الجمـهورية الجزائرية الديمقراطية الشعبيـة
وزارة التعليم العالي والبحث العلمي
جـامعـة سعـيـدة د. مـولاي الطـاهـر
كلية الرياضيات و الإعلام الآلي و الاتصالات السلكية و اللاسلكية
قسم: الإعلام الآلي

Mémoire de Master en informatique

Spécialité : Réseaux Informatiques et Systèmes Répartis

T h è m e

Simulation of Secure Smart Home Automation System based on the Internet of Things

▪ **Présenté par :**

FELLAH Mustapha Habib

DJELLAT Abderrahmane

▪ **Dirigé par :**

DR.TALEB Fadia

Année universitaire 2024-2025

Remerciements

Avant toute chose, je rends grâce à Allah, Le Tout-Puissant, pour m'avoir accordé la force, la patience et la persévérance nécessaires à la réalisation de ce mémoire.

Je tiens à exprimer ma sincère reconnaissance à mon encadrant, pour ses conseils avisés, son encadrement rigoureux et sa disponibilité tout au long de ce travail.

Je remercie également l'ensemble du corps enseignant du Master Réseaux Informatiques et Systèmes Répartis, pour la qualité de leur encadrement, leur engagement constant et la richesse de l'enseignement dispensé.

Enfin, j'adresse ma gratitude à ma famille, mes amis et camarades, pour leur soutien, leur bienveillance et leur aide précieuse tout au long de ce parcours.

Dédicace

Je dédie ce travail à mes parents, pour leur amour, leurs sacrifices et leur soutien sans faille.

Ma gratitude va également à mes frères, à ma famille et à mes amis proches, pour leur présence et leurs encouragements.

Enfin, je remercie toutes les personnes ayant contribué, de près ou de loin, à la réalisation de ce projet.

Mustapha

Je dédie ce mémoire à :

Mes parents, pour leur amour, leur patience et leur soutien constant.

Ma famille, pour leur présence à chaque étape de mon parcours.

Mes amis, pour leurs encouragements et leur bonne humeur dans les moments difficiles.

À toutes les personnes qui m'ont aidé de près ou de loin,

ce travail est aussi le vôtre.

Abderrahmane

Table des matières

الملخص

مع التطور السريع للتقنيات المتصلة، أصبحت المنازل الذكية القائمة على إنترنت الأشياء (IoT) توفر حلولًا مبتكرة لتحسين الراحة، والأمان، واستقلالية المستخدمين. ومع ذلك، فإن هذا الترابط المتزايد يعرض هذه البيئات لمجموعة من الثغرات والتهديدات السيبرانية.

يعرض هذا البحث تصميم ومحاكاة بنية آمنة لمنزل ذكي باستخدام أداة Cisco Packet Tracer. تم تنفيذ عدة سيناريوهات وظيفية، مثل نظام التحكم في الوصول عبر تقنية RFID، وكشف الحرائق باستخدام متحكم دقيق.

لتأمين البنية التحتية، تم إعداد جدار حماية من نوع ASA باستخدام قوائم التحكم في الوصول (ACL)، كما تم إنشاء شبكة VPN افتراضية ومحاكاة تقسيم الشبكة باستخدام شبكات VLAN. وتبرز هذه الدراسة أهمية اعتماد استراتيجية أمنية متعددة الطبقات لحماية فعالة لبيئات المنازل الذكية المتصلة.

الكلمات المفتاحية : المنزل الذكي، إنترنت الأشياء (IoT)، Cisco Packet Tracer، جدار الحماية ASA، VLAN، VPN، المتحكم الدقيق.

Abstract

With the rapid development of connected technologies, smart homes based on the Internet of Things (IoT) offer innovative solutions to enhance user comfort, security, and autonomy. However, this interconnectivity also exposes these environments to various vulnerabilities and cybersecurity threats.

This thesis presents the design and simulation of a secured Smart Home architecture using Cisco Packet Tracer. Functional scenarios such as RFID-based access control and fire detection using a microcontroller were implemented.

To secure the infrastructure, an ASA firewall was configured with ACLs, a simulated VPN was deployed, and the network was segmented using VLANs. This study highlights the importance of a multilayered security strategy to effectively protect connected smart home environments.

Keywords : Smart Home, Internet of Things (IoT), Cisco Packet Tracer, ASA firewall, ACL, VPN, VLAN, RFID.

Résumé

Avec le développement accéléré des technologies connectées, les maisons intelligentes basées sur l'Internet des Objets (IoT) offrent des solutions innovantes pour améliorer le confort, la sécurité et l'autonomie des usagers. Cependant, cette interconnexion expose ces environnements à diverses vulnérabilités et menaces de cybersécurité.

Ce mémoire présente la conception et la simulation d'une architecture sécurisée de Smart Home en utilisant Cisco Packet Tracer. Des scénarios fonctionnels tels que le contrôle d'accès via RFID et la détection d'incendie à l'aide d'un microcontrôleur ont été implémentés.

Pour sécuriser l'infrastructure, un pare-feu ASA a été configuré avec des ACL, un VPN simulé a été mis en place, et le réseau a été segmenté par VLANs. Cette étude souligne la nécessité d'une stratégie de sécurité multicouche pour protéger efficacement les environnements domotiques connectés.

Mots-clés : Smart Home, Internet des Objets (IoT), Cisco Packet Tracer, pare-feu ASA, ACL, VPN, VLAN, RFID .

Liste des abréviations

- **ACL** – Access Control List
- **ASA** – Adaptive Security Appliance (Cisco firewall)
- **BLE** – Bluetooth Low Energy
- **CLI** – Command Line Interface
- **DHCP** – Dynamic Host Configuration Protocol
- **GUI** – Graphical User Interface
- **HTTP** – Hypertext Transfer Protocol
- **HTTPS** – Hypertext Transfer Protocol Secure
- **IP** – Internet Protocol
- **IoT** – Internet of Things
- **LAN** – Local Area Network
- **LED** – Light Emitting Diode
- **MAC** – Media Access Control (address)
- **MCU** – Microcontroller Unit
- **NAT** – Network Address Translation
- **RFID** – Radio Frequency Identification
- **SSID** – Service Set Identifier
- **VLAN** – Virtual Local Area Network
- **VPN** – Virtual Private Network
- **WPA2** – Wi-Fi Protected Access 2

Liste des figures

Liste des figures

Introduction Générale

À l’ère de la transformation numérique, l’**Internet des Objets (IoT)** s’est imposé comme une technologie pivot, redéfinissant notre manière d’interagir avec les systèmes physiques et numériques. Parmi les nombreuses applications de l’IoT, la **maison intelligente (Smart Home)** se distingue par sa capacité à offrir confort, sécurité et efficacité énergétique à travers l’automatisation des tâches domestiques. Grâce à l’intégration de capteurs, d’actionneurs, d’interfaces vocales et de systèmes connectés, les Smart Homes permettent un contrôle affiné des équipements résidentiels, souvent à distance et en temps réel.

Cependant, cette **connectivité permanente**, si elle constitue un avantage en termes de flexibilité et d'interactivité, introduit également de **nouvelles vulnérabilités**. Chaque objet connecté devient un point d’entrée potentiel pour des attaquants, et la diversité des protocoles, des technologies et des fabricants rend l’environnement difficile à sécuriser de manière homogène. Ainsi, la **sécurité des Smart Homes** est devenue une problématique majeure, à la croisée des enjeux techniques, humains et réglementaires.

Ce mémoire s’inscrit dans cette dynamique, avec pour objectif d’**étudier, simuler et sécuriser une architecture de Smart Home**, en s’appuyant sur des techniques modernes de simulation réseau. L’outil **Cisco Packet Tracer** est utilisé comme environnement de modélisation afin de mettre en œuvre différents scénarios domotiques (comme l’ouverture de porte par badge RFID ou la détection incendie via capteurs), puis de renforcer leur sécurité par l’intégration de composants tels que **VPN, pare-feu ASA, VLANs** .

La structure du mémoire est organisée en trois chapitres principaux :

- Le **premier chapitre** pose les fondements théoriques de l’IoT et des Smart Homes, en explorant leurs architectures, composants, protocoles de communication et domaines d’application.
- Le **deuxième chapitre** se concentre sur les **menaces de sécurité**, les **vulnérabilités** propres aux environnements domotiques, ainsi que les contre-mesures techniques, logiques et comportementales adaptées.
- Le **troisième chapitre**, enfin, présente une **implémentation simulée complète** d’une Smart Home sécurisée, illustrant de manière concrète l’apport des mécanismes de protection étudiés.

À travers cette approche combinant théorie, analyse de risques et simulation, ce travail vise à démontrer que la sécurité des environnements IoT résidentiels peut être significativement améliorée par une conception réseau rigoureuse, des pratiques de configuration adaptées, et l’utilisation judicieuse des outils de cybersécurité.

Chapitre 1:Généralités sur l’IoT et les Smart Homes .

Chapitre 1 : Généralités sur l’IoT et les Smart Homes

1.1 Introduction

L'Internet des Objets (IoT) a révolutionné notre façon d’interagir avec le monde numérique en intégrant des objets physiques à des réseaux intelligents. Parmi ses nombreuses applications, la maison intelligente (Smart Home) se distingue par son potentiel à améliorer le confort, la sécurité et l’efficacité énergétique. Grâce à une combinaison de capteurs, d’assistants vocaux et d’automatisation avancée, les Smart Homes permettent un contrôle à distance et une optimisation des ressources domestiques.

Ce chapitre explore en profondeur l’architecture de l’IoT dans les maisons connectées, les technologies utilisées, ainsi que leurs défis et opportunités. Nous aborderons également les protocoles de communication, les tendances émergentes et les enjeux de cybersécurité liés à cette transformation numérique.

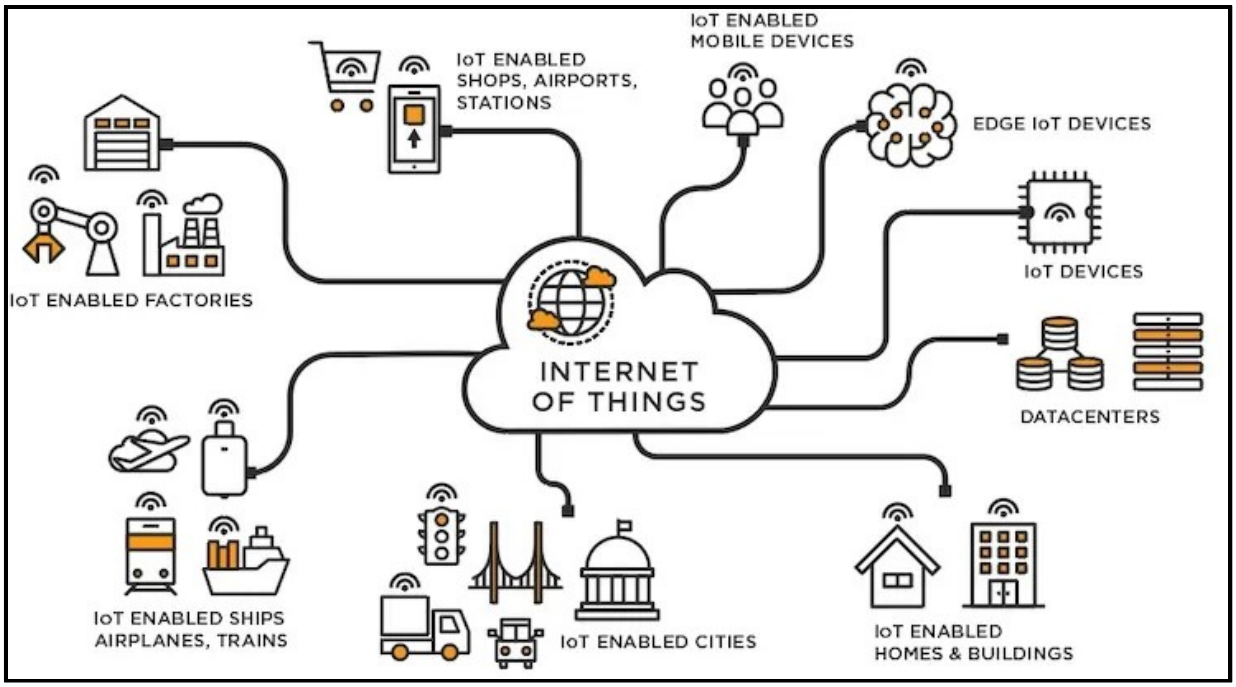


Figure 1: interconnexion du monde de l'Internet Des Objets

1.2 Internet des Objets (IoT)

1.2.1 Définition de l’IoT

- L’Internet des Objets (IoT) désigne un réseau de réseaux qui, grâce à des systèmes d’identification électronique standardisés et sans fil, permet d’identifier, de communiquer et d’échanger des données entre des objets physiques et leurs représentations numériques. L’IoT facilite ainsi la connexion directe et sans ambiguïté d’entités numériques et physiques, permettant la collecte, le stockage, le transfert et le traitement continu des données entre les mondes réel et virtuel.

Au-delà de la simple identification, certains objets deviennent des acteurs autonomes capables de percevoir, analyser et agir dans leurs environnements, souvent via l'intégration d'intelligence artificielle embarquée, distribuée ou dans le Cloud. Ces entités, parfois appelées « cyberobjets », peuvent ainsi intervenir comme assistants, conseillers, décideurs ou organisateurs dans les processus auxquels ils participent.[1]

- L'Internet des objets (IoT) désigne un réseau d'appareils physiques, de véhicules, de dispositifs et d'autres objets physiques disposant de capteurs, de logiciels et d'une connectivité réseau leur permettant de collecter et de partager des données [2].
- L'Internet des objets, abrégé en IoT, est un réseau interconnecté de dispositifs physiques (ordinateurs, capteurs et machines) et de logiciels (applications) qui fonctionnent ensemble pour automatiser et rationaliser les processus. [3].

1.2.2 Historique et évolution

1.2.2.1 Préambule

L'Internet des Objets (IoT - Internet of Things) est une évolution majeure du réseau Internet, qui permet aujourd'hui de connecter des objets physiques à Internet afin qu'ils puissent interagir entre eux et avec les utilisateurs. Ce concept s'inscrit dans une longue tradition d'innovation, issue de la mécanisation, de la standardisation et de l'automatisation du traitement de l'information.

1.2.2.2 Les Premiers Pas : L'Internet des Machines

L'IoT trouve ses origines dans les années 1980, lorsque les premiers dispositifs connectés ont été expérimentés. L'un des premiers exemples concrets remonte à **1982**, avec un distributeur de boissons de l'Université Carnegie-Mellon, capable de signaler son niveau de remplissage et la température de ses boissons via Internet. À cette époque, l'Internet servait principalement à interconnecter des ordinateurs et des serveurs, donnant naissance à ce que certains appelaient l'**Internet des Machines**.

1.2.2.3 L'Émergence des Objets Connectés

Dans les années 1990 et 2000, des avancées technologiques, comme l'introduction des **puces RFID (Radio Frequency Identification)** et le développement du **protocole IP**, ont permis à des objets physiques de communiquer avec des serveurs et entre eux. Cette évolution a conduit à l'émergence du terme **"Internet des Objets"**, popularisé en 1999 par Kevin Ashton, un chercheur du MIT.

C'est à partir de **2008-2009** que l'Internet des Objets a véritablement pris son essor, lorsque le nombre d'objets connectés à Internet a dépassé pour la première fois la population mondiale. L'adoption rapide des smartphones, des capteurs intelligents et des réseaux sans fil a alors favorisé une explosion du nombre d'objets interconnectés. [4]

1.2.2.4 Une Croissance Exponentielle

Depuis les années 2010, l'IoT s'est imposé comme une technologie incontournable. Son application s'est étendue à divers domaines, tels que :

- **L'industrie 4.0**, avec l'automatisation des processus de production.
- **Les villes intelligentes**, optimisant la gestion des transports, de l'énergie et des infrastructures.
- **La santé connectée**, permettant le suivi médical à distance.
- **Les maisons intelligentes**, avec l'intégration d'appareils connectés facilitant la vie quotidienne.

En **2020**, on estimait à plus de **30 milliards** le nombre d'objets connectés, et ce chiffre pourrait atteindre **75 milliards** d'ici **2025**, soit près de **10 objets connectés par habitant** dans le monde.

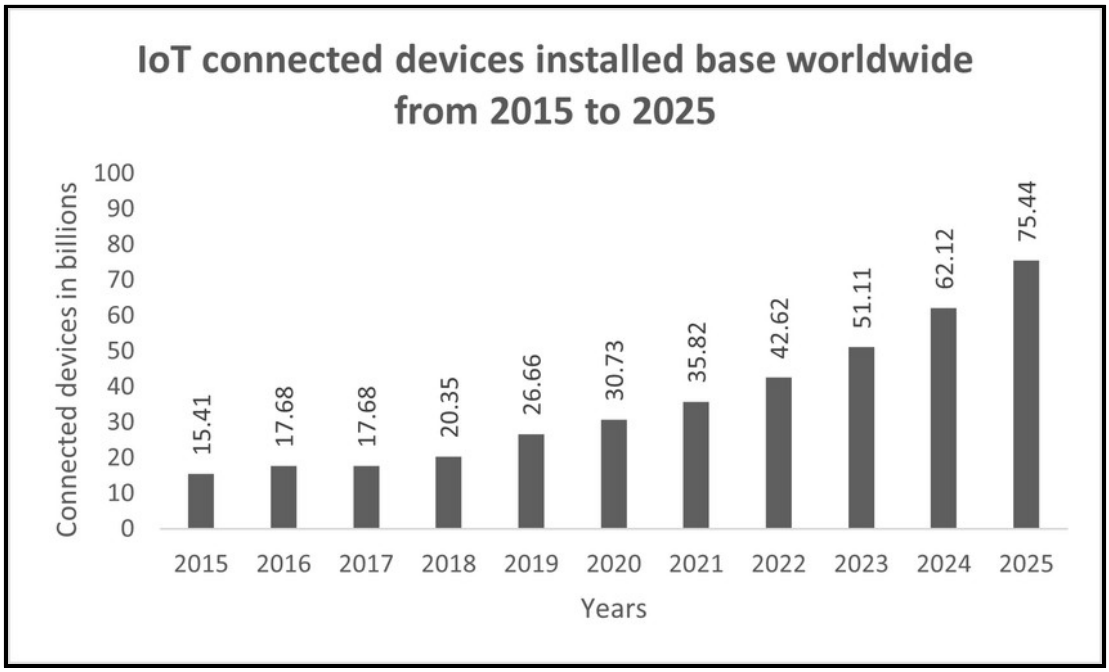


Figure 2 : Évolution des appareils Smart Home au fil du temps

1.2.3 Objectifs de l'IoT

L'Internet des Objets (IoT) cherche à optimiser l'interconnexion des objets physiques pour les rendre intelligents et autonomes dans des secteurs variés tels que la domotique, l'industrie et la santé. Ses objectifs fondamentaux sont orientés vers plusieurs axes stratégiques. D'abord, l'interopérabilité et la communication intelligente, qui visent à intégrer des dispositifs connectés via des protocoles standardisés, permettant ainsi une communication fluide entre équipements hétérogènes et une meilleure coordination des systèmes. Ensuite, l'automatisation et l'efficacité énergétique, qui permettent de réduire la consommation d'énergie par l'optimisation de l'utilisation des appareils, tout en automatisant les tâches répétitives pour améliorer la productivité et le confort des utilisateurs. Un autre objectif clé est l'analyse et l'exploitation des données, où l'IoT collecte des informations en temps réel grâce à des capteurs intelligents et exploite des algorithmes d'intelligence artificielle pour prendre des décisions optimisées, favorisant ainsi une gestion proactive et réactive. Enfin, la sécurisation des données et l'amélioration de l'expérience utilisateur

sont primordiales, en renforçant la protection des informations collectées, en prévenant les cyberattaques, et en offrant des services personnalisés qui améliorent l'interaction entre l'utilisateur et les systèmes connectés.[13]

1.2.4 Fonctionnement et Architecture

a) **Fonctionnement**

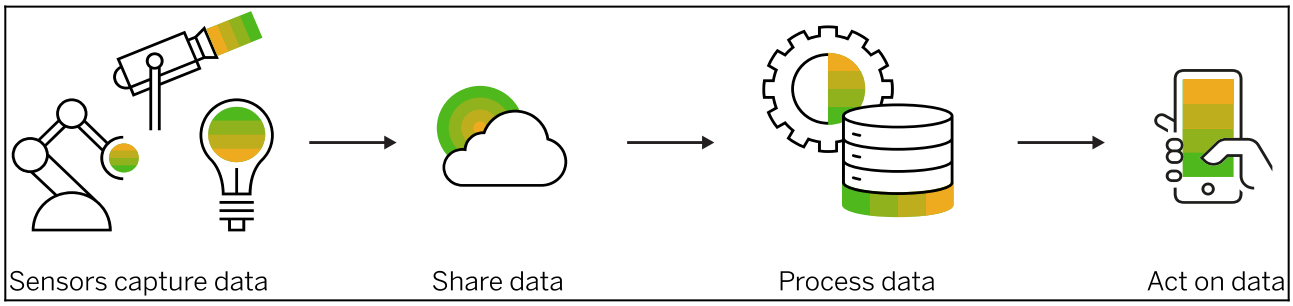


Figure 3 : Fonctionnement de l'IoT *[30]*

Le fonctionnement d'un dispositif IoT peut ainsi être résumé en 4 étapes :

1. **L'acquisition des données :** permise par l'utilisation de capteurs intégrés aux appareils pour collecter des informations sur leur environnement, le fonctionnement de leurs éléments… ce qui peut varier d'une simple mesure de température à une prise de compression sur un moteur
2. **La transmission des données :** une fois les données collectées, celles-ci doivent ensuite être transmises grâce aux réseaux disponibles. Plusieurs options sont possibles, la plus courante étant d'envoyer ces données sur un système cloud (public ou privé), mais elles peuvent également être stockées localement sur un serveur pour un traitement sur place.
3. **Le traitement des données :** à cette étape, des logiciels spécialisés traitent les données recueillies pour déclencher des actions spécifiques, telles que l'émission d'une alerte, ou encore l'activation d'un système auxiliaire.
4. **Action sur les données :** après l'analyse, les décisions prises sont concrètement mises en œuvre par des actionneurs (moteurs, relais, serrures électroniques, etc.) ou traduites sous forme d'alertes, de notifications ou de commandes automatiques. C'est cette étape qui est représentée par « Act on data » dans la Figure 3. Elle permet au système IoT de réagir en temps réel aux événements détectés, fermant ainsi la boucle du processus décisionnel. [5]

b) Architecture de l'IoT [32]

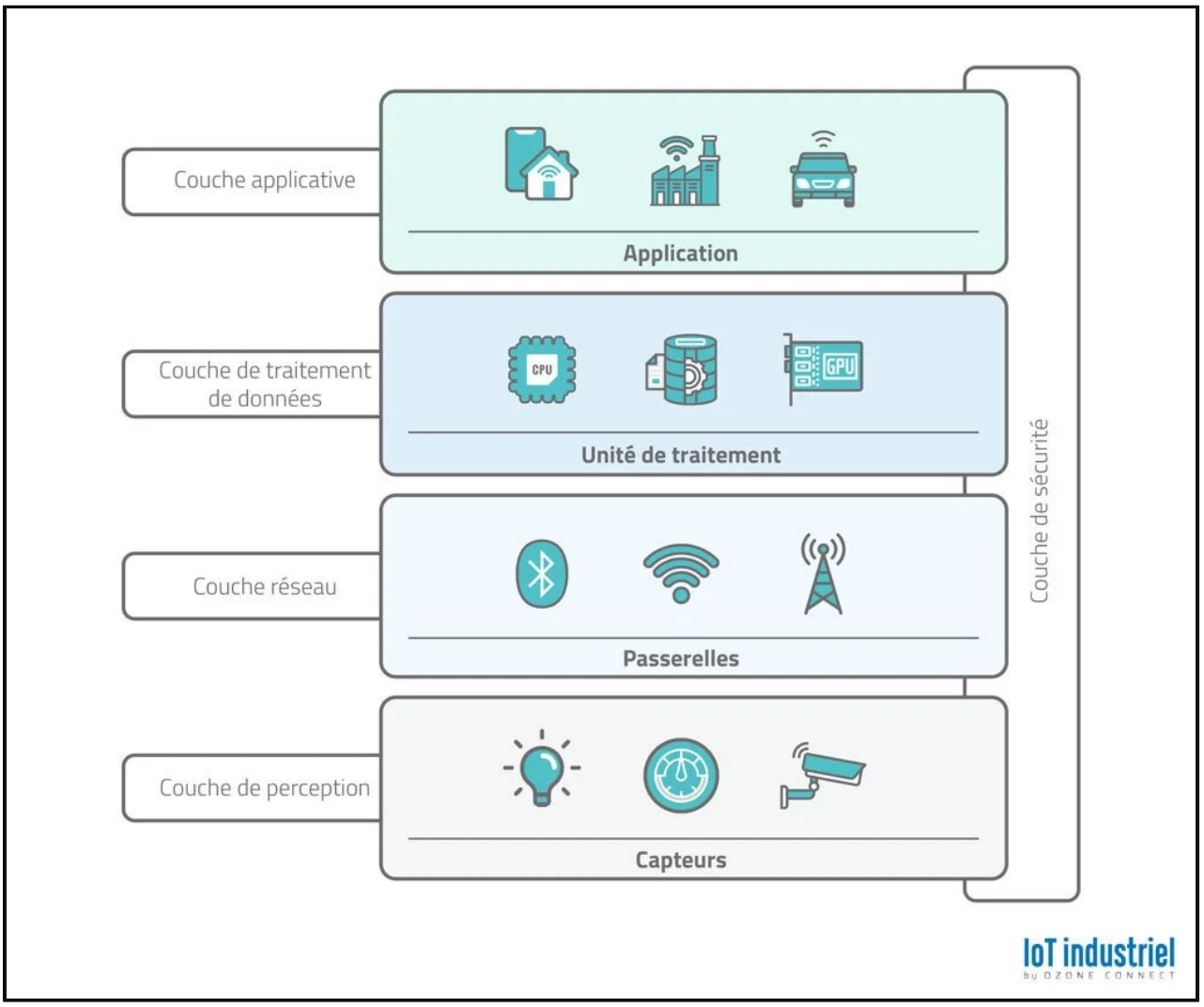


Figure 4 : Architecture de l'IoT [31]

1. **Couche de Perception (Perception Layer)**

La couche de perception constitue le **premier niveau** de l'architecture IoT. Elle est responsable de la **collecte des données** à partir de l'environnement physique à l'aide de **capteurs**, **actionneurs**, et autres dispositifs intelligents.

