REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التـــــــــــعـــليـــــم العـــــالي والبـــــــحث العـــلـــمـــي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جـــــــــــامعة أبي بـكـــــر بلـقـايـد – تـــــلمســـــــــان –

Université Aboubakr Belkaïd– Tlemcen –
Faculté de TECHNOLOGIE

MEMOIRE

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

En : Télécommunications

Spécialité : Réseau et Télécommunications

Par :

BOUREGBA Hanane

BOUKLI HACENE Loubna

Sujet

Détection des risques et des menaces dans le domaine des IoT

Soutenu publiquement le :27/09/2023, devant le jury composé de :

Mme F. BOUSALAH	**Maitre de conférences A**	**Univ. Tlemcen**	**Présidente**
Mme A. SEDJELMACI	**Maitre de conférences B**	**Univ. Tlemcen**	**Examinatrice**
Mr A. RABAH	**Maître de Recherche A**	**C.D.S Oran**	**Examinateur**
Mr O. MAACHOU	**Maître-Assistant A**	**Centre I2E**	**Examinateur**
Mr M. Z. BABA-AHMED	**Maître de conférences A**	**Univ. Tlemcen**	**Encadrant**
Mr B. LASOUANI	**Ingénieur d'état en Télécommunications**	**Algérie Télécom Tlemcen**	**Co-encadrant**

Année universitaire : 2022/2023

Remerciements

Nous souhaitons exprimer notre gratitude envers **ALLAH**, source de sagesse et de guidance, Nous croyons en sa bienveillance qui a éclairé notre chemin à chaque étape de cette aventure académique.

Nous souhaitons sincèrement remercier notre Encadreur, Monsieur **« BABA-AHMED Mohammed Zakarya »,** Maitre de conférences classe A à l'université de Tlemcen, pour son encadrement actif, sa grande disponibilité, sa patience et ses conseils judicieux qui ont contribué à alimenter nos réflexions.

Aussi à notre Co-encadreur Monsieur **« LASOUANI Ibrahim »**, Ingénieur d'état en Télécommunications, à Algérie Télécom Tlemcen d'avoir contribué à la conception de notre PFE.

Nous adressons nos remerciements les plus respectueux à Madame **« BOUSALAH Fayza »** Maître de Conférences classe A à l'Université de Tlemcen, d'avoir accepté de présider le jury de ce mémoire. Sa présence et son expertise ont été un honneur pour nous.

Nos remerciements les plus sincères vont également à Madame « **SEDJELMACI Amina Nadjet »** maitre de conférences classe B à l'université de Tlemcen, d'avoir accepté d'examiner et évalué ce travail modeste.

Nous aimerions adresser nos sincères remerciements à Monsieur **« RABAH Mohammed Amin »** Maître de Recherche classe A au centre de développement spatial et satellitaires CDS d'Oran d'avoir accepté d'examiner et de juger notre travail.

Nos remerciements les plus sincères vont également à Monsieur « **MAACHOU Omar** » Maître-Assistant classe A à l'université de Tlemcen et membre du centre I2E, d'avoir accepté d'examiner et évalué ce projet innovant.

Nous souhaitons également témoigner notre reconnaissance envers le Laboratoire de Télécommunications de Tlemcen **« LTT »** ainsi que le laboratoire d'électronique **ELN1** pour leurs contributions inestimables à notre projet.

Sans oublier Monsieur **« MAACHOU Omar »** Maître-Assistant A, membre du jury du centre de l'Etudiant (I2E), de l'université de Tlemcen d'avoir accepté d'évaluer ce modeste travail.

On tient à exprimer nos sincères remerciements à **Algérie Telecom** pour leur soutien tout au long de la réalisation de notre projet.

On tient également à exprimer notre profonde gratitude envers nos enseignants, qui ont joué un rôle fondamental dans notre parcours académique.

Enfin, nous tenons à remercier chaleureusement toutes les personnes, qu'elles soient proches ou éloignées de notre projet, qui ont apporté leur précieux soutien à la réalisation de cette étude. Nous leur sommes infiniment reconnaissants pour leur contribution inestimable.

Dédicace « Hanane »

Je dédie ce travail a :

Mes chers parents « Houcine » « Fatiha »

Je tiens à vous exprimer ma profonde gratitude pour tout ce que vous avez fait pour moi tout au long de mon parcours académique. Votre amour inconditionnel, votre soutien indéfectible et vos sacrifices inestimables ont été les piliers qui ont soutenu chaque étape de mon éducation. Votre confiance en moi ma constamment motivée à donner le meilleur de moi-même.

Mon frère bien-aimé « Aymen »

Ta présence illumine ma vie de bonheur, Tu es bien plus qu'un petit frère pour moi, tu es unami précieux et un compagnon de vie. Merci d'être toujours là pour moi.

Mes chères sœurs « Niema » et « Zahéra »

Je vous remercie pour les liens indéfectibles que nous partageons, votre soutien inconditionnel et votre amour sont le trésor qui enrichit ma vie.

Ma petite nièce « Houda »

Je t'offre cette dédicace avec tout mon amour. Puisses-tu grandir entourée d'inspiration, de connaissances et de rêves à poursuivre.

Ma très chère amie et binôme « Loubna »

En tant qu'amie, tu es toujours là pour m'écouter, me soutenir et partager des moments joyeux avec moi. En tant que binôme, tu as été une part essentielle de notre réussite commune. Ta compétence, ton dévouement et ta détermination ont été des a touts majeurs.

Mes très chères amies « Ghizlene, Safaa, Manel, Hanane, Rania, Nour, Amira, kevin,Barack »

Je tiens à vous exprimer ma profonde gratitude pour votre amitié. Chacune de vous apporte une lumière unique à ma vie, et je suis reconnaissante de vous avoir comme amies.je vous aimes.

« Zahreddine »

Mon ami cher à mon cœur, je tiens à t'exprimer ma profonde gratitude pour ta précieuse amitié et pour les moments inestimables que nous avons partagés.

Dédicace « Loubna »

Je dédie ce modeste travail à :

Mes chers parents « Zoubir » « Souad »

Je tiens à vous exprimer ma profonde gratitude pour tout ce que vous avez fait pour moi tout au long de mon parcours académique. Votre amour inconditionnel, votre soutien indéfectible et vos sacrifices inestimables ont été les piliers qui ont soutenu chaque étape de mon éducation. Votre confiance en moi m'a constamment motivée à donner le meilleur de moi-même. Vos encouragements chaleureux, vos conseils avisés et votre présence bienveillante ont été ma source d'inspiration. Vous m'avez montré l'importance de la persévérance, de la détermination et de l'intégrité, des leçons qui vont bien au-delà de l'éducation académique. Avec tout mon amour.

Mon cher petit frère « Yanis »

Ta présence dans ma vie est une bénédiction qui m'apporte une joie inestimable. Tu es bien plus qu'un frère, tu es un ami précieux, un confident et un rayon de soleil qui illumine mes journées. Je suis reconnaissante de t'avoir comme petit frère. Sache que je serai toujours là pour toi, comme tu l'as été pour moi. Merci d'être la merveilleuse personne que tu es.

Ma chère sœur « Ghizlene »

Je tiens à te remercier du fond du cœur pour tout ce que tu as fait pour moi au fil des années. Ta présence dans ma vie est une source de réconfort, de joie et de soutien constant.

Mon cher ami « Yacine »

Merci d'être bien plus qu'un ami, mais véritablement ma force et ma source de soutien inébranlable. Ton amitié sincère, ta loyauté indéfectible et ta capacité à toujours me comprendre sont des trésors rares. Tu es le genre d'ami qui fait une différence significative, qui apporte du réconfort dans les moments de doute et qui partage la joie dans les moments de bonheur.

Chère « Hanane »

Merci pour tout ce que tu as apporté à notre projet, ainsi que pour l'amitié extraordinaire que nous partageons. Tu es un binôme exceptionnel et une amie précieuse, et c'est un privilège de compter sur ta présence à mes côtés.

Chères « Dounia » « Narimene » et « Razia »

Vous êtes bien plus que des amies pour moi, vous êtes mes sœurs de cœur, mes complices et mes confidentes les plus précieuses. Votre amitié a apporté une lumière spéciale dans ma vie.

Ma chère famille paternelle , les **« Boukli Hacene »** , et à ma précieuse famille maternelle les **« Terki Hassaine »** , je dédie ce travail avec tout mon amour .

Résumé

L'Internet des Objets (IoT) a révolutionné notre manière d'interagir avec le monde qui nous entoure en intégrant des dispositifs connectés dans notre vie quotidienne. Toutefois, cette expansion rapide de l'IoT a également posé d'importants défis en matière de sécurité. Dans ce cadre, notre Projet de Fin d'Études se focalise sur la détection des risques et des menaces au sein des réseaux IoT. Notre approche novatrice se caractérise par la création d'un prototype de détection d'attaques au sein des environnements IoT. L'objectif de cette solution est de surveiller de manière proactive le trafic réseau IoT en temps réel, permettant ainsi d'identifier instantanément tout comportement suspect et de détecter les éventuelles menaces qui pèsent sur les différents systèmes IoT. Notre projet s'inscrit dans une vision d'un futur IoT plus sûr et plus fiable, où les dispositifs connectés enrichissent nos vies sans compromettre notre sécurité.

Mots-clés : Internet des Objets (IoT), Dispositifs connectés, Prototype, Sécurité IoT, Menaces IoT, Détection d'attaques.

Abstract

The Internet of Things (IoT) has revolutionized our way of interacting with the world around us by integrating connected devices into our daily lives. However, this rapid expansion of IoT has also brought significant security challenges. In this context, our End-of-Studies Project focuses on detecting risks and threats within IoT networks. Our innovative approach is characterized by the creation of a prototype for detecting attacks within IoT environments. The objective of this solution is to proactively monitor IoT network traffic in real-time, thereby instantly identifying any suspicious behavior and detecting potential threats to various IoT systems. Our project aligns with a vision of a safer and more reliable IoT future, where connected devices enrich our lives without compromising our security.

Keywords: Internet of Things (IoT), Connected Devices, Prototype ,IoT Security, IoT Threats

Attack Detection.

الملخص

لقد أحدث إنترنت الأشياء (IoT) ثورة في الطريقة التي نتفاعل بها مع العالم من حولنا من خلال دمج الأجهزة المتصلة في حياتنا اليومية. ومع ذلك، فإن هذا التوسع السريع في إنترنت الأشياء قد فرض أيضًا تحديات أمنية كبيرة. وفي هذا السياق، يركز مشروع نهاية الدراسة لدينا على اكتشاف المخاطر والتهديدات داخل شبكات إنترنت الأشياء. يتميز نهجنا المبتكر بإنشاء نموذج أولي لاكتشاف الهجمات داخل بيئات إنترنت الأشياء.

الهدف من هذا الحل هو مراقبة حركة مرور شبكة إنترنت الأشياء بشكل استباقي في الوقت الفعلي، والتعرف على الفور على أي سلوك مشبوه واكتشاف التهديدات المحتملة لأنظمة إنترنت الأشياء المختلفة. يعد مشروعنا جزءًا من رؤية مستقبلية أكثر أمانًا وموثوقية لإنترنت الأشياء، حيث تعمل الأجهزة المتصلة على إثراء حياتنا دون المساس بأمننا.

كلمات مفتاحية: الإنترنت للأشياء، الأجهزة المتصلة، نموذج أولي, أمان الإنترنت للأشياء , تهديدات الإنترنت للأشياء , اكتشاف الهجمات

Table des matières

Chapitre I : Généralité sur les IoT et leurs applications

Chapitre III : Évaluation de la Performance de Snort 2.9.20 pour la Détection d'Intrusions dans les Réseaux IoT

Listes des figures

Chapitre I : Généralité sur les IoT et leurs applications.

Chapitre II : La cybersécurité et les détection des menaces dans les IoT.

Chapitre III : Évaluation de la Performance de Snort 2.9.20 pour la Détection d'Intrusions dans les Réseaux IoT.

Liste des tableaux

Chapitre I : Généralité sur les IoT et leurs applications.

Chapitre II : La cybersécurité et les détection des menaces dans les IoT.

Chapitre III : Évaluation de la Performance de Snort 2.9.20 pour la Détection d'Intrusions dans les Réseaux IoT.

Acronymes et abréviations

AMQP : Advanced Message Queuing Protocol.

B2B : Business to Business.

B2C : Business to Customers.

BLE : Bluetooth Low Energy.

COAP : Constrained Application Protocol.

CES : Consumer Electronics Show.

DAS : Data Acquisition Systems.

DDoS : Distributed Denial of Service.

DoS : Denial of Service.

ERDF : Électricité Réseau Distribution France.

ERM : Enterprise Risk Management.

GPS : Global Positioning System.

GSM : Global System for Mobile Communications.

HTTP : Hypertext Transfer Protocol.

HTTPS : Hypertext Transfer Protocol Secure.

IETF : Internet Engineering Task Force.

ICMP : Internet Control Message Protocol.

ID : Identification.

IdO : Internet des Objets.

IDS : Intrusion Detection System.

IoT : Internet of Things.

IP : Internet Protocol.

IPV6 : Internet Protocol version 6.

IPV4 : Internet Protocol version 4.

M2M : Machine to Machine.

MQTT : Message Queuing Telemetry Transport).

NFC : Near Field Communication.

NoSQL : Not Only SQL.

OASIS : Organization for the Advancement of Structured Information Standards.

QoS : Quality of Service.

REST : Representational State Transfer.

RFID : Radio Frenquency Identification.

SSL : Secure Socket Layer.

SIM : Subscriber Identity Module.

SYN : SYNchronize.

TCP : Transmission Control Protocol.

TIC : Technologies de l'Information et de la Communication.

TLS : Transport Layer Security.

UIT : Union Internationale des Télécommunications.

Wi-Fi : Wireless-Fidelity.

Introduction générale

L'Internet des Objets (IdO) représente une révolution technologique qui a profondément transformé notre manière d'interagir avec notre environnement. En connectant des objets du quotidien à Internet, l'IoT a ouvert la voie à de nouvelles applications innovantes, de la gestion intelligente de l'énergie à la domotique et aux villes intelligentes. Cette expansion rapide de l'IoT a créé des opportunités sans précédent, mais elle a également posé d'importants défis en matière de sécurité.

Le premier chapitre de cette étude offre une vue d'ensemble approfondie des concepts fondamentaux liés à l'Internet des Objets. Nous explorons les bases de l'IoT (Internet of Things), en mettant en évidence sa définition, son évolution et son rôle crucial dans notre société moderne. L'IoT consiste en l'interconnexion d'objets physiques, tels que les appareils électroménagers, les capteurs, les véhicules, et bien d'autres, via Internet. Cette interconnexion permet une collecte de données en temps réel, une automatisation avancée, et la création de services intelligents. L'IoT est devenu omniprésent dans notre vie quotidienne, révolutionnant des domaines allant de la domotique aux villes intelligentes.

Le deuxième chapitre de notre recherche nous plonge au cœur de la discipline vitale qu'est la cybersécurité. Dans un paysage numérique en constante évolution, la cybersécurité se révèle essentielle pour préserver l'intégrité et la confidentialité de nos systèmes informatiques et de nos données précieuses face aux menaces en ligne. Nous débutons ce chapitre par une définition approfondie de la cybersécurité, soulignant son importance dans la protection des informations sensibles. Les enjeux de la cybersécurité vont au-delà des attaques traditionnelles et englobent désormais les menaces émergentes telles que les attaques par ransomware et les attaques ciblant les objets connectés. Pour mieux comprendre l'ampleur de ce domaine, nous utilisons une carte mentale de la cybersécurité, qui nous permet de visualiser les nombreux aspects et défis de la sécurité en ligne. Nous examinons également la distinction cruciale entre la vulnérabilité, la menace, le risque et l'attaque, des éléments qui constituent la base de la sécurité des objets connectés (IoT). Ces distinctions sont essentielles pour évaluer et atténuer les risques liés à l'IoT, car elles nous aident à comprendre les vulnérabilités potentielles, à anticiper les menaces, à évaluer les risques et à répondre aux attaques.

Dans le troisième chapitre de notre étude, nous dévoilons notre solution de détection de menaces conçue spécifiquement pour répondre aux besoins de sécurité de l'Internet des Objets (IdO). Cette solution, mise en œuvre sur la carte Raspberry Pi 4, revêt une importance

cruciale dans les systèmes IoT. Nous décrivons en détail notre approche innovante, mettant en lumière le rôle déterminant qu'elle joue dans la protection des dispositifs IdO et des réseaux. Notre solution repose sur l'intégration de l'outil de détection d'intrusion Snort, qui est spécialement configuré pour surveiller en temps réel et détecter les activités suspectes dans les environnements IoT. Grâce à cette solution, nous sommes en mesure de détecter rapidement les menaces émergentes, offrant une protection essentielle pour les dispositifs IoT qui sont de plus en plus interconnectés.

En conclusion, notre étude nous a conduit à concevoir un système de détection de menaces innovant qui repose sur l'intégration de l'outil de détection d'intrusion Snort, installé sur notre plateforme Raspberry Pi. Cette solution se démarque par sa capacité à détecter les menaces en temps réel, offrant ainsi une protection essentielle pour les dispositifs de l'Internet des Objets (IdO). Grâce à Snort, notre système assure une surveillance continue des activités réseau, agissant comme un gardien vigilant, prêt à réagir immédiatement aux comportements suspects. Cette réactivité instantanée est cruciale pour anticiper et contrer les menaces émergentes, garantissant ainsi une sécurité inébranlable dans un environnement IdO en constante évolution. Dans un monde où la sécurité est devenue un impératif, la synergie entre notre système de détection des menaces et Snort, déployé sur le Raspberry Pi, s'impose comme un pilier central pour l'adoption sereine de la technologie IdO. Cette alliance assure un avenir plus sûr et plus fiable pour nos réseaux interconnectés, tout en ouvrant la voie à des innovations continues dans le domaine de l'Internet des Objets.

CHAPITRE I

Généralité sur les IoT et leurs applications

Sommaire

I. Introduction

L'Internet des Objets (IdO), plus connu sous le nom d'Internet of Things (IoT) en anglais, représente bien plus qu'une simple avancée technologique. C'est une révolution numérique qui a transformé la façon dont les objets physiques interagissent avec le monde virtuel. L'IoT ouvre la voie à une connectivité et à une intelligence inédite, devenant ainsi un pilier technologique clé dans un monde où la collecte et l'analyse des données sont essentielles pour la prise de décision. Ce chapitre explore les origines, les principes fondamentaux et l'influence croissante de l'IoT dans divers secteurs. Il démontre comment l'IoT redéfinit l'industrie, la santé, l'agriculture, la logistique et d'autres domaines grâce à des exemples concrets. Il aborde également les aspects techniques tels que les protocoles de communication et les architectures IoT, tout en mettant en lumière les défis et opportunités associés à cette révolution. En fin de compte, ce chapitre vise à éduquer, à inspirer et à préparer les lecteurs à un avenir de plus en plus connecté, où la convergence du physique et du numérique redéfinit nos modes de vie et de travail.

II. Internet des Objets (IdO)

II.1Définition

L'Internet des Objets (IdO) ou en anglais internet of things (IoT), est un système qui interconnecte les objets physiques et virtuels via des réseaux de communication en utilisant des protocoles standard et des technologies de l'information et de la communication (TIC). Cela permet aux objets connectés d'échanger des données en temps réel, avec ou sans intervention humaine, en utilisant des capteurs, des dispositifs de traitement de données et de connectivité [1]. Cependant, l'IoT soulève également des préoccupations en matière de sécurité et de confidentialité des données, nécessitant la mise en place de mesures de sécurité appropriées pour protéger les données et les systèmes connectés.

Selon l'Union Internationale des Télécommunications (UIT), l'IdO est une infrastructure mondiale qui interconnecte les objets physiques et virtuels grâce à des technologies de l'information et de la communication interopérables, englobant un écosystème diversifié d'acteurs tels que les fabricants de capteurs, les éditeurs de logiciels, les opérateurs et les intégrateurs [2].

II.2 Historique

L'expression « Internet des objets » a été popularisée par Kevin Ashton en 1999, qui travaillait dans le domaine de l'optimisation de la chaîne d'approvisionnement pour Proctor & Gamble, a

utilisé l'expression comme titre d'une présentation pour un nouveau projet de capteur sur lequel il travaillait, et elle s'est imposée. Cependant, l'Internet des objets est un concept encore plus ancien :

Années 1970 : L'idée d'appareils connectés était alors connue sous le nom « d'informatique ubiquitaire ».

Début des années 1980 : Le premier appareil de l'IoT au monde a été inventé à l'université Carnegie Mellon en Pennsylvanie, États-Unis. Un groupe d'étudiants a créé un système permettant de s'assurer que le distributeur automatique de Coca-Cola de leur campus rende compte de son contenu par le biais d'un réseau, afin de leur éviter de se rendre à la machine s'il n'y avait plus de boissons. Ils ont installé des micro-interrupteurs dans la machine pour indiquer le nombre de canettes de Coca disponibles et si elles étaient froides.

1990 : John Romkey a connecté un grille-pain à Internet pour la première fois.

1991 : Un groupe d'étudiants de l'université de Cambridge en Angleterre a utilisé le premier prototype de caméra Web pour contrôler la quantité de café disponible dans la cafetière de leur laboratoire informatique. Pour ce faire, les étudiants ont programmé la caméra Web de manière à ce qu'elle prenne des photos de la cafetière trois fois par minute. La caméra envoyait les images aux ordinateurs locaux pour que les utilisateurs puissent vérifier s'il restait du café.

2000 : LG Electronics a présenté le premier réfrigérateur au monde connecté à Internet. Les consommateurs ont ainsi pu faire leurs courses alimentaires en ligne et passer des appels vidéo.

2008 : La première conférence internationale consacrée à l'Internet des objets s'est tenue en 2008 en Suisse.

2010 : L'expression « Internet des objets » a commencé à prendre de l'ampleur. On a appris que le service StreetView de Google n'avait pas seulement pris des photos à 360 degrés, mais avait également stocké des données relatives aux réseaux Wi-Fi (Wireless-Fidelity) d'habitants. Un débat s'est alors ouvert pour déterminer si Google avait l'intention d'indexer non seulement Internet, mais également le monde physique. La même année, le gouvernement chinois a annoncé que l'Internet des objets serait une priorité stratégique dans son plan quinquennal.

2011 : Gartner, l'entreprise d'études de marché qui a inventé le « cycle d'effervescence des technologies émergentes », a inclus l'Internet des Objets dans sa liste des phénomènes émergents.

2012 : La plus grande conférence européenne dédiée à Internet, le Web, a porté sur le thème de l'Internet des objets. Parallèlement, des magazines comme Forbes et Wired ont commencé à intégrer l'Ido dans leur vocabulaire.

2014 : Google a annoncé son intention de racheter Nest pour 3,2 milliards de dollars, une opération qui a permis de sensibiliser le grand public à l'Internet des objets. Le "Salon de l'Électronique Grand Public, en anglais Consumer Electronics Show (CES) de Las Vegas s'est tenu la même année autour du thème de l'Internet des objets [3].

Années 2020 et au-dela : L'IoT continue de se développer à un rythme rapide, avec des milliards de dispositifs connectés dans le monde entier. Les avancées en matière d'IA (Intelligence Artificielle) et d'analyse de données permettant d'exploiter encore plus les informations collectées par les dispositifs IoT.

