RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ IBN-KHALDOUN DE TIARET

FACULTÉ DES SCIENCES APPLIQUEES

DÉPARTEMENT DE GENIE ELECTRIQUE

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du diplôme de Master

Domaine : Sciences et Technologie

Filière : Electronique

Spécialité : Electronique des systèmes embarqués

THÈME

La sécurité de l'Internet des Objets (IoT)

Préparé par : Mr. BELHADJ Naceur

Mr. ABBAD Abdelhak

Devant le Jury :

Nom et prénom	**Grade**	**Université**	**Qualité**
BECHEIKH Mustapha	MCB	U-TIARET	Président
MAASKRI Mustapha	MAA	U-TIARET	Examinateur 1
BENATIA Adda Abderrahmane	MCB	U-TIARET	Examinateur 2
BENABID Houari	MAA	U-TIARET	Encadreur

Année universitaire 2021-2022

Remerciements

Ce travail a été effectué au sein du Département de génie électrique de l'Université de Tiaret

En premier lieu nous remercions DIEU tout puissant de nous avoir donné la patience, la santé et la volonté pour achever ce travail

Nous remercions nos parents pour leurs sacrifices et l'aide pour que nous réussissions, de nous avoir donné l'importance, de prendre toujours soin de nous, de nous faire confiance et de toujours nous démontrer l'amour que vous nous portez.

Nous adressons nos sincères remerciements à notre professeur Mr Benabid Houari pour avoir consacrer son temps précieux et avoir accepté de nous encadrer, pour tous les efforts et l'importance qu'il nous a donnée.

Des remercîments spéciaux et chaleureux à notre professeur Mr Belarbi Mustapha de nous avoir offrir un environnement de travail adapté ainsi que son aide et ses conseils.

Nous remercions Les membres de jury pour avoir accepté d'examiner notre modeste travail.

Dédicace

En premier lieu, je tiens à remercier notre Dieu, pour le courage et la Force qu'il m'a donné pour effectuer ce travail

Je dédie ce modeste travail de fin d'étude :

À mes chers parents, que tous les mots du monde ne sauraient exprimer ma profonde gratitude pour leur patience, leurs encouragements et leur soutien. Que dieu leur prête bonheur

À mes frères

À mes sœurs

À toute la famille

À mes amis

Et tous ceux qui m'ont aidé de près ou de loin durant toute la période de travail

BELHADJ NACEUR

Dédicace

Tous nos remerciements et louanges à Dieu qui nous a donné la capacité de terminer ce travail simple

Je dédie ce modeste travail en premier lieu à mes parents qui m'ont soutenu et m'ont encouragé tout au long de mes études.

Et à tous ceux qui ont contribué de près ou de loin pour la réalisation de ce projet, je vous dis merci.

ABBAD ABDELHAK

Table des matières

Chapiter II : Sécurité de IoT

Chapitre III : partie matérielle et logiciel

Chapiter IV : Réalisation & Test

Liste des abréviations

IoT : L'Internet of Things

RFID : Radio Fréquence Identification

RF : radiofréquence

WSN : Wireless Sensors Network

M2M : Machine-to-Machine

NFC : Near Field Communication

RPL : Routing Protocol for Low-Power and Lossy Networks

ETSI : European Telecommunications Standards Institute

xDSL : digital subscriber line

WIMAX : acronyme pour Worldwide Interoperability for Microwave Access

WLAN : Wireless Local Area Network

UUID : identifiant unique universel

SAAS : software as a service

OWASP : Open Web Application Security Project

PaaS : Platform as a Service

CRC : cyclic redundancy check

GPS : Global Positioning System

AOMDV : Adhoc On Demand Distance Vector

FRS : Fragmentation redundancy scattering

ACL : Access Control Lists

RAM : Random Access Memory

ROM : Read Only Memory

EEPROM : Erasable Programmable Read-Only Memory

IDE : Integrated Development Environment

PWM : Pulse Width Modulation

SPI : Serial Peripheral Interface

UART : Universel Asynchronous Receiver Transmitter

PMU : Pari mutuel urbain

PLL : phase-locked loop

Liste des figures

Liste des images

Liste des tableaux

Liste des annexes

Introduction Générale

L'Internet des objets (IoT) est le réseau d'objets physiques - appareils, instruments, véhicules, bâtiments et autres éléments intégrés à l'électronique, aux circuits, aux logiciels, aux capteurs et à la connectivité réseau qui permet à ces objets de collecter et d'échanger des données.

L'IoT est capable d'interagir sans intervention humaine. Certaines applications IoT préliminaires ont déjà été développées dans les secteurs de la santé, des transports et de l'automobile. Cependant, de nombreux nouveaux développements se sont produits dans l'intégration d'objets avec des capteurs dans Internet. Le développement de l'IoT implique de nombreux problèmes tels que l'infrastructure, les communications, la sécurité des données, les interfaces, les protocoles et les normes.

Le but est de fournir le mode avancé de communication entre les différents systèmes et dispositifs en facilitant l'interaction humaine avec l'environnement virtuel. Mais comme tous les dispositifs se basant sur une infrastructure internet pour l'échange d'informations, l'IoT est sensible à divers problèmes de sécurité et a des préoccupations principales de la vie privée des utilisateurs finaux. Les données et infrastructure de l'IoT sont exposées à des risques frauduleuse ou illégale. Les attaques peuvent revêtir diverses formes et provenir de l'extérieur comme de l'intérieur.

Dans la littérature peu de travaux ont traités la problématique de la sécurité de l'internet des objets. Le peu de travaux existants focus sur l'utilisation des mécanismes de cryptographie pour assurer la sécurité des communications entre les objets communicants.

Dans ce mémoire, nous fournissons une étude et une classification approfondies des vulnérabilités existantes, des attaques exploitables, des contre-mesures possibles ainsi que des mécanismes de contrôle d'accès, y compris l'authentification et l'autorisation. Ces défis sont abordés en détail en tenant compte à la fois des technologies et de l'architecture utilisée. En outre, ce travail se concentre également sur les vulnérabilités intrinsèques de l'IoT ainsi que sur les défis de sécurité à chaque couche. En outre, des solutions pour remédier à la sécurité compromise, ainsi que des méthodes d'atténuation des risques, avec prévention et suggestions d'amélioration sont discutées.

Ce manuscrit est subdivisé en quatre chapitres :

1. Le premier chapitre cite l'intérêt de l'IoT, l'évolution d'Internet des objets, principes des IoT, domaines d'applications et composants de l'IoT .
2. Le deuxième chapitre donne le fonctionnement des couches, puis aborde différentes failles de sécurité sur différentes couches de IoT. En outre, il présente les contre-mesures contre les menaces de sécurité de la prévention de tout dommage au réseau IoT.
3. Le troisième chapitre donne un aperçu des moyens que nous utiliserons lors de la réalisation du projet, qui à son divisé en deux partie :
   - partie matérielles, qui sont des appareils électroniques et des capteurs …ect.
   - partie logiciels qui étaient représentés dans les plates-formes, les applications et les services.
4. Le quatrième chapitre décrit la réalisation et l'implémentation de notre prototype d'une maison intelligente afin de montrer la circulation des données dans le système soit entre nodemcu8266 et Firebase soit entre Firebase et l'application Android et iOS.

Enfin, ce travail sera clôturé par une conclusion générale et quelques perspectives de recherche envisagées.

I.1 Introduction

Internet des objets est un réseau global d'objets qui correspond simplement au moment où il a plus de "choses ou d'objets" connectés à Internet que de personnes, chaque objet a une adresse unique. Un objet tel que (ordinateurs, capteurs, RFID et mobile) pourra transmettre des informations et éventuellement recevoir des commandes.

Aujourd'hui l'IoT (Internet of Thinks) est la prochaine évolution d'Internet et permettra d'améliorer considérablement sa capacité même ouvre la voie vers une multitude de scenarios basés sur l'interconnexion entre le monde physique et le monde virtuel

Dans ce chapitre, nous aborderons la définition de cette nouvelle technologie, qui a pu marquer son utilisation dans divers domaines, son histoire depuis qu'elle était inventée jusqu'à nos jours. Puis nous allons voir l'architecture des IoT, leur fonctionnement et les différents domaines d'applications et les problèmes de l'IoT.

I.2 Internet des objets

I.2.1 Définitions d'Internet des objets

Il n'existe pas une définition standard et unifiée de l'Internet des objets, et certaines définitions concernent les aspects techniques de l'IoT, tandis que d'autres définitions évoquent l'utilisation et caractéristique

- **Définition 1 :**

  L'IoT définit différentes solutions techniques avec un ensemble de caractéristiques identification des objets, capter, stocker, traiter, et transférer des données dans les environnements physiques [01].

- **Définition 2 :**

  La technologie IoT est considérée comme l'émergence du futur Internet, certains définir comme "un objet doté d'une identité et d'une personnalité virtuelles, opérant dans des espaces intelligents et en utilisant des interfaces intelligentes pour se connecter et communiquer dans une variété d'environnements d'utilisation". [02]

  D'autres s'en tiennent au côté omniprésent de l'IoT, permettant aux gens de se connecter les uns aux autres, N'importe où, n'importe quand, n'importe quel objet. Ce nouveau paradigme informatique n'est plus basé sur les PC et les périphériques ordinateurs,

mais sur les objets du quotidien en leur attribuant un capteur intégré Intelligence et capacité à communiquer sur Internet. [03]

Figure I. 1: Internet des objets.

I.2.2 Historique de l'IoT

Le terme "Internet des objets" est né en 1999 Le MIT (Massachusetts Institute of Technology) grâce à Kevin Ashton, un chercheur britannique dans le domaine IoT. Ses collaborateurs ont lancé une initiative pour promouvoir la connectivité ouverte. Tous les objets utilisent la RFID (Radio Frequency Identification). Grâce à l'apparition du nouveau protocole IPv6, des secteurs comme l'aéronautique s'enlèvent rapidement du concept de l'Internet des objets et participent aux recherches. Ce dernier est devenu populaire en 2007. Ensuite, nous pensons à la construction d'un Internet mondial des objets

I.2.3 L'évolution d'internet des objets

En 1990, le premier objet de connexion a été reformulé. Ce sont des grille-pain, Machine à café ou autres objets du quotidien. En 2000, le fabricant coréen LG a lancé un industriel qui parle sérieusement d'électroménager connecté à Internet et La même année verra les premières expérimentations d'appareils connectés à Internet pour rechercher automatiquement des informations.

En 2003, la population mondiale atteignait environ 6,3 milliards et 500 millions d'appareil connecté à Internet [3]. Le résultat de la division du nombre d'appareils par La population mondiale (0,08) indique un faible nombre d'appareils connectés par habitant. Selon la définition Cisco IBSG, l'Internet des objets n'existait pas en 2003 en raison du

nombre d'objets la connexion est faible. En raison de l'explosion des smartphones et des tablettes, le nombre d'appareils et le nombre de personnes connectées à Internet a atteint 12,5 milliards en 2010, alors que la population mondiale 6,8 milliards.

C'est pourquoi il y a plus d'un appareil connecté par personne (1.84) pour la première fois dans l'histoire. Cisco explique l'évolution du nombre d'objets dans son livre blanc IoT [04]. Aujourd'hui, il dépasse largement le nombre d'habitants sur Terre, et Comme indiqué, il devrait continuer à croître pour atteindre 50 milliards.

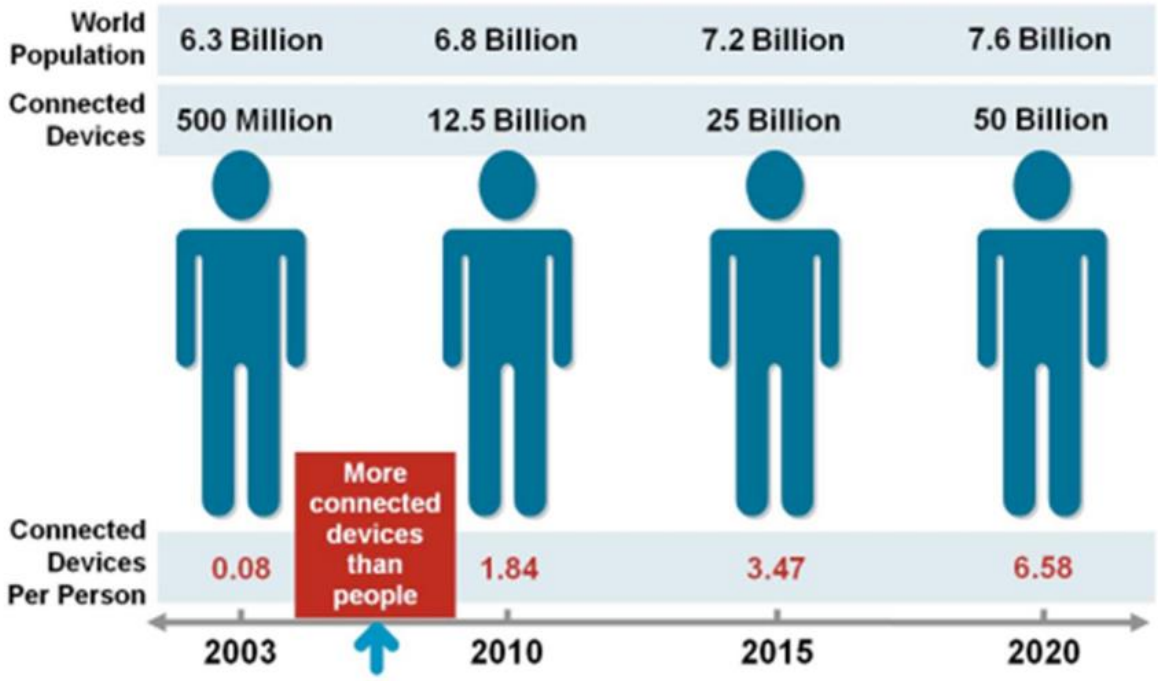

Figure I. 2: IoT Aujourd'hui [3]

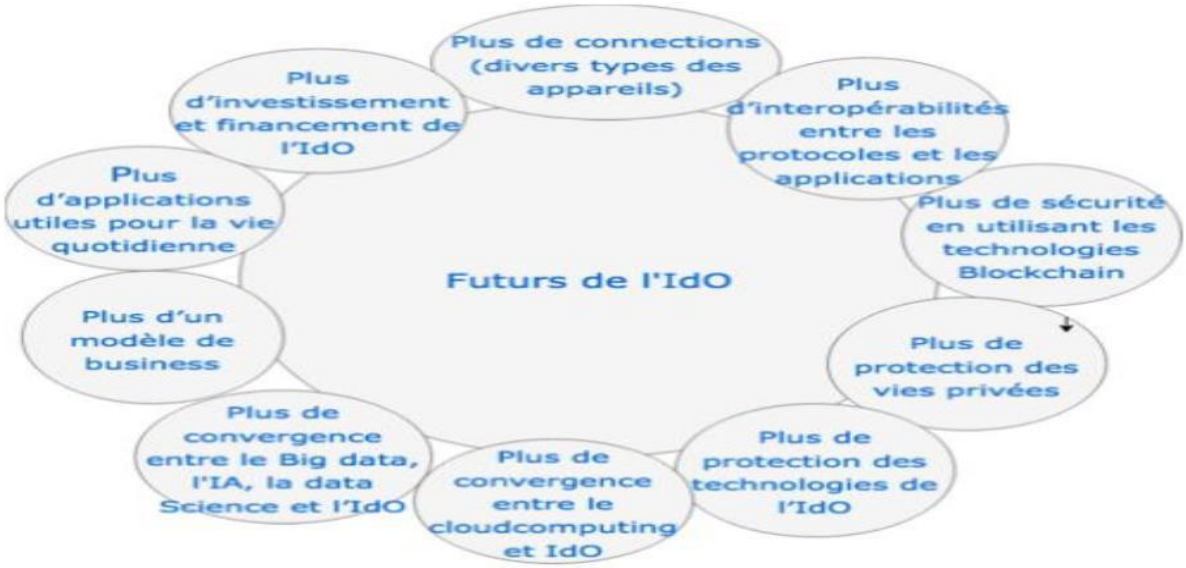

Figure I. 3: Future de l'IoT [3].

I.2.4 Principes des IoT

L'IoT se compose de plusieurs éléments complémentaires, dont chacun a ses propres caractéristiques. Il permet l'utilisation d'un système d'identification électronique appareils mobiles standard et sans fil, identifiés directement et sans ambiguïté objets physiques et capacité à récupérer, stocker, transmettre et traiter sans interruption données connexes. L'IoT est une combinaison d'innovations et de solutions technologiques récentes existant. Chaque objet est équipé d'une identification électronique unique capable de lire et transporter des données par des protocoles dans le réseau Internet. Cependant, il faut définir la nature d'un objet, sa fonction, sa localisation dans l'espace, son histoire pour créer un lien entre physique et virtuel, les dispositifs technologiques doivent modéliser donc l'environnement réel et rendez-le virtuel.

I.2.5 Domaines d'applications

L'Internet des Objets est utilisé dans divers secteurs tel que l'agriculture, soins de santé, la domotique… etc.

- **Domotique (domotique) :**

C'est un ensemble de technologies qui permettent à la maison d'être intelligente, de penser par elle-même, et de contrôler divers équipements depuis la même interface (téléphone, panneau) grâce à l'Internet des objets, qui a facilité et créé la communication entre les appareils électroménagers et les a contrôlés. à distance, et dans ce sens et la propagation de l'Internet des objets nous arrivons aux villes [05].

- **Agriculture (Agriculture):**

Dans ce domaine, des réseaux de capteurs interconnectés l'Internet des objets peut être utilisé pour surveiller l'environnement des cultures [7]. Ce qui conduit à de bons résultats et à l'amélioration de l'eau d'irrigation et de l'utilisation des intrants et de la planification des travaux agricoles grâce à eux, ces réseaux peuvent être utilisés pour lutter contre les dégâts et les catastrophes et améliorer la qualité de l'environnement en général

- **Villes intelligentes** (**Smart City):**

Le terme villes intelligentes est utilisé pour désigner l'écosystème cyber [7]. Grâce à des services avancés, il est en effet peut optimiser l'utilisation de l'infrastructure physique de la ville (réseau routes, réseaux électriques, etc.), améliorant ainsi la qualité de vie des personnes citoyen.

- **Santé:**

En santé, l'IoT surveillera les signes fournir des cliniques aux patients en créant des réseaux personnels et des capteurs médicaux surveiller les constantes biologiques telles que la température corporelle, Tension artérielle et activité respiratoire [05]. Afin de faciliter la surveillance et d'apporter des solutions, notamment aux personnes à mobilité réduite, dans le domaine de la santé, leurs activités dans leur milieu de vie sont surveillées grâce à des capteurs portables (accéléromètres, gyroscopes, etc.) ou fixes.

- **environment:**

Dans ce domaine, un rôle clé est joué par capacité à détecter et autogérer les phénomènes naturels, vent, Hauteurs des rivières, etc. De plus, une intégration transparente de ces données hétérogènes [05]

- **Sécurité de la surveillance:**

La sécurité de la surveillance est Devenir un bâtiment d'entreprise, un centre commercial, usine, parking et autres lieux publics. Tout en protégeant la vie privée utilisateur [05]. Afin d'obtenir et d'acquérir une grande capacité de sécurité et facilement Il existe plusieurs capteurs utilisés pour la surveillance par exemple il y a des capteurs ambiants qui peuvent être utilisés pour surveiller la présence des produits chimiques dangereux, des captures de surveillance du comportement des personnes pour détecter la présence des personnes qui agissent de manières suspectes.

- **Industriel:**

Dans le domaine de l'IoT industriel permettra un suivi complet des produits, En encadrant de la chaîne de production à la chaîne logistique de distribution conditions de fourniture, lutte contre la contrefaçon, la fraude et la criminalité économie transfrontalière.

.

Figure I. 4: Domaine d'application de l'IoT [7]

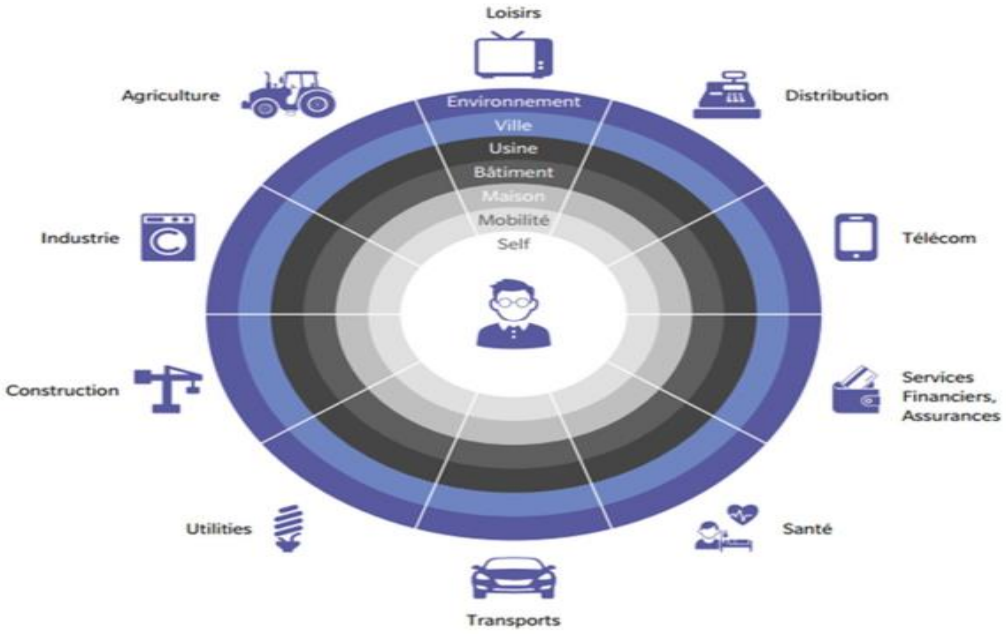

Figure I. 5: divers domaines d'exploitation IoT

I.2.6 Composantes de l'IoT

Les composant l'IoT est cinq. L'objet connecté est d'abord un objet qui a une fonction mécanique et/ou électrique propre, il peut soit être conçu directement connectable, soit il est déjà existant et la connectivité est rajoutée à posteriori. L'objet connecté a pour fonction de collecter des données de capteurs, de traiter ces données et de les communiquer à l'aide de d'une fonction de connectivité et de recevoir des instructions pour exécuter une action. Généralement ces fonctions de l'objet connecté nécessitent une source d'énergie, surtout quand les données sont prétraitées directement dans l'objet [06].

- **Capteur**

Les capteurs sont des dispositifs permettant de transformer une grandeur physique observée (température, luminosité, mouvement etc…) en une grandeur digitale utilisable par des logiciels. Il existe une très grande variété de capteurs de tous types, les objets connectés ont souvent la fonction de captation de ces grandeurs physiques sur leurs lieux d'utilisation. Exemple de capteurs : lumière, présence, proximité, position, déplacement, accélération, rotation, température, humidité, son, vibration, électrique, magnétique, chimique, gaz, flux, force, pression, niveau, … [06].

- **Réseaux de capteurs**

Afin de satisfaire les besoins de communication entre eux, les capteurs sont équipes de dispositifs sans fil pour l'émission et la réception de données. Cela ne suffit cependant pas à

rendre un ensemble de capteurs accessibles ou du moins de manière interopérable, transparente et simplifiée pour cela, les capteurs doivent aussi s'organiser ce qui caractérise un réseau de capteurs, c'est que ses éléments sont de très petits appareils, dotes de capacités de transmission sans fil [07].

- **Énergie**

La plus importante contrainte à laquelle sont soumis les restes aux capteurs concernant l'énergie. L'autonomie temporelle des nœuds s'évalue en termes d'années [08].

- **Actionneurs**

Les actionneurs sont des dispositifs qui transforment une donnée digitale en phénomène physique pour créer une action, ils sont en quelque sorte l'inverse du capteur. Exemple d'actionneurs : Afficheurs, Alarmes, Caméras, Haut-parleurs, Interrupteurs, Lampes, Moteurs, Pompes, Serrures, Vannes, Ventilateur, Vérins, [06].

- **Connectivité**

La connectivité de l'objet est assurée par une petite antenne Radio Fréquence qui va permettre la communication de l'objet vers un ou plusieurs réseaux (qui sont détaillés dans la section « réseaux IoT »). Les objets pourront d'une part remonter des informations telles que leur identité, leur état, une alerte ou les données de capteurs, et d'autre part recevoir des informations telles que des commandes d'action et des données. Le module de connectivité permet aussi de gérer le « cycle de vie de l'objet », c'est-à-dire, l'authentification et l'enregistrement dans le réseau, la mise en service, la mise à jour et la suppression de l'objet du réseau.[06].

I.2.7 Étapes pour configurer IoT

Pour simplifier le cadrage d'un projet IoT, nous l'avons modélisé en 6 étapes élémentaires La construction de l'objet de connexion. Avec une solution IoT simple et pratique, facilement utilisable, pour aider tous les entrepreneurs souhaitant se lancer dans le monde de l'Internet des objets.

- **Éléments centraux des projets IoT**

Un objet Box inséré dans un véhicule pour surveiller le mouvement, des capteurs permettent mesurer les éléments de température ou de pression des équipements industriels, même gérer le matériel médical hospitalier (maintenance, taux d'utilisation), l'objet connecte peut-être représentatif d'éléments extrêmement différents et diversifies. La

première étape est donc d'acquérir, ou de construire le cas échéant, l'objet adapte aux contraintes physiques du cas d'usage de l'entreprise.

- **Connectivité pour la communication de l'objet de connexion**

Une fois cette problématique de l'objet traitée, l'objectif est de le rendre communiquant. Si l'objet captée les données, elles n'ont aucun sens si elles ne sont pas transférées. Un ensemble de solutions de connectivité existe pour faire parler' l'objet. En fonction de la nature de l'objet et des données qu'il capte, il faudra choisir le bon réseau : 2G/3G/4G, réseaux bas débit et basse consommation (type Sigfox, NB-IoT).

- **Collecter toutes les données**

Face a la multitude des objets, la collecte et la modélisation de l'ensemble des données produites est un point crucial. Pour les traiter, toutes les données doivent être collectées et traitées afin d'être exploitable et ce `a travers un seul outil simple et ergonomique.

- **Hébergement et stockage de données**

Les données doivent être stockées, gérées et administrées en toute sécurité. Face à la criticité des données (exemples donnés de sante ou de géo-localisation), il est important de bénéficier d'une infrastructure qui garantit la sécurité des données et qui soit en mesure de s'adapter à la montée en charge du projet.

- **Développement de la logique d'application**

Pour donner un sens aux données collectées et en d´engager toute la valeur (optimisation de l'activité de l'entreprise, fidélisation de ses clients ou encore proposition de nouveaux services innovants), il faut pouvoir les utiliser et les lier entre elles. Cela se traduit par le développement et la mise en œuvre d'une application IoT. Au travers d'une telle application, l'entreprise peut utiliser au mieux ces données et piloter les objets ou les processus.

- **Restauration des données capturées par l'objet de connexion**

Pour proposer ces nouveaux services innovates à ses clients, entreprise doit mettre une interface à leur disposition pour interagir avec eux. Cette application IoT, proposée sous forme d'interface web, d'application mobile permet de partager les données avec ses clients ou ses fournisseurs, en toute simplicité et d'améliorer l'expérience client par exemple.