Principales composantes :

- **Capteurs** : dispositifs permettant de mesurer des paramètres physiques (température, pression, humidité, luminosité, etc.) et de les convertir en signaux électriques .
- **Actionneurs** : dispositifs permettant de transformer un signal numérique en une action mécanique ou électrique, tels que les moteurs et les relais.
- **Technologies d'identification** : RFID (Radio Frequency Identification), NFC (Near Field Communication) permettant l'identification et la communication à courte portée .

2. **Couche Réseau (Network Layer)**

La couche réseau est responsable de **l'acheminement des données** collectées par la couche de perception vers les systèmes de stockage et de traitement. Elle assure la communication entre les dispositifs IoT et les infrastructures informatiques via divers **protocoles et technologies de communication**.

Technologies utilisées :

- **Filaire** : Ethernet, Fibre optique (utilisés dans des infrastructures critiques et industrielles).
- **Sans fil** : Wi-Fi, Bluetooth, Zigbee, etc.
- **Réseaux cellulaires** : 3G, 4G, 5G, avec une latence réduite et une meilleure bande passante pour l'IoT industriel et les villes intelligentes

3. **Couche de Traitement et de Stockage (Processing & Storage Layer)**

Cette couche assure le **traitement, l'analyse et le stockage des données** collectées par les capteurs. Elle repose sur différentes infrastructures informatiques, permettant une gestion optimisée des flux de données.

Principales composantes :

- **Edge Computing** : traitement des données en périphérie du réseau, directement sur les passerelles ou les objets connectés pour réduire la latence et la congestion du réseau.
- **Fog Computing** : intermédiaire entre l'edge et le cloud, permettant une meilleure distribution des ressources de calcul.
- **Cloud Computing** : stockage massif et traitement avancé des données IoT, avec des solutions comme AWS IoT, Microsoft Azure IoT, ou Google Cloud IoT

4. **Couche Applicative (Application Layer)**

La couche applicative représente le **niveau d'interaction utilisateur** et comprend les logiciels et services permettant d'exploiter les données IoT. Cette couche varie selon le domaine d'application et les besoins spécifiques.

Domaines d'application de l'IoT : Domotique ,Santé connectée, Industrie 4.0,Villes intelligentes[6]

1.2.5 *Technologies et protocoles de communication en IoT*

1.2.5.1 Technologies de communication (Wi-Fi, Bluetooth, Zigbee, LoRa, etc.)

Dans l'Internet des Objets (IoT), les protocoles réseau permettent la connectivité et l'échange de données entre les dispositifs connectés. Selon les besoins en portée, en consommation énergétique et en débit, différents protocoles comme Wi-Fi, Bluetooth, Zigbee ou LoRa sont utilisés pour assurer une communication adaptée aux contraintes des objets intelligents

✔ **Wi-Fi**

Le Wi-Fi est une technologie de réseau local sans fil basée sur la norme IEEE 802.11, permettant aux appareils de se connecter à Internet ou de communiquer entre eux sur de courtes distances. Il offre un débit élevé, adapté au transfert de grandes quantités de données, mais consomme généralement plus d'énergie, ce qui peut être une contrainte pour certains dispositifs IoT.

Figure 5 : Logo Wi-Fi

✔ **Bluetooth**

Le Bluetooth, notamment dans sa version Low Energy (BLE), est conçu pour des communications à courte portée avec une consommation énergétique réduite. Il est idéal pour des applications nécessitant des échanges de données sur de faibles distances, comme les appareils portables ou les capteurs personnels.

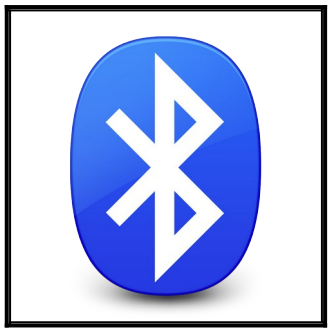


Figure 6 : Logo de Bluetooth

✔ **Zigbee**

ZigBee est une technologie de communication sans fil conçue pour les réseaux personnels à faible consommation énergétique et à faible débit, notamment dans les domaines des capteurs, de l'automatisation domestique et des dispositifs médicaux. Elle repose sur la norme IEEE 802.15.4 et fonctionne dans les bandes de fréquence ISM : 868 MHz en Europe, 915 MHz aux États-Unis et en Australie, 784 MHz en Chine, et 2,4 GHz dans la plupart des autres régions.[7] Sa portée varie généralement entre 10 et 100 mètres en ligne de mire, avec un débit allant de 20 kbit/s (en 868 MHz) à 250 kbit/s (en 2,4 GHz). Les réseaux ZigBee sont souvent plus économiques que les technologies comme le Wi-Fi ou le Bluetooth. Ils sont utilisés dans de nombreuses applications telles que les interrupteurs d'éclairage sans fil, les compteurs intelligents, ou encore la surveillance d'équipements industriels..

Le choix entre ces protocoles dépend des besoins spécifiques de l'application IoT, tels que la portée, la consommation énergétique et le débit de données requis

Figure 7 : Logo de Zigbee

1.2.5.2 Protocoles de communication l'IoT : MQTT et CoAP

Dans l'Internet des Objets (IoT), la communication entre dispositifs repose sur des protocoles de transport adaptés aux contraintes des appareils connectés. Parmi ces protocoles, **MQTT** et **CoAP** sont largement utilisés.

- **MQTT (Message Queuing Telemetry Transport)**

MQTT est un protocole léger basé sur un modèle publication/abonnement, conçu pour les environnements à faible bande passante et les appareils à ressources limitées. Il fonctionne au-dessus de TCP/IP et utilise un courtier pour gérer la distribution des messages entre les clients. [14]Sa simplicité et son efficacité en font un choix privilégié pour les applications IoT nécessitant une communication fiable avec une surcharge minimale.

Fonctionnement

MQTT repose sur un **modèle publication/abonnement (Publish/Subscribe)** qui fonctionne de la manière suivante :

1. **Connexion au courtier** : Chaque client MQTT (éditeur ou abonné) établit une connexion avec un **courtier (broker)** en utilisant le protocole TCP/IP.
2. **Publication d'un message** : Un client éditeur envoie un message sur un sujet (**topic**) spécifique au courtier.
3. **Distribution du message** : Le courtier reçoit le message et l'achemine aux clients abonnés au même topic.
4. **Réception par les abonnés** : Tous les clients abonnés reçoivent le message transmis par le courtier.
5. **Gestion de la qualité de service (QoS)** : MQTT propose trois niveaux de qualité de service pour garantir la livraison des messages :
    - *QoS 0* (*At most once*) : Envoi sans garantie de réception.
    - *QoS 1* (*At least once*) : Message livré au moins une fois avec accusé de réception.
    - *QoS 2* (*Exactly once*) : Message livré exactement une fois, avec un mécanisme de confirmation plus robuste

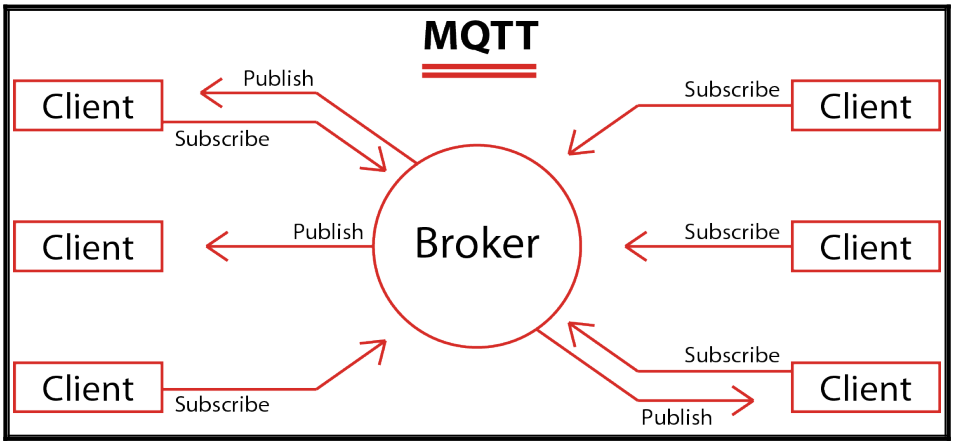


Figure 8 : Protocole MQTT

- **CoAP (Constrained Application Protocol)**

CoAP est un protocole de communication conçu pour les appareils contraints, fonctionnant au-dessus de UDP. Il suit une architecture RESTful similaire à HTTP, permettant des opérations CRUD avec une faible surcharge. CoAP est particulièrement adapté aux réseaux où la consommation de bande passante et d'énergie doit être minimisée, tout en assurant une communication efficace entre les dispositifs IoT.

Fonctionnement

CoAP repose sur un **modèle client/serveur** qui fonctionne comme suit :

1. **Envoi d'une requête** : Un client envoie une requête (GET, POST, PUT ou DELETE) à un serveur CoAP pour interagir avec une ressource.
2. **Transmission via UDP** : La requête est encapsulée dans un **datagramme UDP**, ce qui permet une transmission rapide avec une surcharge minimale.
3. **Traitement par le serveur** : Le serveur CoAP reçoit la requête, la traite et prépare une réponse.
4. **Envoi de la réponse** : Le serveur renvoie un message contenant soit la ressource demandée, soit un accusé de réception.
5. **Mode d'observation (Observer Pattern)** : Contrairement à HTTP, CoAP permet aux clients de **s'abonner à une ressource** et de recevoir des mises à jour automatiques en cas de modification. [10]
6. **Gestion de la fiabilité** :
    - *Messages confirmables (CON)* : Le client attend une réponse du serveur pour s'assurer de la bonne réception.
    - *Messages non-confirmables (NON)* : Utilisés pour les transmissions rapides où la fiabilité n'est pas critique.

Ces deux protocoles offrent des solutions efficaces pour la communication dans des environnements IoT variés, en fonction des besoins spécifiques en termes de ressources et de fiabilité.

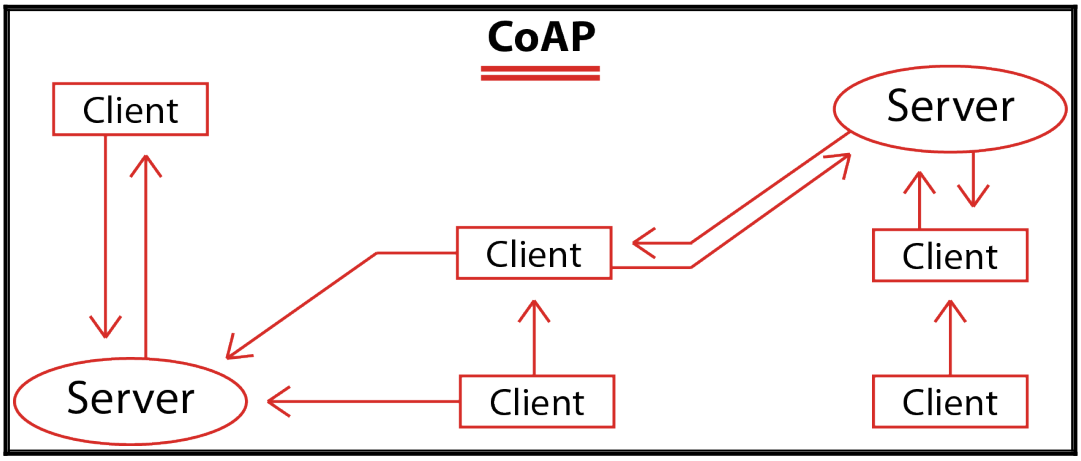


Figure 9 : Protocole CoAP

1.2.6 Domaines d'application de l'IoT

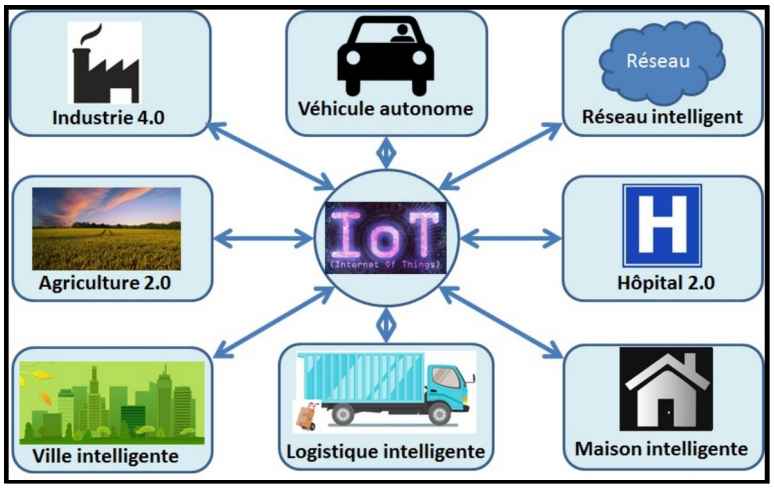


Figure 10 : Domaines d'application de l'IoT

L'Internet des Objets (IoT) a révolutionné de nombreux secteurs en permettant une connectivité avancée et une automatisation intelligente. Grâce à l'intégration de capteurs, d'actuateurs et d'intelligence artificielle, l'IoT optimise l'efficacité des infrastructures et améliore la qualité de vie des utilisateurs. Voici les principaux domaines d'application de l'IoT avec des exemples concrets.

1.2.6.1 Transport intelligent et logistique

L'Internet des Objets (IoT) transforme en profondeur le secteur des transports, en rendant les systèmes plus intelligents, plus sûrs et plus efficaces. Grâce à la connectivité embarquée, les véhicules modernes peuvent surveiller en temps réel leur environnement, anticiper les dangers et adapter leur trajectoire. Les capteurs, modules de communication et logiciels embarqués permettent une circulation plus fluide, une réduction des accidents, et une meilleure gestion des itinéraires.[40]

Dans le domaine de la logistique, l'IoT révolutionne également les pratiques. Le suivi des marchandises en temps réel, via des technologies comme le GPS et la RFID, offre une visibilité accrue sur toute la chaîne d'approvisionnement. Cette traçabilité améliore la gestion des stocks, limite les erreurs et permet aux entreprises de réagir rapidement aux imprévus, tout en optimisant les coûts et les délais de livraison.

1.6.6.2 Santé et e-santé

L'IoT permet la surveillance à distance de la santé et les systèmes de notification d'urgence. Une approche très populaire consiste à utiliser des techniques portables. Ces appareils portables peuvent collecter une gamme de données de santé, telles que la fréquence cardiaque, la température corporelle et la pression artérielle, qui peuvent ensuite être transmises sans fil à un site distant pour le stockage et une analyse plus approfondie. Cela permet également à la télésanté/télémédecine, c'est-à-dire de diagnostiquer ou de traiter les patients à distance [8]

1.2.6.3 Industrie et automatisation

L'intégration de l'IoT dans le secteur industriel est communément désignée sous le terme **Industrie 4.0**, **représentant a quatrième révolution industrielle**.
La première révolution industrielle, au XVIIIe siècle, a été marquée par l'introduction de la machine à vapeur, mécanisant ainsi la production. La deuxième, au XIXe siècle, a vu l'essor de la production de masse grâce à l'électricité. La troisième révolution, dite **numérique**, est survenue à la fin du XXe siècle avec l'apparition de l'électronique et de l'informatique, permettant une automatisation avancée.
L'Industrie 4.0 s'appuie sur des **systèmes cyber-physiques** dans lesquels les machines, les capteurs, les logiciels et les réseaux Internet interagissent de manière intelligente et autonome. Cette nouvelle ère industrielle donne naissance à des **usines intelligentes**, capables d'**auto-optimisation**, **d'auto-configuration**, voire d'intégrer des fonctionnalités d'**intelligence artificielle** pour exécuter des tâches complexes. L'objectif est de générer des gains de productivité significatifs tout en améliorant la qualité des biens et services fournis [9]

1.2.6.4 Ville intelligente (Smart City)

L'Internet des objets (IoT) représente aujourd'hui un élément clé dans l'évolution des environnements urbains vers des modèles intelligents. Déployée dans plusieurs grandes villes à travers le monde, cette technologie intégrée dans les infrastructures urbaines permet le développement de services numériques innovants, qui transforment en profondeur la gestion des espaces publics et des ressources. Elle repose sur une approche collaborative qui vise à offrir aux citoyens un cadre de vie plus confortable, plus sûr et plus durable[29], tout en réduisant les coûts énergétiques et les pertes liées à une gestion inefficace.

L'un des objectifs majeurs de cette transformation est de centraliser et d'optimiser la gestion des réseaux essentiels tels que ceux de l'eau, de l'électricité ou du gaz. Pour y parvenir, les villes intelligentes exploitent un large éventail de fonctionnalités basées sur l'IoT, notamment :

- la mesure des rayonnements électromagnétiques générés par les équipements de communication sans fil,
- la surveillance de l’état des structures comme les ponts ou les bâtiments,
- la gestion optimisée des déchets par détection du remplissage des conteneurs,
- l’identification d’appareils mobiles à travers les signaux Wi-Fi ou Bluetooth,
- la mise en place de routes intelligentes, capables d’adapter la signalisation aux conditions météorologiques ou aux incidents,
- la régulation du stationnement grâce à la détection en temps réel des places disponibles,
- l’éclairage public adaptatif, ajusté selon la luminosité ambiante et la présence humaine,
- la gestion dynamique du trafic, fondée sur la surveillance des flux de piétons et de véhicules,
- et la cartographie sonore, pour surveiller le niveau de bruit dans différentes zones de la ville.

Ces systèmes s’appuient sur des réseaux de capteurs interconnectés capables de collecter et d’analyser des données en continu. Ces informations offrent aux gestionnaires urbains comme aux citoyens de nouvelles opportunités pour créer des services personnalisés, améliorer la réactivité des infrastructures et construire des villes plus durables. L’IoT s’affirme ainsi comme un levier essentiel pour répondre aux défis des métropoles modernes et améliorer le quotidien de leurs habitants.

1.2.6.5 Maison connectée (Smart Home)

L’Internet des Objets (IoT) joue un rôle essentiel dans l’évolution des espaces résidentiels et professionnels en apportant confort, sécurité et performance énergétique. Dans les habitations intelligentes, l’automatisation des équipements devient centrale : les assistants vocaux et les applications mobiles permettent de piloter à distance l’éclairage, le chauffage ou les appareils électroménagers, simplifiant ainsi la gestion quotidienne. [27]

La sécurité est également renforcée grâce à l’intégration de caméras connectées et de capteurs de mouvement, qui assurent une surveillance en temps réel et une détection rapide des anomalies. Enfin, la gestion intelligente de l’énergie, rendue possible par des systèmes capables d’ajuster automatiquement la climatisation ou l’éclairage en fonction des besoins, permet de réduire significativement la consommation et les coûts associés.

1.2.6.6 Agriculture intelligente

L’Internet des Objets (IoT) joue un rôle stratégique dans la modernisation du secteur agricole, en permettant une gestion plus précise, durable et automatisée des exploitations. Grâce aux capteurs intelligents, il est désormais possible de surveiller en temps réel l’état des cultures, la qualité du sol ou encore la santé du bétail.

Dans les champs, des dispositifs IoT mesurent en continu des paramètres clés comme l’humidité, la température ou la concentration en nutriments. Ces données permettent d’optimiser l’irrigation, de

limiter l'usage des intrants chimiques et d'augmenter les rendements tout en réduisant l'impact environnemental.[41]

Dans l'élevage, des capteurs portés par les animaux permettent de suivre leur comportement, leur activité physique et leurs constantes biologiques. Cette surveillance intelligente facilite la détection précoce des maladies, améliore le bien-être animal et renforce la productivité globale de l'exploitation.

1.3 Smart Home

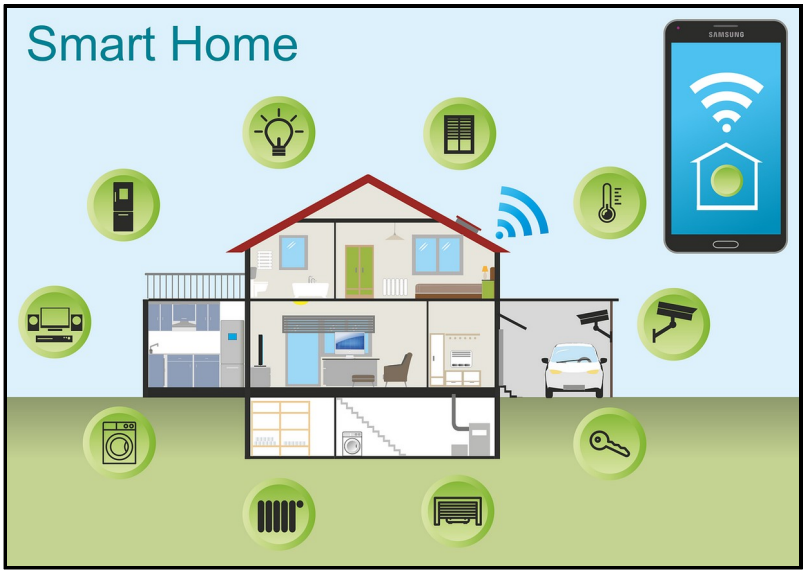


Figure 11 : Représentation d'une maison intelligente (Smart Home)

1.3.1 Définition des Smart Homes

Une **Smart Home** (maison intelligente) est une habitation équipée de dispositifs connectés permettant l'automatisation, le contrôle et la gestion à distance de divers systèmes domestiques tels que l'éclairage, le chauffage, la sécurité et les appareils électroménagers. Ces technologies reposent sur l'Internet des Objets (IoT), l'intelligence artificielle (IA) et le Cloud Computing pour offrir confort, sécurité et efficacité énergétique aux utilisateurs.

Définition renforcée :

"Une maison intelligente est une résidence intégrant de manière transparente des technologies de calcul, de communication, de capteurs et d'actionneurs, qui permettent la surveillance en temps réel, l'automatisation intelligente et le contrôle efficient des fonctions résidentielles. L'objectif est d'optimiser la qualité de vie des résidents, tout en améliorant la durabilité énergétique et la sécurité de l'habitat.[11]

1.3.2 Différences entre la domotique traditionnelle et les Smart Homes

La **domotique traditionnelle** repose sur des infrastructures rigides, souvent basées sur des connexions **filaire** (bus ou relais électriques), et des **systèmes centralisés** à logique fixe. L'automatisation y est généralement limitée à des scénarios simples (ex. : allumage de l’éclairage à une heure donnée) contrôlés localement via des **interrupteurs muraux** ou **télécommandes infrarouges**. Ce type d’installation opère en **circuit fermé**, sans connectivité externe, ce qui **réduit l’interopérabilité** entre dispositifs de marques différentes et **complique toute extension ou reconfiguration** du système.

À l’opposé, une **Smart Home** moderne s’appuie sur les technologies de l’**Internet des Objets (IoT)** et sur des capacités **d’analyse intelligente** pour offrir une automatisation contextuelle, évolutive et sécurisée. Les équipements sont connectés entre eux via des **protocoles de communication sans fil** comme **Wi-Fi**, **Zigbee**, **Z-Wave** ou **Matter**, facilitant leur **intégration modulaire** et leur **contrôle à distance**.

La Smart Home permet une **gestion centralisée via des applications mobiles**, des **interfaces graphiques personnalisées**, ou encore **des assistants vocaux** (Google Assistant, Amazon Alexa, Apple Siri), offrant ainsi une **expérience utilisateur fluide, intuitive et intelligente**. L’automatisation est également enrichie par l’**intelligence artificielle**, permettant des scénarios dynamiques fondés sur l’analyse des comportements, la géolocalisation, les conditions environnementales ou les routines de l'utilisateur.

En résumé, alors que la domotique traditionnelle privilégie la stabilité et la simplicité, la Smart Home se distingue par sa **flexibilité**, son **interopérabilité étendue** et sa capacité à **s’adapter aux besoins évolutifs** des utilisateurs.[11]

1.3.3 Composants d’une Maison Intelligente

Une architecture domotique repose sur l’interopérabilité de plusieurs catégories d’équipements, chacun jouant un rôle spécifique dans l’acquisition de données, l’exécution d’actions et l’interface utilisateur. Les sous-sections suivantes détaillent les principaux composants.

1.3.3.1 Dispositifs connectés

Les dispositifs connectés constituent la couche périphérique de l’écosystème domotique. Ils sont déployés dans l’environnement domestique pour collecter les données physiques (capteurs), exécuter des actions automatiques (actionneurs) et interagir avec les contrôleurs ou hubs via des protocoles comme Zigbee, Z-Wave, BLE ou Wi-Fi. Ils forment la base de l’automatisation intelligente.

Capteurs

Les capteurs assurent une fonction d’observation continue de l’environnement. Leur rôle est de remonter des données précises qui déclenchent ensuite des règles d’automatisation prédéfinies au niveau du contrôleur.

- **Capteurs de mouvement** : Utilisant des technologies infrarouges passives (PIR), ils détectent une présence humaine et permettent d'activer automatiquement l'éclairage, les caméras de surveillance ou les alarmes.
- **Capteurs environnementaux** : Incluent des sondes de température, d'humidité et de qualité de l'air. Ils permettent, par exemple, d'activer la climatisation, d'ouvrir des fenêtres motorisées ou d'ajuster un purificateur d'air.

Figure 12 : Capteurs environnementaux

- **Capteurs de luminosité** : Mesurent l'intensité lumineuse naturelle. Ils permettent de moduler l'éclairage intérieur pour maximiser l'efficacité énergétique, en éteignant les lampes lorsqu'il fait jour ou en adaptant l'intensité en soirée.
- **Détecteurs de fumée, de gaz et de fuite d'eau** : Ces dispositifs utilisent des technologies comme l'ionisation ou la détection électrochimique pour repérer des anomalies dangereuses (fumées, monoxyde de carbone, gaz domestique, fuite d'eau). Lorsqu'une alerte est générée, des mécanismes automatisés sont déclenchés, tels que la fermeture des électrovannes, l'envoi d'une alerte mobile ou le déclenchement d'une alarme sonore .

Ces capteurs communiquent généralement via des protocoles à faible consommation (Zigbee, Z-Wave) et sont conçus pour fonctionner en maillage afin d'étendre leur couverture et de renforcer la tolérance aux pannes.

Actionneurs

Les actionneurs reçoivent des commandes de la part du contrôleur central ou de l'utilisateur et interagissent physiquement avec l'environnement.

- **Prises et interrupteurs intelligents** : Permettent de piloter l'alimentation électrique des équipements domestiques. Ils peuvent être programmés pour fonctionner selon des horaires précis, des scénarios domotiques ou des conditions environnementales.