II.3 L'évolution d'internet des objets (Du M2M a IoT)

Base	IoT (Internet of Things)	M2M (Machine to Machine)
Abréviation	Internet des objets	Machine à machine
Communication	Automatisation des capteurs IoT	Communique directement entre les machines
Connexion	La connexion se fait via différents types de communication	Connexion point à point
Protocoles de communication	HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), Telnet, etc. sont utilisés.	Des techniques de communication et des protocoles traditionnels sont utilisés.
Intelligence	Les objets sont responsables de la prise de décision	Observation d'un certain degré d'intelligence
Technologie	Technologie matérielle et logicielle	Technologie basée sur le matériel
Livraison des données	Selon le protocole Internet	Les appareils peuvent être connectés via des réseaux mobiles ou d'autres réseaux
Connexion Internet	Une connexion Internet active est requise	Les appareils ne dépendent pas d'une connexion Internet
Portée	Plusieurs utilisateurs peuvent se connecter à la fois sur Internet	Communiquer avec une seule machine à la fois
Type d'entreprise	B2C (Business to Customers) et B2B (Business to Business)	Seul le B2B (Business to Business) est utiliser

Tableau I.1 : M2M vs IoT [4].

Prise en charge de l'API ouverte	L'IoT prend en charge les intégrations d'API (Application Programming Interface) ouvertes	M2M ne prend pas en charge l'API ouverte
Partage de données	Les données sont partagées avec des applications qui tendent à améliorer l'expérience de l'utilisateur final	Les données sont partagées avec les parties de communication elles-mêmes.

L'Internet des objets repose sur la technologie du Machine To Machine (M2M), qui existe depuis longtemps et a contribué au développement de l'Internet des objets jusqu'à sa domination du marché. Une différence clé entre le M2M et l'IoT est que l'IoT implique généralement des objets connectés capables de transmettre des données en temps réel et de fonctionner de manière autonome, tandis que le M2M se concentre davantage sur la transmission de données entre des dispositifs pour un objectif précis [2].

II.4 Plateforme de développement d'IoT

Une plateforme IoT offre une infrastructure pour les appareils connectés, permettant la collecte, le stockage, la gestion, l'analyse et la visualisation des données générées. Elle inclut également des outils pour la création d'applications IoT, la gestion des utilisateurs et des appareils, ainsi que des fonctionnalités de sécurité avancées comme la surveillance des menaces, l'authentification et l'autorisation des utilisateurs et des appareils, et la protection contre les attaques. En résumé, une plateforme IoT est une solution complète pour créer, déployer et gérer efficacement et en toute sécurité des applications IoT. Les plateformes IoT permettent de connecter le matériel, gérer les protocoles de communication, assurer la sécurité et l'authentification des dispositifs et des utilisateurs, ainsi que collecter, visualiser et analyser les données des capteurs et des appareils [5].

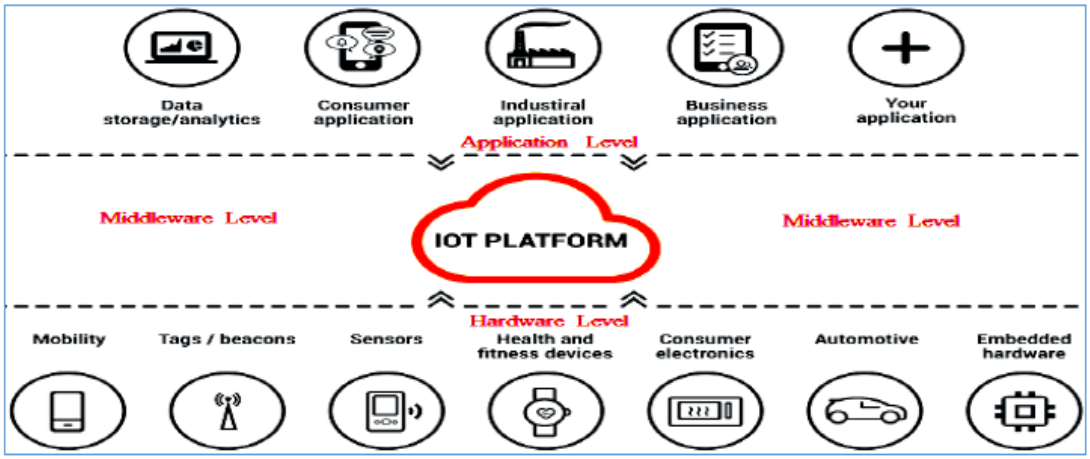

Figure I.1 : plateforme IoT [6].

Parmi ces plateformes d'IoT, nous citons :

II.4.1 Google Cloud Plateforme

Google Cloud Plateforme est une plateforme de « Cloud Computing » fournie par **Google**, proposant un hébergement sur la même infrastructure que celle que **Google** utilise en interne pour des produits tels que son moteur de recherche. Produits permettant de construire une gamme de programmes allant de simples sites web à des applications complexes [6].

II.4.2 AWS IoT

AWS (Amazon Web Services Internet of Things) IoT est une plateforme qui permet aux appareils de se connecter au cloud et de communiquer avec d'autres appareils et applications cloud. Elle fournit un support complet pour MQTT (Message Queuing Telemetry Transport). Les messages MQTT peuvent être envoyés et reçus par les appareils en utilisant le protocole TCP (Transmission Control Protocol), c'est une plateforme qui peut traiter un grand nombre de messages [7].

II.4.3 Azure IoT Hub

Microsoft Azure IoT Hub est une plateforme de cloud computing qui permet la gestion et l'interconnexion des appareils connectés. Elle prend en charge les protocoles MQTT, AMQP (Advanced Message Queuing Protocol) et HTTPS (HyperText Transfer Protocol Secure), et permet l'enregistrement instantané des appareils avec une identité unique pour chaque appareil. Elle offre également un tableau de bord basé sur le cloud pour accéder aux données des appareils et des applications. Cependant, la documentation du hub IoT peut être déroutante et nécessite plus de détails [7].

II.4.4 IBM Watson IoT

IBM (International Business Machines) Watson IoT est une plateforme de développement basée sur le cloud et destinée aux développeurs d'applications IoT. Cette plateforme aide à créer, moderniser et connecter des appareils avec des applications sur le cloud sans aucun effort. Elle fournit aussi un tableau de bord pour améliorer la visualisation ainsi qu'un service d'analyse de données.

Par contre la navigation entre les différents services est complexe et l'interface n'est pas très intuitive [7].

III. Les objets connectés

III.1 Définition

Les objets connectés sont des dispositifs avec leur propre fonctionnalité mécanique et/ou électrique, conçus pour collecter, traiter et transmettre des données à partir de capteurs via des

fonctionnalités de connectivité. Ils nécessitent une source d'énergie pour fonctionner en temps réel, qui peut être une pile, une batterie, le réseau électrique ou des mécanismes de récupération d'énergie tels que les panneaux solaires. L'internet des objets comprend à la fois des objets actifs capables de calculs, de mesures et d'actions sur l'environnement, ainsi que des objets passifs qui peuvent être suivis et détectés par les objets actifs [6].

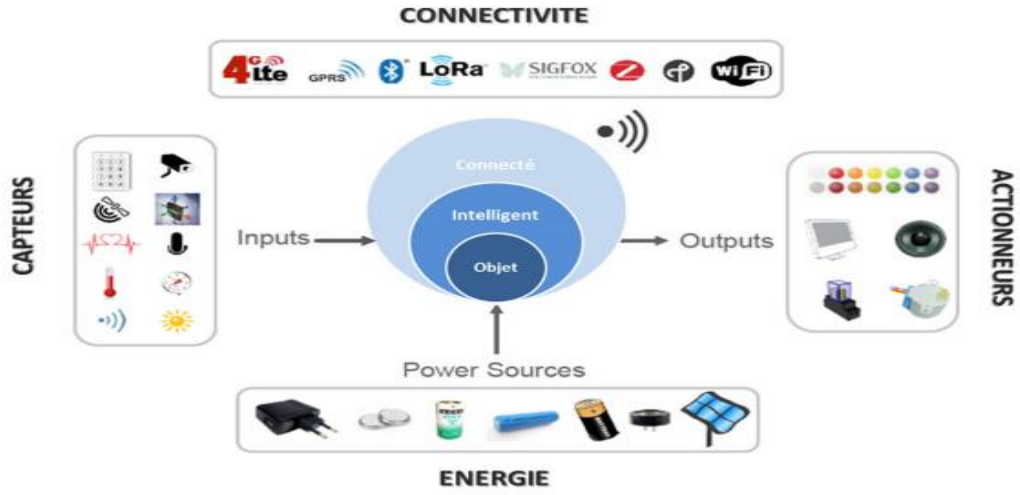

Figure I.2 : Objet Connecté [8].

III.2 Les composants d'un objet connecté

III.2.1 Les capteurs

Les capteurs sont des dispositifs électroniques qui convertissent des grandeurs physiques en signaux numériques pour être traités par des logiciels ou des systèmes électroniques. Il existe trois types de capteurs : analogiques, numériques et à sortie mixte. Les capteurs analogiques produisent une sortie continue proportionnelle à la grandeur mesurée, les capteurs numériques produisent une sortie binaire (0 ou 1), et les capteurs à sortie mixte combinent une sortie analogique et une sortie numérique. [6]

La figure suivante montre quelques types de capteurs.

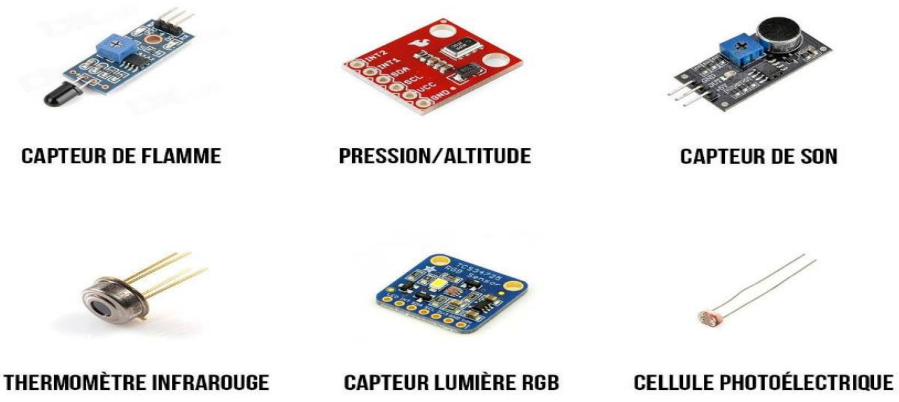

Figure I.3 : capteurs pour mesurer des variables physiques dans un environnement [9].

III.2.2 Les sources d'énergie

Les sources d'énergie pour les objets connectés sont diverses et dépendent des besoins énergétiques et du mode d'utilisation de l'appareil. Les principales sources d'énergie sont : alimentation filaire pour les objets connectés à une prise de courant, piles ou batteries pour les appareils sans accès à une prise, capteurs d'énergie pour convertir l'énergie ambiante en électricité, et objets passifs alimentés par les ondes électromagnétiques émises par les lecteurs RFID (Radio Frenquency Identification) ou NFC (Near Field Communication). L'énergie est un défi majeur pour les objets connectés en raison de leur consommation énergétique et de leur impact environnemental. Il est donc essentiel de trouver des moyens pour prolonger la durée de vie des batteries et utiliser des sources d'énergie renouvelable afin de minimiser leur impact sur l'environnement [8].

La figure suivante montre quelques sources d'énergie :

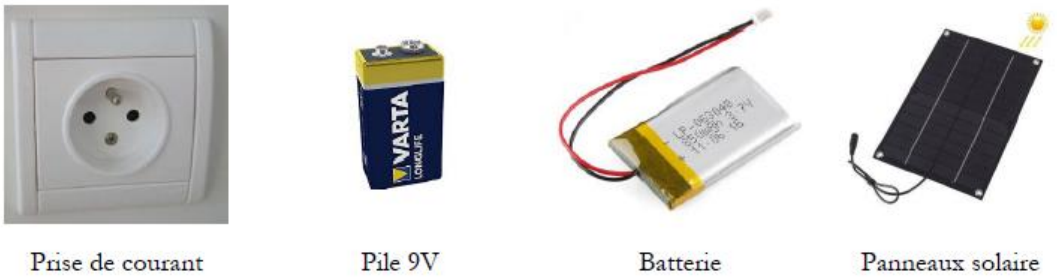

Figure I.4 : Sources d'énergie [6].

III.2.3 Les actionneurs

Les actionneurs sont des composants clés dans les systèmes de contrôle et d'automatisation, permettant de transformer les signaux numériques en actions physiques. Les exemples courants d'actionneurs incluent les moteurs, les vérins, les vannes, les haut-parleurs, les interrupteurs, les pompes, les serrures et les caméras. Ces actionneurs sont utilisés dans une variété d'applications telles que les robots, les machines-outils, les systèmes de refroidissement, les systèmes de sécurité, les systèmes de surveillance, etc. En somme, les actionneurs sont indispensables pour permettre le fonctionnement automatique et contrôlé de nombreux systèmes [8].

La figure montre quelques actionneurs :

Figure I.5 : actionneurs [6]

III.2.4 La connectivité

La connectivité d'un objet IoT est assurée par une antenne Radio Fréquence qui permet à l'objet de communiquer avec un ou plusieurs réseaux IoT. Les objets peuvent envoyer des informations telles que leur identité, leur état, des alertes ou des données de capteurs, et recevoir des informations telles que des commandes d'action et des données. Le module de connectivité assure également la gestion du cycle de vie de l'objet, ce qui inclut l'authentification et l'enregistrement dans le réseau, la mise en service, la mise à jour et la suppression de l'objet du réseau [8].

La figure suivante montre quelques exemples de modules de connectivité :

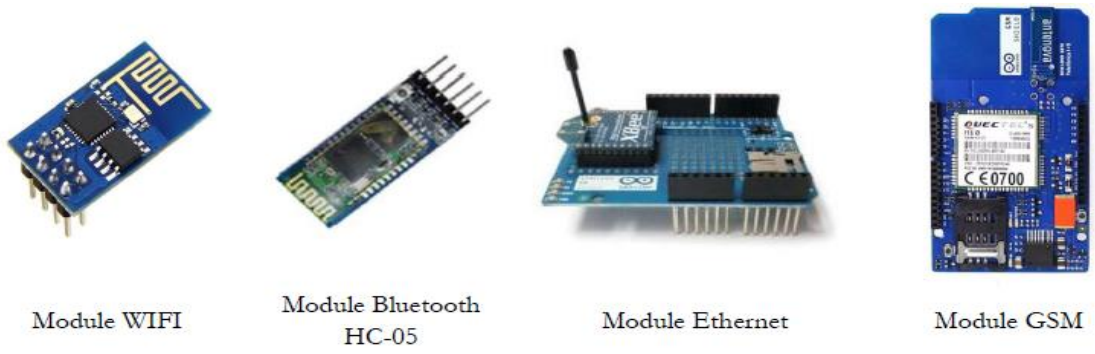

Figure I.6 : Modules de connectivité [6].

III.3 Exemples d'objets connectés

III.3.1 Parrot POT (Pot de fleurs intelligent et connecté pour plantes)

Figure I.7 : Parrot Capteur Intelligent pour Plantes Intérieur/Extérieur [10].

Un pot de fleur connecté qui s'occupe de vos plantes, doté de divers capteurs et d'un réservoir d'eau, le POT pourra entretenir vos fleurs même lors de vos absences du domicile. L'application

vous donnera des conseils d'entretien et des rappels divers. Un gadget idéal pour les personnes qui n'ont pas forcément la main verte [10].

III.3.2 Netgear Arlo Pro 100% sans-fil

Figure I.8 : Arlo Pro Pack de 2 Caméras, Smart caméra HD grand angle avec batterie rechargeable 6 mois et audio bidirectionnel, Intérieure / extérieure et alarme intégrée [10]

La plupart des caméras connectées utilisent une alimentation filaire, Netgear fait le pari un peu fou du 100% sans-fil. La solution Arlo Pro comporte une base qui peut ensuite contrôler plusieurs caméras adaptées aux usages intérieurs et extérieurs. De plus, Netgear offre une excellente solution d'enregistrement sur le Cloud adaptable à tous vos besoins pour la surveillance [10].

IV. Les protocoles de communications

IV.1 Le Protocole d'application contrainte (CoAP)

Le protocole « Constrained Application Protocol » (CoAP), est un protocole de communication web développé par Internet Engineering Task Force (IETF) basé sur l'architecture « Representational State Transfer » (REST), conçu pour les appareils à faible consommation d'énergie et de bande passante, tels que les capteurs, les actionneurs et autres appareils de l'Internet des Objets. Le protocole CoAP utilise une architecture de type client-serveur, similaire au protocole HTTP utilisé sur le web. Les clients CoAP envoient des requêtes à des serveurs CoAP pour récupérer des ressources, telles que des capteurs, des actionneurs ou d'autres types de données. Les serveurs CoAP répondent aux requêtes en envoyant des réponses qui contiennent les données demandées ou des messages d'erreur si la requête n'a pas réussi.

Le protocole CoAP est aussi utilisé dans les dispositifs domotiques, pour permettre une communication efficace et légère entre les appareils connectés [6].

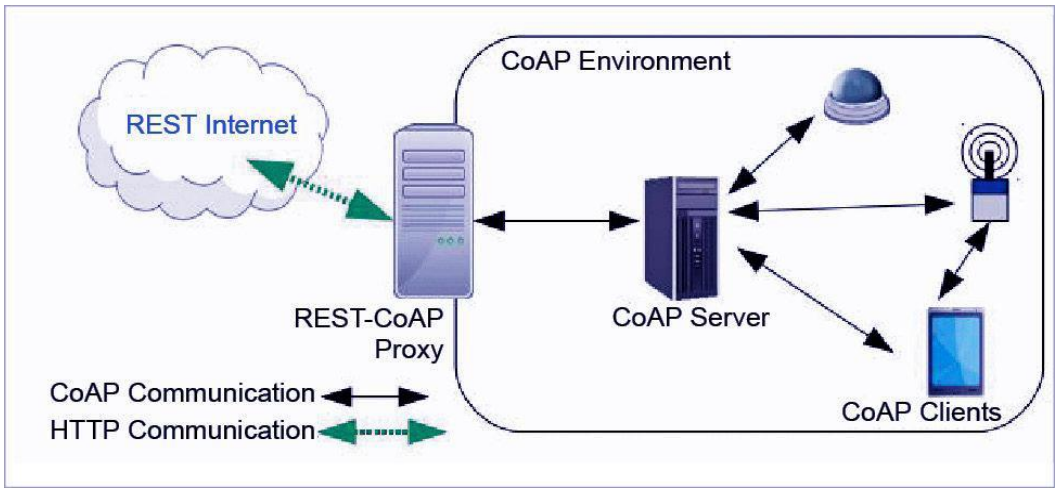

Figure I.9 : protocole COAP [6].

IV.2 Le Protocole AMQP

AMQP signifie « **Advanced Message Queuing Protocol** », est un protocole de messagerie open source qui fournit une plateforme pour la messagerie d'applications. Il a été conçu pour permettre la communication entre des applications indépendantes du langage, de la plateforme et de la technologie utilisée, ce qui présente un énorme frein dans le monde de l'IoT.

AMQP est géré par l'OASIS (Organization for the Advancement of Structured Information Standards), est largement utilisé dans les applications d'entreprise, les services financiers et les centres de données. Le protocole AMQP définit un certain nombre de concepts clés, notamment les suivants :

-Producteur (Publisher) : une application qui crée et envoie des messages.

-Consommateur (Consumer) : une application qui reçoit et traite des messages.

-File d'attente (Queue) : un espace de stockage pour les messages en transit.

-Echange (Exchange) : une entité qui reçoit les messages des producteurs et les distribue aux files d'attente en fonction des règles de routage.

-Liaison (Binding) : une règle qui associe une file d'attente à un échange en fonction de son nom et de son type.

Le protocole AMQP est conçu pour être extensible et évolutif. Il prend en charge plusieurs protocoles de transport, tels que TCP (Transmission Control Protocol), SSL (Secure Socket Layer)/TLS(Transport Layer Security) et WebSocket, ce qui permet aux applications de communiquer de manière sécurisée sur différents types de réseaux. Il est également compatible avec plusieurs langages de programmation, tels que Java, Python, .NET, Ruby, etc., ce qui permet aux développeurs de créer des applications AMQP dans leur langage de choix. [6]

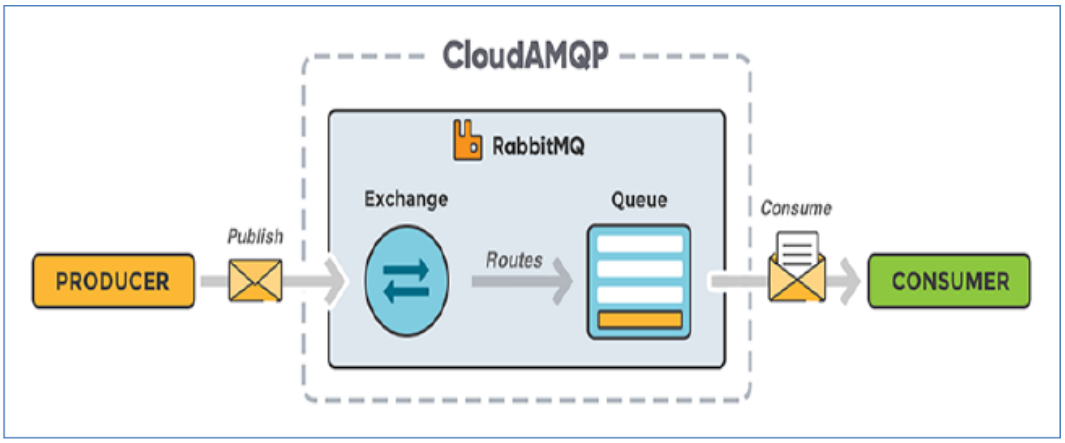

Figure I.10 : Fonctionnement de Protocole AMQP [11].

IV.3 Le Protocole MQTT

MQTT (Message Queuing Telemetry Transport) est un protocole de communication de messagerie légère (messaging) pour l'internet des objets. Il a été développé pour permettre à des appareils de faible puissance et à des réseaux à bande passante limitée de communiquer efficacement avec des systèmes distants.

Le protocole MQTT est basé sur un modèle de publish/subscribe, où les clients s'abonnent à des topics (sujets) pour recevoir des messages publiés par les serveurs. Les messages sont publiés avec une qualité de service, en anglais Quality of Service (QoS) qui peut être configurée en fonction de l'importance et de la fiabilité du message.

Le protocole MQTT est conçu pour être léger, simple et rapide, avec une empreinte mémoire minimale. Il utilise le protocole TCP/IP (Transmission Control Protocol/Internet Protocol) pour la connexion réseau et est souvent utilisé en conjonction avec des protocoles de sécurité tels que TLS/SSL pour assurer la confidentialité et l'authentification des messages échangés [6].

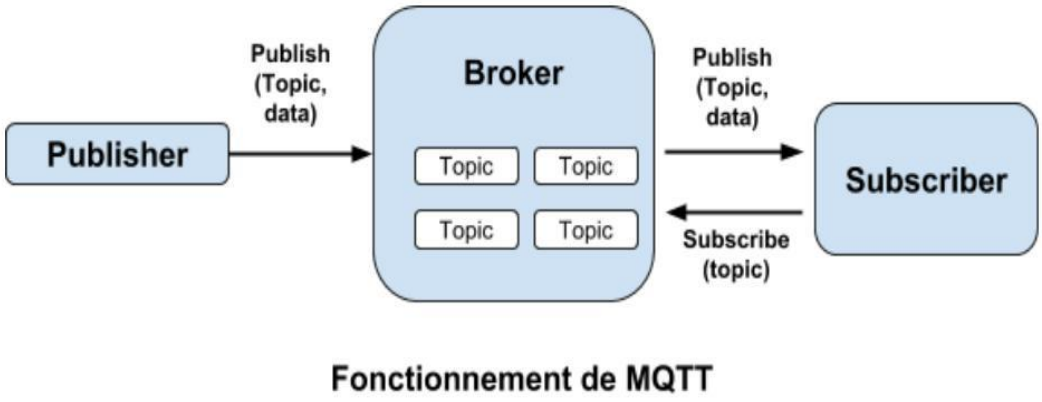

Figure I.11 : fonctionnement du protocole MQTT [12].

