et capables de recevoir de telles informations.

I.5.6 Santé intelligente

- **Surveillance de l'activité physique des personnes âgées :** réseau de capteurs corporels mesure le mouvement, les signes vitaux, la discrétion et une unité mobile recueille visualise et enregistre les données d'activité. [19]
- **Surveillance des patients** : Surveillance de l'état des patients à l'intérieur les hôpitaux et les maisons de retraite.
- **Gestion des maladies chroniques** : Des systèmes de surveillance des patients avec des statistiques complètes sur les patients pourraient être disponibles pour la surveillance résidentielle à distance des patients atteints de maladies chroniques comme les maladies pulmonaires et cardiaques. [19]

I.5.7 Industrie intelligente

- **Digue de réservoir** : Surveillance des niveaux d'eau, de pétrole et de gaz dans les réservoirs de stockage et les citernes. [19]

I.6 Les différences majeures entre le M2M et l'IoT

Il est important de bien différencier les deux notions IoT et M2M. Le M2M est un dispositif qui capture un événement et le transmet sur le réseau à une application. L'application traduit l'événement en information significative. Il s'agit des technologies qui permettent aux systèmes sans fil et câblés de communiquer avec d'autres appareils de ce genre. Ainsi l'IoT est un réseau d'éléments identifiables qui communiquent sans interaction humaine en utilisant la connectivité IP Il s'agit davantage de complémentarité que de différences. En effet, l'IoT est un ensemble technologique plus large, qui comprend les applications M2M, les objets (radars), la connectivité, les données, la gestion des applications d'exploitation et enfin les réseaux. Quant au M2M, il se réfère aux réseaux mobiles et aux technologies traditionnelles 2G ,3G, 4G ,5G.

M2M	IoT
Principe communication point à point entre les machines	Communications dans un écosystème d'objets, plateformes, applications, utilisateurs
Les appareils ne reposent pas nécessairement sur une connexion Internet	Les appareils dépendent d'une connexion Internet
M2M est principalement basé sur la technologie matérielle	L'IoT est une technologie à la fois matérielle et logicielle
Un appareil peut être connecté via un réseau mobile ou autre	La livraison des données dépend du réseau de protocole Internet (IP)
Protocole propriétaires	Standards, ceux l'internet notamment
Solution alimentées (via secteur ou batterie externe à	Capteurs sans fil (sur batterie ou alimentes)
Temps réel possible	Pas de temps réel (hors alarmes)
Grand quantité de données	Très peu de données

Tableau 1: Les différences majeures entre le M2M et l'IoT

I.7Les avantages et les inconvénients du M2M/IoT

I.7.1 Les avantages

- Il peut aider à contrôler plus intelligemment les maisons et les villes via les téléphones portables, à améliorer la sécurité et à offrir une protection personnelle.
- Sans intervention humaine, les machines automatisent et contrôlent une grande quantité d'informations, ce qui conduit à une production plus rapide et plus ponctuelle.

I.7.2 Les inconvénients

- Avec l'avènement de la technologie, les activités quotidiennes sont automatisées par l'utilisation de l'IoT avec moins d'intervention humaine, ce qui entraîne une diminution des besoins en ressources humaines. Cela entraîne un problème de chômage dans la société.
- Les pirates informatiques peuvent accéder au système et voler des informations personnelles. Puisque nous ajoutons tant d'appareils à l'Internet, il y a un risque que nos informations soient utilisées à mauvais escient. [20]

I.8 Conclusion

Dans ce premier chapitre, nous avons présenté une étude générale sur les réseaux IoT/M2M, leurs définitions, architectures et protocoles, ainsi que leurs applications. Nous avons ensuite abordé la différence entre M2M et IoT. Nous avons terminé ce chapitre par citer les avantages et les inconvénients de l'IoT/M2M. Ainsi, dans le prochain chapitre, nous allons aborder le bâtiment intelligent à l'ère du cyber sécurité.

CHAPITRE II

Le Smart Building à l'ère de la cyber sécurité

II.1 Introduction :

Le cyberespace est un nouvel univers sans frontières dans lequel tous les acteurs partagent de l'information et communiquent à travers Internet dans tous les domaines (des services bancaires à l'infrastructure gouvernementale), tout est contrôlé et exploité au moyen d'Internet.

Lorsque nous pensons au smart building, nous pensons immédiatement à leurs avantages. Nous pensons aux gains d'efficacité que cette technologie de bâtiment connecté offre aux promoteurs, aux gestionnaires d'immeubles et aux locataires. Qu'il s'agisse d'efficacité, de valeur à long terme ou de perception de la marque, les parties prenantes souffriront si leur bâtiment n'est pas "intelligent". Cependant, pensons-nous aux risques de cyber sécurité ?

Pour atténuer ces attaques et exploiter pleinement le potentiel des bâtiments intelligents, les exploitants et les occupants doivent modifier la manière dont les systèmes de contrôle des bâtiments intelligents sont conçus et gérés du point de vue du cyber sécurité. L'élimination des barrières organisationnelles et la reconnaissance de la déconnexion entre l'informatique et les technologies de l'information constituent la première étape essentielle de la mise en œuvre et de l'exploitation de systèmes de contrôle de bâtiments intelligents cyber sécurisés.

Fondamentalement, les organisations peuvent créer un bâtiment intelligent sécurisé et opérationnel de quatre manières principales :

1. Évaluer et protéger les anciens systèmes de contrôle OT du bâtiment
2. Choisir des dispositifs IoT et des fournisseurs qui suivent une approche de cycle de vie de développement sécurisé.
3. Mettre en œuvre des architectures de systèmes de contrôle de bâtiments OT sécurisés.
4. Relier les systèmes sécurisés de contrôle des bâtiments OT par une zone de surveillance de la sécurité informatique.

Dans ce chapitre, nous examinerons certains des concepts de smart building, cyber sécurité, Cyberattaque, cyber menaces et cyber défense.

II.2 Le smart building:

II.2.1 Définition :

Le concept de smart building correspond à l'intégration de solutions de gestion active et passive de l'énergie, visant à optimiser la consommation, mais aussi à favoriser le confort et la sécurité des usagers du bâtiment tout en respectant les réglementations en vigueur [21].

Le smart building consiste en la conception d'une maison ou d'un bâtiment où le

fonctionnement du plus grand nombre d'équipements électriques possible est à la fois automatisé et coordonné. Les objectifs principaux d'un bâtiment intelligent sont les suivants :

- Optimiser le confort des résidents
- Améliorer la sécurité du logement
- Réaliser des économies d'énergie, etc.

Cependant, le principe de la maison connectée implique de profonds changements dans le mode de vie de chacun pour se généraliser. Le développement de ce type de construction a donc été lent pendant plusieurs décennies. Cependant, les dernières évolutions, ainsi que l'augmentation des intérêts environnementaux dans le secteur du bâtiment, font du smart building une solution de plus en plus attractive. [21]

I1.2.2 Les nouvelles technologies de l'information et de la communication (NTIC)

Dans le domaine de la construction durable, la domotique est une solution qui optimise l'efficacité énergétique. En effet, un bâtiment communicant est qualifié d'infrastructure à haute efficacité énergétique puisqu'il prend en compte tous les aspects de la maison, parmi lesquels :

- Les équipements consommateurs de l'électricité ;
- Les équipements producteurs de l'électricité ;
- Les équipements de stockage de l'électricité, etc.

Le bâtiment intelligent prend également en compte les panneaux photovoltaïques ainsi que l'électricité stockée pour alimenter les véhicules électriques ou encore la gestion du chauffage.

Les nouvelles technologies de l'information et de la communication (*NTIC*) font référence au secteur de la télématique. Ce terme désigne la multiplication actuelle des sources d'information, leur stockage et leur usage, mais aussi la production, la transmission et les formes que prennent ces informations. La domotique est le prolongement de la télématique, adaptée et appliquée aux bâtiments. La transposition des NTIC au domaine du bâtiment implique quelques changements au sein des maisons, mais également des infrastructures accueillant des travailleurs. En effet, un bâtiment intelligent se charge de la gestion électrique du logement, c'est-à-dire :

- L’éclairage ;
- Le chauffage ;
- Les équipements électroménagers ;
- Les systèmes de surveillance, etc.

Il est possible d’obtenir une maison connectée en construction, mais aussi en rénovation. En effet, les technologies actuelles permettent de mettre en place de nouvelles techniques pour que les équipements soient adaptés aux besoins de la maison connectée :

Types de modifications nécessaires	Types d’équipements adaptés
Equipements adaptés	• Eclairage basse consommation • Ballon d'eau chaude
Nouvelles technologies	• Objets connectés au Wi-Fi • Communication des différents équipements entre eux
Gestion de l'électricité	• Stockage de l'énergie produite • Autoconsommation • Fonctionnement réduit ou différé

Tableau 2: Types de modifications nécessaires et d’équipements adaptés

II.3 Le smart building comme environnement de travail

En dehors du cadre des habitations, le smart building est également une solution pour les entreprises. En effet, le bâtiment connecté permet de créer un véritable écosystème de services pouvant être utilisés par les salariés. L’environnement du bâtiment n’est alors pas géré par les résidents mais par les employés afin d’optimiser la consommation et le confort de l’espace dans lequel ils travaillent.

Le smart building comme environnement de travail permet à tout employé d’une entreprise de gérer son environnement propre à distance. Il peut ainsi allumer le chauffage le matin avant de se rendre au travail ou éteindre la programmation automatique lorsqu’il est parti en voyages d’affaires. Tout comme pour le smart building à destination de l’habitat, le smart building pour le travail permet une gestion du bâtiment rendue possible via une application sur un smartphone et une analyse des habitudes de chacun pour régler la consommation de l’infrastructure au plus près des besoins. [21]

II.4 Les avantages du smart building

La mutation des infrastructures et la mutation des villes accueillent le principe du smart building pour ces apports dans de nombreux domaines. Le smart building apporte en effet :

- Une réelle flexibilité ;
- Une faible empreinte carbone ;

Caractéristiques du smart building	Avantages
Une gestion énergétique connectée	• Permet de réaliser des économies d'énergie • Permet d'améliorer le confort des habitants
Une gestion de la sécurité des bâtiments	• Permet d'améliorer la sécurité des résidents
Une gestion des accès des bâtiments	• Permet de sécuriser les résidences et les logements individuels (gestion des accès : badge, reconnaissance vocale, biométrie.
Une connectivité internet extrêmement performante	• Permet de créer un véritable environnement de vie en réseau
Une interactivité entre les résidents Et le Bâtiment via des objets connectés avec des applications accessibles via smartphone et autres appareils	• Aide à mieux gérer la consommation énergétique d'un logement • Permet de déclencher ou • d'éteindre des appareils à distance • Permet de réaliser des économies d'énergie

Un système analytique des données	• Capable d'optimiser la gestion intelligente du bâtiment grâce à l'analyse des données collectées

Tableau 3: Les avantages du smart building

II.5 La cybersécurité des maisons connectées

Les données personnelles des personnes sont en effet utilisées pour le fonctionnement du smart building. Ainsi, la cybersécurité doit être à même d'éviter les vols de données mais Aussi l'accès à la maison, et aux cambriolages. Raison pour laquelle, le domaine du cyber sécurité se développe à la même vitesse que la technologie propre au smart building. [21]

II.3 Cybersécurité

II.3.1 Définition :

Tout d'abord, définissons deux termes : sécurité de l'information et cybersécurité. La sécurité de l'information est le processus qui consiste à protéger les données contre tout accès non autorisé tout en assurant leur disponibilité, leur confidentialité et leur intégrité. La cybersécurité est l'ensemble des technologies, processus et pratiques conçus pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés ; en d'autres termes, elle implique davantage que la protection des données. Par conséquent, la sécurité de l'information peut réellement être considérée comme un sous-ensemble de la cybersécurité. Cependant, en réalité, ces termes sont utilisés de manière interchangeable. Nous pouvons conclure que la différence entre la sécurité de l'information et la cybersécurité est que la cybersécurité comprend quelques éléments supplémentaires tels que la sécurité des applications, la sécurité des réseaux, la reprise après sinistre et la planification de la continuité des activités. [22]

L'objet du cyber sécurité est de maîtriser les risques liés à l'usage du numérique et du cyberespace. Cela concerne toutes les infrastructures, tous les systèmes d'information, services et données ainsi que tous les acteurs qui dépendent du numérique. Le schéma simplifié, ci-

dessous, permet de mieux comprendre la posture de sécurité et de résilience.