I.2.8 Les Technologies de communication de base

Pour assurer la fonctionnalité de l'IoT, diverses technologies sont utilisées, nous allons juste pour parler de certaines technologies telles que : RFID, WSN et M2M [09] :

- **RFID :** Ce concept regroupe toutes les technologies qui fonctionnent avec les ondes radio afin de reconnaître automatiquement des objets ou des personnes. Ces caractéristiques sont : stockage et récupération à distance d'informations.
- **WSN :** C'est un réseau coopératif, chaque nœud du réseau a un ensemble de caractéristiques telles que : puissance de traitement, différents types de mémoire, Émetteurs-récepteurs RF et alimentations, ainsi que divers capteurs et actionneurs [10].
- **M2M :** C'est la technologie de l'information, combinée à la communication des objets intelligents pour leur donner la possibilité d'interagir sans intervention avec le système d'information d'un organisme ou d'une entreprise [11].

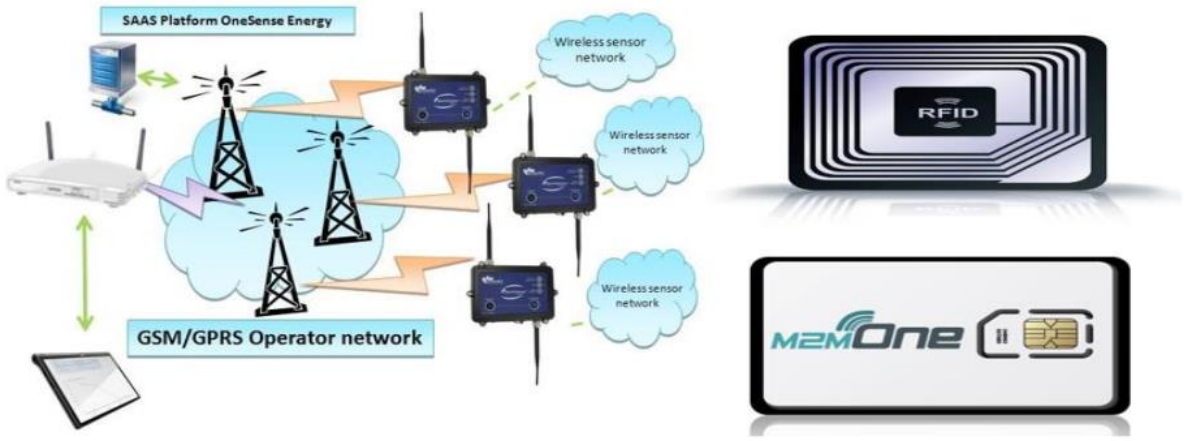

Figure I. 6: Les différentes technologies de communication

I.2.9 Architecture de l'Internet des objets

Le développement rapide de l'Internet des objets est-il une architecture de référence nécessaire pour normaliser la conception des systèmes et favoriser l'interopérabilité ? et la communication entre différents écosystèmes IoT [12].

I.2.9.1 Architecture et normalisation

Les racines de l'IoT remontent à la technologie M2M (Machine-to-Machine) pour le contrôle processus à distance. L'IoT est aujourd'hui un mélange de technologies tels que RFID, NFC, capteurs et actionneurs sans fil, M2M, l'ultrage bande ou 3/4G, IPv6, 6lowPAN et RPL doivent définir des architectures et des standards afin de faciliter son

développement dans le futur. L'ETSI propose une architecture découpée en trois domaines distincts, le domaine du réseau d'objets, le domaine du réseau cœur d'accès et le domaine des applications M2M et applications clientes [13].

I.2.9.2 Domaine de réseau d'objets

Dans ce domaine, nous avons trouvé différentes technologies d'interconnexion d'objets M2M, RFID, Bluetooth, IETF6L Low PAN, IETFRPL et passerelle vers les réseaux cœur de transport [14].

I.2.9.3 Le domaine du réseau cœur

Dans ce domaine, nous découvrirons différentes technologies de réseaux de transport et Accès xDSL, WIMAX, WLAN, 3/4G, etc. [15].

I.2.9.4 Application M2M et d'application client

Ce domaine est composé de plateformes M2M, de middleware et d'API pour les applications M2M, Processus métiers exploitant l'IDO, etc. [15]

I.2.10. Avantage et Inconvénient du réseau IoT

- **Avantage :**

L'IoT est une infrastructure nouvelle qui va intégrer les objets connectés, permettre l'apparition d'un réseau ubiquitaire et nous donner un avantage quotidien. Elle peut être considéré comme un concept ayant des répercussions sur les technologies et la société dans divers secteurs : des secteurs privés, étatique et industrielle 4.0. Elle permettra de rendre l'environnement connecté et pouvoir communiquer avec lui, à l'avenir nous serons informés de l'état du sol, de l'humidité et de la quantité de lumière reçu, ce simple cas, permet de nous donner un aperçu global sur son potentiel et sur ces avantages.

- **Inconvénient :**

L'IoT gère nos données personnelles, en effet, les objets connectés produisent de grandes quantités d'information et le traitement de cette masse de données implique de nouvelle préoccupation notamment autour de la confidentialité et de la sécurité.

I.3 Objet Connecté (OC)

I.3.1 Définition

Un objet connecté est un appareil dont la conception ne se limite pas à la notion de système informatique ou d'interface d'accès au web, mais dont le but principal est d'accéder à la notion d'appareils que l'homme utilise sans interférer avec leur contrôle à travers eux. par exemple, un objet comme une machine à café ou La serrure est conçue sans intégrer de systèmes informatiques ni se connecter à Internet. L'intégration de la connexion Internet avec l'OC permet de l'enrichir en interagissant avec lui environnement, OC s'enrichit (OCE), c'est-à-dire que l'on retrouve l'intégration connexion Internet à la machine à café, facilitant l'accès à distance. OC peut réagir avec le monde matériel de manière indépendante sans avoir besoin des humains. Il a de nombreuses limitations telles que la mémoire, la bande passante et la consommation d'énergie. Il doit être certifié pour l'utilisation, il a une forme d'intelligence et de capacité Recevoir et transmettre des données à l'aide d'un logiciel utilisant des capteurs embarqués [16]

I.3.2 Les éléments des OC

Un OC à trois éléments clés [17] :

- Données générées ou reçues, stockées ou transmises.
- Algorithmes de traitement de ces données.
- L'écosystème dans lequel il va réagir.

I.3.3 Deux types d'objets sont distingués

- **Objets passifs :**

Ils utilisent généralement des tags (puces RFID, codes-barres 2D). Leur disposent d'une faible capacité de stockage (environ un kilo-octet), leur permettant d'assurer un rôle identification. Ils peuvent parfois embarquer des capteurs dans le cas d'une puce RFID (température, humidité) et être réinscriptible.

- **Objets actifs:**

Ils peuvent être équipés de plusieurs capteurs, d'une plus grande capacité de stockage et être doté d'une capacité de traitement ou encore être en mesure de communiquer sur un réseau

I.3.4 Quelques objets connectés

- **Objets traditionnels** : ordinateur, tablette, Smartphone …etc.

Figure I. 7: les objets traditionnels

- **Nouveaux objets connectés :** appareil électroménager, instrument de mesure, robots, serrures, machine-outil, montre, véhicule…etc.

Figure I. 8: nouveaux objets connectés

❖ **Jonction entre le monde physique et le monde numérique**

Les objets connectés sont considérés comme l'avenir d'Internet. Jusque-là, Internet est purement virtuel et n'interagit qu'avec des données numériques. Maïs Avec l'avènement de l'Internet des objets, nous pouvons connecter le monde virtuel au monde physique permet la surveillance et le contrôle à distance. L'IoT est donc la passerelle entre les deux mondes physiques et monde numérique

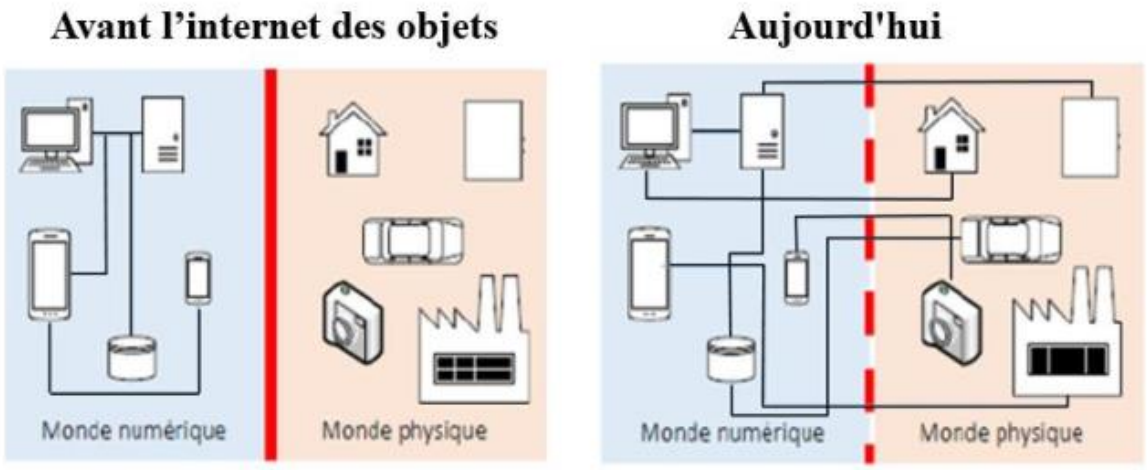

Figure I. 9: Jonction entre le monde physique et le monde numérique.

I.4 Conclusion

L'IoT comme le permet l'évolution de internet actuel notre mode de vie et les objets intelligent se sont considérablement améliorés Le milieu environnement interagit les uns avec les autres.

Dans ce chapitre, nous avons expliqué les concepts qui composent l'internet des objets L'avenir de plusieurs domaines. Nous avons brièvement mentionné les domaines d'application d'Internet des objets. Ensuite, nous avons discuté de son architecture et de son fonctionnement

II.1 Introduction:

La sécurité des informations essentielles sur IoT devrait s'intégrer dans différentes fonctionnalités telles que l'identification, la confidentialité et la confidentialité des données, etc. Ainsi, avec le développement rapide et un mélange d'appareils hétérogènes, il formule une infrastructure IoT à très grande échelle. Il est donc prévu que IoT soit menacé par sa technologie polyvalente et ses capacités futures. Les menaces de sécurité pour l'IoT telles que le déni de service, la force brute, les attaques de l'homme du milieu et de nombreuses autres attaques sont envisagées dans le réseau interconnecté. Ces attaques se produisent en raison d'un mot de passe faible, de l'absence de cryptage, de la fuite d'informations personnelles, etc., de sorte que le stockage de ces données confidentielles sur le cloud est assez alarmant. Si ces attaques de sécurité ne sont pas résolues à un certain niveau de sécurité, ces services de sécurité faibles peuvent être nocifs pour le marché de IoT. Cela implique non seulement de tels problèmes de sécurité, mais également des problèmes de contrôle d'accès, d'authentification de divers réseaux et des problèmes de stockage d'informations. Ce problème nécessite une infrastructure de sécurité bien définie qui puisse résoudre ces problèmes et réduire les défis de sécurité.

II. 2 Les différentes couches dans la sécurité de IoT

II.2.1 Couche physique (Physical Layer)

La couche physique traite de l'environnement physique et collecte toutes les données obtenues du monde réel à l'aide de nœuds de capteurs et d'autres dispositifs physiques. Cette couche est responsable de la communication entre les différents appareils physiques. L'objectif de cette couche est de fournir des services au réseau et l'authentification des appareils. Les principaux appareils [18] de la couche physique comprennent Arduino, ZigBee, les codes-barres, la RFID et tous les autres types de capteurs. Chaque appareil du système IoT doit avoir une étiquette unique qui permet une connexion solide au réseau et la plupart des identifiants universels uniques (UUID) sont utilisés dans l'ensemble du réseau par divers appareils. De manière uniforme, un appareil peut être connecté à de nombreux nœuds de capteurs avec un identifiant unique car l’identification unique des objets. La couche réseau transporte la collecte des informations transmises et transférées au centre système de traitement. [18]

II.2.2 Couche réseau (Network Layer)

La couche réseau est également appelée couche de transmission. Il agit comme un pont entre la couche de perception et la couche d'application. Il transporte et transmet les

informations collectées à partir des objets physiques via des capteurs. Le support de transmission peut être sans fil ou filaire. Il prend également la responsabilité de connecter les objets intelligents, les périphériques réseau et les réseaux les uns aux autres. Par conséquent, il est très sensible aux attaques du côté des attaquants. Il présente des problèmes de sécurité importants concernant l'intégrité et l'authentification des informations transportées sur le réseau.[19]

II.2.3 Couche de traitement (Processing Layer)

La couche de traitement est également appelée couche middleware. Il collecte les informations envoyées à partir d'une couche de transport. Il effectue un traitement sur les informations collectées. Il a la responsabilité d'éliminer les informations supplémentaires qui n'ont pas de sens et d'extraire les informations utiles. Cependant, cela supprime également le problème du Big Data dans IoT. Dans le Big Data, une grande quantité d'informations est reçue, ce qui peut affecter les performances de IoT. De nombreuses attaques peuvent affecter la couche de traitement et perturber les performances de IoT. [19]

II.2.4 Couche d'application (Application Layer)

La couche application définit toutes les applications qui utilisent la technologie IoT ou dans lesquelles IoT s'est déployé. Les applications de IoT peuvent être les maisons intelligentes, les villes intelligentes, la santé intelligente, le suivi des animaux, etc. Il a la responsabilité de fournir les services aux applications. Les services peuvent varier pour chaque application car les services dépendent des informations collectées par les capteurs. Il existe de nombreux problèmes dans la couche application dans laquelle la sécurité est le problème clé. En particulier, lorsque IoT est utilisé pour créer une maison intelligente, il introduit de nombreuses menaces et vulnérabilités de l'intérieur et de l'extérieur. Pour mettre en œuvre une sécurité renforcée dans une maison intelligente basée sur IoT, l'un des principaux problèmes est que les appareils utilisés dans les maisons intelligentes ont une faible puissance de calcul et une faible quantité de stockage. [19]

Figure II. 1: la déférente couche dans sécurité de IoT

II.3 Attaques à différentes couches

Dans cette section, diverses menaces de sécurité qui menacent la confidentialité des données et leurs éventuelles contre-mesures sur chaque couche suggérée récemment est brièvement discutée.

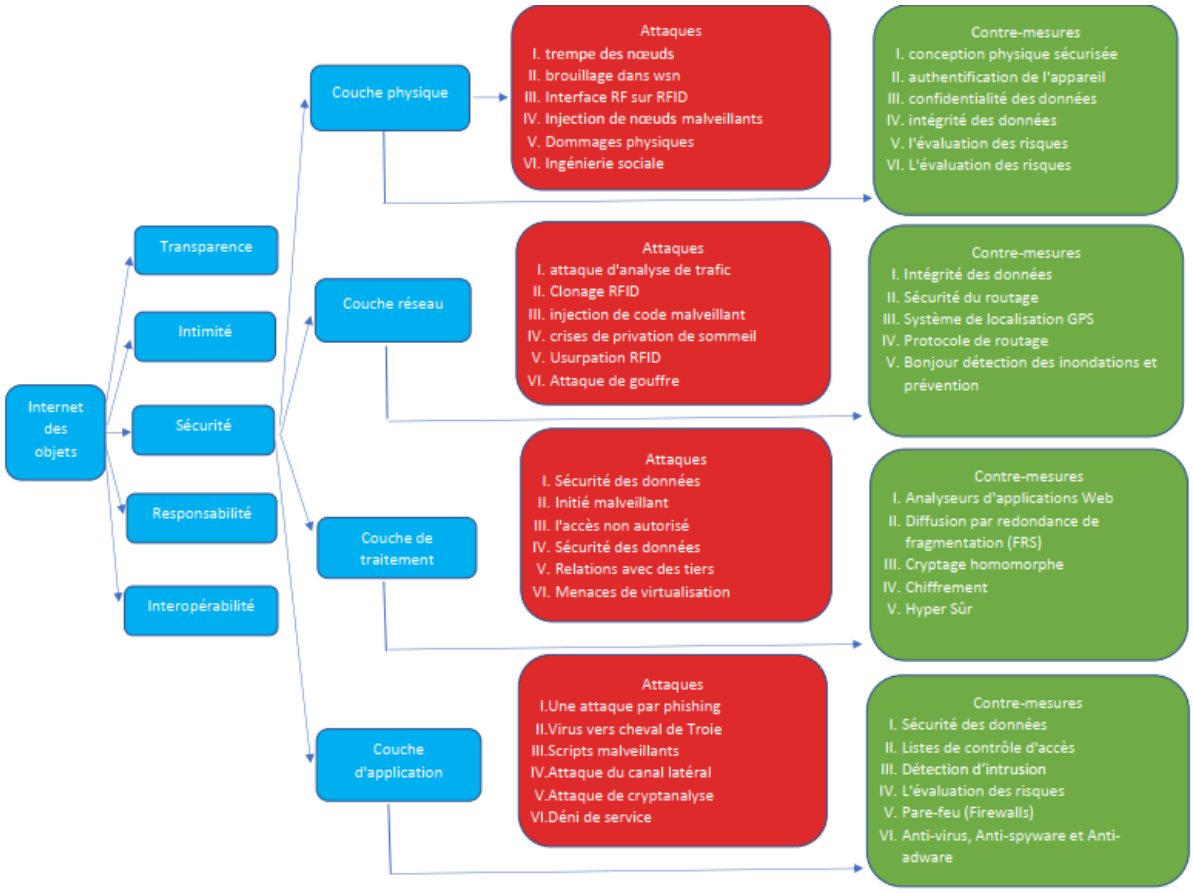

Figure II. 2: Attaques et contre-mesures sur les couches de IoT

II.3.1 Couche physique (Physical Layer)

Couche physique composée de diverses technologies de capteurs habilitants telles que Bluetooth, GPS et Zigbee qui ne sont pas protégées contre différents types d'attaques. Ce type d'attaque est mis en œuvre sur les parties matérielles du réseau IoT et l'adversaire doit être proche des systèmes IoT. Le tableau 1 analyse brièvement les attaques de la couche physique

Nom de l'attaque	Effets	contre-mesures	description des contre-mesures
Nœud Trempé	altérer les informations sensibles en endommageant les capteurs	Conception physiquement sécurisée	Physiquement sécurisé La conception des appareils ne doit pas être modifiable et ne pas être de haute qualité
Brouillage du nœud dans le réseau de capteurs sans fil	blocage de la communication entre les nœuds	Canal de sécurité IPSec	Node tempering and eavesdropping can be stopped by encryption and authentication witch ensures confidentiality of data
Interface RF sur RFID	Arrêter la communication par distorsion des signaux	Authentificatio n de l'appareil	Un nouvel appareil physique avant d'envoyer et de recevoir des données, l'appareil doit s'authentifier lui-même
Injection de nœuds malveillants	Créer une interruption dans le processus de transmission	démarrage sécurisé	le démarrage sécurisé est donné par un algorithme de hachage cryptographique qui vérifie le logiciel sur les appareils par signature numérique
Dommages physiques	Attaquer les appareils et endommager le réseau IoT	L'évaluation des risques	assure la confidentialité des données et évite les plages de sécurité dans un réseau IoT
Ingénierie sociale	fuite d'informations privées	La confidentialité des données	lorsque les données sont envoyées à la destination, cela évite à l'attaquant d'accéder aux données essentielles
Attaque de privation de sommeil	Arrêt des nœuds	Authentificatio n de l'appareil	lorsque les données sont envoyées à la destination, cela évite à l'attaquant d'accéder aux données essentielles
Accès non autorisé aux balises	Modifier ou supprimer l'ensemble des informations	Authentificatio n de l'appareil	avec l'aide de l'authentification de l'appareil, un appareil inconnu ne peut pas communiquer dans le réseau IoT

Tableau II. 1: Analyse de la couche physique

- **Nœud Trempé (Node Tempering):** Ce type d'attaque peut détruire le nœud du capteur ou causer des dommages en envoyant et en recevant physiquement un nœud ou un composant matériel complet ou même en examinant électroniquement les nœuds pour accéder et modifier des informations sensibles [20].
- **Brouillage_du nœud dans le réseau de capteurs sans fil (Jamming of node in Wireless Sensor Network):** Les attaques de brouillage dans les WSN sont perpétrées par des nœuds malveillants du réseau, dans le but de perturber ou d'interférer avec la transmission et la réception de signaux sans fil légitimes entre les nœuds capteurs. Les attaques par brouillage affectent les caractéristiques statistiques (par exemple la moyenne et la variance) d'un flux de paquets avec des fluctuations temporelles. La maîtrise statistique des procédés (SPC), peut donc être utilisée pour détecter cette anomalie en observant des séries d'événements statistiquement homogènes. [21]
- **Interface RF sur RFID (RF Interference on RFIDs):** Une attaque par déni de service peut être mise en œuvre sur n'importe quelle étiquette RFID en créant et en envoyant des signaux de bruit sur les signaux de radiofréquence qui sont utilisés par les RFID pour la communication [22].
- **Injection de nœuds malveillants (Malicious Node Injection):** Dans cette attaque, l'attaquant injecte physiquement un nouveau nœud malveillant entre deux ou plusieurs nœuds. Il modifie ensuite les données et transmet les informations erronées aux autres nœuds. L'attaquant utilise plusieurs nœuds pour effectuer une attaque par injection de nœud malveillant. Le l'adversaire insère d'abord une réplique du nœud B. Après cela, insère d'autres nœuds malveillants (nœud M1). Ces deux nœuds travaillent ensemble pour exécuter l'attaque. Ainsi, une collision se produit au nœud victime. À cause de cela, le nœud attaqué ne peut recevoir/envoyer aucun paquet. Par conséquent, la conclusion des nœuds de surveillance peut être affectée en annonçant à tort que le nœud attaqué (le nœud légitime) agit de manière malveillante. Pour empêcher cette attaque, nous utilisons un schéma de vérification de surveillance. Il peut vérifier le résultat du ou des nœuds de surveillance et identifier correctement tout comportement malveillant. Selon l'accusé de réception, le nœud vérificateur décidera si le le nœud est malveillant ou non [23].
- **Dommages physiques (Physical Damage):** l'attaquant peut endommager le réseau de IoT en attaquant les appareils à ses propres fins. Ce Le type d'attaque traite de la sécurité hébergée par le système IoT. Ce type d'attaque est différent de l'attaque Node

Tempering parce que dans cette attaque l'attaquant essaie d'endommager directement le Services IoT [24].

- **Ingénierie sociale (Social Engineering):** L'attaquant manipule les utilisateurs d'un système IoT, pour extraire des informations privées ou pour effectuer certaines actions qui serviraient ses objectifs. Ce type d'attaque est classé dans la catégorie des attaques physiques car l'attaquant doit interagir physiquement avec les utilisateurs du réseau IoT pour atteindre ses objectifs. [25].
- **Attaque de privation de sommeil (Sleep Deprivation Attack) :** Les nœuds de capteurs du réseau de capteurs sans fil sont alimentés par des batteries dont la durée de vie n'est pas si bonne, de sorte que les nœuds sont tenus de suivre les routines de veille pour prolonger leur durée de vie. La privation de sommeil est le type d'attaque qui maintient les nœuds éveillés, ce qui entraîne une plus grande consommation de la batterie et, par conséquent, la durée de vie de la batterie est minimisée, ce qui provoque l'arrêt des nœuds [26].
- **Injection de code malveillant (Malicious code injection) :** Il s'agit d'un type d'attaque grave dans lequel un attaquant compromet un nœud pour injecter un code malveillant dans le système, ce qui pourrait même entraîner un arrêt complet du réseau ou, dans le pire des cas, l'attaquant peut obtenir un contrôle total du réseau [26].
- **Accès non autorisé aux balises (Unauthorized Access to the Tags):** Dans ce type d'attaque, l'adversaire peut accéder à n'importe quelle balise sans aucune autorisation. Cela peut être fait en raison de l'insuffisance de la procédure d'authentification appropriée dans le système RFID L'attaquant ne peut pas seulement accéder aux données mais peut modifier ou même supprimer l'intégralité des informations ou des données. [27]
- **Clonage de balises (Tag Cloning):** Dans le système IoT, les balises sont déployées sur divers objets physiques qui sont visibles et ainsi les données peuvent être lues et également modifiées par certaines techniques de piratage. Ainsi, les données cruciales peuvent être facilement accessibles par tout cybercriminel qui peut découvrir une étiquette en double et, par conséquent, l'utilisateur ne peut pas faire la distinction entre les données en double et les données originales [28].
- **écoute clandestine (Eavesdropping):** Dans ce type d'attaque, l'attaquant peut facilement obtenir des informations confidentielles telles qu'un mot de passe ou d'autres données qui circulent d'une étiquette à l'autre ou d'un utilisateur à l'autre. Ce type d'attaque peut se produire car la RFID a des caractéristiques sans fil. [29]

- **Usurpation (Spoofing):** Lors de l'usurpation d'identité, l'adversaire diffuse de fausses informations sur le système RFID et les suppose comme originales et fait en sorte que les données proviennent de la source d'origine. Par conséquent, l'attaquant capture des informations et obtient un accès complet au réseau. [30].
- **Attaque chronométrée (Timing Attack):** Une autre attaque menaçante de la confidentialité du système est l'attaque temporelle dans laquelle l'attaquant peut accéder à la clé de cryptage en analysant le temps nécessaire pour effectuer la tâche de cryptage [31]. Side Channel est également un type d'attaque temporelle dans laquelle l'adversaire attaque les dispositifs de cryptage en cas de fuite d'informations sur la durée de fonctionnement du dispositif [32] comme la consommation d'énergie, le traitement ou le rayonnement électromagnétique, etc.
- **Attaque par capture de nœud (Node Capture Attack):** Dans la capture de nœud, l'attaquant capture toutes les données et informations privées en contrôlant complètement le nœud [33]. L'adversaire peut ajouter un nœud en double au réseau et en envoyant des données malveillantes, il menace la confidentialité des données.
- **Rejouer l'attaque (Replay Attack):** La confidentialité de la couche de perception peut être facilement exploitée par ce type d'attaque. L'adversaire modifie ou rejoue le nœud en usurpant les informations telles que l'identité et l'emplacement, etc. du nœud dans le système IoT [34].
- **Routage des menaces (Routing Threats**): L'attaquant peut générer des boucles de routage en modifiant et en faussant les informations de routage, [35] bloque la transmission du réseau et agrandit le chemin du réseau en envoyant de nombreux messages d'erreur, ce qui augmente le délai point à point, etc.

II.3.2 Attaques de la couche réseau (Network Layer Attacks)

Dans l'attaque de réseau, l'adversaire doit se concentrer sur le réseau du système IoT et l'attaquant n'a pas besoin être proche du réseau de l'IoT. Le tableau 2 analyse brièvement les attaques de la couche réseau.

Nom de l'attaque	Effets	contre-mesures	description des contre-mesure
Attaque de gouffre	fuite de données des nœuds	routage ad hoc sensible à la sécurité	arrêter les attaques à l'intérieur du réseau de l'IoT et l'adversaire est retiré du réseau
Attaques d'analyse de trafic	fuite d'informations secrètes sur le réseau de l'IoT	sécurité du routage	la sécurité du routage est utilisée pour la confidentialité des données. Dans cette technique, les données transmises sont stockées dans des paquets après l'analyse des données, puis envoyées au traitement
Clonage RFID	Accéder aux données utiles par imitation RFID	authentification	à l'aide d'une authentification appropriée sur le mécanisme, le clonage de la RFID peut être empêché
Usurpation RFID	Contrôle le processus de transmission et la manipulation des données	Technique du système GPS	rencontrer l'attaque par usurpation d'identité
Attaque de trou de ver	déplacement de bits dans le réseau	protocole de routage	Le protocole de routage est utilisé pour produire les multiples chemins entre l'expéditeur et le destinataire de la route
Bonjour attaque d'inondation	embouteillage et blocage des canaux	Bonjour détection des inondations et prévention	un nœud envoie un message bonjour pour vérifier la force du signal si la force est similaire à une portée radio, le récepteur accepte le message
Attaque d'informations de routage	Destruction du réseau par routage	chiffrement des tables de routage	OWAS identifie différents problèmes de sécurité sur le Web par un processus de cryptage en déroute

Tableau II. 2: Analyse de la couche réseau.