-Broker (Courtier) : Le Broker est le serveur qui distribue les informations aux clients intéressés connectés au serveur.

-Client : L'appareil qui se connecte au Broker pour envoyer ou recevoir des informations.

-Topic (Sujet) : Le nom du message. Les clients publient, s'abonnent ou font les deux à un Topic.

-Publish (Publier) : Clients qui envoient des informations au Broker à distribuer aux clients intéressés en fonction du nom de la rubrique.

-Subscribe (S'abonner) : Les clients indiquent au Broker le ou les Topic(s) qui les intéressent. Lorsqu'un client s'abonne à un Topic, tout message publié sur le Broker est distribué aux abonnés de ce Topic. Les clients peuvent également se désabonner pour ne plus recevoir de messages du Broker sur ce Topic.

-QoS : Chaque connexion peut spécifier une qualité de service au Broker avec une valeur entière comprise entre 0 et 2. La QoS n'affecte pas le traitement des transmissions de données TCP, seulement entre les clients MQTT.

0 spécifie au plus une fois, ou une fois et une seule fois sans qu'un accusé de réception ne soit nécessaire. Ceci est souvent appelé « feu et oublie ».

1 spécifie au moins une fois. Le message est envoyé plusieurs fois jusqu'à la réception d'un accusé de réception, autrement appelé livraison avec accusé de réception.

2 spécifie exactement une fois. Les clients expéditeurs et destinataires utilisent une négociation à deux niveaux pour garantir la réception d'une seule copie du message, appelée livraison assurée [13].

V. Fonctionnement de l'IoT

Le fonctionnement de l'IoT repose sur des étapes essentielles telles que la captation, la conversion en signaux numériques, l'interconnexion avec des réseaux IP, le stockage des données brutes, et bien d'autres encore, voilà les éléments clés de ce processus :

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

-Concentrer : permet d'interfacer un réseau spécialisé d'objet à un réseau IP standard (e.g. WiFi) ou des dispositifs grand public.

-Stocker : qualifie le fait d'agréger des données brutes, produites en temps réel, métas tagués, arrivant de façon non prédictible.

-Enfin, présenter indique la capacité de restituer les informations de façon compréhensible par l'Homme, tout en lui offrant un moyen d'agir et/ou d'interagir. Deux autres processus n'apparaissent pas sur le schéma, car ils sont à la fois transverses et omniprésents : Le traitement des données est un processus qui peut intervenir à tous les niveaux de la chaîne, depuis la capture de l'information jusqu'à sa restitution. Une stratégie pertinente, et commune quand on parle d'Internet des Objets, consiste à stocker l'information dans sa forme intégrale. On collecte de manière exhaustive, « big data », sans préjuger des traitements qu'on fera subir aux données. Cette stratégie est possible aujourd'hui grâce à des architectures distribuées type NoSQL (Not only SQL) est un système de base de données qui est dit "non relationnel", capables d'emmagasiner de grandes quantités d'information tout en offrant la possibilité de réaliser des traitements complexes en leur sein (Map/Reduce par exemple) [14].

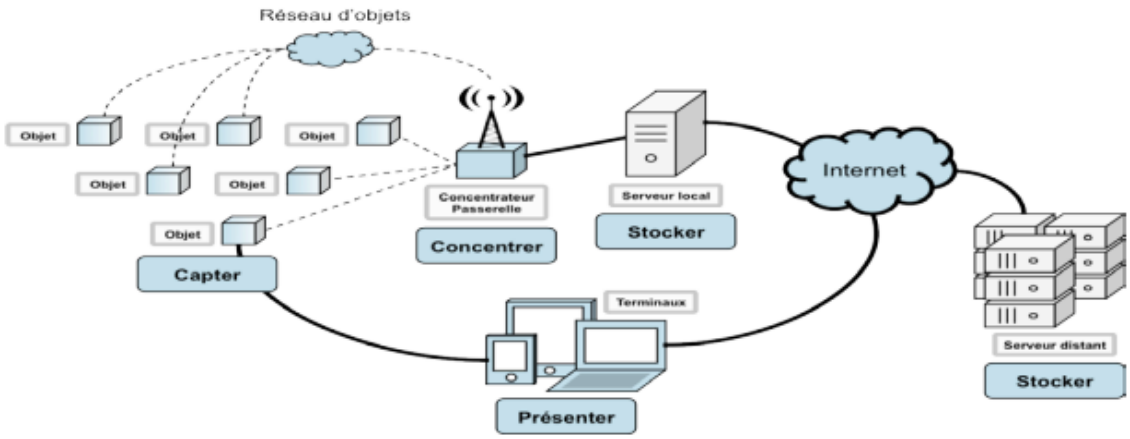

Figure I.12: fonctionnement de l'IoT [14].

V.1 Les composants d'un système IoT

Un système IoT assemble de nombreux acteurs et composants technologiques. Il est composé d'objets connectés, de réseaux de communication sans fil, de plateformes de collecte, d'hébergement et de traitement des données (voir la Figure I.14) [6].

Voici les principaux composants d'un système IoT :

-Les dispositifs ou objets connectés : ce sont des appareils électroniques dotés de capteurs, de processeurs, d'une connectivité réseau et d'une source d'alimentation.

-Les capteurs : ils sont utilisés pour collecter des données sur l'environnement ou le comportement des objets connectés. Les capteurs peuvent mesurer des grandeurs physiques telles que la température, l'humidité, la lumière, la pression, etc.

-Les réseaux : ils fournissent la connectivité nécessaire pour les objets connectés pour échanger des données entre eux et avec le cloud. Les réseaux peuvent être filaires, sans fil ou un mélange des deux.

-Les passerelles : ce sont des appareils qui agissent comme des intermédiaires entre les objets connectés et le cloud. Ils collectent les données des objets connectés et les transmettent au cloud pour traitement.

-Le cloud : c'est l'infrastructure qui stocke, traite et analyse les données collectées par les objets connectés. Il fournit également des services d'application pour traiter les données et prendre des décisions basées sur ces données.

-Les applications : ce sont les interfaces utilisateurs qui permettent aux utilisateurs de visualiser et d'interagir avec les données collectées par les objets connectés. Les applications peuvent être des applications mobiles, des applications web, des tableaux de bord, etc.

-La sécurité : elle est cruciale pour les systèmes IoT pour protéger les données sensibles collectées par les objets connectés et stockées dans le cloud. Les systèmes IoT doivent être protégés contre les attaques de pirates informatiques et les violations de la vie privée [6].

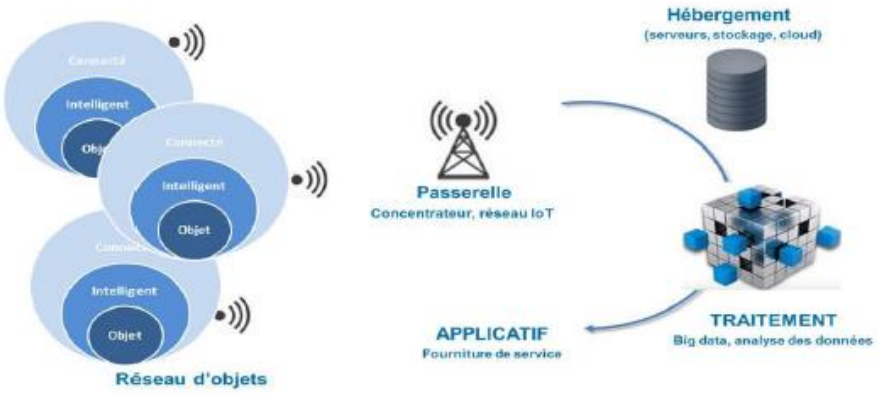

Figure I.13 : système d'IoT [19].

V.2 Etapes de mise en place d'un IoT

Les objets connectés sont au sein de l'IoT, mais il est important de pouvoir connecter l'ensemble de ces objets, les faire échanger des informations et interagir au sein d'un même environnement. La mise en place de l'IoT passe par les étapes suivantes :

1. L'identification : Rendre possible l'identification de chaque élément connecté (IPV4(Internet Protocol version 4), IPV6(Internet Protocol version 6)).

2. L'installation de capteurs : Mise en place de dispositifs nous rapprochant du monde réel.

3. La connexion des objets entre eux : Etablir une connexion entre tous les objets afin qu'ils puissent échanger des informations (SigFox, LoRa, NFC, Bluetooth).

4. L'intégration : C'est Intégration des objets pour que les données soient transmises d'une couche à une autre (middlewares).

5. La connexion à un réseau : Relier les objets et leurs données au monde informatique via un réseau internet par exemple en utilisant (AMQP, CoAP, MQTT) [15].

V.3 Technologies de l'IoT

L'IoT permet l'interconnexion des différents objets intelligents via l'Internet. Ainsi, pour son fonctionnement, plusieurs systèmes technologiques sont nécessaires. L'IoT désigne diverses solutions techniques (RFID, TCP/IP, technologies mobiles, etc.) qui permettent d'identifier des objets, capter, stocker, traiter, et transférer des données dans les environnements physiques, mais aussi entre des contextes physiques et des univers virtuels. En effet, bien qu'il existe plusieurs technologies utilisées dans le fonctionnement de l'IoT, nous mettons l'accent seulement sur quelques-unes citées ci-dessous [16].

V.3.1 Les technologies de courte portée

V.3.1.1 Le protocole NFC

Les protocoles **Near Field Communication (NFC)** sont fondés sur la technologie d'identification par radio fréquence RFID. Les objets équipés d'une puce électronique RFID possèdent une « étiquette » et sont automatiquement identifiés par radio fréquence lorsqu'ils se trouvent à proximité d'un équipement appelé interrogateur. Le protocole NFC est un standard de communication radiofréquence sans contact à très courte distance, de l'ordre de quelques centimètres, permettant une communication simple entre deux équipements électroniques. Il est utilisé dans de nombreux domaines, tels que les paiements mobiles, les transports en commun, la gestion d'accès, le partage de fichiers, la domotique, etc. Les objets équipés de la technologie NFC peuvent être des smartphones, des cartes de paiement, des étiquettes, des capteurs [16].

V.3.1.2 Bluetooth

Le Bluetooth, inventé en 1994 par Ericsson, est un standard de transfert de données sans fil utilisé dans les téléphones mobiles pour la communication avec des objets connectés. Il offre une faible bande passante et une consommation d'énergie réduite, mais permet des distances de transmission courtes. Les différentes versions du protocole, dont le Bluetooth 5, offrent des fonctionnalités variées. Ainsi, le Bluetooth est largement utilisé dans de nombreux dispositifs IoT tels que les oreillettes sans fil, les montres intelligentes, les enceintes portatives, les stations météo, les thermostats, etc [16].

V.3.1.3 Zigbee

Le protocole Zigbee est un standard de communication sans fil utilisé dans l'Internet des objets et la domotique, offrant une faible consommation d'énergie et une faible bande passante. Avec une portée moyenne de 10 mètres, il est idéal pour les appareils fonctionnant sur batterie et pour le transfert de données en faible volume. Zigbee fonctionne en réseau maillé, permettant à chaque nœud d'agir comme un routeur pour transmettre les données à d'autres nœuds, ce qui augmente la portée et la fiabilité du réseau. Il est utilisé dans de nombreux appareils domestiques intelligents tels que les thermostats, les capteurs de mouvement et les systèmes d'éclairage [16].

V.3.2 Les technologies de moyenne portée

V.3.2.1 Z-Wave

Le **Z-Wave** est un protocole de communication sans fil principalement dédié à la domotique. Il permet de transmettre des données sur des distances allant de 30 mètres en intérieur à 100 mètres en plein air. Il fonctionne selon une topologie en maillage (mesh) où chaque appareil communique avec ses voisins proches pour relayer les informations émises, ce qui permet d'étendre la portée du réseau et d'améliorer la qualité de la transmission. Cette architecture de réseau permet également de créer des routes de communication alternatives en cas de perte de connexion avec un nœud du réseau. Le protocole Z-Wave a été développé pour des usages peu énergivores nécessitant un faible débit de données. Tout comme le protocole Zigbee, l'utilisation de Z-Wave ne nécessite que très peu de puissance et les appareils peuvent donc communiquer pendant plusieurs années avec une simple pile [16].

V.3.2.2 Wi-Fi

Le **Wi-Fi** désigne un ensemble de protocoles de communications sans fil, permettant des connexions à **haut débit** sur des distances de 20 à 100 mètres. Il s'agit d'un réseau local sans fil très énergivore, qui ne convient que pour les appareils branchés sur secteur ou dont l'alimentation électrique peut être aisée et fréquente. Il utilise la bande de fréquence libre de 2,4 GHz ou de 5 GHz pour les communications sans fil. Il permet de transférer rapidement beaucoup de données. Il existe différentes normes Wi-Fi correspondant à une portée et un débit variable [16].

V.3.2.3 Bluetooth Low Energy

Aussi connue sous l'appellation Wibree, la technologie **Bluetooth Low Energy** (BLE) est un protocole de réseau personnel sans fil à très basse consommation. Comme la technologie Bluetooth originelle, le BLE ne permet de transférer qu'une quantité limitée de donnée à une distance moyenne de 60 mètres. La principale différence entre le BLE et la technologie

Bluetooth classique est la consommation électrique nécessaire à la communication. En effet, le BLE consomme dix fois moins d'énergie que la technologie Bluetooth classique, ce qui permet aux appareils BLE de fonctionner sur des piles boutons pendant plusieurs années. Cette faible consommation d'énergie permet également une utilisation plus efficace de l'énergie pour les appareils connectés, ce qui est particulièrement important pour les dispositifs alimentés par batterie [16].

V.3.3 Les technologies de longue portée

V.3.3.1 Réseaux cellulaires mobiles

Fournis par les opérateurs de télécommunication, les **réseaux cellulaires mobiles**, basés sur la technologie GSM (Global System for Mobile Communications), permettent de transférer une quantité importante de données à une longue portée. Ils nécessitent l'installation d'une carte SIM (Subscriber Identity Module), dans l'appareil à connecter, afin d'identifier celui-ci sur le réseau de communication. Succédant aux premières générations des standards pour la téléphonie mobile, qui ont progressivement permis d'accroître le débit de communication, la quatrième génération (4G) permet une communication mobile à très haut débit [16].

V.3.3.2 Réseaux radio bas-débit

-Sigfox est un réseau de communication radio sans fil à bas débit et à basse fréquence, d'une portée moyenne de 10 kilomètres en milieu urbain et de 30 à 50 kilomètres en milieu rural. Il est également une technologie créée par l'entreprise du même nom. Ce réseau convient à des appareils à basse consommation, dotés ainsi d'une grande autonomie, qui transfèrent une faible quantité de données [16].

-LoRa est un protocole de communication radio à très basse consommation, qui permet de transmettre des données en petite quantité, à des distances de 2 à 5 kilomètres en ville et jusqu'à 45 kilomètres en milieu urbain. À l'instar de Sigfox, il s'agit d'un dispositif qui convient particulièrement aux équipements peu énergivores n'émettant que périodiquement, notamment les capteurs [16].

Le tableau suivant résume quelques caractéristiques techniques des différentes technologies citées en haut :

	Courte portée			Moyenne portée		Longue portée	
Technologies	NFC	Bluetooth	Zigbee	Wi-Fi	BLE	SigFox	LoRa
Portée moyenne (en intérieur)	< 10 cm	10 m	100 m	100 m	60 m	>2 km	>2 km
Débit (Mbit/s)	1.10^-3	1.10^-3	1.10^-2	1.10^3	1.10^-3	1.10^-3	1.10^-3
Fréquence	2.4 GHZ	2.4 GHZ	2.4 GHZ	2.4 GHZ 5 GHZ	2.4 GHZ	868 MH	868 MH
Usages	Téléphonie, Carte de Paiement	Périphériques Informatiques et multimédia	Domotique	Navigation Internet. Transfert Conséquent de données	Périphériques informatiques et multimédia	Prévention d'incide Collecte de donnée Gestion de réseaux	

Tableau I.2 : Quelques caractéristiques techniques des différentes technologies de l'IoT [15].

V.4 Architecture de l'Internet des objets

Il n'existe pas une architecture IoT unique universellement acceptée mais le format le plus basique et le plus largement accepté est une architecture IoT à cinq couches qui sont :

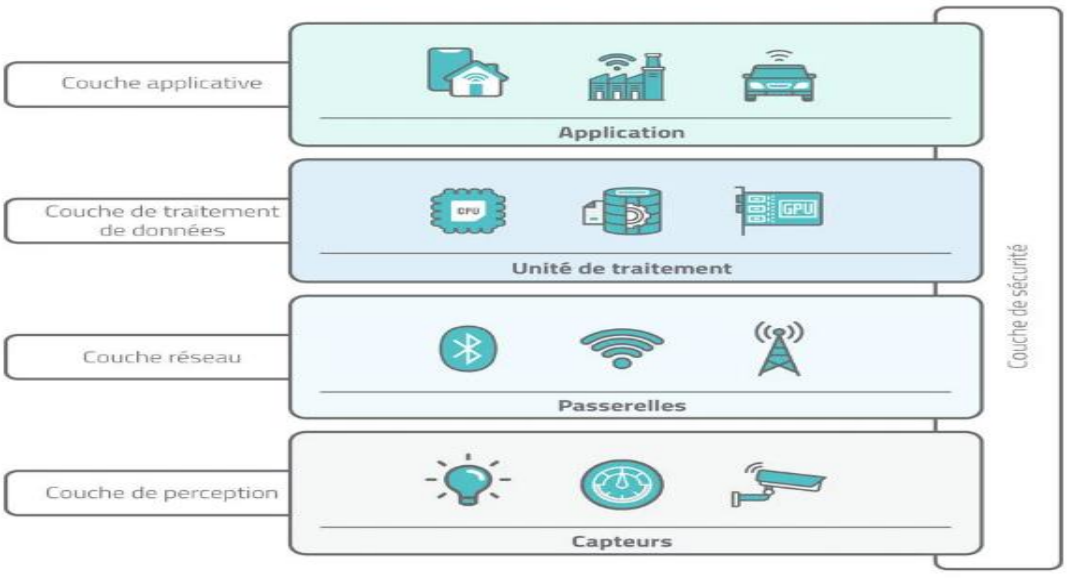

Figure I.14 : architecture en couches d'un système IoT [17].

-Couche de perception : La couche de perception de l'IoT convertit les signaux analogiques en données numériques et vice versa. Elle utilise des équipements physiques intelligents tels que les capteurs et les RFID pour collecter des informations du monde réel et faciliter l'interaction entre les appareils, permettant ainsi d'améliorer les opérations [18].

- Couche réseau : La couche réseau connecte les appareils aux objets intelligents, serveurs et autres appareils réseau pour traiter efficacement les données collectées. Elle gère la transmission des données, y compris les passerelles Internet et réseau qui assurent la connexion entre les réseaux de capteurs et Internet. Les systèmes d'acquisition de données, en anglais Data Acquisition Systems (DAS), agrègent et convertissent également les données dans cette couche [18].

- **Couche de traitement de données** La couche de traitement a 3 missions majeures :

-Rassembler les informations en temps réel provenant de la strate réseau afin que l'administrateur puisse évaluer leur importance et localisation.

-Enregistrer les informations pertinentes et véritablement utiles dans diverses options de stockage.

-Améliorer l'interconnexion des dispositifs intelligents en traitant les données. Des plateformes IoT sont employées pour garantir ces fonctions [18].

-Couche Applicative : La couche applicative communique avec l'utilisateur via des services particuliers. Les plateformes IoT peuvent servir d'infrastructure de développement logiciel avec des outils intégrés pour explorer les données, effectuer une analyse approfondie et visualiser les données. De cette façon, il est possible de construire des applications directement sur ces plateformes [18].

-Couche de sécurité : Cette couche est une couche transversale à toutes les couches précédentes. La sécurité de l'IoT est primordiale [18].

VI. Domaines d'applications de l'IoT

Aujourd'hui l'Internet des objets (IoT) est en train de révolutionner de nombreux domaines de notre vie quotidienne en permettant la connectivité et la communication entre des objets physiques et des systèmes informatiques [18].

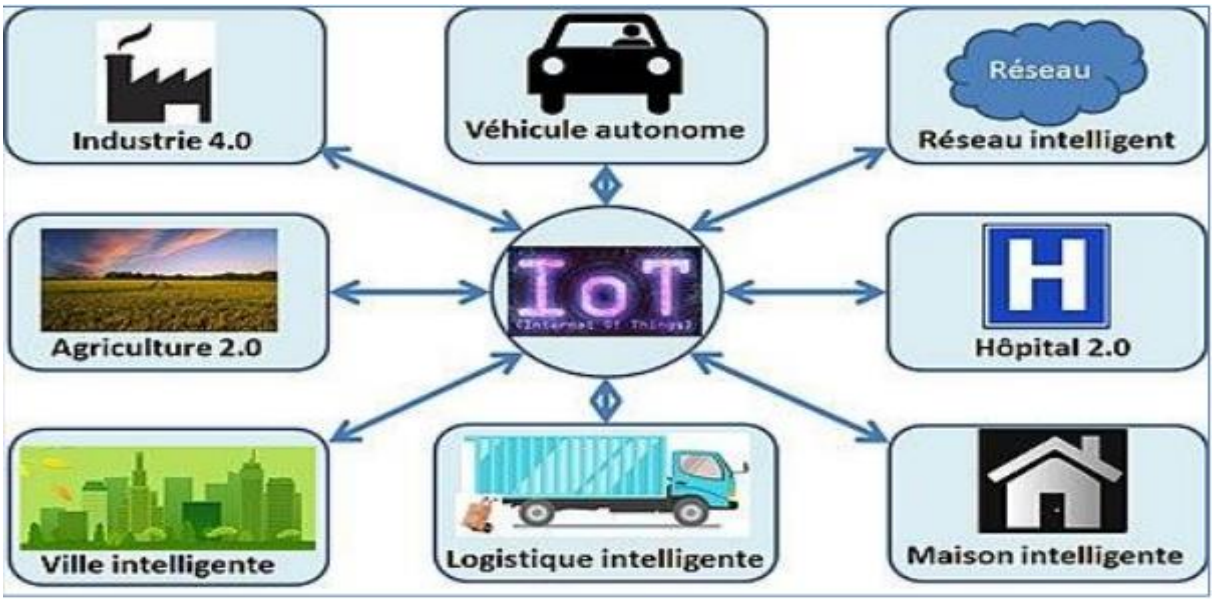

Figure I.15 : Les Domaines d'applications d'IoT [20].

VI.1 La domotique

La domotique regroupe différentes technologies pour permettre de contrôler, programmer et automatiser votre maison. Elle rassemble et utilise les domaines de l'électronique, de l'informatique, des télécommunications et de l'automatique. Elle permet aux utilisateurs de contrôler et de surveiller leur maison à distance, en utilisant des applications mobiles ou des commandes vocales. Par exemple, les utilisateurs peuvent régler la température, allumer ou éteindre les lumières, fermer les volets et vérifier l'état des équipements à distance [19].

VI.2 Le transport

Depuis la création de l'IoT, le nombre des véhicules intelligents sont en croissance, presque Tous les véhicules vendus aujourd'hui dans le monde renferment déjà des capteurs et de moyens de communication pour traiter la congestion du trafic, la sécurité, la pollution et le transport efficace des marchandises, etc [21].

La communication entre les véhicules peut permettre, par exemple, de détecter et d'éviter les situations de collision imminente, même si elles sont hors de la vue directe du conducteur, grâce à des systèmes de freinage d'urgence et d'alerte de collision.[21].

De plus, la communication avec les infrastructures de la route peut permettre de recueillir des informations en temps réel sur les conditions de circulation, les travaux routiers, les accidents ou les événements imprévus, afin de proposer aux conducteurs des itinéraires alternatifs plus rapides et plus sûrs [21].