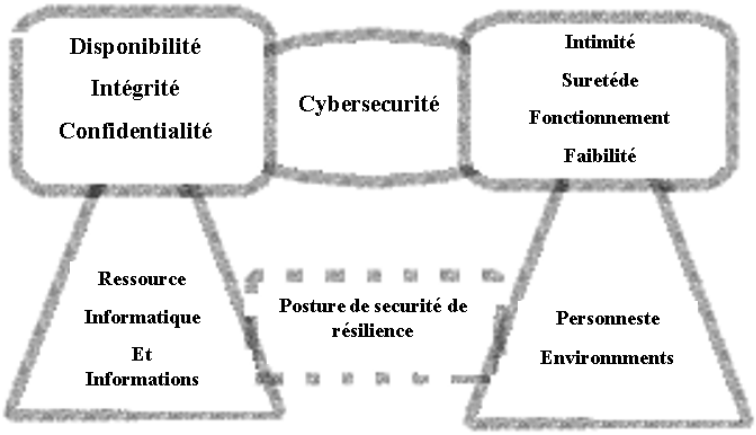

Figure 9: Cybersécurité, posture de sécurité et de résilience

II.3.2 Sécurité de l'information

La sécurité de l'information est un système composé de nombreux éléments : logiciels, matériel informatique, données, personnes, procédures et réseaux (Whitman et Mattord 2012). Chaque composant du système a clairement des exigences de sécurité différentes, mais elles sont toutes basées sur le modèle de triade de sécurité de la CIA (44 United States Code, section 3542). La figure ci-dessous présente : Security triad.

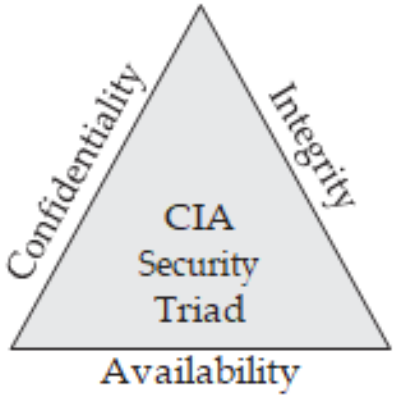

Figure 10: Sécurité triade.

Les définitions officielles des caractéristiques de sécurité et du modèle sont les suivantes [23]

- **Disponibilité :** Garantir un accès fiable aux informations et leur utilisation à tout moment.

- **La confidentialité** : Préserver les restrictions autorisées en matière d'accès et de divulgation, y compris les moyens de protéger la vie privée et les informations exclusives.
- **Intégrité :** Protection contre la modification ou la destruction inappropriée de l'information, et garantie de la non-répudiation (non-négation ou preuve de quelque chose) et de l'authenticité de l'information.

II.3.3. Architecture de sécurité

L'architecture de sécurité est essentiellement une description ou un plan de la manière dont les contrôles de sécurité sont liés aux systèmes d'information. Les contrôles sont ce qui va permettre de maintenir la triade (intégrité, disponibilité et confidentialité). [23]

La figure suivante présente : Spheres of security.

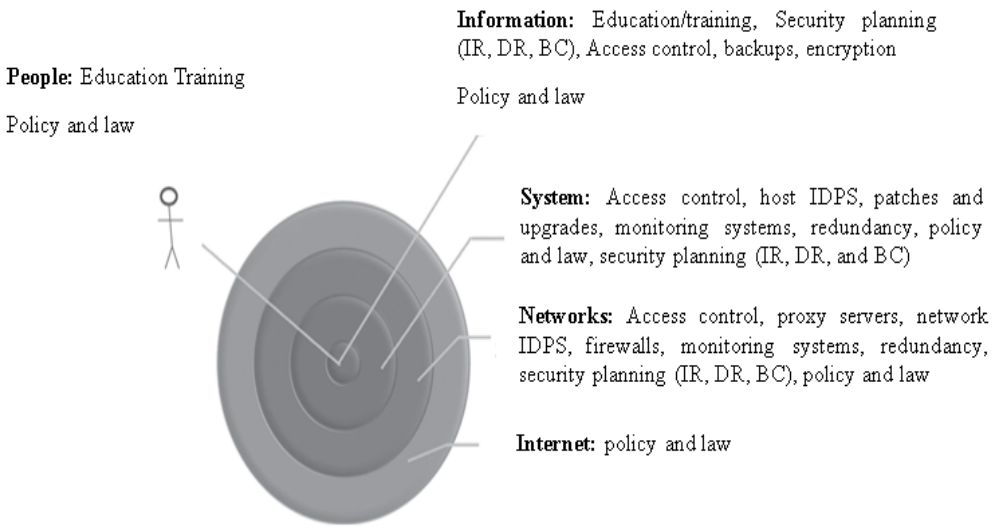

Figure 11: Sphères de sécurité.

II.3.4 Contrôle d'accès

Le contrôle d'accès est essentiel pour minimiser les vulnérabilités du système. Il restreint non seulement qui ou quoi à accès à la ressource, mais aussi le type d'accès autorisé. Voici le contrôle d'accès expliqué en cinq étapes "faciles" [23]

- Identifier de manière fiable l'utilisateur/le système
- Déterminer à quelle ressource l'utilisateur/le système souhaite accéder
- Déterminer si l'utilisateur/le système a la permission d'accéder à la ressource
- Autoriser ou refuser l'accès

- Répéter

II.4 Cyberattaque

Ce crime sur Internet se produit tous les jours, et de nouveaux cas sont signalés chaque semaine dans le monde entier. Les dispositifs à risque d'attaques dans une maison intelligente sont généralement les serrures de porte, les ampoules, les téléviseurs intelligents qui sont utilisés comme écoute par les entreprises de fabrication ou les pirates pour connaître toutes les activités à l'intérieur d'une certaine maison. Dans [24], il est dit que l'Amérique, la Chine et certains pays d'Europe sont vulnérables aux cyber-attaques des maisons intelligentes, les dommages sont enregistrés alors que les propriétaires sont à l'intérieur de la maison ou parfois à l'extérieur, les attaques se font par le biais de courriels malveillants ou via des réseaux intelligents. Dans de nombreux bâtiments, des dispositifs intelligents sont installés, tels que des capteurs, des thermostats, des ampoules intelligentes, de sorte que, si des cyber-attaques
Se produisent, le réseau peut être compromis, en installant des dispositifs pour avoir accès à l'audio de l'ensemble du bâtiment, en installant des logiciels qui donnent la possibilité de savoir quand les propriétaires ne sont pas à la maison ou le réseau entier devient négocié.

Une cyberattaque est l'exploitation délibérée de systèmes informatiques, d'entreprises et de réseaux tributaires de la technologie. Les cyberattaques utilisent des codes malveillants pour modifier le code informatique, la logique ou les données, ce qui entraîne des conséquences perturbatrices qui peuvent compromettre les données et mener à des cybercrimes, comme le vol d'informations et d'identité. La cyberattaque est également connue sous le nom d'attaque de réseau informatique (CNA) computer network Attack [22].

I I.4.1 Anatomie d'une cyberattaque

Le schéma simplifié, ci-dessous, permet de mieux comprendre l'anatomie d'une cyberattaque.

- **Cyber Scanning :** Ou la reconnaissance du réseau, est une étape indispensable dans toutes attaques organisées.C'est la première étape d'une tentative d'intrusion qui permet à un attaquant de récolter un maximum de renseignements sur la cible, de localiser et d'exploiter à distance les systèmes vulnérables.
- **Enumération :** C'est le test des vulnérabilités découvertes pour identifier les points faibles qui permettent à l'attaquant d'avoir accès au système.
- **Tentative d'intrusion :** Le cybercriminel peut pénétrer dans le réseau ou utiliser des attaques avancées pour le rendreinutilisable.

- **Elévation du privilège :** Selon le modèle Microsoft STRIDE, l'élévation de privilège consiste, pour un utilisateur malveillant, à obtenir un niveau d'autorisation plus élevé que celui qui lui est normalement attribué.
- **Effectuer des tâches malveillantes :** Comme endommager ou voler des données.
- **Déployer des logiciels malveillants / porte dérobée :** Le cybercriminel installe des programmes malveillants sur le périphérique du point de terminaison cible pour créer ensuite une porte dérobée à travers laquelle plusieurs types de logiciels malveillants peuvent être téléchargés, permettant l'exécution de différentes attaques.
- **Supprimer les traces et les preuves et quitter :** C'est la dernière étape, les attaquants vont supprimer toutes les preuves de leur présence surle réseau et les systèmes, ils utilisent souvent des virus et des vers pour détruire des preuves potentiellement incriminantes.

La plupart des attaques suivent le schéma illustré dans la figure suivante :

Figure 12: Anatomie d'une cyberattaque

II.5 Le cyber menaces

Plusieurs menaces existent sur Internet, nous présentons les principales parmi celles pouvant être détectées par les systèmes de surveillance du cyberespace.

I I.5.1 Le scanning /probing

C'est une activité de reconnaissance, elle est la première étape d'une cyberattaque. Son objectif est de découvrir les vulnérabilités sur une cible visée. Une fois qu'une machine est jugée vulnérable, l'attaquant tente de la contrôler ou de l'infecter en fonction de la vulnérabilité inférée. Les activités de scanning sont basées généralement sur les protocoles TCP, UDP ou ICMP. [25]

II.5.2 Botnet (réseaux de zombies)

Les attaquants peuvent prendre le contrôle des ordinateurs connectés à Internet via des attaques directes ou indirectes, ces ordinateurs compromis sont appelés botnet. Les pirates informatiques distribuent et amplifient leurs attaques en utilisant les botnets. Un botnet est réquisitionné par un ou plusieurs botmasters pour réaliser des attaques telles que DDoS, spamming ou le scanning de port.

Le botmaster prend le contrôle du botnet par le biais d'un canal de commande et de contrôle (C&C), de cette façon les robots individuels deviennent partie intégrante du botnet et peuvent être utilisés pour effectuer des attaques coordonnées.

II.5.3. Exploit

C'est un logiciel ou une séquence de commandes, utilisé afin d'exploiter une faille de sécurité d'un système d'information pour exécuter des actes malveillants.

II.5.4. Déni de Service (Denial of Service - DoS)

Les attaques par déni de service sont des tentatives de rendre un ordinateur ou des ressourcesréseaux indisponibles, pour but d'empêcher les utilisateurs légitimes d'accéder à ces ressources. Il peut être lancé sous deux formes, le premier en envoyant un ou plusieurs paquets soigneusement conçus exploitant une vulnérabilité logicielle du système cible. Par exemple, l'attaque «Ping-of-Death», la deuxième forme consiste à utiliser des volumes

Massifs de trafic inutile pour occuper toutes les ressources pouvant servir le trafic légitime, Lorsque le trafic d'une attaque DoS provient de sources multiples(en utilisant les botnet), il est appelé un déni de service distribué (DDoS) [26], DDoS attaque est en augmentation constante par exemple le 28 février 2018, le site d'hébergement de code de GitHub a été frappé par la plus

Grande attaque DDoS de l'histoire qui a culminé à 1,35 Tbps, et l'attaque DDoS la plus soutenue a duré 297 h au premier trimestre de cette année, selon le rapport du laboratoire Kaspersky [27].

La figure ci-dessous simplifié les attaques par déni de service.

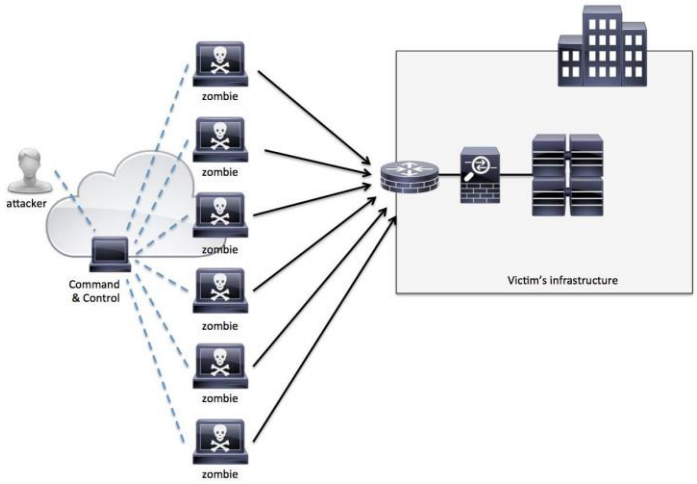

Figure 13:DDoS attaque

II.5.5 Distributed Reflection Denial of Service (DRDoS)

RDoS est un type spécial d'attaques DDoS. L'attaquant masque les sources du trafic d'attaque en utilisant des tiers (routeurs ou serveurs Web) pour relayer le trafic d'attaque à la victime, Ces tiers innocents sont aussi appelés réflecteurs, toute machine qui répond à un paquet entrant peut devenir un réflecteur potentiel.

Après que l'attaquant a pris le contrôle d'un certain nombre de "zombies", au lieu d'ordonneraux "zombies" d'envoyer directement le trafic d'attaque aux victimes, les "zombies" reçoiventl'ordre d'envoyer aux tiers du trafic spoofé avec comme adresse IP source l'adresse IP de la victime. Les tiers enverront ensuite le trafic de réponse à la victime, ce qui constitue une attaque DRDoS [26].

Le schéma simplifié, ci-dessous, permet de mieux comprendre l'attaque DRDoS.