- **Attaques d'analyse de trafic (Traffic Analysis Attacks):** l'attaquant intercepte et examine les messages pour obtenir des informations sur le réseau [36].
- **Clonage RFID (RFID Cloning) :** Un attaquant clone une étiquette RFID en copiant les données de l'étiquette RFID de la victime sur une autre étiquette RFID. Bien que les deux étiquettes RFID aient des données identiques, cette méthode ne réplique pas l'ID

d'origine de la RFID, ce qui permet de faire la distinction entre l'original et le compromis, contrairement à l'événement de l'attaque par usurpation RFID [25].

- **Injection de code malveillant (Malicious Code Injection) :** Ce type d'attaque provoque de graves effets sur le réseau de IoT ou peut même bloquer l'ensemble du réseau. Dans cette attaque, [37] l'adversaire injecte un code malveillant dans un système en comprenant un nœud. Ainsi, l'attaquant obtient un contrôle total sur le réseau IoT.
- **Attaque de privation de sommeil (Sleep Deprivation Attack):** Dans le réseau de capteurs sans fil, les nœuds de capteurs sont chargés avec des batteries qui ne sont pas compatibles car la durée de vie de ces batteries n'est pas si efficace, de sorte que la procédure de routine de veille est utilisée pour les nœuds pour améliorer la durée de vie de la batterie [38]. Dans l'attaque par privation de sommeil, l'adversaire garde la batterie éveillée, ce qui entraîne une plus grande consommation de la batterie et, enfin, il arrête les nœuds de capteur.
- **Usurpation RFID (RFID Spoofing):** Un attaquant usurpe un signal RFID pour lire et enregistrer une transmission de données à partir d'une étiquette RFID. Ensuite, l'attaquant peut envoyer ses propres données contenant l'ID de balise d'origine, ce qui donne l'impression qu'il est valide, d'où l'attaquant obtient un accès complet au système en prétendant être la source d'origine. [39]
- **Accès non autorisé RFID (RFID Unauthorised Access):** En raison du manque de mécanismes d'authentification appropriés dans la majorité des systèmes RFID, les étiquettes sont accessibles à tous. Cela signifie automatiquement que l'attaquant peut lire, modifier ou même supprimer des données sur les nœuds RFID [40].
- **Attaque de gouffre (Sinkhole Attack**): Dans une attaque gouffre, un adversaire compromet un nœud à l'intérieur du réseau et effectue l'attaque en utilisant ce nœud. Le nœud compromis envoie les fausses informations de routage à ses nœuds voisins indiquant qu'il a le chemin de distance minimum vers la station de base, puis attire le trafic. Il peut alors modifier les données et également supprimer les paquets. Ce travail donne la technique simple pour identifier les nœuds dolines. Dans la technique proposée, lorsqu'un nœud envoie un paquet à son nœud voisin, il crée l'entrée des distances de saut et de l'ID dans sa base de données. Il calcule ensuite le nombre de sauts moyen à l'exception du nombre de sauts minimum et compare la valeur moyenne et la valeur minimale. Si cette valeur minimale est trop petite par rapport au nombre moyen de sauts, elle est vulnérable aux attaques de gouffre. [23]

- **L'homme au milieu de l'attaque (Man In the Middle Attack):** L'attaquant sur Internet intercepte la communication entre les deux nœuds. Ils obtiennent les informations sensibles par écoute clandestine.
- **Déni de service (Denial of Service):** Un attaquant inonde le réseau avec un trafic important afin que les services ne soient pas disponibles pour les utilisateurs auxquels il est destiné
- **Attaque d'informations de routage (Routing Information Attack):** Dans cette attaque, l'attaquant peut complexifier le réseau en usurpant, modifiant ou envoyant des informations de routage. Cela se traduit par l'autorisation ou la suppression de paquets, le transfert de données erronées ou le partitionnement du réseau.
- **Attaque Sybille (Sybil Attack) :** Dans cette attaque, un nœud malveillant prend les identités de plusieurs nœuds et agit comme eux. Par ex. dans le réseau de capteurs sans fil, le nœud unique du système de vote peut voter plusieurs fois [26].
- **Attaque de trou de ver (Wormhole attack):** La relocalisation des bits peut être effectuée à partir de l'emplacement d'origine des bits dans le réseau .Le mécanisme de relocalisation se fait à partir de ce canal de bits où il existe un lien à faible latence.
- **Bonjour attaque d'inondation (Hello flood attack):** Dans l'attaque hello flood, l'attaquant envoie des messages inutiles à partir d'un nœud et provoque un embouteillage et bloque le canal du réseau. Un seul nœud malveillant peut faire cela et provoquer le blocage de l'ensemble du réseau en créant un grand nombre de trafic.
- **Transmission sélective (Selective forwarding):** Dans le transfert sélectif, seul le nœud compromis peut transmettre des données à sa destination. L'attaquant sélectionne et restreint les nœuds pour atteindre son objectif malveillant et, par conséquent, certains nœuds ne peuvent pas transmettre le paquet de données [41]

II.3.3 Attaques des couches de traitement (Processing Layer Attacks)

La couche de traitement se compose de différents types de technologies telles que le stockage et le traitement des données. L'attaque cloud est le type d'attaque le plus important dans le système IoT et les menaces de sécurité dans cette couche qui rendent le réseau vulnérable sont analysées dans le tableau 3.

Nom de l'attaque	Effets	contre-mesures	description de la contre-mesure
Menaces de virtualisation	Endommager la ressource	Hyper Safe	Hyper Safe utilisé pour la protection des pages de mémoire contre les modifications
Ressources partagées	Un utilisateur non autorisé peut contrôler les ressources	Cryptage homomorphe	texte chiffré autorisé à être calculé immédiatement sans décryptage
Sécurité des applications	Le vol de données	Analyseurs d'applications Web	Découverte de diverses menaces présentes sur le front-end du web
Sécurité des données	fuite de données confidentielles sur le cloud	Redondance de fragmentation Diffusion	les données sur le cloud sont divisées et allouées à divers fragments pour le stockage dans les services
Sécurité de l'infrastructure sous-jacente	la couche inférieure reste non protégée	Redondance de fragmentation Diffusion	Les données divisent et allouent à différents fragments pour le stockage
Relations avec des tiers	fuite de données	Chiffrement	Dans le chiffrement, les données sont d'abord chiffrées puis envoyées dans le cloud

Tableau II. 3: Analyse de la couche de traitement.

- **Accès non autorisé (Unauthorized Access):** La couche de traitement fournit le stockage des données et diverses fonctionnalités dans la tâche de traitement des applications. Dans cette attaque, l'adversaire peut facilement accéder aux services du système de manière autorisant et en supprimant les données cruciales qui peuvent causer beaucoup de dommages au réseau IoT.
- **Initié malveillant (Malicious Insider):** Il s'agit d'une attaque d'initié dans laquelle l'attaquant de l'intérieur de l'organisation attaque en modifiant les données à cause de son propre but. Dans cette attaque, les données peuvent être facilement modifiées et extraites du but de l'utilisateur interne. [42]
- **Sécurité des applications (Application security**): Dans le contexte de la sécurité des applications, le logiciel en tant que service (SAAS) fournit des logiciels et des données disponibles sur le cloud via Internet. L'adversaire dans le système IoT peut facilement voler des données [41] et peut exploiter des activités malveillantes en utilisant Internet. Leurs problèmes de sécurité sont très différents des problèmes de sécurité réseau normaux. L'Open Web Application Security Project (OWASP) a identifié de nombreux services Web et problèmes de sécurité dans SAAS.

- **Sécurité des données (Data security):** La sécurité des données est assurée par diverses technologies de cryptage qui empêchent les menaces de vol de données. De plus, pour empêcher d'autres activités malveillantes de la part des utilisateurs malveillants, des pare-feu Anti Dos et des logiciels espions et malveillants à jour sont introduits. [26]
- **Sécurité de l'infrastructure sous-jacente (Underlying infrastructure security):** Dans Platform as a Service (PaaS), les développeurs ne peuvent pas accéder à la couche inférieure et la sécurité de cette couche est de la responsabilité des fournisseurs de services [43].
- **Relations avec des tiers (Third-party relationships):** Le PaaS peut également fournir de nombreux composants tiers comme les mushups. Il existe une combinaison de nombreuses sources de mushups, ce qui augmente les problèmes de sécurité des données et du réseau.
- **Menaces de virtualisation (Virtualization threats):** La sécurité de la machine virtuelle est très importante car les autres machines et l'apparition de tout dommage à la machine affecte l'autre. Dans cette couche, la virtualisation est très peu sûre face à de nombreux types d'attaques.
- **Ressources partagées (Shared Resources):** Le même partage et l'utilisation des ressources dans la machine virtuelle peuvent entraîner diverses menaces de sécurité dans le réseau IoT. L'adversaire contrôle toutes les ressources partagées entre les machines virtuelles en utilisant des canaux secrets. Le partage de données peut donc être menacé par le vol de données.

II.3.4 Attaques de la couche application (Software Layer Attacks)

Les attaques logicielles sont les principaux défis qui se posent dans le système IoT. Les attaques logicielles sont utilisées pour endommager les ressources du système en utilisant des virus et des attaques nuisibles tels que des chevaux de Troie, des vers, des logiciels espions, etc. qui peuvent violer les données confidentielles, altérer les données, endommager les appareils IoT et accéder à des informations utiles. Le tableau 4 décrit ses effete sur IoT.

Nom de l'attaque	Effets	contre-mesures	description des contre-mesure
Salles de virtualisation	Endiguer la ressource	Hyper Sûr	Hyper Safe utilisé pour la protection des pages de mémoire contre les modifications
Ressources partagées	Un utilisateur non autorisé peut contrôler les ressources	Cryptage homomorphe	le texte chiffré est autorisé à être calculé immédiatement sans décryptage
Sécurité des applications	Le vol de données	Analyseurs d'applications Web	Découverte de diverses menaces présentes sur le front-end du web
Sécurité des données	fuite de données confidentielles car les données sur le cloud	Diffusion par redondance de fragmentation	Les données sur le cloud sont divisées et allouées à divers fragments pour le stockage sur des serveurs
Sécurité de l'infrastructure sous-jacente	La couche inférieure reste non protégée	Diffusion par redondance de fragmentation	les données se divisent et sont allouées à différents fragments pour le stockage
Relations avec des tiers	Fuite de données	Chiffrement	Dans le chiffrement, les données sont d'abord chiffrées puis envoyées dans le cloud

Tableau II. 4: Analyse de la couche application.

- **Une attaque par phishing (Phishing Attack**): L'attaquant obtient les informations privées telles que le nom d'utilisateur, les mots de passe par usurpation d'e-mail et en utilisant de faux sites Web. [23].
- **Virus vers cheval de Troie spyware et aware (Virus, Worms, Trojan horse, Spyware and Aware):** Un adversaire peut endommager le système en utilisant un code malveillant. Ces codes se propagent par le biais de pièces jointes à des e-mails, en téléchargeant des fichiers sur Internet. Le ver a la capacité de se répliquer sans aucune action humaine. Nous pouvons utiliser un détecteur de vers, un antivirus, des pare-feu, un système de détection d'intrusion pour détecter le virus.
- **Scripts malveillants (Malicious Scripts):** En injectant un script malveillant, l'attaquant peut accéder au système
- **Déni de service (Denial of Service):** L'attaquant bloque les utilisateurs de la couche application en refusant les services.

II.3.5 Attaques de chiffrement (Encryption Attacks)

Dans le système IoT, ces types d'attaques sont entièrement utilisés pour briser la procédure des techniques de cryptage.

- **Attaque de cryptanalyse (Cryptanalysis Attack):** Le but de ce type d'attaque est de récupérer la clé de cryptage qui est utilisée pour casser le mécanisme de cryptage dans le système IoT. Les attaques de cryptanalyse permettent la possession de texte en clair. L'attaque par texte clair choisi, l'attaque par texte clair connu, l'attaque par texte chiffré uniquement et l'attaque par texte chiffré choisi sont quelques exemples d'attaque par cryptanalyse.
- **Attaque du canal latéral (Side channel Attack**): L'attaquant utilise les informations du canal latéral émises par les dispositifs de chiffrement. Ce n'est ni le texte en clair ni le texte chiffré, il contient des informations sur la puissance, le temps nécessaire pour effectuer l'opération, la fréquence des pannes, etc. L'attaquant utilise ces informations pour détecter la clé de chiffrement. [23]
- **L'homme au milieu des attaques (Man in the Middle Attacks**): Lorsque deux utilisateurs échangent la clé, l'attaquant intercepte la communication et obtient la clé [43]

II.4. Contre-mesures de différentes couches

Dans cette section contre-mesure des attaques mentionnées ci-dessus sont discutés.

II.4.1 Sécurité de la couche physique (Physical Layer Security)

La couche physique est la couche la plus basse du réseau IoT qui fournit différentes fonctionnalités de sécurité au matériel. La sécurité au niveau de la couche physique est abordée en quatre types différents, comme indiqué ci-dessous :

- **Conception physique sécurisée (Secure Physical Design**): Dans la couche physique, la plupart des menaces sont résolues en concevant des appareils physiquement sécurisés. La conception d'un tel composant comme une unité d'acquisition, des circuits de radiofréquence, etc. ne doit pas être modifiables et ne pas être de haute qualité. Dans WSN, la conception de l'antenne est physiquement sécurisée et a la capacité de communiquer sur de longues distances.
- **Authentification de l'appareil (Device authentication):** Lorsqu'un nouvel appareil physique entre dans le réseau IoT, avant d'envoyer et de recevoir des données, l'appareil doit s'authentifier [44]

- **Démarrage sécurisé (Secure Booting):** L'authenticité et l'originalité du logiciel peuvent être vérifiées en appliquant un algorithme de hachage cryptographique. Cet algorithme vérifie le logiciel sur les appareils par signature numérique [45].
- **Confidentialité des données (Data Confidentiality):** Dans la confidentialité des données, toutes les balises et les données de chaque appareil physique doivent être cryptées avant d'envoyer les données pour assurer la confidentialité [46].
- **Intégrité des données (Data integrity**): Pour éviter la trempe des données sensibles, la technique de détection d'erreurs est prévue au niveau de chaque dispositif physique. De meilleures techniques de détection d'erreurs peuvent être appliquées, telles que la méthode de hachage cryptographique WH, mais elles font référence à ce type de mécanisme qui a la capacité d'utiliser une faible puissance, comme les contrôles de redondance cyclique (CRC) et le bit de parité. [42].
- **La confidentialité des données (Data Privacy):** La fonction de cryptage symétrique et asymétrique comme DSA, RSA, BLOWFISH et DES, etc. garantit la confidentialité des données en empêchant l'attaquant d'accéder sans autorisation aux données essentielles lorsque les données sont envoyées à la destination. Ces algorithmes de chiffrement peuvent être facilement appliqués en raison de leur moindre consommation d'énergie
- **L'évaluation des risques (Risk Assessment):** La technique d'évaluation dynamique des risques assure la confidentialité des données et évite les failles de sécurité dans un réseau IoT [47].
- **Confidentialité des informations sensibles (Privacy of sensitive information):** La confidentialité des informations sensibles est le concept le plus crucial pour assurer la sécurité des données sur le système. Avec l'aide de la technique K-anonymity, il fournit un mécanisme permettant de masquer les informations sensibles sur le système, d'où l'anonymat de l'identité. obtenu en assurant la protection des informations telles qu'emplacement et identité, etc.
- **Anonymat (Anonymity) :** L'identification des nœuds et la dissimulation d'informations privées telles que l'adresse et l'emplacement des données sont très importantes pour la confidentialité. La technique Zero-Knowledge serait la meilleure solution pour l'anonymat mais elle a l'inconvénient d'avoir une grande puissance de traitement en raison d'un algorithme fort, elle ne peut pas être implémentée sur les appareils qui consomment moins d'énergie. L'anonymat K est donc la meilleure approche pour les appareils physiques à faible consommation d'énergie dans le réseau IoT [42].

- **Canal de sécurité IPSec (IPSec Security channel):** Le canal de sécurité IPSec a deux types de fonctionnalités sécurisées, le cryptage et l'authentification qui assure la sécurité. La trempe et l'écoute clandestine des nœuds peuvent être arrêtées par le cryptage qui garantit la confidentialité des données. Le récepteur peut identifier que l'expéditeur des données sur IP est faux ou réel.

II.4.2 Sécurité de la couche réseau (Network Layer Security)

La couche réseau est menacée par de nombreux types d'attaques. En raison du respect des nombreux canaux sans fil, l'attaquant peut facilement contrôler la communication entre les appareils. Le la sécurité de la couche réseau est divisée en quatre types qui sont décrit ci-dessous

- **Sécurité du routage (Routing security**): Dans de nombreuses applications, un routage sécurisé est essentiel pour le réseau de capteurs. En raison des protocoles de routage non sécurisés, différents algorithmes de routage sont appliqués pour sécuriser la confidentialité des données transférées vers divers nœuds de capteurs dans le système IoT [48].
- **Système de localisation GPS (GPS location system):** Le système GPS a rencontré l'attaque par usurpation de la couche réseau du système IoT. S. Daneshmand et al. décrire et mettre en œuvre la technique de localisation GPS qui est la meilleure solution proposée à ce jour.
- **Protocole de routage (Routing protocol):** Ad hoc On demand Multipath Distance Vector (AOMDV) est un protocole de routage qui a rencontré l'attaque wormhole. Amish et al. proposent cette technique en produisant des chemins multiples entre l'expéditeur et le destinataire à chaque découverte de routage. Dans cette technique, la table de routage est vérifiée par l'expéditeur pour savoir si, pour la communication à deux nœuds, la route est disponible ou non. Si le routage est disponible, il fournit des informations sur le routage plutôt qu'il transmet le paquet. [42].
- **Bonjour détection des inondations et prévention (Hello flood Détection cum Prevention):** Virendra et al. proposer une technique pour empêcher l'attaque hello flood dans IoT. Dans cette technique, un nœud envoie un message bonjour pour vérifier la force du signal si la force est similaire à celle de la portée radio, puis le récepteur accepte le message et des informations sur le routage sont envoyées au route [49].

- **Intégrité des données (Data Integrity):** Un mécanisme de hachage cryptographique est utilisé pour l'intégrité des données. Cette fonction permet de vérifier la transmission des données sur l'autre nœud. Lorsque la modification des données est prouvée, un processus de correction d'erreurs peut également être utilisé.

II.4.3 Sécurité de la couche de traitement (Processing Layer Security)

Il existe certains concepts de mesures de sécurité dans le traitement couche qui est discutée ci-dessous :

- **Analyseurs d'applications Web (Web application scanners**): son application utilise pour l'identification des différentes menaces qui est présent dans le front-end du web. D'autres applications de pare-feu Web détectent également les attaques d'attaquants potentiels.
- **Diffusion par redondance de fragmentation (FRS) (Fragmentation redundancy scattering (FRS)):** Dans FRS, les données essentielles sur le cloud sont divisées et allouées dans à divers fragments de stockage dans les serveurs. Le fragment a pas d'informations utiles sur les données donc risque de vol de données est minimisé dans ce scénario.
- **Cryptage homomorphe (Holomorphic encryption):** Cette technique est basée sur tout le mécanisme de chiffrement homomorphe. Dans cette technique, le texte chiffré est autorisé à être calculé immédiatement sans décryptage. Un calcul élevé nécessite pour la sécurité des données dans cette méthode.
- **Chiffrement (Encryption):** La technique de cryptage est utilisée pour assurer la confidentialité des données dans IoT. Les données sont d'abord cryptées puis envoyées dans le cloud. Le cryptage aide à surmonter les attaques par canal latéral. Il existe différents types de cryptage tel qu'Advanced Encryptions Standard, etc.
- **Hyper Sûr (Hyper Safe):** Hyper safe provides protection for the memory pages from being altered and also allows restriction of pointing index that changes monitored data onto the pointer indexes [50].

II.4.4 Sécurité de la couche application (Application Layer Security)

La catégorisation des mécanismes de sécurité en application couche est discuté ci-dessous:

- **Sécurité des données (Data security):** Pour sécuriser la confidentialité des données et la confidentialité de l'ensemble du système IoT, le cryptage, l'authentification et

l'intégrité sont les procédures les plus essentielles à ce niveau. Il évite tout accès non autorisé aux données et protège les données contre le piratage ou le vol.

- **Listes de contrôle d'accès (ACL) (Access Control Lists (ACLs)):** La mise en place des règles et permet la demande d'accès et de surveillance du réseau est la partie importante qui garantit la confidentialité du système et la confidentialité des données. ACL peut gérer en arrêtant ou en autorisant le trafic entrant ou sortant et surveille les demandes d'accès de nombreux utilisateurs dans le système IoT.
- **Détection d'intrusion (Intrusion Detection):** Le processus de détection d'intrusion fournit des solutions de sécurité à de nombreuses menaces en produisant une alarme lorsqu'une action incertaine est effectuée dans le système en raison du contrôle continu d'un journal de l'activité de l'intrus. La détection d'intrusion peut être effectuée par diverses techniques de détection telles que la détection d'anomalies dans l'exploration de données [45].
- **L'évaluation des risques (Risk Assessment):** L'évaluation des risques produit des approches de sécurité efficaces et améliore les architectures et la planification de la sécurité déjà existantes..
- **Pare-feu (Firewalls):** Lorsque le cryptage, l'authentification et le processus ACL n'ont pas réussi à bloquer l'utilisateur non autorisé, le pare-feu entre en action pour le blocage. Lorsqu'un mot de passe faible a été choisi, le processus de cryptage et d'authentification peut échouer. Dans le pare-feu, la filtration des paquets est effectuée, les paquets indésirables sont donc bloqués par ce processus. [42].
- **Anti-virus, Anti-spyware et Anti-adware (Anti-virus, Anti-spyware and Anti-adware):** Les logiciels qui assurent la sécurité tels que l'antivirus, l'anti-spyware et l'anti-adware sont essentiels pour la confidentialité, la fiabilité et l'intégrité du réseau IoT.

II.5. Conclusion

L'IoT a été considéré comme un sujet de recherche important ces dernières années où les objets physiques communiqueraient en utilisant diverses technologies de réseau. Le vaste avancement des services de IoT nécessite le mécanisme de sécurité authentique et factuel. Ce chapitre donne le fonctionnement des couches, puis aborde différentes failles de sécurité sur différentes couches de IoT (couche physique, couche réseau, couche de traitement et couche application). En outre, il présente les contre-mesures contre les menaces de sécurité de la prévention de tout dommage au réseau IoT. Comme IoT va être une partie essentielle de notre vie, des mesures doivent être prises pour assurer la sécurité et la confidentialité de l'utilisateur.

III.1. Introduction

La première étape pour concrétiser ce projet est la maquette initiale et fournir l'ensemble des moyens et capacités nécessaires à sa réalisation, qu'il s'agisse de moyens logiciels ou de moyens matérielles et même les moyens que sont les plateformes ou les applications

Dans ce chapitre, nous introduisons une maison intelligente et nous passerons en revue tous les moyens nécessaires à notre projet, qui est un exemple simple sur les maisons intelligentes, qui se divise en deux parties, des moyens matérielles tels que les microcontrôleurs et autres, ainsi que des moyens logiciels tels que les plateformes sur lesquels ces contrôleurs sont programmés et d'autres moyens intégrés au projet

III.2. Maison intelligent

III.2.1. Historique

Les premières applications domotiques sont apparues au début des années 1980. Né de la miniaturisation des systèmes électroniques et informatiques. Le développement de ces composants électroniques des produits ménagers s'améliorent tandis que les performances réduire les coûts énergétiques des équipements .Ce calendrier se concentre sur le matériel, cela signifie l'invention réelle de la maison Intelligent tel que nous le connaissons aujourd'hui

1901 - 1920 - Invention de l'électroménager - voire de l'électroménager Les appareils ne sont pas ce que nous considérons comme "intelligents", ils sont Un exploit incroyable réalisé au début du XXe siècle. Ces réalisations commencent par le premier Un aspirateur électrique de 1901. Un aspirateur électrique plus pratique a été inventé en 1907. Au cours des deux décennies suivantes, les réfrigérateurs, les sécheuses, Machine à laver, fer à repasser, grille-pain, etc.

1966 - 1967 - ECHO IV et ordinateur de cuisine - bien qu'il n'ait jamais L'ECHO IV disponible dans le commerce a été le premier appareil intelligent. cet appareil Smart peut calculer la liste de courses, contrôler la température de la maison et Allumez et éteignez l'appareil. L'ordinateur de cuisine développé un an plus tard, Peut stocker des recettes

1991 - Gérontechnologie - La gérontechnologie combine la médecine gériatrique et la technologie, Facilitez la vie des seniors. Les années 90 ont eu beaucoup de nouveautés recherche et technologie dans le domaine.

1998-début des années 2000: La Smart Home - La popularité de la maison La domotique ou la domotique a pris son essor au début des années 2000. Par conséquent, différentes technologies ont commencé à émerger. la maison intelligente est Du coup une option plus abordable et donc une technologie viable consommateur. Technologie domestique, réseau domestique et autres gadgets A commencé à apparaître dans les rayons des magasins.

III.2.2. Définition

C'est une maison avec des fonctions pour simplifier la vie des habitants chaque jour, pour réaliser des économies d'énergie et assurer un certain niveau de confort et sécurité. Il est en constante évolution et ouvert au monde numérique. Le niveau "intelligent" de votre maison dépendra du nombre de captures, Les exécuteurs et les règles que vous souhaitez installer. Il n'y a donc pas de maison intelligente mais la maison intelligente comporte plusieurs couches, de la gestion des fonctions de base (chauffage, Porté par de nombreux nouveaux produits Bénéficiez de fonctionnalités supplémentaires plus abordables haut de gamme.

III.2.3. Les avantages

Le principal avantage de la domotique est :

- d'améliorer la vie quotidienne à l'intérieur La maison, du point de vue du confort, de la sécurité et de la gestion de l'énergie.
- Ce type d'appareil vous simplifie la vie et maisons avec différentes scènes de la vie quotidienne.
- Il permet notamment d'éteindre tous les appareils électriques, de mettre régler l'ambiance lumineuse avec une alarme lorsque vous quittez la maison (ambiance lecture, ambiance détente en lumière tamisée), réveil le café est prêt à chauffer la maison, commencer à arroser automatiquement ou ouvrez les volets tous les matins.
- La domotique permet également d'économiser de l'énergie grâce à la gestion Chauffage, climatisation et éclairage automatiques et programmation appareils électroménagers pendant les heures creuses.
- Il a l'avantage d'une sécurité accrue grâce aux alarmes, aux systèmes ouverture automatique des portes (reconnaissance vocale, carte magnétique, etc.)
- Appel automatique si quelqu'un essaie de s'introduire dans la maison vous pouvez contacter le propriétaire ou la société de sécurité.

- Enfin, ces différentes technologies sont une aide précieuse aux personnes Dépend et désactive.

III.2.4. Les inconvenients

- Les prix sont beaucoup plus élevés, mais les factures d'énergie vont baisser. Il faut donc Inclus dans le budget initial.
- Le verrouillage proposé par certaines marques dans leurs produits ne permet pas avoir un logiciel ouvert.