- **Moteurs pour volets et stores** : Utilisés pour automatiser l’ouverture et la fermeture des rideaux, stores ou volets roulants. Ils s’intègrent généralement à des scénarios dictés par la météo, la température intérieure, l’ensoleillement ou la présence.
- **Serrures connectées** : Intègrent des méthodes d’authentification avancées (codes PIN, cartes RFID, biométrie ou Bluetooth) pour contrôler l’accès aux espaces résidentiels. Elles peuvent être monitorées à distance, générer des journaux d'accès et s’intégrer dans des règles de sécurité avancées.

Ces actionneurs jouent un rôle déterminant dans la concrétisation physique des règles logiques définies dans le système de gestion domotique

Appareils connectés

Ces appareils intègrent des fonctions de communication et peuvent être contrôlés ou automatisés :

- **Éclairage intelligent** : Ampoules connectées permettant la variation d’intensité ou de couleur selon des scénarios préprogrammés.
- **Électroménagers intelligents** : Appareils tels que réfrigérateurs, fours ou lave-linge, optimisant la consommation d’énergie et pouvant être pilotés à distance .

1.3.3.2 Hubs domotiques

Les **hubs domotiques** jouent un rôle central dans la gestion d’une maison intelligente. Ils assurent la **centralisation des communications** entre les dispositifs connectés, tout en garantissant une **compatibilité multi-protocoles**. Cette capacité est essentielle car les objets connectés peuvent utiliser différents standards sans fil (Zigbee, Z-Wave, Wi-Fi, Bluetooth).

- **Samsung SmartThings** :

  Compatible avec Zigbee, Z-Wave et Wi-Fi, SmartThings permet une gestion unifiée et fluide de nombreux périphériques, quels que soient leurs protocoles natifs. Cette interopérabilité facilite la création d’automatisations complexes dans un même écosystème.

- **Apple HomeKit** :

  Intégré à l’écosystème iOS, HomeKit offre une interface sécurisée pour la configuration et le contrôle des équipements compatibles. Sa force réside dans la simplicité d’utilisation et la robustesse de son architecture en termes de confidentialité .

- **Google Nest Hub**

  Exploitant Google Assistant, ce hub propose un contrôle vocal intuitif et une automatisation intelligente basée sur l’apprentissage contextuel, améliorant ainsi l’expérience utilisateur dans la maison connectée.

1.3.3.3 Contrôleurs locaux

Les **contrôleurs locaux** permettent de gérer les dispositifs domotiques directement au sein du réseau domestique, sans dépendre d'une connexion Internet ou de serveurs cloud externes. Ce modèle est privilégié pour garantir **sécurité**, **confidentialité** et **fiabilité**.

- **Home Assistant** :

  Plateforme open-source, extensible et très flexible, Home Assistant permet la création d'automatisations avancées et offre une interface web et mobile hautement personnalisable. Son exécution locale garantit que les données sensibles ne quittent pas le domicile.

- **OpenHAB** :
  Système modulaire, OpenHAB supporte une large gamme de dispositifs de différents fabricants tout en assurant une gestion locale des commandes et scénarios. Son architecture ouverte favorise l'intégration personnalisée et la durabilité des solutions domotiques.

1.3.3.4 Passerelles de communication

Figure 13 : iot home gateway

Les **passerelles de communication** servent d'interfaces techniques entre les protocoles spécifiques aux objets connectés (souvent des protocoles basse couche, comme Zigbee) et les réseaux IP utilisés pour la communication à plus haut niveau.

- **Exemple** : La **passerelle Philips Hue** convertit les signaux Zigbee des ampoules intelligentes en trames IP, permettant leur contrôle via smartphone ou assistants vocaux. Cette conversion est indispensable pour intégrer des équipements à des réseaux domestiques standards.

1.3.3.5 Interfaces utilisateur

Pour garantir une interaction efficace entre les occupants et le système domotique, plusieurs types d'interfaces sont déployés :

Applications mobiles

- **Google Home** :

Centralise le contrôle des appareils compatibles via Google Assistant, offrant une interface simple pour gérer à distance l'ensemble des équipements.

- **Apple Home** :

  Intégrée nativement dans iOS, cette application permet une gestion fluide des appareils HomeKit avec une ergonomie soignée.

Assistants vocaux

- **Amazon Alexa** :

  Large compatibilité avec des milliers d'appareils tiers, Alexa offre un contrôle vocal naturel et intuitif, facilitant l'accès aux fonctions domotiques sans interface physique.

- **Google Assistant** :

  Profondément intégré aux produits Google, il permet des automatisations contextuelles basées sur les habitudes et l'environnement de l'utilisateur.

- **Apple Siri** :

  Grâce à une intégration sécurisée dans l'écosystème Apple, Siri assure une interaction vocale fluide tout en respectant la confidentialité des données.

Interfaces graphiques

- **Écrans tactiles muraux** :

  Installés dans des solutions haut de gamme (ex. : Control4, Crestron), ils fournissent un point de contrôle centralisé et accessible à tout moment dans la maison.

- **Tableaux de bord personnalisés** :

  Avec des plateformes comme Home Assistant, il est possible de créer des interfaces graphiques sur mesure, adaptées aux besoins spécifiques des utilisateurs, offrant à la fois visualisation et contrôle précis des équipements .

1.3.4 Cas d'Usage et Applications Pratiques

1.3.4.1Gestion de l'énergie et efficacité énergétique

Les maisons intelligentes exploitent des technologies avancées pour **optimiser la consommation énergétique, réduire les coûts et améliorer l'efficacité globale**. En intégrant des capteurs, des actionneurs et des algorithmes d'intelligence artificielle, ces systèmes adaptent automatiquement l'utilisation de l'électricité en fonction des habitudes et des besoins des occupants.

Innovations majeures :

- **Thermostats intelligents** : Ajustent la température intérieure en analysant les habitudes des résidents et les conditions environnementales, permettant ainsi une réduction significative de la consommation énergétique .
- **Énergies renouvelables et Smart Grid** : Associent des panneaux solaires et des batteries domestiques pour optimiser la production et l'autoconsommation d'électricité. Grâce à leur intégration aux réseaux électriques intelligents, ces systèmes facilitent une gestion dynamique de l'énergie, réduisant ainsi la dépendance au réseau traditionnel.

1.3.4.2 Sécurité et Surveillance Connectée

L'intégration de technologies intelligentes dans les maisons connectées permet d'améliorer **la sécurité des occupants et la protection des biens** grâce à des systèmes autonomes et interconnectés. Ces solutions offrent une surveillance en temps réel, un contrôle à distance et une réactivité accrue face aux menaces potentielles.

Principales innovations :

- **Systèmes d'alarme et détection de présence** : Utilisation de capteurs de mouvement, d'ouverture de porte et de fenêtres pour identifier toute intrusion et déclencher une alerte en temps réel.
- **Caméras intelligentes et reconnaissance faciale** : Surveillance avancée avec enregistrement automatique, détection des visages et notifications instantanées en cas d'activité suspecte.

1.3.4.3Automatisation et Confort au Quotidien

L'automatisation des maisons intelligentes vise à **simplifier le quotidien des occupants** en assurant une gestion fluide et intuitive des équipements domestiques. Grâce à l'intelligence artificielle et aux objets connectés, les Smart Homes offrent **un environnement personnalisé et adaptatif** selon les préférences des utilisateurs.

Fonctionnalité clé :

- **Gestion centralisée des appareils** : Commande unifiée des téléviseurs, systèmes audio, électroménagers et autres équipements via une application mobile ou un assistant vocal.

1.3.4.4 Santé et Bien-être dans les Smart Homes

Les maisons intelligentes intègrent des technologies avancées pour **assurer le suivi de la santé et du bien-être des occupants**. Grâce aux objets connectés et à l'intelligence artificielle, les Smart Homes offrent un **environnement sécurisé et adapté aux besoins médicaux**, en particulier pour les personnes âgées ou souffrant de maladies chroniques.

Fonctionnalité clé

- **Monitoring de la santé** : Suivi en temps réel des signes vitaux (fréquence cardiaque, tension artérielle, taux de glucose) grâce à des capteurs portables et des dispositifs connectés.

1.3.5 Défis des Smart Homes

Les maisons intelligentes offrent de nombreux avantages, mais elles présentent également plusieurs défis liés à la **technologie, la sécurité, l'environnement, les coûts et la fiabilité**.

1.3.5.1 Contraintes techniques des équipements IoT

Les équipements IoT utilisés dans les environnements Smart Home sont généralement conçus pour maximiser l'efficacité énergétique, réduire les coûts et conserver une taille minimale. Ces choix d'optimisation imposent plusieurs limitations techniques majeures, impactant directement l'implémentation de mécanismes de sécurité réseau avancés.

- **Capacités limitées en calcul et en mémoire** : La majorité des dispositifs IoT embarquent des microcontrôleurs à faible consommation, comme l'ESP8266, l'ESP32 ou des ARM Cortex-M, dotés de quelques centaines de kilooctets de mémoire vive (RAM) et d'une capacité de calcul très réduite (souvent inférieure à 200 MHz). Ces ressources limitées rendent difficile le déploiement de protocoles lourds comme TLS 1.3, l'utilisation de bibliothèques cryptographiques modernes (ECC, AES-256), ou encore la génération dynamique de trafic dummy. Les algorithmes à complexité élevée peuvent entraîner un ralentissement du fonctionnement normal de l'appareil, voire des plantages.[12]
- **Autonomie énergétique restreinte** : De nombreux objets connectés fonctionnent sur batterie (capteurs de température, détecteurs de mouvement, caméras sans fil, etc.). L'exécution continue de tâches telles que le chiffrement fort, la transmission régulière de données chiffrées ou l'injection de trafic artificiel pour brouiller les métadonnées réseau engendre une consommation énergétique non négligeable. Cela réduit considérablement la durée de vie de la batterie, ce qui est incompatible avec des usages domestiques nécessitant autonomie et fiabilité sur plusieurs mois.
- **Systèmes d'exploitation embarqués minimalistes** : Les objets IoT reposent souvent sur des systèmes comme FreeRTOS, Contiki, Zephyr ou TinyOS. Ces OS embarqués offrent des fonctionnalités de base, mais ne prennent pas toujours en charge les piles de protocoles de sécurité avancés. Par exemple, l'implémentation native du DNS chiffré (DoH/DoT) ou de TLS avec chiffrement ECC n'est pas systématiquement disponible, ou nécessite un portage manuel complexe. Cette contrainte limite la capacité de ces dispositifs à interagir avec des services modernes utilisant des protocoles sécurisés récents.

1.3.5.2 Complexité technologique et interopérabilité

- **Écosystèmes fermés** : Apple HomeKit, Google Home et Amazon Alexa ne sont pas toujours compatibles entre eux, limitant la flexibilité des utilisateurs.

- **Multiplicité des protocoles** : Z-Wave, Zigbee, Thread et autres nécessitent des passerelles pour fonctionner ensemble, rendant l’installation plus complexe.
- **Fragmentation du marché** : L’absence de standardisation oblige les utilisateurs à choisir un écosystème, réduisant l’interopérabilité entre appareils.

1.3.5.3 Sécurité et confidentialité des données

La sécurité et la confidentialité des données constituent des enjeux majeurs dans les environnements de maisons intelligentes, où de nombreux dispositifs IoT collectent, stockent et transmettent des informations sensibles.

- **Vulnérabilités des appareils IoT :**

  De nombreux équipements connectés présentent des faiblesses structurelles en matière de sécurité. Il est fréquent que ces appareils soient livrés avec des identifiants par défaut (par exemple, "admin/admin"), rarement modifiés par les utilisateurs. De plus, certains fabricants n'assurent aucun suivi logiciel, laissant les firmwares obsolètes sans correctifs de sécurité. Ces failles peuvent être exploitées par des attaquants pour accéder au réseau local, manipuler les appareils ou intercepter les données transmises.

- **Risque de cyberattaque**

  Les objets connectés peuvent devenir des points d'entrée privilégiés pour les cybercriminels. Des attaques notoires comme Mirai ont montré comment des milliers de dispositifs mal sécurisés (caméras, routeurs, capteurs) peuvent être détournés pour constituer des botnets et mener des attaques DDoS massives. D'autres attaques visent la prise de contrôle de serrures connectées, l'écoute audio/vidéo, ou l'altération de scénarios domotiques (par exemple, extinction d'alarmes, déverrouillage de portes).

- **Conformité réglementaire** :

  Dans l'Union européenne, le Règlement Général sur la Protection des Données (RGPD) impose un cadre strict pour la collecte, le traitement et le stockage des données personnelles. Les fabricants et intégrateurs de solutions IoT doivent garantir la minimisation des données collectées, l'obtention du consentement explicite des utilisateurs, la sécurisation des flux (via chiffrement, anonymisation), et la traçabilité des opérations. Le non-respect de ces exigences peut entraîner des sanctions lourdes et nuit à la confiance des utilisateur

1.3.5.4 Impact environnemental et consommation énergétique

Déchets électroniques : L’obsolescence rapide des équipements génère un volume important de déchets électroniques, souvent difficiles à recycler.

- **Consommation énergétique** : Les appareils connectés continuent de consommer de l’énergie même en mode veille, ce qui augmente leur empreinte énergétique.
- **Matériaux non durables** : La fabrication des objets connectés utilise fréquemment des plastiques et composants peu recyclables, ce qui réduit leur durabilité environnementale.

1.3.5.5 Coûts et accessibilité

- **Prix élevé** : Les équipements domotiques restent coûteux, limitant leur adoption par le grand public.
- **Complexité d'installation** : Certaines solutions nécessitent des compétences techniques, rendant leur mise en place difficile sans assistance professionnelle.
- **Fracture numérique** : Les personnes âgées ou peu familiarisées avec la technologie peuvent être exclues de ces innovations.

1.3.5.6 Fiabilité et maintenance

- **Pannes techniques** : Les objets connectés peuvent tomber en panne ou devenir obsolètes rapidement, nécessitant des remplacements fréquents.
- **Dépendance au cloud** : En cas de panne Internet, certains services deviennent inutilisables, affectant le fonctionnement global de la maison.
- **Mises à jour et compatibilité** : Les fabricants abandonnent parfois la maintenance logicielle des anciens appareils, compromettant leur sécurité et leur efficacité.*[7]*

Chapitre 2:Sécurité des Smart Homes .

Chapitre 2 : Sécurité des Smart Homes

2.1 Introduction

Avec la généralisation de l'Internet des Objets (IoT), les **Smart Homes** — ou maisons intelligentes — sont devenues une réalité dans de nombreux foyers à travers le monde. Elles permettent

d'automatiser des tâches domestiques, de surveiller son domicile à distance, d'optimiser la consommation énergétique, ou encore d'améliorer le confort au quotidien. Ces systèmes s'appuient sur une **infrastructure distribuée** composée de capteurs, actionneurs, objets connectés, interfaces mobiles, services cloud, et connexions Internet constantes.

Toutefois, cette connectivité généralisée et permanente introduit de **nombreux risques de sécurité**. Chaque objet connecté représente une **porte d'entrée potentielle pour un attaquant**, et la diversité des technologies utilisées — souvent peu normalisées — augmente considérablement la surface d'attaque. De plus, la majorité des utilisateurs de Smart Homes ne sont pas des professionnels de la sécurité informatique, ce qui rend l'écosystème encore plus vulnérable à des erreurs de configuration, à des produits mal sécurisés ou à des pratiques négligentes.

La **problématique centrale** de ce chapitre est donc la suivante : **comment garantir la sécurité d'un système aussi hétérogène, distribué et exposé que celui d'une maison intelligente connectée ?** Quelles sont les **menaces concrètes** qui pèsent sur ce type d'environnement, et quelles sont les **vulnérabilités techniques** les plus critiques que les attaquants peuvent exploiter ? Surtout, quelles sont les **solutions de sécurité pertinentes, réalistes et applicables**, même dans un contexte résidentiel ou simulé, comme dans notre cas avec l'outil Cisco Packet Tracer ?

Ce chapitre vise à :

- Identifier les **principales menaces** pesant sur les Smart Homes.
- Analyser les **vulnérabilités spécifiques** à ces systèmes connectés.
- Étudier les **contre-mesures techniques, logiques et comportementales** existantes, en évaluant leur applicabilité dans un contexte de simulation.

L'ensemble de ces éléments constituera une base théorique solide pour la partie pratique du chapitre suivant, où certaines de ces mesures seront modélisées à travers une **implémentation simulée d'une Smart Home sécurisée**.

2.2 Les enjeux de la sécurité dans les Smart Homes

L'intégration croissante de l'Internet des Objets dans les habitations modernes transforme les maisons traditionnelles en environnements connectés, intelligents et interactifs. Cependant, cette évolution technologique soulève des enjeux de sécurité majeurs, touchant à la fois les données personnelles, la sécurité physique des résidents, et la fiabilité des systèmes. Ces enjeux doivent être rigoureusement analysés pour concevoir des Smart Homes résilientes face aux menaces actuelles et futures.

2.2.1 Nature sensible des données collectées

Les Smart Homes s'appuient sur un réseau d'objets connectés capables de collecter, analyser et transmettre des données personnelles en continu. Ces données couvrent un large spectre d'informations sensibles :

- Données comportementales : habitudes de vie, horaires de présence, mouvements dans la maison.
- Données biométriques ou médicales : issues de dispositifs de santé connectés (ex. tensiomètre, oxymètre).
- Préférences personnelles : température préférée, routines de sommeil, consommation énergétique.

Cette collecte massive de données expose les utilisateurs à des risques de profilage, de harcèlement ciblé, voire de cambriolage, en cas d'interception ou de divulgation non autorisée [18]

2.2.2 Contrôle d'éléments physiques critiques

Outre la dimension informationnelle, les Smart Homes permettent le pilotage à distance d'équipements physiques sensibles : caméras, serrures connectées, volets roulants, éclairage, thermostat, etc. Ces éléments peuvent représenter un risque direct pour la sécurité physique en cas de compromission. Par exemple :

- Une serrure intelligente piratée peut permettre l'accès à un domicile sans effraction visible.
- Une alarme désactivée à distance peut rendre la maison vulnérable.
- Un thermostat manipulé pourrait engendrer des risques pour les occupants (températures extrêmes).

La literature souligne que des attaques exploitant ces interfaces peuvent avoir des conséquences physiques graves, mettant en danger la sécurité des résidents [35].

2.2.3 Complexité du système

Les Smart Homes reposent sur une architecture distribuée et hétérogène, impliquant :

- Une multitude d'objets connectés, parfois conçus par des fabricants différents, avec des niveaux de sécurité variables.
- Des protocoles de communication diversifiés (Wi-Fi, Zigbee, Bluetooth, MQTT, etc.), pas toujours compatibles ni sécurisés.
- Des mises à jour logicielles non systématiques ou inexistantes.
- Des interactions entre éléments locaux (capteurs, passerelles) et des services distants (cloud, applications mobiles).

Cette complexité crée un environnement où une seule faille peut suffire à compromettre l'ensemble du système. Les études recensent comme causes principales de ces failles la forte hétérogénéité des composants, la personnalisation par les vendeurs et l'absence de normes de sécurité unifiées [19]

2.2.4 Risques nouveaux liés à l'interconnexion permanente

L'un des fondements des Smart Homes est leur **connexion constante à Internet**, nécessaire au fonctionnement des services de contrôle à distance, de synchronisation ou de cloud computing. Cette interconnexion continue introduit plusieurs **risques nouveaux** :

- Une **exposition accrue aux cyberattaques**, notamment via des services cloud vulnérables ou des interfaces web non protégées.
- Une **dépendance forte à la connectivité** : en cas de panne d'Internet, certains équipements peuvent devenir inopérants.
- Une **multiplication des points d'entrée** pour un attaquant : chaque objet, chaque API, chaque application mobile devient une cible potentielle.

Cette connectivité permanente rend **l'isolation du réseau domestique plus difficile**, et accentue l'urgence d'intégrer des mécanismes de sécurité efficaces à tous les niveaux.

2.3 Quelques exemples d'attaquants dans les environnements de maison intelligente

Même lorsque le contenu des communications est chiffré via TLS ou IPsec, les métadonnées associées aux paquets (fréquence, volume, adresse IP de destination, timestamps, etc.) peuvent être exploitées par des attaquants pour reconstituer des scénarios d'usage, profiler les habitudes des occupants, ou même identifier les objets connectés en activité. Cette forme d'attaque est connue sous le nom d'**attaque par canal auxiliaire réseau**.

2.3.1 L'observateur de dernier kilomètre (Last-Mile Observer)

Ce modèle d'attaquant se situe à l'interface entre le réseau domestique et Internet. Il peut s'agir d'un **fournisseur d'accès à Internet (FAI)**, d'un **opérateur de transit**, ou d'un **acteur institutionnel ayant accès à l'infrastructure de transport IP**. Bien que ce type d'observateur ne puisse pas déchiffrer le contenu des sessions protégées par **TLS**, **IPsec** ou **HTTPS**, il bénéficie d'un accès complet à l'ensemble des **métadonnées de flux réseau**, à savoir :

- **Adresse IP source** du domicile,
- **Adresse IP de destination** (souvent associée à un service cloud spécifique),
- **Horodatage précis** des paquets,
- **Fréquence d'envoi**,
- **Taille cumulée et individuelle des paquets**.

À partir de ces éléments, plusieurs types d'attaques sont possibles :

- **Identification des dispositifs** : en l'absence de DNS chiffré, l'analyse des requêtes DNS permet de détecter des domaines caractéristiques (`api.ring.com`, `cloud.nest.com`, etc.), révélant directement la nature et le fabricant du dispositif connecté.
- **Profilage temporel** : l'observation de pics de trafic réguliers (ex. en soirée, à l'aube) peut permettre de déduire des routines domestiques, comme l'heure de réveil, de coucher, ou les absences.
- **Inférence comportementale** : dans les cas où l'objet connecté est dédié à une fonction unique (serrure intelligente, pacemaker, moniteur de sommeil), le lien entre trafic réseau et comportement est immédiat.

L'application d'algorithmes d'apprentissage automatique comme le **k-NN** ou **Random Forest** sur des features simples (moyenne et écart-type du trafic par fenêtres de 30 secondes) permet une **reconnaissance des appareils avec une précision de plus de 95 %**, sans avoir besoin du contenu des paquets[24].

2.3.2 L'espion Wi-Fi local (Local Wi-Fi Eavesdropper)

Contrairement à l'observateur de dernier kilomètre, ce modèle d'attaquant agit **au niveau physique**. Il s'installe **à portée du signal Wi-Fi domestique** : cela peut être un voisin immédiat, une voiture stationnée à proximité, ou un dispositif espion doté d'une **antenne directionnelle à gain élevé**. Sans nécessiter d'accès authentifié, cet espion peut intercepter les **trames Wi-Fi 802.11** diffusées dans l'environnement.

Bien que **WPA2/WPA3** protège le contenu des trames, **les en-têtes MAC et les paramètres physiques (PHY)** ne sont pas chiffrés. Cela permet à l'attaquant de :

- **Capturer les adresses MAC** des objets IoT, qui sont souvent associées à des fabricants (via les OUI – Organizationally Unique Identifier) ;
- **Surveiller la fréquence d'émission**, la longueur des trames, et les périodes d'inactivité ou de rafales, indicateurs clés de l'usage du dispositif ;
- **Corréler les schémas d'émission à des événements précis** : par exemple, une activation de caméra génère des trames longues et soutenues, alors qu'un interrupteur connecté produit une série brève de paquets courts.

Certains attaquants peuvent également utiliser le **RSSI (Received Signal Strength Indicator)** pour **trianguler la position physique des appareils**, en exploitant la puissance du signal reçue par plusieurs antennes synchronisées. Cette technique permet une **cartographie spatiale passive** des objets dans un domicile.

2.4 Menaces courantes dans les environnements Smart Home

Les maisons intelligentes sont exposées à plusieurs types de menaces dues à leur connexion constante à Internet. Cette section présente quelques-unes des attaques les plus fréquentes dans ce type d'environnement.

2.4.1 Interception passive du trafic (Sniffing)

a) Définition et fonctionnement

Le sniffing réseau est une méthode d'interception passive qui consiste à capturer et analyser les paquets de données transitant entre les dispositifs connectés d'un réseau IoT, comme ceux présents dans une maison intelligente. Ces dispositifs comprennent, par exemple, des capteurs, des caméras de surveillance, des assistants vocaux, ou encore des actionneurs.

Dans le contexte des Smart Homes, les réseaux sont souvent sans fil et utilisent plusieurs protocoles de communication (Wi-Fi, Zigbee, Bluetooth Low Energy - BLE). Un outil appelé *sniffer* est configuré en mode *promiscuous* (ou *monitor* sur les réseaux sans fil), ce qui lui permet de recevoir non seulement les paquets destinés à son adresse MAC, mais aussi tous ceux circulant sur le canal radio ou segment réseau.

Cette interception se fait sur différents canaux radio (dans le cas du sans fil) pour saisir un maximum de communications entre les objets connectés, même si ces paquets ne sont pas directement adressés au sniffer. Le sniffer enregistre ensuite ces données pour une analyse détaillée, déchiffrant les protocoles utilisés, et extrait les informations sensibles (identifiants, mots de passe, commandes, contenus audio ou vidéo) [33], [34].

b) Enjeux spécifiques aux Smart Homes

Dans un environnement domestique IoT, le sniffing pose des risques critiques liés à la nature sensible des données échangées :

- **Vol de données personnelles** : Les informations capturées peuvent inclure des identifiants d'accès, mots de passe Wi-Fi, données bancaires ou des profils d'utilisation des occupants (heures de présence, habitudes).
- **Atteinte à la confidentialité** : Les communications interceptées peuvent contenir des flux vidéo (caméras de surveillance), des commandes vocales (assistants personnels), ou encore des informations privées, exposant ainsi la vie privée des utilisateurs.
- **Préparation d'attaques avancées** : En collectant ces données, un attaquant peut élaborer des attaques ciblées, notamment des attaques de type Man-in-the-Middle (MITM), où il intercepte puis modifie le trafic réseau pour usurper des identités ou injecter des commandes malveillantes dans le système domotique [35].

c) Types de sniffing

Le sniffing peut se diviser en deux catégories principales, en fonction du mode d'interception :

- **Sniffing passif** : L'attaquant se contente d'écouter et d'enregistrer le trafic réseau sans interagir ni modifier les paquets. Cette méthode est difficile à détecter car elle n'affecte pas le fonctionnement normal du réseau. Elle est souvent utilisée pour collecter discrètement des informations sur le réseau et ses utilisateurs, sans alerter les systèmes de sécurité.

- **Sniffing actif** : Ici, l'attaquant ne se limite pas à l'écoute. Il injecte ou modifie les paquets en circulation afin d'intercepter les données, par exemple en menant une attaque MITM. Cette méthode est plus intrusive et peut provoquer des anomalies dans le trafic, mais elle permet d'obtenir des accès plus profonds aux communications et de manipuler le comportement des dispositifs IoT [15].