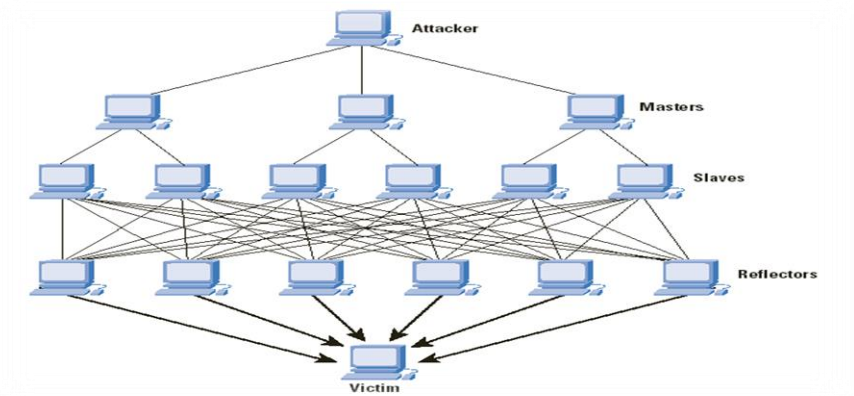

Figure 14: DR Dos attaque

II.5.6 Malware

C'est un programme développé ou une partie d'un code conçu pour effectuer des activités malveillantes tels que les virus, les vers, les chevaux de Troie, etc. Certaines de ses caractéristiques peuvent inclure la propagation et la réplication.

II.5.7 Menaces persistantes avancées (Advanced Persistent Threats) :

Les APT font généralement référence à un groupe, tel qu'un gouvernement étranger, ayant àla fois la capacité et l'intention de cibler de manière persistante et efficace une entité. Ces cyberattaques possèdent des techniques de furtivité élevées et sont souvent spécifiques à unecible. Ils sont avancés car leurs opérateurs disposent de tout un éventail de techniques de collecte de renseignements. Les APT attribuent des priorités à des tâches spécifiques plutôt que de rechercher de manière opportuniste des informations pour un gain financier ou autre. L'attaque est menée par une surveillance continue et une interaction afin d'atteindre les objectifs définis. Les attaques sont exécutées par des actions humaines coordonnées plutôt que par de simples morceaux de code automatisés. Leurs opérateurs sont généralement très compétents, motivés, organisés et bien financés [28].

II.5.8 Zero Day Attacks

Ces attaques exploitent l'observation de vulnérabilités récemment découvertes mais non corrigées pour mener à bien leurs tâches malveillantes. Un certain nombre de mécanismes de détection ont été proposées pour se protéger contre ces attaques, mais ces attaques informatiques restent très dominantes et posent de graves problèmes [28]. Exemple : The Heartbleed Bug.

II.5.9 Forever-day vulnérabilités

Ce sont les vulnérabilités qui prennent beaucoup de temps pour se fixer, ou ne sont jamais fixées. Certaines entreprises utilisent encore des programmes qui n'ont plus de mises à jour comme WindowsXP.

II.6 Cyberdéfense

Pour atténuer les impacts de cybermenaces, de nombreuses entreprises et chercheurs proposent des mesures, réglementaires et techniques. Dans ce qui suit, nous nous concentronssur les aspects techniques.

Les mesures techniques de cybersécurité comprennent les outils technologiques (logiciels etmatériels) permettant de prévenir, détecter, atténuer et réagir aux cyberattaques.

II.6.1 Les normes de sécurité informatique

La mise en œuvre de normes internationalement reconnues (Ex : ISO 27001).

II.6.2 Les mises à jour système

Pour éviter les dénis de services applicatifs, on doit maintenir tous les logiciels de son

systèmeà jour puisque les mises à jour permettent souvent de corriger des failles logicielles, qui peuvent être utilisées par un attaquant.

II.6.3 Les Antivirus

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. L'antivirus analyse les fichiers stockés dans le disque dur et les fichiers entrants (fichiers téléchargés ou courriers électroniques) périodiquement, mais aussi la mémoire vive, l'analyse basée sur une base de données de signatures des logiciels malveillants et le comportement anormal de système.

II.6.4 Systèmes de détection du trafic malveillant

Les techniques classiques pour la détection du trafic malveillant, de surveillance des réseaux et d'analyse du trafic réseau en général sont l'usage de pare-feu (fonctionne aussi comme un mécanisme de contrôle d'accès pour protéger la partie privée d'un réseau), les systèmes de détections d'intrusion IDS et IPS (Prévention /Protection contre les intrusions et non seulement la détection). Ces deux derniers aussi comme l'antivirus utilisent une base de signatures de vers et d'autres logiciels malfaisants.

II.6.5 Architecture DMZ (Demilitarized zone) [29] :

Une DMZ est un réseau situé entre le réseau local et Internet, il n'est ni à l'intérieur ni à l'extérieur du pare-feu. Il est accessible depuis les réseaux internes et externes. Les règles de sécurité empêchent les périphériques externes de se connecter aux périphériquesinternes. Une zone démilitarisée est plus sécurisée que le réseau extérieur, mais moins sécurisée que le réseau intérieur. L'internet (réseau extérieur) est connecté à un pare-feu sur l'interface extérieure. Les utilisateurs et les serveurs qui n'ont pas besoin d'être accessibles à partir d'Internet sont connectés à l'interface interne. Les serveurs accessibles à partir d'Internet sont situés dans la zone démilitarisée. Une DMZ a principalement deux objectifs :

- La première consiste à séparer les ressources d'accès public du reste du réseau.
- La seconde est de réduire la complexité.

II.6.6 Cyber threat intelligence :

Cyber threat intelligence fait référence à la collecte de renseignements avant qu'un cyberattaquant ne cible un système victime. L'objectif est d'aider les organisations à comprendre et à atténuer les risques liés aux exploits Zero Day Attacks, aux menaces persistantes avancées (APT) et aux acteurs internes et externes de la menace. Cela permet aux organisations d'adopter une approche proactive en matière de cybersécurité et de prendredes contre-mesures préventives à l'avance, les données peuvent être obtenues de différentes sources [30].

II.6.7 Tactical Cyber threat intelligence:

Ces données proviennent de la surveillance en temps réel des systèmes (système de monitoring de cyberspace). Il s'agit d'événements en temps réel et d'informations relatives aux actions de l'adversaire à l'intérieur de l'organisation. Tactical threat intelligence (le renseignement tactique sur les menaces) est utilisé par les défenseurs pour s'assurer que leurs systèmes d'intervention en cas d'incident et leurs enquêtes sont préparés -à cette tactique.

II.7 Conclusion

Dans ce chapitre, nous avons présenté l'importance de la sécurité du cyber espace qui est devenu une partie importante de nos vies. Nous avons également fourni les mesures de protection pour la cybersécurité. Dans le chapitre suivant on va détailler la réalisation de notre projet.

CHAPITRE III

Conception d'une solution de sécurité pour les smart buildings

III.1 Introduction

La réalisation sécurisée d'un smart building se fait à travers un ensemble de modules et de composants. Dans notre système, nous avons utilisé plusieurs solutions logicielles et matérielles disponibles pour réaliser notre projet.

Dans cette dernière chapitre, nous allons présentent deux partie principales :

La première partie concerne matériels et logiciels utilisés et la deuxième partie les déférentes étapes pour la réalisation de notre projet.

III.2 Présentation du projet

L'architecture que nous proposons pour un système d'IoT/M2M Smart building utilise des capteurs, des actionneurs et d'autres outils pour collecter des données et les gérer en fonction des services d'une entreprise, tandis qu'Arduino UNO représente le cerveau.

Figure 15: Présentation du système

III.3 Matériel et logiciel du système

III.3.1 Matériel du système

Les principaux composants utilisés sont décrits dans le tableau suivant.

Composant	Type	Caractéristiques techniques
Arduino	**UNO**	Est un microcontrôleur qui se compose de 14 broches d'entrée/sortie numériques, dont 6 sont des sorties PWM, 6 entrées analogiques, un oscillateur à cristal de 16 MHz, une

		connexion USB, une alimentation, un connecteur ICSP et un bouton de réinitialisation.
NodeMCU	**V3**	Est une carte basé sur un ESP8266 cadencé à 80 MHz et exécutant le firmware open source NodeMCU, est programmé via l'IDE Arduino
Camera	**ESP32-CAM**	Est basé sur le microcontrôleur ESP32 d'Expressif. Il peut être intégré dans un système de caméra avec un module ESP32.
Modules	**RFID**	Détecte les badges ou les cartes magnétiques à moins de 10 cm. Le passage d'un composant magnétique permet de lire l'UID de la carte, ainsi que les données enregistrées.
	SIM800L	Est un module GSM qui peut accéder au GPRS pour envoyer des données à l'Internet avec le système M2M. Il permet de passer des appels et d'envoyer des messages.
Captures	**Pluie**	Est un outil simple de détection de la pluie. Il est composé de deux modules : une carte de pluie qui détecte la pluie et un module de contrôle qui Tampon de détection : 5cm x 4 cm .
	Flamme	Il détecte la présence d'une flamme ou des incendies à courte distance (100 cm).
Actuators	**Servo motor**	C'est un moteur capable de maintenir l'opposition à une force statique et dont la position est continuellement vérifiée et corrigée en fonction de la mesure.
	LCD 16*2	L'écran à cristaux liquides est un outil permettant d'afficher des caractères dans le traitement de l'information. Il est utilisé pour afficher la réponse de différents capteurs.
	Serrure solénoïde	Une serrure électromagnétique fonctionne sur le mécanisme de verrouillage électromécanique. Ce type de serrure comporte un ergot avec une coupe oblique et un bon support de montage. Lorsqu'une alimentation est appliquée, le courant continu crée un champ magnétique qui déplace l'ergot à l'intérieur et

		maintient la porte en position déverrouillée.
	Clavier matriciel	Est un appareil utilisé dans un caractère de saisie des chiffres et des lettres qui peuvent être utilisés comme entrée du mot de passe.
	Relais	Ils sont utilisés pour commuter des charges et pour contrôler des appareils. Dans notre système, après avoir reçu une commande particulière via le clavier, le microcontrôleur commande le relais en conséquence.
	Buzzer	Est un élément électromécanique qui produit un son quand on lui applique une tension. Certains nécessitent une tension continue DC, d'autres nécessitent une tension alternative AC.

III.3.2 Logiciel du système

III.4 L'application mobile

III.4.1 Définition :

Une application mobile est un logiciel applicatif transportable et autonome, développé pour être installé sur un appareil électronique mobile. Elle est identifiée par un ou plusieurs programmes téléchargeables de façon gratuite ou payante depuis un magasin d'applications "Application Store ", permettant d'accéder à un contenu homogène et exécutable à partir du système d'exploitation du Smartphone. Les applications mobiles permettent en général un accès plus pratique, rapide et efficace à des sites en version mobile ou web. [29]

III.4.2 Environnement de développement

Logiciel	Caractéristiques
Arduino IDE	Est une application écrite en Java inspirée du langage Processing. Elle permet d'écrire, de modifier un programme et de le convertir en une série d'instructions compréhensibles pour la carte Arduino.
Fritzing	Est un projet de logiciel libre, Il a notamment pour vocation de favoriser l'échange de circuits électroniques libres et d'accompagner l'apprentissage de la conception de circuits

Tableau 4: Logiciel du système

- **Kodular :** Kodular (anciennement Makeroid) est un constructeur d'applications moderne qui permet aux utilisateurs de créer de superbes applications Android sans aucune connaissance particulière de la programmation. C'est une suite complète qui permet aux utilisateurs de commencer à programmer sans passer des années à apprendre un langage de programmation.

Kodular fournit principalement Kodular Creator. Il s'agit d'un créateur d'applications Android par glisser-déposé. Il suffit de glisser-déposer quelques composants et de joindre des blocs pour que l'application souhaitée soit prête!

Il fournit également une alternative gratuite au Play Store pour héberger et distribuer vos applications, projets, extensions et écrans à un large public.

Kodular apporte également un IDE Extensions pour utilisateurs avancés, qui est un IDE en ligne permettant de créer de nouveaux composants sur Kodular Creator sans télécharger de logiciel.