Des applications Smartphone (comme Waze) sont déjà très répandues dans le monde. Ont permis aux conducteurs de bénéficier de mises à jour en temps réel sur les conditions de circulation, y compris les ralentissements, les accidents et la présence de radars de vitesse [21].

Figure I.16: voitures connectées [22].

VI.3 La santé

L'IoT a permis le développement de nombreuses applications dans le domaine de la santé telles que les capteurs portables qui peuvent collecter des données sur la santé d'un patient et être transmises à des professionnels de la santé pour un suivi à distance. Un exemple de cela est le médicament connecté Porteuse Digital Health, qui contient un capteur intégré pour suivre si le patient a bien pris son médicament et envoyer ces informations à un professionnel de santé. D'autres exemples incluent les dispositifs de surveillance à distance pour les maladies chroniques, la télémédecine et les systèmes de gestion de stocks de médicaments pour les hôpitaux et les pharmacies. Ces applications peuvent aider à améliorer la conformité des patients à leur traitement et à éviter les erreurs médicamenteuses [21].

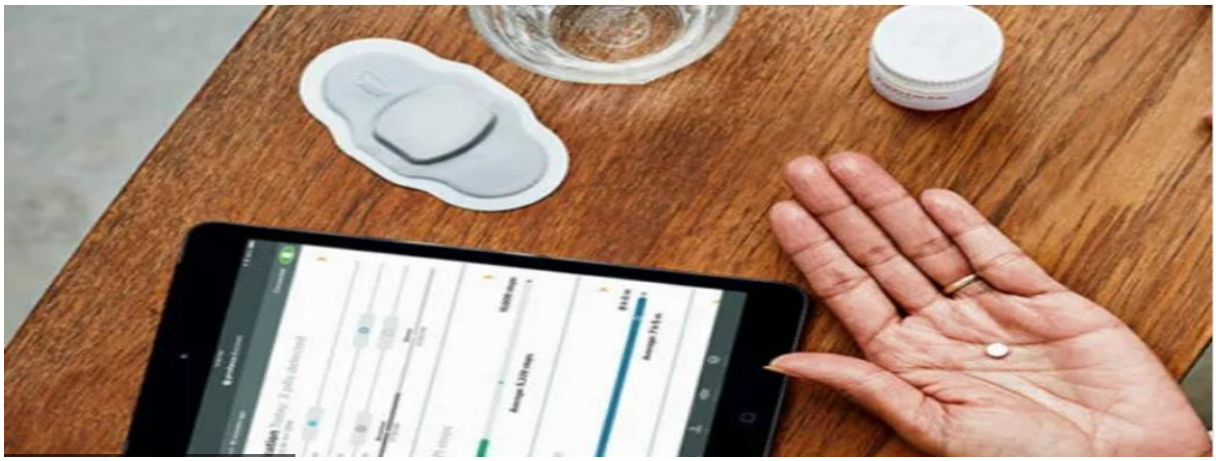

Figure I.17: le médicament Porteuse Digital Health [23].

VI.4 L’agriculture

L'agriculture intelligente est une stratégie de développement agricole durable qui vise à améliorer la production tout en préservant les ressources naturelles et en réduisant les émissions de gaz à effet de serre [21]. Les technologies de l'IoT, comme les réseaux de capteurs interconnectés, peuvent être très utiles dans le domaine de l'agriculture et de l'environnement en permettant une surveillance en temps réel de différentes variables environnementales telles que l'humidité du sol, la qualité de l'eau et de l'air, etc. Cela peut aider à prévenir la pollution et à améliorer la qualité de l'environnement pour les communautés locales[6].

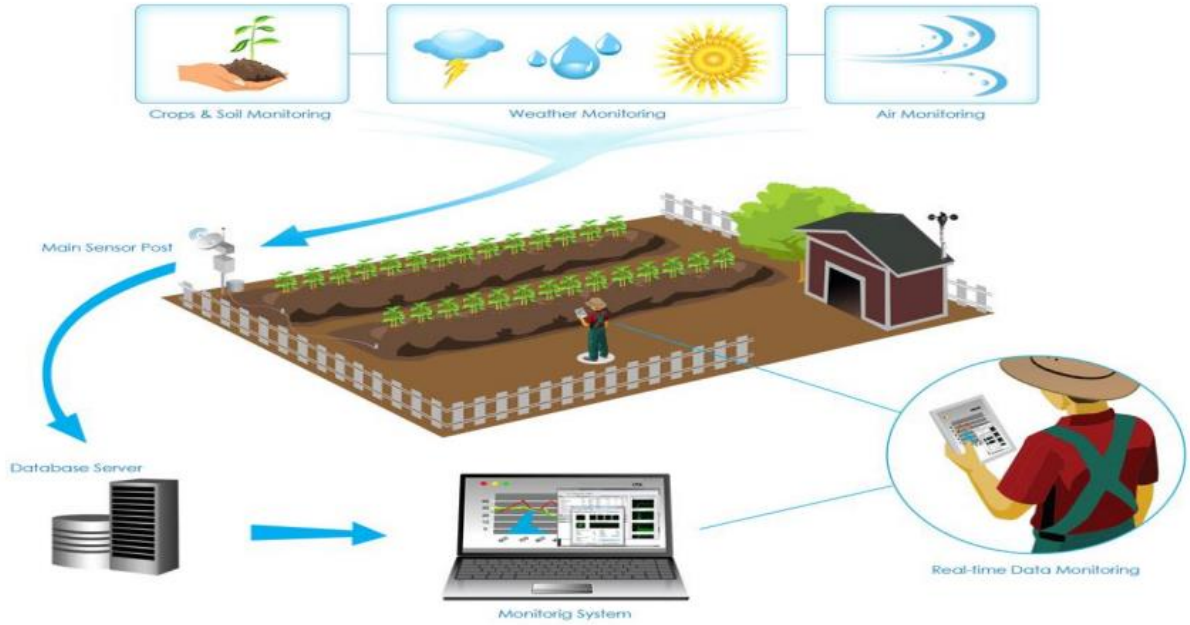

Figure I.18 : L’agriculture intelligente basée sur l’IoT [2].

VI.5 Les villes intelligentes (Smart City)

Les villes intelligentes ou smart cities sont de plus en plus nombreuses dans les pays qui connaissent une avancée technologique. Ces villes sont conçues pour utiliser les technologies de l'information et de la communication pour améliorer la qualité de vie et la durabilité environnementale. L'internet des objets peut offrir des avantages en matière de sécurité pour la gestion du trafic dans les zones à forte affluence. Les capteurs IoT peuvent collecter des données en temps réel sur le trafic routier pour aider les autorités à prendre des décisions éclairées en matière de gestion du trafic et améliorer l'efficacité de la circulation [2].

Figure I.19 : villes intelligentes (Smart City) [20]

VI.6 L'industrie

La révolution des industries et de la fabrication est devenue l'une des plus technologies développées de nos jours, la croissance de l'évolution de l'industrie a pris de nombreuses générations dont la dernière est l'industrie intelligente ou Industrie 4.0, qui est basée sur les systèmes de chiffrement physiques connectés à Internet [25].

Cette nouvelle génération d'industrie vise à créer des usines intelligentes et connectées, capables de collecter et d'analyser des données en temps réel pour optimiser les processus de production de manière autonome et produire des produits personnalisés en masse. L'Industrie 4.0 présente de nombreux avantages tels que l'optimisation des processus, la réduction des coûts, l'amélioration de la qualité et une production plus durable [25].

VI.7 Smart Grid

L'IoT est un élément clé de la mise en place de réseaux électriques intelligents (Smart Grid), qui permettent une gestion plus efficace et plus durable de la production, de la distribution et de la consommation d'énergie. ERDF (Électricité Réseau Distribution France) et d'autres acteurs du secteur sont très actifs dans le développement de cette technologie en France, pour répondre aux besoins croissants en matière de gestion de l'énergie et de protection de l'environnements [25].

Figure I.20 : Représentation d'une Smart Grid [26].

VII. Avantages et inconvénients de l'IoT

Comme toutes les technologies, l'Internet des Objets présente des avantages et des inconvénients.

VIII.1 Avantages

L'IoT présente de nombreux avantages dans différents domaines de la vie. Voici une liste de certains avantages :

-Communication

Grâce à la connectivité IoT, les appareils physiques peuvent rester connectés en permanence, ce qui offre une transparence totale qui permet de collecter, d'analyser et de partager des données en temps réel pour améliorer l'efficacité, la qualité et la sécurité des processus et des produits.

-Automatisation et contrôle

L'automatisation et le contrôle dans les IoT peuvent permettre une production plus rapide sans intervention humaine directe. Les machines peuvent surveiller et collecter des données en temps réel sur l'environnement, les processus et les machines elles-mêmes, ce qui peut aider à détecter les problèmes plus rapidement et à réduire les temps d'arrêt [24].

-La surveillance permet d'économiser de l'argent et du temps

L'IoT surveille différents aspects de notre vie quotidienne grâce à des capteurs intelligents, ce qui permet d'économiser de l'argent et du temps. Par exemple, la surveillance des niveaux d'inventaire dans les entreprises permet de maintenir des stocks optimaux et de minimiser les coûts liés à la gestion des stocks [24].

-Meilleure qualité de vie

Les applications basées sur l'IoT peuvent certainement améliorer la qualité de vie en offrant des solutions innovantes pour le confort et la gestion de notre vie quotidienne [24].

-Un meilleur environnement

L'Internet des objets offre un potentiel énorme pour créer un environnement plus intelligent, plus vert et plus durable. En utilisant la connectivité des objets, des capteurs et des dispositifs, l'IoT peut aider à économiser les ressources naturelles et les arbres de différentes manières [24].

VIII.2 Inconvénients

Alors que l'Internet des Objets contribuera à faciliter la vie humaine et à éliminer les problèmes majeurs, mais aussi il a plusieurs inconvénients nous citons :

-Les systèmes et les services IoT peuvent être vulnérables aux cyberattaques, ce qui peut causer des dommages matériels ou mettre en danger la vie des utilisateurs.

-D'autre part, l'Internet des objets peut avoir un impact sur l'emploi dans certains secteurs où les tâches peuvent être automatisées ou remplies par des machines, il est bien connu que les projets d'Internet des Objets et d'Intelligence Artificielle sont venus faciliter la vie, réduire les coûts et ignorer l'emploi des gens.

- En plus, l'utilisation excessive d'Internet et de la technologie peut entraîner une dépendance et une paresse accrues, ce qui peut causer des problèmes de santé tels que l'obésité.

- Les négatifs ne s'arrêtent pas là, mais aussi la dépendance à Internet peut provoquer des problèmes psychologiques chez certaines personnes. Certaines études ont montré que l'utilisation excessive d'Internet peut entraîner des problèmes tels que l'anxiété, la dépression, la solitude, la dépendance et l'isolement social [26].

VIII. Conclusion

En conclusion, les IoT ont un impact significatif sur notre vie quotidienne et sur la façon dont nous interagissons avec les technologies modernes. Les appareils connectés offrent de nombreuses fonctionnalités qui améliorent notre confort et notre sécurité, mais leur utilisation peut également présenter des défis en termes de sécurité et de vie privée. Il est essentiel de comprendre les avantages et les risques associés aux IoT et de prendre des mesures pour protéger nos données et nos appareils. Le chapitre suivant englobe le terme de la cybersécurité qui est un enjeu crucial pour les IoT. Les appareils connectés peuvent être vulnérables à diverses menaces telles que les attaques par déni de service, les malwares ou les attaques par phishing, etc. La détection précoce des menaces et la mise en place de mesures de sécurité solides sont essentielles pour protéger nos données et nos appareils contre les cyberattaques.

Chapitre II

La cybersécurité et la détection des menaces dans les IoT

Sommaire

I. Introduction

L'internet des Objets (IdO) est une technologie en constante expansion, qui permet à de nombreux appareils de se connecter et de communiquer entre eux via Internet. Cependant, cette connectivité accrue présente également de nouveaux défis en matière de cybersécurité, car les appareils IoT peuvent être vulnérables aux cyberattaques et aux menaces de sécurité.

Avec l'augmentation du nombre de dispositifs connectés, les risques de cyberattaques ont également augmenté. La cybersécurité dans le domaine des IoT (Internet of Things) est donc d'une importance capitale pour protéger les données personnelles, les systèmes critiques et les infrastructures des organisations. La détection des menaces est un élément essentiel de cette cybersécurité, car elle permet de surveiller en temps réel les dispositifs IoT et de détecter les activités malveillantes.

Dans ce chapitre, nous allons examiner de plus près les enjeux de la cybersécurité dans le domaine des IoT, et comment la détection des menaces peut aider à protéger les appareils connectés et les données associées.

II. La cybersécurité

II.1 Définition

La cybersécurité est un concept global qui englobe toutes les mesures prises pour protéger les systèmes informatiques, les réseaux, les dispositifs et les données contre les attaques, les intrusions et les pertes. Cela comprend des aspects techniques tels que l'utilisation de logiciels de sécurité, de pare-feu, de chiffrement de données, etc., ainsi que des mesures organisationnelles telles que la sensibilisation à la sécurité. L'Union International des Télécommunications (UIT) nous propose une définition précise :

On entend par la cybersécurité l'ensemble des moyens, concepts, directives, technologies, garanties et bonnes pratiques visant à protéger les actifs des organisations et des utilisateurs dans le cyber environnement. Les actifs en question incluent les dispositifs connectés, les applications, le personnel, les infrastructures, les services, les systèmes de télécommunication, ainsi que les informations stockées et transmises. La cybersécurité a pour objectif de préserver les propriétés de sécurité des organisations et des utilisateurs en les protégeant contre les risques qui affectent la sécurité dans le cyber environnement, tout en employant des méthodes de gestion des risques, des formations et des actions pour y parvenir [27].

II.2 Objectif de la cybersécurité

L'objectif de la cybersécurité est de protéger les systèmes informatiques, les réseaux, les dispositifs électroniques, les données et les informations confidentielles contre les attaques

malveillantes, les piratages, les virus et les autres menaces potentielles. La cybersécurité vise également à garantir :

-La confidentialité : fait référence à la protection des informations contre la divulgation à des parties non autorisées. Elle est essentielle pour protéger la vie privée et les droits des individus, ainsi que pour préserver les secrets commerciaux et les informations confidentielles des organisations [28].

-L'intégrité : est une des composantes essentielles de la protection des données. Elle fait référence à la garantie que les données ne sont pas altérées, modifiées ou détruites de manière malveillante ou non autorisée. Les mécanismes de contrôle d'intégrité visent à assurer que les données restent fiables et cohérentes, et qu'elles ne sont pas altérées par des tiers [28].

-La disponibilité : le service de disponibilité veille à ce que l'information puisse être utilisable, elle permet aux utilisateurs d'avoir accès aux systèmes, aux informations et aux applications qui traitent ces informations. La disponibilité couvre aussi les systèmes de communication qui transmettent les informations entre sites ou entre systèmes. En temps de disponibilité, c'est à l'information et aux services électroniques que nous pensons le plus souvent. Cependant, la disponibilité des fichiers papier peut aussi être assurée [29].

-La responsabilité : le service de responsabilité est souvent négligé lorsque nous évoquons la sécurité. La principale raison est que le service de responsabilité seul ne protège pas contre les attaques. Il doit être employé en association avec d'autre services afin de rendre ceux-ci plus efficaces. La responsabilité est la partie la plus déplaisante de la sécurité : elle apporte des difficultés supplémentaires sans pour autant ajouter de la valeur. En outre, elle augmente le cout et réduit la rentabilité des systèmes. Cependant, sans elle, les mécanismes de confidentialité et d'intégrité échoueraient [29].

II.3 La carte de la cybersécurité (cyber security mind map)

Elle représente les différents domaines de la cybersécurité, avec leurs sous-catégories et leurs interconnexions. Cela peut aider les professionnels de la cybersécurité à mieux comprendre les différents aspects de leur domaine et à planifier leurs stratégies de sécurité en conséquence [30]. Prenons un exemple populaire créé par Henry Jiang, le créateur de la carte des domaines de cybersécurité v3.1, considérée comme la plus neutre en termes de fournisseurs. Son modèle répertorie 11 domaines de cybersécurité [31].

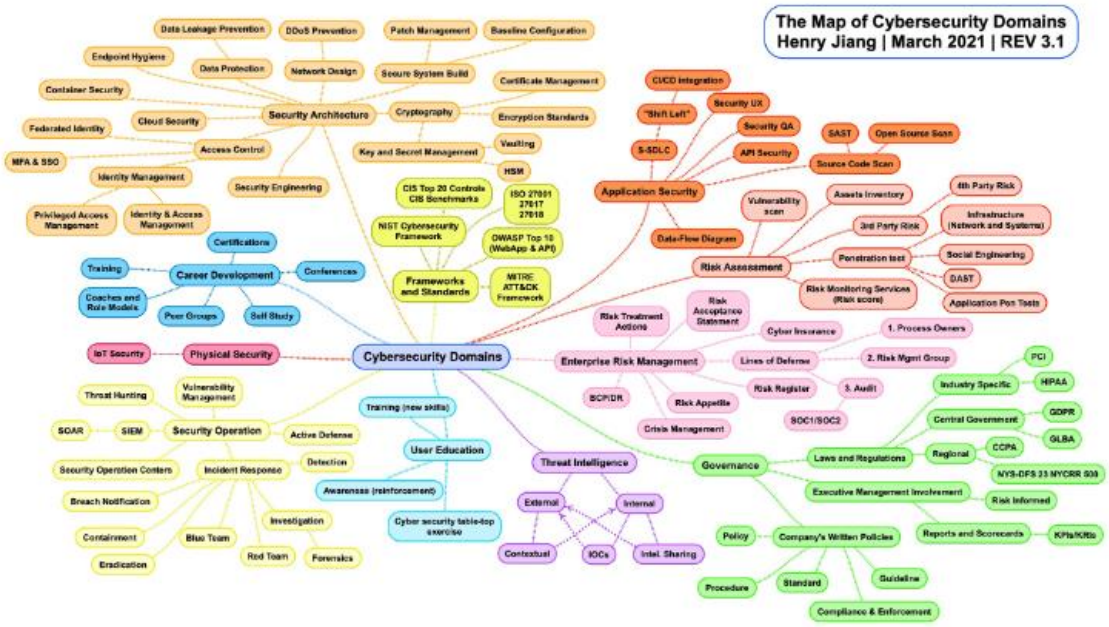

Figure II.1 : la carte des domaines de cybersécurité v3.1 [32].

1. **Cadres et normes (Framework & Standards) :** Les Framework revêtent une importance capitale car ils offrent un modèle standardisé que tous peuvent adopter. Ils garantissent que les équipes de sécurité suivent une voie organisée pour atteindre les objectifs de sécurité [31].
2. **Sécurité des applications (Application Security) :** Andreas Happe affirme que la sécurité des applications "comprend toutes les activités qui (idéalement) instaurent un cycle de développement de logiciels sécurisé au sein des équipes de développement. Son but ultime est d'améliorer les pratiques de sécurité et, de cette manière, de détecter, corriger et de préférence éviter les problèmes de sécurité dans les applications [31].
3. **L'évaluation des risques (Risk assessment) :** L'analyse des risques est une étape cruciale pour une entreprise, qui permet d'identifier les dangers et les vulnérabilités qui pourraient nuire à l'organisation et à ses actifs. Cette analyse implique d'évaluer la probabilité et les conséquences des menaces repérées, afin de déterminer les dispositifs de sécurité adéquats pour réduire les impacts d'un éventuel incident de sécurité [31].
4. **La gestion des risques d'entreprise (Enterprise Risk Management) :** ERM est une activité essentielle pour toute organisation qui vise à évaluer, surveiller et gérer les risques qui peuvent menacer ses activités. Contrairement à une simple prestation de service ou un produit, l'ERM est un processus continu qui doit faire partie intégrante de la culture de l'entreprise pour être efficace. Son objectif est de réduire les risques liés à la continuité des activités, à la réputation et à la valeur de la marque [31].

5. **La gouvernance (Governance) :** est un processus crucial qui consiste à prendre des décisions et à mettre en place des politiques de sécurité. Elle vise à garantir que les décisions appropriées sont prises au bon moment et que les politiques adéquates sont mises en place pour réduire les risques de manière efficace et économique, tout en respectant les droits à la vie privée et les obligations de conformité [31].
6. **L'intelligence des menaces (Threat Intelligence) :** est une méthode qui permet de rassembler et d'analyser des informations sur les menaces numériques. En utilisant cette approche combinée à d'autres outils de cybersécurité, il est possible de se prémunir contre les attaques informatiques. L'objectif est de collecter et de traiter les données liées aux menaces afin de détecter les failles potentielles dans le système et de prévenir les attaques [31].
7. **Formations des utilisateurs (user education) :** la formation des utilisateurs est un élément essentiel des différents domaines de la cybersécurité. Elle fait partie intégrante du cycle de sécurité, car elle vise à sensibiliser les utilisateurs sur l'importance de la sécurité informatique [31].
8. **La sécurité opérationnelle (Security Operations) :** est l'équipe qui assure la continuité des systèmes tout en garantissant leur sécurité [31].
9. **La sécurité physique (Physical Security) :** regroupe un ensemble de mesures visant à prévenir tout accès non autorisé aux personnes ou aux biens. Cette catégorie englobe toutes les stratégies qui permettent de protéger physiquement les éléments vitaux d'une entreprise ou d'une organisation [31].
10. **Le développement de carrière (Career Development) :** a été intégré en tant que domaine de la cybersécurité. Cela est dû à la forte demande de professionnels qualifiés en cybersécurité qui disposent d'une éducation, de compétences et d'une expérience de qualité [31].
11. **L'architecture de sécurité (Security architecture) :** est un domaine assez vaste qui concerne la conception de la politique et de la stratégie de sécurité d'une organisation. Elle englobe un ensemble de catégories liées à la sécurité qui doivent être prises en compte lors de la conception de l'architecture d'une application [31].

III. La différence entre vulnérabilité – menace – risque -attaque

III.1 Vulnérabilité

La vulnérabilité s'applique à une voie potentielle pour une attaque. Les vulnérabilités existent également dans les systèmes et les réseaux (un système vulnérable à une attaque technique) ou dans les procédures administratives (un environnement vulnérable à une attaque non technique

ou type ingénierie sociale). Une vulnérabilité est caractérisée par la difficulté de son exploitation et par le niveau de compétence technique requis pour l'exploiter.

Le résultat de cette exploitation doit aussi être pris en compte. Par exemple, une vulnérabilité facile à exploiter (en raison de l'existence d'un scénario pour exécuter l'attaque) et qui permet à l'attaquant d'obtenir le contrôle complet d'un système est une vulnérabilité de niveau majeur. En revanche, une vulnérabilité qui exigerait que l'attaquant investisse des moyens humains importants et un équipement considérable, et qui lui permettrait seulement d'obtenir l'accès à des informations publiques, serait considérée comme une vulnérabilité de niveau.

Les systèmes et les réseaux ne sont pas les seuls à être vulnérables. La sécurité physique d'un site, la sécurité relative aux employés et la sécurité de l'information en circulation doivent également être évaluées [29].

III.2 Menace

Une menace est une action ou un événement qui pourrait violer la sécurité d'un système d'informations. La menace est composée de trois éléments :

-Les cibles. : L'objet qui pourrait être attaqué.

-Les agents : Les personnes ou les organisations à l'origine de la menace.

-Les événements. : Le type d'action qui crée la menace [29].

III.3 Risque

Le risque est la probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée du système [15]. Le risque est le concept sous-jacent de ce que nous appelons la "sécurité" et la perte potentielle de ce qui exige une protection. S'il n'y a aucun risque, il n'y a aucun besoin de sécurité [29].