2.4.2 Usurpation d'identité (Spoofing)

Le spoofing est une attaque d'usurpation d'identité réseau où un dispositif malveillant imite l'identité d'un objet IoT légitime — par exemple, une adresse IP, une adresse MAC ou d'autres identifiants — afin de compromettre la confidentialité, l'intégrité et la disponibilité du système. Dans le contexte des maisons intelligentes, où de nombreux capteurs, actionneurs, passerelles et contrôleurs communiquent en continu, cette menace est particulièrement critique.[36]

L'attaquant peut ainsi :

- Injecter de fausses données (par exemple, des mesures erronées de température, de mouvement ou d'ouverture de porte), ce qui perturbe la gestion automatisée et peut déclencher des actions inappropriées ou dangereuses ;
- Détourner ou intercepter des commandes destinées à des dispositifs légitimes (comme l'ouverture à distance d'une serrure ou l'activation de l'éclairage), causant des risques de sécurité physique et d'intrusion ;
- Escalader ses privilèges en usurpant l'identité d'une passerelle ou d'un routeur, facilitant l'accès non autorisé à des segments critiques du réseau domestique et ouvrant la voie à d'autres attaques plus sophistiquées.[16]

Type de Spoofing	Description	Impact dans une Smart Home
IP Spoofing	Falsification de l'adresse IP source dans les paquets réseau pour masquer l'origine de l'attaque.	Contournement des filtres IP, DoS/DDoS sur la passerelle domotique ou serveurs cloud.
MAC Spoofing	Usurpation de l'adresse physique (MAC) d'un autre appareil sur un réseau local (Wi-Fi, Zigbee, Bluetooth).	Accès non autorisé au réseau, contournement des ACLs, interception des communications entre dispositifs.
ARP Spoofing / Poisoning	Manipulation frauduleuse des tables ARP pour rediriger le trafic réseau local.	Attaque Man-in-the-Middle : interception, modification ou blocage des échanges entre capteurs, caméras, passerelles.
DNS Spoofing	Détournement des requêtes DNS en falsifiant les réponses, redirigeant vers des serveurs malveillants.	Les objets connectés contactent de faux services cloud ou sites malveillants → vol de données, commandes malicieuses.

GPS Spoofing	Émission de faux signaux GPS pour tromper un appareil géolocalisé.	Désorientation de dispositifs mobiles (robots, caméras), perturbation des services basés sur la localisation.

Tableau 1: Types de Spoofing dans les environnements IoT et Smart Homes [37]

2.4.3 Déni de service distribué (DoS/DDoS)

a) Définition

Les attaques par déni de service (DoS) ont pour objectif de perturber la disponibilité d'un système ou d'un service en le saturant de requêtes jusqu'à ce qu'il devienne inopérant. Dans le contexte des maisons intelligentes, les cibles privilégiées comprennent les routeurs Wi-Fi, les passerelles domotiques ainsi que les serveurs cloud assurant la gestion centralisée des objets connectés. Ces attaques peuvent entraîner :

- Une indisponibilité temporaire ou prolongée des services critiques, tels que la vidéosurveillance, les systèmes d'alarme, ou le contrôle d'accès ;
- Une perte de connectivité rendant les dispositifs inaccessibles à distance, compromettant ainsi leur fonctionnalité ;
- Une dégradation significative des performances du réseau local, impactant l'ensemble de l'écosystème domestique.

Les attaques distribuées par déni de service (DDoS), particulièrement redoutées, sont orchestrées via des réseaux de dispositifs compromis, appelés botnets. Dans l'univers de l'Internet des Objets (IoT), la prolifération massive d'appareils connectés faiblement sécurisés — caméras IP, capteurs, assistants vocaux — constitue un terrain propice à la création de ces botnets. Ces équipements sont souvent victimes de configurations par défaut non sécurisées, d'absences de mises à jour, ou même d'abandons, ce qui facilite leur prise de contrôle par des acteurs malveillants.

b) Fonctionnement

Le fonctionnement typique d'une attaque DDoS basée sur l'IoT suit plusieurs étapes :

1. Identification des vulnérabilités sur les dispositifs IoT (mots de passe par défaut, firmwares obsolètes) ;
2. Prise de contrôle des appareils via un serveur de commande et contrôle (C&C) qui orchestre les actions du botnet ;
3. Injection de commandes malveillantesPropagation autonome du malware (exemple : Mirai) permettant au botnet de s'étendre automatiquement en infectant de nouveaux appareils ;
4. Lancement simultané d'un assaut massif sur la cible, générant un trafic considérable qui surcharge la bande passante ou les ressources du système visé.

Ce phénomène connaît une croissance exponentielle. En 2023, les attaques DDoS issues de l'IoT ont augmenté de 300 %, mobilisant près d'un million d'appareils compromis et occasionnant des pertes financières estimées à plus de 2,5 milliards de dollars. Certaines attaques ont atteint des débits record de 800 Gbps, tandis que des scénarios futurs envisagent des pics de trafic pouvant atteindre 100 Tbps, mettant en péril des infrastructures critiques telles que la santé, les transports, ou la finance

c) Processus d'infection et d'intégration des dispositifs IoT dans un botnet

1. **Commande initiale** : L'attaquant utilise le serveur de commande et contrôle (C&C) pour envoyer une directive au botnet, l'incitant à lancer une attaque ciblée tout en intégrant de nouveaux dispositifs vulnérables.
2. **Orchestration** : Le serveur C&C coordonne l'ensemble des actions du botnet, distribuant les instructions à tous les appareils compromis.
3. **Scan et compromission** : Le botnet effectue un balayage automatisé des réseaux à la recherche de dispositifs IoT vulnérables. Il exploite des faiblesses telles que des mots de passe faibles ou par défaut, des firmwares obsolètes, ou des configurations non sécurisées pour prendre le contrôle des appareils.
4. **Rapport de données** : Une fois un dispositif compromis, le botnet transmet son adresse IP ainsi que les identifiants d'accès au serveur chargeur (loader server), qui joue un rôle clé dans l'infection.
5. **Distribution du malware et infection** : Le serveur chargeur envoie le logiciel malveillant ou des instructions malicieuses au dispositif ciblé. Celui-ci exécute alors le code reçu, devenant ainsi un nœud actif du botnet.
6. **Intégration au botnet** : Le dispositif nouvellement infecté rejoint le réseau de bots et attend les prochaines commandes du serveur C&C, tout en restant généralement indétectable pour l'utilisateur

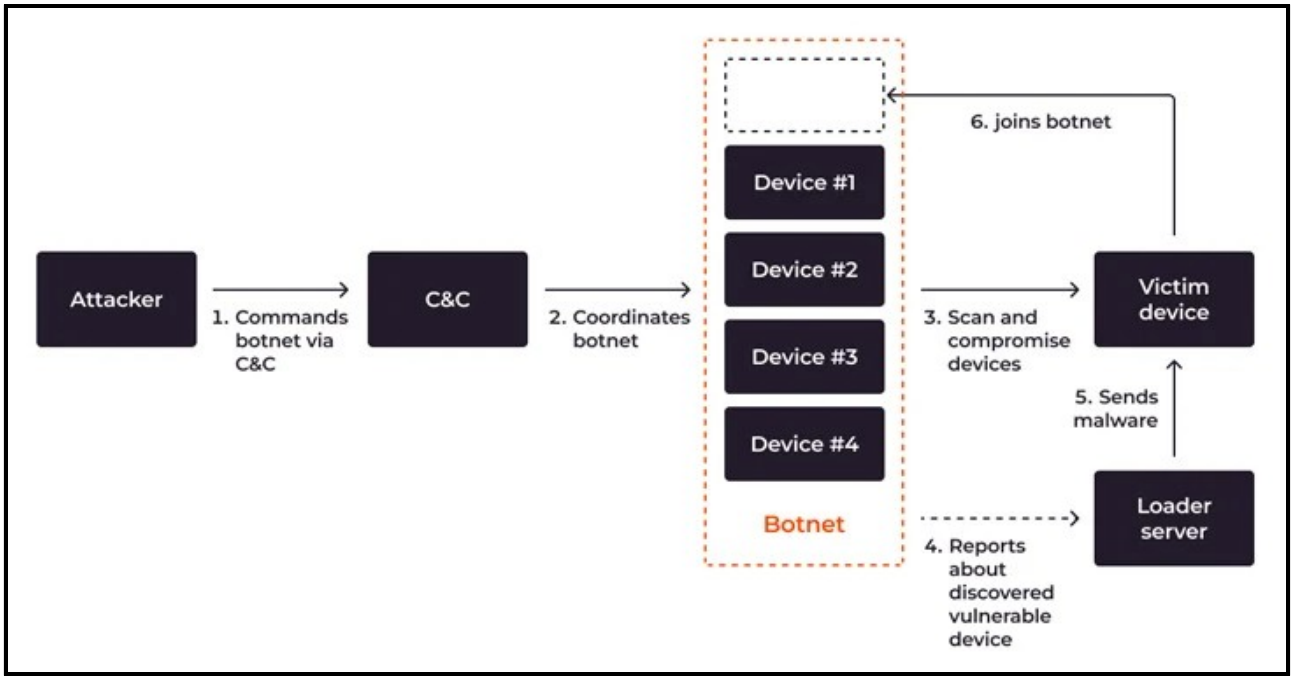


Figure 14: Processus d'infection d'un objet IoT dans un botnet. [42]

2.4.4 Attaque de l'homme du milieu (Man-in-the-Middle)

L'attaque dite **Man-in-the-Middle (MitM)** constitue une forme avancée d'interception active, dans laquelle un acteur malveillant parvient à **s'insérer furtivement entre deux entités communicantes**, typiquement sans que ces dernières n'en aient conscience. Dans les réseaux IoT, où les communications entre dispositifs sont fréquentes, continues et souvent insuffisamment sécurisées, cette attaque revêt une criticité particulière.

Le principe repose sur une **usurpation simultanée de l'identité des deux parties**, permettant à l'attaquant d'établir **deux sessions distinctes** : l'une avec l'expéditeur, l'autre avec le destinataire. En contrôlant ce point intermédiaire, il est en mesure d'**écouter, modifier, retarder, rejouer, bloquer ou rediriger** les messages échangés, tout en maintenant l'illusion d'une communication directe et légitime entre les dispositifs ciblés.

Dans un **contexte domestique**, cela peut se traduire par le vol de données sensibles (ex. : historiques d'activités, commandes envoyées à des objets connectés, identifiants de sessions), ou par la prise de contrôle de dispositifs critiques comme les caméras, serrures intelligentes ou alarmes. Dans un cadre **industriel ou médical**, l'attaque MitM peut compromettre l'intégrité de systèmes automatisés ou médicaux, exposant potentiellement des vies humaines à des risques significatifs.

Les vecteurs techniques de cette attaque incluent notamment :

- la manipulation de protocoles non sécurisés (ex. : ARP spoofing, DNS spoofing) ;
- la compromission d'un point d'accès Wi-Fi ou d'un routeur intermédiaire ;
- ou encore l'exploitation de défauts dans les procédures d'authentification initiales entre dispositifs.[75]

2.4.5 Injection de commandes malveillantes

L'injection de commandes malveillantes consiste à envoyer des instructions non autorisées à un objet connecté, généralement en exploitant des failles dans les interfaces de contrôle (applications mobiles, interfaces vocales, pages web de configuration). Cette attaque peut entraîner :

- L'ouverture involontaire d'une porte ou d'un garage connecté ;
- La désactivation d'un système d'alarme ou d'un détecteur de mouvement ;
- La manipulation du chauffage, de l'éclairage ou d'autres systèmes de confort.

Certains vecteurs d'attaque utilisent même des commandes inaudibles diffusées par ultrasons pour abuser des assistants vocaux, exploitant le fait qu'ils répondent à des commandes qu'un utilisateur humain ne peut percevoir. Des études ont démontré que des attaques par injection de commandes peuvent être réalisées à distance, même à travers des barrières physiques, en utilisant des signaux audio spécifiques pour contrôler des assistants vocaux tels qu'Amazon Echo ou Google Home [17].

2.4.6 Analyse comportementale du trafic (Traffic Analysis)

Dans les environnements **Internet of Things (IoT)**, où la connectivité entre dispositifs est constante et souvent critique, les attaques ne se limitent plus au contenu des messages. Même lorsque les échanges sont chiffrés (via TLS, WPA3, etc.), les **métadonnées** — telles que la fréquence des transmissions, la taille des paquets, les adresses IP ou encore les horaires — peuvent être exploitées par un adversaire. Ce type d'exploitation constitue le fondement des **attaques par analyse de trafic** (*Traffic Analysis Attacks*), qui menacent aujourd'hui directement la confidentialité dans les systèmes Smart Home.

- **Principes de l'analyse de trafic**

L'analyse de trafic désigne un ensemble de techniques utilisées pour observer, enregistrer et interpréter les schémas de communication dans un réseau, sans pour autant avoir besoin d'accéder au contenu des paquets. Un attaquant peut, par exemple :

- déduire les habitudes d'un utilisateur, comme ses heures de présence ou d'inactivité, en observant l'activité de capteurs de mouvement ;
- identifier des objets connectés actifs en se basant sur leurs signatures de trafic caractéristiques, comme une caméra IP ou une serrure intelligente ;
- reconstituer des scénarios d'usage à partir de corrélations temporelles entre différents flux (par exemple, déclenchement d'une alarme suivi d'un envoi vidéo) ;
- détecter des événements critiques, comme des alertes médicales, simplement à partir de pics inhabituels de trafic.[44]

Même avec un chiffrement fort, ces attaques demeurent efficaces car les métadonnées ne sont généralement pas protégées.

- **Environnements vulnérables**

Les systèmes **Smart Home** sont particulièrement exposés à ce type d'attaque en raison de plusieurs facteurs. D'abord, les objets connectés ont souvent des ressources limitées, ce qui empêche l'implémentation de contre-mesures complexes comme le brouillage temporel ou le remplissage aléatoire des paquets. Ensuite, leurs transmissions sont souvent régulières et prévisibles, ce qui facilite leur profilage. Enfin, de nombreux protocoles utilisés, tels que **MQTT**, **CoAP**, **Zigbee** ou **Bluetooth Low Energy (BLE)**, ne prévoient pas de mécanismes intégrés contre ce type d'observation passive.[45]

- **Techniques utilisées par les attaquants**

Plusieurs méthodes sont employées pour mener une attaque par analyse de trafic. L'analyse temporelle permet de repérer les moments d'activité selon la fréquence des échanges. La technique de reconnaissance par la taille des paquets (size fingerprinting) consiste à identifier les objets ou les commandes selon les volumes de données échangés. La corrélation de flux permet de relier plusieurs événements pour reconstituer un scénario. Enfin, des approches basées sur l'intelligence artificielle permettent de classifier les objets et de prédire les usages en fonction des modèles de trafic.

Des études ont démontré qu'il est possible d'identifier avec précision plus de **90 % des objets IoT** présents dans un réseau domestique uniquement à partir de ces méthodes.

2.4.7 Menaces physiques

Certaines attaques ciblent directement l'environnement physique de la Smart Home, en exploitant la **connexion entre le monde numérique et le monde réel**.

Par exemple :

- Une **serrure intelligente piratée** peut être déverrouillée à distance sans alerte ni effraction visible.
- Une **caméra de surveillance compromise** peut permettre à un attaquant de visualiser en temps réel l'intérieur du domicile, facilitant ainsi un cambriolage ou une violation de la vie privée.
- Des **capteurs désactivés** ou trompés peuvent perturber les systèmes d'alarme.

Ces menaces soulignent l'importance de sécuriser non seulement les données, mais également les **interfaces physiques contrôlées par le système domotique**.

2.4.8 Menaces émergentes (IA, assistants vocaux, deepfakes)

Avec l'intégration croissante de l'intelligence artificielle dans les assistants domestiques, de **nouvelles menaces apparaissent**, encore peu maîtrisées.

- Les **deepfakes vocaux** peuvent tromper un assistant vocal en reproduisant la voix d'un utilisateur autorisé, et ainsi **contourner les systèmes d'authentification par commande vocale**.
- Les **attaques par social engineering assistées par IA** permettent de générer automatiquement des messages personnalisés ou des tentatives d'hameçonnage très crédibles, augmentant le risque de compromission.
- La **surveillance passive par les assistants vocaux** eux-mêmes constitue un risque intrinsèque : ces appareils sont toujours à l'écoute et peuvent être activés, volontairement ou non, par un signal externe.

Ces menaces émergentes montrent que la sécurité des Smart Homes n'est pas un objectif statique, mais un **processus dynamique**, qui doit évoluer au rythme des technologies.

Le **Tableau 2** présente une synthèse extraite de [39][38], des principales menaces sur les Smart Homes IoT et des contre-mesures associées.

Menace	**Description simplifiée**	**Contre-mesures recommandées**
Sniffing réseau	Interception passive des communications entre objets connectés (Wi-Fi, Zigbee,BLE).	Chiffrement (TLS, WPA3), VPN, segmentation réseau (VLAN), détection par IDS.
Spoofing (usurpation d'identité)	Falsification de l'identité d'un appareil ou d'un utilisateur pour accéder au système.	Authentification forte, certificats numériques, surveillance réseau, signatures ECC.
Attaques par déni de service (DoS / DDoS)	Saturation du réseau ou des équipements pour rendre le service indisponible.	Pare-feux domestiques, filtrage ACL, limitation de bande passante, supervision active.
Injection de commandes malveillantes	Envoi d'instructions non autorisées à des objets via failles dans les interfaces	HTTPS, authentification forte, filtrage applicatif, contrôle d'accès basé sur les rôles (RBAC).
Man-in-the-Middle (MitM)	Interception et modification active de la communication entre deux nœuds sans qu'ils le sachent	Chiffrement de bout en bout (TLS/IPsec), certificats mutuels, protection ARP/DNS, détection d'anomalies réseau.
Analyse de trafic	Observation des métadonnées (taille, fréquence, IP) pour déduire des comportements privés.	VPN, tunnels Ipsec, fragmentation + padding, traffic shaping, segmentation (VLAN), IDS.

Tableau 2: Synthèse des principales menaces sur les Smart Homes IoT et contre-mesures associées.

2.5 Exemples d'attaques réelles

De nombreux incidents documentés montrent la gravité croissante des menaces pesant sur les dispositifs IoT, y compris dans le cadre domestique. Voici quelques cas emblématiques :

- **Caméras connectées Ring (2019)**

  En 2019, plusieurs utilisateurs de caméras de surveillance de la marque *Ring* ont signalé que des attaquants avaient pris le contrôle à distance de leurs appareils. Dans certains cas, les intrus ont utilisé les haut-parleurs intégrés pour harceler verbalement les occupants. Ces intrusions étaient rendues possibles par des mots de passe faibles et l'absence d'authentification à deux facteurs, soulignant l'importance des bonnes pratiques de sécurité dès l'installation.

- **Botnet Mirai (2016)**

  L'attaque du botnet *Mirai* constitue un tournant majeur dans l'histoire de la cybersécurité des objets connectés. En exploitant des failles dans des dispositifs tels que des caméras IP, routeurs ou enregistreurs numériques (DVR), les attaquants ont constitué un réseau de centaines de milliers de machines infectées. Ce botnet a ensuite été utilisé pour lancer une attaque DDoS massive contre les services DNS de Dyn, paralysant temporairement des plateformes comme Twitter, GitHub et Spotify.

2.6 Vulnérabilités spécifiques des Smart Homes

Malgré les efforts d'innovation dans le domaine des objets connectés, les Smart Homes demeurent vulnérables en raison de **défauts structurels** liés aux technologies utilisées, à leur configuration, et à leur maintenance. Ces vulnérabilités sont souvent **sous-estimées par les fabricants** et **ignorées par les utilisateurs finaux**, ce qui laisse une large surface d'attaque exploitable.

2.6.1 Failles des protocoles IoT (Zigbee, MQTT…)

Les protocoles de communication utilisés dans les Smart Homes — tels que **Zigbee**, **Z-Wave**, **Bluetooth Low Energy (BLE)**, ou encore **MQTT** — ont été conçus pour être **légers**, **faiblement énergivores** et **adaptés aux petits appareils**, mais **pas toujours sécurisés**.

- Zigbee, par exemple, utilise un chiffrement symétrique (AES-128), mais dans certaines implémentations, la clé de chiffrement est partagée statiquement ou peut être interceptée lors de l'appairage initial.
- **MQTT**, protocole très répandu dans les architectures domotiques, **n'intègre pas nativement de chiffrement** ni d'authentification forte. Il repose sur les couches supérieures pour la sécurité (TLS), mais cette protection est souvent désactivée dans les appareils grand public pour des raisons de performance ou de simplicité.

L'absence de **normes de sécurité obligatoires** pour ces protocoles laisse place à des implémentations vulnérables, facilitant les attaques par interception, injection ou replay.

2.6.2 Mauvaises configurations par défaut

De nombreux objets connectés sont livrés avec des **paramètres de configuration très faibles ou non sécurisés par défaut** :

- **Identifiants standards** ("admin/admin", "user/1234") non modifiables à l'installation.
- **Interfaces d'administration accessibles sans authentification**, parfois même à distance.
- **Ports ouverts inutilement** (HTTP, Telnet), sans filtre ni chiffrement.

Ces défauts de configuration sont d'autant plus critiques que **la majorité des utilisateurs ne les modifient jamais**. Des attaques automatisées peuvent alors **scanner Internet** à la recherche de ces appareils exposés, les identifier par leur signature, et les intégrer dans des botnets ou les compromettre individuellement.

2.6.3 Dépendance aux services cloud

La majorité des objets connectés reposent sur des **services cloud tiers** pour fonctionner (stockage, contrôle à distance, intelligence embarquée). Cette **dépendance à l'extérieur du réseau domestique** pose plusieurs problèmes :

1. **Perte de contrôle sur les données** : les flux sont souvent transmis en clair ou partiellement chiffrés à des serveurs appartenant aux fabricants, sans garantie de conformité au RGPD ou de respect de la vie privée.

2. **Indisponibilité fonctionnelle** : si le service cloud tombe en panne, est mis hors service ou subit une attaque, l'objet devient inutilisable, même localement.

3. **Failles chez le fournisseur** : les vulnérabilités ne sont plus sous le contrôle de l'utilisateur. Une mauvaise configuration, un stockage mal protégé ou une mauvaise gestion des API peut exposer l'ensemble des utilisateurs.

Ainsi, même si le réseau local est correctement configuré, la **chaîne de confiance est rompue dès lors qu'un élément cloud est compromis**.

2.6.4 Obsolescence logicielle

Un problème majeur dans le domaine de l'Internet des Objets (IoT) est l'obsolescence rapide des logiciels embarqués dans les dispositifs. Contrairement aux smartphones ou aux ordinateurs, la plupart des objets connectés ne bénéficient pas de mécanismes de mise à jour automatique, ou leur maintenance logicielle cesse après seulement quelques mois.

Premièrement, certains produits ne reçoivent aucune mise à jour de sécurité post-commercialisation. Deuxièmement, d'autres dépendent de fabricants peu fiables qui peuvent disparaître ou abandonner leur support. Enfin, même lorsque des mises à jour sont disponibles, les utilisateurs ne sont souvent ni informés ni formés pour les appliquer correctement.*[33]*

En conséquence, ces dispositifs deviennent des « passoires numériques » à long terme, restant souvent connectés au réseau plusieurs années après la découverte de vulnérabilités, ce qui engendre un risque de sécurité persistant et difficile à atténuer.

2.7 Contre-mesures et solutions de sécurité

Face à la diversité des menaces et vulnérabilités identifiées dans les environnements domotiques, il est impératif d'adopter une approche de sécurité **multi-couches** et **adaptée au contexte résidentiel**. Les solutions doivent être à la fois efficaces, soutenues par des standards reconnus, et compatibles avec les contraintes techniques et financières des utilisateurs finaux. Cette section présente les principales mesures de protection envisageables, à différents niveaux du système.

2.7.1 Mesures réseau

Le réseau local constitue le socle de communication de la Smart Home. Sa sécurisation est une priorité pour éviter les intrusions et la propagation d'attaques.

2.7.1.1 Listes de Contrôle d'Accès (ACLs)

Les **Listes de Contrôle d'Accès (ACLs)** sont des ensembles de règles utilisées pour **filtrer le trafic réseau** traversant les interfaces d'un routeur ou d'un pare-feu. Chaque ACL définit un ordre séquentiel d'instructions qui autorisent ou refusent les paquets selon des critères précis, tels que les adresses IP source et destination, le protocole (TCP, UDP, ICMP), et les numéros de ports.[21]

Types d'ACLs

- **ACL standard**

  Filtrent uniquement en fonction de l'adresse IP **source**. Elles sont simples mais peu granulaires et doivent être placées près de la **destination** donné qu'elles ne précisent pas les adresses de destination.

- **ACL étendue**

  Permettent un filtrage plus avancé en prenant en compte les adresses IP **source et destination**, le protocole et les ports concernés. Elles offrent une granularité fine et doivent être placées près de la **source** du trafic à filtrer.

- **ACL nommée**

  Introduites dans les versions plus récentes de Cisco IOS, elles permettent d'attribuer un nom plutôt qu'un numéro à une ACL. Elles sont modifiables sans suppression complète, ce qui facilite leur gestion et leur documentation.

Fonctionnement

- Les ACLs sont évaluées **de haut en bas** : Si le paquet correspond à une instruction, il est soit accepté soit rejeté.
- Une règle implicite finale `deny any` rejette tout paquet non explicitement autorisé.

- Les ACLs peuvent être appliquées sur des interfaces en direction **entrante (in)** ou **sortante (out)**.
- Chaque interface peut avoir plusieurs ACLs, une par protocole et direction.
- Le masque générique, spécifique à Cisco, est utilisé pour déterminer dans quelles parties de l'adresse IP il doit y avoir correspondance parfaite et dans quelles partie la correspondance parfaite n'est pas exigée..

Règles de bonnes pratiques

- Appliquer les **ACLs étendues près de la source** pour limiter la propagation des flux non désirés ou inutile.
- Appliquer les **ACLs standards près de la destination**, car elles ne filtrent que par IP source.
- Utiliser des commentaires dans les ACLs pour documenter la logique des règles.
- Ne jamais modifier une ACL active directement : toute modification d'une ACL en cours d'utilisation peut engendrer des interruptions de service ou des incohérences dans le filtrage du trafic. Il est fortement recommandé de sauvegarder la configuration, puis de supprimer l'ACL existante avant de la recréer avec les modifications souhaitées. Cette méthode garantit une meilleure stabilité et un contrôle plus sûr du comportement réseau.
- Tester les ACLs via des commandes de vérification (`show access-lists`, `show ip interface`) et par simulation de trafic [21].