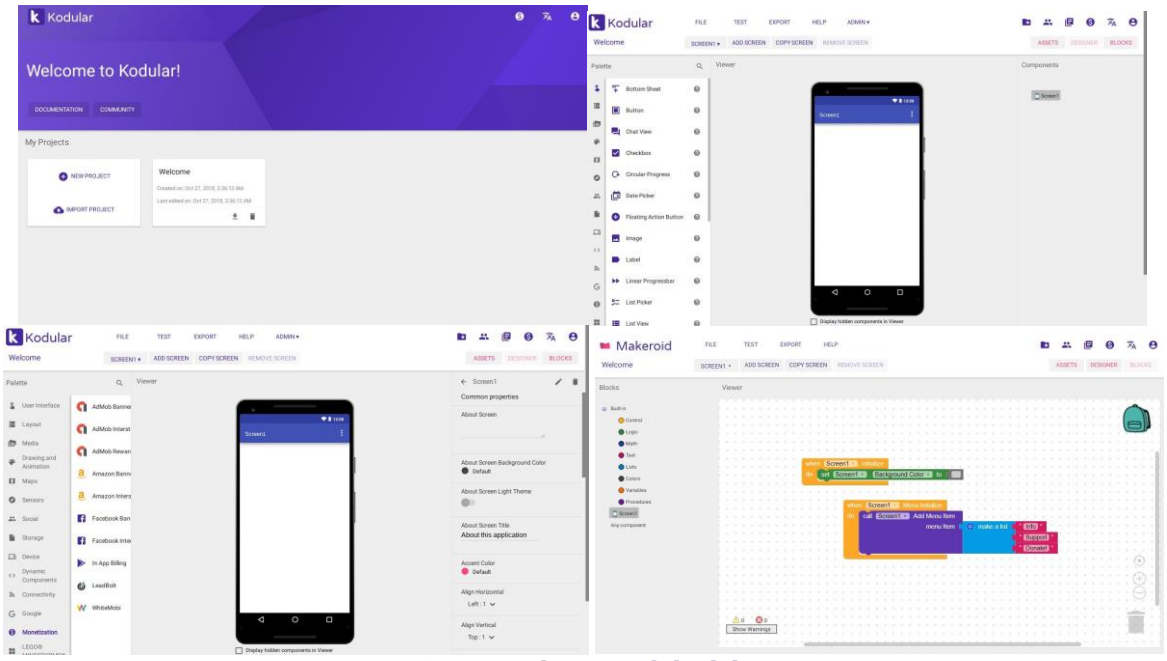

Figure 16: le site web kodular

❖ **Notre propre application mobile**

Nome : BDF-Security

- Description

BDF-Security est une application mobile écrite en Java, a été créé en mars 2022 par nous, en utilisant kodular**.**

Notre application sert à contrôler quelque objet dans notre smart home, elle assure le confort à partir de contrôler l'éclairage.

Nous allons présenter dans ce qui suit les principales interfaces illustrant le fonctionnement de l'application :

- Interface d'entrée
- Interface login
- Interface d'authentification.
- Volet commandes.
- Interface light control

Interface d'entrée

Figure 17: Interface d'entrée

- **Interface login**

Figure 18: Interface login

- **Interface d'authentification.**

Figure 19: Interface d'authentification.

- **Interface d’authentification. (Errer)**

Figure 20: Interface d’authentification. (Errer)

- **Volet commandes**

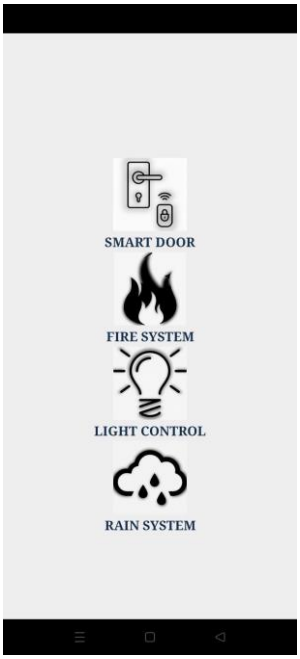

Figure 21: Volet commandes

- **Interface light control**

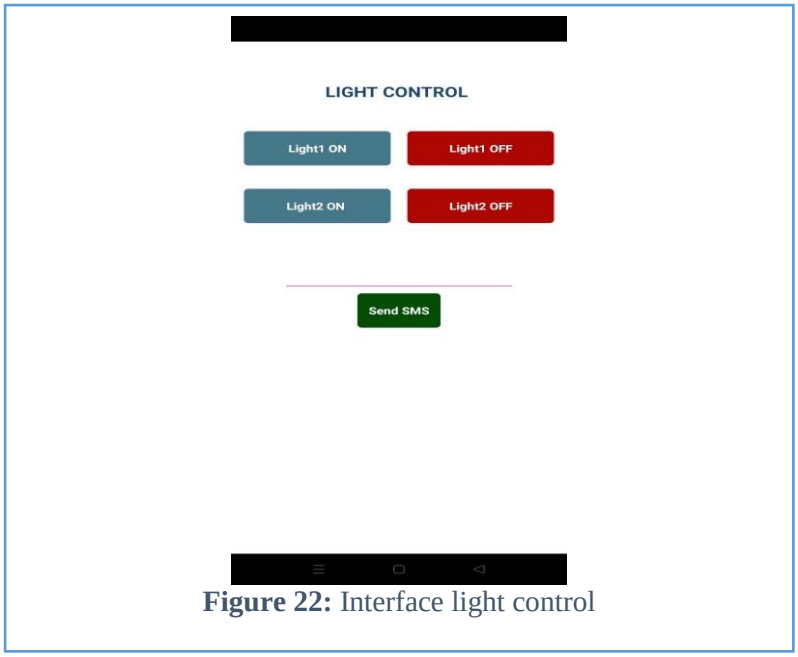

Figure 22: Interface light control

III.5 Maquette proposé

Dans ce prototype, nous avons installé tous les composants du système et relies entre eux de manière organisée.

Figure 23: Maquette proposé

III.6 Le système de verrouillage de porte

Le système d'accès intelligent proposé au bâtiment est un dispositif électronique qui permet de verrouiller ou de déverrouiller toutes les ouvertures de manière contrôlable et programmable en façade dans le logiciel IDE, il permet d'apporter du confort et d'augmenter le niveau de sécurité du bâtiment, en s'appuyant sur le système Arduino et les composants RFID, ESP32 -Cam, clavier matriciel ainsi que d'autres composants, il consiste à vérifier un badge et à entrer un mot de passe et une reconnaissance faciale pour la confirmation de l'identité ou le lancement d'une alarme en cas d'intrusion .

- **Organigramme d'ouverture et fermeture de la porte**

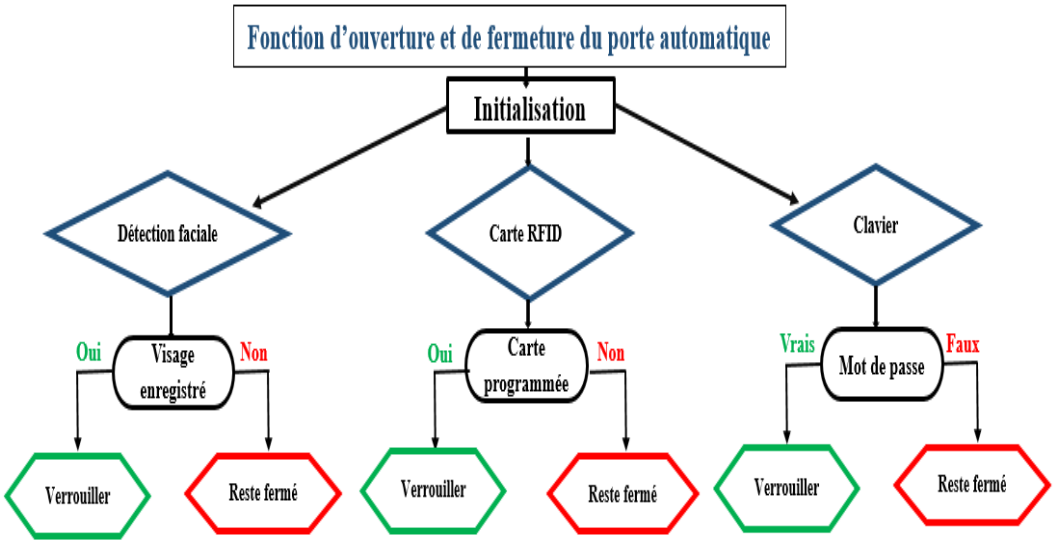

Figure 24: Organigramme d'ouverture et fermeture de la porte

III.6.1 Simulation virtuelle du montage

- **Schéma global du système sur le logiciel fritzing**

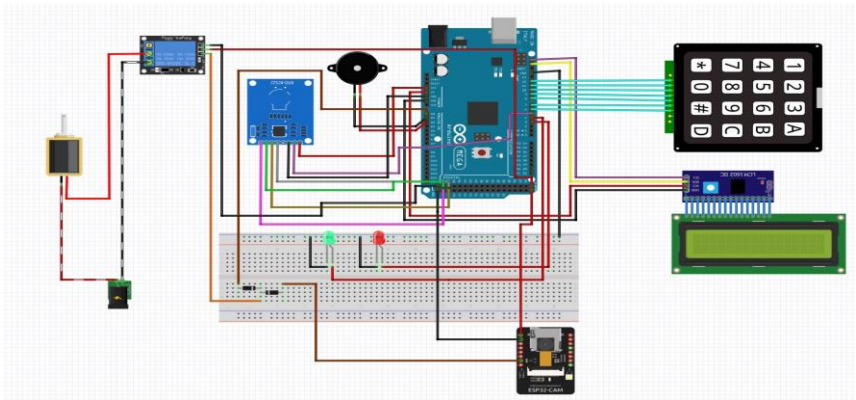

Figure 25: Schéma du montage pratique de la porte intelligente

➢ **Le montage expérimental**

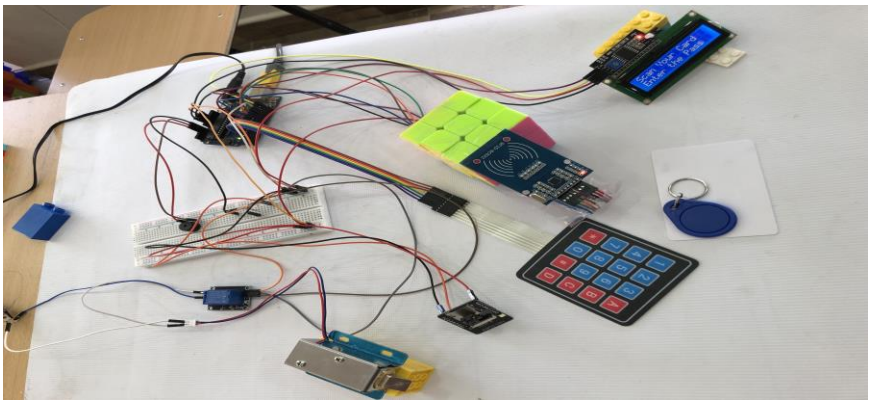

Figure 26: La réalisation de la fonction d'accès sécurisé au building

1. Le système de verrouillage de porte Basé sur Carte RFID

➢ **Matériel utilisés**

Matériels utilisés	Caractéristiques	Nombre
Arduino	UNO	1
Lads	Rouge /vert	2
Module RFID	RC522	1
Relais	5v	1
Adaptateur	12V	1
Serrure	Electrique	1

Tableau 5: Matériel utilisés pour la porte base sur carte RFID

➢ **Simulation virtuelle**

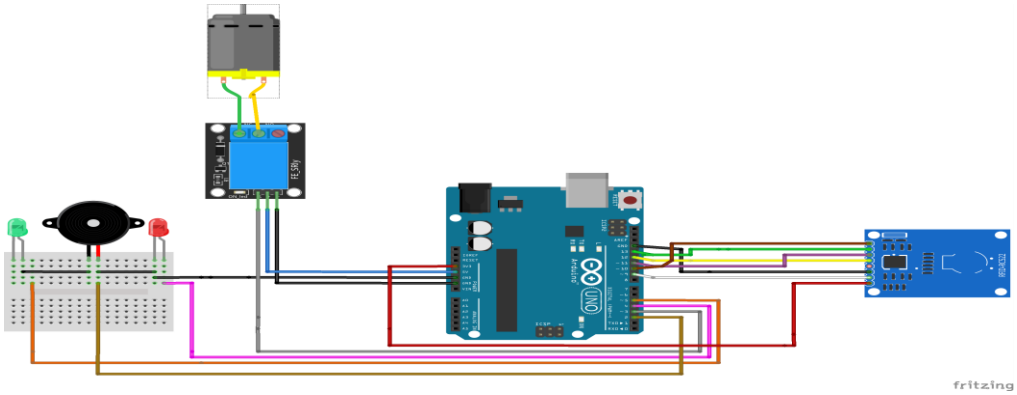

Figure 27: Schéma d'interconnexion entre les composants du système d'ouverture du port basé sur RFID (fritzing)

➢ **Résultats pratique**

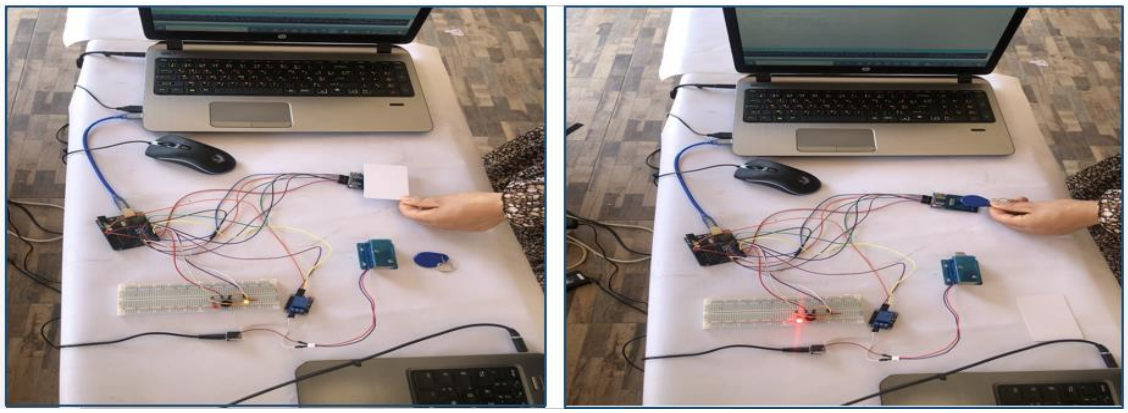

Figure 28: Ouvrir la porte avec une carte programmée / la porte ne s'ouvre pas cas le badge n'est pas programmée

Commentaire :

Après avoir connecté les fils et le circuit, puis téléchargé le programme dans le microcontrôleur arduino UNO, le robot fonctionne correctement.