III.4 Attaque

Une attaque est une action spécifique entreprise par une menace dans le but de compromettre la sécurité d'un système. Il s'agit d'une mise en œuvre concrète d'une menace. Les attaques sont souvent planifiées et exécutées dans le but d'obtenir un accès non autorisé, de voler des informations sensibles, de perturber les services ou d'endommager le système [33].

IV. Attaques IoT à différentes couches

Dans cette section, nous explorerons les attaques IoT a différentes couches qui menacent la vie privée [34] :

IV.1 Couche physique (Physical Layer)

La couche physique comprend un éventail de technologies de capteurs, notamment Bluetooth, GPS (Global Positioning System) et Zigbee, qui ne bénéficient pas d'une protection adéquate contre diverses formes d'attaques. Ces attaques ciblent spécifiquement les composants matériels du réseau IoT et nécessitent que l'attaquant soit en proximité des systèmes IoT. Le tableau ci-dessous offre une brève analyse des attaques ciblant la couche physique [34].

Nom de l'attaque	Effet
Nœud Trempé	Altérer les informations sensibles en endommageant les capteurs
Interface RF sur RFID (Radio Frenquency IDentification)	Arrêter la communication par distorsion des signaux
Ingénierie sociale	Fuite d'informations privées
Attaque de privation de sommeil	Arrêt des nœuds
Usurpation (Spoofing)	Capture d'informations
Injection de code malveillant (Malicious code injection)	La prise de contrôle
Ecoute clandestine (Eavesdropping)	Vol de données.

Tableau II.1 : Analyse de la couche physique [34]

-Nœud Trempé (Node Tempering) : L'attaque de « Nœud trempé » vise à compromettre l'intégrité, la disponibilité et la confidentialité du système de capteurs, l'attaquant peut endommager physiquement les nœuds de capteurs en les détruisant, en les désactivant ou en les perturbant de manière à les rendre inopérant [34].

-Interface RF sur RFID (RF Interference on RFID) : il s'agit plutôt d'une attaque visant à perturber ou à manipuler les communications sans fil entre les étiquettes RFID et les lecteurs RFID en utilisant des interférences RF. Cette attaque ne bloque pas nécessairement complètement le service, mais elle peut entrainer des dysfonctionnements dans les communications RFID, des erreurs de lecture ou des perturbations [34].

-Ingénierie sociale : L'attaquant manipule les utilisateurs d'un système IoT, pour extraire des informations privées ou pour effectuer certaines actions qui serviraient ses objectifs. Ce type d'attaque est classé dans la catégorie des attaques physiques car l'attaquant doit interagir physiquement avec les utilisateurs du réseau IoT pour atteindre ses objectifs [34].

-Attaque de privation de sommeil (Sleep Deprivation Attack) : Dans un réseau de capteurs sans fil, les appareils fonctionnent sur des batteries et pour économiser l'énergie de la batterie,

ces appareils passent la plupart du temps en mode sommeil. L'attaque de privation de sommeil force ces appareils à rester éveillés en permanence, ce qui épuise rapidement leur batterie et peut les rendre inutilisables [34].

-Usurpation (Spoofing) : Lors de l'usurpation d'identité, l'adversaire diffuse de fausses informations sur le système RFID et les suppose comme originales et fait en sorte que les données proviennent de la source d'origine. Par conséquent, l'attaquant capture des informations et obtient un accès complet au réseau [34].

- Injection de code malveillant (Malicious code injection) : C'est un type d'attaque grave où un assaillant prend le contrôle d'un point du réseau afin d'y introduire un code nuisible. Les conséquences peuvent être très dommageables, allant de la perturbation complète du réseau à la prise de contrôle totale par l'attaquant dans les scénarios les plus critiques [34].

-Ecoute clandestine (Eavesdropping): Dans l'écoute clandestine, un assaillant peut aisément acquérir des informations confidentielles telles qu'un mot de passe ou d'autres données en transit entre des étiquettes ou des utilisateurs. Cette vulnérabilité découle des propriétés sans fil inhérentes à la RFID [34].

IV.2 Attaques de la couche réseau (Network Layer Attacks)

Dans une attaque réseau visant un système IoT, l'attaquant se concentre sur le réseau du système IoT, et il n'est pas nécessaire qu'il soit physiquement proche du réseau. Le tableau 2 analyse brièvement les attaques de la couche réseau [34].

Nom de l'attaque	Effet
Attaque de gouffre	Fuite de données des nœuds.
L'homme au milieu de l'attaque	Contrôle les échanges réseau entre deux systèmes
Botnet	Prendre le contrôle d'un grand nombre d'ordinateurs
DoS (Denial of Service)	Rendre un serveur indisponible
DDoS (Distributed Denial of Service)	Perturber ou paralyser totalement le fonctionnement d'un serveur
Attaque de trou de ver (Wormhole attack)	Reroutage de données.
Clonage RFID (RFID Cloning)	Clonage d'étiquettes.

Tableau II.2 : Analyse de la couche réseau [34**].**

-Attaque de gouffre (Sinkhole Attack) : Dans une attaque gouffre, un adversaire compromet un nœud à l'intérieur du réseau et effectue l'attaque en utilisant ce nœud. Le nœud compromis envoie les fausses informations de routage à ses nœuds voisins indiquant qu'il a le chemin de distance minimum vers la station de base, puis attire le trafic. Il peut alors modifier les données et également supprimer les paquets. Ce travail donne la technique simple pour identifier les nœuds dolines. Dans la technique proposée, lorsqu'un nœud envoie un paquet à son nœud voisin, il crée l'entrée des distances de saut et de l'ID dans sa base de données. Il calcule ensuite le nombre de sauts moyen à l'exception du nombre de sauts minimum et compare la valeur moyenne et la valeur minimale. Si cette valeur minimale est trop petite par rapport au nombre moyen de sauts, elle est vulnérable aux attaques de gouffre [34].

-L'homme au milieu de l'attaque (Man In the Middle Attack) : cette attaque consiste à intercepter les communications entre deux systèmes en les faisant passer par un troisième système contrôlé par un pirate. Le pirate peut manipuler les données en temps réel tout en cachant la véritable identité des parties en communication. Pour réussir cette attaque, le pirate doit soit être physiquement sur le chemin des données du réseau, soit modifier le chemin du réseau pour inclure sa propre machine en tant que relais [35].

-Botnet (réseaux de zombies) : les attaquants prennent le contrôle d'ordinateurs connectés à internet, appelés botnets, soit par des attaques directes, soit indirectement, ces ordinateurs compromis sont utilisés par les pirates pour distribuer et amplifier leurs attaques, telles que les attaques par déni de services distribué (DDoS) [36].

-Attaque de trou de ver (Wormhole attack) : Dans une attaque de type trou de ver, il est possible de déplacer des données depuis leur emplacement initial dans le réseau vers un autre endroit. Ce déplacement s'effectue à travers un canal de données où il existe une faible latence [34].

-Clonage RFID (RFID Cloning) : Un assaillant duplique une étiquette RFID en reproduisant les informations de l'étiquette RFID de la cible sur une autre étiquette RFID. Bien que ces deux étiquettes RFID contiennent des données identiques, cette technique ne recopie pas l'identifiant original de la RFID, ce qui permet de différencier l'authentique du compromis, contrairement à ce qui se produit lors d'une attaque d'usurpation RFID [34].

-Déni de service (Denial of Service) : Le déni de service est une attaque qui vise à rendre un service, un système ou un réseau indisponible. Cette attaque s'appuie généralement sur une faiblesse d'implémentation, ou bogue, ou sur une faiblesse de protocole.

Les premières attaques par déni de service sont apparues entre 1998 et l'an 2000. Elles visaient de grands sites Internet (Yahoo!, Ebay, eTrade, etc.). Le site Yahoo!, premier annuaire de recherche au monde, a été attaqué en février 2000 et a été inondé (flood) pendant plus de trois heures sous un gigaoctet de données provenant d'au moins cinquante points réseau différents [35].

-Déni de service distribué (Distributed Denial of Service) : L'attaque par déni de service distribué, ou DDoS, vise à perturber ou paralyser totalement le fonctionnement d'un serveur informatique en le bombardant à outrance de requêtes erronées [37].

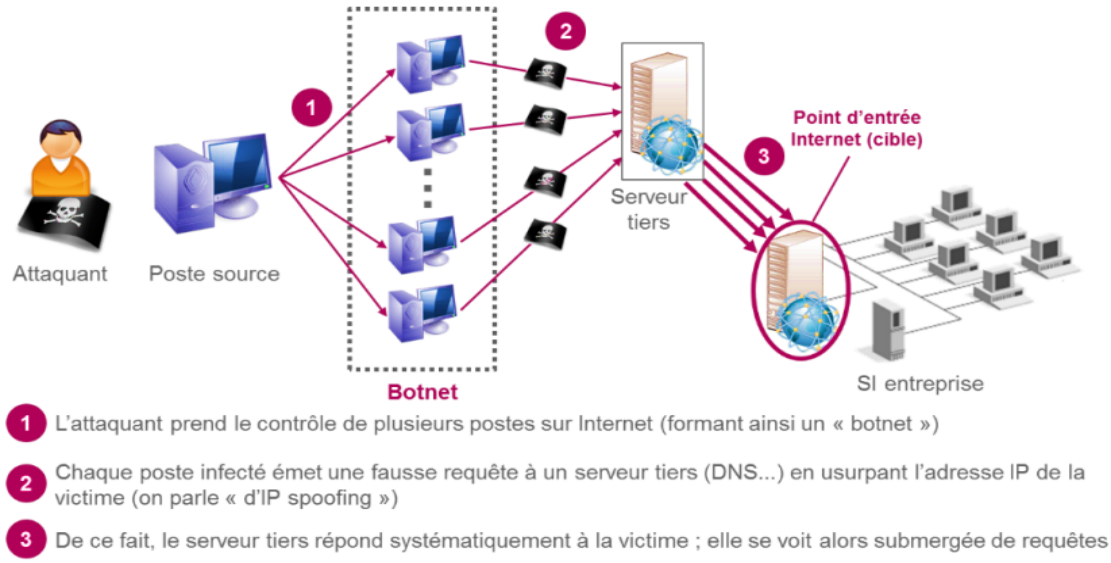

Figure II.2 : Exemple d'attaque DDoS (Distributed Denial of Service) [37].

IV.3 Attaques des couches de traitement (Processing Layer Attacks)

La couche de traitement se compose de différents types de technologies telles que le stockage et le traitement des données. Les menaces de sécurité dans cette couche qui rendent le réseau vulnérable sont analysées dans le tableau II.3 [34].

Nom de l'attaque	**Effet**
Attaque par menaces de virtualisation	Endommagement de la ressource
Attaque par ressources partagées	Un utilisateur non autorisé peut contrôler les ressources
Attaque par sécurité des applications	Le vol de données
Attaque par sécurité des données	Fuite de données confidentielles sur le cloud

Tableau II.3 : Analyse de la couche de traitement [34].

-Attaque par menaces de virtualisation (Virtualization threats attack) : Dans cette couche, la virtualisation est très peu sûre face à de nombreux types d'attaques, Les attaques visant les

vulnérabilités de la virtualisation peuvent permettre à un attaquant de compromettre les environnements virtualisés dans le cloud, potentiellement entraînant des interruptions de service ou des dommages aux ressources virtuelles [34].

-Attaque par ressources partagées (Shared Resources attack) : est un scénario de menace courant dans les environnements de virtualisation, y compris les réseaux IoT. Cette attaque se produit lorsque des ressources sont partagées entre différentes machines virtuelles (VMs) ou dispositifs IoT au sein d'un même système ou réseau, et qu'un attaquant parvient à exploiter ces ressources partagées pour compromettre la sécurité du système [34].

-Attaque par sécurité des applications (Application security attack) : Dans le contexte de la sécurité des applications, le modèle de fourniture de logiciels en tant que service (SAAS, Software As A Service) offre un accès via Internet à des logiciels et des données stockés dans le cloud. Dans le système IoT, les attaquants peuvent facilement voler des données et mener des activités malveillantes via Internet, créant des problèmes de sécurité distincts des menaces réseau habituelles. L'OWASP (Open Web Application Security Project) a identifié de nombreuses vulnérabilités et problèmes de sécurité associés aux services Web SAAS [34].

-Attaque par sécurité des données (Data security) : Cette attaque vise à exfiltrer des données confidentielles stockées dans le cloud. Les attaquants cherchent à accéder à des informations sensibles, telles que des données personnelles ou commerciales, et à les divulguer ou les exploiter à des fins malveillantes [34].

IV.4 Attaques de la couche application (Software Layer Attacks)

Les attaques logicielles sont les principaux défis qui se posent dans le système IoT. Les attaques logicielles sont utilisées pour endommager les ressources du système en utilisant des virus et des attaques nuisibles tels que des chevaux de Troie, des vers, des logiciels espions, etc. qui peuvent violer les données confidentielles, altérer les données, endommager les appareils IoT et accéder à des informations utiles [34].

-Une attaque par phishing (Phishing Attack) : L'attaquant obtient les informations privées telles que le nom d'utilisateur, les mots de passe par usurpation d'e-mail et en utilisant de faux sites Web [34].

-Virus, vers, cheval de Troie, spyware et aware (Virus, Worms, Trojan horse, Spyware and Aware) : Un adversaire peut endommager le système en utilisant un code malveillant. Ces codes se propagent par le biais de pièces jointes à des e-mails, en téléchargeant des fichiers sur Internet. Le ver a la capacité de se répliquer sans aucune action humaine. Nous pouvons utiliser

un détecteur de vers, un antivirus, des pares-feux, un système de détection d'intrusion pour détecter le virus [34].

- **Malware :** C'est un programme développé ou une partie d'un code conçu pour effectuer des activités malveillantes tels que les virus, les vers, les chevaux de Troie, etc. Certaines de ses caractéristiques peuvent inclure la propagation et la réplication [36].

V. Détection des menaces

La détection de menaces est une tâche complexe qui nécessite une grande expertise et une maturité en matière de cybersécurité. Les attaquants évoluent constamment et développent des techniques toujours plus sophistiquées pour s'infiltrer dans les systèmes informatiques. Par conséquent, il est essentiel de disposer d'une approche proactive de la sécurité, qui comprend une surveillance continue et la détection précoce des menaces potentielles [38].

V.1 Méthode de détection des menaces dans les IoT

-L'analyse des données en temps réel : Utilisation de techniques d'apprentissage automatique (machine learning) pour surveiller en continu les données générées par les appareils IoT. Les modèles de machine learning peuvent être formés pour détecter des schémas de comportement anormaux ou malveillants [38]

- La gestion des vulnérabilités : Mener des évaluations régulières de la sécurité des appareils IoT pour identifier les vulnérabilités. Les correctifs doivent être appliqués dès que possible pour minimiser les risques [38].

- La segmentation du réseau : Diviser le réseau IoT en segments distincts pour isoler les dispositifs critiques des dispositifs moins critiques. Cela limite la propagation des attaques [38].

-L'authentification forte : Exiger une authentification robuste, comme l'utilisation de certificats numériques ou de clés d'authentification pour chaque appareil IoT, afin de garantir que seuls les appareils autorisés peuvent se connecter au réseau [38].

-La gestion centralisée : Utilisation d'une plateforme centralisée de gestion de la sécurité pour surveiller et gérer l'ensemble de l'écosystème IoT [38].

-La mise à jour à distance : Capacité à mettre à jour les dispositifs IoT à distance pour corriger les vulnérabilités connues et les failles de sécurité [38].

-La sécurité matérielle : L'intégration de mesures de sécurité au niveau matériel, telles que des puces sécurisées (secure elements) et des mécanismes de protection de l'intégrité du firmware [38].

-La sensibilisation à la sécurité : Former les utilisateurs et les administrateurs sur les meilleures pratiques en matière de sécurité IoT pour éviter des erreurs humaines qui pourraient compromettre la sécurité [38].

-La détection d'intrusion : Dans le contexte de la détection d'intrusion dans l'Internet des objets (IoT), la mise en place de systèmes de détection d'intrusion (IDS) revêt une importance cruciale. Ces IDS spécifiques à l'IoT sont conçus pour surveiller en temps réel le trafic généré par les dispositifs connectés et pour repérer les activités suspectes ou malveillantes. Les IDS IoT peuvent adopter deux approches principales : celle basée sur des règles et celle utilisant des méthodes d'analyse comportementale [38].

Voici quelques exemples de systèmes de détection d'intrusion open source couramment utilisés dans le domaine de l'IoT :

- **Bro IDS (Zeek) :** Bro IDS, désormais connu sous le nom de Zeek, est un système de détection d'intrusion open source qui se concentre sur l'analyse du trafic réseau en temps réel. Il est capable de surveiller les activités réseau, de générer des journaux détaillés et de signaler des comportements suspects.
- **Suricata :** Suricata est un système de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) open source de haute performance. Il est conçu pour surveiller le trafic réseau en temps réel, il est largement utilisé dans les environnements de sécurité réseau pour détecter et prévenir les intrusions, les attaques DDoS, les tentatives d'exploitation de vulnérabilités et d'autres menaces. Il peut être déployé sur des pare-feu, des routeurs, des passerelles et d'autres dispositifs réseau pour renforcer la sécurité du réseau.
- **Wazuh :** Est une plateforme de détection de menaces open source qui intègre des fonctionnalités d'IDS. Il offre une surveillance en temps réel, l'analyse des journaux et des alertes personnalisables pour les environnements IoT.
- **Snort :** Est un système de détection d'intrusion open source largement reconnu. Snort fonctionne en surveillant le trafic réseau à la recherche de modèles de comportement anormaux, en comparant le trafic à des signatures de menaces connues et en générant des alertes en cas de détection [38].

VI. Conclusion

En conclusion, la cybersécurité et la détection des risques et des menaces sont des aspects critiques dans le domaine de l'IoT. Comme nous l'avons vu dans ce chapitre, les dispositifs IoT sont de plus en plus ciblés par les attaquants, ce qui peut entraîner des conséquences potentiellement graves pour les utilisateurs.

Il est essentiel de mettre en place des mesures de sécurité appropriées pour protéger les dispositifs IoT et les réseaux qui les connectent, et de surveiller en permanence les activités suspectes pour détecter rapidement les attaques et y réagir, il est important donc de prendre la cybersécurité au sérieux dans le domaine de l'IoT pour protéger la vie privée, la sécurité et la confiance des utilisateurs dans les technologies intelligentes.

Dans le prochain chapitre, nous allons présenter notre solution de détection des menaces basée sur le système de détection Snort, en mettant en évidence son importance dans le contexte de l'Internet des Objets (IdO). Cette solution joue un rôle essentiel dans la sécurisation des dispositifs IoT et des réseaux associés, en garantissant une surveillance constante des activités suspectes et une réaction rapide aux menaces émergentes.

CHAPITRE III

Évaluation de la Performance de Snort pour la détection d'intrusions dans les Réseaux IoT

Sommaire

I. Introduction

Dans ce chapitre, nous vous guiderons à travers les étapes cruciales nécessaires à la configuration et à l'évaluation de notre système de détection d'attaques. Notre parcours commence par la préparation minutieuse de notre Raspberry Pi 4 pour qu'il puisse fonctionner comme un système de détection d'attaques. Cela englobe des étapes telles que l'installation du système d'exploitation, la configuration du matériel essentiel et l'établissement de la connectivité réseau.

Nous poursuivrons en plongeant dans l'univers de Snort, un outil de détection d'intrusion puissant. Au cours de cette phase, nous vous montrerons comment installer et configurer Snort, en mettant l'accent sur la création de règles personnalisées adaptées à notre environnement spécifique.

En parallèle, nous explorerons les fonctionnalités d'hping3, un outil essentiel pour simuler divers types d'attaques. Cette simulation nous permettra de tester l'efficacité de notre système de détection, nous passerons ensuite à la phase d'expérimentation. Nous élaborerons et exécuterons des tests en conditions réelles, en surveillant Snort en temps réel pour détecter les attaques que nous aurons simulées.

Ce chapitre marque un tournant décisif dans notre projet innovant, nous rapprochant de notre objectif final de créer un système de détection d'attaques robuste et efficace à l'aide du Raspberry Pi 4, de Snort et de hping3.

II. Partie matérielle (Hardware)

II.1 Raspberry Pi

II.1.1 Qu'est-ce que le Raspberry Pi ?

Le Raspberry Pi est un nano-ordinateur monocarte révolutionnaire, abordable et incroyablement polyvalent, qui a été conçu par la Fondation Raspberry Pi. Depuis son introduction en 2012, la Raspberry Pi a captivé l'imagination des passionnés de l'informatique, des éducateurs et des bricoleurs du monde entier. Elle se distingue par sa petite taille, son coût modique et sa puissance de calcul surprenante, ce qui en fait un outil idéal pour une variété d'applications allant de l'éducation à la domotique en passant par la robotique [39].

II.1.2 Le Raspberry Pi 4 Model B 8GB :

Le Raspberry Pi 4 Model B 8GB est la dernière itération de cette série emblématique. Elle représente un saut significatif en termes de performances et de capacités par rapport à ses prédécesseurs. Voici un aperçu de cette version particulière :

Caractéristiques Clés :

- ✓ Processeur Puissant : Elle est alimentée par un processeur quad-core ARM Cortex-A72, offrant des performances de calcul remarquables pour sa taille et son prix.
- ✓ 8 Go de RAM LPDDR4 : Cette mise à niveau majeure de la mémoire vive permet d'exécuter des applications plus gourmandes en mémoire et d'améliorer la réactivité globale du système.
- ✓ Connectivité Avancée : La Raspberry Pi 4 8GB est équipée de ports USB 3.0 et 2.0, d'un port HDMI 2.0 et d'un port Gigabit Ethernet, offrant des possibilités de connectivité étendues.
- ✓ Prise en Charge Double Écran 4K : Elle peut gérer la sortie vidéo sur deux écrans 4K, ce qui en fait un choix idéal pour les projets multimédias et les solutions d'affichage.
- ✓ Connectivité Sans Fil : Elle intègre le WiFi 802.11ac et le Bluetooth 5.0, ce qui simplifie connectivité sans fil pour diverses applications [39].

Figure III.1: Raspberry Pi 4 model B (8GB)

II.1.3 Que peut-on faire avec un Raspberry Pi ?

Un Raspberry Pi est un outil incroyablement polyvalent, ouvrant un vaste éventail de possibilités, et voici ce que l'on peut faire avec :

- ✓ Serveur Web : Il peut être configuré comme un serveur web léger, comme Apache ou Nginx, pour héberger un site web personnel ou pour expérimenter le développement web.
- ✓ Domotique : En utilisant des capteurs et des actionneurs, le Raspberry Pi peut être intégré dans un système de domotique pour contrôler l'éclairage, la sécurité et d'autres aspects d'une maison.
- ✓ Internet des Objets (IoT) : Il permet de créer des projets IoT en connectant des capteurs et des appareils au Raspberry Pi pour surveiller et contrôler divers aspects de l'environnement.
- ✓ Robotique : Le Raspberry Pi peut être utilisé pour alimenter des robots et des drones, permettant la création de projets de robotique interactifs.
- ✓ Détecteur d'Attaque : Il peut être employé pour surveiller le trafic réseau et détecter les attaques en temps réel. Des outils tels que Snort peuvent être utilisés pour la détection d'intrusion [40].

III. Partie logiciel (Software)

III.1 Système d'exploitation

Un système d'exploitation (OS) pour Raspberry Pi est un logiciel essentiel qui permet de faire fonctionner l'ordinateur en gérant ses ressources matérielles et en offrant une plateforme sur laquelle les utilisateurs peuvent exécuter des applications.

Les Raspberry Pi sont livrés par défaut vierges de tout système d'exploitation et de tout dispositif de stockage. C'est à l'utilisateur de choisir et d'installer le système d'exploitation qu'il veut (la plus grande majorité sont des systèmes Linux) et de choisir la carte de stockage de type micro-SD avec la capacité qu'il veut (8 Go minimum conseillés).

