REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE IBN KHALDOUN - TIARET

MEMOIRE

Présenté à :

FACULTÉ MATHEMATIQUES ET INFORMATIQUE
DÉPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

MASTER

Spécialité : Réseaux et

Télécommunications Par :

SerardiSouraya et Benhamouda Mohamed El houcine

Sur le thème

Vers un système de détection d'intrusion dans l'Internet des Objets

Soutenu publiquement à Tiaret devant le jury composé de :

Mr BENGHANI abdelmalek	M.C.B	Université IBN-KHALDOUN Tiaret	Président
Mr. ALEM Abdelkader	M.A.A	Université IBN-KHALDOUN Tiaret	Encadreur
Mr. NASSEN samir	M.C.B	Université IBN-KHALDOUN Tiaret	Examinateur

2022-2023

Remerciements

Nous tenons tout d'abord à remercier DIEU le tout puissantet Le miséricordieux, qui nous a donné laforce

et la patience d'accomplir ce modestetravail

Un très grand merci à :

Nos parents qui nous ont suivis pendant nos études.

En second lieu nous tenons à remercier notre encadreur

Mr ***ALEM Abdelkader*** *pour son aide, pour son encouragement,*

et pour ses précieux conseils durant la réalisation de ce travail.

Nos vifs remerciements vont également aux membres du jury

Mr ***NASSEN SAMIRE*** *et Mr* ***BENGHANI ABDEL MALEK****qui ont*

pris de leur temps pour juger ce modeste travail,

qu'ils trouvent ici l'expression de notre gratitude et tout notre respect.

Comme nous n'oublions pas M. BOUAZZA Abdelhamid pour son soutien et son assistance.

Nous adressons aussi nos remerciements à tous les professeurs qui nous ont enseignés durant ce cursus universitaire.

RESUME

Les applications de l'Internet des objets (IoT) augmentent de jour en jour, car elles sont utilisées dans de nombreux domaines et systèmes, et à mesure que leurs utilisations et leurs modes d'emploi se multiplient, de nombreuses lacunes apparaissent, le problème le plus important étant la sécurité.

L'IoT compte un grand nombre d'appareils connectés, ce qui entraîne un trafic de données mobiles important, et les protocoles de routage sont un élément clé.

L'IoT dispose de nombreux protocoles de routage, le plus largement utilisé étant le protocole RPL (Routing Protocol for Low-Power and Lossy Networks), qui prend en compte la puissance limitée et les capacités de l'appareil, mais il souffre de plusieurs faiblesses, la plus importante étant les attaques basées sur le routage qui ciblent ce protocole.

Dans ce travail, notre objectif est de résoudre le problème de l'Internet des objets (IoT) aux attaques basées sur le protocole RPL en tant que protocole de routage. Pour cela, nous avons utilisé un système de détection d'intrusion basé sur l'apprentissage en profondeur. Nous avons utilisé un ensemble de données appelé Minerva-IoT qui contient des attaques IoT.

Pour construire cet ensemble de données, nous avons utilisé le simulateur Cooja et mis en œuvre différents scénarios pour générer des attaques représentatives. Cela nous a permis d'extraire des caractéristiques importantes pour la détection d'intrusion. De plus, nous avons inclus de nouvelles caractéristiques sensibles, telles que la puissance des nœuds et leur emplacement géographique, afin d'améliorer la précision de notre système de détection.

Un aspect crucial de notre travail a été d'équilibrer l'ensemble de données en corrigeant les classes minoritaires, en particulier les attaques rares. Cette étape vise à éviter les performances trompeuses lors de l'utilisation de l'intelligence artificielle (IA) pour détecter les intrusions.

Les résultats étaient très satisfaisants après avoir relevé les défis les plus importants dans les systèmes de détection d'intrusion en termes de taux de fausses alarmes (faux positifs), de précision et d'exactitude.

Mots-clés : Internet des objets, Routing Protocol for Low-Power and Lossy Networks, Long Short-Term Memory, Sécurité, systèmes de détection d'intrusion.

ABSTRACT

The applications of the Internet of Things (IoT) are increasing day by day as they are used in various fields and systems, and as their uses and deployments multiply, many gaps emerge, with security being the most significant problem.

The IoT consists of a large number of connected devices, leading to significant mobile data traffic, and routing protocols are a key element.

The IoT has numerous routing protocols, with the most widely used being the RPL protocol, which takes into account the limited power and capabilities of the device, but it suffers from several weaknesses, the most significant being routing-based attacks targeting this protocol.

In this work, our objective is to address the problem of IoT's exposure to RPL-based attacks as a routing protocol. For this purpose, we have used a deep learning-based intrusion detection system. We utilized a dataset called Minerva-IoT, which contains IoT attacks.

To construct this dataset, we used the Cooja simulator and implemented different scenarios to generate representative attacks. This allowed us to extract important features for intrusion detection. Additionally, we included new sensitive features such as node power and geographical location to enhance the accuracy of our detection system.

A crucial aspect of our work was to balance the dataset by addressing minority classes, particularly rare attacks. This step aims to avoid misleading performance when using artificial intelligence (AI) for intrusion detection.

The results were highly satisfactory after addressing the most significant challenges in intrusion detection systems in terms of false alarm rates (false positives), accuracy, and precision.

Keywords: Internet of Things, Routing Protocol for Low-Power and Lossy Networks, Long Short-Term Memory, Security, Intrusion Detection Systems.

الملخص

تزداد الحاجة يوما بعد يوم إلى تطبيقات إنترنت الاشياء، حيث أصبحت تُستخدم في العديد من المجالات والأنظمة، ومع هذا التزايد الواسع لاستخداماتها وطرق توظيفها، بدأت تظهر معها ثغرات عديدة أهمها مشكل الحماية.

إن شبكات أنترنت الاشياء تحتوي على عدد كبير من الاجهزة المتصلة وبالتالي حركة البيانات المتنقلة فيها تكون كبيرة و بروتوكولات التوجيه هي عنصر أساسي لذلك .

يوجد العديد من بروتوكولات التوجيه في أنترنت الأشياء ,أكثرها إستخداما و إعتمادا هو بروتوكول (RPL) الذي يأخذ بعين الاعتبار محدودية الطاقة و امكانيات الأجهزة المتصلة لكنه يعاني من عدة نقاط ضعف اهمها الهجمات و التسللات التي تستهدف هذا البروتوكول .

نهدف في هذا العمل إلى حل مشكلة تعرض شبكات أنترنت الاشياء إلى الهجمات التي تعتمد على بروتوكول (RPL) كبروتوكول توجيه.قمنا ببناء نموذج بإستخدام التعلم العميق ومجموعة بيانات تحتوي على أهم الهجمات تم بنائها من خلال عمل محاكاة بأداة (Cooja) وتنفيذ سيناريوهات مختلفة سمحت بالتوصل إلى سمات مهمة مع إضافة سمات جديدة مؤثرة كطاقة العقد ومقرها الجغرافي مما جعل مجموعة البيانات شاملة لأغلب هجمات التوجيه الخاصة بأنترنت الاشياء كما تم حل مشكل البيانات القليلة (فئات الهجمات) بالإعتماد على خوارزميات ذكية لجعل عددها كافي من أجل بناء نموذج قوي .

كانت النتائج المتوصل إليها مرضية للغاية وذلك بعد تحقيق أهم التحديات في أنظمة كشف التسلل من معدل أدنى من الانذارات الكاذبة (إيجابية كاذبة) و معدل أقصى لاكتشاف الهجمات.

الكلمات المفتاحية : أنترنت الاشياء , أنظمة كشف التسلل,بروتوكول التوجيه ,الأمن....

Table des matières

LISTE DES FIGURES

LISTE DE TABLEAUX

LISTE DES ABREVIATIONS

IOT:Internet of Things.

IDO : Internet des objets **.**

IETF: Internet Engineering Task Force

6LoPAN :IPv6 over Low-Power wireless Personal Area Networks.

RFID : Radio-Frequency Identification.

NFC : Near-Field Communication

IDS : Intrusion Detection Systems .

RPL :IPv6 Routing Protocol for Low-Power and Lossy Networks.

DIS : DODAG Information sollicitation .

DIO : DODAG Information Object.

DAO :DODAGAdvertisment Object.

DODAG : Destination Oriented Directed Acyclic graph.

WLAN : Wireless Local Area Network..

DNN : Deep Neural Network.

RNN : Recurrent Neural Network.

CNN : Convolutional Neural Network.

LSTM : Long Short-Term Memory.

Introduction générale

INTRODUCTIONGENERALE:

Avec l'évolution de la technologie, l'internet est devenu une nécessité dans la vie moderne. Dans cette optique, les chercheurs se sont efforcés d'améliorer la vie quotidienne en permettant aux objets de se connecter à internet sans intervention humaine. C'est ce qu'on appelle l'Internet des objets (IdO) ou IoT.

Les avancées technologiques récentes rendent possible la connexion des objets du quotidien à internet, ouvrant ainsi de nouvelles perspectives. Cependant, pour assurer une communication optimale entre ces objets, il est essentiel d'utiliser des solutions ouvertes et interopérables.

RPL est un protocole de routage vectoriel à distance novateur standardisé pour les réseaux 6LoWPAN contraints, permettant aux nœuds de communiquer dans une topologie en maillage. Malheureusement, plusieurs attaques existent sur le protocole RPL, qui cible la disponibilité d'un nœud et augmentent considérablement sa consommation d'énergie.

La sécurité du routage dans les réseaux IoT demeure l'un des problèmes majeurs qui entrave le déploiement rapide de cette technologie en raison de l'évolution constante des attaques visant les protocoles de routage. Il est essentiel de mettre en place des mesures de sécurité pour garantir la confiance dans ces réseaux connectés à des dispositifs IoT, ce qui constitue un objectif pour les chercheurs afin de trouver un mécanisme de sécurité fiable. Cependant, des défis persistent, tels que la difficulté de distinguer les attaques qui peuvent passer inaperçues (faux négatifs) pendant la phase d'apprentissage, ainsi que les fausses alertes (faux positifs).

Avec la prolifération croissante des dispositifs IoT, l'Internet des objets devient une plateforme attrayante pour diverses attaques sur Internet. Ces attaques prennent différentes formes et ciblent diverses ressources sur une multitude de dispositifs IoT. Afin de sécuriser les systèmes IoT, il est crucial d'assurer une surveillance et une analyse constantes.

Étant donné le volume considérable de données réseau et de capteurs générées par ces dispositifs et systèmes IoT (Big Data), il est nécessaire d'intégrer des techniques d'apprentissage automatique (ML) pour assurer une surveillance en continu et analyser la sécurité des systèmes IoT. Cela permet de détecter les anomalies, les attaques et les comportements suspects dans les systèmes IoT, renforçant ainsi la sécurité globale.

L'objectif de cette étude de recherche est de créer un système de détection d'intrusion basé sur le Deep Learning (DL) spécifiquement conçu pour détecter les attaques de routage dans l'Internet des Objets (IoT). Nous nous sommes concentrés sur des attaques de routage spécifiques à l'IoT, telles que la diminution du rang, le numéro de version, le trou noir et l'inondation de messages Hello. Une fois une intrusion détectée, le système est en mesure de prendre des mesures d'atténuation appropriées. Il a été conçu pour être compatible avec une large gamme de réseaux IoT.