Utilisation des ACLs dans les Smart Homes

Dans un environnement Smart Home, la sécurité réseau repose en grande partie sur une gestion fine des communications entre les multiples dispositifs connectés. Les **ACLs jouent un rôle clé** dans ce contexte en permettant de maîtriser précisément qui peut communiquer avec quoi, et comment. Voici les principaux usages détaillés :

- **Segmentation et isolation des objets IoT :**

Les ACLs permettent de **limiter les échanges entre objets connectés**, souvent très hétérogènes et sensibles. Par exemple, une caméra de surveillance ne devrait pas pouvoir initier une communication avec un thermostat ou une ampoule intelligente, sauf si un cas d'usage précis le justifie. En restreignant ces flux, on réduit les risques de propagation latérale en cas de compromission d'un appareil.

- **Protection des interfaces sensibles du réseau domestique** :

L'interface d'administration du routeur ou des passerelles domotiques constitue un point d'entrée critique. Les **ACLs permettent de restreindre l'accès** à ces interfaces uniquement à des adresses IP ou appareils de confiance (par exemple, le PC de l'administrateur). Cela réduit considérablement les risques d'accès non autorisé ou de prise de contrôle à distance.

Cependant, **les ACLs standard ou étendues ne sont pas efficaces contre le spoofing IP**, car elles se basent uniquement sur l'adresse IP présente dans les paquets, qui peut être falsifiée. Pour contrer le spoofing, il est nécessaire de combiner les ACLs avec d'autres mécanismes tels que **l'anti-spoofing (uRPF), les firewalls à inspection de paquets, ou les systèmes d'authentification renforcée**.

- **Blocage des protocoles et ports non sécurisés** :

De nombreux objets IoT continuent d'utiliser des protocoles anciens ou non sécurisés comme Telnet (port 23), FTP ou HTTP non chiffré. Les ACLs permettent de **bloquer ces protocoles sur le réseau local ou à la frontière Internet**, évitant ainsi des risques d'écoute, d'injection ou d'usurpation.

- **Contrôle strict du trafic sortant vers Internet** :

Les ACLs peuvent limiter la capacité des appareils à se connecter uniquement aux serveurs et services autorisés (par exemple, le cloud officiel du fabricant ou des services de mise à jour). Cela empêche les communications vers des serveurs malveillants ou inconnus, réduisant le risque d'exfiltration de données ou de commande à distance par des attaquants.

2.7.1.2 Accès sécurisé aux équipements réseau via SSH dans un environnement IoT

Dans une architecture de maison intelligente (smart home), les équipements réseau tels que les routeurs, les commutateurs ou les contrôleurs domotiques représentent des points névralgiques de gestion. Leur compromission peut entraîner un accès global au réseau domestique, aux objets connectés, ainsi qu'aux données personnelles échangées. Dans ce contexte, sécuriser l'accès à ces équipements constitue une exigence prioritaire.

Traditionnellement, l'administration distante de ces dispositifs s'effectuait via **Telnet**, un protocole aujourd'hui considéré comme obsolète car il transmet les données — notamment les identifiants — en clair. Dans un environnement IoT, où des services sensibles peuvent être déployés (vidéosurveillance, alarmes, contrôle d'accès), cette faiblesse représente un risque majeur d'interception et d'exploitation malveillante.

Pour répondre à ces enjeux, il est fortement recommandé de **désactiver Telnet** et de le **remplacer par SSH (Secure Shell)**. SSH est un protocole de communication sécurisé qui chiffre l'ensemble du trafic entre l'administrateur et l'équipement, garantissant ainsi **confidentialité**, **intégrité**, et **authenticité** des échanges.

Configuration sécurisée de SSH

La sécurisation de l'accès SSH repose sur plusieurs mécanismes complémentaires, essentiels dans le cadre d'un réseau IoT fiable :

- **Chiffrement des communications** : SSH chiffre les sessions d'administration, empêchant ainsi tout espionnage ou détournement d'informations sensibles (identifiants, configurations réseau, commandes critiques).

- **Utilisateurs locaux avec mots de passe robustes** : Il est impératif de créer des comptes d'administration protégés par des mots de passe complexes (longueur suffisante, usage de majuscules, minuscules, chiffres et symboles). Cela limite l'exposition aux attaques par dictionnaire ou force brute, notamment via les interfaces exposées au réseau local ou distant.
- **Authentification par paire de clés SSH** : Pour renforcer encore la sécurité, une authentification par **clé publique/clé privée** peut être mise en place. Cette méthode élimine l'envoi de mots de passe sur le réseau et réduit considérablement le risque de compromission, tout en simplifiant l'automatisation sécurisée des connexions (scripts de supervision, mises à jour, etc.).
- **Filtrage des accès VTY** : Les lignes VTY (Virtual Teletype) sont des ports d'accès logiques permettant l'administration à distance des équipements réseau (routeurs, commutateurs), généralement via les protocoles Telnet ou SSH. En tant que points d'entrée critiques, leur sécurisation s'avère essentielle.

  La première étape consiste à désactiver Telnet, protocole non sécurisé, en configurant le périphérique pour n'accepter que les connexions SSH (`transport input ssh`). Cette configuration garantit la confidentialité des échanges entre l'administrateur et l'équipement. En complément, l'accès aux lignes VTY peut être restreint à une plage d'adresses IP spécifique, typiquement celle d'un réseau de gestion (VLAN d'administration).

  Cette stratégie combinée permet de réduire significativement la surface d'attaque et de limiter les accès aux seuls hôtes autorisés, renforçant ainsi la sécurité des interfaces d'administration réseau.
- **Gestion des délais et tentatives de connexion** : La définition de délais d'inactivité (`exec-timeout`) et la limitation du nombre d'essais de connexion réduisent les possibilités de persistance des attaques par bruteforce ou scripts automatisés.

2.7.1.3 Pare-feux domestiques

Les pare-feux domestiques constituent un mécanisme de défense périmétrique essentiel dans le cadre de la sécurité des maisons intelligentes. Intégrés à la majorité des routeurs grand public ou installés sous forme de dispositifs dédiés, ils permettent de contrôler le trafic réseau entrant et sortant, en se basant sur des règles prédéfinies.

Le rôle principal d'un pare-feu est d'analyser les paquets de données transitant entre le réseau local et l'extérieur (notamment Internet) afin de bloquer les connexions non sollicitées ou suspectes. Il agit comme un filtre, permettant uniquement le trafic jugé légitime et bloquant l'accès aux services ou ports non nécessaires au bon fonctionnement des dispositifs.

En configurant correctement un pare-feu domestique, il est possible :

- De restreindre l'exposition des objets connectés aux menaces extérieures en fermant les ports ouverts non utilisés.

- D'empêcher certaines communications sortantes non autorisées vers des serveurs distants potentiellement malveillants.
- De limiter les flux internes entre appareils, en complément d'une segmentation réseau.

Les pare-feux domestiques contribuent à réduire la surface d'attaque du réseau en limitant les vecteurs d'intrusion et en renforçant le contrôle des communications autorisées. Cette maîtrise passe notamment par l'utilisation des listes de contrôle d'accès (ACLs), qui définissent précisément les règles de filtrage du trafic en fonction des adresses IP, ports et protocoles. Ainsi, les ACLs sont un élément central de la configuration des pare-feux, garantissant un filtrage granulaire et efficace. Une bonne configuration des pare-feux, complétée par des ACLs adaptées et une mise à jour régulière du firmware du routeur, est indispensable pour assurer un niveau de sécurité élevé dans un environnement domotique.

2.7.2 Sécurisation des objets

Chaque dispositif IoT doit intégrer **un minimum de protections embarquées**, souvent négligées par les fabricants.

- **Authentification forte** : obligation de changer les identifiants par défaut, utilisation de mots de passe complexes, voire authentification à deux facteurs pour les applications mobiles.
- **Mise à jour régulière du firmware** : les fabricants doivent proposer des patchs de sécurité facilement installables par les utilisateurs, idéalement automatisés.
- **Désactivation des ports inutiles** : de nombreux objets laissent actifs des services comme Telnet, HTTP ou UPnP, qui doivent être désactivés si non utilisés.

Ces bonnes pratiques relèvent autant du développement logiciel que de l'éducation des utilisateurs.

2.7.3 Sécurité du cloud

Dans l'écosystème des Smart Homes, de nombreux dispositifs connectés s'appuient sur des services cloud pour le stockage des données, le contrôle à distance ou encore les mises à jour logicielles. Cette dépendance aux plateformes distantes soulève des enjeux cruciaux en matière de sécurité, de confidentialité et de conformité réglementaire.

Principes fondamentaux à respecter :

a) Conformité réglementaire (ex. : RGPD)
Il est essentiel de sélectionner des fournisseurs de services cloud qui respectent les exigences légales, notamment le Règlement Général sur la Protection des Données (RGPD). Cela inclut :

- La **localisation des données** dans des centres certifiés situés dans des juridictions conformes (idéalement dans l'Union européenne).
- La mise en œuvre de **mesures de sécurité techniques et organisationnelles** pour protéger les données personnelles contre tout accès non autorisé.

- La garantie de **droits pour les utilisateurs**, tels que l'accès, la rectification ou la suppression de leurs données.

b) Sécurisation des interfaces (APIs)

Les objets connectés interagissent fréquemment avec le cloud via des interfaces de programmation d'applications (APIs). Ces interfaces doivent être rigoureusement sécurisées :

- **Authentification robuste** (ex. : clés API, HMAC, OAuth2).
- **Validation des entrées** pour prévenir les injections malveillantes.
- **Chiffrement des échanges** via HTTPS/TLS pour protéger l'intégrité et la confidentialité des données transmises.

c) Gestion des sessions et des accès

L'utilisation de **jetons d'authentification temporaires** (comme les tokens JWT ou OAuth2 avec durée de validité limitée) permet d'éviter les sessions longues ou permanentes, qui représentent un risque accru en cas de compromission. Ces jetons doivent :

- Expirer automatiquement après un délai court.
- Être stockés de manière sécurisée côté client (jamais en clair).
- Être rafraîchissables uniquement via des mécanismes sécurisés (refresh token, re-authentification). [39]

2.7.4 Techniques de protection de la vie privée

Certaines attaques visent à **profiler l'utilisateur** par analyse de trafic. Pour s'en prémunir, des solutions spécifiques peuvent être mises en place.

2.7.4.1 Réseau Privé Virtuel (VPN)

Le **VPN (Virtual Private Network)** est une technologie qui permet de sécuriser les communications réseau en créant un **tunnel chiffré** entre le réseau domestique et un serveur distant. Dans le contexte des maisons intelligentes, le VPN constitue une mesure de protection efficace contre l'interception, l'analyse et la manipulation du trafic réseau par des acteurs malveillants.

En encapsulant l'ensemble du trafic sortant dans ce tunnel sécurisé, le VPN masque les **métadonnées réseau** sensibles — telles que les adresses IP des objets connectés, les ports utilisés, ou encore les horaires de communication. Ainsi, un observateur extérieur (fournisseur d'accès, cybercriminel, etc.) ne peut ni identifier les dispositifs présents, ni déduire les actions effectuées au sein du réseau domestique.

Cette couche de confidentialité supplémentaire apporte plusieurs bénéfices majeurs :

- **Préservation de la vie privée et de l'anonymat** des utilisateurs, empêchant le profilage basé sur l'analyse des flux.

- **Protection contre les attaques de type sniffing et Man-in-the-Middle**, qui consistent à intercepter ou modifier les données circulant sur le réseau.
- **Réduction des risques liés à la surveillance passive**, notamment sur les réseaux Wi-Fi domestiques.

Le VPN est généralement configuré au niveau du routeur domestique, ce qui permet de sécuriser l'ensemble des objets connectés, même ceux dépourvus de capacités de chiffrement avancées, assurant ainsi une protection globale et homogène.

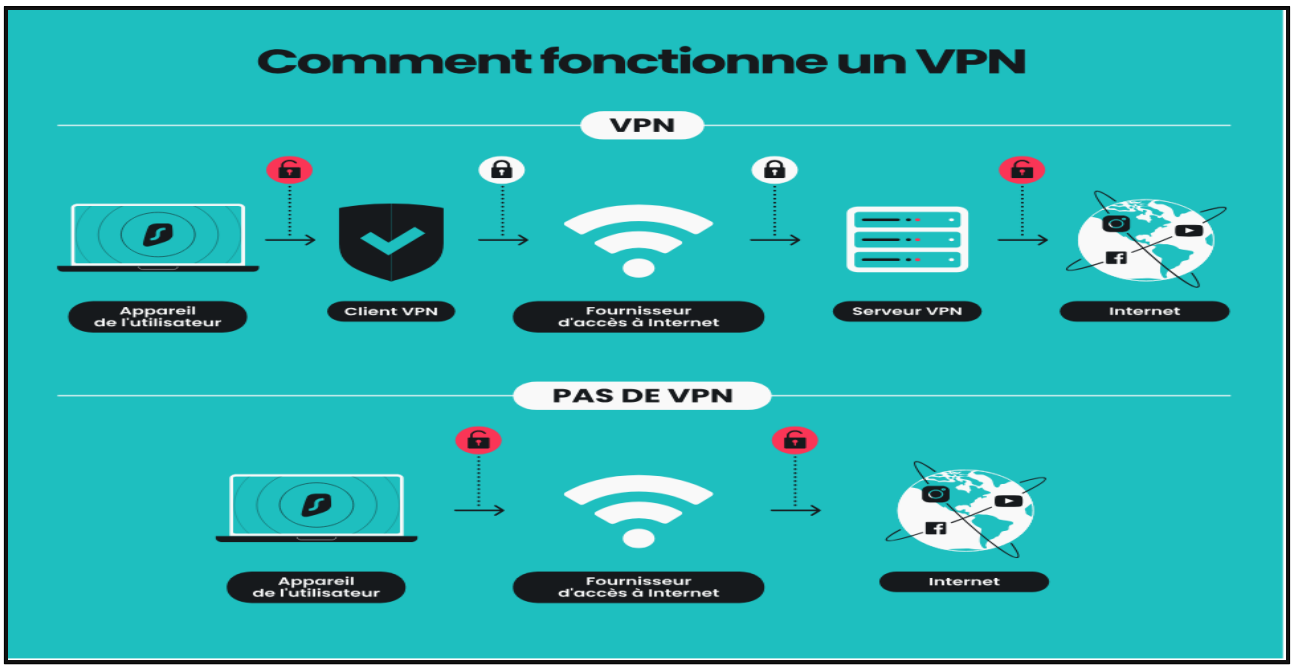


Figure 15: Fonctionnement d'un VPN.

a) Mécanismes de chiffrement et d'intégrité

Les VPN modernes s'appuient sur des **algorithmes cryptographiques robustes** assurant confidentialité, intégrité et authenticité. Parmi les plus utilisés dans les VPN IPsec ou OpenVPN :

- **Chiffrement AES (Advanced Encryption Standard)**

L'**Advanced Encryption Standard (AES)** est aujourd'hui la norme de référence pour le chiffrement symétrique dans les systèmes de communication sécurisés. Standardisé en 2001 par le **National Institute of Standards and Technology (NIST)** sous la publication **FIPS PUB 197**, il a été conçu pour succéder aux algorithmes **DES** et **3DES**, devenus vulnérables face aux avancées en cryptanalyse et à la puissance de calcul moderne.

◆ **Caractéristiques techniques**

AES repose sur un algorithme de **chiffrement symétrique par blocs**, dans lequel la même clé est utilisée pour le chiffrement et le déchiffrement. Il présente les paramètres suivants :

1. **Taille de bloc** : 128 bits (fixe), chaque message est segmenté en blocs traités de manière indépendante.
2. **Tailles de clé disponibles** : 128, 192 ou 256 bits.
3. **Nombre de rondes de transformation** :
    1. 10 rondes pour **AES-128**
    2. 12 rondes pour **AES-192**
    3. 14 rondes pour **AES-256**

Chaque ronde repose sur une architecture en **réseau de substitution-permutation (SPN)**, combinant les opérations suivantes :

- **SubBytes** : substitution non linéaire via une S-Box, résistant aux attaques différentielles.
- **ShiftRows** : permutation circulaire des lignes de l'état interne.
- **MixColumns** : transformation linéaire assurant la diffusion des bits dans chaque colonne.
- **AddRoundKey** : opération XOR avec une sous-clé dérivée de la clé principale.

Ces transformations implémentent les principes de **confusion** et **diffusion**, fondamentaux en cryptographie selon les travaux de **Claude Shannon**, afin de maximiser la résistance à l'analyse statistique et à la cryptanalyse linéaire.

◆ **Intégration dans les VPN**

AES est massivement utilisé dans les solutions **VPN modernes** (telles que **IPsec**, **OpenVPN**, ou **WireGuard**) pour assurer la **confidentialité** et l'**intégrité** des communications. Deux principaux **modes opératoires** sont couramment déployés :

- **CBC (Cipher Block Chaining)** : introduit un couplage entre les blocs successifs, renforçant la sécurité par dépendance contextuelle.
- **GCM (Galois/Counter Mode)** : combine chiffrement et authentification des données, réduisant la latence tout en assurant une sécurité renforcée.

Le mode **AES-256**, en particulier, est préféré dans les environnements critiques en raison de sa robustesse face aux attaques par force brute.

◆ **Accélération matérielle**

Les processeurs récents (Intel, AMD, ARM) prennent en charge les instructions **AES-NI (Advanced Encryption Standard New Instructions)**, permettant l'exécution matérielle des opérations cryptographiques AES. Cela présente plusieurs avantages :

- **Réduction de la consommation CPU**, permettant des performances élevées même sur des dispositifs embarqués.
- **Augmentation significative du débit de chiffrement**, crucial pour les VPN à haut volume de trafic.
- **Optimisation énergétique**, adaptée aux équipements connectés à ressources limitées (IoT, NAS, routeurs domestiques).

[25]

➢ **Fonction de hachage SHA-256 (Secure Hash Algorithm 256 bits)**

Le **SHA-256** est une fonction de hachage cryptographique conçue par la NSA et normalisée par le NIST. Elle prend en entrée un message de longueur arbitraire et produit une empreinte numérique (hash) de 256 bits, généralement représentée en hexadécimal. Cette fonction est largement utilisée en cybersécurité, cryptographie et technologies blockchain pour garantir l'intégrité, l'authenticité et la sécurité des données.

Dans le cadre des **VPN**, SHA-256 est employé pour assurer l'intégrité des données transmises, en générant une empreinte unique qui permet de détecter toute altération du message pendant le transport.

Étapes principales du fonctionnement de SHA-256 :

1. **Prétraitement (Padding)** : Le message est complété par un bit à 1 suivi de zéros, puis la longueur initiale du message est ajoutée pour atteindre un multiple de 512 bits.
2. **Division en blocs** : Le message est découpé en blocs de 512 bits.
3. **Initialisation** : Huit registres de 32 bits sont initialisés avec des constantes définies par la norme.
4. **Expansion** : Chaque bloc de 512 bits est étendu en 64 mots de 32 bits via des fonctions de permutation.
5. **Compression** : Chaque mot est traité sur 64 itérations impliquant des opérations logiques (AND, XOR, ROTR) et l'utilisation de constantes précalculées.
6. **Mise à jour des registres** : Les résultats modifient les registres d'état à chaque itération.
7. **Concaténation finale** : Après traitement de tous les blocs, l'empreinte SHA-256 est obtenue par la concaténation des registres finaux.

Propriétés essentielles de SHA-256 :

- **Résistance aux collisions** : Il est pratiquement impossible de trouver deux messages différents ayant la même empreinte.
- **Résistance à la préimage** : Il est extrêmement difficile de retrouver l'entrée originale à partir de l'empreinte.

- **Résistance à la seconde préimage** : Même en connaissant une entrée et son empreinte, trouver une autre entrée produisant la même empreinte est quasi impossible.
- **Effet avalanche** : Une modification minime de l'entrée modifie radicalement l'empreinte, renforçant la sécurité.

2.7.4.2 DNS chiffré (DoH / DoT) et rôle de l'ECC

Le **DNS chiffré** est une mesure de sécurité incontournable dans les environnements Smart Home, où chaque objet connecté échange régulièrement des requêtes DNS vers des services distants. Sans chiffrement, ces requêtes peuvent être interceptées et analysées par un attaquant, révélant la nature des objets présents, les services utilisés, ainsi que les habitudes des occupants. Pour protéger ces échanges, deux protocoles standards sont principalement utilisés :

a) DNS over HTTPS (DoH)

Le protocole **DoH** transmet les requêtes DNS encapsulées dans des sessions **HTTPS** via le port **443**. Grâce à l'utilisation de **TLS**, les requêtes DNS sont entièrement chiffrées, assurant la confidentialité et l'intégrité des échanges entre le client et le serveur DNS. De plus, en utilisant le protocole HTTP/2 ou HTTP/3, DoH masque les requêtes DNS dans le trafic HTTPS classique, ce qui complique la détection, l'interception ou la censure par des équipements réseaux.

b) DNS over TLS (DoT)

Le protocole **DoT** établit une connexion sécurisée exclusivement dédiée aux requêtes DNS en utilisant **TLS** sur le port **853**. Cette connexion chiffre toutes les requêtes et réponses DNS, assurant confidentialité, intégrité et authentification du serveur DNS. Bien que le trafic DoT soit facilement identifiable par son port spécifique, il offre un canal sécurisé robuste pour protéger les résolutions DNS contre l'écoute et la manipulation.

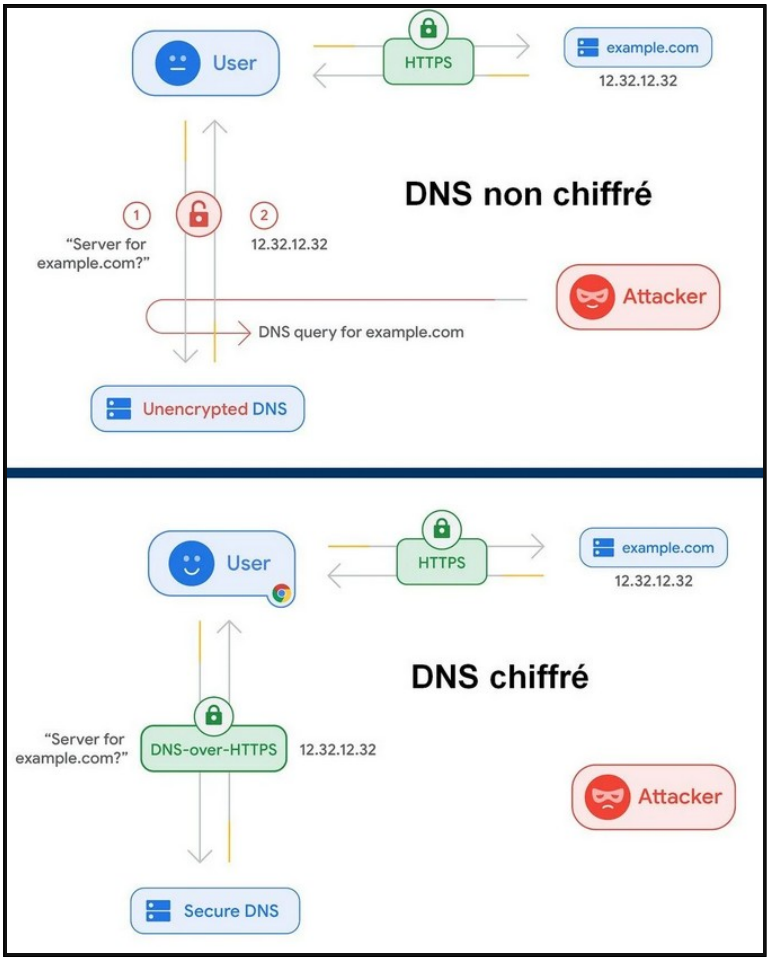


Figure 16: Comparaison entre requêtes DNS non chiffrées et chiffrées (DoH).

c) Intégration de la cryptographie à courbe elliptique (ECC)

La sécurité des canaux DNS chiffrés repose sur TLS, qui utilise largement la cryptographie à courbe elliptique (ECC) dans ses suites cryptographiques. ECC intervient notamment dans deux aspects essentiels :

- **Échange sécurisé de clés** : via l'algorithme ECDHE (Elliptic Curve Diffie-Hellman Ephemeral), qui permet de générer dynamiquement une clé de session partagée sans l'échanger directement. Ceci garantit la confidentialité parfaite des sessions (Perfect Forward Secrecy).
- **Authentification des serveurs DNS** : grâce aux certificats numériques utilisant l'algorithme ECDSA (Elliptic Curve Digital Signature Algorithm), qui offre un niveau de sécurité comparable à RSA, mais avec des clés beaucoup plus courtes et une meilleure efficacité de calcul.

ECC est aujourd'hui privilégiée dans TLS 1.3, notamment pour les implémentations de DNS over HTTPS (DoH) et DNS over TLS (DoT) fournies par des acteurs comme Cloudflare, Quad9 ou NextDNS. Cette adoption permet des connexions plus rapides, une charge CPU réduite, tout en

assurant une sécurité renforcée — par exemple, une clé ECC de 256 bits équivaut en sécurité à une clé RSA de 3072 bits.