Dans le cadre de notre projet, nous avons délibérément opté pour Raspberry Pi OS (64 bits), qui est basé sur Debian Bullseye et est doté de l'environnement de bureau Raspberry Pi. Cette décision a été prise dès l'installation de l'image du système à l'aide de l'outil Imager 1.7.5. Cette version de Raspberry Pi OS est conçue pour être compatible avec un large éventail de modèles Raspberry Pi, y compris les Raspberry Pi 3, 4 et 400, et offre une expérience optimisée pour nos besoins spécifiques en matière de projet IoT [40]. Nous avons choisi d'utiliser un Raspberry Pi 4 pour ce projet en raison de ses performances matérielles supérieures, ce qui est essentiel pour les exigences de notre application IoT.

Figure III.2 : système d'exploitation (OS) [44].

III.2 Snort

Snort est un système de détection d'intrusion (IDS, Intrusion Detection System) open source largement utilisé dans le domaine de la sécurité informatique. Développé par Sourcefire, désormais une division de Cisco, Snort est conçu pour surveiller le trafic réseau en temps réel à la recherche de comportements ou de schémas suspects qui pourraient indiquer des tentatives d'intrusion, des attaques ou d'autres activités malveillantes. Il fonctionne en analysant les paquets réseau à la recherche de signatures et d'anomalies préalablement définies, tout en offrant la possibilité de personnaliser ses règles de détection pour s'adapter à des environnements spécifiques.

Il fonctionne principalement en trois modes : le mode Sniffer, qui capture passivement le trafic réseau, le mode Packet Logger, qui enregistre le trafic pour une analyse ultérieure, et le mode NIDS (Network Intrusion Detection System), qui effectue une analyse en temps réel du trafic, détecte les intrusions et génère des alertes en fonction de règles prédéfinies [41].

Dans les sections à venir, nous explorerons en détail la manière dont nous avons configuré Snort 2.9.20 pour qu'il s'intègre efficacement à notre projet de détection d'attaques utilisant le Raspberry Pi 4 et hping3. Cette configuration nous permettra de surveiller le trafic réseau, d'analyser les paquets et d'alerter en cas de comportement suspect, renforçant ainsi la sécurité de notre environnement.

III.2.1 Architecture de Snort

Snort est basé sur une architecture modulaire et flexible qui lui permet d'effectuer des analyses de trafic réseau en temps réel pour la détection d'intrusions. Voici un aperçu de l'architecture de Snort :

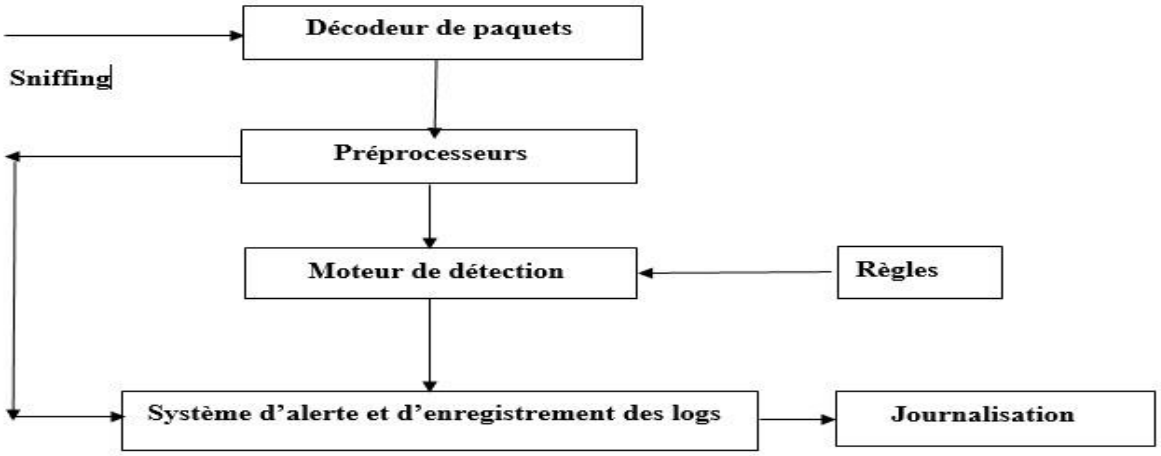

Figure III.3 : Architecture de Snort [43].

- ✓ **Sniffing (Capture)** : La première étape consiste à capturer le trafic réseau entrant et sortant. Snort utilise généralement des interfaces réseau en mode promiscuité pour capturer l'ensemble du trafic sur un segment de réseau donné. Cela signifie que Snort examine tout le trafic, pas seulement le trafic destiné à l'ordinateur sur lequel il est installé.
- ✓ **Le décodeur de paquets :** dans un système de détection d'intrusion fonctionne en activant une ou plusieurs interfaces réseau de la machine en mode promiscuité. Cette opération permet au système de surveiller et d'analyser tous les paquets de données qui transitent par la connexion réseau. Dans le cas de SNORT, cette fonction de capture est réalisée en utilisant la bibliothèque libpcap. Le décodeur de paquets se compose de plusieurs sous-décodeurs, chacun étant organisé par protocole (comme Ethernet, IP, TCP, etc.). Ces sous-décodeurs ont pour rôle de convertir les différents éléments des protocoles réseau en une structure de données interne, ce qui facilite l'analyse et la détection des comportements suspects ou des attaques potentielles dans le trafic réseau.
- ✓ **Préprocesseurs :** Les préprocesseurs sont des modules qui traitent les paquets capturés avant l'analyse proprement dite. Ils effectuent des tâches telles que la défragmentation

des paquets IP, la reconstruction des flux TCP, la normalisation du trafic, et la gestion de certaines anomalies. Les préprocesseurs préparent les données pour l'inspection ultérieure.

- ✓ **Moteur de détection** : Le cœur d'un IDS réside dans son moteur de détection, une composante essentielle. Ce moteur exploite des règles pour détecter des activités d'intrusion potentielles. Lorsqu'un paquet réseau correspond à une de ces règles, cela déclenche la génération d'une alerte. Ces règles sont organisées en diverses catégories et regroupées dans des fichiers distincts. Lors de son installation, SNORT inclut un ensemble de règles préétablies. Toutefois, elles ne sont pas activées automatiquement ; il est nécessaire de les activer manuellement dans le fichier de configuration **snort.conf**. Chaque fichier de règles spécifie les types de trafic à surveiller et à signaler.
- ✓ **Règle :** Une règle dans l'architecture de Snort est une directive conditionnelle qui spécifie des critères de correspondance pour identifier des activités malveillantes dans le trafic réseau. Elle peut inclure des signatures, des adresses IP, des ports, et d'autres paramètres pour déclencher des alertes en cas de détection d'une menace spécifique.
- ✓ **Le système d'alerte et d'enregistrement des logs de Snort** : est une composante cruciale de ce système de détection d'intrusion. Il a pour mission de signaler et de documenter les activités suspectes ou malveillantes détectées par Snort. Voici comment il fonctionne :
    - Alertes en temps réel : Lorsque le moteur de détection de Snort identifie une activité qui correspond à l'une des règles de détection configurées, il génère une alerte en temps réel. Cette alerte peut prendre la forme d'un message d'alerte système ou être envoyée à un système de gestion des événements de sécurité pour une analyse plus approfondie.
    - Logs : Snort enregistre les détails de chaque alerte dans des fichiers de logs. Ces fichiers de logs contiennent des informations précises sur les événements, tels que l'heure à laquelle l'alerte a été déclenchée, l'adresse IP source et de destination, le type d'attaque détectée, et d'autres données pertinentes.
- ✓ **Journalisation** : Snort enregistre de manière méticuleuse les détails de chaque alerte dans des fichiers de journaux. Ces fichiers de journaux renferment des données précises concernant les événements, comprenant l'horodatage de l'alerte, les adresses IP source et destination, la nature de l'attaque identifiée, ainsi que d'autres informations pertinentes [43].

III.2.2 Règle snort

Les règles de Snort sont composées de deux parties distinctes : L'en-tête (Header) et les options (options)

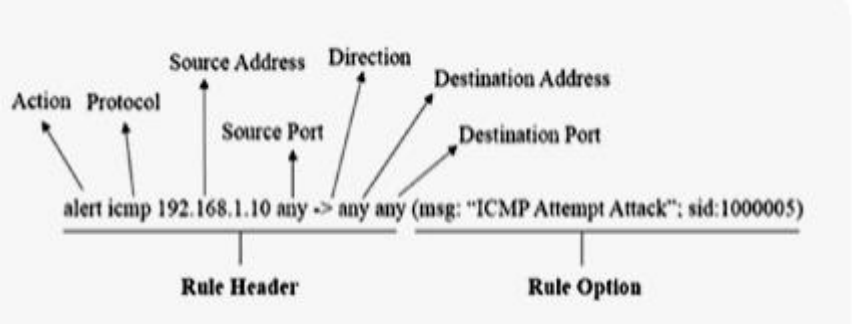

Figure III.4 : Structure de base des règles de snort [45].

L'en-tête est la partie principale qui spécifie les critères de détection de la règle :

- **L'action (Action) :** L'action spécifie ce qui doit être fait lorsque la règle correspond à un trafic. Les actions courantes incluent "Alert" (l'action va générer une alerte), "log" (l'action va enregistrer les logs du paquet tout simplement), et "pass" (ignorer le trafic correspondant).
- **Le Protocole (Protocol) :** Le champ "Protocol" dans une règle Snort détermine le protocole réseau sur lequel la règle s'applique, comme TCP, UDP ou ICMP (Internet Control Message Protocol). Cette spécification permet une détection ciblée des menaces en fonction du protocole utilisé dans le trafic réseau.
- **L'adresse source (Source adress) et L'adresse de destination (Destination adress) :** Pour chaque règle de Snort, il faut évidemment une adresse IP source et une adresse IP destination. On peut néanmoins indiquer plusieurs choix, comme une liste d'adresses IP, ou bien même un **any** pour autoriser n'importe quelle adresse IP.
- **Le port source (Source Port) et le port de destination (Destination port) :** Les ports jouent un rôle essentiel dans l'optimisation des règles de détection. Ils permettent de cibler spécifiquement les flux de données transitant par des ports particuliers. On peut spécifier un port unique ou une plage de ports.
- **La direction (Direction) :** La direction spécifie la direction du trafic, qui peut être "->" (de source à destination) ou "<-" (de destination à source).

La partie "Options" des règles Snort est un composant essentiel qui permet d'affiner et de personnaliser la détection des menaces en fonction de divers critères. Voici une description détaillée des éléments couramment utilisés dans les options des règles Snort :

-Clé "msg" (Message) : La clé "msg" permet de spécifier un message ou une description pour l'alerte qui sera générée lorsque la règle correspond à un paquet. Elle est utile pour fournir des informations sur la nature de la menace détectée.

Exemple : **msg:"Détection d'une tentative d'intrusion"**

-Clé "content" (Contenu) : La clé "content" permet de spécifier une séquence de données ou un motif que Snort recherche dans le paquet. Si le motif est trouvé, la règle est déclenchée.

Exemple : **content:"/etc/passwd" ;**

-Clé "Sid" (Signature ID) : La clé "sid" est un identifiant unique attribué à chaque règle Snort. Elle permet de référencer spécifiquement une règle dans les journaux ou les alertes générées.

Exemple : sid:1000001;

-Clé "rev" (Version de la règle) : La clé "rev" spécifie la version de la règle. Elle permet de gérer les mises à jour et les révisions des règles.

Exemple : **rev :2 ;**

-Classtype (Type classification) : La clé "classtype" permet de classifier la règle en fonction de la nature de la menace détectée. Cela peut être utile pour organiser et filtrer les alertes.

Exemple : **classtype:attempted-admin;**

Clé "threshold"(seuil) : La clé "threshold" permet de définir un seuil pour le déclenchement de la règle. Cela signifie que la règle ne sera activée que si un certain nombre d'occurrences du motif spécifié sont détectées dans un laps de temps donné.

Exemple : **threshold: type limit, track by_src, count 5, seconds 60;**

-Clé "**reference**"**(référence) :** La clé "reference" permet de fournir des références à des sources externes, telles que des CVE (Common Vulnerabilities and Exposures) ou des URL, qui décrivent davantage la menace ou la vulnérabilité.

Exemple : **reference:cve,CVE-2021-12345;**

-Clé "**Metadata**"**(Métadonnées) :** La clé "metadata" permet de spécifier des métadonnées liées à la règle, telles que l'auteur, la licence, la version, et d'autres informations pertinentes.

Exemple : **metadata: author JohnDoe, license GPL, version 1.0;**

-Clé "**Flow**"**(flux) :** La clé "flow" permet de définir des conditions spécifiques de flux de paquets pour le déclenchement de la règle. Cela peut inclure des opérations telles que "established" (flux établi) ou "to_server" (vers le serveur) [41]

Exemple : **flow : ethablished, to_server;**

III.2.3 Les Raisons d'Utiliser Snort

Snort, le logiciel que nous avons judicieusement choisi pour notre projet, présente une série d'avantages significatifs qui renforcent sa pertinence dans le contexte de la détection d'attaques :

-Open Source et Mises à Jour Gratuites : L'un des atouts majeurs de Snort réside dans son statut de logiciel open source. Cette caractéristique fondamentale garantit que les mises à jour du logiciel sont disponibles gratuitement. Cela signifie que nous pouvons maintenir notre système de détection d'attaques à jour sans encourir de frais supplémentaires, ce qui est essentiel pour garantir une sécurité continue et adaptée aux évolutions des menaces.

-Compatibilité Étendue : Snort est compatible avec une large gamme de systèmes d'exploitation couramment utilisés. Cela inclut Windows, ainsi que différentes distributions Linux telles qu'Ubuntu, Debian et CentOS. Cette compatibilité étendue nous offre une flexibilité essentielle dans le choix de notre infrastructure, nous permettant d'adopter Snort dans divers environnements et de l'intégrer facilement à notre infrastructure existante.

-Efficacité de Détection Éprouvée : Enfin, Snort est déjà bien reconnu pour sa capacité à détecter et à signaler des attaques. Son historique dans la détection d'attaques lui confère une solide réputation. Grâce à sa technologie de détection basée sur des signatures et à sa capacité à analyser le trafic réseau en temps réel, Snort est parfaitement adapté à notre projet de détection d'attaques, offrant une solution de confiance pour identifier et réagir aux menaces potentielles [42].

IV. Installation et configuration de Snort version 2.9.20

En ce qui concerne notre travail, nous avons utilisé Snort 2.9.20 comme l'un des principaux outils de détection d'attaques. Cette version de Snort est bien établie et réputée pour sa robustesse ainsi que sa flexibilité en matière de personnalisation des règles de détection. En utilisant Snort 2.9.20, nous avons pu configurer notre système de détection pour analyser le trafic réseau en temps réel et détecter les signes d'attaques.

Le déploiement de Snort 2.9.20 sur notre carte Raspberry Pi pour surveiller l'interface (Eth0) représente une étape majeure de notre projet. Dans cette section, nous expliquerons en détail les étapes que nous avons suivies pour installer, configurer et préparer Snort à la détection d'intrusions sur notre réseau local.

- ✓ **Etape 1 : Préparation de la connexion SSH**

Avant de commencer l'installation, nous avons établi une connexion sécurisée SSH (Secure Shel) entre notre PC Dell Core i3 sous Windows 10 et le Raspberry Pi 4.

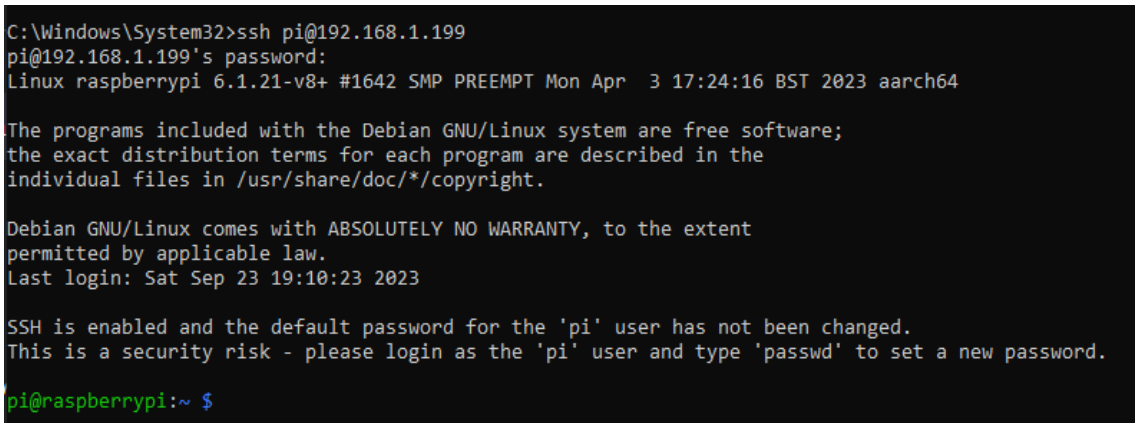

Figure III.5 : Établissement de la Connexion SSH entre le PC Dell Core i3 et le Raspberry Pi 4.

-SSH : Il s'agit du nom de la commande qu'on a utilisée pour établir une connexion SSH. Est un protocole de communication sécurisé permettant d'accéder à des systèmes distants de manière sécurisée.

-Pi : C'est le nom d'utilisateur que l'on a utilisé pour se connecter au système distant, dans ce cas, au Raspberry Pi 4.

-192.168.1.199 : Il s'agit de l'adresse IP statique donnée au Raspberry Pi.

✓ **Etape 2 : Mise à jour du système**

Pour assurer que notre Raspberry Pi est à jour, nous avons exécuté les commandes suivantes :

```
pi@raspberrypi:~ $ sudo apt upgrade
```


```
pi@raspberrypi:~ $ sudo apt upgrade
```


Figure III.6 : Mise à Jour du Système du Raspberry Pi 4.

Ces commandes ont mis à jour tous les paquets du système à la dernière version disponible.

✓ **Etape 3 : Installation de Snort**

Nous avons procédé à l'installation de Snort en utilisant la commande suivante :

```
pi@raspberrypi:~ $ sudo apt install snort
```

Figure III.7 : Installation de Snort.

Nous avons vérifié que Snort est installé correctement en exécutent « sudo snort –v ».

```
pi@raspberrypi:~ $ sudo snort -v
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

        --== Initialization Complete ==--

           -*> Snort! <*-
  ,,_      Version 2.9.20 GRE (Build 82)
 o"  )~    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
  ''''     Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.0 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=3142)
```

Figure III.8 : Vérification de l'Installation de Snort.

✓ **Etape 4 : Configuration de Snort**

Dans le but de personnaliser notre système de détection d'intrusions Snort pour répondre aux besoins spécifiques de notre réseau IoT, nous allons maintenant explorer le fichier de

configuration snort.conf. Cette étape est essentielle pour définir les règles de détection, les paramètres de journalisation et d'autres configurations clés nécessaires à une surveillance efficace du trafic réseau.

```
pi@raspberrypi:~ $ sudo nano /etc/snort/snort.conf
```

Figure III.9 : Configuration de Snort.

Nous avons défini HOME_NET comme 192.168.1.0/24, ce qui signifie que Snort surveillera le trafic à l'intérieur de cette plage d'adresses IP, couvrant potentiellement tous les dispositifs de notre réseau local avec des adresses IP dans cette plage, y compris notre Raspberry Pi à l'adresse 192.168.1.199."

Nous avons également défini EXTERNAL_NET comme any, ce qui signifie que Snort surveillera tout le trafic provenant de l'extérieur du réseau, c'est-à-dire tout trafic qui n'appartient pas à HOME_NET. Cela peut inclure le trafic en provenance d'Internet ou de tout autre réseau externe.

```
#
ipvar HOME_NET 192.168.1.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
```

Figure III.10 : Configuration des adresses IP de surveillance de snort.conf.

Nous avons ajouté deux règles personnalisées dans le fichier **local.rules**. Ces règles ont été conçues dans le but spécifique de tester la capacité de notre système à détecter une attaque de type SYN flood, l'une des attaques courantes visant à submerger un réseau en inondant le serveur cible de connexions SYN (synchronize). Cette attaque fait partie des attaques de type Déni de Service (DoS), qui visent à perturber la disponibilité d'un service ou d'un réseau en submergeant ses ressources. De plus, nous avons inclus une règle pour tester la détection d'une attaque de type ICMP flood, une autre variante d'attaque DoS, visant à submerger le réseau de requêtes ICMP, souvent utilisée pour perturber la connectivité du réseau.

- **La règle utiliser pour l'attaque SYN Flood**

alert tcp any any -> any any (flags: S; msg: "under SYN Flood Attack"; sid:100002; rev:1;)

- **La règle utiliser pour l'attaque ICMP Flood**

alert icmp any any -> $HOME_NET any (msg:"ICMP Flood Detected"; sid:1000001; threshold: type threshold, track by_src, count 100, seconds 60;)

V. Partie Test

Dans le cadre de notre évaluation de la robustesse de notre système de détection d'intrusions, nous avons mené des tests de simulation d'attaque en utilisant un autre ordinateur exécutant le système d'exploitation Ubuntu.

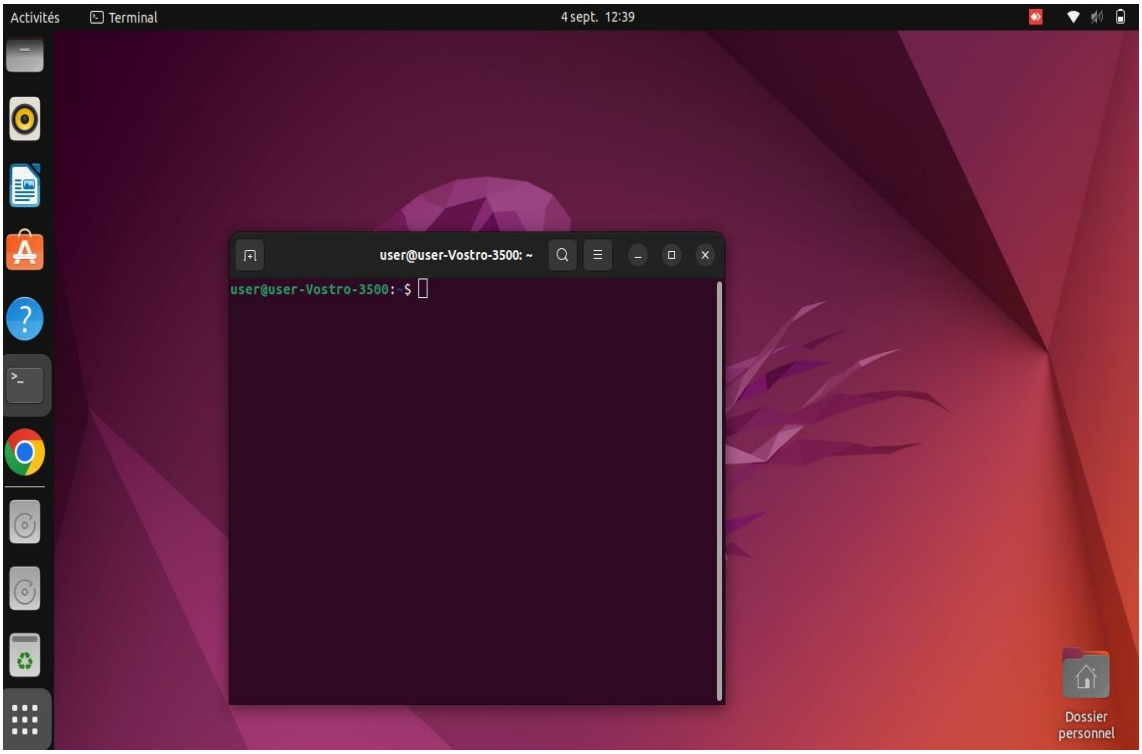

Figure III.11 : Bureau Linux Ubuntu.