- Si un tag incorrect est donné, la porte ne s'ouvre pas et un message est affiché sur le LCD.
- Si une étiquette est donnée, la porte s'ouvre et un message s'affiche sur l'écran LCD.

2. Le système de verrouillage de porte Basé sur clavier (4*4)16 boutons

➢ **Matériel utilisés**

Matériels utilisés	Caractéristiques	Nombre
Arduino	UNO	1
LCD + I2C	16*2	1
Clavier matriciel	4*4	1
Relais	5v	1
Adaptateur	12 v	1
Serrure	Electrique	1

Tableau 6: Matériel utilisés pour la porte base sur clavier matriciel

Quand on entre le mot de passe correct qu'est '1256987', la serrure s'ouvre alors la porte s'ouvre .Et l'écran affiche «WELCOM ».Si le mot de passe d'entrée est incorrect, l'écran affiche « Wrong password » et la porte reste fermée. Et pour fermer la porte on clique sur '#'.

➢ **Simulation virtuelle**

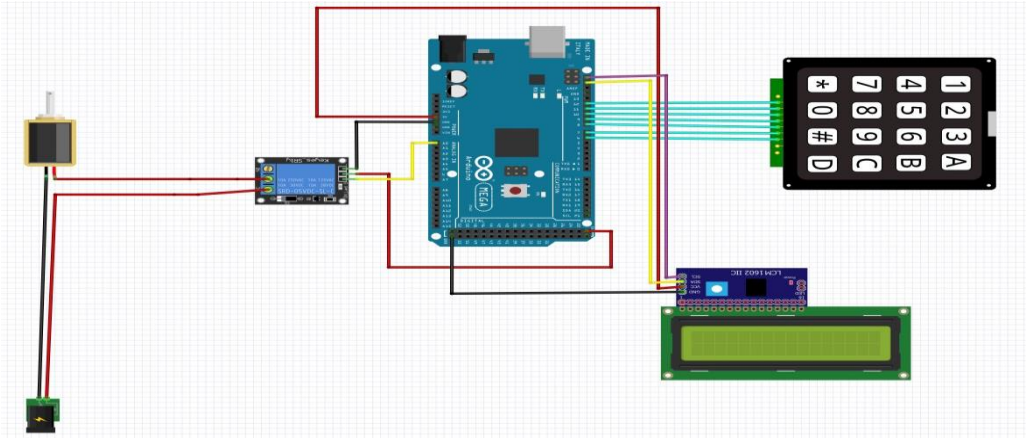

Figure 29: Schéma d'interconnexion entre les composants du système d'ouverture du port basé sur clavier (fritzing)

➢ **Résultat pratique**

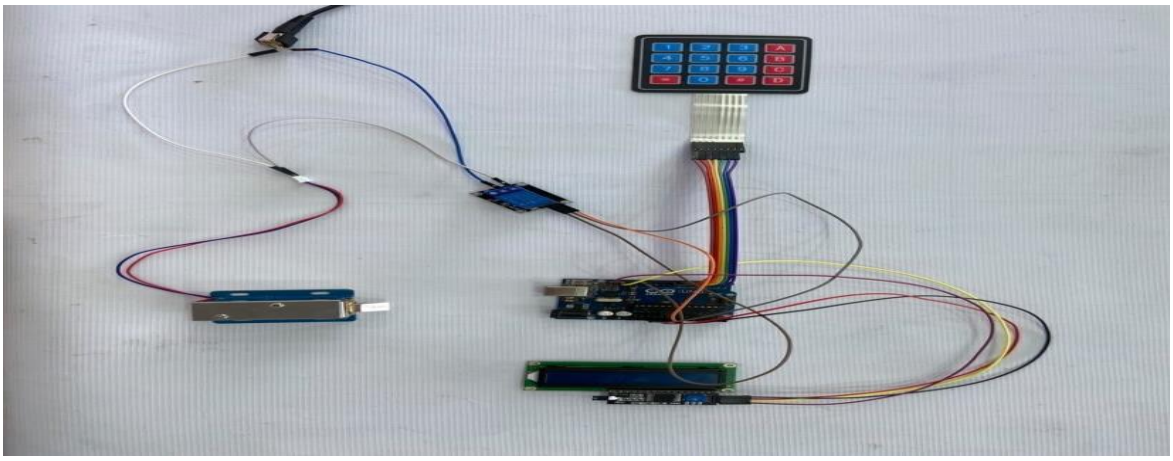

Figure 30: Ouvrir la porte avec clavier matriciel

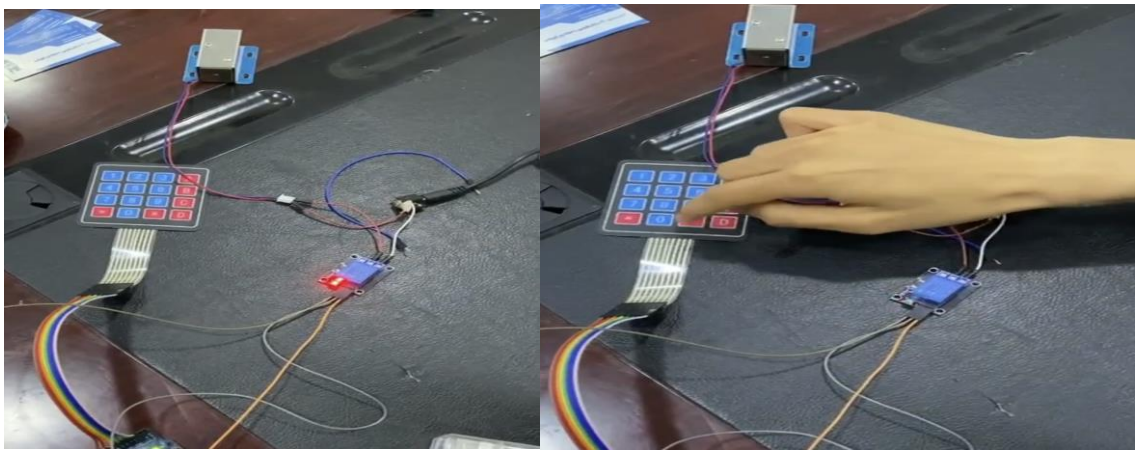

Figure 31: Entre le mot de passe correct /fermez la porte lorsque vous appuyez sur‘#’

3. Le système de verrouillage de porte basé sur la reconnaissance Faciale

Nous a poussé à apprendre et utiliser une grande panoplie d'outils comme programmation de carte esp32 Cam avec Arduino IDE, connecter à un réseau en utilisant la technologie WIFI, Création échange de paquets http avec la Cam, et le plus important la réalisation de système la serrure s'ouvre juste après détection d'un visage enregistré.

- **Matériel utilisés**

Matériels utilisés	Caractéristiques	Nombre
Arduino	UNO	1
ESP32	Cam	1
Relais	5v	1
Adaptateur	12v	1
Serrure	Electrique	1

Tableau 7: Matériel utilisés pour la porte base sur ESP32-cam

- **Simulation virtuelle**

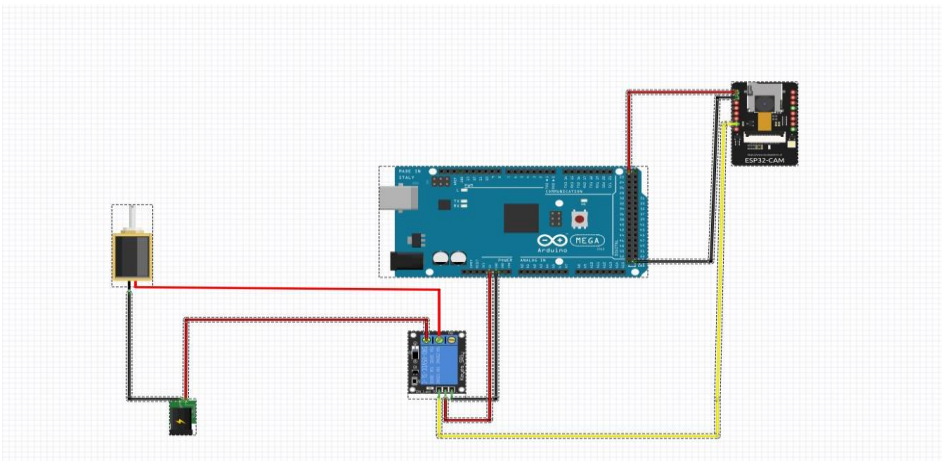

Figure 32: Schéma d'interconnexion entre les composants du système d'ouverture du port basé sur ESP32-cam (fritzing)

- **Le montage expérimental**

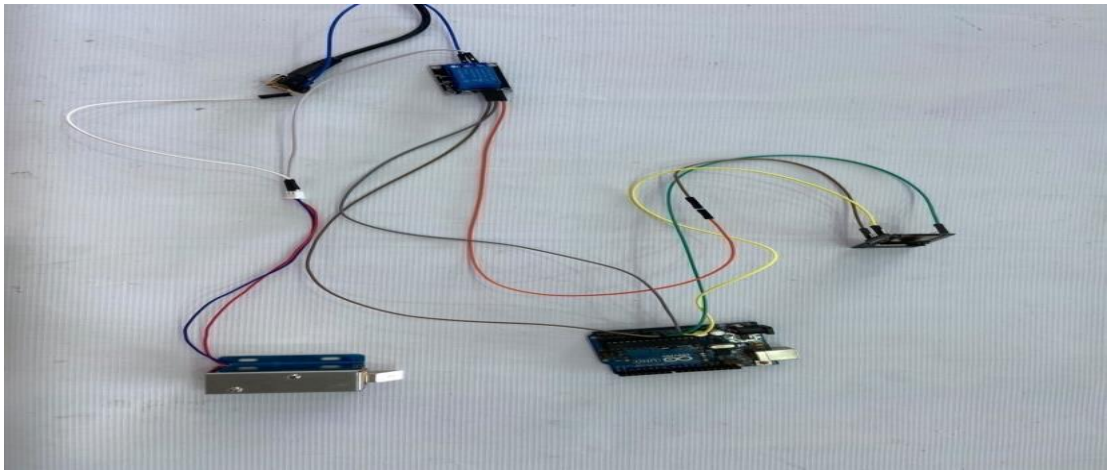

Figure 33: Ouvrir la porte avec ESP32-cam

- **Résultat pratique**

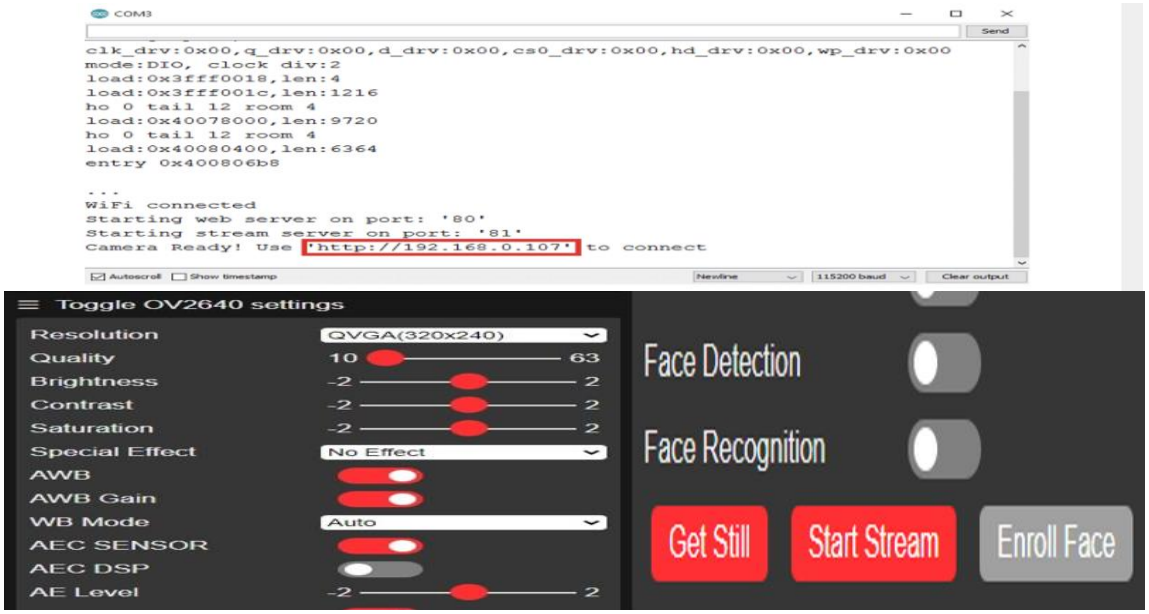

Figure 34: Streaming de Cam

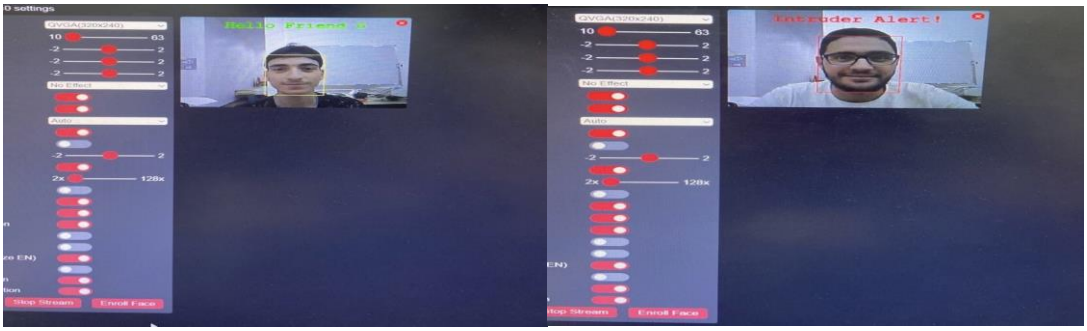

Figure35: Le visage est reconnu dans le flux vidéo/ le visage n'est pas reconnu dans le flux vidéo