Intégration dans les Smart Homes

Le chiffrement DNS avec ECC peut être mis en œuvre à différents niveaux dans une maison intelligente :

- Sur les objets connectés dont le firmware supporte DoH/DoT avec TLS et ECC.
- Sur le routeur domestique, via des firmwares comme OpenWRT ou pfSense, ou des serveurs DNS sécurisés (ex. Unbound), configurés pour établir des connexions TLS utilisant ECC vers les résolveurs DNS.
- Dans des environnements simulés ou limités (ex. Cisco Packet Tracer), la protection DNS chiffrée peut être symbolisée par des tunnels VPN sécurisés ou des ACL restrictives, qui bloquent le DNS classique (port 53) et n'autorisent que le trafic vers les résolveurs sécurisés (ports 443 pour DoH, 853 pour DoT).[22]

2.7.4.3 Injection de trafic ou trafic dummy

L'injection de trafic, également appelée **trafic dummy**, est une technique avancée de protection de la confidentialité visant à **perturber l'analyse des métadonnées réseau**. Cette méthode consiste à générer délibérément des paquets de données factices ou à introduire des **délais aléatoires** dans la transmission des messages légitimes, dans le but d'obscurcir les caractéristiques temporelles, volumétriques et comportementales du trafic réel. [22]

a) Techniques utilisées

- **Génération de paquets factices (Padding)** : Injection de paquets additionnels simulant le trafic réel pour masquer le volume et la fréquence des communications authentiques. Ces paquets sont conçus pour avoir des tailles et des caractéristiques similaires au trafic légitime afin de se fondre efficacement dans le flux global.
- **Obfuscation temporelle (Random Delay Injection)** : Introduction de délais aléatoires entre l'envoi des paquets afin de perturber les analyses basées sur les schémas temporels. Cette variabilité rend plus difficile la corrélation des événements et l'identification des comportements réseau.
- **Traffic Morphing** : Modification dynamique des caractéristiques du trafic, telles que la taille des paquets et la fréquence d'émission, pour imiter d'autres types de flux. Cette technique complique la classification et le filtrage du trafic par des outils de surveillance.
- **Mix Networks (Mélange et Reordonnancement)** : Regroupement de paquets provenant de plusieurs sources et réarrangement de leur ordre, souvent combiné avec des délais aléatoires. Cette méthode casse les liens directs entre émetteurs et récepteurs, renforçant l'anonymat.
- **Cover Traffic Injection** : Maintien d'un flux continu et constant de trafic factice pour créer un bruit de fond permanent, masquant ainsi toute variation dans le trafic réel.

b) Limites et contraintes en Smart Homes

- **Consommation accrue de bande passante** : L'injection de paquets factices augmente le trafic total, ce qui peut saturer les connexions Internet domestiques limitées. Cela provoque des ralentissements et peut générer des coûts additionnels pour les forfaits avec quotas. Cette surcharge affecte la fluidité globale du réseau domestique.
- **Impact sur la latence et la qualité de service (QoS)** : Les délais artificiels ajoutés perturbent la synchronisation normale des paquets, augmentant latence et jitter. Ces effets sont particulièrement nuisibles pour la vidéo en streaming, la VoIP et les commandes domotiques sensibles au temps réel. Une mauvaise gestion de ces délais peut dégrader l'expérience utilisateur.
- **Complexité d'implémentation sur des objets aux ressources limitées** : Les objets IoT ont souvent des capacités processeur et mémoire réduites, ainsi qu'une autonomie énergétique limitée. Les algorithmes d'injection de trafic demandent des ressources importantes, risquant d'affecter la stabilité et la durée de vie des appareils. Cette contrainte freine l'adoption de cette technique à grande échelle.

2.7.5 Sécurité distribuée via la blockchain dans les Smart Homes

La **blockchain** émerge comme une technologie prometteuse pour renforcer la sécurité des **maisons intelligentes**. En tant que registre distribué, immuable et transparent, elle permet l'enregistrement sécurisé des événements et transactions sans nécessiter d'entité centrale. Dans le contexte des Smart Homes, où la multiplication des objets connectés augmente la surface d'attaque, la blockchain offre un cadre sécurisé et décentralisé pour la gestion des accès, l'authentification, la traçabilité et la protection des données.

2.7.5.1 Applications concrètes de la blockchain dans les Smart Homes :

- **Journalisation inviolable des événements critiques** : Chaque action sensible (comme l'ouverture de porte ou l'activation d'une alarme) peut être enregistrée dans une blockchain, garantissant l'intégrité des journaux et empêchant toute falsification.
- **Authentification sécurisée des utilisateurs et des objets** : Grâce à des certificats numériques inscrits dans la blockchain, chaque entité du réseau (utilisateur, capteur, appareil) peut être identifiée de manière unique et fiable, réduisant les risques d'usurpation d'identité.
- **Exécution automatique de règles de sécurité via des smart contracts** : Ces programmes autonomes permettent de déclencher des actions uniquement si certaines conditions de sécurité sont remplies. Par exemple, une serrure intelligente ne s'ouvre que si la requête provient d'un utilisateur autorisé et que le contexte horaire est conforme.
- **Sécurisation des mises à jour logicielles (firmware)** : Les firmwares peuvent être vérifiés via leur empreinte inscrite dans la blockchain avant installation, garantissant leur origine et intégrité, et empêchant toute mise à jour malveillante.

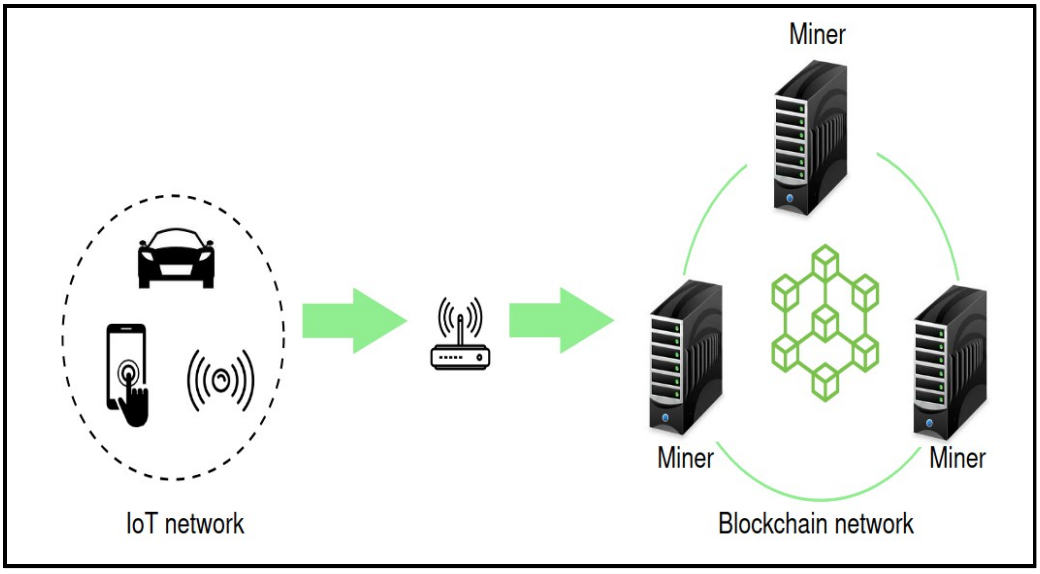


Figure 17: Architecture de la Blockchain.

2.7.5.2 Avantages supplémentaires :

- **Décentralisation** : La blockchain élimine le besoin d'une autorité centrale, réduisant ainsi les points de défaillance uniques et les risques associés.
- **Transparence et traçabilité** : Toutes les transactions sont enregistrées de manière transparente, permettant une traçabilité complète des actions et facilitant les audits de sécurité.
- **Résilience accrue** : En répartissant les données sur plusieurs nœuds, la blockchain offre une résistance supérieure aux attaques et aux pannes système.

Des recherches récentes ont démontré l'efficacité de la blockchain dans le renforcement de la sécurité des Smart Homes. Par exemple, une étude a proposé une architecture de passerelle domestique intelligente basée sur la blockchain pour contrer les attaques potentielles sur les passerelles des maisons intelligentes, en assurant la confidentialité, l'intégrité et l'authentification des données transmises . Une autre recherche a présenté un système de maison intelligente basé sur la blockchain conçu pour surveiller en continu les appareils IoT, assurant une gestion sécurisée des données et une prédiction de la consommation d'énergie [20].

Bien que l'intégration de la blockchain dans les foyers classiques soit encore limitée en raison de contraintes techniques et énergétiques, elle constitue une contre-mesure robuste face aux menaces réseau, aux falsifications de journaux, aux usurpations d'identité et aux intrusions invisibles. Son adoption croissante dans les architectures de sécurité des Smart Homes témoigne de son potentiel à transformer la manière dont nous sécurisons nos environnements domestiques intelligents.

2.8 Normes et bonnes pratiques

La sécurisation des environnements IoT, notamment dans les maisons intelligentes, repose sur l'adoption de **normes industrielles reconnues** et sur l'application de **bonnes pratiques de cybersécurité** tout au long du cycle de vie des dispositifs connectés. Ces mesures permettent de garantir une protection proactive contre les menaces potentielles.

- **Norme ETSI EN 303 645**

Élaborée par l'**European Telecommunications Standards Institute (ETSI)**, cette norme constitue une référence incontournable pour la cybersécurité des appareils IoT grand public. Elle définit une **liste de 13 exigences de base** et de **recommandations supplémentaires** visant à :

- **Éliminer les identifiants par défaut** (comme admin/admin), en forçant la création d'un mot de passe unique et robuste.
- **Assurer des mises à jour logicielles sécurisées**, incluant la vérification de l'intégrité du firmware et l'authentification de la source.
- **Limiter l'exposition des interfaces réseau**, en désactivant les ports non utilisés ou en appliquant des mécanismes de contrôle d'accès.
- **Protéger les données sensibles** stockées et transmises (chiffrement, anonymisation, gestion des clés).
- **Garantir la résilience du système** face aux attaques de type DDoS ou brute-force.

Cette norme s'applique aussi bien aux fabricants qu'aux développeurs d'applications ou aux intégrateurs de solutions IoT.

- **Recommandations de la IoT Security Foundation (IoTSF)**

La **IoTSF** propose une série de **livres blancs**, de **cadres méthodologiques** et d'outils pour aider les acteurs du domaine à concevoir des produits IoT sûrs. Ses principales lignes directrices comprennent :

- Une **approche par niveau de risque**, basée sur l'analyse de la menace et du contexte d'usage.
- L'application du **principe du moindre privilège** dans la gestion des droits d'accès.
- L'**évaluation continue des vulnérabilités** et la gestion réactive des incidents de sécurité.
- Des **guides sectoriels** (domotique, santé, automobile…) adaptés aux contraintes spécifiques de chaque domaine.

- **Principe de Security by Design**

Le concept de *Security by Design* implique que la sécurité ne soit pas une option ajoutée après la mise en service du dispositif, mais une **composante intrinsèque de l'architecture IoT** :

- Intégration de la sécurité **dès la phase de conception** (choix de microcontrôleurs sécurisés, systèmes d'exploitation durcis…).
- Mise en œuvre de mécanismes **proactifs** (chiffrement, authentification mutuelle, journalisation des événements).
- Tests de sécurité **dès le développement**, via des outils d'analyse statique/dynamique et des tests de pénétration.

2.9 Limites des solutions actuelles et défis persistants

Malgré l'existence de nombreuses contre-mesures et standards, la **sécurité des Smart Homes** reste un domaine **complexe, imparfait et en constante évolution**. La mise en œuvre des solutions de protection se heurte à plusieurs obstacles, tant techniques qu'organisationnels, qui ralentissent leur adoption et en limitent l'efficacité. Cette section met en lumière les principales limites actuelles et les défis persistants auxquels les chercheurs, industriels et utilisateurs doivent faire face.

2.9.1 Complexité pour les utilisateurs finaux

L'un des obstacles majeurs est la **complexité d'utilisation des outils de sécurité** pour les non-initiés. La majorité des solutions proposées nécessitent une **configuration manuelle**, une **connaissance des réseaux**, ou une **compréhension fine des risques**, ce qui dépasse les compétences du grand public.

- Peu de systèmes intègrent une **automatisation intelligente** des mesures de protection.
- Les interfaces de configuration sont souvent **peu intuitives**.
- Certaines contre-mesures (ex. : segmentation réseau, VPN local, filtrage DNS) nécessitent des manipulations techniques peu accessibles aux utilisateurs lambda.

Cela crée un **décalage entre les bonnes pratiques théoriques** et la **réalité de leur mise en œuvre**, laissant de nombreuses maisons intelligentes **sous-protégées malgré les recommandations disponibles**.

2.9.2 Incompatibilités entre équipements

Le marché de la domotique est extrêmement fragmenté, avec une multitude de fabricants, chacun utilisant **ses propres protocoles, formats, interfaces et niveaux de sécurité**. Cette absence d'uniformisation complique l'intégration des équipements et empêche une **gestion centralisée cohérente de la sécurité**.

- Les dispositifs peuvent **ne pas communiquer entre eux**, ou fonctionner partiellement.
- Certains équipements ne permettent **aucune modification de paramètres de sécurité** (ports ouverts, firmware bloqué, etc.).
- Le manque de **standards universels** ralentit l'adoption de solutions transversales de sécurité.

Même les plateformes domotiques centralisées (ex. : Alexa, HomeKit, SmartThings) souffrent de **limitations liées à l'interopérabilité**, ce qui fragilise la chaîne de protection globale.

2.9.3 Manque de réglementation mondiale

Actuellement, la **réglementation relative à la sécurité des objets connectés est insuffisante**, voire inexistante dans de nombreux pays. Il n'existe **aucune obligation stricte** pour les fabricants d'intégrer des protections minimales dans leurs produits IoT.

- La mise sur le marché ne requiert **pas de certification de sécurité** dans la majorité des cas.
- Les objets connectés vulnérables continuent d'être vendus et utilisés à grande échelle.
- Même des produits grand public de grandes marques peuvent présenter **des défauts de sécurité graves**.

Ce **vide réglementaire** laisse la responsabilité de la protection au seul utilisateur final, ce qui est irréaliste dans un contexte grand public. Certaines initiatives (comme la norme **ETSI EN 303 645**) commencent à encadrer le secteur, mais leur adoption reste volontaire dans la plupart des régions.

2.9.4 Menaces en constante évolution

La cybersécurité des Smart Homes est confrontée à des **menaces dynamiques**, qui évoluent aussi rapidement que les technologies elles-mêmes. L'introduction de l'**intelligence artificielle** dans les assistants vocaux, les caméras intelligentes ou les plateformes de gestion rend l'environnement plus complexe et donc plus vulnérable.

- Les **deepfakes vocaux** permettent désormais de duper des systèmes à reconnaissance vocale.
- Les modèles d'IA embarqués peuvent être manipulés (adversarial attacks).
- Des **attaques comportementales** sont en cours d'expérimentation pour tromper les routines intelligentes (ex. : provoquer des déclenchements par imitation d'usage normal).

La capacité des attaquants à **s'adapter plus vite que les défenses**, associée à la **vulnérabilité systémique des objets non maintenus**, laisse présager une **augmentation du niveau de risque** dans les années à venir.

2.10 conclusion

L'essor des Smart Homes marque une avancée majeure dans la numérisation de notre quotidien, offrant aux utilisateurs un **confort inégalé, une gestion optimisée des ressources** et une interaction fluide avec leur environnement domestique. Toutefois, cette transformation s'accompagne de **nouveaux défis de sécurité** considérables, directement liés à la nature distribuée, interconnectée et souvent sous-sécurisée de ces systèmes.

Ce chapitre a permis d'identifier les **principales menaces techniques, physiques et comportementales** auxquelles les maisons intelligentes sont confrontées. Il a également mis en lumière les **vulnérabilités structurelles** spécifiques aux protocoles IoT, aux configurations par

défaut, à la dépendance au cloud et à l'absence de mise à jour logicielle. En réponse à ces risques, une série de **contre-mesures réalistes et hiérarchisées** a été présentée, couvrant la sécurisation du réseau, des objets, des données personnelles, ainsi que l'adoption de bonnes pratiques et de standards internationaux.

Néanmoins, l'application de ces mesures reste limitée par des **contraintes techniques, économiques et humaines**, notamment la complexité de mise en œuvre, la fragmentation du marché et l'évolution rapide des menaces. Il apparaît donc nécessaire de **tester concrètement la faisabilité** de certaines de ces solutions dans un environnement simulé.

C'est dans cette optique que le **chapitre suivant** *présentera une* **implémentation pratique d'une Smart Home sécurisée à l'aide de Cisco Packet Tracer**. *À travers cette simulation, nous illustrerons plusieurs concepts clés abordés dans ce chapitre :* **segmentation réseau, contrôle d'accès, logique conditionnelle de sécurité, et gestion des interactions entre objets connectés**.

Chapitre 3:Simulation .

3.1 Introduction

L'évolution des maisons intelligentes repose sur des infrastructures réseau fiables et sécurisées, capables de gérer un grand nombre de dispositifs IoT variés et de garantir la confidentialité des données. Face à la complexité croissante de ces environnements, la simulation de réseaux constitue un outil indispensable pour évaluer et valider les architectures, protocoles et mécanismes de sécurité avant tout déploiement réel. Elle permet d'anticiper les dysfonctionnements, d'optimiser la performance et d'assurer la robustesse du système global. Ce chapitre présente une simulation complète d'une smart home sécurisée, s'appuyant sur les techniques abordées dans le chapitre précédent, et détaille la conception, la mise en œuvre ainsi que les tests réalisés pour garantir la sécurité et la fiabilité du réseau domestique intelligent. Plusieurs scénarios pratiques illustrent le comportement du système face à différents usages et menaces potentielles.

3.2 Utilité de la simulation des réseaux dans les Smart Homes

La simulation réseau constitue un outil essentiel dans la conception, l'analyse et la sécurisation des environnements intelligents tels que les Smart Homes. Elle présente de nombreux avantages, notamment :

- **Évaluation sans matériel physique** : La simulation permet de concevoir et tester des architectures réseau complètes sans recourir à des équipements réels, réduisant ainsi les coûts et les contraintes logistiques.
- **Analyse du comportement des objets connectés (IoT)** : Elle facilite l'observation du fonctionnement et des interactions entre les différents objets intelligents, dans divers scénarios d'usage.
- **Vérification des mécanismes de sécurité** : Les configurations de sécurité telles que les VPN, les listes de contrôle d'accès (ACL), ou encore les protocoles d'authentification centralisée peuvent être implémentées et validées dans un environnement contrôlé.
- **Détection des points de vulnérabilité** : Grâce à la simulation, il est possible d'identifier les failles potentielles de l'architecture, et d'envisager des solutions correctives avant le déploiement réel.
- **Formation et renforcement des compétences** : Les plateformes de simulation offrent un cadre pédagogique idéal pour s'initier ou se perfectionner dans la configuration, le déploiement et la sécurisation des réseaux domestiques intelligents.

3.3 Travaux similaires

Dans le cadre de ce mémoire, nous avons identifié plusieurs travaux académiques portant sur des thématiques connexes à notre projet de simulation d'une maison intelligente sécurisée. Ces mémoires abordent divers aspects techniques tels que l'assistance aux personnes, la domotique connectée et l'usage de Cisco Packet Tracer pour la simulation IoT. Ci-dessous, nous présentons trois exemples pertinents.

Travail [26]

Titre : *Développement et simulation d'une maison intelligente dédiée pour des personnes handicapées basée sur l'IoT*

Réalisé par Hanane Messaoud et Sarra Chourouk Sidi Bachir, ce travail propose de modéliser et simuler une maison intelligente exploitant l'Internet des objets afin d'améliorer l'autonomie des personnes en situation de handicap. Les auteurs ont utilisé UML pour la modélisation fonctionnelle et Cisco Packet Tracer pour le développement et la validation du système. L'étude met l'accent sur les aspects liés à l'accessibilité et à l'assistance, mais ne traite pas les mécanismes de sécurisation réseau, tels que la segmentation par VLAN ou l'utilisation de VPN pour la confidentialité des échanges.

Travail [27]

Titre : *IoT-based Smart Home System for Elderly and Disabled Assistance*

Réalisé par Mhd. Wasim Raed, Ilham Huseyinov, Ghina Ozdemir, Igor Kotenko et Elena Fedorchenko, ce projet propose un système domotique piloté à distance via un client 3G/4G et un serveur IoT. Le système intègre plusieurs capteurs (flamme, mouvement, ouverture de porte) connectés en Wi-Fi à une passerelle. La simulation a été réalisée à l'aide de Cisco Packet Tracer. L'étude présente une interface de contrôle à distance fonctionnelle, mais n'aborde pas les aspects de segmentation réseau ni de mécanismes d'authentification sécurisée.

Travail [28]

Titre : *Simulation d'un réseau domotique à base d'Internet des Objets*

Réalisé par Lamia Ouabba et Siham Mehah, ce mémoire présente la conception d'un modèle réduit de maison intelligente intégrant des scénarios automatisés axés sur le confort, la sécurité et l'économie d'énergie. La simulation est effectuée avec Cisco Packet Tracer. Bien que riche en fonctionnalités domotiques, ce travail ne traite pas les aspects de protection des échanges réseau ni les mécanismes de contrôle d'accès sécurisés.

3.4 Méthodologie et outils

3.4.1 Outil principal – Cisco Packet Tracer

Cisco Packet Tracer est un environnement de simulation réseau interactif développé par Cisco Systems. Il constitue un outil pédagogique de référence, notamment dans les formations CCNA (Cisco Certified Network Associate) et autres cursus orientés réseau. Son principal avantage réside dans sa capacité à reproduire virtuellement des scénarios réels de configuration, de communication et de sécurisation des réseaux.

Il permet la **création de topologies réseau complètes**, intégrant une large gamme d'équipements Cisco (routeurs, commutateurs, terminaux, points d'accès, pare-feu ASA), mais aussi des **objets connectés (IoT)**, tels que des capteurs, des caméras, des lampes ou des microcontrôleurs (MCU).

Les utilisateurs peuvent interconnecter ces dispositifs pour concevoir des environnements complexes et dynamiques, comme ceux d'une **maison intelligente**.

Parmi ses fonctionnalités clés, on peut citer :

- **Interface graphique intuitive** : glisser-déposer des équipements, connexion facile des interfaces, visualisation claire de la topologie.
- **Support du CLI Cisco (Command Line Interface)** : permet de configurer les appareils de façon réaliste, comme sur du matériel réel, en utilisant les mêmes commandes IOS.
- **Simulation de protocoles réseau** : DHCP, DNS, HTTP, FTP, ICMP, SSH, telnet, RIP, OSPF, ACLs, VLANs, VPN, etc.
- **Scénarios IoT** : interactions via des capteurs (fumée, température, mouvement), actionneurs (moteurs, LED, portes), automatisation avec microcontrôleurs programmables (langage de type C).
- **Composants de sécurité** : configuration de pare-feux ASA, VPN simulés, filtrage avec ACL standard ou étendues.

L'outil dispose aussi d'un **mode simulation** qui permet de visualiser le flux des paquets en temps réel, facilitant l'analyse des échanges réseau et la détection d'anomalies. Cela s'avère particulièrement utile pour tester la réaction du réseau face à des attaques simulées ou à des comportements anormaux.

3.4.2 Méthode

La méthode suivie repose sur la conception d'une architecture réseau intelligente, la configuration des protocoles de base, puis l'intégration progressive de mesures de sécurité. Chaque configuration est testée à travers des scénarios pratiques simulés dans Cisco Packet Tracer. Cette approche permet d'évaluer la robustesse du réseau face à différents contextes. Cela permet d'observer le comportement du réseau dans divers scénarios pratiques et sécuritaires.

3.4.3 Outils complémentaires

En plus de Cisco Packet Tracer, des outils comme **GNS3** et **Wireshark** peuvent être utilisés pour compléter l'analyse. **GNS3** permet une simulation plus avancée et réaliste des réseaux avec des images réelles d'IOS, tandis que **Wireshark** sert à capturer et analyser le trafic réseau en détail, notamment pour observer le comportement des protocoles et identifier d'éventuelles failles de sécurité. Ces outils offrent une vision plus approfondie des scénarios testés

3.5 Architecture simulée

Dans notre travail, nous avons d'abord simulé une Smart Home sans mesures de sécurité, puis nous avons intégré progressivement plusieurs mécanismes de protection.

3.5.1 Architecture simulée (sans mesures de securite)

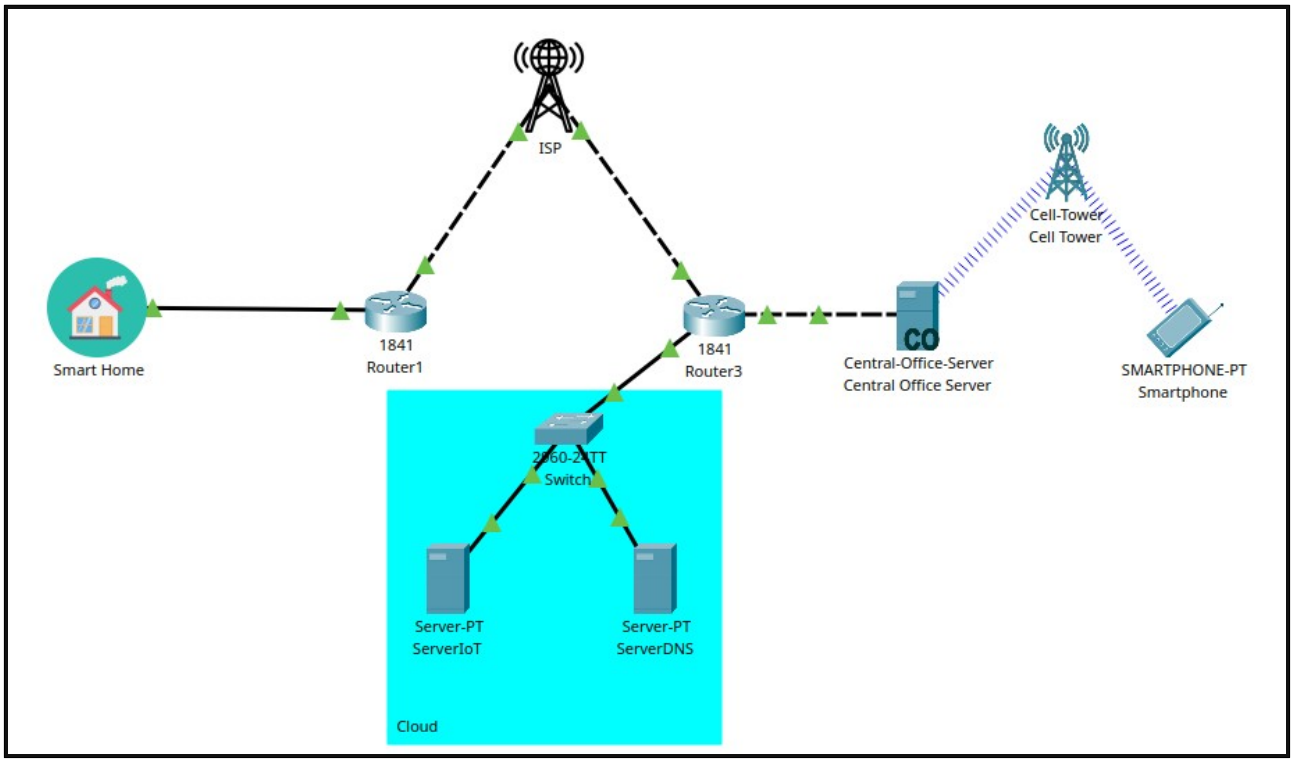


Figure 18 : Schéma global de la topologie réseau .

3.5.1.1 Équipements utilisés

- **Home Gateway**

  Passerelle centrale de la maison intelligente. Elle connecte, coordonne et contrôle tous les objets IoT locaux, assurant la gestion domotique interne.