Pour effectuer ces simulations, nous avons choisi d'utiliser l'outil HPing3 de test de réseau en ligne de commande qui permet de générer et de manipuler divers types de paquets réseau. Il est souvent utilisé pour simuler des attaques et des tests de pénétration sur des réseaux et des systèmes, tout en permettant aux chercheurs en sécurité de comprendre comment un système réagit à des situations de trafic réseau inhabituelles.

En utilisant HPing3 sur notre système Ubuntu, nous avons pu simuler des attaques de type SYN flood et ICMP flood, parmi d'autres, en envoyant délibérément un grand nombre de connexions SYN et de requêtes ICMP vers notre réseau, mettant ainsi à l'épreuve notre système de détection basé sur Snort 2.9.20. Notre dispositif Raspberry Pi, qui joue le rôle d'un dispositif IoT dans notre réseau local, a été spécifiquement ciblé lors de ces attaques.

V.1 Simulation de l'attaque SYN Flood (Test 1)

Dans le cadre de cette étude, nous avons entrepris une série de simulations d'attaques SYN flood, avec des paquets SYN variables (10, 20, 50 et 100).

Le tableau présente le nombre de paquets SYN utilisés dans chaque simulation, ainsi que le temps de détection correspondant en millisecondes. Ces données permettront de visualiser clairement la relation entre l'intensité de l'attaque et la réactivité de notre système de détection

Nombre de Paquets SYN	Temps de Détection par Snort (en millisecondes)
10	**199 ms**
20	**201 ms**
50	**222 ms**
100	**331 ms**

Tableau III.1 : Temps de Détection de l'Attaque SYN Flood en Fonction du Nombre de Paquets SYN.

V.2 Simulation de l'attaque ICMP Flood (Test 2)

Nous avons aussi procédé à une évaluation minutieuse de la capacité de détection de Snort 2.9.20 en simulant une attaque ICMP flood sur notre réseau local, déployant une série croissante de paquets ICMP pour mesurer la réactivité et les performances de notre système de détection.

Nombre de Paquets ICMP	Temps de Détection par Snort (en millisecondes)
10	**302 ms**
20	**408 ms**
50	**502 ms**
100	**672 ms**

Tableau III.2 : Temps de Détection de l'Attaque ICMP Flood en Fonction du Nombre de Paquets ICMP.

La figure ci-dessous représente une Comparaison entre le temps de détection des deux attaques (SYN flood et ICMP flood) en fonction du nombres de paquets .

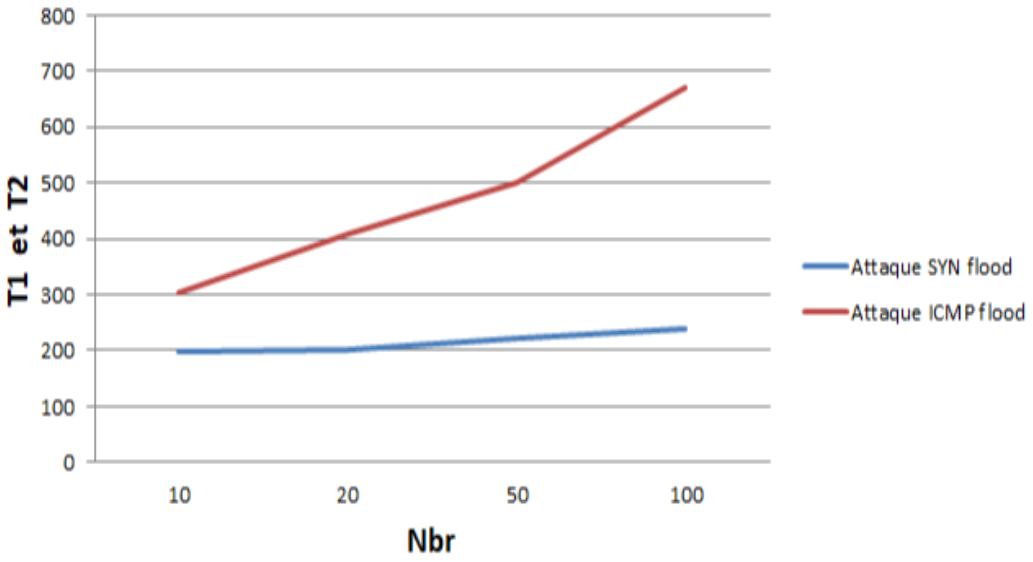

Figure III.12 : Comparaison entre attaque SYN flood et ICMP flood.

V.3 Simulation d'Attaques SYN Flood et ICMP Flood Simultanées (Test 3)

Pour ce dernier test nous continuerons de cibler le Raspberry Pi 4 en tant que dispositif IoT au sein de notre réseau local. L'objectif est de mettre en évidence la capacité de Snort 2.9.20 à gérer des attaques multiples et diversifiées en temps réel. Nous allons mesurer manuellement le temps de détection de chaque attaque et analyser la réactivité du système.

Résultat et Evaluation

Pour illustrer ces résultats, nous avons généré un journal de sécurité Snort **/var/log/snort/alert** qui affiche clairement la détection des attaques ICMP Flood et SYN Flood. La figure ci-dessous présente un instantané de ce journal, montrant comment Snort identifie et signale ces menaces simultanément.

```
pi@raspberrypi:~ $ sudo tail -f /var/log/snort/alert
09/25-15:28:16.350485  [**] [1:100002:1] under SYN Flood Attack [**] [Priority: 0] {TCP} 192.168.1.6:51599 -> 192.168.1.199:80
09/25-15:28:16.350486  [**] [1:100002:1] under SYN Flood Attack [**] [Priority: 0] {TCP} 192.168.1.6:51600 -> 192.168.1.199:80
09/25-15:28:16.351122  [**] [1:100002:1] under SYN Flood Attack [**] [Priority: 0] {TCP} 192.168.1.6:51601 -> 192.168.1.199:80
09/25-15:28:16.353254  [**] [1:100002:1] under SYN Flood Attack [**] [Priority: 0] {TCP} 192.168.1.6:51602 -> 192.168.1.199:80
09/25-15:28:16.353280  [**] [1:100002:1] under SYN Flood Attack [**] [Priority: 0] {TCP} 192.168.1.6:51623 -> 192.168.1.199:80
09/25-15:28:16.353308  [**] [1:100002:1] under SYN Flood Attack [**] [Priority: 0] {TCP} 192.168.1.6:51624 -> 192.168.1.199:80
09/25-15:28:16.353310  [**] [1:100002:1] under SYN Flood Attack [**] [Priority: 0] {TCP} 192.168.1.6:51625 -> 192.168.1.199:80
09/25-15:28:16.353349  [**] [1:100002:1] under SYN Flood Attack [**] [Priority: 0] {TCP} 192.168.1.6:51655 -> 192.168.1.199:80
09/25-15:28:16.353351  [**] [1:100002:1] under SYN Flood Attack [**] [Priority: 0] {TCP} 192.168.1.6:51656 -> 192.168.1.199:80
09/25-15:28:16.353352  [**] [1:100002:1] under SYN Flood Attack [**] [Priority: 0] {TCP} 192.168.1.6:51657 -> 192.168.1.199:80
```

Figure III.13 : Journal de Sécurité Snort - Détection d'attaque SYN Flood.

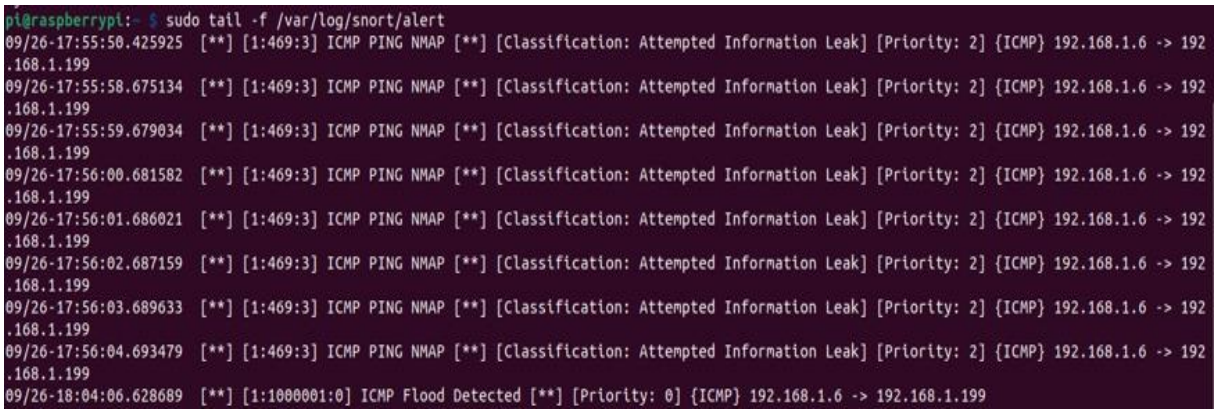

Figure III.14 : Journal de Sécurité Snort - Détection Simultanée d'ICMP Flood.

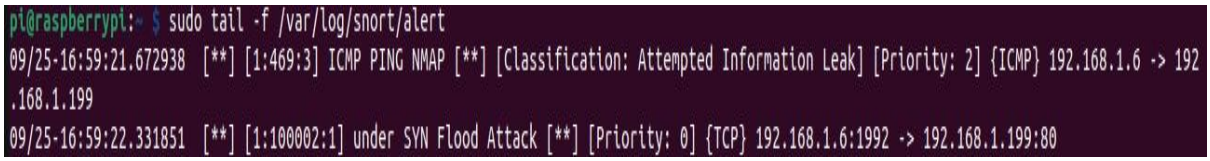

Figure III.15 : Journal de Sécurité Snort - Détection Simultanée d'ICMP Flood et SYN Flood.

-Lors de test 1, nous avons observé la réactivité de Snort 2.9.20 face à des attaques SYN Flood avec différents volumes de paquets. Les résultats montrent que Snort détecte rapidement ces attaques, avec des temps de détection allant de 199 ms pour 10 paquets à 331 ms pour 100 paquets.

-Cette première série de tests met en évidence la capacité de Snort 2.9.20 à réagir efficacement aux attaques SYN Flood en fonction de leur intensité.

- Dans le deuxième test, nous avons évalué la capacité de détection de Snort 2.9.20 face à une attaque ICMP Flood avec des volumes croissants de paquets. Les résultats montrent des temps de détection de 302 ms pour 10 paquets à 672 ms pour 100 paquets. Cette évaluation met en lumière la performance de Snort 2.9.20 comme système de détection dans la détection d'attaques ICMP Flood de différentes intensités.

- Pour le dernier test, nous avons poussé plus loin en lançant simultanément des attaques SYN Flood et ICMP Flood sur le Raspberry Pi 4, un dispositif IoT au sein de notre réseau local. L'objectif était de tester la capacité de Snort à gérer des attaques multiples en temps réel.

Bien que les temps de détection individuels varient en fonction de la nature des attaques, nous avons constaté que Snort 2.9.20 était capable de détecter les attaques SYN Flood et ICMP Flood en simultané.

Cette épreuve confirme la robustesse de Snort en tant que système de détection d'intrusion pour protéger les dispositifs IoT dans notre réseau.

VI. Analyse des Méthodes Précédentes : Défis et Limitations

Avant d'opter pour Snort comme composant central de notre solution de détection des menaces IoT, nous avons entrepris un périple à travers diverses approches et technologies. Notre première tentative a consisté à suivre un tutoriel basé sur PiHunter, un ensemble d'outils comprenant Suricata, Zeek, Filebeat, Kibana, et Elasticsearch, Arkime. Cependant, ce voyage s'est révélé semé d'embûches, car le processus de téléchargement et de configuration de ces systèmes a été entravé par des problèmes de compatibilité matérielle et de stabilité de la carte Raspberry Pi 4.

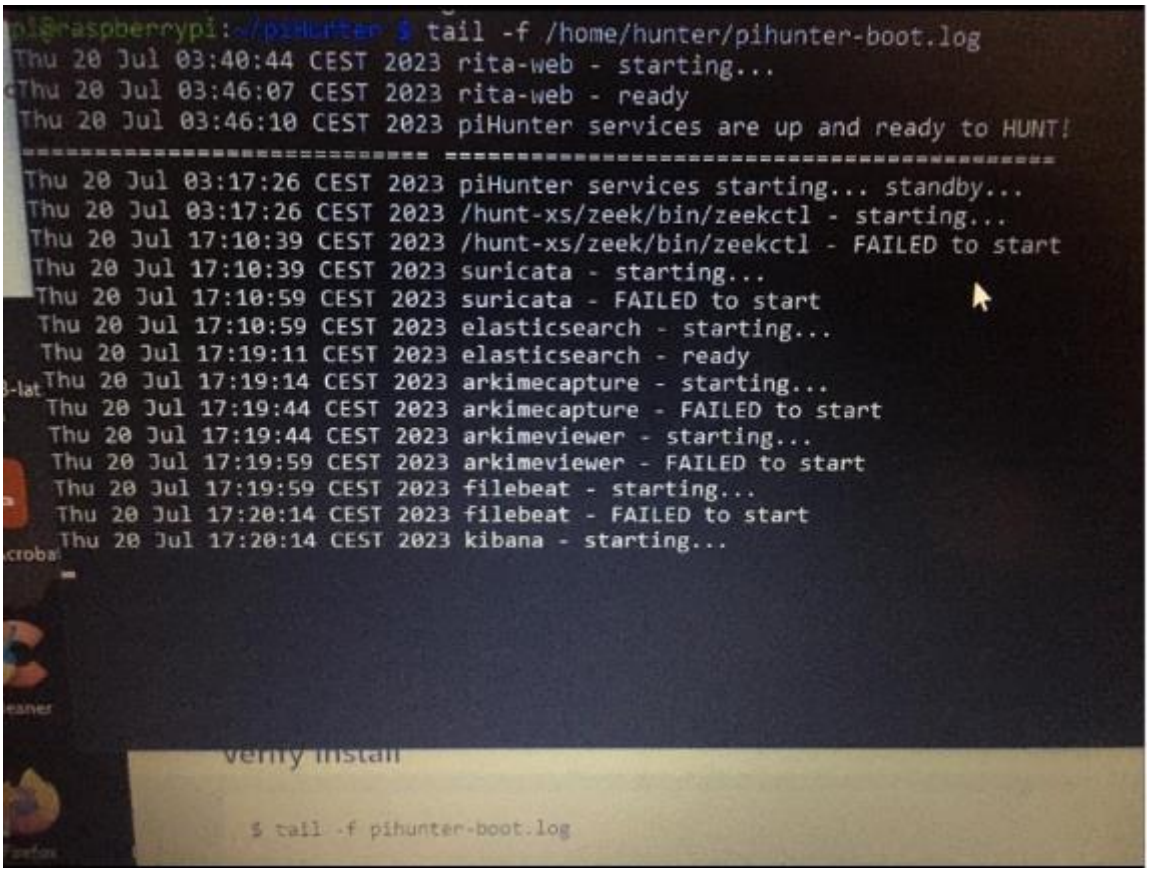

Figure III.16 : Problèmes de Démarrage partiel.

Lors de nos premiers essais avec PiHunter, nous avons rencontré des difficultés à faire fonctionner certains de ces systèmes de manière cohérente sur la carte Raspberry. Des

problèmes liés à l'architecture matérielle et aux ressources limitées de la carte ont entraîné des dysfonctionnements et des blocages récurrents. Ces obstacles ont rapidement éclairé la nécessité de trouver une alternative plus adaptée à notre projet.

Nous avons ensuite exploré la voie des réseaux de neurones convolutionnels (CNN), en suivant un tutoriel « Lucid », basé sur la bibliothèque TensorFlow 2.7.1. Malheureusement, cette aventure s'est heurtée à un obstacle majeur : l'incompatibilité de la version 2.7.1 de TensorFlow avec l'architecture arm64 de notre Raspberry Pi 4. Nos efforts pour compiler cette version se sont avérés infructueux, entraînant une perte de temps considérable.

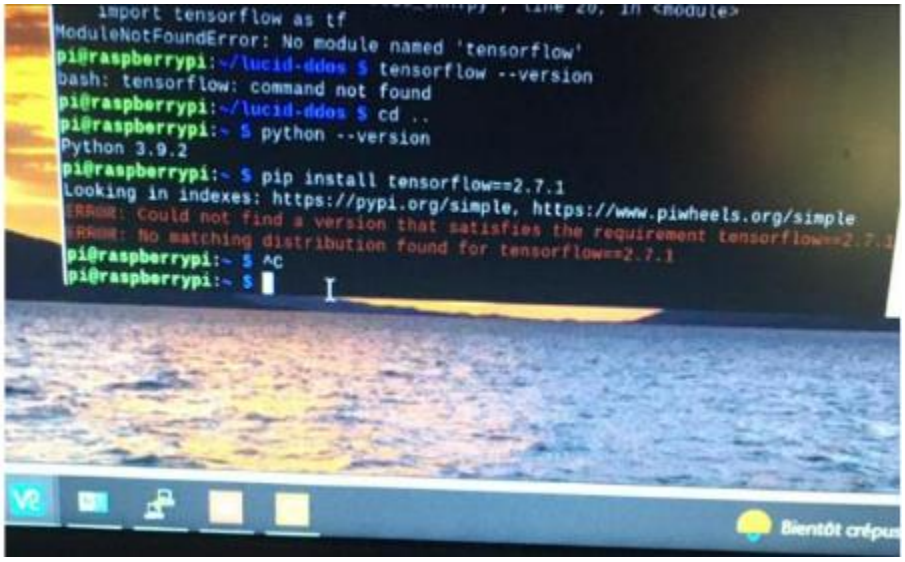

Figure III.17 : Erreur lors de l'installation de TensorFlow 2.7.1.

Finalement, nous avons trouvé une solution solide en Snort, un système de détection d'intrusion (IDS) bien établi. Grâce à une configuration personnalisée et à des tests préliminaires, nous avons pu le mettre en place sur notre Raspberry Pi 4. Les premiers résultats nous ont convaincus de la faisabilité de notre projet. Cependant, ce n'est qu'un premier pas dans notre parcours. Nos futurs tests impliqueront un réseau IoT plus complexe avec de multiples dispositifs, dans le but de perfectionner notre solution innovante.

Dans le cadre de nos prochaines étapes, nous envisageons également d'intégrer la technique du 'port mirroring'. Le port mirroring est une méthode essentielle pour la surveillance du trafic réseau au sein de notre environnement IoT. En utilisant cette technique, nous serons en mesure de dupliquer le trafic réseau depuis d'autres ports vers notre Raspberry Pi 4, où Snort effectuera son analyse de détection des menaces. Cette approche renforcera notre capacité à surveiller l'ensemble de notre réseau IoT,

garantissant ainsi une détection plus robuste des menaces émergentes et une meilleure protection de notre écosystème connecté.

VIII. Conclusion

En conclusion de ce chapitre, nous avons exploré en détail l'installation et la configuration du système de détection d'intrusions Snort 2.9.20 sur le Raspberry Pi 4, que nous avons délibérément choisi comme dispositif IoT ciblé au sein de notre réseau local. Notre objectif était d'évaluer l'efficacité de Snort face à des attaques spécifiques, à savoir l'attaque ICMP Flood et l'attaque SYN Flood.

Les résultats de nos tests ont démontré que Snort se positionne comme un rempart robuste contre ces attaques, réagissant rapidement et de manière fiable pour identifier et signaler les menaces. Notamment, le temps de détection s'est avéré significativement plus court pour l'attaque SYN Flood, Cette réactivité impressionnante renforce le rôle clé de Snort dans la protection des dispositifs IoT au sein de réseaux domestiques et industriels.

En somme, Snort 2.9.20 se révèle être un atout précieux pour la sécurité des réseaux modernes, offrant une réponse proactive aux attaques potentielles et contribuant ainsi à la protection des dispositifs IoT. Ces résultats renforcent notre compréhension de la performance de Snort dans un environnement IoT et mettent en avant son importance dans la sauvegarde de la sécurité des réseaux contemporains.

Conclusion Générale

L'Internet des Objets (IoT) a pris d'assaut notre monde moderne, transformant la façon dont nous interagissons avec notre environnement. Cette révolution technologique a donné naissance à une myriade d'applications novatrices, allant de la domotique à la gestion intelligente de l'énergie, en passant par les villes intelligentes. Cependant, cette expansion fulgurante de l'IoT. S'est accompagnée d'une préoccupation croissante en matière de sécurité. La protection des dispositifs interconnectés, de nos données personnelles et de nos infrastructures est devenue une priorité absolue.

Dans cette étude, nous avons plongé au cœur de cette question cruciale de la sécurité de l'IoT. Nous avons exploré les concepts fondamentaux de l'Internet des Objets, définissant clairement son rôle dans notre société moderne. L'IoT, qui consiste en l'interconnexion d'objets physiques via Internet, offre des avantages indéniables en termes d'efficacité, d'automatisation et de création de services intelligents. Cependant, cette interconnexion crée également des vulnérabilités potentielles qui nécessitent une vigilance constante.

Le deuxième chapitre de notre recherche nous a immergés dans le monde complexe de la cybersécurité. Face à une multitude de menaces émergentes, la cybersécurité est devenue une discipline vitale pour la préservation de l'intégrité de nos systèmes et de nos données. Nous avons plongé dans la définition de la cybersécurité, en soulignant son rôle essentiel dans la protection des informations sensibles. La carte mentale de la cybersécurité que nous avons créée a illustré la diversité des défis que nous devons relever pour assurer la sécurité de nos dispositifs IoT.

Le troisième chapitre de notre étude a introduit notre solution innovante de détection de menaces spécialement conçue pour l'IoT. Nous avons détaillé l'implémentation de cette solution sur la carte Raspberry Pi 4, mettant en évidence son rôle central dans la sécurité des dispositifs IoT. Snort, un outil de détection d'intrusion puissant, a été configuré pour surveiller en temps réel les activités suspectes dans l'environnement IoT. Cette solution offre une protection cruciale en détectant rapidement les menaces émergentes, assurant ainsi la sécurité des dispositifs de l'IoT.

Nous avons mené une série de tests approfondis pour évaluer l'efficacité de notre système. Les résultats ont été édifiants. Lors de la simulation d'attaques SYN Flood et ICMP Flood, notre solution a démontré une capacité remarquable à détecter rapidement ces menaces. Notre système a identifié les attaques en quelques millisecondes seulement, soulignant sa réactivité exceptionnelle.

En conclusion, notre étude a abouti à la création d'un système de détection de menaces innovant, déployé sur la Raspberry Pi 4, qui renforce considérablement la sécurité de l'Internet des Objets. Cette solution réactive et proactive se positionne comme un rempart essentiel contre les menaces potentielles. Nos résultats montrent que notre système est capable de détecter rapidement et de manière fiable les attaques, même lorsque celles-ci sont lancées de manière simultanée. Dans un monde où la sécurité est un impératif, notre solution offre une réponse solide pour l'adoption sereine de la technologie IoT. Elle permet d'imaginer un avenir où l'IoT apporte des avantages sans compromis pour notre vie quotidienne.

Bibliographies

[1] https://www.semanticscholar.org/paper/Introduction-to-IOT

GokhaleBhat/8dc715e70ebe3790a24904a9a76a2cb948445661#references (Consulté le 23/08/2023).

[2] TERIR, Karim, et al. Gstion de la con dentialité des données pour les dispositifs IOT (Internet of Things). 2020. University of Jijel.

[3] https://www.kaspersky.fr/resource-center/definitions/what-is-iot (Consulté le 29/08/2023).

[4]https://www.interviewbit.com/blog/difference-between-iot-and-m2m/?fbclid=IwAR0axp6OkEif98xxVqUtP56Wko6TT0RID75g86ZGD3R0FcByDRVBbUJrKLU (Consulté le 05 /09 /2023).

[5] https://www.oracle.com/fr/cloud/iot-platform/ (Consulté le 17 /08 /2023).