Ce mémoire est structuré en quatre chapitres, qui sont répartis de la manière suivante :

1. Le premier chapitre : Dans ce chapitre, nous abordons une étude sur l'Internet des Objets (IoT), le protocole RPL et les problèmes de sécurité associés à l'IoT. Nous examinons en détail les concepts clés de l'IoT, ainsi que le protocole RPL utilisé comme protocole de routage. De plus, nous analysons les principales vulnérabilités et les défis de sécurité auxquels l'IoT est confronté.
2. Le deuxième chapitre : Ce chapitre est dédié à la présentation des IDS (Intrusion DetectionSystems). Nous explorons les différentes techniques et approches utilisées dans les systèmes de détection d'intrusion pour détecter les attaques et les comportements malveillants. Nous discutons également des différents types d'IDS, tels que les IDS basés sur les signatures et les IDS basés sur l'anomalie.
3. Le troisième chapitre : Dans ce chapitre, nous abordons le Deep Learning (DL) et son application dans le domaine de la cybersécurité. Nous explorons les concepts fondamentaux du Deep Learning, tels que les réseaux de neurones profonds, l'apprentissage en profondeur et les architectures de réseaux couramment utilisées. En outre, nous examinons comment le DL peut être utilisé pour améliorer la détection d'intrusion et renforcer la sécurité des systèmes IoT.
4. Le dernier chapitre : Ce chapitre est consacré à la simulation et à l'analyse des résultats obtenus à partir de notre modèle proposé. Nous décrivons en détail la méthodologie de simulation que nous avons utilisée, y compris les outils et les scénarios de simulation. Ensuite, nous présentons les résultats de notre modèle de détection d'intrusion basé sur l'apprentissage en profondeur et discutons de leur performance et de leur efficacité dans la détection des attaques IoT.

Chapitre 1 : Internet des objets

INTRODUCTION

L'Internet des objets (IdO), connu également sous le nom d'Internet of Things (IoT) en anglais, est un réseau d'objets dotés de technologies intégrées qui leur permettent de se connecter à Internet. Il englobe également les connexions établies entre ces objets et d'autres appareils et systèmes Internet. Les éléments constitutifs de cet écosystème peuvent être des machines, des composants physiques, des animaux, voire des individus. L'IdO étend la connectivité Internet au-delà des dispositifs classiques tels que les ordinateurs et les smartphones, englobant un large éventail d'objets du quotidien. Parmi les exemples courants d'objets connectés, on retrouve les thermostats de climatisation, les voitures, les lampes domestiques, les montres d'alarme, et bien d'autres encore.

1 DEFINITION:

En règle générale, le concept d'Internet des objets se réfère à des situations où la connectivité et les capacités informatiques sont étendues aux objets, aux capteurs et aux articles du quotidien qui ne sont pas traditionnellement considérés comme des ordinateurs. Cela permet à ces dispositifs de collecter, échanger et utiliser des données avec une intervention humaine minimale. Il convient toutefois de noter qu'il n'existe pas de définition unique et universelle de ce concept[1].

2 CARACTERISTIQUE DE L'INTERNET DES OBJETS :

Les caractéristiques fondamentales de l'IoT sont les suivantes :

- ***Interconnectivité:***

  L'Internet des objets permet la connexion de tout objet à l'infrastructure mondiale de communication et d'information[2].

- ***Services liés aux objets:***

  L'Internet des objets permet la fourniture de services liés à l'objet en assurant la cohérence entre les objets physiques et virtuels qui leur sont associés, tout en garantissant la confidentialité des données. Cette technologie est en train de transformer le monde physique et numérique en créant un monde interconnecté où les objets peuvent devenir "intelligents". [2].

- ***Hétérogénéité :***

Les dispositifs de l'IoT sont hétérogènes car ils sont basés sur différentes plateformes matérielles et réseaux, et peuvent interagir avec d'autres dispositifs ou plateformes de service via divers réseaux.[2].

- ***Changements dynamiques :***

  Les états des dispositifs de l'IoT évoluent dynamiquement, tels que leur état de veille et d'activité, leur connectivité, ainsi que leur contexte, tels que leur localisation et leur vitesse. De plus, le nombre d'appareils peut également changer de manière dynamique.[2].

- ***Échelle énorme :***

  Le nombre d'appareils qui doivent être gérés et qui communiquent entre eux sera au moins un ordre de grandeur plus grand que les appareils connectés à l'Internet actuel. La gestion des données générées et leur interprétation à des fins d'application seront encore plus importantes. Cela concerne la sémantique des données, ainsi que le traitement efficace des données[2].

- ***Sécurité :***

  Alors que nous bénéficions de l'Internet des objets, il est crucial de ne pas négliger la question de la sécurité. En tant que concepteurs et utilisateurs de l'IdO, nous devons intégrer la sécurité dès la conception. Cela implique de garantir la sécurité de nos données personnelles et de notre sécurité physique. La sécurisation des appareils, des réseaux et des données qui transitent par l'IdO nécessite la mise en place d'un nouveau paradigme de sécurité qui sera essentiel pour assurer la fiabilité et la confidentialité des informations échangées.[2].

- ***Connectivité*** :

  La connectivité dans l'Internet des objets assure l'accessibilité et la compatibilité du réseau. L'accessibilité se réfère à la capacité de se connecter au réseau, tandis que la compatibilité permet une capacité commune de consommer et produire des données.[2].

3 ARCHITECTURE DE L'IOT :

Il n'y a pas de consensus unique sur l'architecture de l'Internet des objets, qui est universellement reconnu. Différentes architectures ont été proposées par différents chercheurs[2].

3.1 Architectures à trois couches :

L'architecture IoT peut être décrite comme une pile technologique à trois couches :

- **La couche de perception** : C'est la couche physique, qui dispose des capteurs pour la détection et la collecte d'informations sur l'environnement. Elle détecte certains paramètres physiques où identifient d'autres objets intelligents dans l'environnement[3].
- **La couche réseau** : Cette couche est responsable de la connexion à d'autres objets intelligents, à des dispositifs réseau et à des serveurs. Ses caractéristiques sont également utilisées pour la transmission et le traitement des données des capteurs[4].
- **La couche application** : Cette couche est responsable de la prestation de services spécifiques à l'application à l'utilisateur. Elle définit diverses applications dans lesquelles l'Internet des objets peut être déployé, par exemple, les maisons intelligentes, les villes intelligentes et la santé intelligente[4].

Les données proviennent de la couche de l'appareil et passent par la couche de la passerelle avant d'entrer dans le Cloud où réside la couche de la plate-forme IoT. Chaque couche joue un rôle important dans la fourniture de services IoT.

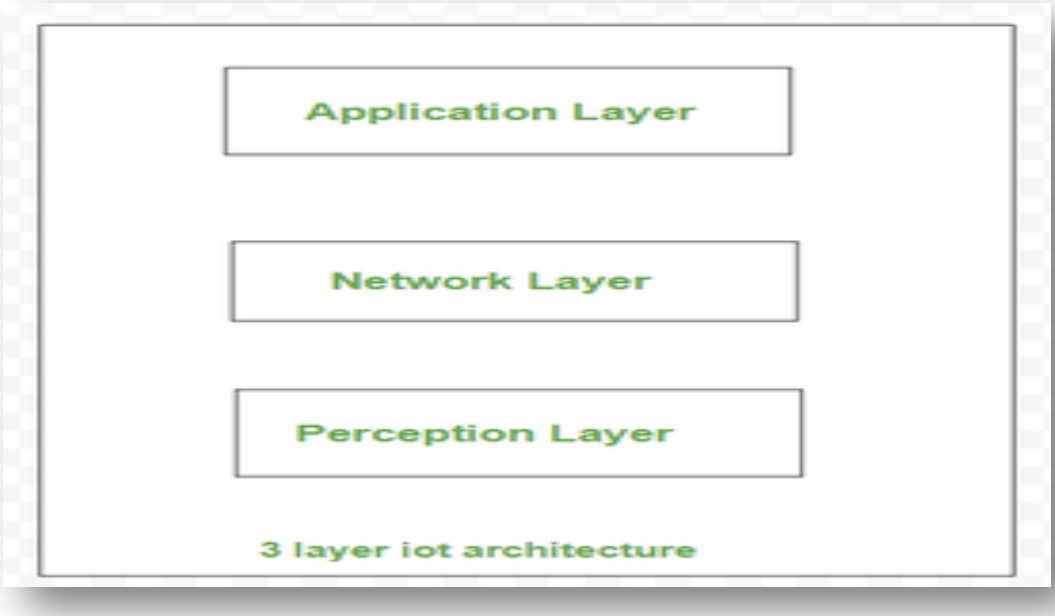

Figure 1: Architectures à trois couches

3.2 Architectures àcinq couches :

L'architecture en trois couches définit le concept central de l'Internet des objets (IdO), mais elle ne suffit pas pour répondre aux exigences de la recherche dans ce domaine, car celle-ci se concentre souvent sur des aspects plus spécifiques de l'IdO. C'est pourquoi une architecture en cinq couches a été définie. Les rôles des couches de perception et d'application dans cette architecture sont similaires à ceux de l'architecture en trois couches. Les trois autres couches ont les fonctions suivantes :

- **la couche transport** : est responsable de l'envoi des données collectées au Cloud ou à l'appareil périphérique pour traitement. La couche de transport s'appuie sur des passerelles Internet pour déplacer les données de la couche de perception physique vers la phase de traitement[5].
- **La couche de traitement** : une fois que les données atteignent le Cloud ou l'appareil périphérique, le serveur peut transformer ces données en informations. Les architectures IoT modernes tirent parti de l'apprentissage automatique et de l'intelligence artificielle qui créent de la valeur en analysant ces données[5].
- **La couche métier** : enfin, nous arrivons à la couche métier, où l'information est transformée en intelligence économique qui guide la prise de décision. Les parties prenantes et les dirigeants peuvent utiliser les informations collectées au niveau de la couche d'application pour prendre de meilleures décisions commerciales[5].

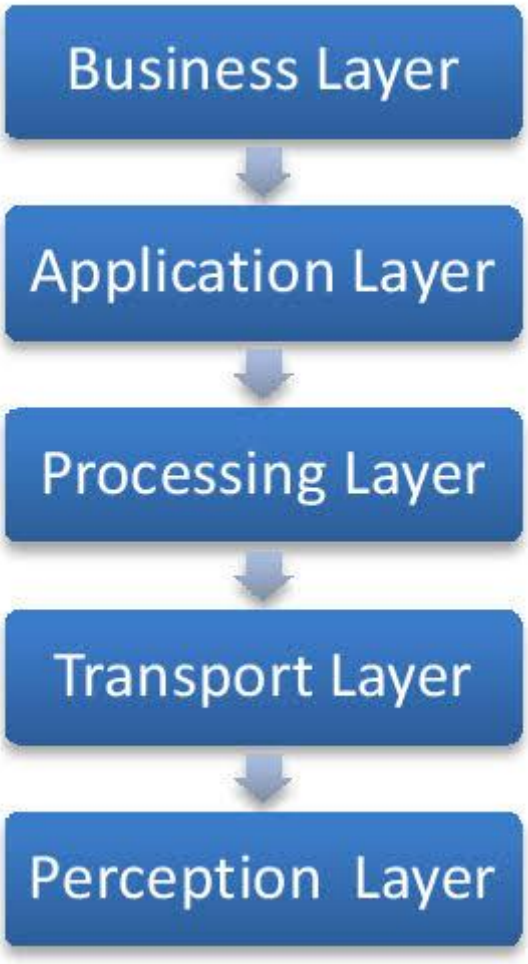

Figure 2 : Architectures à cinq couches.