III.3. Partie matérielle

III.3.1. Etude des microcontrôleurs

Un microcontrôleur (µc, uc, ou encore MCU en anglais) est un circuit intégré et compact, conçu pour régir une opération spécifique et dans un système intégré. Il comprend un processeur, une mémoire et des périphériques d'entrée et de sortie sur une seule carte ou une seule puce. Ces circuits sont utilisés dans les véhicules, les robots, les machines industrielles, les appareils médicaux, l'émetteurs-récepteurs radio mobiles, les distributeurs automatiques ou encore les appareils ménagers.[51]

III.3.1.1. Un microcontrôleur comporte entre autres [52]

- Un microprocesseur.
- Une mémoire vive (RAM).
- Une mémoire permanente (ROM).
- Interfaces d'E/S parallèles et séries (RS232, I2C, SPI…).
- Interfaces d'E/S analogiques.
- Registres « Timers » pour la gestion du temps et d'évènements.
- Les microcontrôleurs 4 bits sont principalement utilisés pour des tâches simples. De tels microcontrôleurs sont utilisés par exemple dans les appareils électroménagers grand public
- Les microcontrôleurs 8 bits peuvent répondre à des exigences plus élevées.
- Microcontrôleur 32 bits pour le contrôle ou le contrôle de la machine Quand les contraintes temps réel sont sévères ou les algorithmes de contrôle Une forte puissance de calcul est nécessaire.

III.3.1.2. Les avantage d'un microcontrôleur

L'utilisation d'un microcontrôleur présente plusieurs avantages par rapport à un microprocesseur, parmi lesquels on peut citer :

- Le microcontrôleur contribue à réduire les coûts à plusieurs niveaux, car il est moins cher que les autres composants qu`il remplace.
- Les outils de développement sont, en général, téléchargeable gratuitement sur le WEB.
- Une diminution évidente de l'encombrement matériel et de circuit imprimé.
- Une plus grande fiabilité du système, car le nombre des composants sera plus réduit, donc un nombre de connexion composants/supports ou composants/circuits plus réduit.
- Le jeu d'instruction réduit est souple, puissant et facile à maîtriser.
- Les versions avec mémoire flash présentent une souplesse d'utilisation et des avantages pratiques indéniables.

Nous montrons ci-dessous certains des modèles de microcontrôleurs les plus populaires en raison de leur flexibilité, de leurs puissants outils de développement ou de leur documentation complète disponible sur le Web.

III.3.1.3. Arduino

Arduino est une plate-forme électronique open source basée sur du matériel et des logiciels faciles à utiliser. Les cartes Arduino sont capables de lire les entrées - la lumière sur un capteur, un doigt sur un bouton ou un message Twitter - et de les transformer en une sortie - en activant un moteur, en allumant une LED, en publiant quelque chose en ligne. Vous pouvez dire à votre carte quoi faire en envoyant un ensemble d'instructions au microcontrôleur sur la carte. Pour ce faire, nous utilisons le langage de programmation Arduino (basé sur le câblage) et le logiciel Arduino (IDE), basé sur le traitement. [53]

Au fil des ans, Arduino a été le cerveau de milliers de projets, des objets du quotidien aux instruments scientifiques complexes. Une communauté mondiale de créateurs - étudiants, amateurs, artistes, programmeurs et professionnels - s'est réunie autour de cette plate-forme open source, leurs contributions se sont ajoutées à une quantité incroyable de connaissances accessibles qui peuvent être d'une grande aide pour les novices comme pour les experts. [53]

Figure III. 1: Arduino Uno Rev3

III.3.1.3.1. Les avantages

- **Peu coûteux :** Les cartes Arduino sont relativement peu coûteuses par rapport aux autres plates-formes de microcontrôleur. La version la moins chère du module Arduino peut être assemblée à la main, et même les modules Arduino pré-assemblés coûtent moins de 2400 DA [53]
- **Multiplateforme :** Le logiciel Arduino (IDE) fonctionne sur les systèmes d'exploitation Windows, Macintosh OSX et Linux. La plupart des systèmes de microcontrôleurs sont limités à Windows. [53]
- **Environnement de programmation simple et clair** : Le logiciel Arduino (IDE) est facile à utiliser pour les débutants, mais suffisamment flexible pour que les utilisateurs avancés en profitent également. Pour les enseignants, il est basé sur l'environnement de programmation de traitement, de sorte que les étudiants qui apprennent à programmer dans cet environnement seront familiarisés avec le fonctionnement de l'IDE Arduino. [53]
- **Logiciel open source et extensible :** Le logiciel Arduino est publié sous forme d'outils open source, disponibles pour extension par des programmeurs expérimentés. Le langage peut être étendu via les bibliothèques C++, et les personnes souhaitant comprendre les détails techniques peuvent passer d'Arduino au langage de

programmation AVR C sur lequel il est basé. De même, vous pouvez ajouter du code AVR-C directement dans vos programmes Arduino si vous le souhaitez. [53]

- **Matériel open source et extensible :** Les plans des cartes Arduino sont publiés sous une licence Créative Commons, afin que les concepteurs de circuits expérimentés puissent créer leur propre version du module, l'étendre et l'améliorer. Même les utilisateurs relativement inexpérimentés peuvent créer la version maquette du module afin de comprendre son fonctionnement et d'économiser de l'argent. [53]

III.3.1.3.2. Inconvenient

- **Basique :** pas de composants Ethernet, Bluetooth ou WIFI.
- **Processeur ATMEGA lent.**
- **Mémoire et stockage limités.**

III.3.1.4. NodeMcu

Le NodeMCU (Node MicroController Unit) est un environnement de développement logiciel et matériel open source qui est construit autour d'un système sur puce (SoC) très peu coûteux appelé ESP8266. L'ESP8266, conçu et fabriqué par Espressif Systems, contient tous les éléments cruciaux de l'ordinateur moderne : CPU, RAM, mise en réseau (wifi), et même un système d'exploitation et un SDK modernes. Lorsqu'elle est achetée en gros, la puce ESP8266 ne coûte que 2 USD pièce. Cela en fait un excellent choix pour les projets IoT de toutes sortes.

Grâce à ses broches, nous pouvons lire des entrées - lumière sur un capteur, un doigt sur un bouton ou un message Twitter - et les transformer en une sortie - activer un moteur, allumer une LED, publier quelque chose en ligne. Il a également des capacités Wi-Fi, nous pouvons donc le contrôler sans fil et le faire fonctionner facilement sur une installation à distance ! Nous pouvons dire à notre carte quoi faire en envoyant un ensemble d'instructions au microcontrôleur sur la carte. Pour ce faire, nous pouvons utiliser le logiciel Arduino (IDE). [54]

III.3.1.4.1. Les Avantages

- **Matériel Open source et extensible :** les NodeMCU les plus trouvés sur le marché viennent de chez Amica,DOIT ou Lolin et D1 mini / Wemos parmi bien d'autres et ils ne ressemblent pas obligatoirement a l'original.
- **Bas prix :** Les couts différent d'un modèles a l'autre du à leurs spécifications techniques mais ils restent néanmoins assez bas.
- **Facilité de programmation :** Programmer en Lua via L'IDE Arduino avec un grand nombre de bibliothèques déjà disponibles pour créer vos firmware.
- **Wifi inclus.**
- **Port microUSB inclus.**

III.3.1.5. Raspberry Pi

Le Raspberry Pi est le plus avancé. En termes simples, il s'agit d'un ordinateur entier sur un tableau de la taille d'une carte de crédit. Branchez un moniteur, un clavier et une carte MicroSD avec un système d'exploitation dessus, et vous avez un bon ordinateur.

Figure III. 2: Raspberry Pi 4 Model B

Maintenant, évidemment, il ne va pas rivaliser avec votre ordinateur de tous les jours. Il a un rôle particulier, qui, en réalité, est assez diversifié.de nos jours, les RasPis exécutent tout, des distributeurs automatiques aux tableaux de bord de voiture. Tout comme les contrôleurs précédents, vous pouvez construire tout ce que vous voulez, sauf que vous contrôlez beaucoup plus la façon dont vous faites les choses. de plus, vous pouvez coder dans à peu près n'importe quelle langue que vous préférez. Encore une fois pour les débutants, je suggérerais Python car c'est un excellent langage non seulement pour apprendre mais aussi pour utiliser le GPIO sur le Pi au maximum. Comme il s'agit également d'un ordinateur à part entière, les gens en ont fait fonctionner des serveurs

entiers. Je l'ai utilisé comme serveur de sauvegarde, comme une télévision intelligente, un miroir intelligent, pour construire un prototype de voiture autonome et comme ordinateur de sauvegarde. [55]

III.3.1.6. Choix du microcontrôleur

Le choix du microcontrôleur dépend de nombreux facteurs. Votre niveau de confort avec leurs capacités de travail ou de codage ou selon les exigences de votre projet. En d'autres termes : si vous voulez apprendre l'électronique à partir de zéro, vous devriez vous procurer un Arduino. Si vous devez réaliser un projet nécessitant beaucoup de puissance, utilisez un Raspberry Pi. Si votre projet est connecté à Internet de quelque manière que ce soit, veuillez utiliser NodeMCU.

Nous résumons dans ce tableau une comparaison technique de quelques cartes programmables disponible sur notre marché [56] :

Nom de la carte	**Arduino UNO**	**Arduino Méga**	**NodeMcu ESP8266**	**NodeMcu ESP32**	**Raspberry Pi B+**
Naissance	2005	2010	2014	**2016**	2016
Prix (DA)	2400	4500	1800	**3000**	12000
Processeur	ATMEGA 328	ATMEGA 2560	Xtensa L106 Single-Core	**Xtensa Lx6 Dual-Core**	Broadcom BCM2837
Fmax	16 Mhz	20 Mhz	160 Mhz	**240 Mhz**	1,2 Ghz
ROM	2 KB	256 KB	512 KB UP TO 4 MB	**4 MB UP TO 16 MB**	MicroSD
RAM	32 KB	8 KB	160 KB	**512 KB**	512 MB
EEPROM	1 KB	2 KB	1 KB	**1 KB**	MicroSD
E/S Didital	14	42	16	**23**	40
E/S Analog	6	16	1	**18**	0
WiFi	NON	NON	OUI	**OUI**	OUI

Tableau III. 1: Etude comparative de quelques modèles de microcontrôleurs

Sur la base d'un examen des caractéristiques techniques des modules ci-dessus, et sur la base de notre choix du système à mettre en œuvre, en tenant compte de l'abordabilité et de la disponibilité sur le marché local ; notre choix s'est porté sur le modèle NodeMCU ESP8266, dont nous discuterons dans plus en détail ci-dessous analyser:

III.3.2. Le microcontrôleur ESP8266

Espressif Systems (une société de semi-conducteurs basée à Shanghai) publié en 2014, un joli petit microcontrôleur 32 bits compatible WiFi, le ESP8266, permettant d'établir des connexions TCP/IP, en mode client/serveur HTTP à un prix incroyable! pour moins de 1800 DA US.

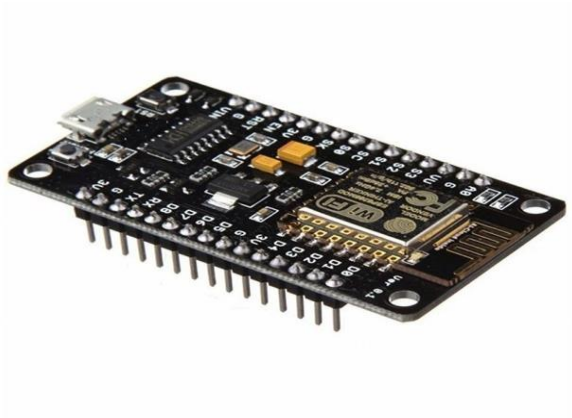

Figure III. 3: Module ESP8266 sur NodeMCU

Il ya plus de 12 versions de modules qui ont été construits a partir de ce composant. Chaque version est identifiée par une nomenclature sous la forme : ESP-01 ,ESP-02 ou ESP-12E…La puce quant a elle ,est fabriquée par une société tierce : AI-Thinker.

Le NodeMCU est arrivé quelques mois après le module ESP8260, qui est basé sur le SoC Wi-Fi ESP8266, l'ESP-12E d'Espressif. Le terme "NodeMCU" désigne par défaut le firmware qui permet de programmer le microcontrôleur en Lua, et non le kit de développement. Notez que vous pouvez toujours le programmer dans l'IDE Arduino.[57]

III.3.2.1. Principales caractéristiques de l'ESP8266

Les principales caractéristiques sont [52] :

- Processeur RISC 32bits cadencé à 80Mhz (par défaut) ou à 160 Mhz.
- 64 Ko de RAM pour les instructions et 96 Ko pour les données.
- Mémoire flash externe QSPI entre 512 KB et 4MB selon les modèles.
- Puce Wifi 2.4 GHz (802.11 b/g/n) avec antenne intégré.
- WEP or WPA/WPA2 authentication, or open networks.
- 16 Entrées/sorties numériques GPIO.
- PWM / ADC 10bits (variante 12E).
- UART / I2C / I2S / SPI.
- Alimentation en 3,3V.
- Consommation : entre 60mA et 215mA en fonctionnement normal, quelques dizaines de µA en veille

III.3.2.2. Brochage du NodeMCU ESP8266

Le NodeMCU ESP8266 possède un total de 30 broches qui nous permettent de le connecter à d'autres périphériques et de prendre en charge des fonctions telles que PWM, I2C, SPI et UART. **[57]**

Remarque : Pour une raison inconnue, les numéros de broches de la carte NodeMCU ne correspondent pas à ceux de l'ESP8266, ils ne correspondent donc pas à ceux de l'IDE Arduino lors de la programmation. Le schéma suivant montre la correspondance entre les noms de port indiqués sur la carte, les GPIO et la fonction spécifique associée à chaque port

:

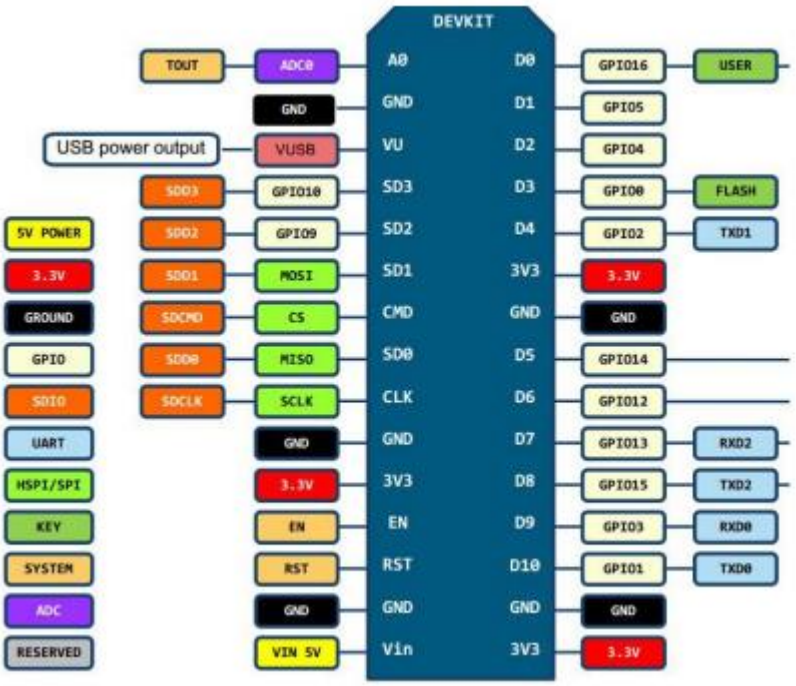

Figure III. 4: Correspondance des broches du NodeMCU ESP8266-Lolin

III.3.2.3. Architecture interne d'un ESP8266

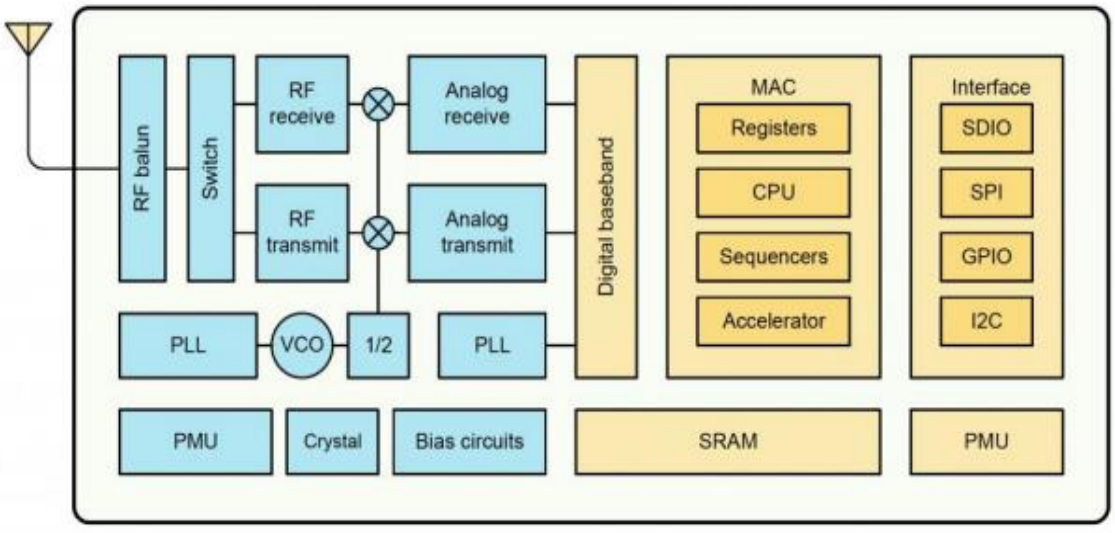

Figure III. 5: Schéma bloc représentant l'architecture interne de l'ESP8266.[52]

- **L'architecture de l'ESP8266 est composée de deux parties [52] :**

- **Partie RF ou Radio fréquence (couleur bleue dans la figure II.3)** : Cette partie permet de gérer la communication entre deux appareils par ondes radio, elle est Se compose principalement d'un émetteur/récepteur radio, de deux synthétiseurs de fréquence (PLL) et l'unité de gestion de l'alimentation (PMU).

❖ **Partie logique (couleur jaune dans la figure II.3) :** Elle contient tous les éléments d'une structure à base de microprocesseur :

- **Unité de calcul** : interprète les instructions et traite les données du programme pour La vitesse définie par la fréquence d'horloge (généralement du quartz).
- **Unité de contrôle :** Le fonctionnement du système de commande et de contrôle qui permet Optimiser la séquence de transfert de base pendant et entre la gestion Traitement des instructions.
- **Random Access Memory ou RAM :** est un type de mémoire volatile. il est utilisé pour le stockage Données temporaires. L'ESP8266 utilise un type de RAM dit "statique" ou SRAM, qui utilise des bascules pour stocker des données, contrairement à la mémoire Dynamique, il n'a pas besoin de rafraîchir périodiquement son contenu.
- **Mémoire FlashROM :** Fournit un stockage de programme ou une mémoire mettre en place. Il peut conserver ses données même lorsque le microcontrôleur n'est pas alimenté.
- **Registres temporaires :** ils garantissent que la valeur souhaitée est stockée Opérations unitaires de calcul
- **Port ou GPIO :** Assurez la connexion avec l'environnement externe.
- **Interface série :** permet au microcontrôleur de communiquer avec d'autres systèmes Basé sur un microprocesseur. Le format des données envoyées ou reçues est une série temporelle (sur un seul bit) de valeurs d'image binaires pour un mot.

Il ya deux Types de liaison série : synchrone et asynchrone.

- Liaison série synchrone : Dans ce dispositif la transmission est synchronisée par un signal d'horloge émis par l'unité maître.
- Liaison série asynchrone : Ce dispositif ne possède pas de signal d'horloge de synchronisation. Les unités en liaison possèdent chacune une horloge interne cadencée à la même fréquence.

- **Modules annexes :** ils représentent toutes les fonctions annexes (timers, comparateurs, convertisseurs analogiques/numériques…).

III.3.3. Capteur de température LM35

La série LM35 sont des dispositifs de température à circuit intégré de précision avec une tension de sortie linéairement proportionnelle à la température centigrade. Le dispositif LM35 présente un avantage par rapport aux capteurs de température linéaires calibrés en Kelvin, car l'utilisateur n'est pas obligé de soustraire une grande tension constante de la sortie

pour obtenir une mise à l'échelle centigrade pratique. L'appareil LM35 ne nécessite aucun étalonnage ou ajustement externe pour fournir une précisions de ±¼°C à température ambiante et de ±¾°C sur une plage de température complète de −55°C à 150°C. Un coût inférieur est assuré par le rognage et l'étalonnage au niveau de la tranche. L'impédance de sortie faible, la sortie linéaire et l'étalonnage inhérent précis de l'appareil LM35 rend l'interfaçage avec les circuits de lecture ou de contrôle particulièrement facile. L'appareil est utilisé avec des alimentations simples ou avec des alimentations positives et négatives. Comme le dispositif LM35 ne consomme que 60 μA de l'alimentation, il a un très faible auto-échauffement de moins de 0,1°C en air calme. Le dispositif LM35 est conçu pour fonctionner sur une plage de températures de -55 °C à 150 °C, tandis que le dispositif LM35C est conçu pour une plage de -40 °C à 110 °C (-10 ° avec une précision améliorée). Les appareils de la série LM35 sont disponibles emballés dans des boîtiers de transistor TO hermétiques, tandis que les dispositifs LM35C, LM35CA et LM35D sont disponibles dans le boîtier de transistor TO-92 en plastique. Le dispositif LM35D est disponible dans un boîtier à 8 dérivations petit boîtier à montage en surface et un boîtier TO-220 en plastique [58]

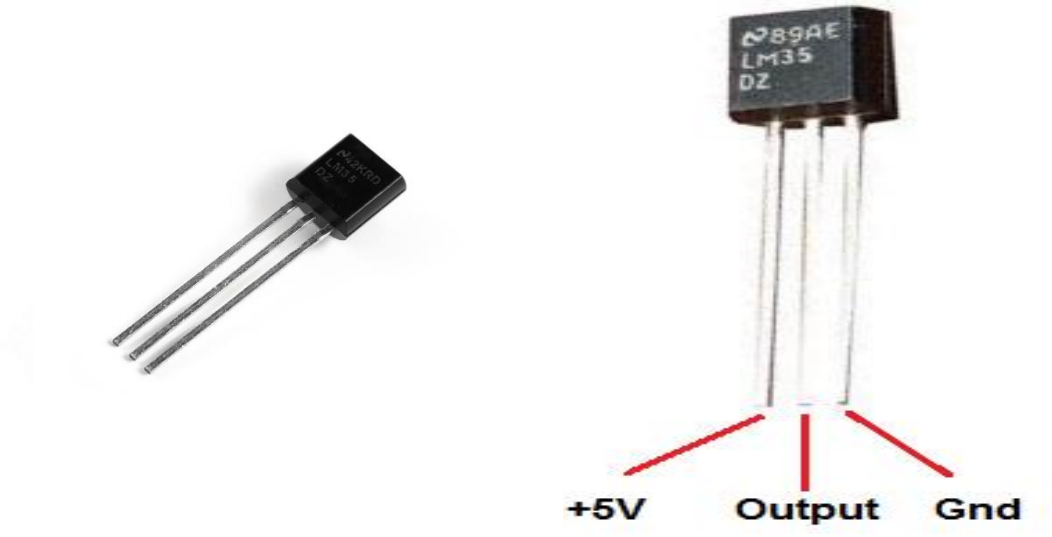

Figure III. 6: Capteur LM35.

III.3.3.1. Les Caractéristiques

Les caractéristiques sont [58] :

- Calibré directement en Celsius (Centigrade)
- Facteur d'échelle linéaire + 10 mV/°C
- Précision garantie de 0,5 °C (à 25 °C)
- Évalué pour une plage complète de −55 °C à 150 °C

- Convient aux applications à distance
- Faible coût grâce à la coupe au niveau de la plaquette
- Fonctionne de 4 V à 30 V
- Consommation de courant inférieure à 60 μA
- Faible auto-échauffement, 0,08 °C dans l'air calme
- Non-linéarité uniquement ±¼ °C typique
- Sortie à faible impédance, 0,1 Ω pour une charge de 1 mA

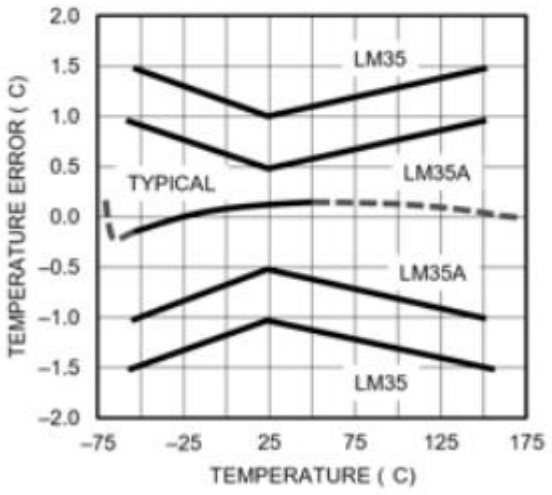

Figure III. 7: Précision des différentes versions LM35

❖ Nous avons choisi ce capteur pour les raisons suivantes :

- Simplicité d'utilisation.
- Il ne nécessite aucun étalonnage externe.
- Précisions typique ± 1°C dans la plage de mesure -55 °C à +150°C.
- Peu coûteux.
- Disponible sur le marché.

III.3.4. Led

Une diode électroluminescente est un dispositif optoélectronique qui émet de la lumière lorsqu'un courant électrique le traverse. Les diodes électroluminescentes permettent au courant de circuler dans une seule direction et produisent un rayonnement monochromatique ou polychromatique incohérent par conversion d'énergie électrique lorsque le courant passe.

Remarque : Nous avons choisi les led comme exemple de fonctionnement des lampe.

III.3.5. Le moteur

Un moteur à courant continu est un actionneur électromécanique largement utilisé, notamment dans les applications à vitesse variable. Les principaux avantages des moteurs à courant continu sont Dans leur simple adaptation à des dispositifs capables de régler ou de modifier leur vitesse, leur couple et leur sens de rotation. Un moteur à courant continu se compose d'un stator et d'un rotor. [52]

- Le stator à l'origine du cycle de flux magnétique longitudinal fixe, produit par des bobinages statiques (bobinages) ou des aimants permanents ; à l'arrière du stator se trouvent la partie porte-balais et les balais qui assurent le contact électrique avec le rotor. On l'appelle aussi inducteur.
- Le rotor est constitué d'un ensemble de bobines reliées à un collecteur tournant. Le collecteur tournant peut inverser la polarité du champ magnétique produit par le stator avant qu'il ne soit en phase avec le champ magnétique produit par le rotor. Grâce à cette disposition, le rotor et le champ magnétique statique sont toujours orthogonaux, entraînant la rotation du rotor. L'enroulement du rotor est également appelé enroulement d'induit, ou plus communément l'induit.

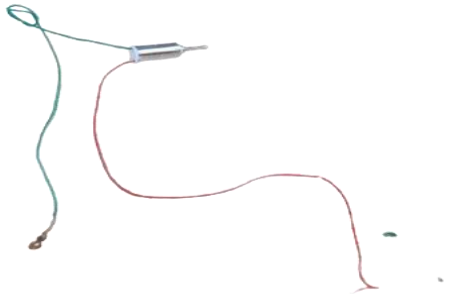

Figure III. 8: le micro moteur

Remarque : Nous avons choisi le moteur comme exemple de fonctionnement du ventilateur

III.4. Partie logicielle

III.4.1. Arduino IDE

Le logiciel de programmation du module Arduino est une application Java, gratuite et multiplateforme, qui agit comme un éditeur de code et un compilateur, et peut transférer des firmwares et des programmes via le port série (RS-232, Bluetooth ou USB, selon le module). Il est également possible d'utiliser sans l'interface Arduino, de compiler et de télécharger des

programmes via l'interface de ligne de commande. Le langage de programmation utilisé est C++, compilé avec avr-g++, Et lien vers la bibliothèque de développement Arduino, permettant d'utiliser la carte et ses entrées/sorties. L'implémentation de ce langage standard permet à toute personne familiarisée avec C ou C++ de développer facilement des programmes sur la plate-forme Arduino. Le logiciel Arduino est un environnement de développement (IDE) open source gratuite sous licence GPL. [57]

Figure III. 9: Arduino IDE

III.4.2. Google firebase

Firebase est un ensemble de services d'hébergement pour n'importe quel type d'application (Android, iOS, Javascript, Node.js, Java, Unity, PHP, C++ …). Il propose d'héberger en NoSQL et en temps réel des bases de données, du contenu, de l'authentification sociale (Google, Facebook, Twitter et GitHub), et des notifications, ou encore des services, tel que par exemple un serveur de communication temps réel. Lancé en 2011 sous le nom d'envolve, par Andrew Lee et par James Templin, le service est racheté par Google en octobre 2014. Il appartient aujourd'hui à la maison mère de Google : Alphabet.