III.7 Système de couverture automatique (piscine)

Le système de couverture automatique proposé protège plusieurs endroits : parking, piscine, jardin…etc. Lorsque le capteur de pluie (capteur de pluie) détecte de l'eau, il donne l'ordre au Servo moteur de tourner, ce dernier est à son tour relié à la couverture de la piscine.

- **Organigramme de couverture de piscine**

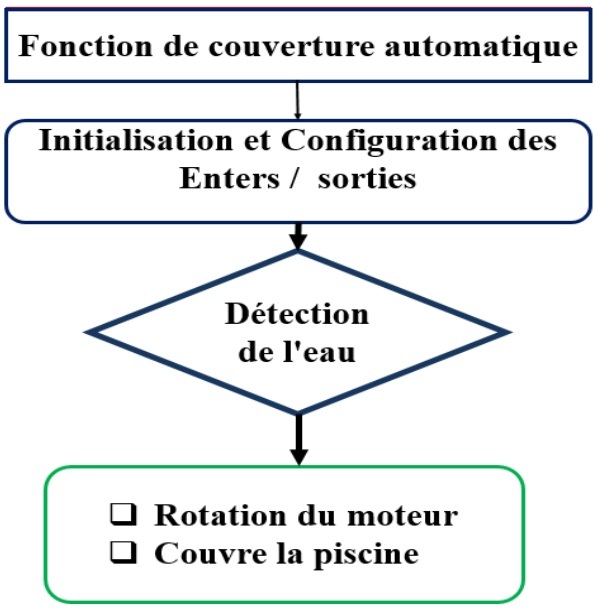

Figure 36 : Organigramme de couverture de piscine

- **Matériel utilisé**

Matériels utilisés	Caractéristiques	Nombre
Arduino	UNO	1
Servo motor	SG90	1
Capteur de pluie	YL-83	1

Tableau 8: Matériel utilisé Système de couverture automatique

➢ **Simulation virtuelle**

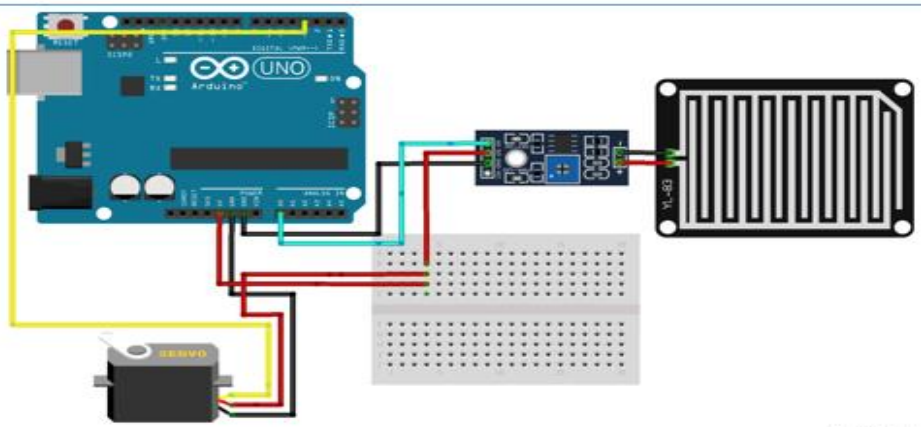

Figure 37: Schéma de système de pluie

➢ **Le montage expérimental de système pluie**

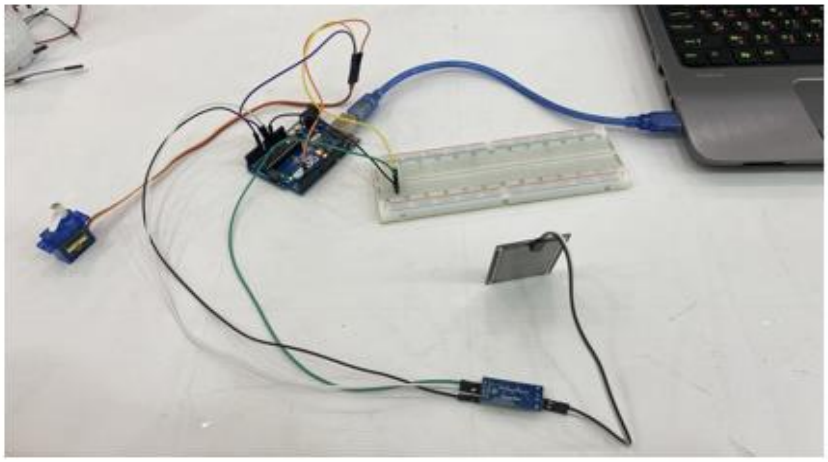

Figure 38: Le montage expérimental de système pluie

➢ **Maquette de système pluie**

Figure 39: Maquette de système pluie

- **Résultat pratique**

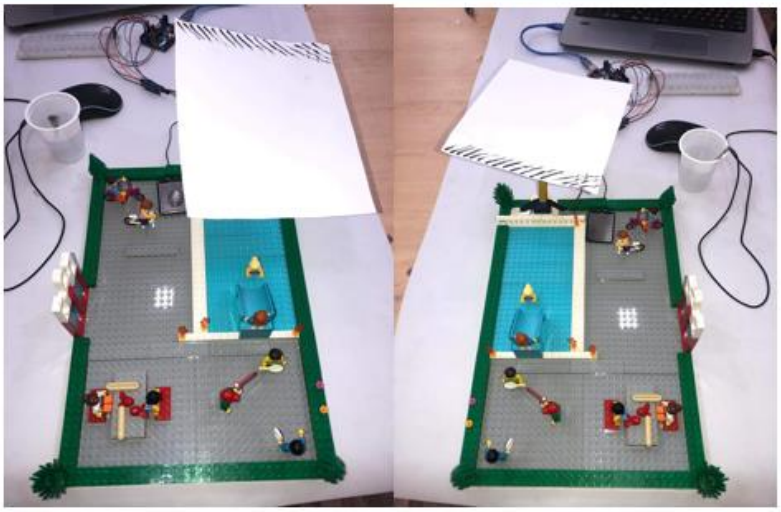

Figure 40:Résultat de l'ouverture et la fermeture de la couverture de la piscine

III.8 Système de détection des incendies

Le système de détection des incendies proposé est basé sur le GSM en utilisant Arduino et un capteur de détection de flamme. Ici, le module GSM SIM800L, un buzzer et le capteur de flamme sont utilisés pour détecter le feu. Lorsque le capteur de flamme détecte un incendie, le buzzer s'allume et les alertes SMS, ainsi que les appels téléphoniques, sont envoyés aux numéros de téléphone prédéfinis stockés dans le sketch Arduino.

➢ **Matériel utilisé**

Matériels utilisés	Caractéristiques	Nombre
Arduino	UNO	1
Capteur de flamme	IR3	1
Gsm	800l	1
Buzzer	3.3-5v	1

Tableau 9: Matériel utilisé pour le système de feu

➢ **Organigramme de détection des incendies**

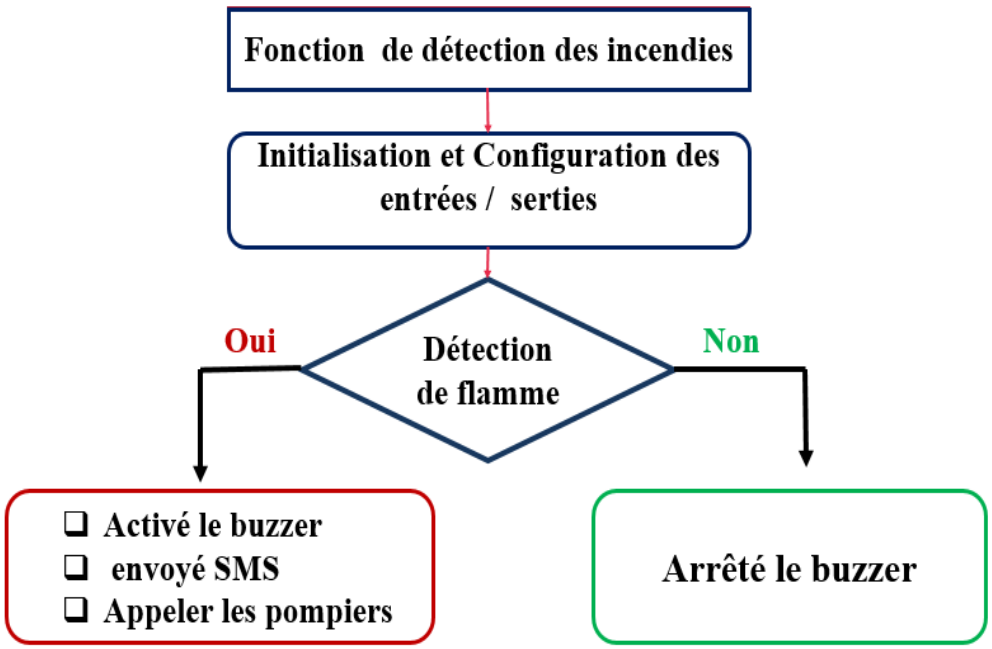

Figure 41 : Organigramme de détection des incendies

➢ **Simulation virtuelle**

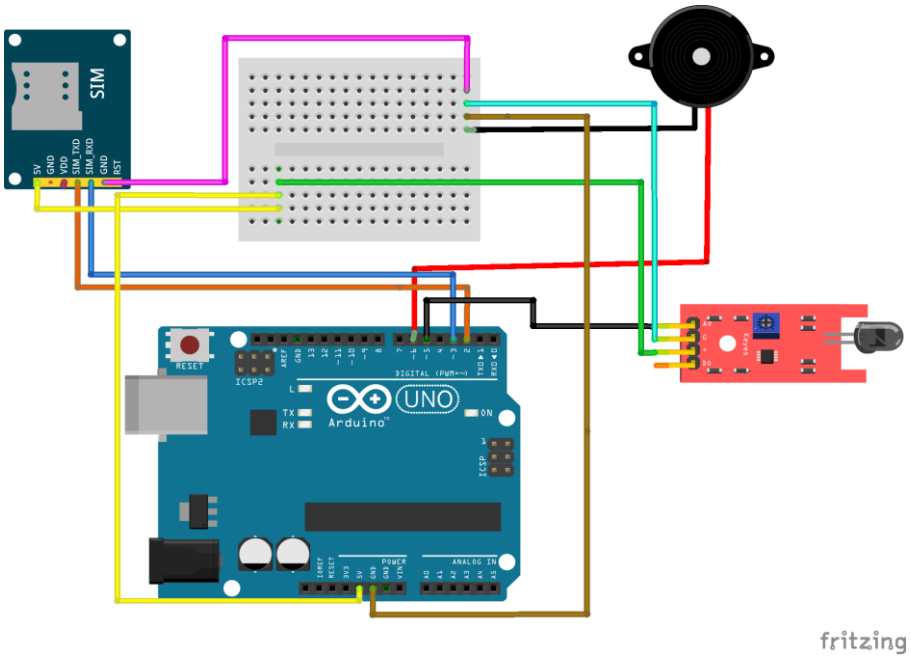

Figure 42: Simulation virtuelle de la détection des incendies

➢ **Résultat pratique**

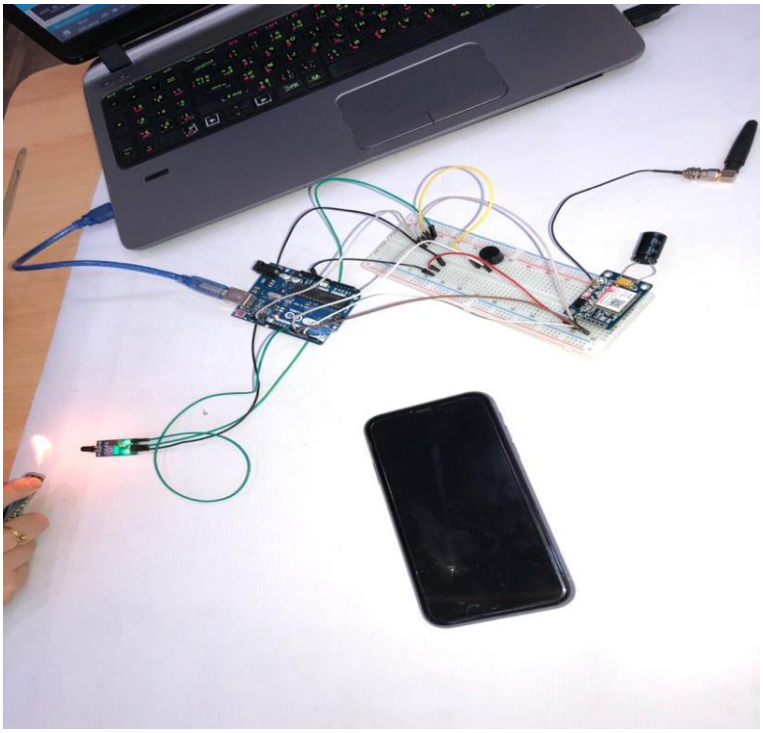

Figure 43: Montage d'un système des incendies.