4 LES PROTOCOLES DE COMMUNICATION DE L'INTERNET DES OBJETS :

Il existe des options de connectivité presque distinctes pour s'adapter aux applications modernes. Ces cellules sont basées sur des produits et des systèmes liés à l'IoT. Les principales technologies de communication IoT sont présentées dans la figure suivante

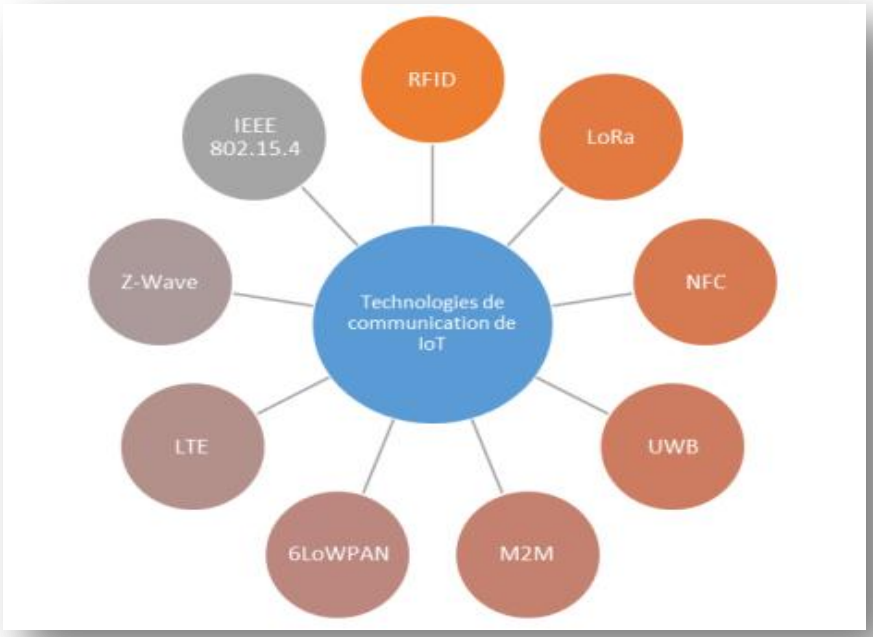

Figure 3 : Les Protocoles de communication de l'internet Des Objets[6]

4.1 Identification par radiofréquence (RFID) :

Les technologies d'identification par radiofréquences (RFID), également connues sous le nom de « Radio Frequency IDentification », permettent d'identifier à distance, à l'aide d'ondes radio, tout objet équipé d'une étiquette RFID. Cette étiquette peut être lue par un lecteur externe qui collecte et transmet les informations contenues dans l'étiquette. Ce mode d'identification, qui ne nécessite aucun contact entre les étiquettes et le lecteur, répond à de nombreux besoins. Les technologies RFID sont aujourd'hui en plein essor, avec des applications déjà largement répandues. Elles couvrent divers domaines allant de la détection à distance aux transactions de la vie quotidienne (titres de transport en commun, télépéage, étiquettes sur les emballages, etc.) et contribuent à

améliorer la traçabilité des produits et des marchandises [6].

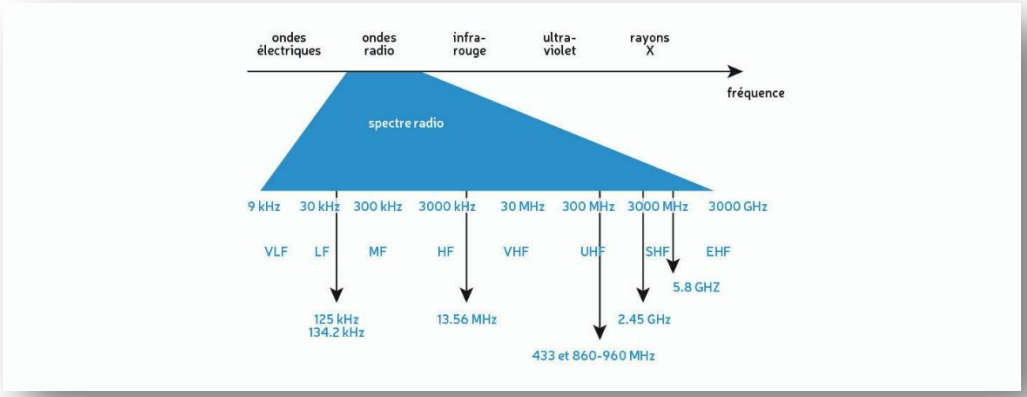

Figure 4 : Fonctionnement de la RFID.

4.2IEEE 802.15.4 :

Le protocole IEEE 802.15.4 a été développé pour définir une sous-couche de contrôle d'accès au support (MAC) ainsi qu'une couche physique (PHY) pour les réseaux sans fil à faible débit appelés LR-WPAN (Low-Rate Wireless Personal Area Networks) [7]. En raison de ses caractéristiques telles qu'une consommation d'énergie réduite, un faible débit de données, un coût abordable et une capacité élevée de traitement des messages, il est également utilisé dans des domaines tels que l'IdO (Internet des Objets), la communication entre machines (M2M) et les réseaux de capteurs sans fil (WSN). Il offre une communication fiable, une interopérabilité entre différentes plateformes et peut prendre en charge un grand nombre de nœuds (environ 65 000). De plus, il propose des services de sécurité avancés tels que le chiffrement et l'authentification. Cependant, il ne garantit pas la qualité de service. Ce protocole constitue la base du protocole ZigBee, car tous deux se concentrent sur la fourniture de services à faible débit de données pour des dispositifs à consommation d'énergie limitée et construisent une pile de protocoles réseau complète pour les WSN. IEEE 802.15.4 prend en charge trois bandes de fréquences et utilise la technique de diffusion en séquence directe (DSSS). En fonction des canaux de fréquences utilisés, la couche physique transmet et reçoit des données à des débits de 250 kbps à 2,4 GHz, 40 kbps à 915 MHz et 20 kbps à 868 MHz. Les fréquences plus élevées et les bandes plus larges offrent un débit plus élevé et une latence réduite, tandis que les fréquences plus basses permettent une meilleure sensibilité et une couverture étendue. Pour

minimiser les collisions potentielles, la couche MAC de l'IEEE 802.15.4 utilise le protocoleCSMA/CA[8].

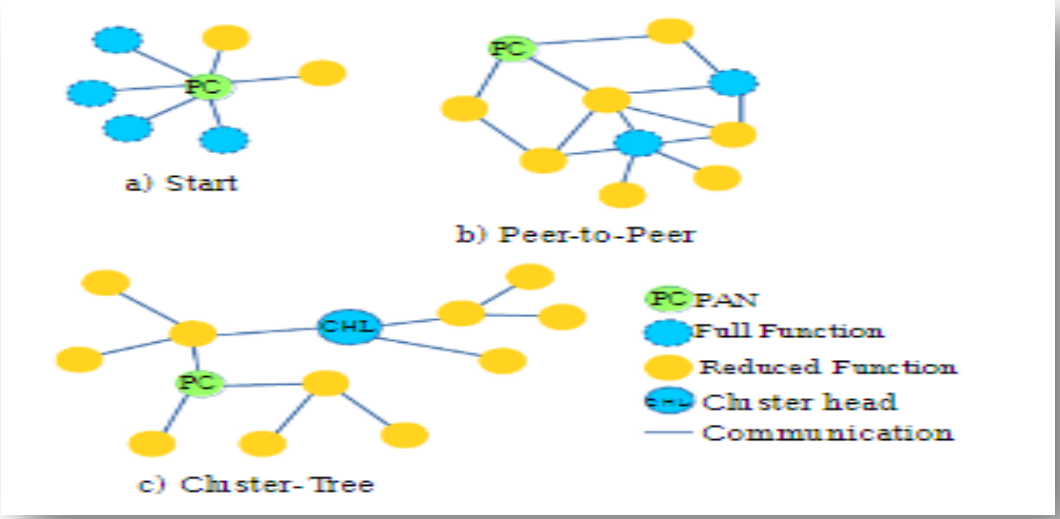

Figure 5: les topologies de IEEE 802.15.4

4.3 Near-field communication (NFC) :

La communication en champ proche (NFC) est une technologie sans fil à courte portée qui utilise l'induction de champ magnétique pour permettre la communication entre les appareils lorsqu'ils sont en contact ou à quelques centimètres l'un de l'autre. Cela englobe des fonctionnalités telles que l'authentification des cartes de crédit, l'activation d'accès physique, le transfert de petits fichiers et l'établissement de connexions sans fil plus rapides. En général, NFC repose sur les écosystèmes et les normes existants autour des étiquettes d'identification par radiofréquence (RFID) et étend leurs capacités.

NFC étend les fonctionnalités RFID et sans contact en ajoutant des fonctionnalités plus dynamiques activées par les smartphones modernes. Tous les téléphones modernes prennent désormais en charge les puces et les applications NFC, telles que ApplePay et Google Pay, afin de tirer parti des milliards d'étiquettes et de terminaux RFID déjà déployés. NFC facilite le regroupement de plusieurs cartes dans un seul téléphone pour les paiements, les transports en commun, l'accès aux bâtiments, l'ouverture des portes de voiture et d'autres cas d'utilisation. NFC prend en charge des applications interactives basées sur les fonctionnalités RFID de base, comme le couplage automatique d'écouteurs Bluetooth et les connexions Wi-Fi. Il peut

également extraire automatiquement des données ou des applications à partir d'affiches ou de publicités [9].

5 *LES PROTOCOLES DE ROUTAGES DE L'INTERNET DES OBJETS :*

5.1 IPv6 Low-power Wireless Personal Area Network (6LoWPAN) :

Le protocole 6LoWPAN est une norme de communication utilisée dans les réseaux de capteurs à faible puissance et à pertes. Il opère au niveau de la couche 2 du modèle OSI et utilise une topologie de réseau maillé. Ce protocole a été développé pour être compatible avec les adresses IPv6, qui sont plus longues et complexes que celles utilisées dans les réseaux IPv4 traditionnels. Il est spécifiquement conçu pour offrir une efficacité élevée en termes de bande passante et d'utilisation de l'énergie, ce qui le rend particulièrement adapté aux dispositifs à faible puissance tels que les nœuds de capteurs.

Les réseaux 6LoWPAN sont couramment utilisés dans les domaines suivants :

- Applications industrielles.
- Domotique.
- Connexion d'appareils intelligents dans l'Internet des objets.
- Suivi des actifs.
- Surveillance de l'environnement.
- Suivi des soins de santé et de la condition physique.