Figure III. 10: logo de Google firebase

III.4.2.1. Les applications de développement de google firebase

Les applications de développement de google firebase sont [59] :

- **La suite d'émulateurs locaux Firebase**

Firebase Local Emulator Kit est un ensemble d'outils avancés pour les développeurs qui souhaitent créer et tester des applications localement à l'aide de Cloud Firestore, Realtime Database, Cloud Storage, Authentication, Cloud Functions, Pub/Sub, Firebase Hosting et Firebase Extensions. Il fournit une interface utilisateur riche pour vous aider à démarrer et à prototyper rapidement.

L'utilisation de Local Emulator Suite pour le développement local peut être un bon choix pour vos workflows de prototypage, de développement et d'intégration continue.

- **Cloud firebase**

Cloud Firestore est une base de données flexible et évolutive pour le développement mobile, Web et serveur avec Firebase et Google Cloud. Comme la base de données en temps réel Firebase, elle synchronise vos données entre les applications clientes via un écouteur en temps réel et fournit une prise en charge hors ligne pour les mobiles et le Web, afin que vous puissiez créer des applications réactives indépendamment de la latence du réseau ou de la connectivité Internet. Cloud Firestore offre également une intégration transparente avec d'autres produits Firebase et Google Cloud, y compris Cloud Fonctions.

❖ **Authentification Firebase**

La plupart des applications ont besoin de connaître l'identité de l'utilisateur. Connaissant l'identité de l'utilisateur, les applications peuvent enregistrer en toute sécurité les données de l'utilisateur dans le cloud et offrir la même expérience personnalisée sur tous les appareils des utilisateurs. Firebase Authentication fournit des services backend, un SDK facile à utiliser et des bibliothèques d'interface utilisateur prêtes à l'emploi pour authentifier les utilisateurs de votre application. Il prend en charge l'authentification à l'aide de mots de passe, de numéros de téléphone, de fournisseurs d'identité fédérés populaires tels que Google, Facebook, Twitter, etc. Firebase Authentication est étroitement intégré à d'autres services Firebase et repose sur des normes industrielles telles que OAuth 2.0 et OpenID Connect, de sorte qu'il peut facilement s'intégrer à votre backend personnalisé.

❖ **Base de données en temps réel Firebase**

tockez et synchronisez les données avec notre base de données cloud NoSQL. Les données sont synchronisées en temps réel sur tous les clients et restent disponibles lorsque votre application est hors ligne.

❖ **Stockage en nuage pour Firebase**

Cloud Storage pour Firebase est conçu pour les développeurs d'applications qui ont besoin de stocker et de diffuser du contenu généré par l'utilisateur, tel que des photos ou des vidéos.

Cloud Storage pour Firebase est un service de stockage d'objets puissant, simple et économique conçu pour l'échelle de Google. Le SDK Firebase pour Cloud Storage ajoute la sécurité Google aux importations et téléchargements de fichiers de votre application Firebase, quelle que soit la qualité du réseau.

Vous pouvez utiliser notre SDK pour stocker des images, de l'audio, de la vidéo ou tout autre contenu généré par l'utilisateur. Sur le serveur, vous pouvez accéder aux mêmes fichiers à l'aide de l'API Google Cloud Storage.

❖ **Apprentissage automatique Firebase**

L'utilisation de l'apprentissage automatique dans les applications pour résoudre des problèmes réels. Firebase Machine Learning est un SDK mobile qui apporte l'expertise de Google en matière d'apprentissage automatique aux applications Android et Apple dans un package puissant et facile à utiliser. Pour débuter dans l'apprentissage automatique, on peut

réaliser ce qu'on veut avec seulement quelques lignes de code. On n'a pas besoin de connaissances approfondies des réseaux de neurones ou de l'optimisation des modèles pour commencer. D'autre part, si on est un développeur ML expérimenté, Firebase ML fournit des API pratiques pour nous aider à utiliser des modèles TensorFlow Lite personnalisés dans des applications mobiles.

- **Hébergement Firebase**

Firebase Hosting fournit un hébergement rapide et sécurisé pour nos applications Web, notre contenu statique et dynamique et nos microservices. Firebase Hosting est un hébergement de contenu Web de qualité production pour les développeurs. Avec une seule commande, vous pouvez rapidement déployer des applications Web et diffuser du contenu statique et dynamique via un CDN (Content Delivery Network) mondial. nous pouvons également combiner Firebase Hosting avec Cloud Functions ou Cloud Run pour créer et héberger des microservices sur Firebase.

- **Fonctions cloud pour Firebase**

Cloud Functions for Firebase est une infrastructure sans serveur qui nous permet d'exécuter automatiquement du code backend en réponse aux événements déclenchés par les fonctions Firebase et les requêtes HTTPS. Notre code JavaScript ou TypeScript est stocké dans Google Cloud et s'exécute dans un environnement hébergé. Pas besoin de gérer et de faire évoluer notre propre serveur. Nous utilisons déjà Cloud Functions dans Google Cloud ? En savoir plus sur la façon dont Firebase s'intègre.

- **Règles de sécurité Firebase**

Protégeons nos données dans Cloud Firestore, Firebase Realtime Database et Cloud Storage grâce à notre politique de sécurité Firebase flexible et évolutive.

Les règles de sécurité de Firebase se situent entre nos données et les utilisateurs malveillants. Nous pouvons écrire des règles simples ou complexes pour protéger nos données d'application au niveau de granularité requis par une application spécifique.

Les politiques de sécurité Firebase exploitent un langage de configuration extensible et flexible pour définir les données auxquelles nos utilisateurs peuvent accéder pour une utilisation avec Realtime Database, Cloud Firestore et Cloud Storage. Les règles de base de données en temps réel Firebase utilisent JSON dans les définitions de règles, tandis que les règles de sécurité Cloud Firestore et les règles de sécurité Firebase pour Cloud Storage

utilisent un langage unique conçu pour s'adapter aux cadres spécifiques à l'utilisateur et aux règles plus complexes.

❖ **Vérification de l'application Firebase**

App Check aide à protéger nos ressources backend contre les abus, tels que la fraude à la facturation et le phishing. Il fonctionne avec les services Firebase et votre propre backend pour assurer la sécurité de nos ressources. Avec App Check, l'appareil exécutant notre application utilise un fournisseur d'attestation d'application ou d'appareil qui certifie l'un ou les deux des éléments suivants : La demande provient de notre application authentique réclamé à partir d'un appareil réel et non altéré cette preuve est jointe à chaque demande que notre application adresse aux ressources backend de Firebase.

❖ **Extensions Firebase**

Les extensions Firebase nous aident à déployer rapidement des fonctionnalités dans notre application avec des solutions prépackagées. Une fois installée, l'extension Firebase exécute une tâche ou un ensemble de tâches spécifiques en réponse aux requêtes HTTPS, aux événements Cloud Scheduler ou aux événements déclencheurs d'autres produits Firebase tels que Cloud Firestore ou Firebase Cloud Messaging.

Nous avons sélectionné parmi ces produits base de données en temps réel firebase pour deux raisons

- Nos données sont très sécurisées et protégées.
- Les données sont synchronisées en temps réel.

III.4.3. Adalo

Adalo est un outil de développement sans code qui nous permet de créer des sites Web ou des applications mobiles iOS ou Android sans écrire de code. Découvrez Adalo Solutions. **[60]**

Adalo est une solution pour créer des applications mobiles et web sans coder. Cet outil de développement no-code permet de réaliser des applications **[60]** :

- De contenu ;
- De type boutique en ligne ;
- De type réseaux sociaux ;
- De réservation ;
- De collaboration en entreprise ;

- De suivi de performance.

Figure III. 11: Logo de Adalo.

III.4.3.1 les fonctionnalités d'Adalo

Les principales fonctionnalités d'Adalo sont :

- La création du design de l'appli ;
- La création de la base de données ;
- L'intégration d'un API ;
- La possibilité de publier son appli en version ios et Android.

III.4.3.2. Fonctionnement d'Adalo

Se voulant très simple d'utilisation, Adalo propose deux façons de développer son application:

- Utiliser un template d'appli qu'il faut simplement éditer bâtir l'appli de A à Z en rajoutant un à un tous les éléments souhaités (textes, boutons, illustrations…).

- Adalo utilise le système de "drag and drop" : il suffit de glisser-déposer les différents éléments que l'on souhaite ajouter à son appli.

III.4.4. Google Sheets

Google Sheets est un tableur inclus dans la suite Web gratuite Google Docs Editors proposée par Google. Le service comprend également : Google Docs, Google Slides, Google Drawings, Google Forms, Google Sites et Google Keep. Google Sheets est disponible en tant qu'application Web, application mobile pour : Android, iOS, Microsoft Windows, BlackBerry OS et en tant qu'application de bureau sur Chrome OS de Google. L'application est compatible avec les formats de fichiers Microsoft Excel. L'application permet aux utilisateurs de créer et de modifier des fichiers en ligne tout en collaborant avec d'autres utilisateurs en temps réel. Les modifications sont suivies par l'utilisateur avec un historique des révisions présentant les modifications. La position d'un éditeur est mise en évidence avec

une couleur et un curseur spécifique à l'éditeur et un système d'autorisations régule ce que les utilisateurs peuvent faire. Les mises à jour ont introduit des fonctionnalités utilisant l'apprentissage automatique, notamment "Explorer", offrant des réponses basées sur des questions en langage naturel dans une feuille de calcul.

Figure III. 12: Logo de google Sheets.

III.4.4.1. Les avantages de Google Sheets

Les avantages de Google Sheets sont [61] :

- Collaborez sur les données, où que vous soyez
- Bénéficiez plus rapidement d'informations pertinentes grâce aux fonctionnalités intelligentes intégrées
- Connectez-vous facilement à vos autres applications google
- Étendez les fonctionnalités collaboratives et intelligentes aux fichiers Excel

Nous avons choisi google Sheets dans notre projet comme intermédiaire avec lequel nous connectons Google firebase avec adalo.

III.4.5. Javascript

JavaScript est un langage de script intégré dans les documents HTML. Historiquement, c'était même le premier langage de script pour le web. Ce langage est un langage de programmation qui améliore le langage HTML en permettant l'exécution de commandes côté client, c'est-à-dire au niveau du navigateur plutôt qu'au niveau du serveur Web. [62]

III.5. Conclusion

Dans ce chapitre nous avons donné un aperçu des moyens que nous utiliserons lors de la réalisation du projet, qui à son divisé en deux parties :

- Partie matérielle, qui sont des appareils électroniques et des capteurs …ect.
- Partie logicielle qui étaient représentés dans les plates-formes, les applications et les services

Les services fournis par des entreprises pionnier dans le domaine de la technologie, telles que Google, nous ont facilité la pose des bases de la construction du projet, ainsi que de sa réalisation, et nous ont fait gagner beaucoup de temps, en plus de la haute qualité et protection qui caractérisent ses services, et c'est ce que nous cherchons à atteindre dans notre projet

IV.1 Introduction

Après une étude approfondie des concepts théoriques des technique a implémenter et après la modélisation des fonctionnalités du système nous nous intéressons dans ce chapitre au processus de réalisation d'un prototype d'un maison intelligente supervisée par un système d'internet des objets sous la direction de la plateforme Google Firebase. Nous avons également créé une application « androïde » qui nous permet d'obtenir et contrôlé des données sur l'évolution et la sécurité de ces données tels que le contrôle de l'éclairage et le fonctionnement automatique du ventilateur.

IV.2 Installer le module ESP8266 dans Arduino IDE

Pour installer la carte ESP8266 dans votre IDE Arduino, on a suivi les instructions suivantes :

1- Dans Arduino IDE 1.8.20, on accède au menu fichier > Préférences.

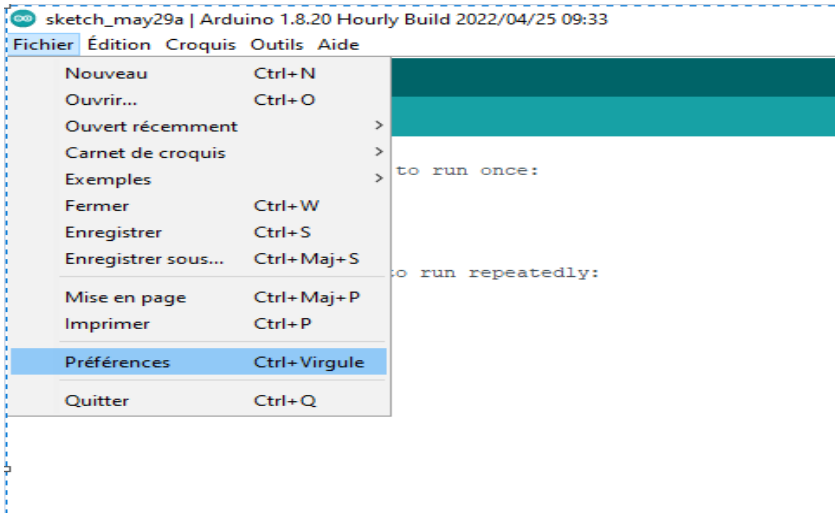

Image IV. 1: 1-ère étape d'installation de carte ESP8266 dans Arduino IDE.

2- Copier et coller la ligne suivante dans le Gestionnaire de cartes supplémentaires champ URL. http://arduino.esp8266.com/stable/package_esp8266com_index.json

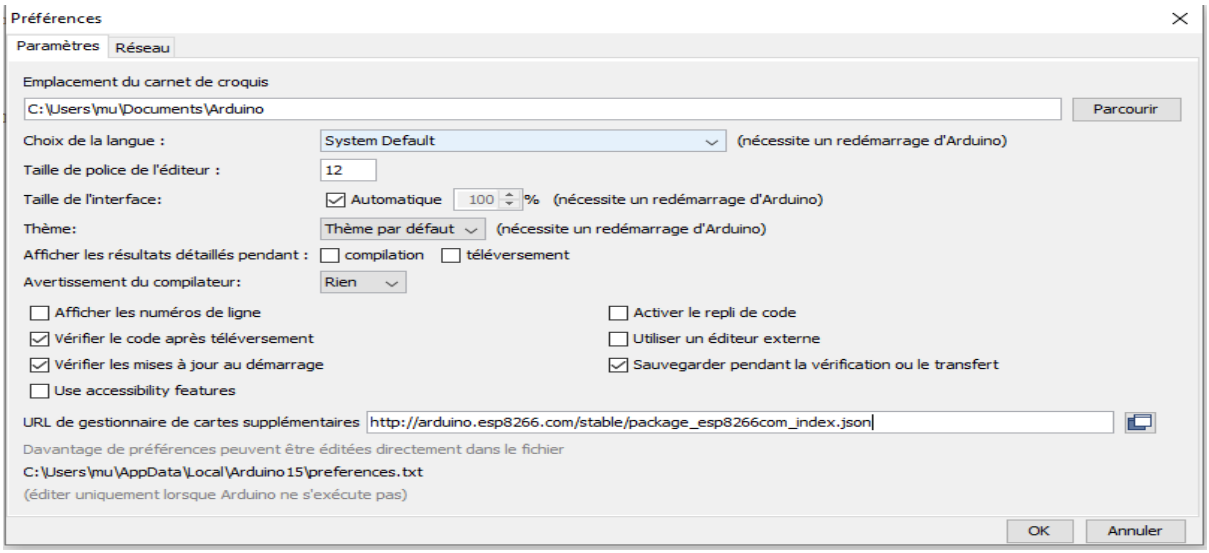

Image IV. 2: 2-ème étape d'installation.

3- Aller à Outils → Type de carte : « Arduino Uno » → Gestionnaire de carte

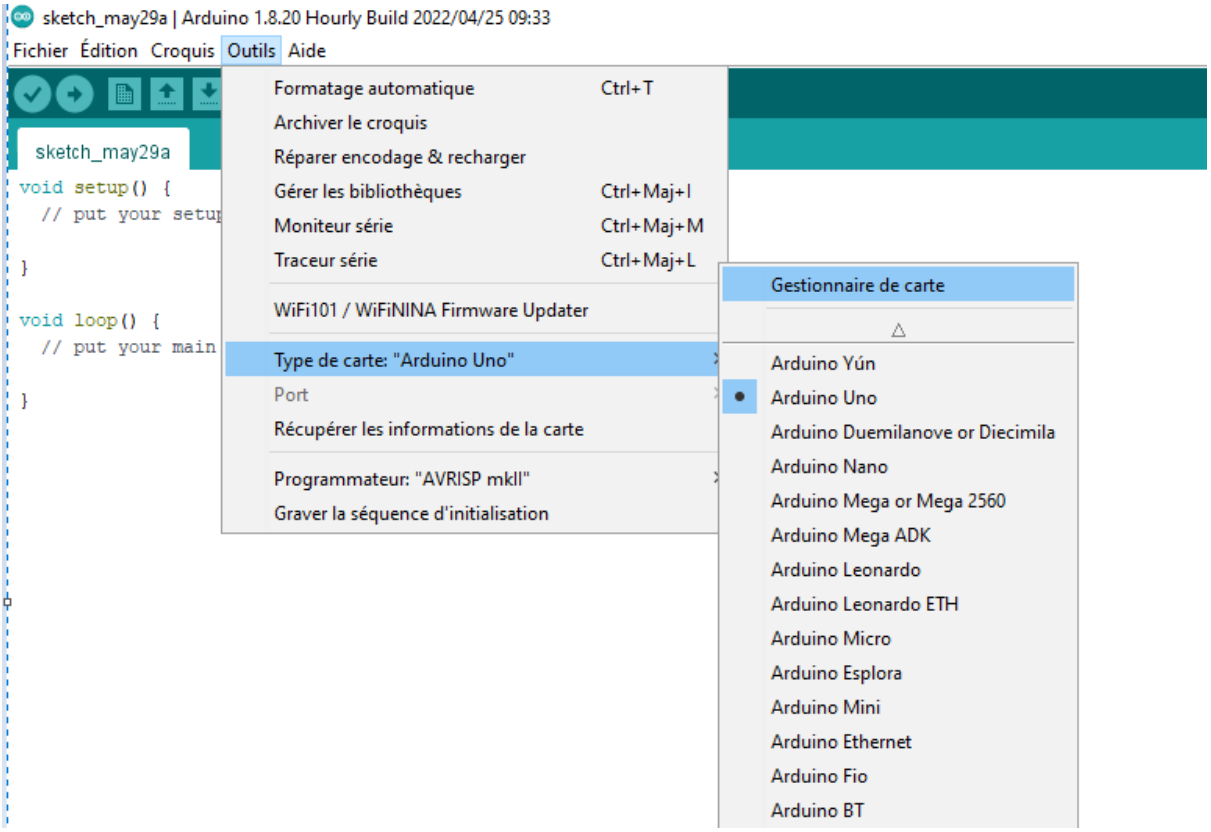

Image IV. 3: 3-ème étape d'installation de carte nodemcu8266 dans Arduino IDE.

4- Dans la barre de recherche écrire esp8266 et après la sélection de la version 2.4.1 et taper installer

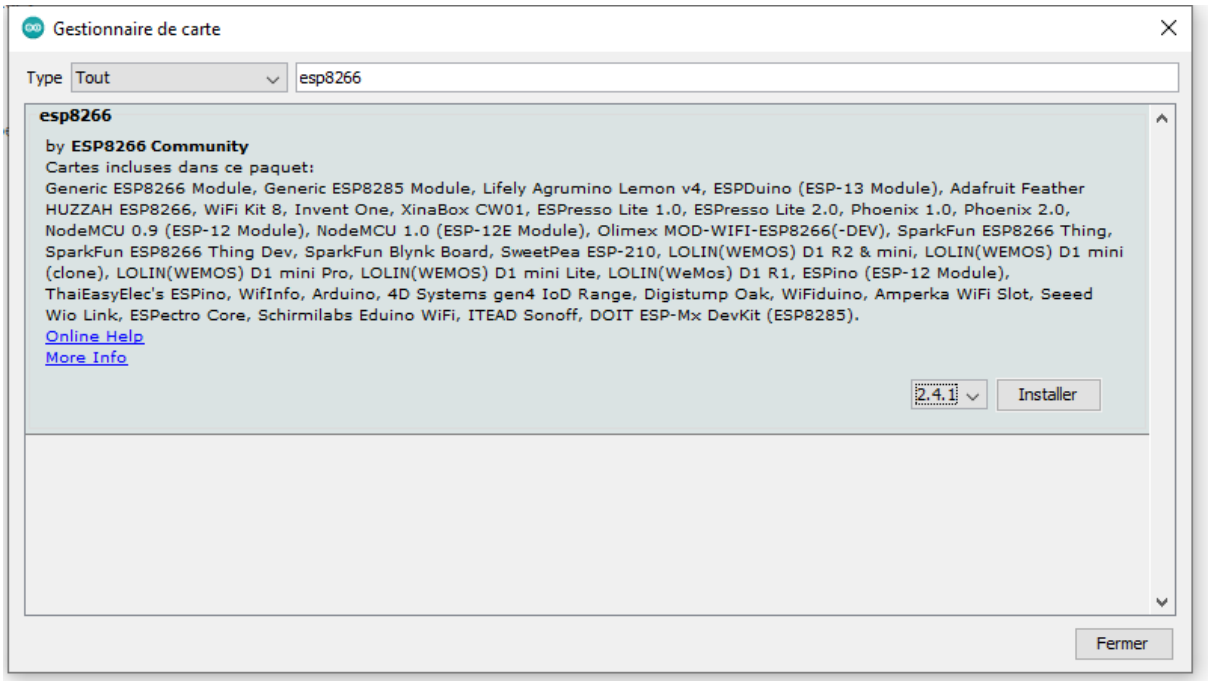

Image IV. 4: 4-ème étape d'installation de carte nodemcu8266 dans Arduino IDE.

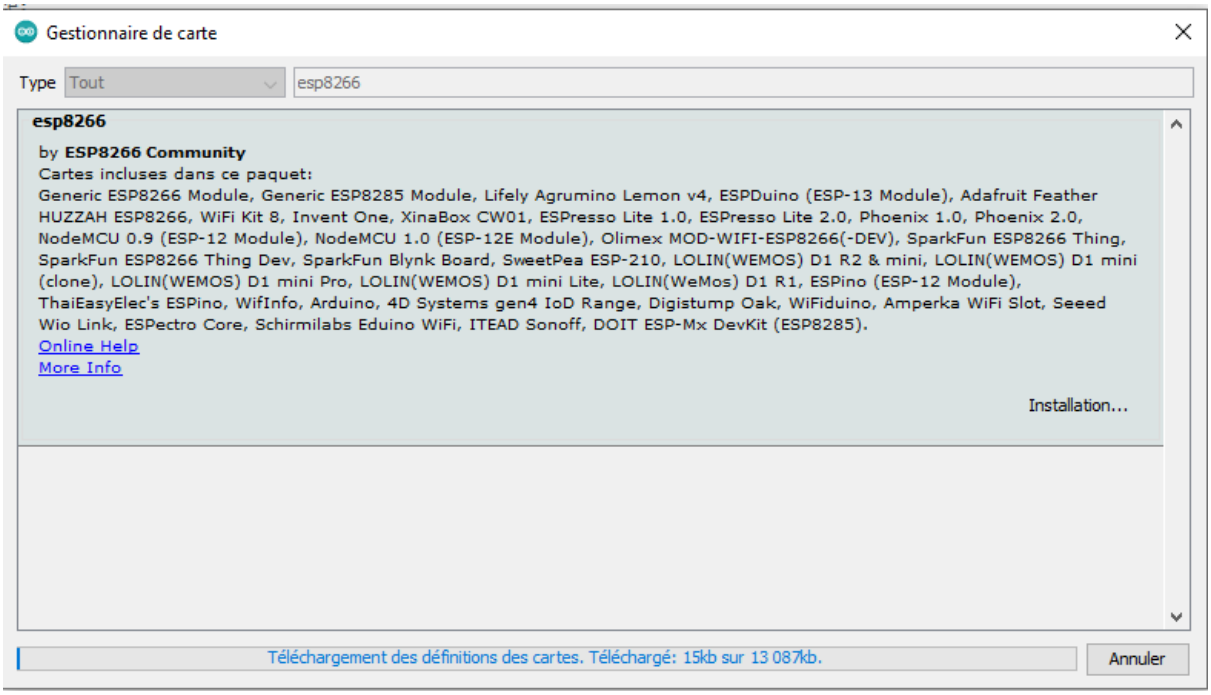

Image IV. 5: 5-ème étape d'installation de carte nodemcu8266 dans Arduino IDE.

IV.3 Création d'un projet firebase

1- Ouvrir compte firabase et créé un projet qui s'appelle smart-home

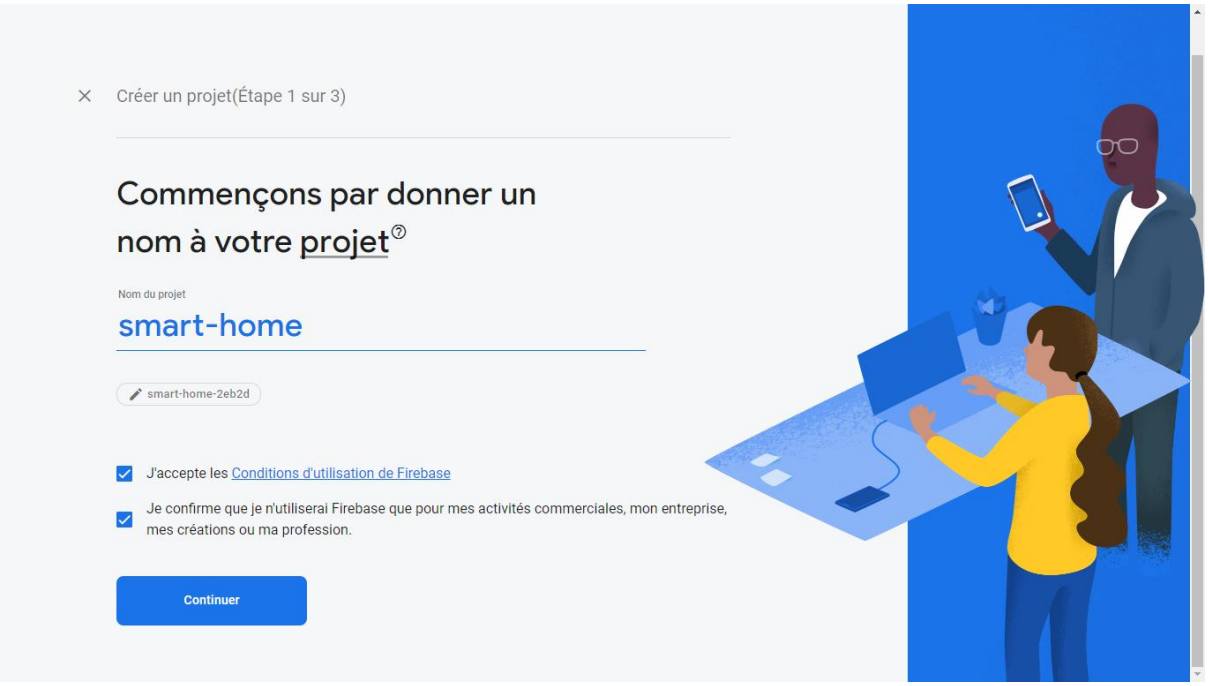

Image IV. 6: création un projet dans firebase.