[6] AFOUF, Oussama et KOUAH, Sofia. Développement d'un Système d'IoT (Internet of Things) dans le cadre de Smart University. 2020. Université d'Oum Bouaghi

[7] https://iotindustriel.com/iot-iiot/les-4-plateformes-iot-les-plus-populaires / (Consulté le 05/09/2023).

[8] https://www.connectwave.fr/techno-appli-iot/iot/reseaux-et-infrastructures-iot/ (Consulté le 06/09/2023).

[9] http://www.lafabriquediy.com/tutoriel/liste-des-capteurs-229/ (Consulté 12/08/2023).

[10] Hidouci Farid, Réalisation et implémentation d'une application a base de protocole MQTT dans IoT, Soutenu le 07 juillet 2019. Université Mohamed Khider – BISKRA

[11] https://www.cloudamqp.com/docs/amqp.html (Consulté le 04 /09 /2023).

[12]https://docplayer.fr/179300501-Conception-d-objets-connectes-par-prototypage-rapide-et-protocole-mqtt-tp3.html (Consulté le 27/08/02023).

[13] https://www.reec.be/wp-content/uploads/2019/06/mqtt-1.pdf (Consulté 10/09/2023).

[14] CHIBANI, Samir, BOUKHADRA, Foudil, DJEBABLA, Ali, et al. Commande Intélligente Des Différents Objets D'une Maison. 2021. Université d'Oum Bouaghi

[15] MELISSA, Larras et DJAMILA, Khalfouni. Défis de sécurité de l'Internet des Objets Problèmes et solutions. 2019. Université Mouloud Mammeri.

[16]https://www.smartgrids-cre.fr/encyclopedie/linternet-des-objets-au-coeur-des-smart-grids/definitions-autour-des-objets-connectes technologies.

[17] https://iotindustriel.com/iot-iiot/architecture-iot-lessentiel-a-savoir (Consulté le 15 /08 /2023).

[18] https://www.objetconnecte.com/architecture-reseau-iot/ (Consulté 15/08/2023).

[19] : ABDELLAOUI, Seyf Eddine et ABDELALI, Djelloul. Conception et réalisation d'un système IoT pour le suivi des patients cardiaques. 2022. Université de tlemcen

[20] CHAOUI, Nourhane, BERKANI, Aya, et KOUAH, Sofia. Un Système d'internet of t hings (IoT) à base de flou pour la prévision météorologique. 2022. Université d'Oum Bouaghi

[21]. W. (2021, 11 février). Domaines d'applications de l'IoT, travaux et risques. WikiMemoires. https://wikimemoires.net/2019/09/domaines-d-applications-de-l-iot/. (Consulté le 01/09/2023).

[22] BAOUCH, Touhami et BELKHITER, Saad Eddine. Surveillance à distance d'un malade d'Alzheimer via un système IoT. 2017. Université de Tlemcen

[23] https://www.cnbc.com/2019/12/08/proteus-digital-struggles-to-raise-cash-after-1point5-billion-valuation.html (Consulté le 27/08/2023).

[24] BOUKHNAISSI, Fatima Zohra et GHOMARI, Ghizlane Ammaria. Conception d'un prototype IoT pour la régulation de la température d'un lieu. 2020 . Université de Tlemcen

[25] HADJADJ, Walid et ZAITER, Meriem. L'utilisation de N-Version de programmation pour la prise en charge des fautes dans un environnement IoT. 2018. Université d'Oum Bouaghi

[26] BENMAKHLOUF, Soulef, AMAROUCHE, Manel, et CHIHA, Yamina. Commande intelligente de l'éclairage d'une maison. 2020. Université d'Oum Bouaghi

[27] LAKIA-SOUCALIE, Angélique. Communication, gouvernance et cybersécurité : suite à la cyberattaque contre TV5 Monde, quels sont pour la France les nouveaux enjeux de cybersécurité et de cyberdiplomatie ? 2017.

[28] GIRAUD, Loïc. Epistémologie contemporaine autour de la Cybersécurité et des Données.

[29] MAIWALD, Eric. Sécurité des réseaux. CampusPress, 2001.

[30]https://taosecurity.blogspot.com/2017/03/cybersecurity-domains-mind-map.html (Consulté le 22/08/2023).

[31]https://myturn.careers/blog/cyber-security-domains-do-they-exist/ (Consulté le 22/08/2023).

[32] https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang.

[33] SALAMON, Yann. Cybersécurité et cyberdéfense : enjeux stratégiques. Editions Ellipses, 2020.

[34] LLORENS, Cédric, LEVIER, Laurent, VALOIS, Denis, et al. Tableaux de bord de la sécurité réseau. Editions Eyrolles, 2011.

[35] FATIMA, BOURENNANE et DALIA, BORDJI YAMINA. techniques de Cyber sécurité de Smart-Building à la base des technologies IoT/M2M. 2022. Faculté des sciences et de la technologie univ bba.

[36] AMARA, SAKINA. Une Approche IntelligenteDeep LerningPour La Detection Des Attaques Ddos Pour Le ReseauSdn. 2022. Université de Larbi Tebessi–Tebessa.

[37] https://www.logpoint.com/fr/blog/re.ponses-solutions-avantages-detection-avancee-des-menaces/ (Consulté le 14/08/2023).

[38] BENZITOUNI, Rabah, MERABET, Linda, et ZERTAL, Soumia. La Proposition d'une Architecture basée Deep Learning pour la prédiction des maladies cardiaques dans un environnement IoT. 2022. Université d'Oum Bouaghi

[39] HACHEMANE Abdelhalim , SYSTEME DE DETECTION DE SOMNOLENCE POUR CONDUCTEURS UTILISANT RASPBERRY-PI ET OPEN-CV , UNIVERSITE BADJI MOKHTAR – ANNABA, 2020 /2021.

[40] Atef Ballouche, La sécurité de l'Internet des objets (I O T) a l'aide d'un CIDS et de la Blockchain, UNIVERSITÉ BADJI MOKHTAR-ANNABA ,2020/2021.

[41] REZIG, Sabrine et KHELLADI, Nacera. Mise en place de Snort sur un réseau local. 2016.. Université Ibn Khaldoun-Tiaret-.

[42]https://www.cyberuniversity.com/post/snort-definition-fonctionnement-avantages (Consulter le 11/09/2023/).

[43] BRAHIM EMBARKA, Ben et SELYNA, Amiche. Mise en place d'une solution de détection d'intrusion. 2017. Université Mouloud Mammeri.

[44] https://www.raspberrypi.com/software/ (Consultéle 19/09/2023).

[45]https://www.researchgate.net/publication/281564631/figure/fig1/AS:669059632869383@1536527655710/Example-of-Snort-IDS-Rule-The-rule-options-of-Snort-consist-of-two-parts-a-keyword-and.jpg (Consulté le 19/09/2023).

Annexe

<table>
<tr><td>Business Model Canvas</td><td></td><td>Nom de l’entreprise :
AMEN</td><td></td><td>Date :27/09/2023</td></tr>
<tr><td>Partenaires clés</td><td>Activités Clés</td><td>Propositions de valeur</td><td>Relation Client</td><td>Clients</td></tr>
<tr><td rowspan="2">1. Entreprises de Construction (p. ex., Algérie Télécom)
2. Installateurs de Systèmes de Sécurité
3. Compagnies d'Assurance
4. Fournisseurs de Services Publics</td><td>1. Conception et Développement de Systèmes Embarqués
2. Tests et Améliorations Continus du Produit
3. Fourniture d'un Support Clientèle de Qualité
4. Développement de Mises à Jour et de Nouvelles Fonctionnalités
Ressources clés
1. Raspberry Pi 4
2. Logiciel Snort
3. Hping3
4. Objet connecté
5. Applications et Interfaces Utilisateur</td><td rowspan="2">1. Innovation, Qualité et Accessibilité
2. Économie Significative (a 30%)
3. Réduction des Coûts Matériels
4. Prototype qui détecte les menaces en temps réel a cout réduit</td><td>1. Premier Contact chez un Fournisseur
2. Publicité sur les Réseaux Sociaux
3. Accès au Site Web pour Plus de Détails
4. Service Clientèle Personnalisé
Canaux
1. Vente directe en ligne
2. Collaboration avec des Fournisseurs
3. Partenariats avec des Entreprises de Sécurité et d'Alarme
4. Publicité en ligne</td><td rowspan="2">1. Fournisseurs de Services de Sécurité (B2B)
2. Installateurs de Systèmes de Sécurité
3. Fournisseurs de Services Publics : (par exemple : Algérie télécom)
4. Propriétaires de Maisons Connectées Intelligentes</td></tr>
<tr><td colspan="2">Coûts
1. Coût de Production du Prototype
2. Coûts de Recherche et Développement (R&D)
3. Coûts Marketing et de Promotion
4. Coûts de Distribution
5. Coûts de Maintenance et de Support Client
6. Coûts de Matériel utilisé : 22000 DA + 2400 DA+ 300 DA .</td><td colspan="2">Revenus
1. Vente de Matériel
2. Licences Logicielles
3. Modèle d’abonnement
4. Services de Configuration et d'Installation
5. Service de formation
6. Partenariats avec des Entreprises de Sécurité</td></tr>
</table>

La proposition de valeur (Value proposition) :

Proposition de Valeur Complète :

- ✓ Notre proposition de valeur met en avant une solution complète de sécurité et de surveillance des réseaux locaux.

Innovation, Qualité et Accessibilité :

- ✓ Cette solution se caractérise par son mélange d'innovation, de qualité et d'accessibilité, grâce à l'intégration de Snort, un logiciel de détection d'intrusion, dans le Raspberry Pi 4.

Économie Significative :

- ✓ Elle se distingue par sa capacité à fournir une solution de sécurité et de surveillance des réseaux locaux à un coût abordable.
- ✓ Notre solution offre une économie d'environ 30% par rapport aux solutions concurrentes qui coûtent généralement plus de 15 millions.

Réduction des Coûts Matériels :

- ✓ Les systèmes de détection d'attaques IoT traditionnels sont souvent coûteux en raison de leur matériel spécialisé et de leurs licences logicielles.
- ✓ En optant pour le Raspberry Pi 4, une plateforme abordable et polyvalente, nous parvenons à réduire significativement les coûts matériels.

Segments de clients (Customer segments) :

Fournisseurs de Services de Sécurité (B2B) :

- ✓ Exemple : Un fournisseur de services de sécurité propose notre solution comme complément à ses services existants à ses clients entreprises. Grâce à notre solution, le fournisseur n'a rien à perdre, car notre modèle de prix compétitif et la qualité de notre solution IoT peuvent surprendre positivement les clients. Une fois que les clients expérimentent la sécurité renforcée à un coût abordable, ils sont plus enclins à acheter notre solution, ce qui renforce la rentabilité du fournisseur de services de sécurité.

Installateurs de Systèmes de Sécurité :

- ✓ Exemple : Les installateurs de systèmes de sécurité peuvent tester notre solution sur un projet client sans investir massivement. Si les résultats sont convaincants, ils peuvent étendre l'utilisation de notre solution à l'ensemble de leurs installations.

Fournisseurs de Services Publics : (par exemple : Algérie télécom)

- ✓ Exemple : Les fournisseurs de services publics peuvent déployer notre solution sur une partie de leurs infrastructures IoT pour évaluer son efficacité. S'ils constatent une réduction des vulnérabilités et des risques, ils peuvent ensuite étendre son utilisation à l'ensemble de leur réseau.

Propriétaires de Maisons Connectées Intelligentes :

- ✓ Exemple : Les propriétaires de maisons connectées peuvent adopter notre solution sans prendre de risque financier important. Notre modèle de tarification compétitif signifie qu'ils peuvent renforcer la sécurité de leur domicile sans compromettre leur budget. Ils bénéficient de la tranquillité d'esprit en sachant que notre solution, qui intègre Snort dans un Raspberry Pi, surveille activement leurs objets connectés, détectant rapidement les menaces potentielles et leur permettant de prendre des mesures proactives pour protéger leur maison et leur famille.

Relation avec les clients (Customer Relationship)

- ✓ Premier Contact chez un Fournisseur : Notre approche commence par un premier contact chez un fournisseur. Dans ce modèle de relation, nous travaillons en partenariat avec des fournisseurs qui intègrent notre solution dans leur catalogue de produits.

Lorsqu'un client visite le magasin ou la plateforme en ligne du fournisseur à la recherche de solutions de sécurité pour les objets connectés, notre produit est mis en avant comme une option de choix. Les représentants du fournisseur sont formés pour expliquer les avantages de notre solution, répondre aux questions des clients et les orienter vers des démonstrations en magasin si nécessaire.

- ✓ Publicité sur les Réseaux Sociaux : Une fois que les clients sont exposés à notre produit chez le fournisseur, nous renforçons notre présence en ligne par le biais de publicités ciblées sur les réseaux sociaux. Ces publicités mettent en avant les fonctionnalités avancées, l'accessibilité financière et la qualité de notre solution, attirant ainsi l'attention des clients potentiels. Les publicités sont conçues de manière à susciter l'intérêt des utilisateurs, mais elles ne fournissent que des informations de base.

- ✓ Accès au Site Web pour Plus de Détails : Lorsque les clients cliquent sur nos publicités, ils sont redirigés vers notre site web dédié. Le site web présente en détail notre proposition de valeur, les spécifications techniques, les témoignages de clients satisfaits, des vidéos de démonstration et des guides d'installation. Nous veillons à ce que le site soit convivial, informatif et engageant, permettant aux clients de trouver rapidement les informations dont ils ont besoin. Ils peuvent également trouver notre numéro de contact sur le site pour poser des questions supplémentaires ou obtenir une assistance personnalisée.

- ✓ Service Clientèle Personnalisé : Nous accordons une grande importance à un service clientèle personnalisé. Les clients peuvent nous contacter par e-mail, par téléphone ou via un chat en direct pour obtenir une assistance en temps réel. Notre équipe est formée pour fournir des réponses précises et rapides aux questions des clients, qu'il s'agisse de la compatibilité de notre solution avec leurs appareils IoT spécifiques ou de l'assistance à l'installation.

- ✓ Mises à Jour Régulières : Enfin, nous maintenons une relation continue avec nos clients en leur fournissant des mises à jour régulières de notre solution de détection de menaces. Cela garantit que notre produit reste pertinent et efficace à mesure que de nouvelles menaces émergent sur le marché des objets connectés. Nous informons nos clients des mises à jour par le biais de notifications sur notre site web et par e-mail.

- ✓ Séances de Formation Personnalisées : Dans un souci de partenariat durable avec nos clients professionnels, nous organiserons des séances de formation personnalisées. Ces sessions seront conçues pour répondre aux besoins spécifiques de leurs équipes techniques, les aidant à maximiser l'efficacité de notre solution dans le contexte de leurs opérations. Cette démarche renforcera leur expertise et favorisera une utilisation optimale de notre produit.

Canaux de distribution :

- ✓ Vente Directe en Ligne : Notre produit est disponible en vente directe sur notre site web dédié. Les clients peuvent parcourir nos offres, passer des commandes en ligne et effectuer des paiements sécurisés. Cette méthode offre une commodité maximale pour les clients qui préfèrent acheter en ligne.

- ✓ Collaboration avec des Fournisseurs : Nous collaborons avec des fournisseurs tels que des chaînes de magasins spécialisés dans la sécurité IoT. Ils intègrent notre solution dans leur catalogue de produits, ce qui permet aux clients de l'acheter lorsqu'ils visitent ces points de vente physiques ou en ligne.

- ✓ Publicité en Ligne : Nous utilisons des publicités ciblées sur les réseaux sociaux et des moteurs de recherche pour atteindre un public plus large. Les clients intéressés sont redirigés vers notre site web pour en savoir plus et effectuer des achats.

- ✓ Partenariats avec des Entreprises de Sécurité et d'Alarme : Nous établissons des partenariats stratégiques avec des entreprises spécialisées dans la sécurité et les alarmes. Ces partenaires intègrent notre solution dans leurs offres de service, ce qui étend notre portée à leur base de clients existante.

- ✓ Partenariats avec des Fournisseurs de Services Publics(tel qu'Algérie telecom) : Nous travaillons en collaboration avec des fournisseurs de services publics, notamment dans le domaine de l'IoT. Cela nous permet de proposer notre solution comme une option de sécurité pour leurs clients utilisant des appareils connectés.

Partenaires clés :

- ✓ Entreprises de Construction (p. ex., Algérie Télécom) : Notre collaboration avec des entreprises de construction, notamment des acteurs majeurs tels qu'Algérie Télécom, est essentielle pour intégrer notre solution dans les nouvelles constructions intelligentes. Ces partenaires intègrent notre solution de sécurité IoT dès la phase de conception, ce qui garantit une sécurité optimale dès le début.

- ✓ Installateurs de Systèmes de Sécurité : Les installateurs de systèmes de sécurité sont des partenaires clés qui prennent en charge l'installation et la configuration de notre solution chez les clients. Ils jouent un rôle essentiel dans la mise en place réussie de notre produit chez les utilisateurs finaux.

- ✓ Compagnies d'Assurance : Les compagnies d'assurance peuvent devenir des partenaires stratégiques en intégrant notre solution dans leurs offres de services. Cela pourrait inclure des réductions d'assurance pour les clients qui utilisent notre solution de sécurité IoT, encourageant ainsi l'adoption.

- ✓ Fournisseurs de Services Publics : Les partenariats avec des fournisseurs de services publics, tels qu'Algérie Télécom, peuvent permettre une distribution plus étendue de notre solution. Ces partenaires peuvent recommander notre produit aux clients qui utilisent des services publics liés à l'IoT.

Activités Clés :

- ✓ Conception et Développement de Systèmes Embarqués : L'une de nos activités clés est la conception et le développement de systèmes embarqués, en utilisant le Raspberry Pi 4 comme plateforme de base. Cela inclut la création du matériel nécessaire, le développement des composants logiciels spécifiques et l'intégration de Snort pour la détection d'intrusion.
- ✓ Tests et Améliorations Continus du Produit : Nous effectuons des tests rigoureux de notre solution pour garantir sa sécurité et son efficacité. Cela comprend des tests d'intrusion, des tests de performance et des mises à l'épreuve dans des scénarios réalistes. Les résultats de ces tests sont utilisés pour améliorer constamment notre produit.
- ✓ Fourniture d'un Support Clientèle de Qualité : Nous offrons un support clientèle de haute qualité pour aider nos clients dans l'installation, la configuration et l'utilisation de notre solution. Cette activité inclut la formation de notre équipe de support pour fournir une assistance précise et efficace.
- ✓ Développement de Mises à Jour et de Nouvelles Fonctionnalités : Nous continuons à développer des mises à jour de notre solution pour répondre aux besoins changeants du marché et pour rester en avance sur les nouvelles menaces potentielles. L'ajout de nouvelles fonctionnalités et l'amélioration des capacités existantes sont des activités clés pour maintenir la pertinence de notre produit.

Ressource clés :

- ✓ Notre Compétence Technique et Humaine : Notre équipe multidisciplinaire possédant des compétences en sécurité, en développement logiciel, en électronique et en réseaux est une ressource clé pour la conception, le développement et la maintenance de notre solution.
- ✓ Raspberry Pi 4 : La Raspberry Pi 4 est la pierre angulaire de notre solution. Elle sert de plateforme matérielle pour le déploiement de notre système embarqué de détection de menaces IoT.
- ✓ Logiciel Snort : Snort, en tant que logiciel de détection d'intrusion, est une ressource essentielle qui nous permet de surveiller et de détecter en temps réel les menaces potentielles au sein des réseaux IoT.
- ✓ hping3 : L'outil hping3 est une ressource technique clé qui nous aide à tester la résilience de notre solution en simulant divers scénarios d'attaque et en évaluant sa réactivité.

- ✓ Objets Connectés : Les objets connectés eux-mêmes, tels que les caméras de sécurité, les capteurs de mouvement, les thermostats intelligents, etc., font partie intégrante de notre solution, car ils sont les points d'entrée potentiels pour les menaces. Leur prise en charge et leur intégration sont des ressources cruciales.
- ✓ Applications et Interfaces Utilisateur : Les applications logicielles que nous développons pour configurer, surveiller et gérer notre solution sont des ressources clés pour l'interaction avec nos utilisateurs.

Les sources de revenus :

- ✓ Vente de Matériel : Nous pouvons générer des revenus en vendant des kits de matériel comprenant la Raspberry Pi 4, les capteurs, les dispositifs IoT compatibles, et le logiciel snort pré-installé pour la détection de menaces.
- ✓ Licences Logicielles : Nous proposons des licences logicielles payantes pour l'utilisation de notre solution de détection de menaces, en fonction du nombre de dispositifs IoT connectés ou de la couverture réseau.
- ✓ Modèle d'Abonnement : Nous offrons un modèle d'abonnement mensuel ou annuel pour l'accès continu à notre service de détection de menaces, avec des fonctionnalités avancées, des mises à jour de sécurité et un support client dédié.
- ✓ Services de Configuration et d'Installation : Nous facturons des frais de services pour l'installation, la configuration et la personnalisation de notre solution chez les clients, en particulier pour les entreprises qui ont besoin d'une assistance professionnelle.
- ✓ Maintenance et Support Technique : Nous proposons un service de maintenance et de support technique payant pour garantir le bon fonctionnement continu de la solution, avec des options de dépannage en cas de problèmes.
- ✓ Partenariats avec des Entreprises de Sécurité : Nous établissons des partenariats avec des entreprises de sécurité informatique et de surveillance pour intégrer notre solution dans leurs offres de service et partageons les revenus générés.
- ✓ Tarification à l'Utilisation : Notre solution est tarifée en fonction de l'utilisation, comme le nombre d'alertes générées, pour répondre aux besoins spécifiques de nos clients.
- ✓ Services de Formation : Nous proposons des programmes de formation payants pour les utilisateurs finaux, les intégrateurs de systèmes, et les professionnels de la sécurité intéressés par notre produit .

Structure de cout :

- ✓ Coût de Production du Prototype : Le coût de production du prototype, qui s'élève à 50 000 DA, représente une part significative de nos dépenses initiales. Cela inclut le Raspberry Pi 4, les composants matériels, les coûts de fabrication et d'assemblage, ainsi que les licences logicielles nécessaires, comme Snort. Cette dépense est essentielle pour la création de notre solution.
- ✓ Coûts de Recherche et Développement (R&D) : Les coûts de R&D englobent les dépenses liées à la conception, au développement et à l'amélioration de notre solution. Cela comprend les salaires de l'équipe de développement, l'achat d'équipements de test, les frais de prototypage, les logiciels de développement, et autres ressources nécessaires pour perfectionner notre produit.
- ✓ Coûts Marketing et de Promotion : Pour faire connaître notre solution, nous devrons allouer des fonds pour le marketing et la promotion. Cela comprend la création de sites web, la publicité en ligne, la participation à des salons et événements de l'industrie, ainsi que la création de supports promotionnels. Toutefois, grâce à notre modèle de tarification abordable, ces coûts sont réduits par rapport aux solutions concurrentes.
- ✓ Coûts de Distribution : Les coûts de distribution incluent les dépenses liées à la mise en place de canaux de distribution. Cela peut englober les commissions versées aux partenaires de distribution.
- ✓ Coûts de Maintenance et de Support Client : Pour assurer la satisfaction de nos clients, nous devons allouer des ressources aux services de maintenance, aux mises à jour logicielles et au support client. Ces coûts sont importants pour garantir que notre solution fonctionne de manière optimale.
- ✓ Coûts de Matériel utilisé : 22000 DA + 2400 DA+ 300 DA .

Grâce à notre approche innovante de réduction des coûts et à notre modèle de tarification compétitif, notre solution offre une économie d'environ 30 % par rapport aux solutions concurrentes coûtant au moins 150 000 DA. Cela nous permet de rester compétitifs sur le marché tout en offrant une valeur exceptionnelle à nos clients.