Les avantages de cette technologie sont les suivants :

- Elle est spécifiquement conçue pour les appareils à faible consommation, ce qui la rend bien plus efficace en termes de consommation d'énergie par rapport aux protocoles traditionnels tels que l'IPv4.
- 6LoWPAN utilise une topologie de réseau maillé, ce qui offre une plus grande fiabilité et une plus grande flexibilité en termes de réseau.
- Elle permet à des dispositifs ayant des capacités de traitement et de mémoire limitées de communiquer efficacement sur des réseaux sans fil [10].

5.2Routing Protocol for Low Power and Lossy Networks (RPL) :

Le groupe de travail IETF Routing over low-power and lossy links (ROLL) a standardisé le protocole de routage RPL, basé sur IPv6, pour les nœuds à ressources limitées. RPL a été développé dans le but de répondre aux exigences minimales de routage en établissant une topologie robuste sur des liaisons avec perte. Ce protocole de routage prend en charge des modèles de trafic variés tels que le multipoint à point, le point à multipoint et le point à point. Le cœur de RPL est représenté par un graphe acyclique orienté vers la destination (DODAG), qui décrit le schéma de routage des nœuds. Le DODAG est un graphe acyclique dirigé avec une seule racine.

Chaque nœud du DODAG est conscient de ses parents, mais il n'a aucune information sur les nœuds enfants associés. De plus, RPL maintient au moins un chemin pour chaque nœud vers la racine, ainsi qu'un parent préféré permettant de suivre un chemin plus rapide et d'améliorer les performances.

Pour maintenir la topologie de routage et mettre à jour les informations de routage, RPL utilise quatre types de messages de contrôle. Le plus important d'entre eux est l'objet d'information DODAG (DIO), utilisé pour conserver le rang actuel du nœud, déterminer la distance de chaque nœud par rapport à la racine en fonction de certaines métriques spécifiques, et sélectionner le parent préféré. Un autre type de message est l'objet d'annonce de destination (DAO). RPL prend en charge à la fois le trafic ascendant et le trafic descendant en utilisant des messages DAO pour diffuser des informations de destination aux parents sélectionnés. Le troisième message est la sollicitation d'informations DODAG (DIS), utilisée par un nœud pour acquérir des messages DIO à partir d'un nœud adjacent accessible. Enfin, le dernier type de message est l'accusé de réception de DAO (DAO-ACK), qui est une réponse à un message DAO et est envoyé par un nœud destinataire DAO, tel qu'un parent DAO ou une racine DODAG.

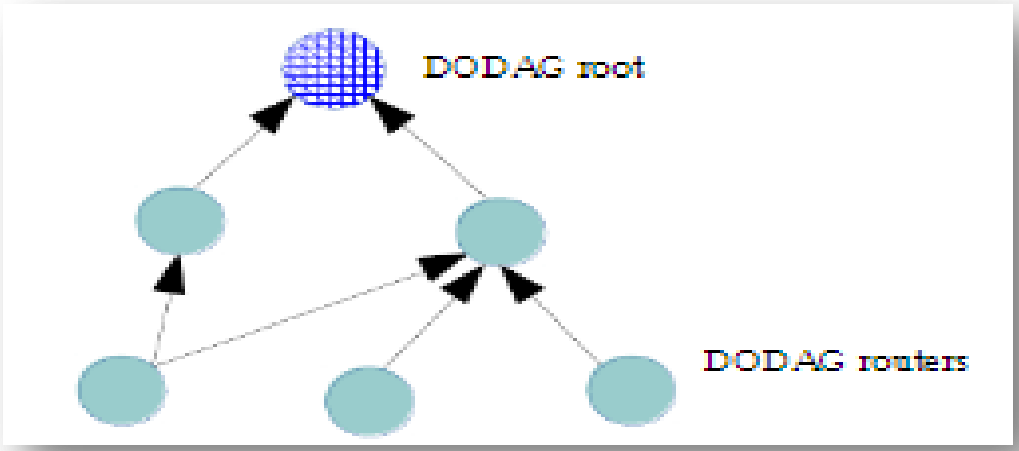

Figure 6 : la topologie de DODAG.

La formation d'un DODAG débute lorsque la racine, étant le seul nœud composant le DODAG, envoie son emplacement aux différents niveaux du réseau à faible puissance et à pertes (LLN) à l'aide d'un message DIO. À chaque niveau, les routeurs destinataires enregistrent le chemin parent et les chemins de participation pour chaque nœud, puis ils propagent leurs propres messages DIO, permettant ainsi une construction progressive du DODAG. Une fois que le DODAG est construit, le parent préféré obtenu par un routeur devient le chemin par défaut vers la racine (routes ascendantes). La racine peut également stocker des informations de destination pour les itinéraires ascendants. Pour prendre en charge les routes descendantes, les routeurs doivent émettre et diffuser des messages DAO unicast à la racine via les parents. Ces messages identifient le nœud correspondant à un préfixe de route ainsi que la route à suivre.Les routeurs RPL fonctionnent selon l'un des deux modes de fonctionnement (MOP) : sans stockage ou avec stockage. En mode sans stockage, RPL achemine les messages vers les niveaux inférieurs en se basant sur le routage source IP, tandis qu'en mode stockage, le routage descendant est basé sur les adresses IPv6 de destination. Dans un exemple de code présenté dans une référence pour un réseau de capteurs sans fil, ContikiRPL est utilisé comme implémentation du protocole RPL pour acheminer les paquets[11].

6 VULNERABILITES ET MENACES DANS L'INTERNET DES OBJETS :

Une fois connectés à Internet, tous les types d'appareils sont susceptibles d'être exposés aux risques de sécurité liés à l'IoT. En effet, cette vaste infrastructure interconnectée contenant une multitude d'informations sensibles présente des vulnérabilités. Voici certains des dangers potentiels auxquels les objets connectés sont confrontés [12] :

- **Manque de renforcement physique :**

  Le déploiement à distance des appareils de l'IOT les expose en permanence aux attaques physiques, car nombreux d'entre eux ne sont pas sécurisés quant à leur emplacement. De plus l'absence de surveillance continue offre aux cybercriminels des opportunités d'attaques à distance et de prise de contrôle.

- **Non sécurisation du stockage et du transfert de données :**

  Le stockage des données sur le cloud présente de nombreux avantages pour l'IoT, mais il comporte également un risque élevé de violation des données si des pirates parviennent à les compromettre. Ce danger provientprincipalement du manque de sécurité et de cryptage lors du stockage et du transfert des données. Les mesures de sécurité telles que les pare-feux et les contrôles d'accès robustes ne sont souvent pas mises en place.

- **Absence de surveillance et de gestion des appareils :**

  Avec l'essor des objets connectés, notamment dans les projets de villes connectées, la sécurité de l'IOT est de plus en plus préoccupante, en particulier en l'absence de surveillance et de gestion des appareils. Cette lacune entraine un manque de détection surveillance adéquat pour faire face à ces défis.

- **Les botnets :**

  Les botnets sont conçus pour infiltrer les réseaux et les systèmes, et leur grande capacité d'adaptation leur permet de facilement accéder aux appareils peu sécurisés.

  Pour réduire les risques pour la sécurité de l'IOT, il est important de surveiller en permanence l'évolution de ces bot nets et de prendre les mesures appropriées.

- **La vulnérabilité des codes d'accès :**

Les mots de passe faibles peuvent créer une brèche dans le réseau et faciliter les piratages. Afin de sécuriser efficacement l'accès à un compte ou à un système, il est essetiel d'utiliser des mots de passe de niveau élevé et d'éviter d'utiliser des chiffres liés directement à l'utilisateur.

- **Interfaces de programmation d'applications(API) non sécurisées :**
  Les interfaces de programmation d'applications(API) permettent aux serveurs de se connecter, mais lorsqu'elles ne sont pas sécurisées, elles ouvrent une fenêtre d'attaque pour les cybercriminels. Il est donc recommandé de vérifier la sécurité de la connexion et l'écosystème de l'appareil avant-garde. Ainsi, il existe un risque pour la sécurité de l'IOT**[12] .**

7LES ATTAQUES DES ROUTAGES RPL SUR L'IOT :

La multitude de menaces qui présent sur l'Internet des Objets et les vulnérabilités qui s'en suivent rendent possibles de nombreuses attaques sur ces systèmes. Les éléments de l'IoT sont sensibles aux mêmes attaques que les systèmes informatiques.

7.1 Les attaques basées sur les ressources :

Ce genre d'attaque a deux types [13]:

- **Les attaques directes :**
  Hello Flooding (DIO Flooding) : Hello Floodingattack est une attaque où un nœud attaquant envoie des messages hello périodiquement aux nœuds voisins pour perturber le réseau.
- **Les attaquesindirectes :**
  Increase Rank Attack :C'est lorsque le nœud attaquant change son rang pour un rang supérieur dans le but d'être plus loin de la racine

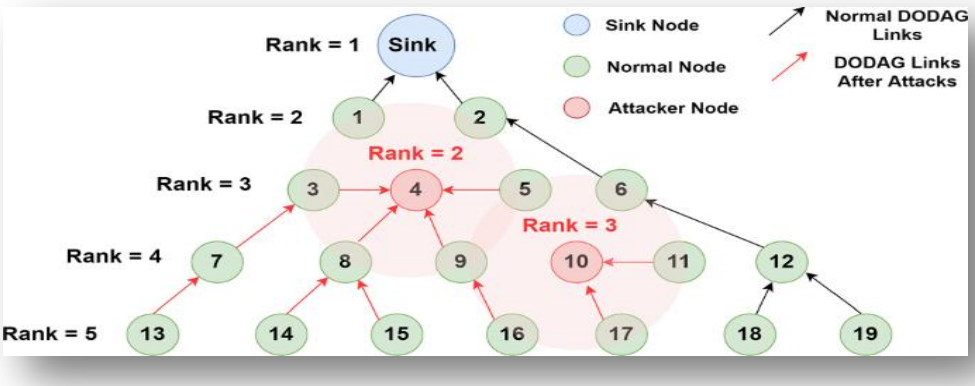

Figure 7 : Illustration de l'attaque Increase Rank Attack.

7.2 Les attaques basées sur la topologie :

Ce genre d'attaque a de types :

- **Les attaques de sous-optimisations :**

  SinkHoleAttack Il s'agit d'une attaque où le nœud compromis tente d'attirer le trafic réseau en se faisant passer pour un nœud légitime dans le processus de routage. Elle bloque la station de base dans l'obtention des informations légitimes, provoque une menace et ouvre la voie à d'autres attaques aussi. Le nœudcompromiseessayer de supprimer les paquets.

- **Les attaquesd'isolements :**

  Black-HoleAttack: Dans cette attaque le nœud attaquant prétend qu'il a le chemin le plus court vers la destination après avoir illégalement changé son rang. Il abandonne les paquets de routage reçu de ses victimes et ne propage pas les paquets au point précis de destination.