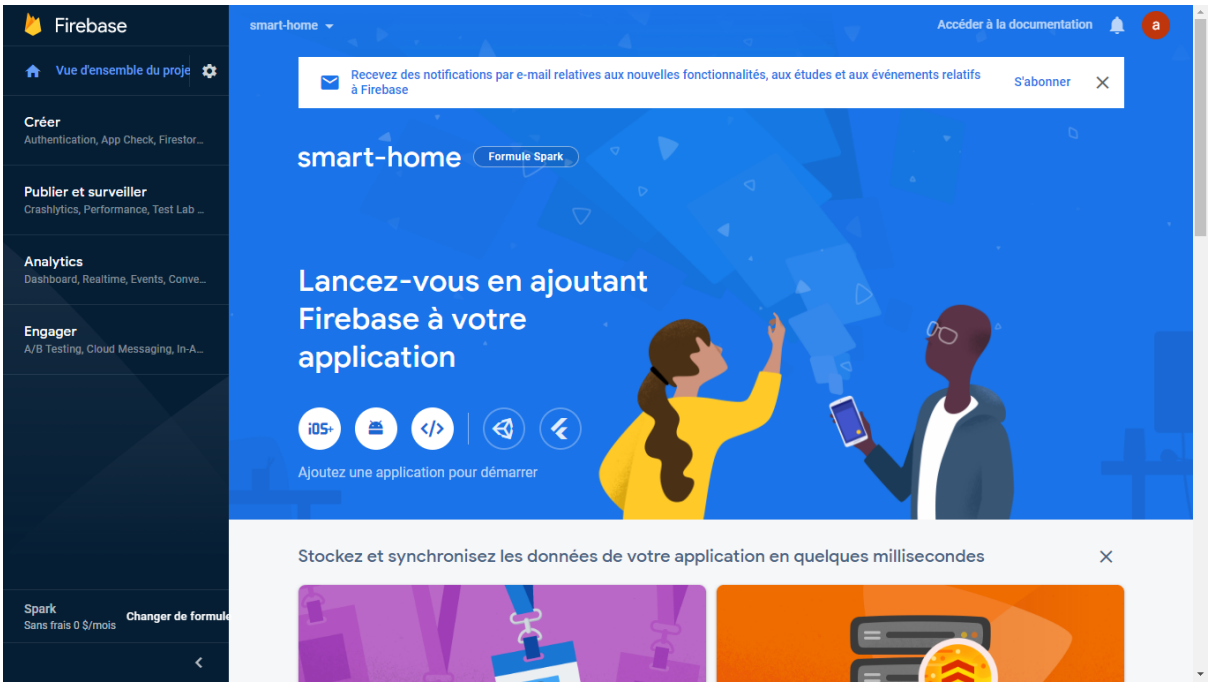

Image IV. 7: interface de firebase.

2- Après la création d'un projet firebase on clique sur « realtime database » pour crée une base donnée de notre projet

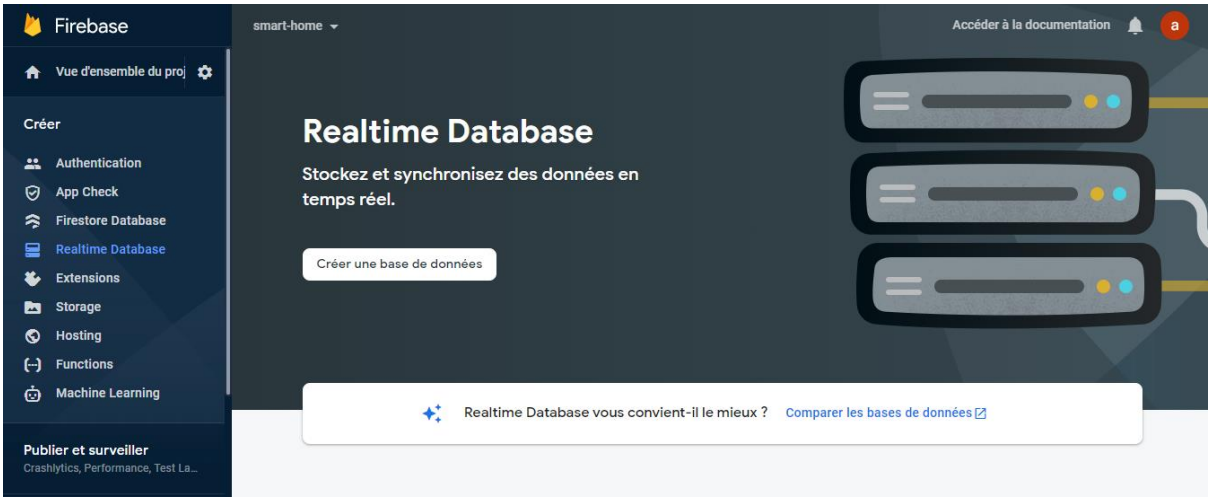

Image IV. 8: Création de base de données.

- **Les règles de firebase:**

Le bloc de construction principal des règles de sécurité de la base de données en temps réel c'est la condition. Une condition est une expression booléenne qui détermine si une opération particulière doit être autorisée ou refusée. Pour les règles de base, l'utilisation de littéraux true et false comme conditions fonctionne parfaitement bien. Mais le langage des règles de sécurité de la base de données en temps réel vous permet d'écrire des conditions plus complexes qui peuvent :

- Vérifier l'authentification de l'utilisateur
- Évaluer les données existantes par rapport aux données nouvellement soumises
- Accédez et comparez différentes parties de votre base de données
- Valider les données entrantes
- Utiliser la structure des requêtes entrantes pour la logique de sécurité

Image IV. 9: Modifier les règles de la base de données.

IV.4 Connexion NodeMCU8266 avec firebase

1- Ajouté bibliothèque de firebase dans Arduino IDE :

2- Télécharger firebase bibliothèque à partir du site web : https://github.com/FirebaseExtended/firebase-arduino De Arduino IDE sélectionner Croquis → inclure une bibliothèque → Ajouter la bibliothèque zip

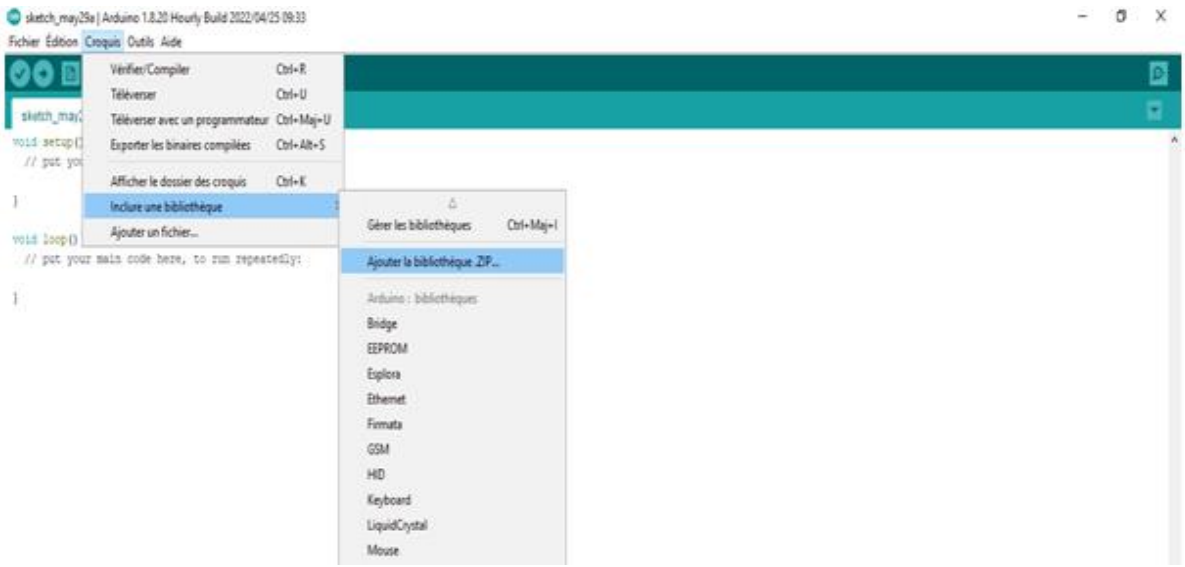

Image IV. 10: ajouter firebase bibliothèque

3- Installer ArduinoJson

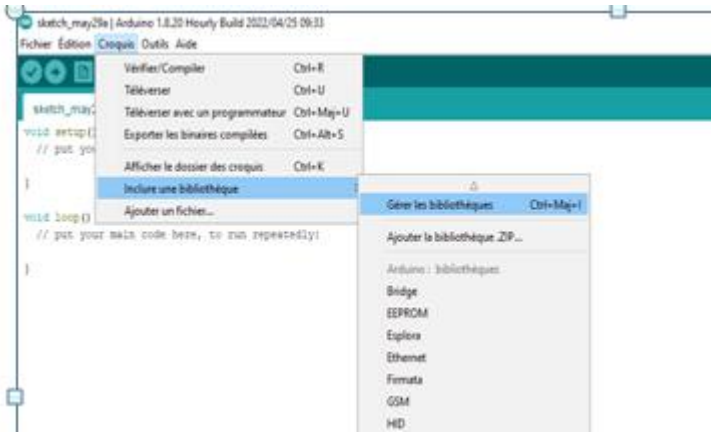

Image IV. 11: 1ère étape installation ArduinoJson.

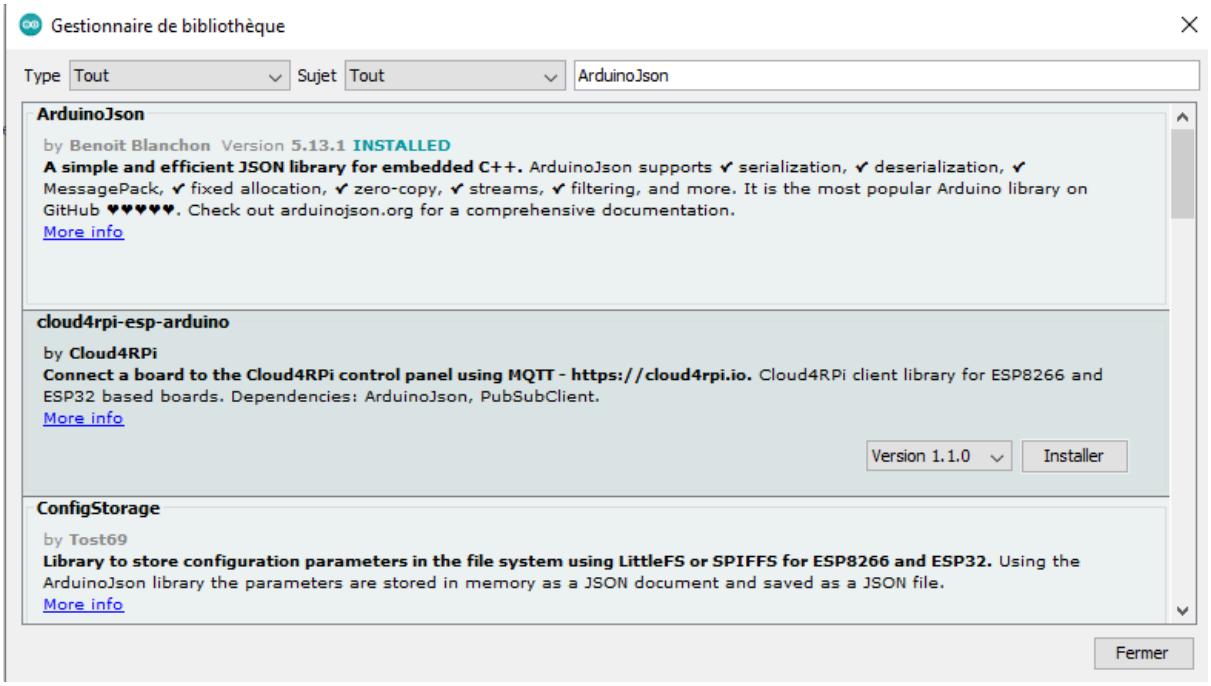

Image IV. 12: 2ème étape d'installation ArduinoJson.

4- Code de la bibliothèque firebase dans Arduino IDE

```
#include <Firebase.h>
#include <FirebaseArduino.h>
#include <FirebaseCloudMessaging.h>
#include <FirebaseError.h>
#include <FirebaseHttpClient.h>
#include <FirebaseObject.h>

#include <Firebase.h>
#include <FirebaseArduino.h>
#include <FirebaseCloudMessaging.h>
#include <FirebaseError.h>
#include <FirebaseHttpClient.h>
#include <FirebaseObject.h>

#include <ESP8266WiFi.h>

 // l'adresse du nom du projet à partir de l'identifiant firebase
#define FIREBASE_HOST "smart-home-2eb2d-default-rtdb.firebaseio.com"
 // la clé secrète générée à partir de firebase
#define FIREBASE_AUTH "mCUEMSgVwJGWxdmVIjT4d5wZeOuOjIwBv423YReS"
```

Image IV. 13: Code de la bibliothèque firebase dans Arduino IDE

IV.5 Synchronisation firebase avec google Sheets

IV.5.1 Google apps script

Google Apps Script vous permet de faire des choses nouvelles et intéressantes avec Google Sheets. Vous pouvez utiliser Apps Script pour ajouter des menus, des boîtes de dialogue et des barres latérales personnalisés à Google Sheets. Il vous permet également d'écrire des fonctions personnalisées pour Sheets, ainsi que d'intégrer Sheets à d'autres services Google tels que Calendar, Drive et Gmail. [63]

La plupart des scripts conçus pour Google Sheets manipulent des tableaux pour interagir avec les cellules, les lignes et les colonnes d'une feuille de calcul. Si vous n'êtes pas familier avec les tableaux en JavaScript, Codecademy propose un excellent module de formation pour les tableaux. [63]

1- Dans notre feuille google sheets Click sur Extension et après sur Apps Script

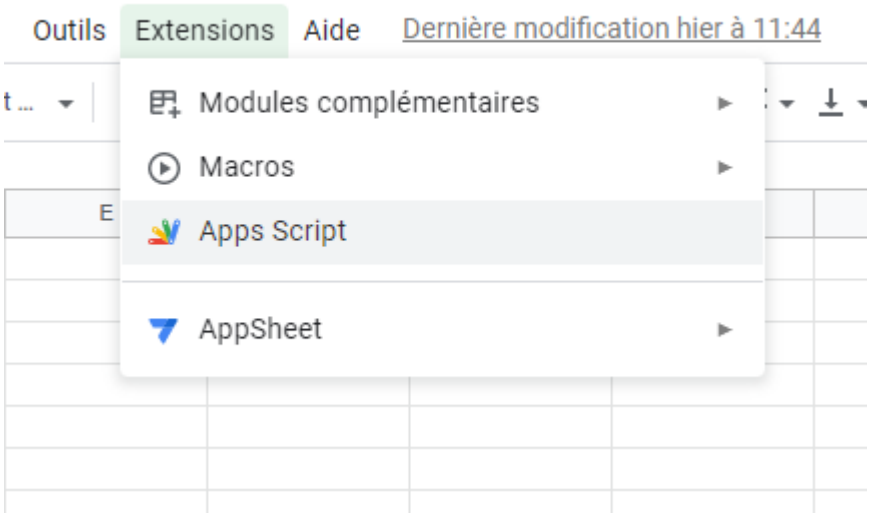

Image IV. 14: fenêtre de Google apps script

2- On écrire notre code de synchronisation dans cette fenêtre

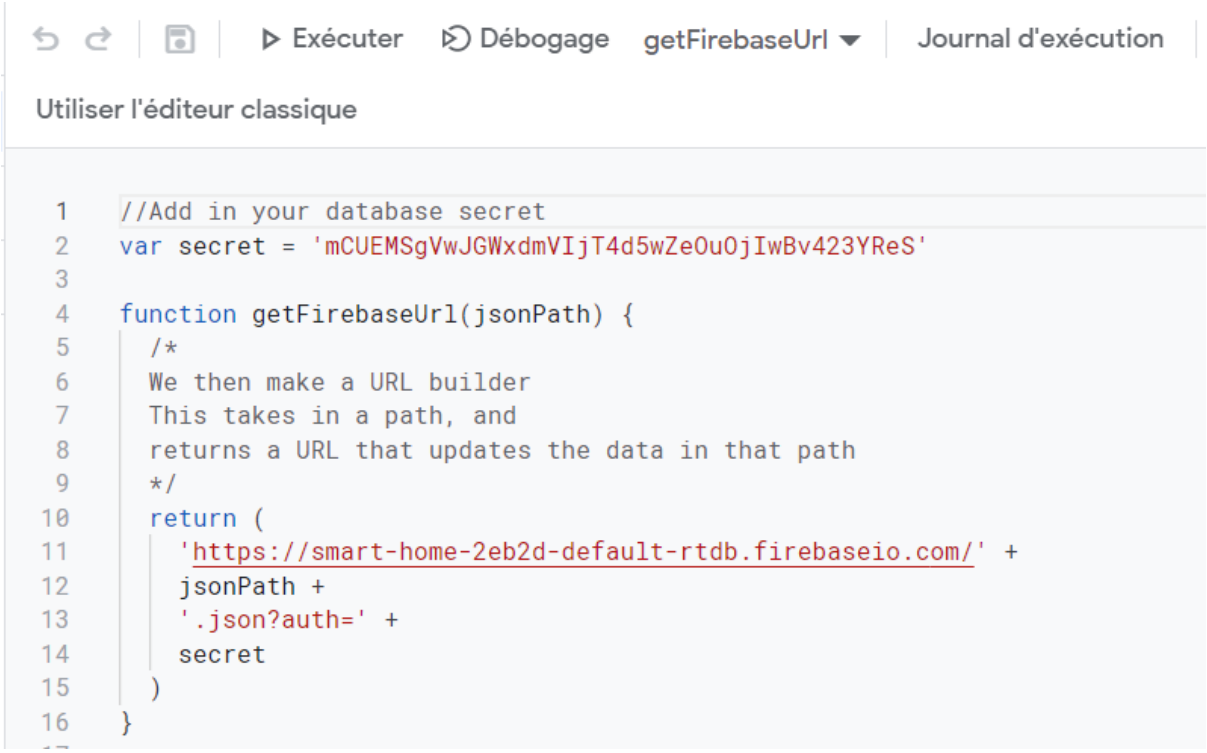

Image IV. 15: partie 1 de programme de synchronisation

```
function syncMasterSheet(excelData) {
  /*
  We make a PUT (update) request,
  and send a JSON payload
  More info on the REST API here : https://firebase.google.com/docs/database/rest/start
  */
  var options = {
    method: 'put',
    contentType: 'application/json',
    payload: JSON.stringify(excelData)
  }
  var fireBaseUrl = getFirebaseUrl('masterSheet')

  /*
  We use the UrlFetchApp google scripts module
  More info on this here : https://developers.google.com/apps-script/reference/url-fetch/url-fetch-app
  */
  UrlFetchApp.fetch(fireBaseUrl, options)
}
```

Image IV. 16: partie 2 de programme de synchronisation

```
function startSync() {
  //Get the currently active sheet
  var sheet = SpreadsheetApp.getActiveSheet()
  //Get the number of rows and columns which contain some content
  var [rows, columns] = [sheet.getLastRow(), sheet.getLastColumn()]
  //Get the data contained in those rows and columns as a 2 dimensional array
  var data = sheet.getRange(1, 1, rows, columns).getValues()
  var dataObject={};
  for(i=1 ; i<data.length ; i++){
  var dataRow=data[i];
  var Led_chambre1=dataRow[0];
  var Led_chambre2=dataRow[1];
    dataObject["IoT"] = {
    Led_chambre1:Led_chambre1,
    Led_chambre2:Led_chambre2,
  }
    syncMasterSheet(dataObject);
  }
//Use the syncMasterSheet function defined before to push this data to the "masterSheet" key in the firebase database
}
```

Image IV. 17: partie 3 de programme de synchronisation

3- Après on clique sur statSync

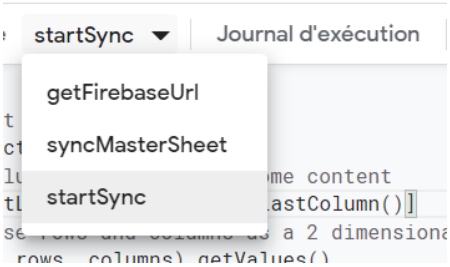

Image IV. 18: Fenêtre de startSync.

IV.5.2 Le déclencheur

Un déclencheur ou plus connu sous le nom anglais “trigger” permet d’exécuter une fonction automatiquement après un certain événement, comme modifier une cellule, ouvrir un document ou en recevant une requête HTTPS.

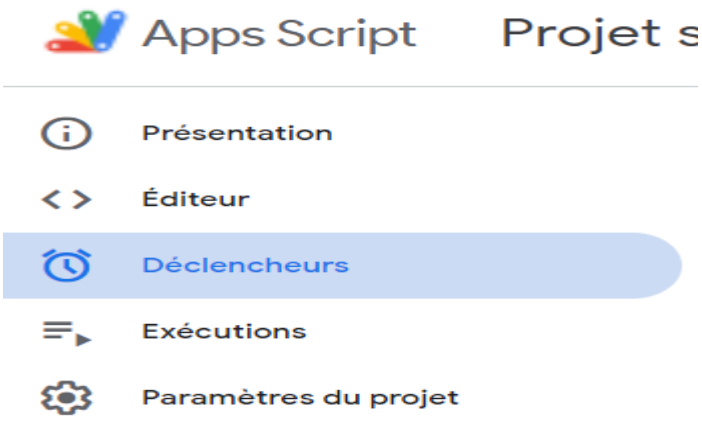

Image IV. 19: Le déclencheur

On modifier les paramétré de fenêtre on choisir la fonction de l’exécution « startSync » et le déploiement a exécuté « Head » et dans la source de l’événement « Basé sur la feuille de calcul » Et dans le type de l’événement « Lors d’un changement »

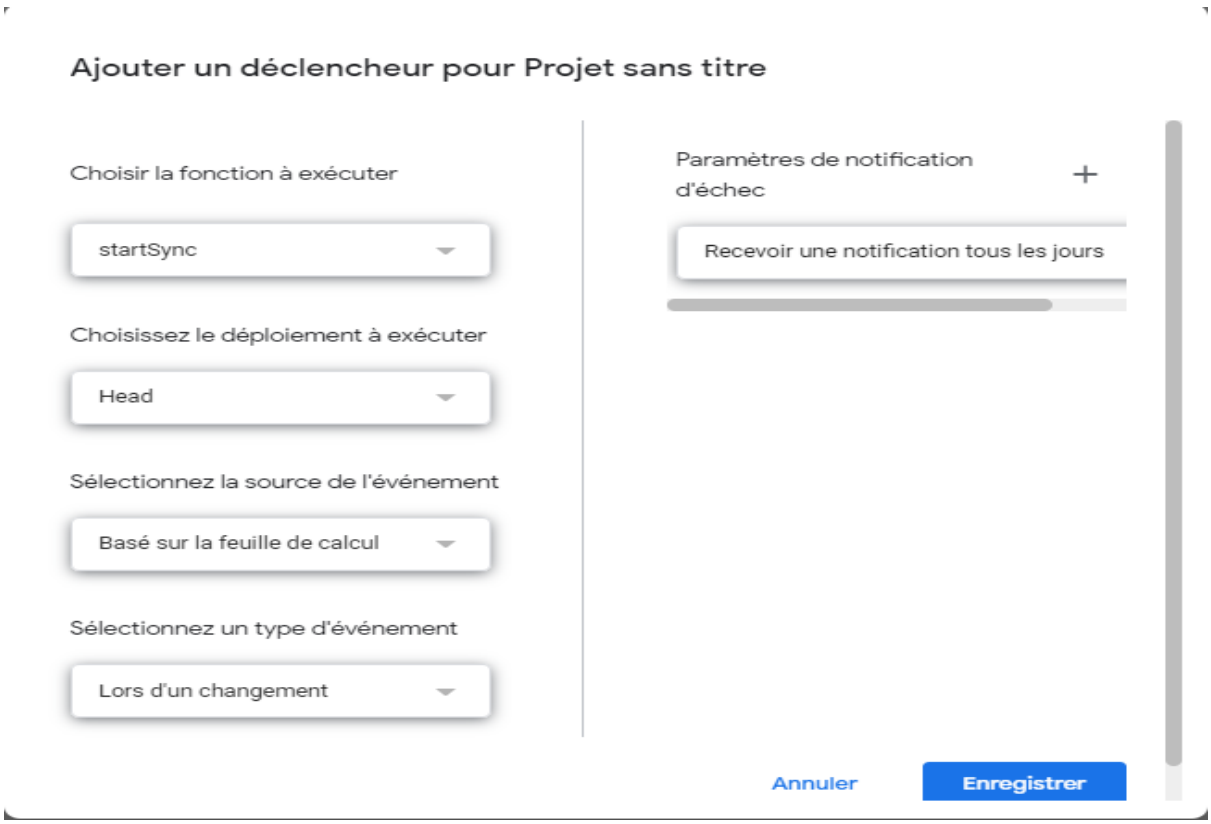

Image IV. 20: La fenêtre de déclencheur

Après la synchronisation on a cette feuille si on change les valeurs on cette feuille alors les valeurs se change aussi dans google firebase

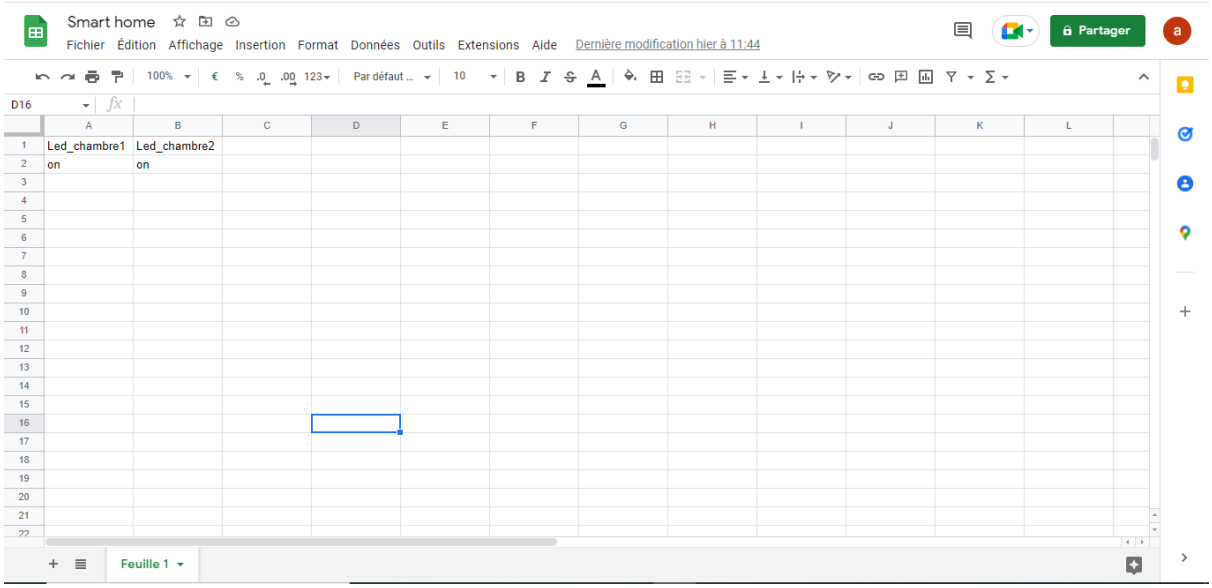

Image IV. 21: feuille finale de spreetsheets après la synchronisation.