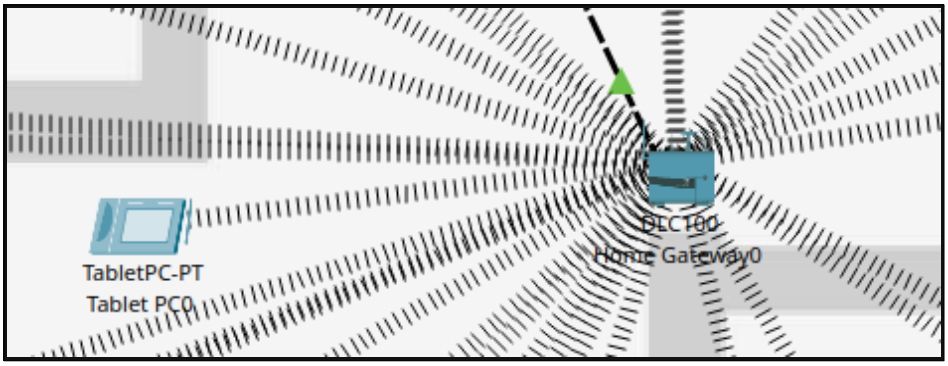


Figure 19 : La passerelle Home Gateway .

➢ **Paramètres de configuration de HomeGateway0 :**

- **SSID** : `HomeGateway0`

- **Sécurité** : WPA2-PSK

- **Mot de passe** : `smarthome`

- Chiffrement : AES

-DHCP activé : `192.168.25.2 – 192.168.25.200`

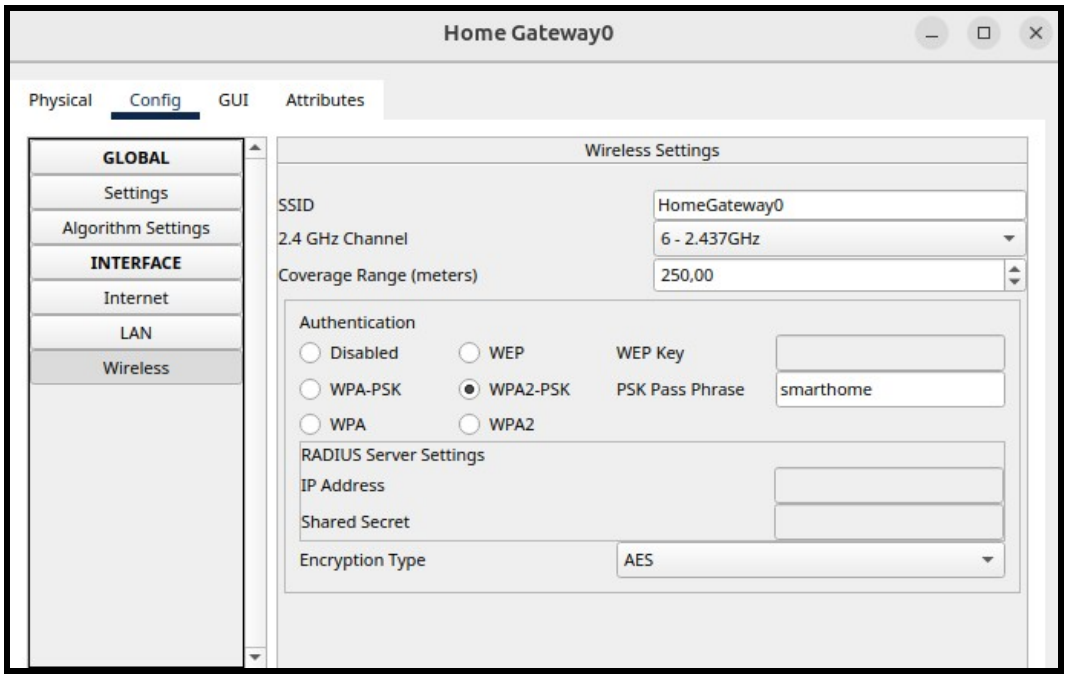


Figure 20 : Interface de configuration de la passerelle HomeGateway0 .

- **Capteurs (température, fumée, mouvement)**

  Dispositifs de détection transmettant les données environnementales à la passerelle ou au microcontrôleur pour traitement et réaction.

- **Actionneurs (lumières, prises, caméras, serrures)**

  Exécutent automatiquement des actions suite à des événements (ex. ouverture de porte, activation d'alarme, allumage de lumière).

- **Microcontrôleur (MCU**

  Interface de logique locale qui déclenche des actions basées sur les signaux des capteurs (ex. détection incendie → activer alarme).

- **PCs et Tablettes**

  Outils d'administration locale de la maison. Permettent la configuration, la surveillance en temps réel, et le contrôle manuel des équipements.

- **Routeur sans fil**

  Fournit l'accès Internet et relie le réseau domestique au monde extérieur. Sert de lien entre la maison et les services distants.

- **Switch (Cisco 2960)**

  Commutateur réseau interconnectant les équipements filaires (PC, serveurs, passerelle) dans le réseau local.

- **Serveur IoT**

  Point d’accès distant centralisé. Il héberge les interfaces de contrôle à distance (web/mobile) et relaie les commandes vers la maison.

- **Serveur DNSWPA2**

  Gère la résolution des noms de domaine dans le réseau pour permettre un accès simplifié aux services internes et distants.

- **Centrale Office Server**

  Représente le service cloud externe d’un fournisseur. Sert à superviser et collecter les données de plusieurs maisons intelligentes.

- **Smartphone**

  Principal outil d’accès à distance. Via des applications mobiles connectées au serveur IoT, il permet à l’utilisateur de contrôler, surveiller et gérer la maison intelligente depuis n’importe quel lieu avec une connexion Internet sécurisée.

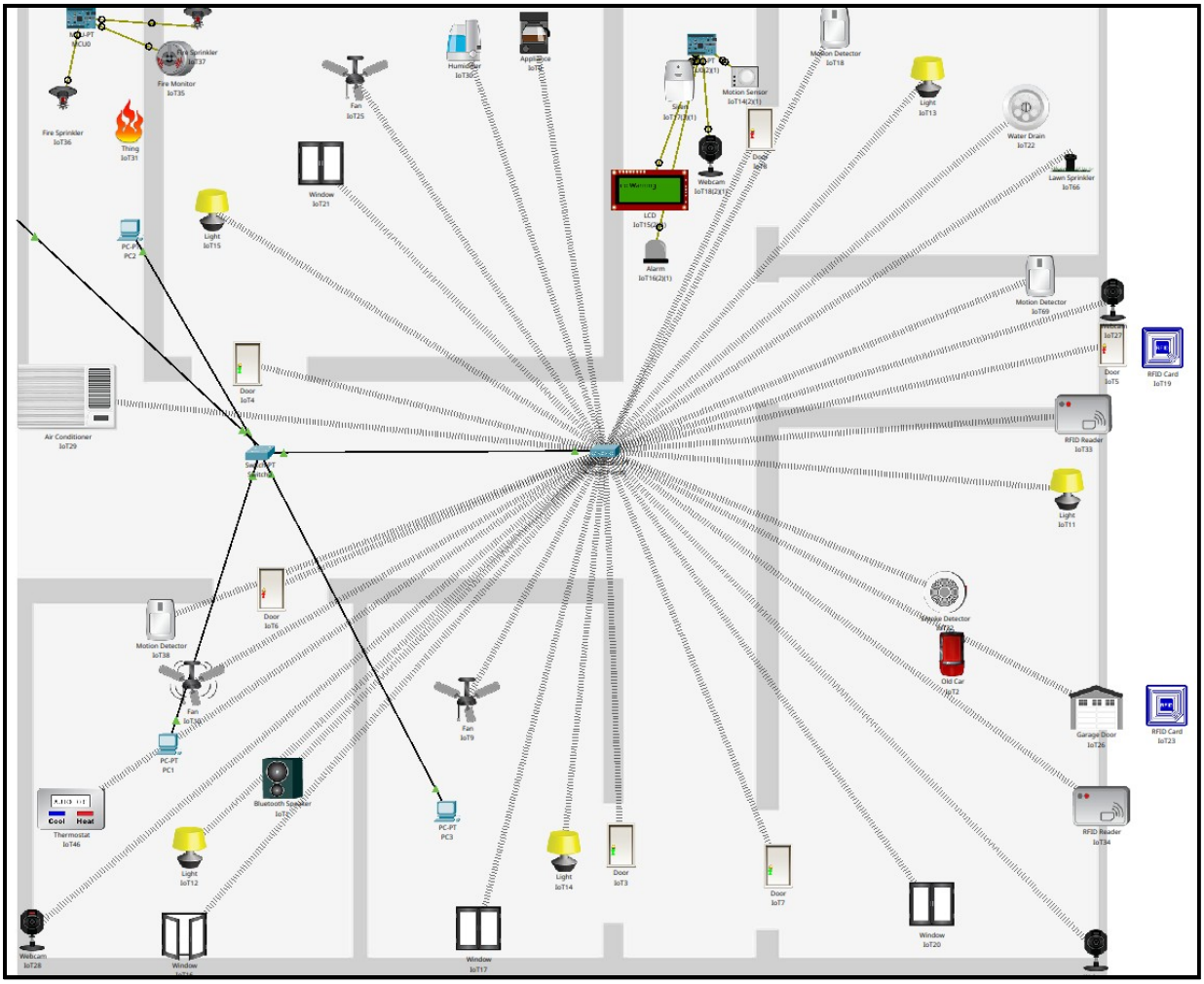


Figure 21 : Vue d'ensemble de l'architecture de la maison intelligente simulée.

3.5.1.2 Scénarios simulés – Fonctionnalités de base

a) Accès à distance via le serveur IoT

- **Connexion à l'interface web du serveur IoT** (via smartphone ou PC distant) :

La page de connexion permet à l'administrateur d'accéder à l'interface de gestion du serveur IoT depuis un smartphone ou un PC. L'accès se fait en saisissant un nom d'utilisateur et un mot de passe sécurisés. Une fois connecté, l'administrateur peut gérer les objets connectés, surveiller l'état du réseau et configurer les paramètres de sécurité.

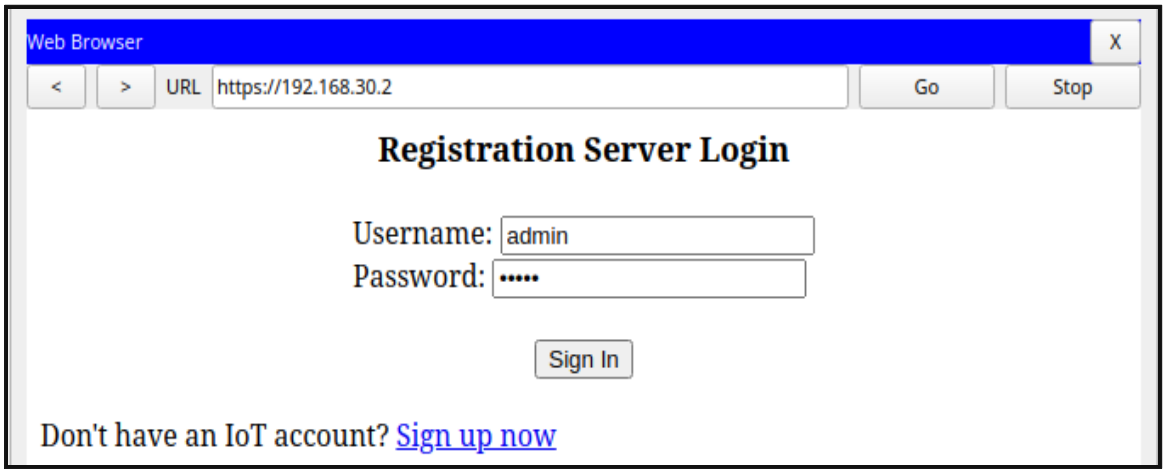


Figure 22 : page de connexion au serveur IoT

- **liste des objets connectés**

Après l'enregistrement dans le serveur IoT, une **liste des objets connectés** s'affiche dans l'interface. On y retrouve les **caméras**, **capteurs** (température, fumée, mouvement), **lampes intelligentes**, etc. Chaque objet est identifié par son nom, son état (actif/inactif) et peut être surveillé ou contrôlé à distance.

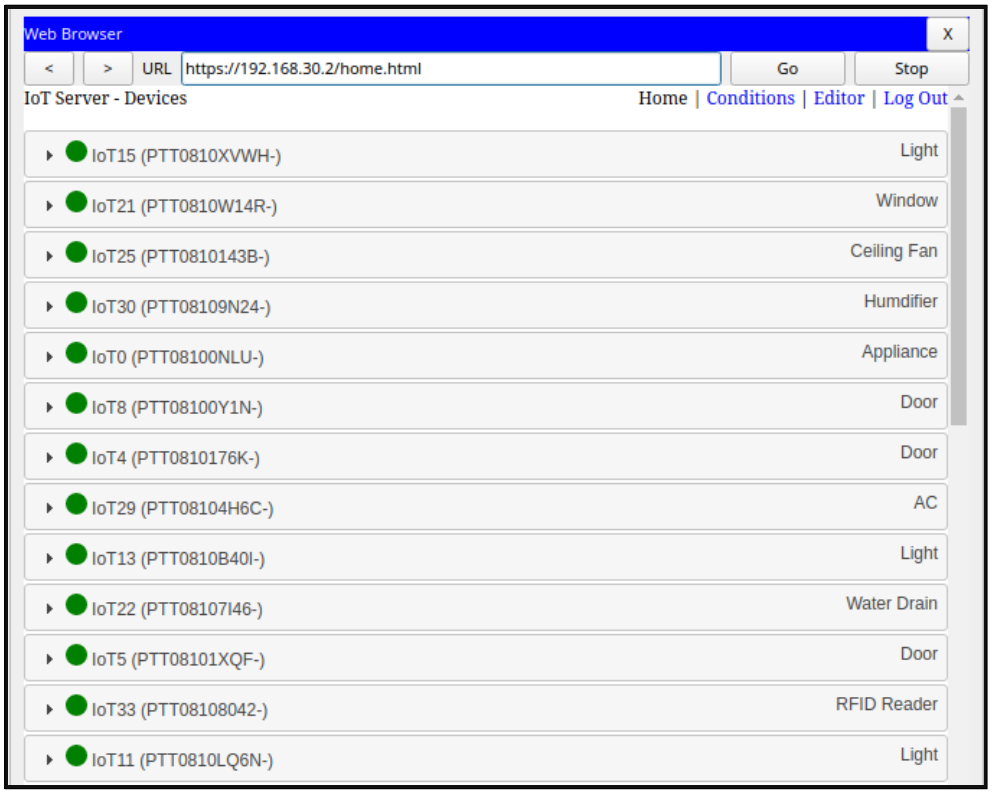
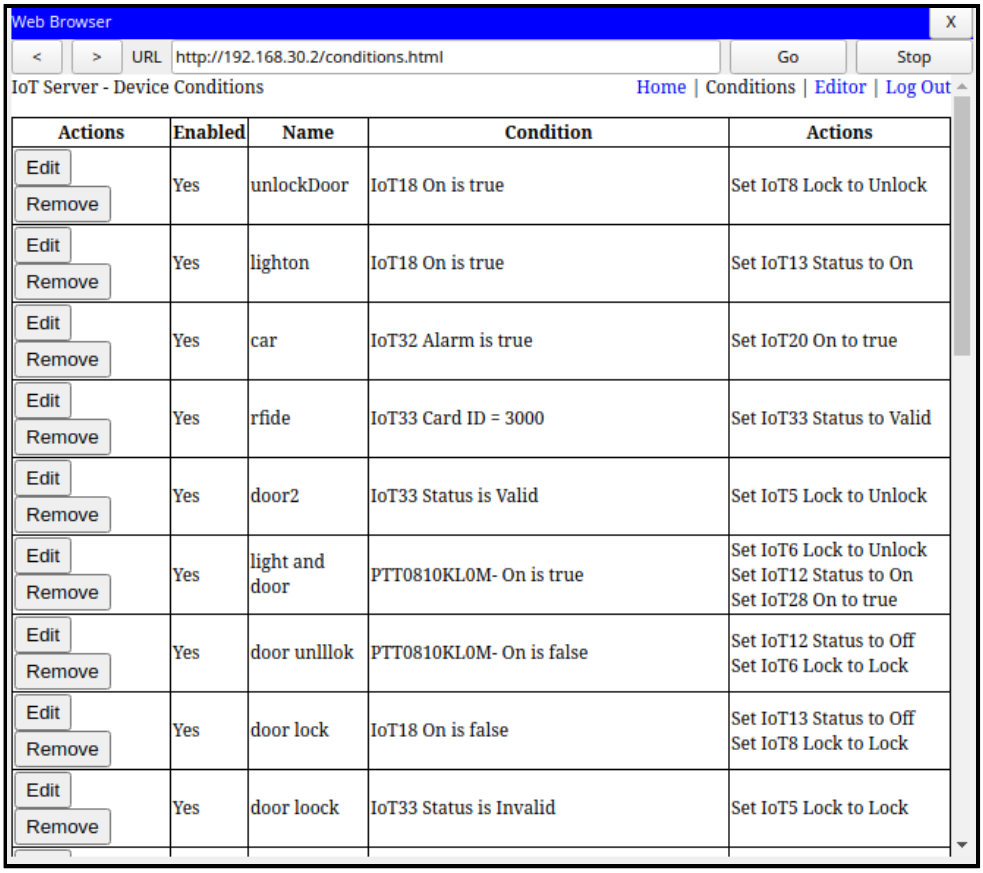


Figure 23 : Affichage des objets connectés enregistrés sur le serveur IoT .

• Conditions associées aux objets IoT

L'interface permet aussi de configurer des **conditions logiques** associées aux objets connectés. Par exemple, une porte peut être déverrouillée si une carte RFID valide est détectée, ou une lumière peut s'allumer automatiquement en fonction d'un capteur de mouvement ou d'un bouton poussoir. Ces règles conditionnelles renforcent l'automatisation et la sécurité dans l'environnement smart home.



Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	unlockDoor	IoT18 On is true	Set IoT8 Lock to Unlock
Edit Remove	Yes	lighton	IoT18 On is true	Set IoT13 Status to On
Edit Remove	Yes	car	IoT32 Alarm is true	Set IoT20 On to true
Edit Remove	Yes	rfide	IoT33 Card ID = 3000	Set IoT33 Status to Valid
Edit Remove	Yes	door2	IoT33 Status is Valid	Set IoT5 Lock to Unlock
Edit Remove	Yes	light and door	PTT0810KL0M- On is true	Set IoT6 Lock to Unlock Set IoT12 Status to On Set IoT28 On to true
Edit Remove	Yes	door unlllok	PTT0810KL0M- On is false	Set IoT12 Status to Off Set IoT6 Lock to Lock
Edit Remove	Yes	door lock	IoT18 On is false	Set IoT13 Status to Off Set IoT8 Lock to Lock
Edit Remove	Yes	door loock	IoT33 Status is Invalid	Set IoT5 Lock to Lock

Figure 24 : Conditions configurées dans le serveur IoT

b) Scénario 1 : Ouverture de porte via badge RFID

Dans ce scénario, un utilisateur approche un badge RFID du **lecteur RFID** placé à l'entrée de la maison. Le **lecteur RFID** lit l'identifiant (ID) du badge et le transmet au système de contrôle (ex. : serveur ou contrôleur local) pour vérification.

- **Si l'ID est valide** :
  - Un signal est envoyé à la **serrure électronique** pour déverrouiller la porte.
  - Une **LED verte** s'allume pour indiquer un accès autorisé.
  - La **caméra de sécurité** s'active automatiquement pour enregistrer l'entrée ou permettre une visualisation en temps réel.

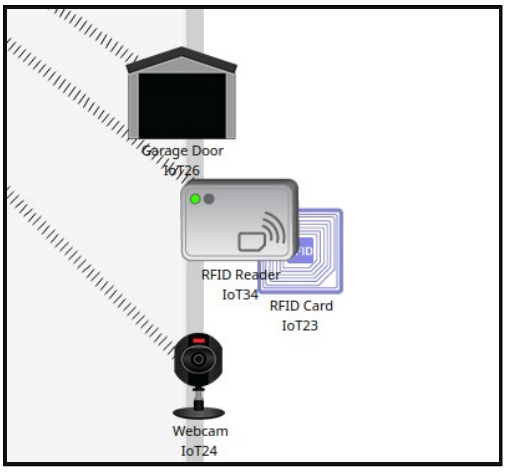


Figure 25 : Lecture du badge RFID

c) Scénario : Détection de mouvement et activation de la caméra de surveillance

Dans ce scénario, un **capteur de mouvement (motion detector)** est installé dans une pièce sensible de la maison (ex. : entrée, salon). Lorsqu'il **détecte une présence ou un mouvement**, il envoie immédiatement une notification au **serveur IoT**.

Le **serveur IoT**, en réponse à cet événement, déclenche automatiquement les actions suivantes :

- **Activation de la caméra de sécurité**,
- **Lancement de l'enregistrement vidéo**,
- **Sauvegarde des images ou vidéos** sur un stockage local ou distant.

Ce scénario permet une **surveillance réactive et intelligente**, en n'activant la caméra qu'en cas de détection réelle, ce qui optimise la sécurité tout en réduisant la consommation de ressources.

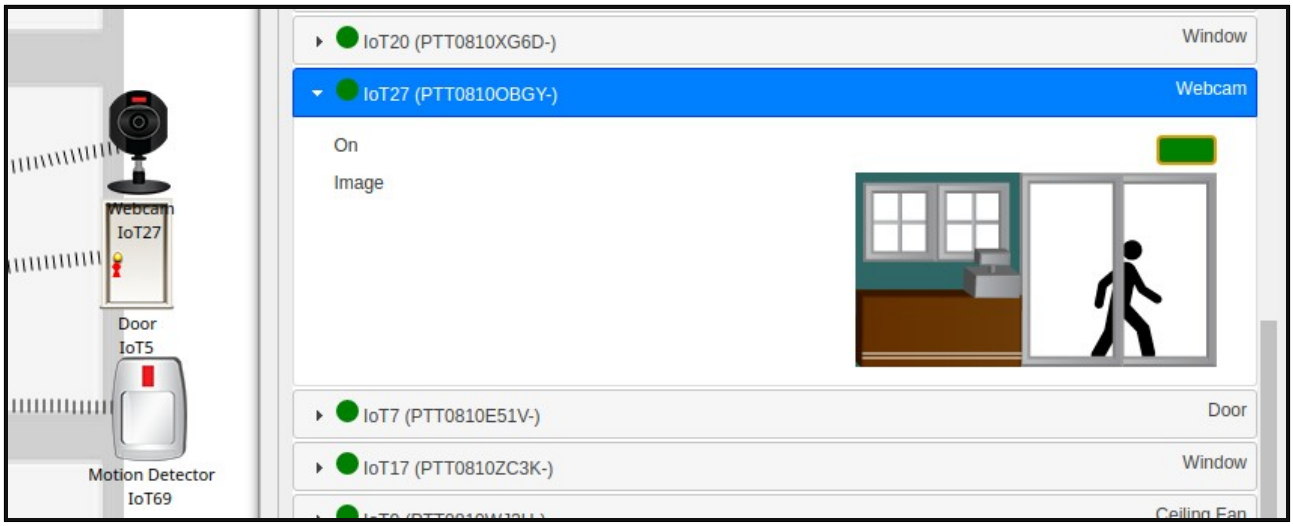


Figure 26 : Réaction du système à la détection de mouvement – activation de la caméra

d) Scénario 2 : Détection d'incendie avec activation automatique du sprinkler

Lorsque le **capteur de fumée** détecte un début d'incendie, il envoie un **signal** au **microcontrôleur (MCU)**. Celui-ci réagit immédiatement en **déclenchant le système d'extinction automatique** : les 12 pt**sprinklers** s'activent et **projetent de l'eau** pour éteindre le feu et limiter les dégâts.

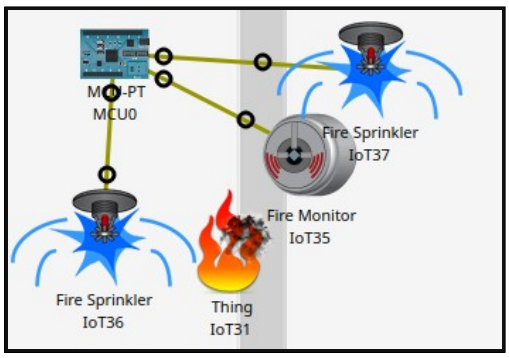


Figure 27 : Déclenchement automatique des sprinklers en cas d'incendie

- **Code python pour le microcontrôleur :**

```
from gpio import *
from time import *
def handleSensorData():
    value = digitalRead(0)
    if value == 0:
        customWrite(1, '0')
        customWrite(2, '0')
    else:
        customWrite(1, '1')
        customWrite(2, '1')
    def main():
    add_event_detect(0, handleSensorData)
    while True:
        delay(1000)
if __name__ == "__main__":
    main()
```

Figure 28 : Conditions d'activation définies dans l'interface pour le code Python du microcontrôleur

3.5.2 Renforcement de la sécurité de la Smart Home

3.5.2.1 Intégration du pare-feu ASA

- **Ajout dans la topologie**

Le pare-feu Cisco ASA a été inséré entre le routeur principal de la smart home et le réseau local, afin de contrôler et sécuriser le trafic réseau. Cette position stratégique permet de filtrer les communications entrantes et sortantes, assurant ainsi une protection efficace contre les accès non autorisés et les attaques externes.

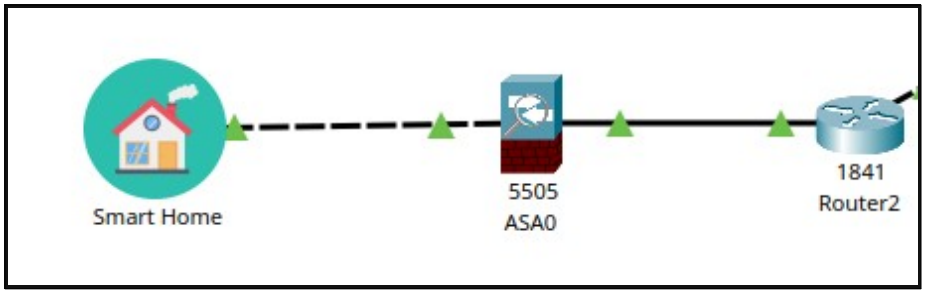


Figure 29 : Intégration du pare-feu ASA dans la topologie

- **Configuration des ACLs**

La politique de sécurité mise en place sur le pare-feu ASA repose sur trois piliers :

- La **définition de listes de contrôle d'accès (ACLs)** selon les flux autorisés,
- L'**association des ACLs** aux interfaces ASA appropriées,
- L'**activation d'inspections profondes** sur les protocoles critiques.