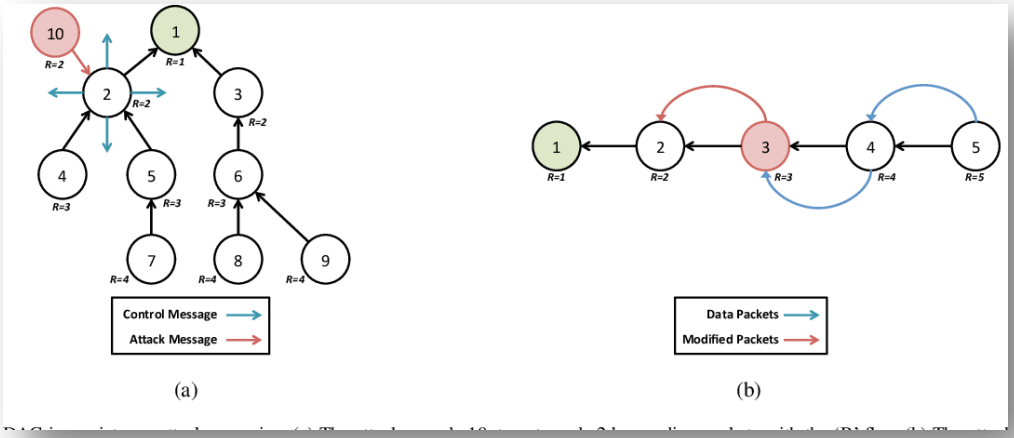

Figure 8: Illustration de l'attaque Black Hole.

7.3 Les attaques basées sur le trafic :

Ce genre d'attaque a deux types :

- **Les attaquesd'écoute clandestine :**

  SniffingAttack : Cette attaque consiste à écouter les paquets transmis sur le réseau à l'aide d'un nœud compromis ou par capture direct des paquets sur le support de partage dans le cas des réseaux sans fil.

- **Les attaquesd'imitations :**

  Clone ID : C'est lorsqu'un nœud malveillant prétend être un nœud existant légitime. Après avoir reniflé les informations du trafic réseau et identifié la racine (root), il usurpe son adresse et prend le contrôle du DODAG.

8 EXIGENCES DE LA SECURITE DANS L'IOT :

Le système IoT requiert une sécurité en raison des problèmes de sécurité associés. Ainsi, pour garantir cette sécurité, il est nécessaire de mettre en place un système IoT sécurisé qui respecte les paramètres traditionnels de demande de sécurité suivants [14]:

- ***Authenticité:*** Les informations reçues par un lecteur doivent être vérifiables, qu'elles proviennent d'une étiquette électronique authentifiée ou non.
- ***Intégrité:*** Lors de la transmission des informations via l'IoT, l'intégrité des données est essentielle pour garantir l'authenticité des informations. Il est crucial de s'assurer que les informations transmises ne sont pas altérées, c'est-à-dire qu'elles ne sont pas modifiées, copiées ou remplacées par un attaquant.
- ***Confidentialité:*** Le système IoT sécurisé doit protéger la confidentialité des utilisateurs individuels, tels que leur identité ou leurs informations commerciales confidentielles.
- ***Disponibilité:*** Les utilisateurs autorisés doivent pouvoir accéder aux différents services fournis par l'IoT, tout en empêchant les attaques par déni de service (DoS) qui compromettent la disponibilité des services. Les attaques DoS sont une menace majeure pour la disponibilité.

9 LES DÉFIS DE LA SÉCURITÉ IOT :

Pour mettre en place et gérer efficacement la sécurité IoT, il est nécessaire d'adopter une approche holistique qui englobe une variété de tactiques et d'outils, tout en tenant compte des systèmes adjacents tels que les réseaux. Trois fonctionnalités clés pour assurer une solution de sécurité IoT robuste sont les suivantes [15]:

- ***Apprentissage :*** Profiter des solutions de sécurité qui offrent une visibilité sur le réseau pour comprendre la portée de l'écosystème IoT et évaluer les profils de risque pour chaque groupe d'appareils IoT.
- ***Protection :*** Surveiller, inspecter et appliquer les politiques de sécurité IoT en accord avec les activités à différents niveaux de l'infrastructure.
- ***Segmentation :*** Tout comme les réseaux sont segmentés, utiliser la segmentation basée sur les groupes de politiques et les profils de risque pour segmenter les systèmes IoT.

Les fonctionnalités spécifiques requises pour sécuriser les appareils IoT comprennent [15]:

- Sécurité des API.
- Inventaire plus large et approfondi des appareils IoT.
- Mises à jour logicielles continues.
- Filtrage DNS.
- Sensibilisation et formation du personnel, des fournisseurs et des partenaires.
- Chiffrement des données au repos et en transit.
- Authentification multi-facteur.
- Surveillance et analyse du trafic réseau.
- Gestion des mots de passe.
- Gestion des correctifs.
- Utilisation de passerelles de sécurité.
- Détection d'appareils IoT non autorisés par le biais d'analyses.

CONCLUSION:

Ce chapitre aborde les vulnérabilités de l'IoT face à de nombreuses attaques et menaces, en se concentrant sur l'Internet des objets et ses protocoles, notamment le protocole de routage RPL. Nous avons également discuté de certains concepts relatifs à la sécurité de l'Internet des objets et de leurs problèmes. Le chapitre suivant se concentrera sur les systèmes de détection d'intrusion (IDS).

CHAPITRE 2 : LES SYSTEMES DE DETECTION D'INTRUSION (IDS)

INTRODUCTION

L'avènement d'Internet a révolutionné le paysage de l'informatique tel que nous le connaissions. Les possibilités et les opportunités offertes sont désormais illimitées, mais cela s'accompagne également de risques et de possibilités de percées. Par conséquent, la question de la sécurité devient de plus en plus préoccupante. Il est donc essentiel d'établir un mécanisme de surveillance et de contrôle de ces activités. Dans ce contexte, nous présentons un mécanisme intéressant appelé IDS (système de détection d'intrusion) [16].

1 LE SYSTEME DE DETECTION D'INTRUSION :

Le premier modèle de détection d'intrusion est développé en 1984 par Dorothy Denning et Peter Neuman, qui s'appuie sur des règles de l'approche comportementale. Ce système appelé (Intrusion Détection Expert System), en 1988 Il est développé à un IDS (système de détection d'intrusion)[17] .

Ce dernier et un logiciel conçus pour surveiller le trafic réseau entrant et sortant afin de découvrir les irrégularités, les activités suspectes ainsi que les activités malveillantes. Ils alertent les responsables informatiques lorsque des activités suspectes sont découvertes. Un administrateur examine ensuite les alarmes et prend des mesures pour supprimer la menace.

Si par exemple des logiciels malveillants ont réussi à pénétrer votre réseau, l'IDS en place les détectera s'ils sont visibles au niveau des données transportées par le trafic réseau. Et dès qu'une menace est détectée, quasiment au même moment, la solution IDS déclenche une alerte qui sera diffusée à l'équipe de sécurité afin qu'elle puisse enquêter et y remédier [18].

Exemple : Cisco Secure IDS ,ISS RealSecure, Symantec IDS ,Checkpoint SmartDefense ..

2 LES TYPES DE SYSTEME DETECTION D'INTRUSION :

Il existe plusieurs manières de classer les systèmes de détection d'intrusion qui ont été décrites à l'aide de différentes méthodes d'analyse et de surveillance, il y-a trois grandes familles distinctes d'IDS :

2.1 La détection d'intrusion basée sur l'hôte :

L'HIDS (Host Based IDS) surveille le trafic sur une seule machine en analysant les journaux systèmes, les appels, et en vérifiant l'intégrité des fichiers. Cependant, pour garantir l'intégrité des données.Le système doit être sain. Si le système a été compromis par un pirate, le HIDS ne sera plus efficace. (Les sondes de sécurité IDS/IPS) .

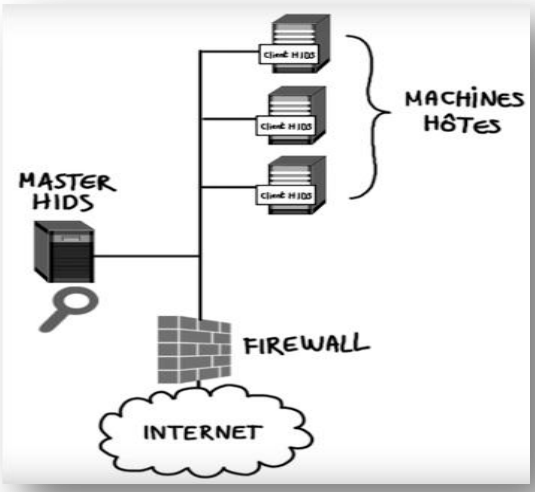

Figure 9: Exemple d'un Schéma d'architecture HIDS[19].

Avantages :

- Découvrir plus facilement un Cheval de Troie puisque les informations et les possibilités sont très étendues.
- Détecter des attaques impossibles à détecter avec des IDS réseau puisque le trafic est souvent crypté.
- Surveiller les activités du système.
- le HIDS analysera les programmes en cours et leur utilisation des ressources.

Inconvénients :

- Ils ont moins de facilité à détecter les scans.
- Ils sont plus vulnérables aux attaques de type DoS.
- Ils consomment beaucoup de ressources CPU.

2.2 La détection d'intrusion réseau NIDS (Network Intrusion Detection System) :

Les NIDS sont des IDS utilisés pour protéger les réseaux en écoutant et surveillant en temps réel tout le trafic réseau. Ils analysent ensuite les données et génèrent des alertes s'ils détectent des intrusions ou des paquets potentiellement [19]

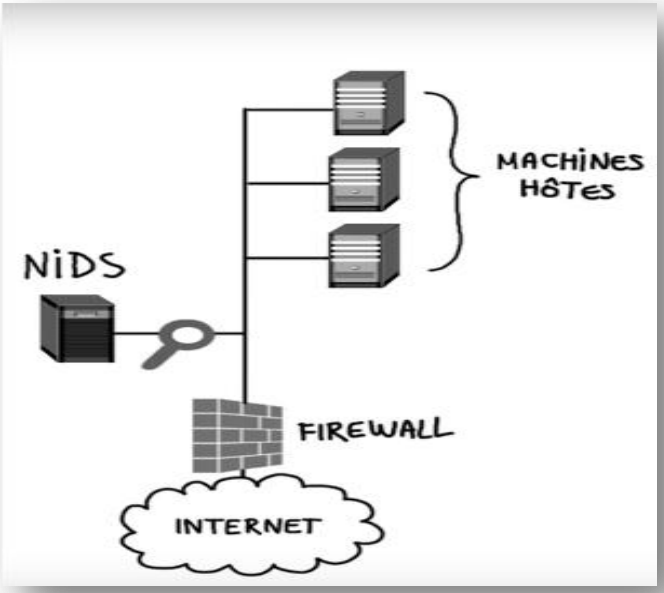

Figure 10 : Exemple d'un Schéma d'architecture NIDS[19].

Avantages:

- Les capteurs peuvent être bien sécurisés puisqu'ils se contentent d'observer le trafic.
- Détecter plus facilement les scans grâce aux signatures.
- Filtrage de trafic.
- assurer la sécurité contre les attaques puisqu'il est invisible.
- Facile à appliquer, car il n'a aucun impact sur les systèmes ou l'infrastructure standard.
- le NIDS permet d'analyser le trafic réseau.

Inconvénients:

- NIDS peut ne pas reconnaître l'attaque lorsque la taille du réseau devient trop grande.
- NIDS ne peut pas analyser les paquets chiffrés, ce qui rend une partie du trafic invisible pour le processus, ce qui réduit l'efficacité de NIDS.
- Les attaques impliquant des paquets corrompus ou fragmentés ne sont pas facilement détectées.