Image IV. 22: Les valeurs de base de données dans firebase après la synchronisation

IV.6 La création d'une application Android et iOS

Dans cette étape nous avons créé une application Android et iOS à l'aide d'une plateforme « Adalo » Il présente de nombreux avantages qui correspondent à notre projet, dont le plus important est la sécurité des données et la difficulté de pénétrer les applications basées sur cette plate-forme, en plus de fournir des avantages très professionnels, que ce soit de la conception et le dessein ou des fenêtres prêtes à programmation très précises et excellentes c'est la première plateforme professionnelle dans le domaine de la construction d'applications sans programmation

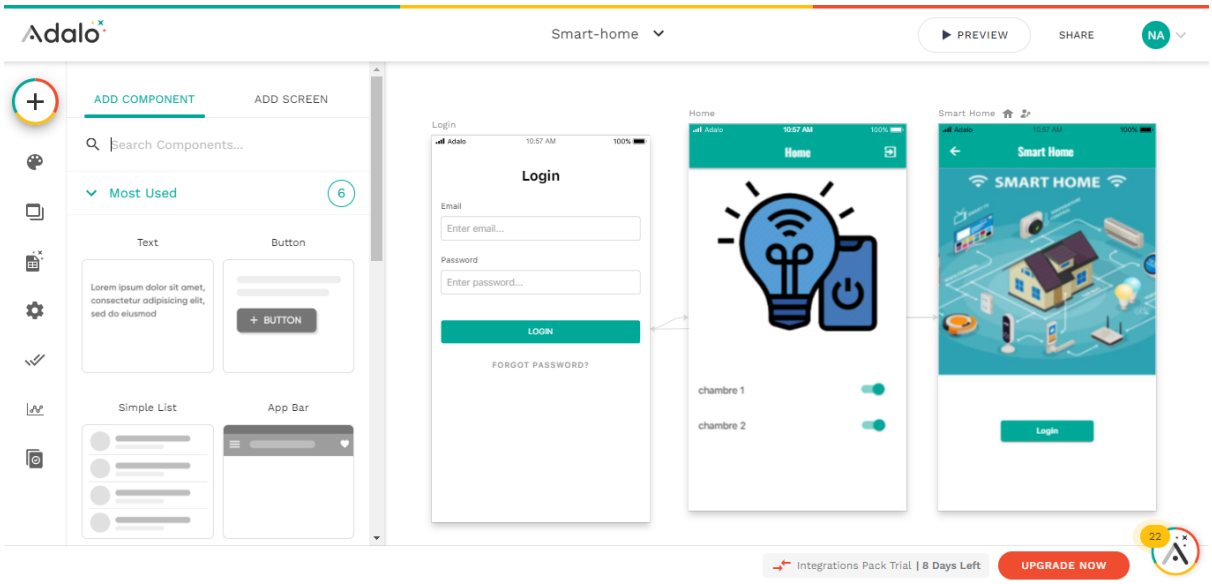

Image IV. 23: Interface de Adalo

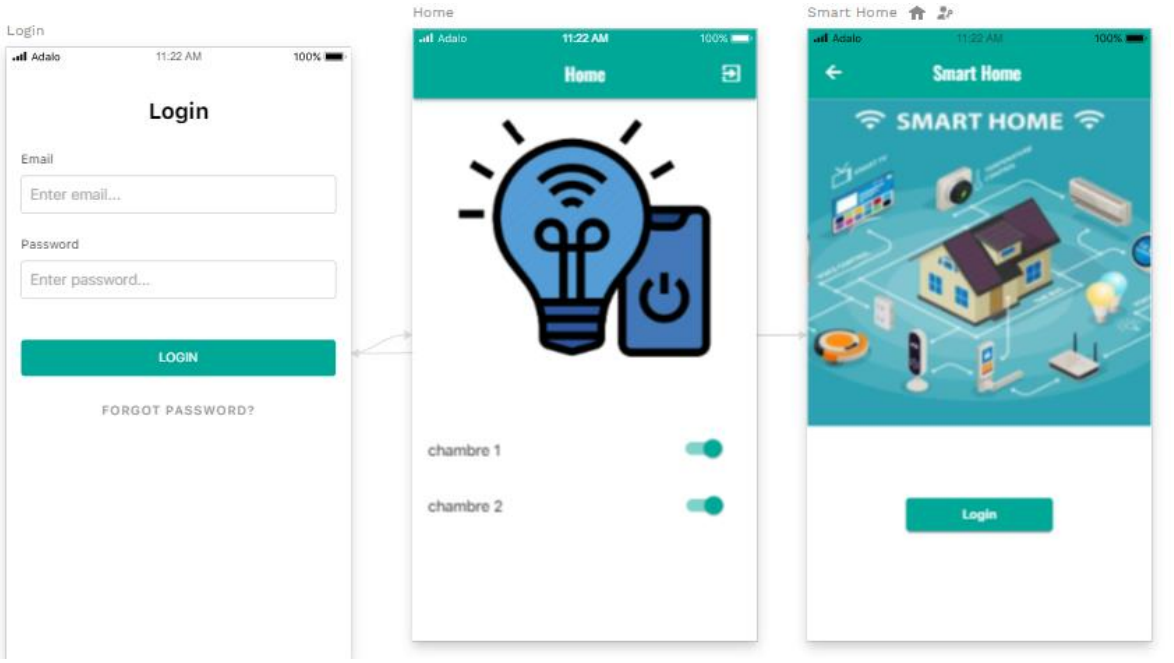

Image IV. 24: les interfaces des fenêtres « smart-home », « login » et « Home »

- Dans la fenêtre « login » email et le mot de passe sont enregistrer danse la base de donnée « Users »

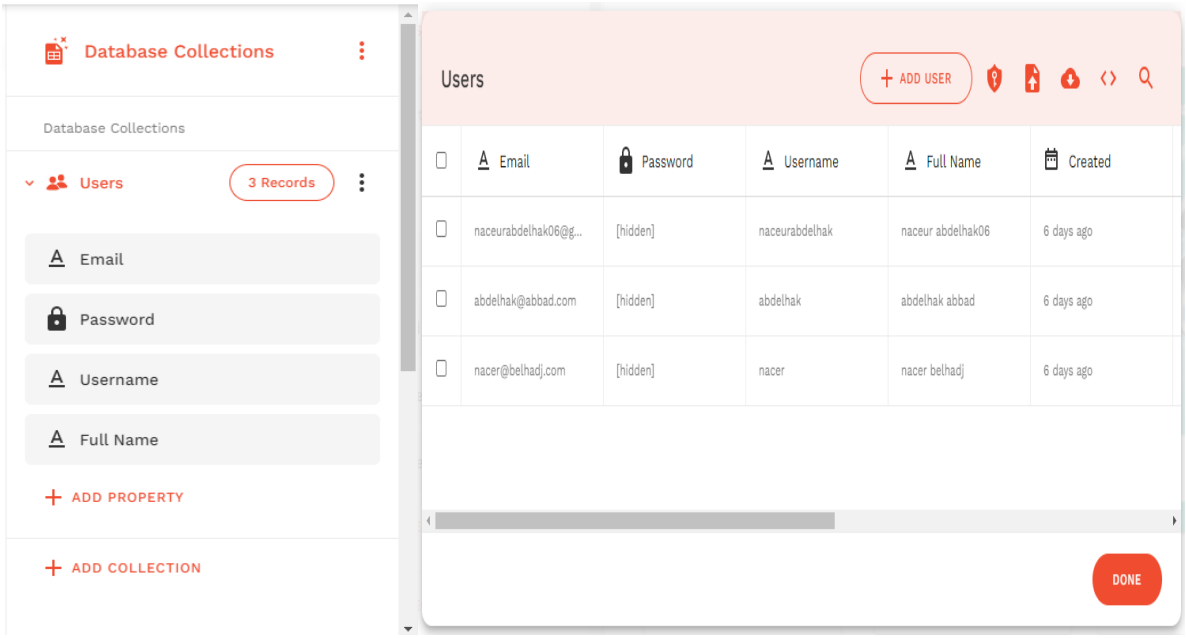

Image IV. 25: La base de données Users

IV.7 La synchronisation de Google Sheets avec Adalo

Si on prend un bouton de type switch la configuration de ce bouton est pour changer les données dans google Sheets alors la configuration comme si dessous :

Etape 1 : on copie le lien de la feuille de notre projet dans google Sheets et le coller dans le site web : « https://sheetdb.io/apis » pour obtient son API.

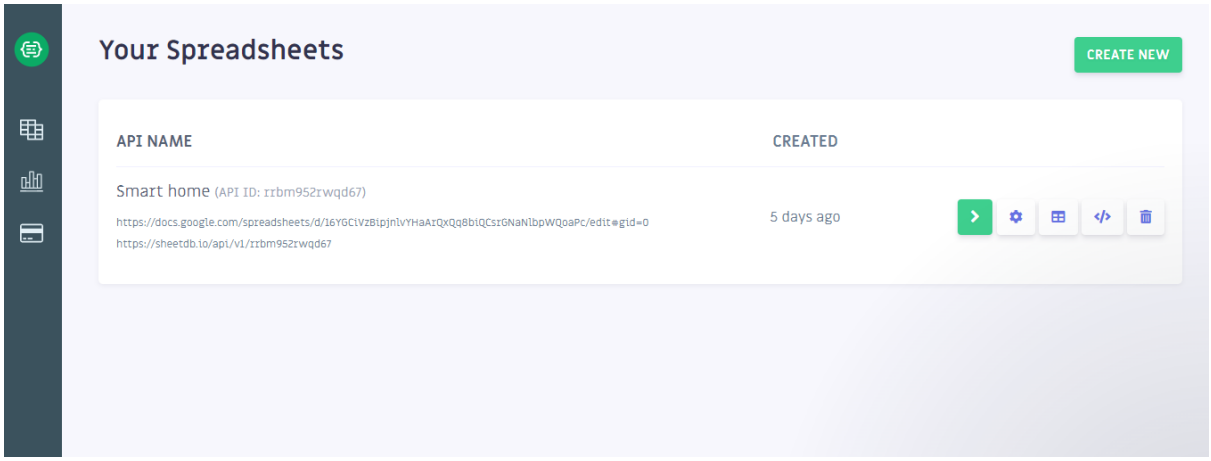

Image IV. 26: API de la feuille de notre projet dans google Sheets

- Configuration de action « on »

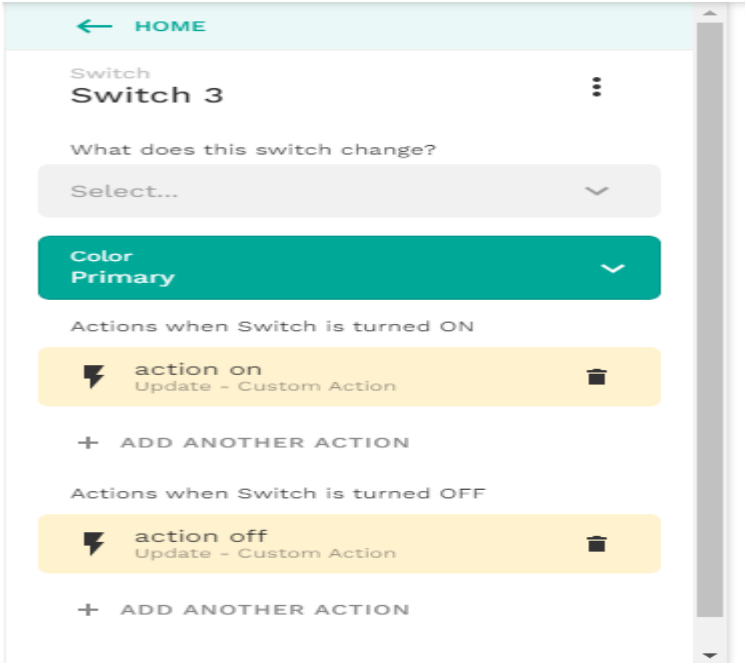

Image IV. 27: Fenêtre d'action de button switch on/off

Dans la première boîte on écrit le nom de l'action et la deuxième boîte on choisit son type

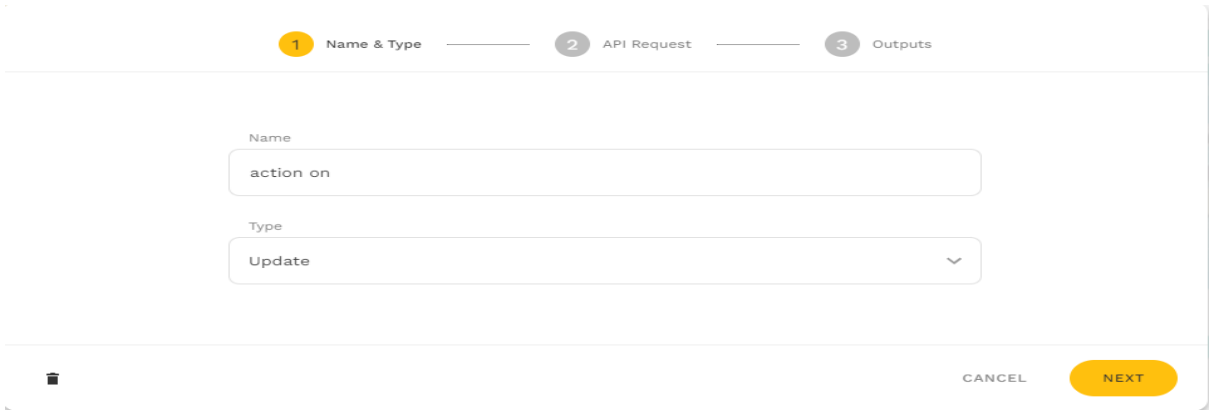

Image IV. 28: Etape 1 de configuration action 1

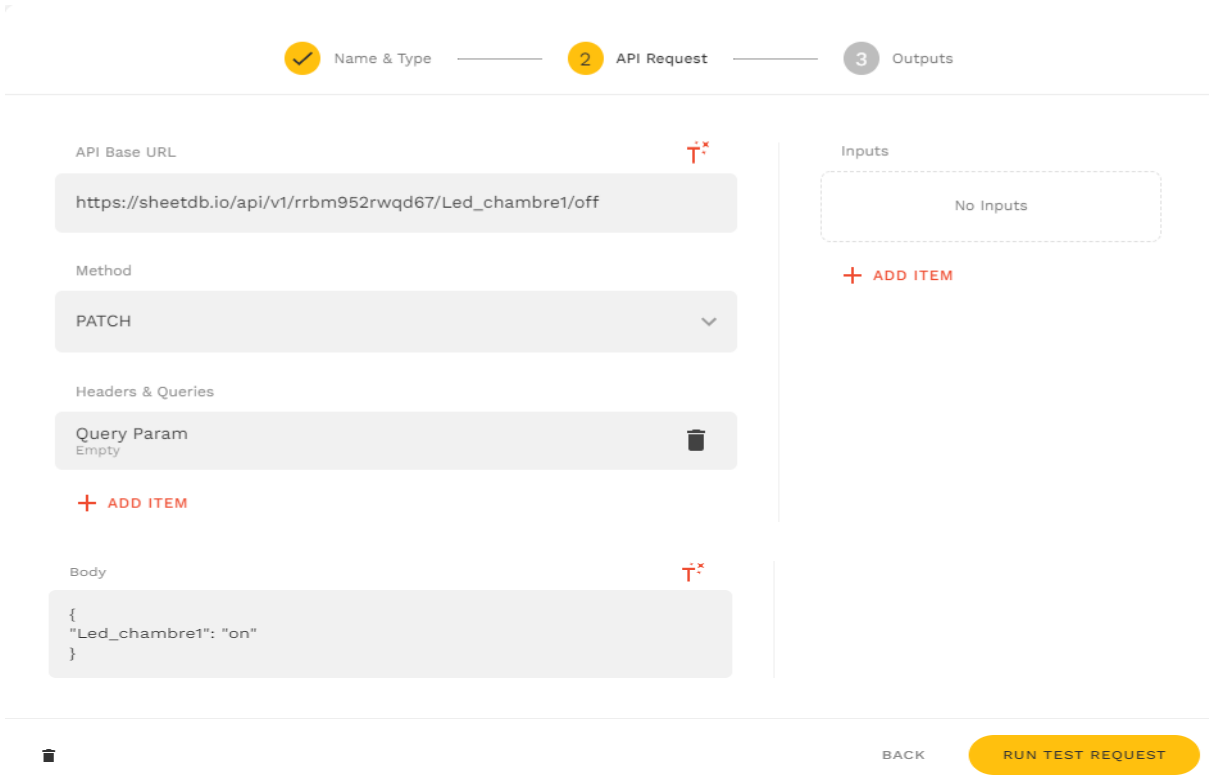

Image IV. 29: étape 2 de configuration action 2

Dans la première boîte on écrit le lien d'API et on ajoute la valeur de colonne et la valeur de ligne à la deuxième boîte on choisit la méthode « PATCH » et dans la troisième boîte on choisit « Quercy Param » et à la quatrième boîte on écrit le code Json qui va modifier les données dans google Sheets.

– On fait le test de notre synchronisation

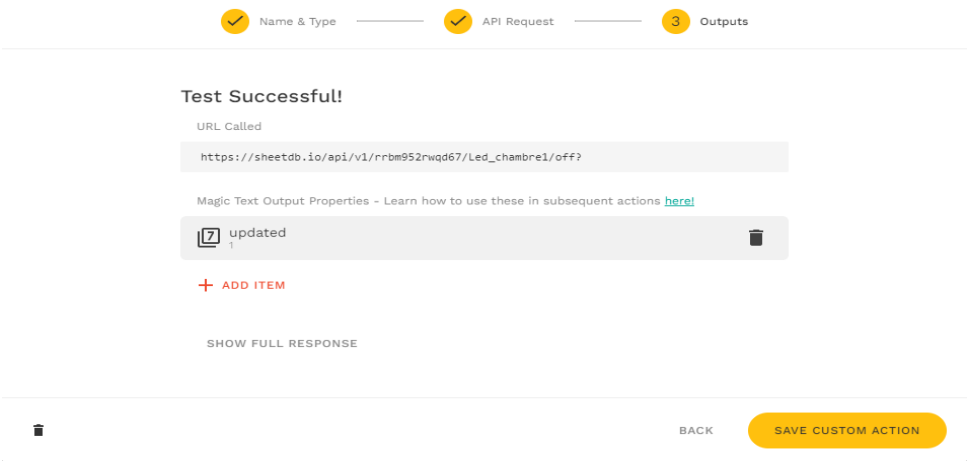

Image IV. 30: Etape 03 le test de la synchronisation.

- L’application finale de notre projet :

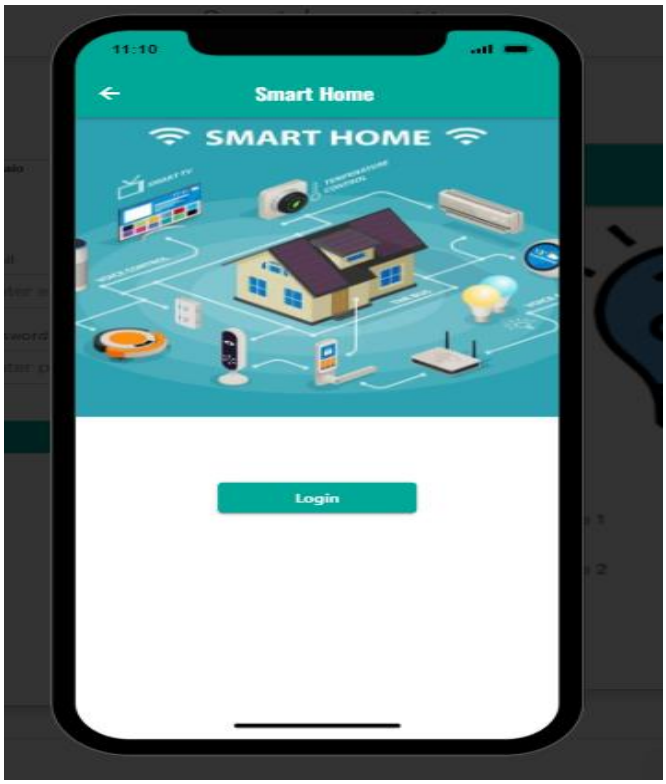

Image IV. 31: La première fenêtre qui apparaît dans l'application

Quand on clique sur « Login » On va directement à la fenêtre de connexion « Login »

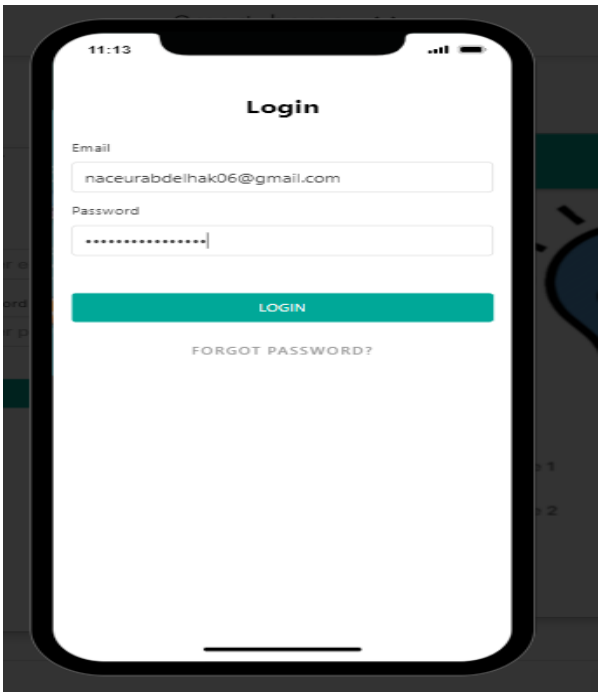

Image IV. 32: fenêtre de connexion « Login »

Après la connexion on va directement à la fenêtre de controlle des lamps « Home> »

Dans cette fenêtre, nous pouvons contrôler l'éclairage de la maison.

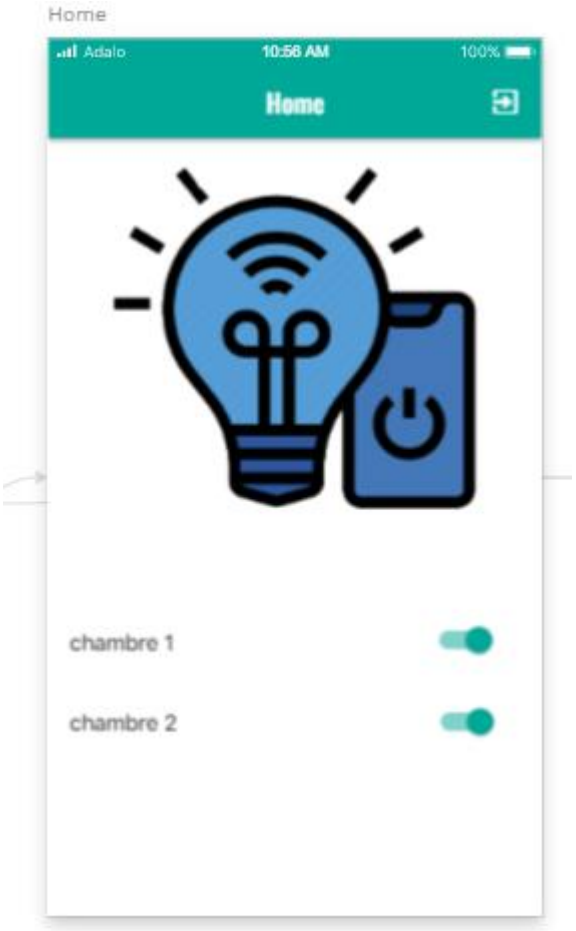

Image IV. 33:fenêtre de contrôle « Home »

– Dans le cas où le mot de passe oublié : on clique sur « forgot password »

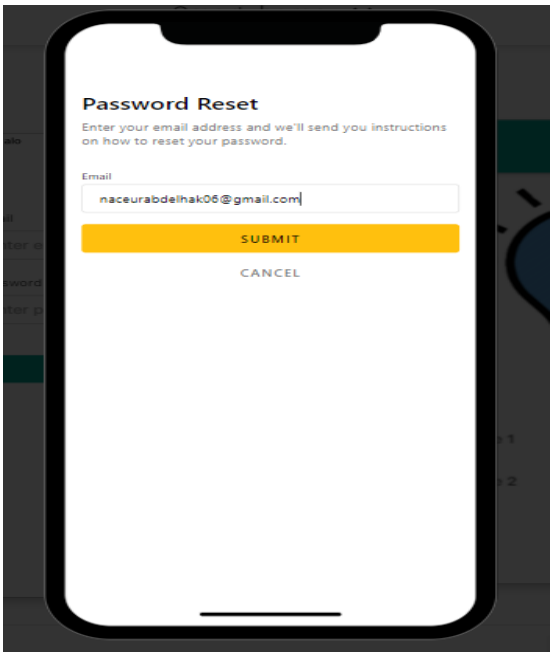

Image IV. 34: La fenêtre de « Forgot password »

L'application va envoyer automatiquement un mot de passe temporaire valable pendant 24 heures à l'email de l'utilisateur.

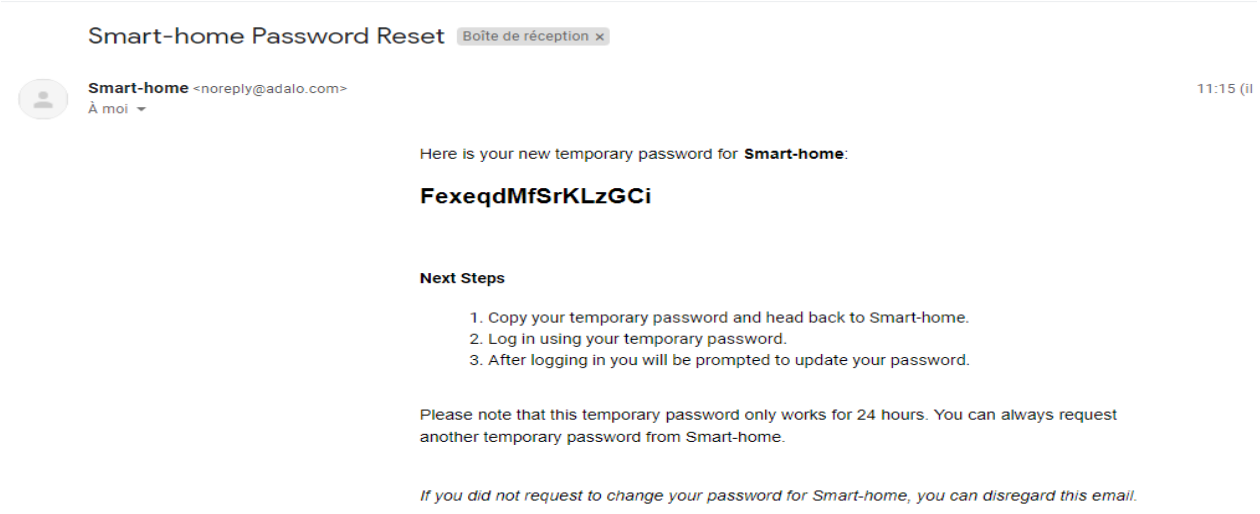

Image IV. 35: Mot de passe envoyé par email.