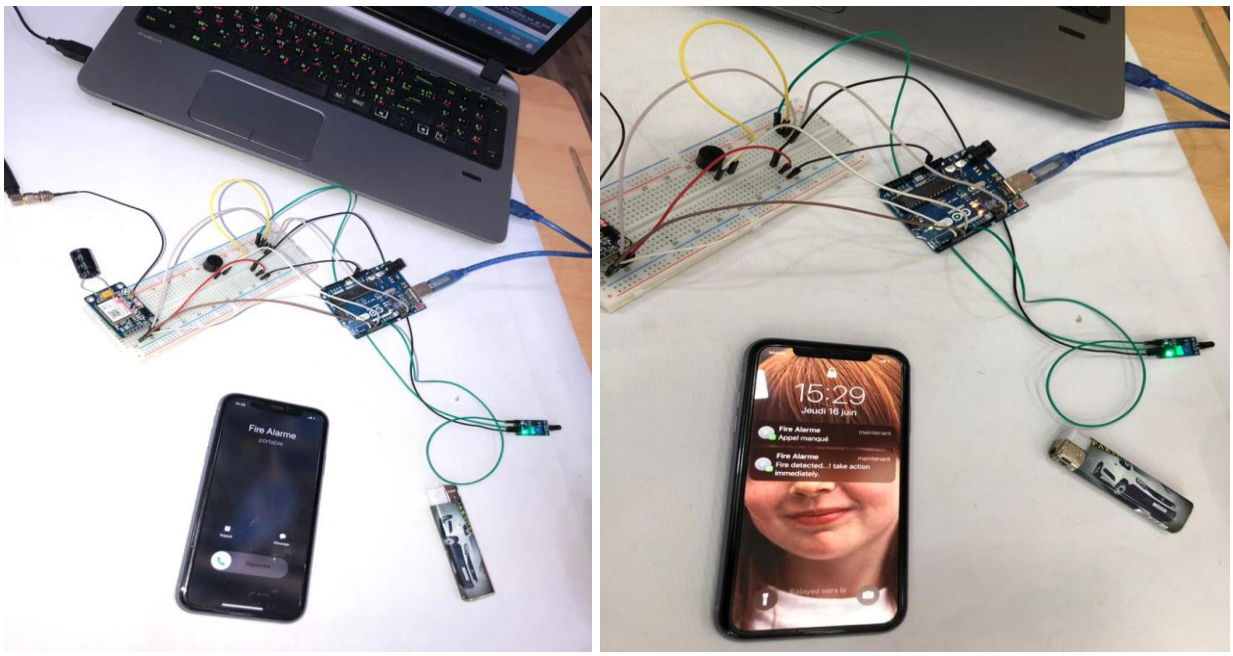

Figure 44: Appel de fire alert/ notification d'un message de fire alert

III.9 Contrôle de la lumière par l'App (BDF Security)

Le système de contrôle de la lumière fonctionne pour contrôler 2 led en utilisant une application (BDF Security) qui est à son tour programmée pour donner des commandes pour allumer et éteindre les led, en utilisant esp32 et un relais connecté aux led

- Lorsque vous appuyez sur light1 on, le premier led s'allume, et un message texte arrive pour le numéro programmé dans l'application.
- Lorsque vous appuyez sur light1 off, led 1 s'éteint et un message texte arrive.
- Lorsque j'appuie sur light2 on, led 2 s'allume et un message texte arrive.
- Lorsque vous appuyez sur light2 off, led 2 s'éteint.

➢ **Organigramme de contrôle de la lumière**

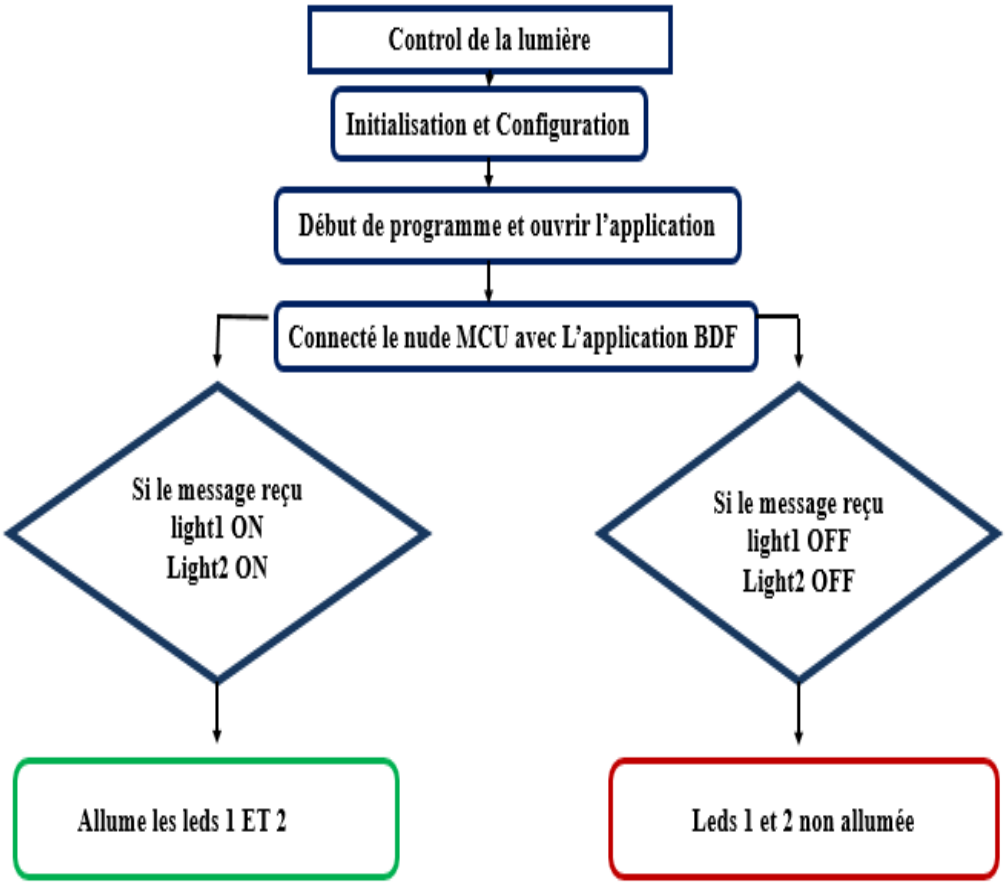

Figure 45 : Organigramme de contrôle de la lumière

➢ **Matériel utilisé**

Matériels utilisés	Caractéristiques	Nombre
Esp32	32	1
Relay	5v	1
Gsm	800l	1
Led	Blanc	2