2.3 Système de détection d'intrusion Hybride :

Les IDS hybrides combinent les caractéristiques des NIDS et HIDS pour surveiller à la fois le réseau et les terminaux. Les sondes sont placées a des points stratégiques et agissent comme des NIDS et/ou HIDSen fonction de leurs emplacements. Les alertes remontent ensuite à une machine centrale qui les centraliser et relier les informations d'origines multiples. Les IDS hybrides utilisent une architecture distribuée dans laquelle chaque composant unifie son format d'envoi, permettant une communication et une extraire d'alertes plus précises[19].

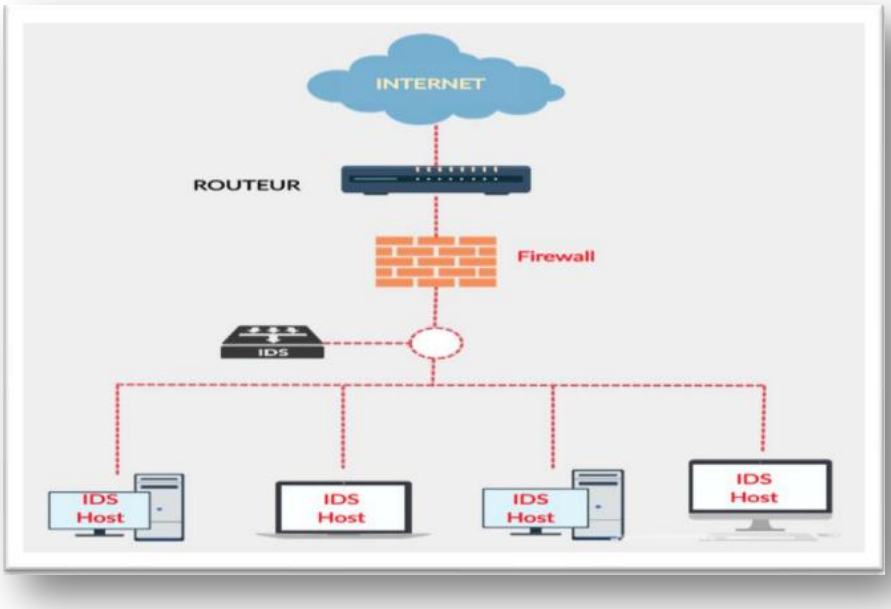

Figure 11 : Exemple d'une architecture d'Hybride[19] .

Avantages :

- moins de faux positifs.

- meilleure corrélation (la corrélation permet de générer de nouvelles alertes à partir de celles existantes).
- possibilité de réaction sur les analyseurs.

Inconvenients:

- taux élevé de faux positifs.

Exemple: Prelude et OSSIM .

3 ARCHITECTURE D'UN IDS:

L'architecture de base d'un système de détection d'intrusion est composée de trois modules :

- **Capteurs(Sensor)** :c'est le responsable de filtrer et de formater les informations brutes envoyées par la source de données. Le résultat de ce traitement sera un message formaté, appelé aussi événement, il représente l'unité de base dans un scenario d'attaque[20].
- **Analyseur(Analyzer) :**Permet d'analyser les événements générés par le capteur. Si une activité intrusive est détectée, une alerte est émise sous un format standard. Dans cette architecture, le capteur et l'analyseur forment ensemble une sonde[20].
- **Gestionnaire(Response /Manager)**: le gestionnaire recueille l'alarme bénéficiaire du capteur et présente les transmettre à l'administrateur pour d'autres activités[21].

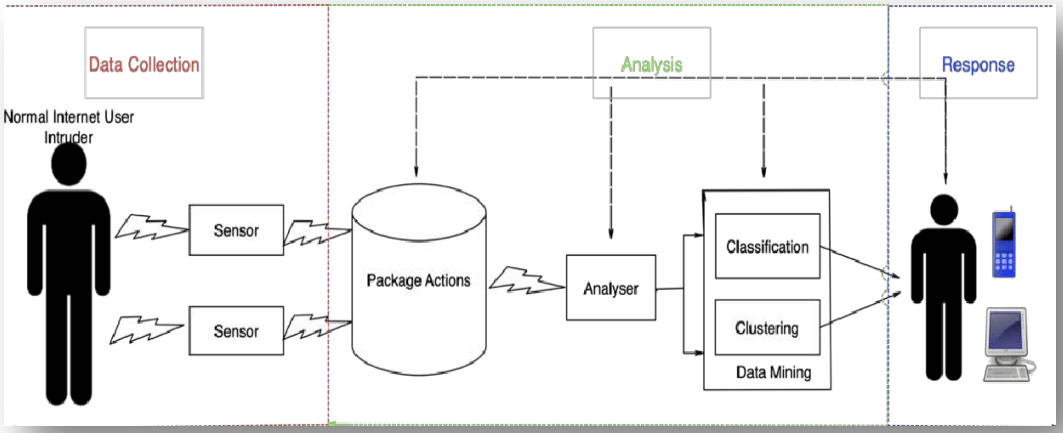

Figure 12 : Schéma d'architecture d'un IDS .

4 CRITERES DE CHOIX D'UN IDS :

Les systèmes de détection d'intrusion sont devenus indispensables lors de la mise en place d'une infrastructure de sécurité opérationnelle. Ils s'intègrent donc toujours dans un contexte et dans une architecture imposants des contraintes très diverses[22]

Certains critères imposant le choix d'un IDS peuvent être dégagés :

- **Fiabilité** :

  Aucune intrusion ne doit pouvoir échapper aux alertes générées. Qui doivent être justifiées. Si une intrusion n'est pas signalée, Cela constitue une défaillance de l'IDS, appelée faux négatif.

- **Pertinence des alertes** :

  Toutes les alertes correspondre à une intrusion effective. Cependant, toute « fausse alerte » (appelée également faux positif) diminue la pertinence de l'IDS. (voir Figure 12), un IDS est considéré comme parfaitement fiable en absence de faux négatif et parfaitement pertinent en l'absence de faux positif.

- **Réactivité** :

  Pour être efficace, un IDS doit être constamment à jour pour être en mesure de détecter rapidement les nouveaux types d'attaque. Des capacités de mise à jour automatique sont indispensables.

- **Facilité de mise en œuvre et adaptabilité** :

Un IDS doit être facile à mettre en œuvre et s'adapter au contexte dans lequel il doit opérer.

Il est inutile d'avoir un IDS émet des alertes en moins de 10 secondes si les ressources nécessaires pour réagir dans les mêmes contraintes de temps ne sont pas disponibles.

- **Performance** :

  La mise en place d'un IDS ne doit en aucun cas affecter les performances des systèmessurveillés[22]. De plus, il est essentiel de s'assurer que l'IDS est capable de traiter toutes les informations à sa disposition, car dans le cas contraire il devient facile de masquer les attaques en augmentant la quantité d'information.

5 LES FONCTIONS PRINCIPALES D'UN IDS :

Les IDS proposent les fonctions suivantes**[22]:**

• Détection d'attaques (actives ou passives).

• Génération des rapports.

• Outils de corrélation avec d'autres éléments de l'architecture de sécurité.

• Réaction aux attaques par le blocage de route ou la fermeture de connexion.

6 CHOIX DU PLACEMENT D'UN IDS :

Il y a plusieurs emplacements stratégiques pour placer un IDS (système de détection d'intrusion) dans un réseau local. Le schéma ci-dessous représente un réseau local et les trois positions possibles pour un IDS.

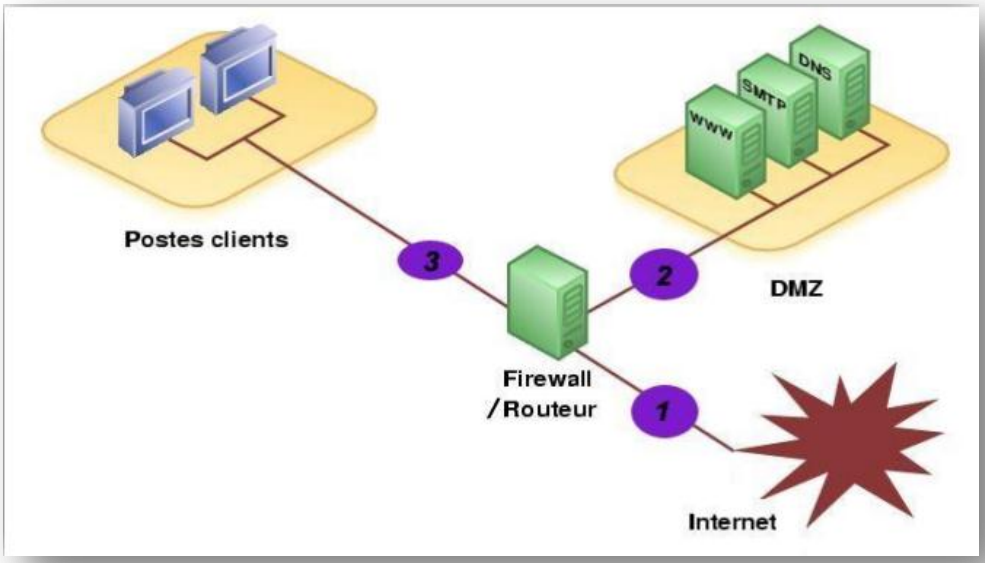

Figure 13 : Choix du placement d'un IDS.

- **Position (1):** L'IDS Sur cette position sert à détecter l'ensemble des attaques frontales, provenant de l'extérieur, vers le firewall. Dans ce cas beaucoup d'alertes seront remontées ce qui rendra les logs difficilement consultables.
- **Position (2):** Si l'IDS est placé sur la DMZ, il détectera les attaques qui n'ont pas été filtrées par le firewall et qui relèvent d'un certain niveau de compétence. Les logs seront ici plus clairs à consulter puisque les attaques bénignes ne seront pas recensées.
- **Position (3):** L'IDS peut ici rendre compte des attaques internes, provenant du réseau local de l'entreprise. Il peut être judicieux d'en placer un à cet endroit étant donné le fait que 80% des attaques proviennent de l'intérieur. De plus, si des trojans ont contaminé le parc informatique (navigation peu méfiante sur internet) ils pourrontêtre ici facilement identifiés pour être ensuite éradiqués.

Idéalement, on placerait des IDS sur les trois positions puis on délèguerait la consultation des logs à l'application "acide" (http://acidlab.sourceforge.net/) qui permet d'analyser les alertes et d'en présenter clairement les résultats via une interface web complète. Si une seule machine peut être déployée, autant la mettre sur la position 2, crucial pour le bon fonctionnement des services.

7 CLASSIFICATION DES SYSTEMES DE DETECTION D'INTRUSION :

Les différents systèmes de détection d'intrusion disponibles peuvent être classés selon plusieurs critères qui sont[23] :

• La méthode de détection.

• Le comportement du système après la détection.

• La source des données.

• La fréquence d'utilisation.