Lors de la saisie du mot de passe envoyé par e-mail on se rendre directement à la fenêtre de saisie du nouveau mot de passe.

IV.8 Le projet prototype final

– L'image suivante présente un prototype d'une maison intelligente.

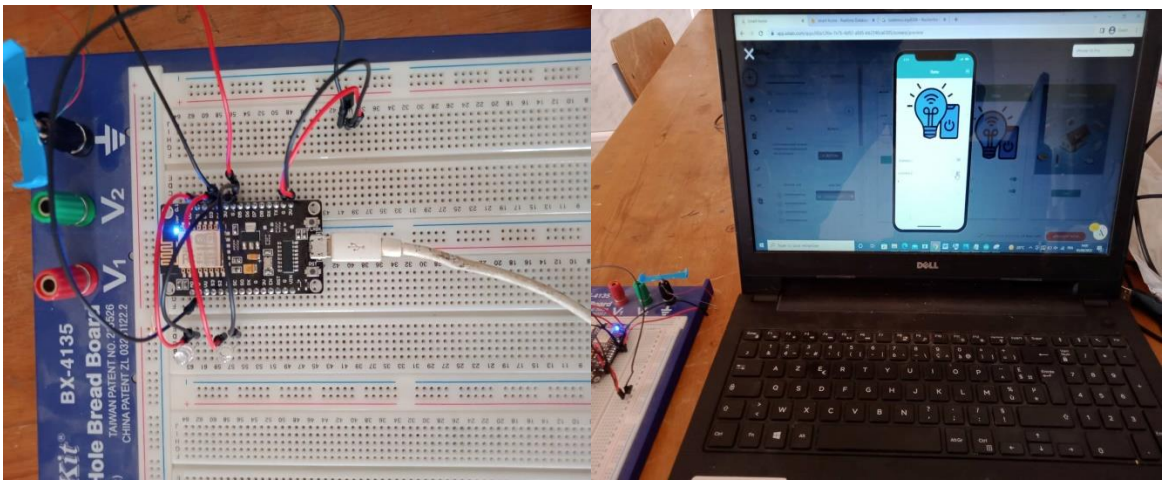

Image IV. 36: prototype d'une maison intelligente

IV.9 Résultat

– L'image suivante présente notre projet qui est l'automatisation d'une maison intelligente grâce à un système IoT.

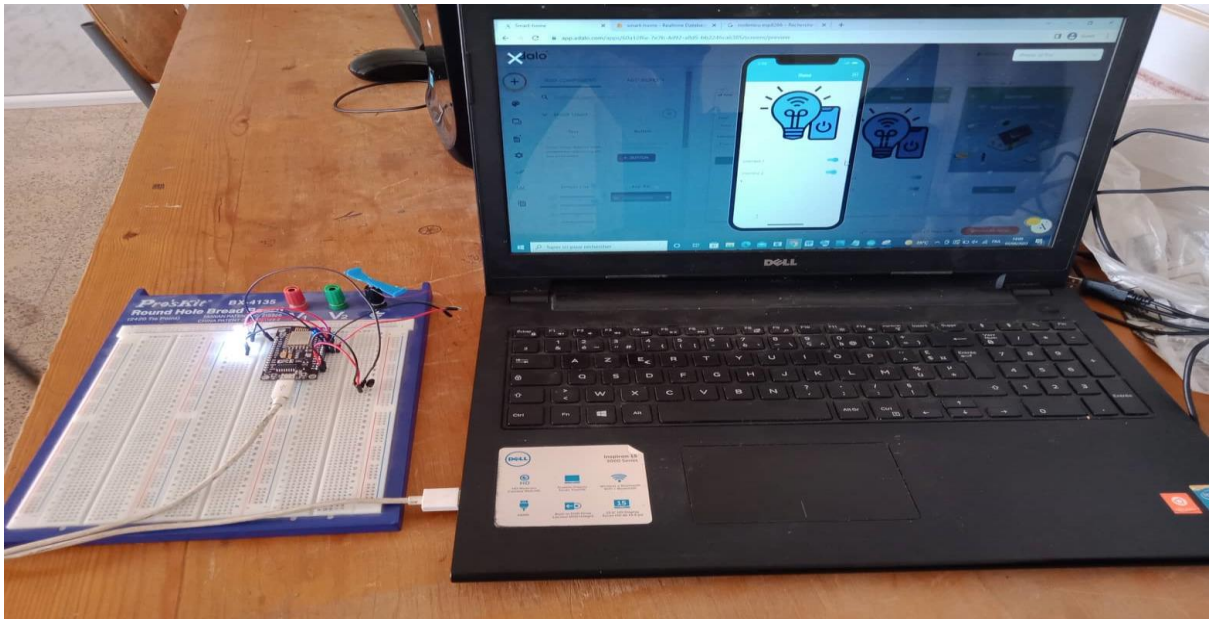

Image IV. 37: l'automatisation d'une maison intelligente à la base un système IoT

L'image ci-dessous montre les mesures des température capturées selon le capteur LM35 dans le serial monitor de Arduino IDE.

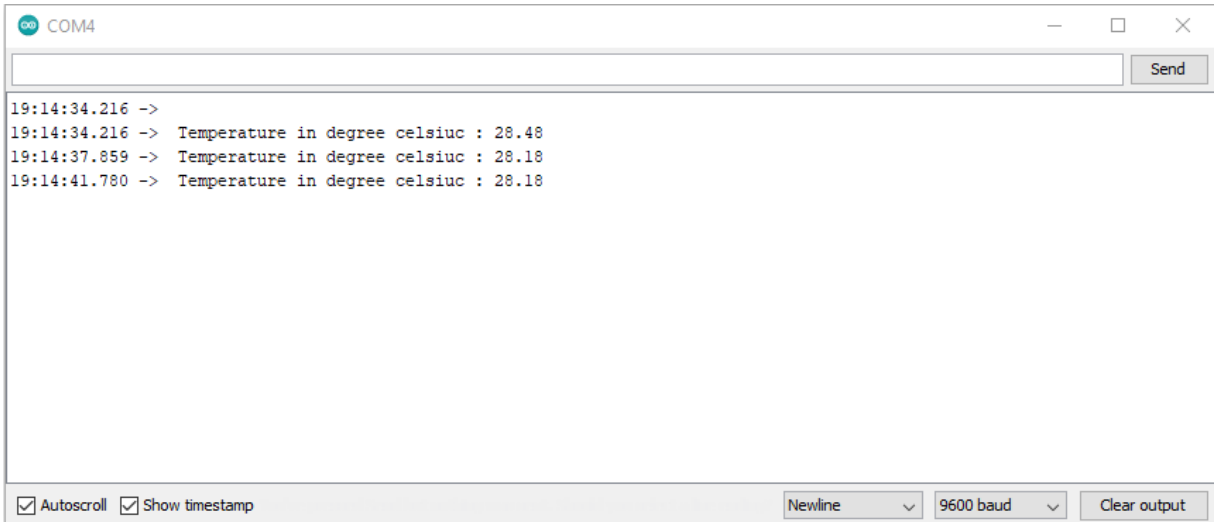

Image IV. 38: Les mesures de LM35 dans le serial monitor

Ces mesures sont utilisées pour contrôler le fonctionnement du ventilateur. Dans notre exemple, si la température est supérieure ou égale à 24 degrés Celsius, alors le moteur démarre automatiquement, ce qui représente le rôle du ventilateur.

L'image suivante montre les données dans la base de données Firebase.

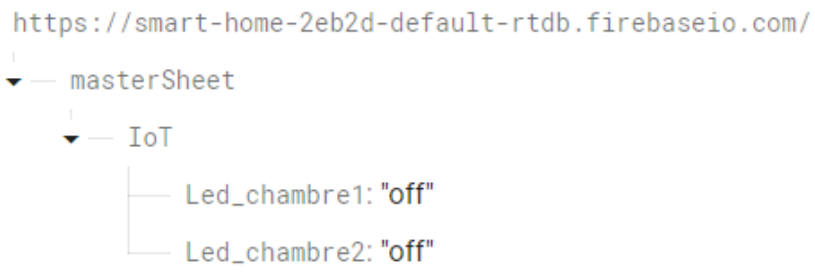

Image IV. 39: les données dans la base de données Firebase

Ces données sont envoyées à nodemcu8266 pour contrôler les Leds qui représentent le rôle des lampes.

IV.10. Conclusion

Ce chapitre décrit la partie importante de ce mémoire qu'est la réalisation, où on a présenté les détails d'implémentation de notre prototype d'une maison intelligente afin de montrer les déférentes configuration et les paramètres qui lié et synchroniser les déférentes service dans le système soit entre nodemcu8266 et Firebase ou entre Firebase et google Sheets et aussi google Sheets avec l'application Android et iOS que nous avons créé.

Conclusion générale et perspectives

Depuis quelques années, les objets connectés deviennent omniprésent dans notre vie quotidienne en montrant une croissance exponentielle. L'Internet des objets (IdO), ou l'IoT (Internet of Things), offre aux objets dans le monde entiers la capacité de se connecter à internet et de communiquer avec les autres objets.

Dans la littérature, la plupart des travaux qui ont traité la problématique de sécurité dans l'internet des objets, se sont limités sur des solutions cryptographiques. Cependant, ces solutions deviennent de plus en plus inefficaces voir inapplicable à des objets ayant de fortes contraintes de ressources.

pour ces raison on a discuter dans ce mémoire les différents types de menace et la classification approfondies des attaques exploitables et les contre-mesures possibles puis on a développé un petite application IoT d'une maison intelligente pour montrer d'un coté le fonctionnement de ce système et d'un autre cote la circulation des données échangées entre les composants de cette application pour les protéger.

Perspective

Les nombreuses menaces de sécurité et le manque de politiques de sécurité adaptés à ces applications pourraient réduire considérablement leur développement donc il faut combiner l’utilisation des méthodes de cryptographies ainsi que les modèles basés sur l’intelligence artificielle

Références bibliographiques

[01] 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, 2009.

[02] Tafazolli, R., 2006. Technologies for the wireless future. Chichester: Wiley.

[03] Taleb Omar, Mankouri Abdelkrim. « Programmation de la sécurité Internet des Objet, Etude de cas module WIFI Electric imp », Mémoire de master, Université de Tlemcen, Algérie, 2016.

[04] Evans, D., 2011. The Internet of Things How the Next Evolution of the Internet Is Changing Everything. [Ebook] Etats-Unis : Cisco internet business solutions group (IBSG), pp.2-5. Disponible à : <https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf> [Consulté le 4 février 2022].

[05] Atoumi .M Y, Bensadi. S, « Approche évolutionnaire pour la composition de services sensible à la QoS dans l'Internet des Objets à large échelle », Mémoire de master, Université de Bejaia, Algérie, 2018

[06] Connectwave. 2022. Comment se compose un système IoT ? [En ligne] Disponible à : <https://www.connectwave.fr/techno-appli-iot/iot/reseaux-et-infrastructures-iot> [Consulté le 4 février 2022].

[07] Yick, J., Mukherjee, B. and Ghosal, D., 2008. Wireless sensor network survey. Computer Networks, 52(12), pp.2292-2330.

[08] Puccinelli, D. and Haenggi, M., 2005. Wireless sensor networks: applications and challenges of ubiquitous sensing. IEEE Circuits and Systems Magazine, 5(3), pp.19-31.

[09] H. Ali, « implémentation d'un protocole d'élection d'un serveur d'authentification dans l'internet des objets, » Mémoire de master, Université de Bejaia, Algérie, 2017

[10] Stankovic, J., 2008. Wireless Sensor Networks. Computer, 41(10), pp.92-95.

[11] S. Rabeb, « Modèle collaboratif pour l'Internet of Things (IoT), » Mémoire de maitrise université de Québec à Chicoutimi, 2016.

[12] Saleh, I., 2018. Internet des Objets (IdO) : Concepts, Enjeux, Défis et Perspectives. Internet des objets, 2(1).

[13] Yacine Challal. Sécurité de l'Internet des Objets : vers une approche cognitive et systémique. PhD thesis, 2012.

[14] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M., 2015. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys &amp ; Tutorials, 17(4), pp.2347-2376.

[15] F. Bouchebbah Y.ait mouhoub. « Proportion d'un modèle de confiance pour l'internet des objets ». Mémoire de master, Université de Bejaia, Algérie,2015.

[16] Roxin. I, Bouchereau. A, 2017, Ecosystème de l'Internet des Objets : Évolutions et Innovations, pp.23-52.

[17] Saleh, I., 2017. Les enjeux et les défis de l'Internet des Objets (IdO). Internet des objets, 17(1).

[18] Mukherjee, A., 2015. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. Proceedings of the IEEE, 103(10), pp.1747-1761.

[19] Burhan, M., Rehman, R., Khan, B. and Kim, B., 2018. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors, 18(9), p.2796.

[20] Kaushal, K. and Sahni, V., 2015. DoS Attacks on different Layers of WSN: A Review. International Journal of Computer Applications, 130(17), pp.8-11.

[21] Osanaiye, O., Alfa, A. and Hancke, G., 2018. A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks. Sensors, 18(6), p.1691.

[22] L. Li, 2012 «Study on security architecture in the Internet of Things: In Measurement, Information and Control (MIC) », International Conference on, vol. 1, pp. 374-377.

[23] Deogirikar, J. and Vidhate, A., 2017. Security Attacks inIoT: A Survey. [En ligne] Faratarjome.ir. Disponible à : <http://faratarjome.ir/u/media/shopping_files/store-EN-1520245543-1185.pdf> [Consulté le 2 mars 2022].

[24] Jacobson, M., 2015. Vulnerable Progress: The Internet of Things, the Department of Defense and the Dangers of Networked Warfare. [ebook] COMP-116: Computer Systems Security. Disponible à : <https://www.cs.tufts.edu/comp/116/archive/fall2015/mjacobson.pdf> [Consulté le 2 mars 2022].

[25] Andrea, I., Chrysostomou, C. and Hadjichristofi, G., 2015. Internet of Things: Security vulnerabilities and challenges. IEEE.

[26] U.Farooq, M., Waseem, M., Khairi, A. and Mazhar, S., 2015. A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications, 111(7), pp.1-6.

[27] Xu, L., He, W. and Li, S., 2014. Internet of Things in Industries: A Survey. IEEE Transactions on Industrial Informatics, 10(4), pp.2233-2243.

[28] DOINEA, M., BOJA, C., BATAGAN, L., TOMA, C. and POPA, M., 2015. Internet of Things Based Systems for Food Safety Management. Informatica Economica, 19(1/2015), pp.87-97.

[29] Rahman, Abdul Fuad Abdul, Maslina Daud, and Madihah Zulfa Mohamad. 2016, Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework. Proceedings of the International Conference on Internet of things and Cloud Computing. ACM,

[30] Jeyanthi, N., Shreyansh Banthia, and Akhil Sharma,2017 Security in IoT Devices. Security Breaches and Threat Prevention in the Internet of Things. IGI Global, pp 96-116.

[31] Sadeghi, Ahmad-Reza, Christian Wachsmann, and Michael Waidner. 2015 Security and privacy challenges in industrial internet of things. Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE.

[32] Babar, Sachin, et al. 2011, Proposed embedded security framework for internet of things (iot). Wireless Communication, Vehicular Technology, Information Theory and Aerospace &

Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on. IEEE.

[33] Roman, R., Zhou, J. and Lopez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), pp.2266-2279.

[34] Jan, Mian Ahmad, and Muhammad Khan. 2013 Denial of Service Attacks and Their Countermeasures in WSN." IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC) 3.

[35] Puthal, D., Nepal, S., Ranjan, R. and Chen, J., 2016. Threats to Networking Cloud and Edge Datacenters in the Internet of Things. IEEE Cloud Computing, 3(3), pp.64-71.

[36] Nuke, S., R. Mahajan, A. and C Thool, R., 2013. UML Modeling of Physical and Data Link Layer Security Attacks in WSN. International Journal of Computer Applications, 70(11), pp.25-28.

[37] Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. 2015. Towards an analysis of security issues, challenges, and open problems in the internet of things." Services (SERVICES), 2015 IEEE World Congress on. IEEE.

[38] Nia, Arsalan Mohsen, and Niraj K. Jha. 2016. A comprehensive study of security of internet-of-things." IEEE Transactions on Emerging Topics in Computing.

[39] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, 2010. Classification of RFID attacks. Gen 15693 (14443):14

[40] Uttarkar, R. and Kulkarni, R., 2014. Internet of Things: Architecture and Security. [ebook] International Journal of Computer Application. Disponible à: <http://www.rspublication.com/ijca/ijca_index.htm> [Consulté le 23 mars 2022].

[41] Airehrour, D., Gutierrez, J. and Ray, S., 2017. A Trust-Aware RPL Routing Protocol to Detect Blackhole and Selective Forwarding Attacks. Journal of Telecommunications and the Digital Economy, 5(1), pp.50-69.

[42] A. Ahmed, M. Ahmed, O. Khan and M. Shah, L (2017). A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT", International Journal of Advanced Computer Science and Applications, Vol. 8, No. 7, pp.489-501

[43] Chandramouli, R. and Mell, P., 2010. State of security readiness. XRDS: Crossroads, The ACM Magazine for Students, 16(3), pp.23-25.

[44] Trappe, W., 2015. The challenges facing physical layer security. IEEE Communications Magazine, 53(6), pp.16-20.

[45] Lake, D., Milito, R., Morrow, M. and Vargheese, R., 2014. Internet of Things: Architectural Framework for eHealth Security. Journal of ICT Standardization, 1(3), pp.301-328.

[46] Kaps, J. (2006). Cryptography for Ultra-Low Power Devices: Worcester Polytechnic Institute.

[47] Liu, C., Zhang, Y., Zeng, J., Peng, L., & Chen, R. 2012. Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology. 2012 8th International Conference on Natural Computation, 874-878.

[48] Granjal, J., Monteiro, E. and Sa Silva, J., 2015. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Communications Surveys & Tutorials, 17(3), pp.1294-1312.

[49] PalSingh, V., S. Anand Ukey, A. and Jain, S., 2013. Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks. International Journal of Computer Applications, 62(15), pp.1-6.

[50] S. Kumar, S. Pal, A. Kumar, and J. Ali, 2013. Virtualization, The Great Thing and Issues in Cloud Computing," Int. J. Curr. Eng. Technol., pp. 338–341.

[51] Rédaction, L., 2022. Microcontrôleur : définition et composants. [En ligne] Journaldunet.fr. Disponible à : <https://www.journaldunet.fr/web-tech/dictionnaire-de-l-iot/1440684-microcontroleur-definition-et-composants/> [Consulté le 2 avril 2022].

[52] Lemdani Rafik, Malouadjmi Nabil. 2017. Etude, conception et réalisation d'une plateforme pour l'automatisation et le contrôle à distance des serres agricoles. Mémoire de master, Université de Boumerdes.

[53] Arduino.cc. 2022. What is Arduino? [En ligne] Disponible à : <https://www.arduino.cc/en/Guide/Introduction> [Consulté le 2 avril 2022].

[54] Elearn.ellak.gr. 2022. Day 5 - Section 1 - Introduction to NodeMCU: What is NodeMCU?. [En ligne] Disponible à: <https://elearn.ellak.gr/mod/book/view.php?id=2326&chapterid=844> [Consulté le 3 avril 2022].

[55] Abidi, Y., 2022. NodeMCU vs Arduino vs Raspberry Pi. [En ligne] Candid.Technology. Disponible à : <https://candid.technology/nodemcu-vs-arduino-vs-raspberry-pi/> [Consulté le 6 avril 2022].

[56] Z. Haoua et O. Mohamed Mahmoud. 2019. Vers des Bâtiments Intelligent pour l'élevage de volaille. Mémoire de master, Université de Blida.

[57] Abdallah Fethi.2017. Conception d'un Système immotique "Smart Building" pour la société CNAS. Mémoire de master, Université de Blida .

[58] Datasheet du capteur de température lm35. [En ligne]. Disponible à : https://www.ti.com/lit/ds/symlink/lm35.pdf?HQS=TI-null-null-alldatasheets-df-pf-SEP-wwe

[59] Firebase. 2022. Construire la documentation, Construire la documentation | Firebase Documentation. [En ligne] Disponible à : <https://firebase.google.com/docs/build?hl=fr&authuser=0> [Consulté le 19 avril 2022].

[60] Rédaction, L., 2022. Adalo : comment l'utiliser pour créer une app sans coder. [En ligne] Journaldunet.fr. Disponible à : <https://www.journaldunet.fr/web-tech/guide-de-l-entreprise-digitale/1511263-adalo-comment-l-utiliser-pour-creer-une-app-sans-coder/> [Consulté le 20 avril 2022].

[61] Google.com. 2022. Google Sheets: tableur en ligne intégré | Google Workspace. [En ligne] Disponible à : <https://www.google.com/intl/fr/sheets/about/> [Consulté le 27 avril 2022].

[62] Pillou, J., 2022. Javascript - Introduction au langage Javascript. [En ligne] Web.maths.unsw.edu.au. Disponible à : <https://web.maths.unsw.edu.au/~lafaye/CCM/javascript/jsintro.htm> [Consulté le 27 avril 2022].

[63] Google Developers. 2022. Extending Google Sheets | Apps Script | Google Developers. [en ligne] Disponible à: <https://developers.google.com/apps-script/guides/sheets> [Consulté le 10 mai 2022

Annexe

```
#include <Firebase.h>
#include <FirebaseArduino.h>
#include <FirebaseCloudMessaging.h>
#include <FirebaseError.h>
#include <FirebaseHttpClient.h>
#include <FirebaseObject.h>
#include <Firebase.h>
#include <FirebaseArduino.h>
#include <FirebaseCloudMessaging.h>
#include <FirebaseError.h>
#include <FirebaseHttpClient.h>
#include <FirebaseObject.h>
#include <ESP8266WiFi.h>
#define FIREBASE_HOST "smart-home-2eb2d-default-rtdb.firebaseio.com"
#define FIREBASE_AUTH "mCUEMSgVwJGWxdmVIjT4d5wZeOuOjIwBv423YReS"
#define WIFI_SSID "OPPO A5s"
#define WIFI_PASSWORD "123456789"
#define Led_1 5
#define Led_2 0
#define vont 2

int sensorPin=A0;
float tempC;
float sVoltage;

void setup()
{
  pinMode(Led_1, OUTPUT);
  pinMode(Led_2, OUTPUT);
```

```
  pinMode(vont, OUTPUT);
  Serial.begin(9600);
  delay(1000);
  WiFi.begin(WIFI_SSID, WIFI_PASSWORD);
  Serial.print("Connecting to ");
  Serial.print(WIFI_SSID);
  while (WiFi.status() != WL_CONNECTED)
  {
    Serial.print(".");
    delay(500);
  }
  Serial.println();
  Serial.print("Connected to ");
  Serial.println(WIFI_SSID);
  Firebase.begin(FIREBASE_HOST, FIREBASE_AUTH);
}
void loop()
{

    float xVal=analogRead(sensorPin);

    sVoltage = (xVal*3100.0)/1023;
    tempC=sVoltage/10;
    Serial.print("Temperature in degree celsiuc : ");
    Serial.print(tempC);
    delay(2000);
    if(tempC >= 24)
      {
        digitalWrite(vont, HIGH);
      }
    else
```

```
    {
      digitalWrite(vont, LOW);
    }
  String Ld1;
  Ld1=Firebase.getString("/masterSheet/IoT/Led_chambre1");
  if (Ld1 == "on")
    {
     Serial.println("Led Turned ON");
     digitalWrite(Led_1, HIGH);
    }
  else
    {
     Serial.println("Led Turned off");
     digitalWrite(Led_1, LOW);
    }
  String Ld2;
  Ld2=Firebase.getString("/masterSheet/IoT/Led_chambre2");
  if (Ld2 == "on")
    {
      Serial.println("Led Turned ON");
      digitalWrite(Led_2, HIGH);
    }
  else
    {
      Serial.println("Led Turned off");
      digitalWrite(Led_2, LOW);
    }
}
```

الملخص :

الهدف الرئيسي من اطروحة الماستر الاكادمية هو التركيز على دراسة و تطبيق امن انترنت الاشياء في ظل التطور السريع الرهيب لمجال انترنت الاشياء و كذلك التزايد الكبير و المستمر في استعماله في مختلف المجالات و هذا ما استلزم توفير حماية و تحقيق مستوى امان عالي لضمان السير الجيد و الجودة الممتازة في الخدمات المتعلقة بنظام انترنت الاشياء و كذلك زيادة الثقة و الاقبال الكبير للمستخدمين لهذا المجال و ذلك من خلال التصدي لجميع طرق الاختراق و التجسس التي تهدد حماية البيانات و المعلومات داخل النظام وهذا ما قمنا بتجسيده في مشروعنا حيث قمنا بانشاء نموذج بسيط لمنزل ذكي باستعمال بطاقة الكترونية nodemcu8266 وقمنا بانشاء واجهة تطبيق Android و iOS للتحكم في المنزل الذكي اما بانسبة لجزء امن هذا النظام فقد قمنا بربط المنزل الذكي و التطبيق باستخدام خدمات و برامج التي توفر ميزات عديدة اهمها الامن و الحماية المشددة و التشفير ذو المستوى العالي للبيانات و المعلومات المتنقلة داخل النظام مثل خدمات google firebase

الكلمات المفتاحية: انترنت الأشياء ، المنزل الذكي ، امن انترنت الأشياء ، التحكم عن بعد ، حماية البيانات.

Abstract:

The main objective of this work, which falls within the scope of obtaining the academic master's degree, is to focus on the study and application of IoT security in the light of the terrible rapid development of the field. of the IoT, as well as the significant and continuous increase in its use in various fields, which has required the protection and achievement of a high level of security to ensure the integrity, confidentiality of data and good quality in the services related to the Internet of Things system, as well as the increase in confidence and the high demand of users in this field, and it is through confronting all the methods of hacking and espionage that threaten the protection of data and information within the system, and this is what we have addressed in our project, where we have created a simple model for a smart home using the NodeMCU 8266 electronic board and we have created a I Android and iOS app interface to control the home.

Regarding the security part of this system, we have linked the smart home and the application using services and platforms that provide many features, the most important of which are security, strict protection and high-level encryption of mobile data and information in IoT system like google firebase services.

Keywords: Internet of Things, smart home, IoT security, remote control, data protection.

Résumé

L'objectif principal de ce travail, qui entre dans le cadre de l'obtention du diplôme master académique, est de se concentrer sur l'étude et l'application de la sécurité de l'IoT à la lumière du terrible développement rapide du domaine de l'IoT, ainsi que de l'augmentation importante et continue de son utilisation dans divers domaines, ce qui a nécessité la protection et la réalisation d'un haut niveau de sécurité pour assurer l'intégrité , la confidentialité des données et une bonne qualité dans les services liés au système Internet des objets, ainsi que l'augmentation de la confiance et de la forte demande des utilisateurs dans ce domaine, et c'est à travers d'affrontement à toutes les méthodes de piratage et espionnage qui menacent la protection des données et des informations au sein du système, et c'est ce que nous avons abordé dans notre projet, où nous avons créé un modèle simple pour une maison intelligente à l'aide de la carte électronique NodeMCU 8266 et nous avons créé une interface d'application Android et iOS pour contrôler la maison.

En ce qui concerne la partie de la sécurité de ce système, nous avons lié la maison intelligente et l'application en utilisant des services et des plates-formes qui offrent de nombreuses fonctionnalités, dont les plus importantes sont la sécurité, la protection stricte et le cryptage de haut niveau des données et des informations mobiles dans le système de l'IoT comme les services de google firebase.

Mots clés : Internet des objets, maison intelligente, sécurité IoT, contrôle à distance, protection des données.