Les règles suivantes ont été configurées sur le pare-feu :

```
access-list in_to_internet extended permit icmp any any
access-list inside_access extended deny tcp any any eq 80
access-list inside_access extended permit tcp any any eq 443
access-list inside_access extended permit udp any any eq domain
access-list inside_access extended permit icmp any any
access-list FROM_SERVERS_TO_INSIDE extended permit ip host 192.168.30.3 172.16.1.0
255.255.255.0
access-list FROM_SERVERS_TO_INSIDE extended permit icmp any host 172.16.1.37
access-list FROM_SERVERS_TO_INSIDE extended permit ip host 192.168.30.4 172.16.1.0
255.255.255.0
```

- **Explication des ACLs :**

◆ inside_access autorise les connexions sortantes HTTPS (port 443), DNS (port 53 UDP) et ICMP depuis le réseau interne, tout en refusant le trafic HTTP (port 80).

- `FROM_SERVERS_TO_INSIDE` permet à certains serveurs spécifiques (192.168.30.3 et 192.168.30.4) d'accéder au réseau interne 172.16.1.0/24.
- `in_to_internet` autorise le protocole ICMP pour le diagnostic réseau (ping).

- **Configuration d'inspections**

  Les inspections suivantes ont été activées à l'aide de la **policy-map** globale ASA :

```
policy-map global_policy
 class inspection_default
  inspect dns
  inspect http
  inspect icmp
```

  - Ces inspections permettent à l'ASA d'**analyser dynamiquement** les flux DNS, HTTP et ICMP pour détecter des anomalies, bloquer certaines attaques réseau et gérer les connexions retournées de manière plus fine.

- **Validation et vérification**

Pour valider l'efficacité du pare-feu ASA et des règles de filtrage mises en place, plusieurs tests ont été effectués depuis différents hôtes du réseau.

En particulier, un **test de ping** a été lancé depuis une machine non autorisée (non incluse dans les règles `access-list FROM_SERVERS_TO_INSIDE`) vers une machine protégée du réseau interne (`172.16.1.37`). Le résultat montre que la **requête ICMP a été bloquée** par l'ASA, comme prévu par la politique de sécurité :

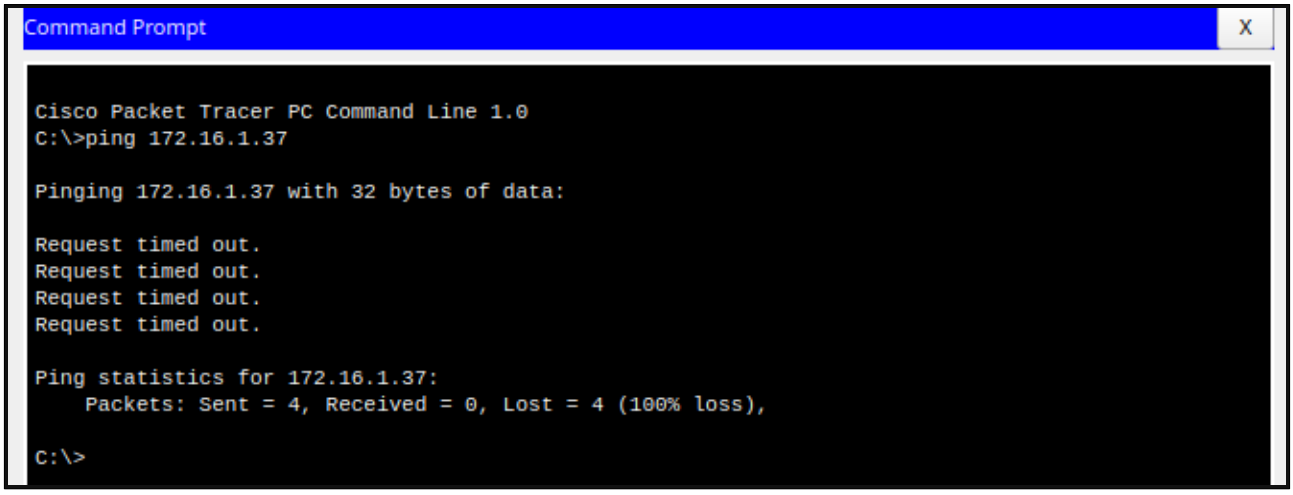


Figure 30 : Test de blocage ICMP par le pare-feu ASA selon la politique ACL

"Ce test démontre que le pare-feu ASA n'autorise que les flux explicitement définis, en bloquant tout trafic non autorisé — par exemple celui provenant d'une machine non spécifiée dans la liste de contrôle d'accès `ACLFROM_SERVERS_TO_INSIDE`.

Ce comportement confirme le **principe du pare-feu basé sur les règles explicites** et la **stratégie "deny by default"**, renforçant la sécurité du réseau local.

3.5.2.2 Implémentation d'un VPN simulé

- **Justification de l'utilisation du VPN**

Dans une maison intelligente, plusieurs équipements communiquent avec des serveurs distants (IoT, DNS, cloud, authentification). Sans protection, ces échanges sont vulnérables à l'interception. Pour cette raison, un **tunnel VPN simulé** a été mis en place dans notre architecture Packet Tracer. Il établit un lien sécurisé entre :

- le **routeur de la maison intelligente**, et
- le **routeur du réseau distant des serveurs**.

L'objectif est de **simuler un canal chiffré IPSec** pour protéger les données sensibles (commandes de contrôle, identifiants, requêtes DNS, etc.) contre toute écoute ou attaque « man-in-the-middle ».

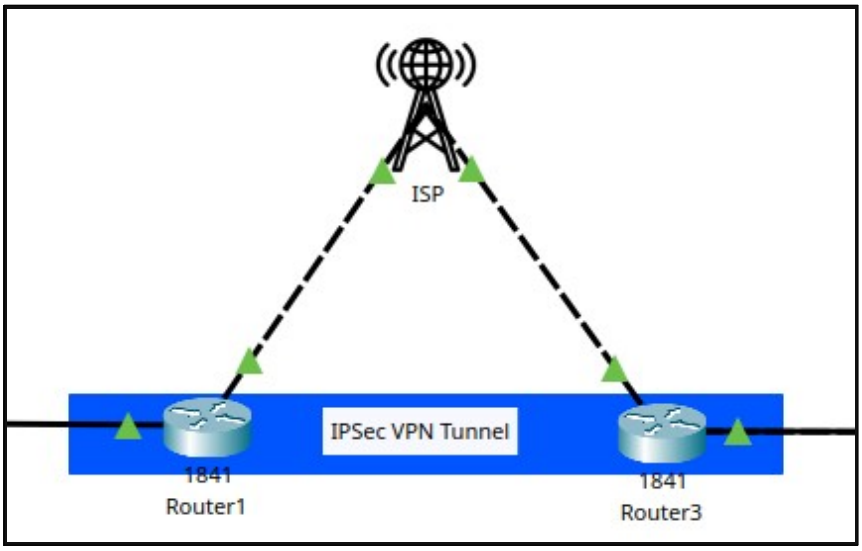


Figure 31 : Tunnel VPN IPSec entre les deux routeurs

- **Configuration du tunnel VPN (symbolique dans Packet Tracer)**

```
crypto isakmp policy 20
encr 3des
hash md5
authentication pre-share
lifetime 3600
!
crypto isakmp key cisco123 address 172.168.85.9
```

```
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map mymap 20 ipsec-isakmp
set peer 172.168.85.9
set transform-set myset
match address 100
!
interface FastEthernet0/1
ip address 9.9.9.1 255.255.255.0
duplex auto
speed auto
crypto map mymap
!
access-list 100 permit ip 203.1.1.0 0.0.0.255 192.168.30.0 0.0.0.255
```

- **Vérification et validation**

Afin de vérifier l'efficacité du tunnel VPN simulé, nous avons comparé les résultats de la commande `tracert 192.168.30.2` depuis un poste client, avant et après la mise en place du tunnel. Sans VPN, le trafic passe par une adresse intermédiaire non sécurisée (ex. : `9.9.9.9`), représentant un réseau public simulé. En revanche, après la mise en œuvre du tunnel VPN, le chemin devient plus direct et sécurisé, passant par l'interface du routeur chiffré (`203.1.1.1`). Cette redirection prouve que les données sont acheminées via le tunnel symbolique, simulant ainsi une communication sécurisée entre les deux sites et évitant toute exposition des paquets sur des nœuds intermédiaires.

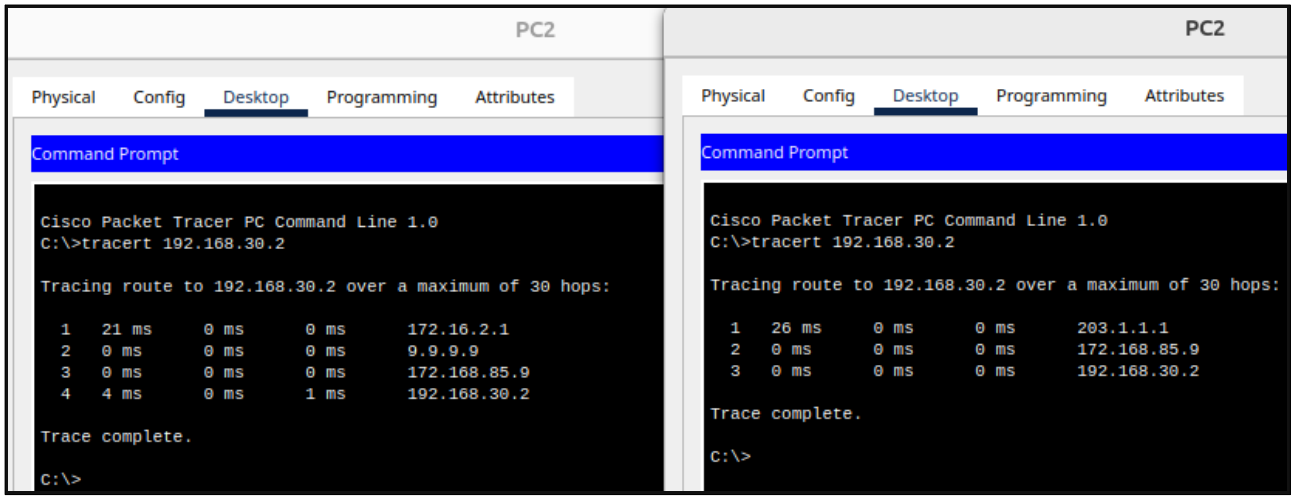


Figure 32 : Comparaison du tracert avant et après activation du tunnel VPN

3.5.2.3 Segmentation du réseau par VLANs

L’utilisation des VLANs dans le réseau de la maison intelligente permet une segmentation logique et sécurisée des équipements selon leur usage et leur niveau de sensibilité. Les appareils IoT, souvent vulnérables et faiblement protégés, sont regroupés dans un VLAN dédié (VLAN 10) afin d’isoler leur trafic. Les postes administrateurs (PC, serveurs) sont placés dans un VLAN sécurisé (VLAN 20), tandis que les utilisateurs invités sont confinés dans un VLAN séparé (VLAN 30) sans accès aux ressources critiques. Cette organisation permet de limiter les domaines de diffusion, de bloquer les communications directes entre VLANs, et de réduire les risques d’attaques latérales, sauf si des règles spécifiques (ACLs ou routage inter-VLAN contrôlé) les autorisent. Ainsi, même si un invité est connecté physiquement au même réseau, il ne pourra ni interagir avec les équipements IoT ni accéder aux systèmes d’administration.

- **Création des VLANs**

Trois VLANs ont été créés sur le switch principal afin de séparer les usages :

- **VLAN 10 (IoT)** : pour les objets connectés (capteurs, microcontrôleurs, caméras).
- **VLAN 20 (Administration)** : réservé aux PC de gestion du réseau et à l’administration des équipements.
- **VLAN 30 (Invités)** : pour les périphériques mobiles des visiteurs.

- **La configuration des VLANs**

switch :

```
Switch(config)# vlan 10
Switch(config-vlan)# name IoT
Switch(config)# vlan 20
Switch(config-vlan)# name PCS
Switch(config)# vlan 30
Switch(config-vlan)# name guest
```

router :

```
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 172.16.1.1 255.255.255.0
ip access-group ACL-VLAN1 in
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
```

```
ip address 172.16.2.1 255.255.255.0
ip access-group ACL-VLAN2 in
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 172.16.3.1 255.255.255.0
ip access-group ACL-VLAN3 in
!
access-list 100 permit ip 0.0.0.0 255.255.255.0 0.0.0.0 255.255.255.0
```

3.6 Comparaison avec des travaux similaires

Cette section propose une analyse comparative entre notre simulation de Smart Home sécurisée et plusieurs travaux antérieurs présentés dans la section 3.3. Le tableau ci-dessous met en évidence les principales caractéristiques techniques, les mécanismes de sécurité intégrés, ainsi que les outils utilisés dans ces projets, afin de situer notre approche par rapport aux contributions existantes.

Critère	**Notre travail**	[26]	[27]	[28]
Outil de simulation	Cisco Packet Tracer	Cisco Packet Tracer	Cisco Packet Tracer	Cisco Packet Tracer
Objectif principal	Simulation d'une smart home sécurisée et segmentée	Assistance pour personnes handicapées	Domotique à distance pour personnes fragiles	Simulation de scénarios domotiques
Contrôle distant	Oui (client 3G/4G + serveur IoT)	Non	Oui (client 3G/4G + serveur IoT)	Non
Utilisation des VLANs	Oui (IoT, admin, guest)	Non	Non	Non
Pare-feu ASA (Firewall)	Oui (filtrage du trafic, inspections activées)	Non	Non	Non
ACLs (Listes de contrôle)	Oui (règles de filtrage entre VLANs, sécurité ASA)	Non	Non	Non
Tunnel VPN simulé	Oui (liaison sécurisée inter sites)	Non	Non	Non

Tableau 3 : Comparaison des travaux sur la simulation de smart homes IoT

3.7 Défis rencontrés et limites de la simulation

La mise en œuvre de ce projet a été confrontée à plusieurs difficultés, essentiellement dues aux limitations de l'environnement de simulation et aux contraintes liées à certaines configurations réseau avancées.

- **Limites de Cisco Packet Tracer**

Cisco Packet Tracer, bien qu'efficace dans un cadre pédagogique, ne prend pas en charge certaines fonctionnalités avancées. Il ne permet notamment pas l'implémentation réelle de protocoles VPN sécurisés tels qu'IPSec avec authentification et chiffrement, ni l'intégration de services cloud, de scripts personnalisés ou d'outils d'analyse approfondie du trafic réseau.

- **Contraintes de configuration réseau**

Certaines fonctionnalités complexes, comme la configuration détaillée du pare-feu ASA est partiellement supportée dans la version éducative du simulateur. Par conséquent, le tunnel VPN n'a pu être représenté que de manière symbolique, sans encapsulation réelle des paquets. De plus, certains équipements comme les *home gateways* n'autorisent pas simultanément l'accès local et distant, ce qui limite la flexibilité dans les scénarios de supervision. Ils ne prennent pas non plus en charge les ports trunk nécessaires à la gestion multi-VLAN, restreignant ainsi la simulation d'une segmentation réseau complète.

- **Fonctionnalités restreintes des objets IoT**

Les objets connectés disponibles dans Packet Tracer sont rudimentaires. Ils offrent des interactions limitées, ne reflétant pas fidèlement le comportement réel de dispositifs physiques. Ainsi, certaines fonctions comme la lecture de capteurs complexes (température, détection de mouvement, RFID évolué) ou l'automatisation conditionnelle ne peuvent être simulées avec précision. Cela contraint à simplifier les scénarios pour rester dans les possibilités offertes par la plateforme.

3.8 Conclusion

Ce chapitre a présenté l'ensemble des étapes de conception, de simulation et de sécurisation d'une architecture de maison intelligente basée sur les technologies IoT. À travers une approche progressive, nous avons d'abord établi une topologie fonctionnelle sans mécanismes de sécurité, avant d'y intégrer plusieurs dispositifs de protection réseau, tels que le pare-feu ASA, le tunnel VPN, les VLANs, les ACLs .

Les tests réalisés ont permis de valider la cohérence de l'architecture ainsi que l'efficacité des mesures de sécurité mises en place. Malgré certaines limites imposées par l'environnement Cisco Packet Tracer, le projet a démontré la faisabilité d'une solution domotique sécurisée simulée, proche d'un déploiement réel.

Les résultats obtenus constituent une base solide pour de futurs travaux orientés vers des environnements réels, incluant l'utilisation de capteurs physiques, l'intégration cloud, et l'intelligence artificielle dans la gestion adaptative des objets connectés.

Conclusion Générale

L’évolution rapide des technologies de l’**Internet des Objets (IoT)** a permis l’émergence des **Smart Homes**, des environnements résidentiels intelligents capables d’automatiser les tâches, d’optimiser la consommation énergétique et de renforcer le confort des occupants. Toutefois, cette connectivité omniprésente s'accompagne de risques croissants en matière de **cybersécurité**, mettant en péril la confidentialité des données, l'intégrité des systèmes et la sécurité physique des utilisateurs.

Ce mémoire a permis d’explorer cette problématique en trois étapes complémentaires. Dans un premier temps, nous avons étudié les fondements techniques des Smart Homes et de l’IoT, en mettant en lumière leurs architectures, leurs protocoles de communication et leurs domaines d’application. Ensuite, une analyse approfondie des **menaces**, des **vulnérabilités** et des **contre-mesures** a été menée, en tenant compte des spécificités des environnements domotiques, souvent hétérogènes et peu normalisés.

Enfin, une **implémentation simulée dans Cisco Packet Tracer** a été réalisée afin d’illustrer concrètement les enjeux et les solutions de sécurisation d’une maison intelligente. Plusieurs fonctionnalités (RFID, détection incendie, caméras IP) ont été modélisées, puis sécurisées à travers l’ajout progressif de **pare-feu ASA, VPN, VLANs et** . Cette approche a permis de valider la faisabilité technique des mesures de protection dans un contexte résidentiel, tout en mettant en évidence l’importance d’une architecture réseau bien conçue.

Ainsi, ce travail montre que la sécurité des Smart Homes ne peut reposer uniquement sur la technologie, mais nécessite une **vision globale**, intégrant la **conception sécurisée**, la **configuration rigoureuse** et la **sensibilisation des utilisateurs**. Il ouvre également la voie à de futures recherches, notamment sur l’intégration de **l’intelligence artificielle pour la détection d’intrusion**, l’analyse en temps réel des flux réseau, ou encore le **déploiement sécurisé à grande échelle** dans le cadre des **villes intelligentes**.

En somme, dans un monde de plus en plus connecté, sécuriser les environnements domestiques intelligents constitue non seulement un défi technique, mais aussi un **enjeu sociétal majeur**, au cœur des préoccupations liées à la vie privée, à la confiance numérique et à la résilience des infrastructures du futur.

[1] P.-J. Benghozi, S. Bureau, et F. Massit-Folléa, L'Internet des objets : Quels enjeux pour l'Europe, Paris : Éditions de la Maison des sciences de l'homme, 2009.

[2] IBM, « Internet des objets (IoT) », IBM.com. [En ligne]. Disponible : https://www.ibm.com/fr-fr/topics/internet-of-things

[3] Kinsta, « Qu'est-ce que l'Internet des objets (IoT) ? », Kinsta.com. [En ligne]. Disponible : https://kinsta.com/fr/base-de-connaissances/qu-est-ce-que-iot/

[4] J. Wang, M. K. Lim, C. Wang, and M. L. Tseng, « The Evolution of the Internet of Things (IoT) over the Past 20 Years », Comput. Ind. Eng., vol. 155, p. 107174, 2021.

[5] H. Xue, D. Chen, N. Zhang, H. N. Dai, and K. Yu, « Integration of Blockchain and Edge Computing in Internet of Things: A Survey », Future Gener. Comput. Syst., vol. 144, pp. 307–326, 2023.

[6] P. P. Ray, « A Survey on Internet of Things Architectures », J. King Saud Univ. – Comput. Inf. Sci., vol. 30, no. 3, pp. 291–319, Jul. 2018.

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, « Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications », IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 2015,

[8] L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, and L. Tarricone, « An IoT-aware Architecture for Smart Healthcare Systems », IEEE Internet Things J., vol. 2, no. 6, pp. 515–526, Dec. 2015.

[9] J. Wan, H. Cai, and K. Zhou, « Industrie 4.0: Enabling Technologies », in Proc. 2015 Int. Conf. Intelligent Computing and Internet of Things (ICIT), Harbin, China, Jan. 2015, pp. 135–140.

[10] T. A. Alghamdi, A. Lasebae, and M. Aiash, « Security Analysis of the Constrained Application Protocol in the Internet of Things », in Proc. 2nd Int. Conf. Future Generation Communication Technologies (FGCT 2013), London, UK, Nov. 2013.

[11] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, « Internet of Things (IoT): A vision, architectural elements, and future directions », Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[12] I. Rozlomii, A. Yarmilko, and S. Naumenko, « Data Security of IoT Devices with Limited Resources: Challenges and Potential Solutions », in Proc. 4th Edge Comput. Workshop (DOORS 2024), CEUR Workshop Proc., vol. 3666, Zhytomyr, Ukraine, Apr. 2024, pp. 85–96

[13] I. Saleh, « Internet des Objets (IdO): Concepts, enjeux, défis et perspectives », Revue Internet des objets, vol. 2, 2018.

[14] G. Lampkin, MQTT Essentials - A Lightweight IoT Protocol. Birmingham, UK: Packt Publishing, 2017.

[15] A. Acar, H. Fereidooni, T. Abera, A. K. Sikder, M. Miettinen, H. Aksu, et al., "Peek-a-boo: I see your smart home activities, even encrypted!", Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, July 2020

[16]V. Vajrobol, G. J. Saxena, A. Pundir, S. Singh, B. B. Gupta, A. Gaurav, and M. Rahaman, "Identify spoofing attacks in Internet of Things (IoT) environments using machine learning algorithms," Journal of High Speed Networks, vol. 31, no. 1, pp. 61–70, 2025

[17] P. Walker, T. Zhang, C. Shi, N. Saxena, and Y. Chen, "BarrierBypass: Out-of-sight clean voice command injection attacks through physical barriers," Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, May 2023

[18] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: threats and challenges," Security and Communication Networks, vol. 7, no. 12, pp. 2728–2742, 2014.

[19] B. Yuan, J. Wan, Y. H. Wu, D. Q. Zou, and H. Jin, "On the security of smart home systems: A survey," Journal of Computer Science and Technology, vol. 38, no. 2, pp. 228–247, 2023

[20] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Mar. 2017.

[21] Cisco Networking Academy, "CCNA2: Notions de base sur les routeurs et routage, Version 3.1.1," 2023.

[22]P. Hoffman and P. McManus, "DNS queries over HTTPS (DoH)," RFC 8484, Oct. 2018.

[23] D. A. Worae and S. Mastorakis, "Hiding in plain sight: An IoT traffic camouflage framework for enhanced privacy," arXiv preprint arXiv:2501.15395, 2025.

[24] N. Apthorpe, D. Reisman, and N. Feamster, "Closing the blinds: Four strategies for protecting smart home privacy from network observers," arXiv preprint arXiv:1705.06809, 2017.

[25] S. Devi and H. D. Kotha, "AES encryption and decryption standards," in Journal of Physics: Conference Series, vol. 1228, no. 1, p. 012006, May 2019.

[26] H. Messaoud, S. B. S. Chourouk, "Développement et simulation d'une maison intelligente dédiée pour des personnes handicapées basée sur l'IoT," Université Belhadj Bouchaib Ain-Temouchent, 2020/2021.

[27] D. E. Aroussi et O. Ounassi, "IoT-based Smart Home System for Elderly and Disabled Assistance," Université M'Hamed Bougara de Boumerdes, 2021.

[28] Y. Otmani, "Simulation d'un réseau domotique à base d'Internet des Objets," Université Badji Mokhtar - Annaba, 2020/2021.

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

[30]SAPinsider, SAP Internet of Things, MasteringSAP, [En ligne]. Disponible : https://masteringsap.com/topic/sap-intelligent-technologies/sap-internet-of-things/.

[31]F. Skandrani, "Architecture IoT : L'essentiel à savoir," IoT Industriel Blog, 2 janv. 2022. [En ligne]. Disponible : https://iotindustriel.com/iot-iiot/architecture-iot-lessentiel-a-savoir/.

[32] N. Belhadj et A. Abbad, "La sécurité de l'Internet des Objets (IoT)," Mémoire de fin d'études, Département de Génie Electrique, Faculté des Sciences Appliquées, Université Ibn-Khaldoun de Tiaret, Algérie, 2022.

[33] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics: Challenges and opportunities,” Future Generation Computer Systems, vol. 78, pp. 544–546, 2018.
[34] A. Sivanathan, D. Sherratt, H. H. Gharakheili, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman, “Characterizing and classifying IoT traffic in smart cities and campuses,” Proc. IEEE Conf. on Computer Communications Workshops (INFOCOM WKSHPS), Atlanta, GA, USA, 2017, pp. 559–564.
[35] R. H. Weber, “Internet of Things – New security and privacy challenges,” Computer Law & Security Review, vol. 26, no. 1, pp. 23–30, 2010.

[36] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: threats and challenges," Security and Communication Networks, vol. 7, no. 12, pp. 2728–2742, 2014.

[37] P. R. Babu, D. L. Bhaskari, and C. H. Satyanarayana, "A comprehensive analysis of spoofing," International Journal of Advanced Computer Science and Applications, vol. 1, no. 6, pp. –, 2010.

[38] N. Belhadj et A. Abbad, La sécurité de l’Internet des Objets (IoT), Mémoire de Master, Spécialité : Électronique des systèmes embarqués, Université Ibn-Khaldoun de Tiaret, Algérie, 2022.

[39] NIST, Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5, 2020. [Online].

[40] N. Mahdad and D. Lairedj, Développement d’un device IoT pour la supervision d’un système de transport intelligent, Mémoire de Master, Spécialité Systèmes des Télécommunications, Univ. Aboubakr Belkaïd – Tlemcen, Algérie, 2020

[41] S. Kambouche et I. Attou, Conception et réalisation d'un système d'agriculture intelligent, Projet de fin d’études, Département de Génie Mécanique, Institut de Technologie, Centre Universitaire Belhadj Bouchaib d’Ain-Temouchent, 2018.

[42] The Hacker News, “DDoS 2.0: IoT Sparks New DDoS Alert,” The Hacker News, Sep. 15, 2023. [Online]. Available: https://thehackernews.com/2023/09/ddos-20-iot-sparks-new-ddos-alert.html

[43] Ronen, Eyal, and Adi Shamir. "Extended functionality attacks on IoT devices : The case of smart lights." 2016 IEEE European Symposium on Security and Privacy (EuroSP). IEEE, 2016.

[44]Tiwari, A., & Waoo, A. A. (2023). IoT based Smart Home Cyber-Attack Detection and Defense. TIJER-International Research Journal, 10(8).

[45]Huang, D. Y., Apthorpe, N., Li, F., Acar, G., & Feamster, N. (2020). Iot inspector: Crowdsourcing labeled network traffic from smart home devices at scale. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 4(2), 1-21.