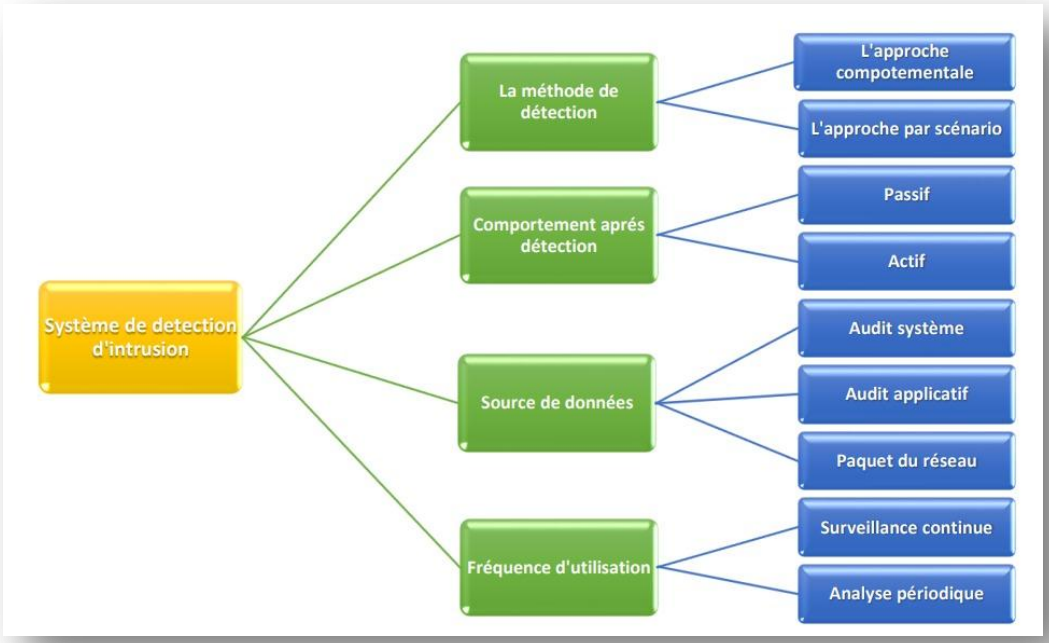

Figure 14 : Classification d'un système de détection d'itrusion [23].

8 METHODES DE DETECTION DES IDS :

Les techniques de détection d'intrusions se répartissent en deux classes :

Détection d'anomalies (approche comportementale), et détection par signature, dite détection de mauvais usage, détection par l'apparence ou encore approche par scénario[24].

8.1 Approche par scénario ou par signature :

Cette méthode repose sur la connaissance des techniques utilisées par les attaquants, stockées dans une base de données. Elle compare ensuite l'activité de l'utilisateur à cette base de données pour détecter les événements qui sortent du cadre normal. Lorsqu'une activité suspecte est identifiée, elle déclenche une alerte pour signaler un potentiel risque[22].

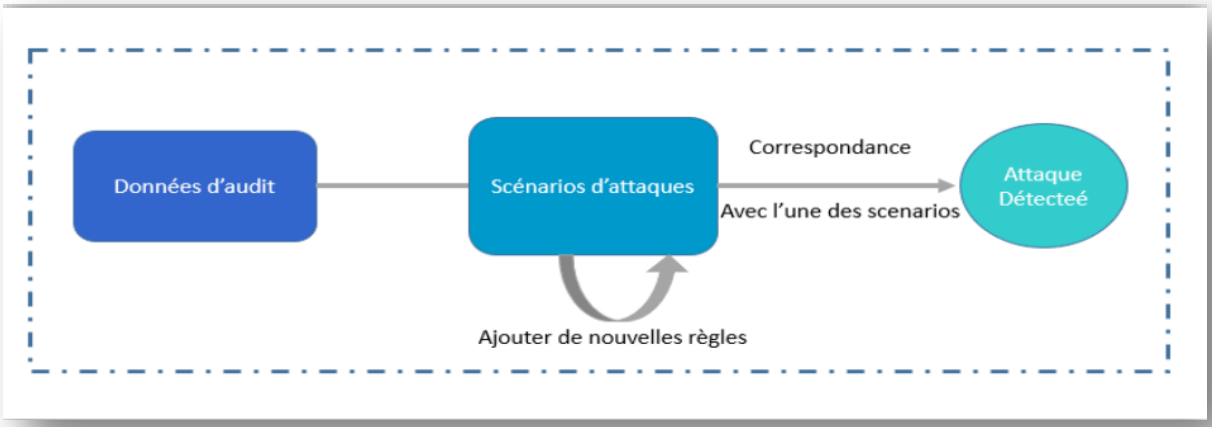

Figure 15 : Fonctionnement d'un IDS par l'approche basée connaissance.

Les avantages de l'Approche par scénario ou par signature :

- Très efficace pour détecter les attaques sans générer un grand nombre de fausses alarmes.
- Difficult à container.

Les inconvénients de l'Approche par scénario ou par signature :

- Détectez uniquement les attaques dont vous avez déjà connaissance.
- Vous devez constamment mettre à jour les signatures des nouvelles attaques.
- Inefficace à haute vitesse, car il doit faire correspondre tous les paquets avec des signatures afin de détecter l'attaque, ce qui nécessite évidemment une grande quantité de ressources informatiques.

8.2 L'approche comportementale (détection d'anomalies):

Cette méthode de détection consiste à surveiller le comportement de l'utilisateur ou d'une application afin de détecter une intrusion. Elle repose sur la création d'un

modèle basé sur le comportement habituel du système, et toute déviation par rapport à ce modèle est surveillée. Ainsi, toute activité suspecte peut être détectée et signalée comme une potentielle intrusion[25].

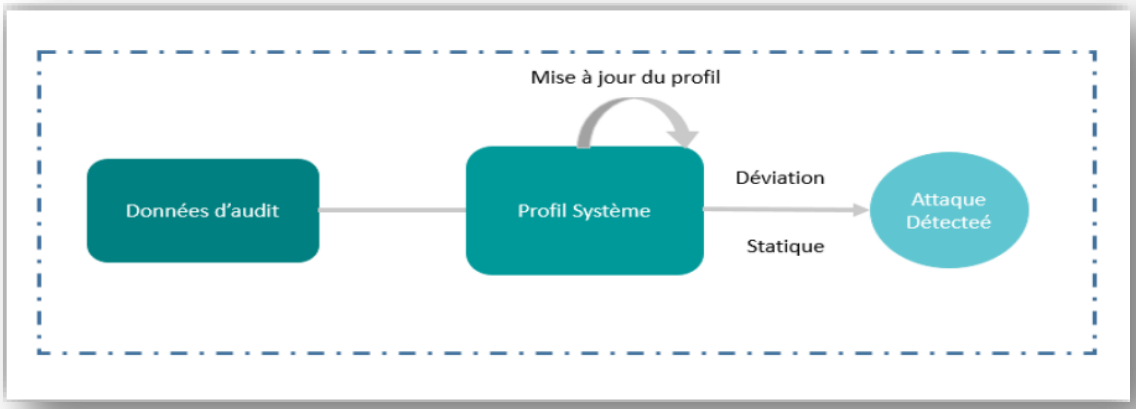

Figure 16 : Fonctionnement d'un IDS par l'approche comportementale.

Les avantages de l'Approche Comportementale (Anomalie) :

- Les informations générées par les détecteurs d'anomalies peuvent être utilisées pour identifier des signatures d'attaque pour les détecteurs d'abus.
- Efficace pour détecter de nouvelles attaques inconnues.
- Il ne nécessite pas d'entretien continu.

Les inconvénients de l'Approche Comportementale (Anomalie) :

- De très grands groupes de formation sont nécessaires pour faire la distinction entre le trafic légitime et illégal.
- Génère un grand nombre de fausses alarmes.
- Il ne peut pas identifier précisément l'attaque, ni savoir si l'attaque a réussi ou non.
- Utilisateur pouvant changer lentement de comportement dans le but d'habituer le système à un comportement intrusif (faux négatif).

8.3 Comparaison entre les deux approches :

Le tableau 1 suivant établi une comparaison entre les caractéristiques des deux précédentes approches

Scénario	Comportementale
Pas de faux positifs	**Faux positifs nombreux**
Pas de détection d'attaques non connues	**Prise en compte de nouvelles attaques**
Mise à jour rapide	**Mise à jour délicate (phase d'entrainement)**

Tableau 1 : Comparaison entre l'approche par scénario et l'approche comportementale

9 LES MESURES D'EVALUATION DE L'IDS :

Il existe de nombreuses mesures de classification pour les IDS, dont certaines sont commues sous plusieurs noms. La figure suivante montre la matrice de confusion pour un classificateur à deux classes, qui peut être utilisée pour évaluer les performances d'un IDS. Chaque colonne de la matrice représente les instances d'une classe prédite, tandis que chaque ligne représente les instances d'une classe réelle. Les IDS sont

Généralement évalués sur la base des mesures de performance standard suivante[26]

Actual Class	Predicted Class		
	Class	Normal	Attack
	Normal	True negative (TN)	False Positive (FP)
	Attack	False Negative (FN)	True positive (TP)

Figure 17: Matrice de confusion pour le système IDS.

- **Taux de vrai positifs(TPR)** : Il est calculé comme le rapport entre le nombre d'attaques correctement prédites et le nombre total d'attaques. Si toutes les intrusions sont détectées, le TPR est de 1, ce qui est extrêmement rare pour un IDS. Le TPR est également appelé taux de détection (DR) ou sensibilité. Le TPR peutêtreexprimémathématiquementcomme suit :

TPR= TP/TP+FN

- **Taux de faux positifs (FPR) :** Il est calculé comme le rapport entre le nombre d'instances normales incorrectement classées comme une attaque et le nombre total d'instances normales :

  FPR=FP/FP+TN

- **Taux de faux négatifs (FNR) :** On parle de faux négatifs lorsqu'un détecteur n'identifie pas une anomalie er classe comme normale. N'identifie pas une Anomalie et la classe comme normale le FNR peut être exprimé mathématiquement comme suit :

  FPR=FN/FN+TP

- **Taux de classification (CR) ou précision : Le** taux de classification (CR) mesure la précision avec laquelle l'IDS détecte un comportement normal ou anormal du trafic. Il est décrit comme le pourcentage de toutes les instances correctement prédites par rapport à toutes les instances :

  Precision= TP+TN/TP+TN+FN+FP

10COMPORTEMENT D'UN IDS EN CAS D'ATTAQUE DETECTEE :

Ils existent deux types d'IDS, actifs et passifs[27] :

10.1 Réponse passive :

La réponse passive d'un IDS consiste à enregistrer les intrusions détectées dans un fichier de log qui sera analysé par le responsable de sécurité ou générer des alarmes, envoi d'un E-mail à un ou plusieurs utilisateurs, etc. Ceci permet de remédier aux failles de sécurité pour empêcher les attaques enregistrées de se reproduire, mais elle n'empêche pas directement une attaque de se produire.

10.2 Réponse active :

La réponse active au contraire a pour but de stopper une attaque au moment de sa détection sans attendre l'intervention humaine. Pour cela on dispose de deux techniques : la reconfiguration du firewall et l'interruption de la session TCP courante. La reconfiguration du firewall permet de bloquer le trafic malveillant au niveau du firewall, en fermant le port utilisé ou en interdisant l'adresse de l'attaquant. Cette fonctionnalité dépend du modèle de firewall utilisé, tous les modèles ne permettant

pas la reconfiguration par un IDS. De plus, cette reconfiguration ne peut se faire qu'en fonction des capacités du firewall. L'IDS peut également interrompre une session établie entre un attaquant et sa machine cible, de façon à empêcher le transfert de données ou la modification du système attaque.