Tableau 10: Matériel utilisé pour light control

- **Simulation virtuelle**

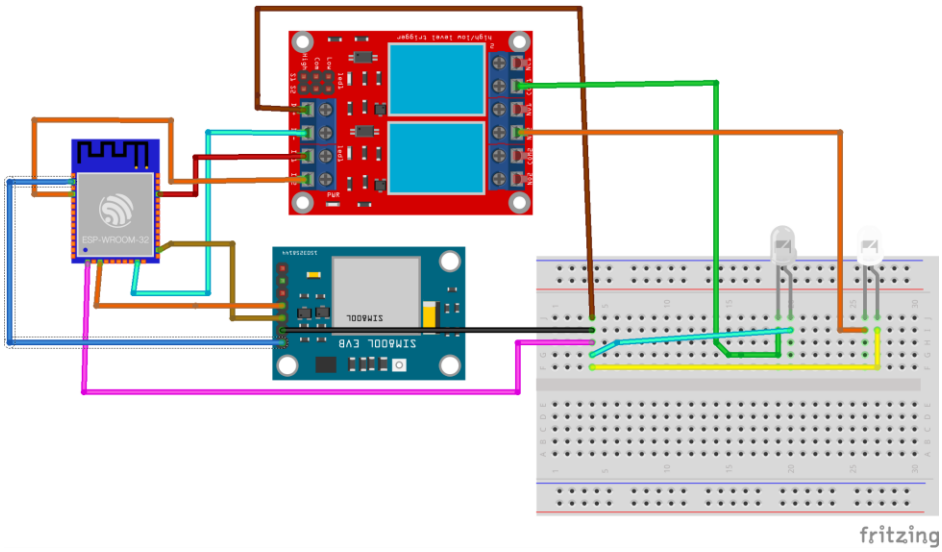

Figure 356: Simulation virtuelle du light control

- **Résultat pratique**

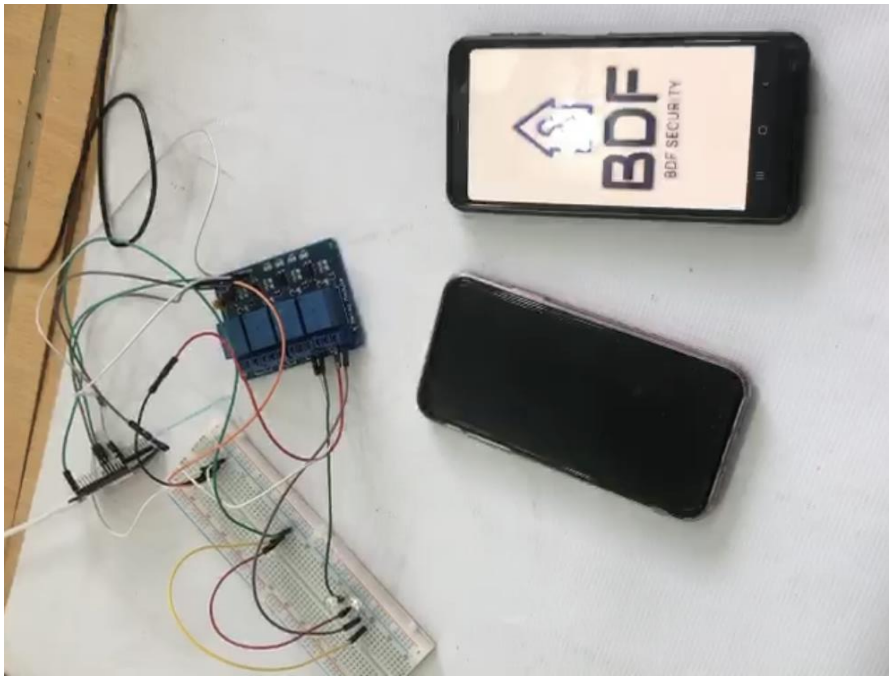

Figure 47: Le montage expérimental du light control

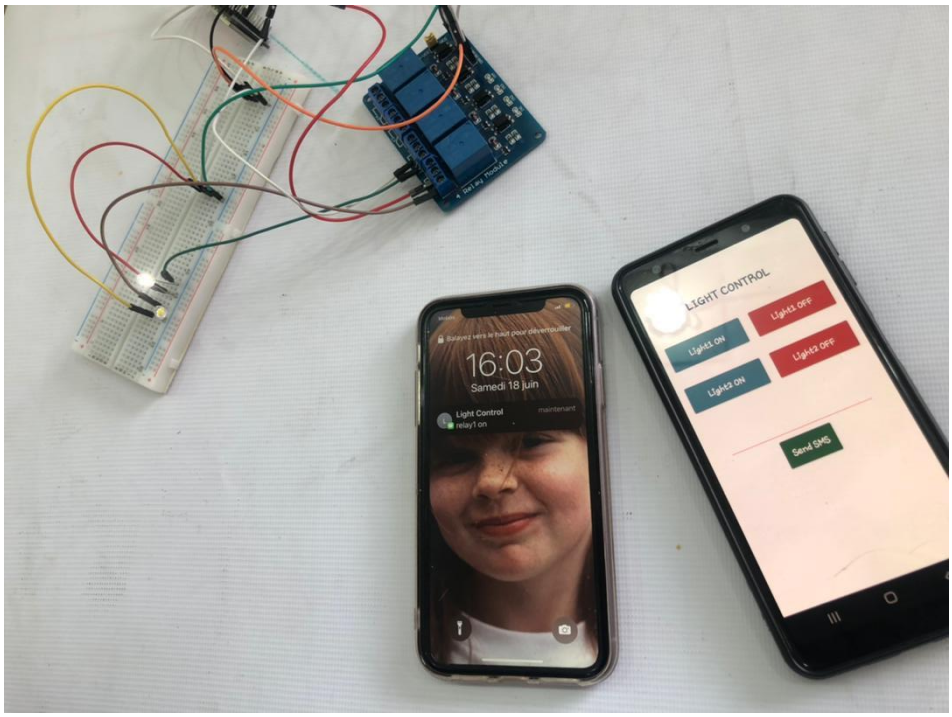

Figure 48: Light1 ON

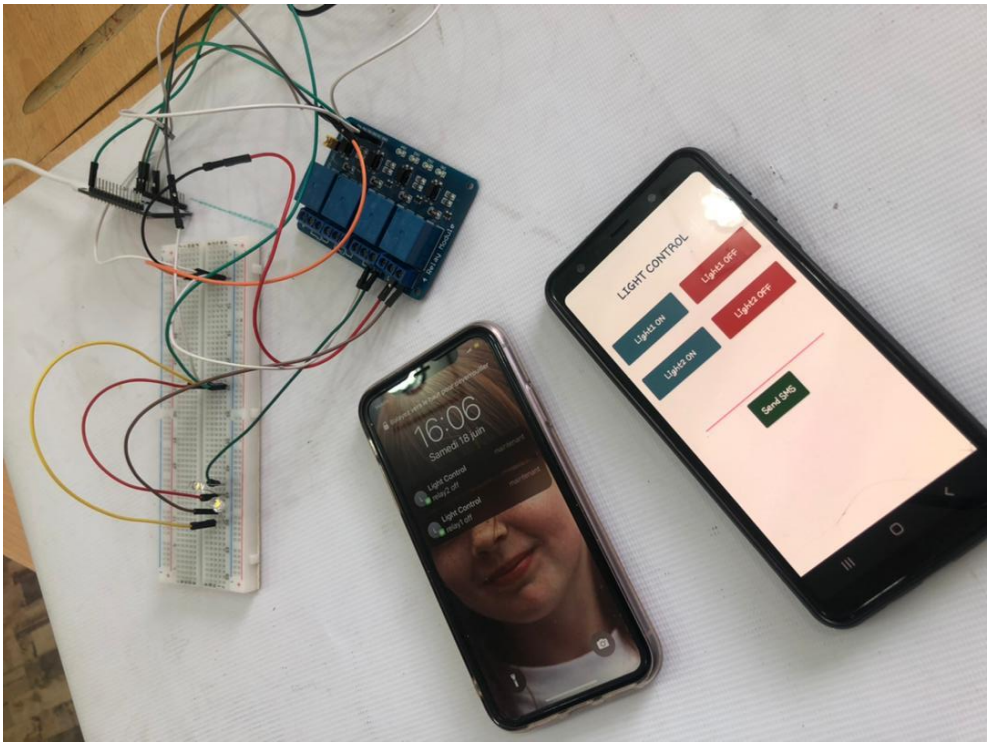

Figure 49: Light1 OFF et light2 OFF

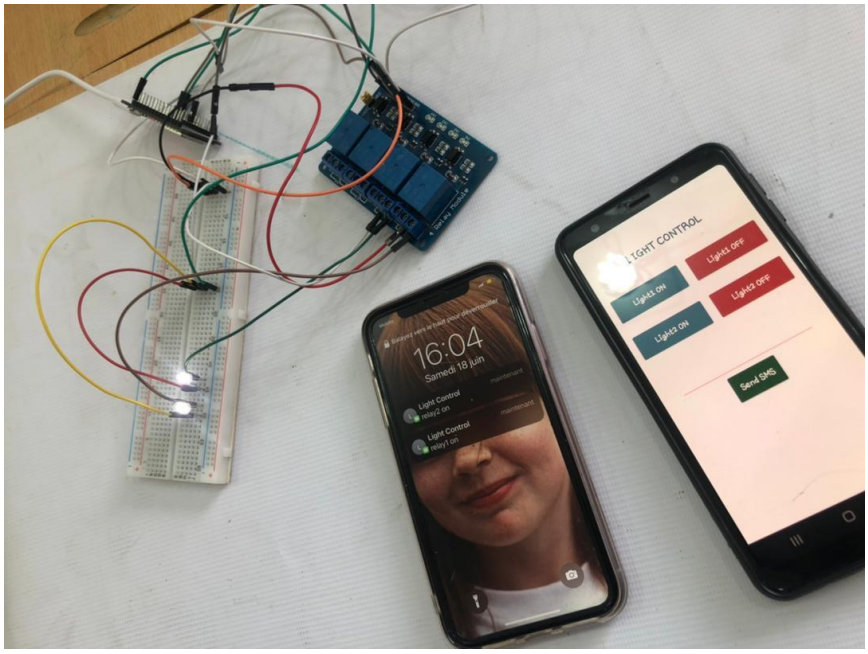

Figure 50: Light1 ON et light2 ON

III.10 Conclusion

Pour conclure, on pourrait dire que la partie réalisation est la partie la plus importante, car elle nous a permis de savoir que notre projet est réalisable.

La partie réalisation et test de notre travail permet de comprendre la conception de notre projet sur la sécurité de smart building ou nous avons réalisé quatre services principales qui sont : la porte intelligente, le système de détection des incendies, la gestion de l'éclairage, et le système de couverture automatique. Tous ces services sont implémentés avec succès sur une smart maquette ou les utilisateurs peuvent contrôlés leur smart buildings à distance par notre application mobile "BDF Security".

Conclusion générale

Ce projet porte sur un système de sécurité de smart building basé sur la communication de machine à machine (M2M) et la technologie de l'Internet des objets(IoT).

Machine à machine (M2M) et la technologie de l'Internet des objets. La mise en œuvre de notre système a commencé par une étude critique des solutions existantes afin de concevoir un système plus fonctionnel.

Ensuite, en construisant un prototype de notre solution intelligente, nous avons essayé de faire un travail concret qui performe trois fonctions principales, à savoir la sécurité, l'entretien intérieur et l'entretien extérieur. Nous avons mis en place quatre services importants : porte intelligente, système de détection des incendies, gestion de l'éclairage, et système de couverture automatique.

Tous ces services peuvent être contrôlés à distance par notre application mobile "BDF Security".

Cette étude se concentre sur la sécurité de conception prototype pour le contrôle, l'automatisation, la surveillance et la commande à distance des systèmes domestiques en temps réel.

Le modèle de système domotique M2M/IoT proposé a été construit et testé. Il a donné exactement les résultats attendus.

Références Bibliographique

[1]: Djehaiche, R., Aidel, S., Benziouche, N. (2021). Design and Implementation of M2M-Smart Home Based on Arduino-UNO. In: Hatti, M. (eds) Artificial Intelligence and Renewables Towards an Energy Transition. ICAIRES 2020. Lecture Notes in Networks and Systems, vol 174. Springer, Cham. https://doi.org/10.1007/978-3-030-63846-7_66

[2]: Kim and Youm EURASIP Journal on Wireless Communications and Networking 2013, 2013:79 http://jwcn.eurasipjournals.com/content/2013/1/79

[3]: https://www.ionos.fr/digitalguide/serveur/know-how/definition-communication-machine-to-machine-m2m/

[4]:https://www.researchgate.net/publication/308266132_Etude_des_mecanismes_de_gestion_de_congestion_dans_la_EUTRAN_pour_les_applications_M2M_IoT_cas_d%27etude_PRACH

[5]: https://mbamci.com/le-m2m-au-coeur-de-la-transformation-digitale/

[6]: Gronbaek, I., Architecture for the Internet of Things (IoT): API and Interconnect, Sensor Technologies and Applications, 2008. SENSORCOMM 08. Second International Conference on, vol., no., pp.802, 807, 25-31 Aug. 2008

[7]: Djehaiche, Rania; Aidel, Salih (2021): Application of M2M Communication based on ZigBee to Control Smart home automation. figshare. Conference contribution. https://doi.org/10.6084/m9.figshare.14748486.v1

[8]: Government of India, "National Telecom M2M Roadmap," 2015.

[9]:P.-J. Benghozi, S. Bureau, F. Massit-Folléa, C. Waroquiers, and S. Davidson, L'internet des objets: quels enjeux pour l'Europe, Éd. de la Maison des sciences de l'homme éd., 2009, 66 p.

[10]: Djehaiche, R., Aidel, S., Saeed, N. (2022). Implementation of M2M-IoT Smart Building System Using Blynk App. In: Hatti, M. (eds) Artificial Intelligence and Heuristics for Smart Energy Efficiency in Smart Cities. IC-AIRES 2021. Lecture Notes in Networks and Systems, vol 361. Springer, Cham. https://doi.org/10.1007/978-3-030-92038-8_44

[11]: Dave Evans L'Internet des objets « Comment l'évolution actuelle d'Internet transforme-t-elle le monde ? » Livre blanc Cisco.

[12]:KEVIN ASHTON. That 'internet of things' thing. In the real world, things matter more than ideas.

[13]: Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications.

IEEE internet of things journal,

Abel C Lima-Filho, Ruan D Gomes, Marceu O Adissi, Tássio Alessandro da Silva, Francisco

[14]: A Belo, and Marco A Spohn. Embedded system integrated into a wireless sensor network for online dynamic torque and efficiency monitoring in induction motors. IEEE/ASME transactions on mechatronics, 17(3)

[15]: Les bases de données dans les réseaux de capteurs sans fil - Scientific Figure on ResearchGate.

[16]: Natarajan Meghanathan et al. (Eds): CSEIT, CMLA, NeTCOM, CIoT, SPM, NCS, WiMoNe,

[17]: Djehaiche, Rania; Benziouche, Nihad (2021): Etude et Application d'un Système de Communication M2M. figshare. Thesis. https://doi.org/10.6084/m9.figshare.14710710.v2

[18]: Djehaiche, Rania; Aidel, Salih; Benhamimid, Karima (2022): A Smart Home Management based on M2M/IoT Technologies. figshare. Conference contribution. https://doi.org/10.6084/m9.figshare.19103315.v1

[19]: Meliti N, « Architecture Basée Agents pour le diagnostic d'un système d'IoT (Internet of Things) » University d'Oum Bouaghi Larbi Ben M'hidi,

[20]: ROSE, Karen, ELDRIDGE, Scott, ET CHAPIN, Lyman. The internet of things: An overview. The Internet Society (ISOC),

[21]: Kim Y., Kim I., Park N. Analysis of Cyber Attacks and Security Intelligence. In: Park J., Adeli H., Park N., Woungang I. (eds) Mobile, Ubiquitous, and Intelligent Computing.Lecture Notes in Electrical Engineering, vol 274. Springer, Berlin, Heidelberg.

[22] : Joanna F, DeFranco .What Every EngineerShould Know About Cyber Security and Digital Forensics, 2014 by Taylor & Francis Group, LLC p39-44

[23]: M. Alaa, A. Zaidan, B. Zaidan, M. Talal, and M. Kiah, *"Things, journal of network and computer applications,"*

[24]:https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers. xhtml [RFC 6335].

[25]: Peng, Tao & Leckie, Christopher & Ramamohanarao, Kotagiri. Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Comput.Surv .

[26]: Xu, Ruomeng & Cheng, Jieren & Wang, Fengkai & Tang, Xiangyan & Xu, Jinying. . A DRDoS Detection and Defense Method Based on Deep Forest in the Big Data Environment. Symmetry.

[27]: Bou-Harb, Elias & Debbabi, Mourad & Assi, Chadi. (2014). Cyber Scanning : A

Comprehensive Survey. Communications Surveys & Tutorials, IEEE. 16. 1496-1519. 10.1109 / SURV.2013.102913. 00020.

[28]: Rababah, Baha & Zhou, Shikun & Bader, Mansour. (2018). Evaluation the Performance of DMZ. I.J. Wireless and Microwave Technologies. 1. 1-13. 10.5815/ijwmt.

[29]: Maglaras, Leandros & Ferrag, Mohamed Amine & Derhab, Abdelouahid & Mukherjee, Mithun & Janicke, Helge & Rallis, Stylianos. (2018). Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures. Security and Safety. 5. 1-9. 10.4108/eai.

[30]: http://www.uky.edu/~jclark/mas490apps/History%20of%20Mobile%20Apps.pdf

.