11LIMITER DES IDS :

- Détecter, signaler et répondre instantanément à une attaque, lorsqu'il y a une forte charge de réseau ou de traitement.
- Détection des attaques nouvellement publiées ou des variantes d'attaques existantes.
- Répondre efficacement aux attaques lancées par des attaquants sophistiqués.
- Composer les problèmes de fidélité.
- Traiter efficacement les réseaux commutés[28].

CONCLUSION :

Ce chapitre nous a permis de constater que les IDS sont de plus en plus fiables, d'où le fait qu'ils soient souvent intégrés dans les solutions modernes de sécurité. Les avantages qu'ils présentent par rapport aux autres outils de sécurité les favorisent. Il nous a également permis de comprendre que ces derniers sont indispensables aux entreprises afin d'assurer leur sécurité informatique.

Chapitre3 : Deep Learning

INTRODUCTION

Ces dernières années, l'intelligence artificielle (IA) a fait l'objet d'un engouement médiatique intense. Et il y a un sous-domaine de l'IA qui a particulièrement fait parler de lui : l'apprentissage profond**,** ou *Deep Learning* en anglais[29].

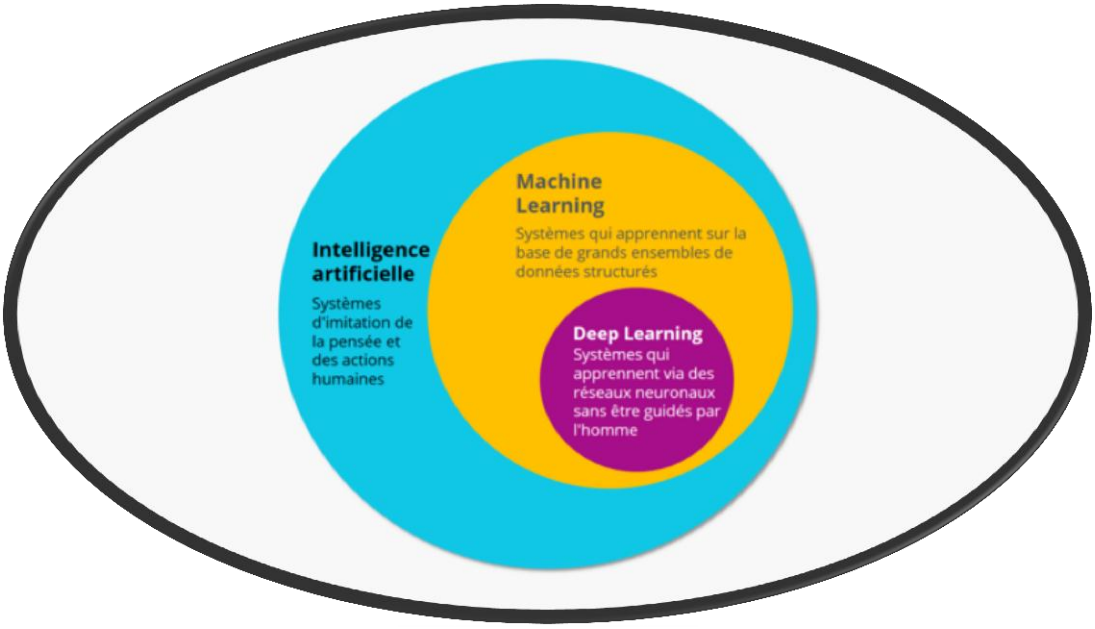

Figure 18:Domaines de l'intelligence artificielle.

1 DEFINITION D'INTELLIGENCE ARTIFICIELLE :

L'intelligence artificielle est un domaine de l'informatique qui vise à créer des machines capables de reproduire des comportements intelligents. Les applications de l'IA sont nombreuses et variées, allant de la reconnaissance de la parole à la conduite autonome en passant par la recommandation de produits[30].

2 L'APPRENTISSAGE AUTOMATIQUE (MACHINE LEARNING) :

3 2.1 DÉFINITION:

L'apprentissage automatique est un sous-domaine de l'intelligence artificielle (IA) qui se concentre sur la conception de systèmes qui apprennent – ou améliorent le rendement – en fonction des données qu'ils consomment. L'intelligence artificielle et l'apprentissage automatique sont souvent évoqués ensemble [31].

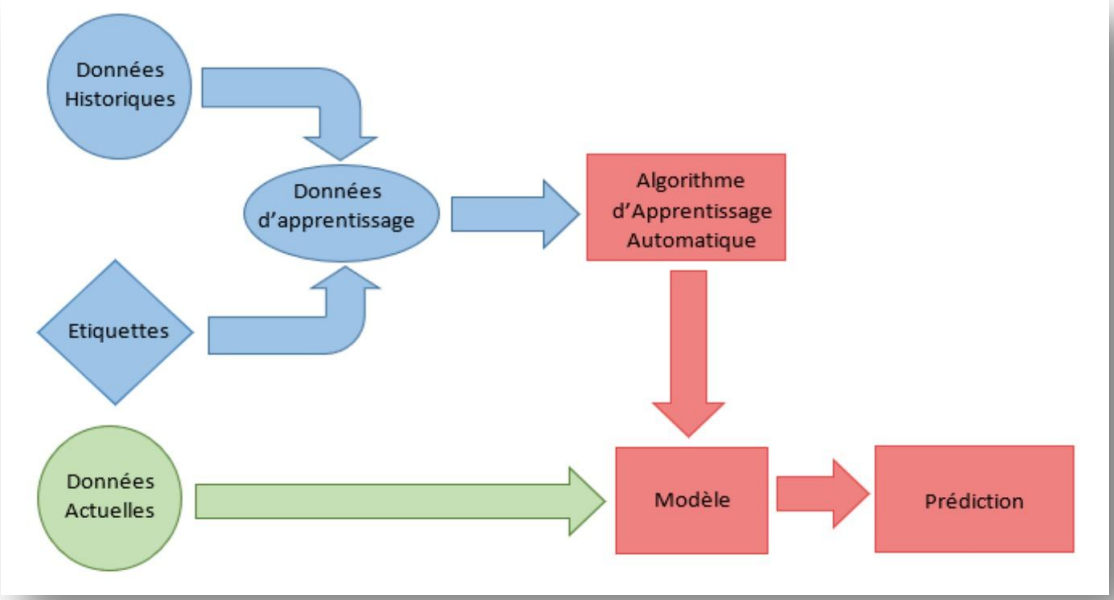

Figure 19 : Méthodes permettant d'apprendre et de prédire des données .

2. 2 Types d'apprentissage :

Il existe trois types d'apprentissage en Machine Learning : l'apprentissage supervisé, l'apprentissage non supervisé et l'apprentissage par renforcement.

- ***Supervisé*** : consiste à entrainer un modèle à partir d'un ensemble de données étiquetées. Le modèle apprend ainsi à prédire la sortie pour de nouvelles entrées[32/33].
- ***Non supervisé*** : consiste à entrainer un modèle à partir d'un ensemble de données non étiquetées. Le modèle apprend ainsi à découvrir des structures ou des relations cachées dans les données.

- ***L'apprentissage par renforcement*** : consiste à entraîner un modèle à partir d'un environnement dans lequel il interagit. Le modèle apprend ainsi à prendre des décisions afin d'optimiser une performance.

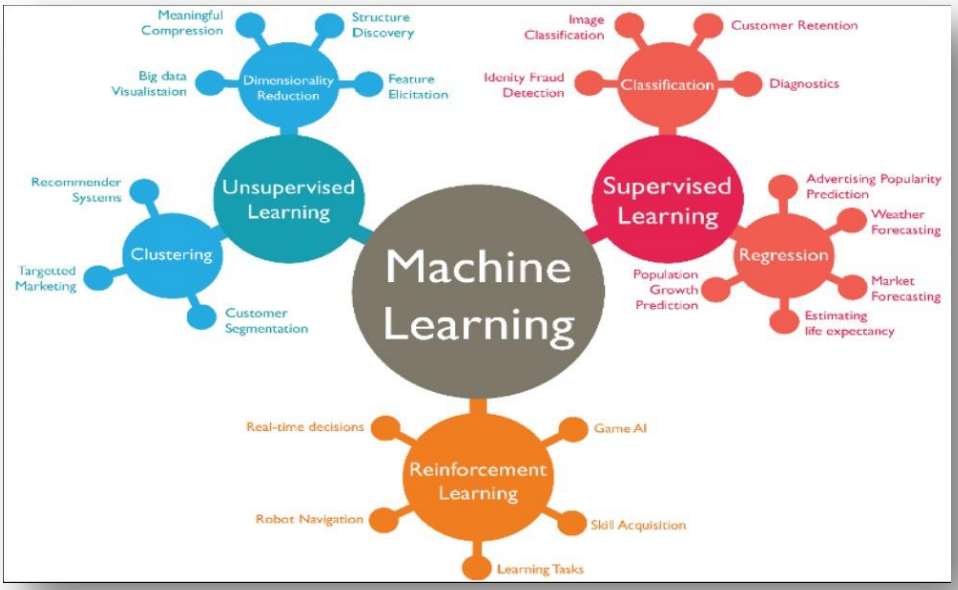

Figure 20: Schéma des différents cas d'utilisation pour un type d'entrainement donné.

4 L'APPRENTISSAGE PROFOND (DEEP LEARNING DL) :

3.1 Définition :

L'apprentissage profonde (Deeplearning ou DL) appartient à une classe de techniques d'apprentissage automatique (machine learning ou ML), il obtient un grand succès dans de nombreuses tâches de l'intelligence artificielle (IA) par rapport aux algorithmes de ML classiques. Les architectures des modèles profondes sont relativement récentes où de nombreuses étapes de traitement non linéaire de l'information sont exploitées, dans lesquelles les informations sont traitées en couches hiérarchiques, chacune recevant et interprétant les informations de la couche précédente pour l'apprentissage des représentations de données [32].

3.2 Compariason entre l'apprentissage automatique et l'apprentissage profond :

On an résumer la comparaison entre les deux types d'apprentissage dans le tableau suivant :

	Apprentissageprofound	Apprentissageautomatique
Exigences en matiére de donneés	Nécessite de grandes qualités de données	Peut s'entrainer sur moins de données
Précision	Fournitunegrandeprecision	Donne moins de precision
Temps de d'éxecution	Prend plus de temps pour s'entrainer	Prend moins de temps pour s'entrainer
Dépendancematérielle	Nécessite un GPU pour s'entrainer correctement	Trains sur CPU
Réglage de hypre-paramétres	Peut etre réglé de différentes maniéres	Capacités de réglagelimitées

Tableau 2 : comparaison entre l'apprentissage profond et l'apprentissage automatique.

3.3 Fonctionnement :

Le fonctionnement de l'apprentissage profond se base sur un réseau de neurones artificiels organisés en couches hiérarchiques.

Tout d'abord un réseau de neurones artificiels est composé de nombreux neurones artificiels reliés entre eux selon une architecture de réseau spécifique.

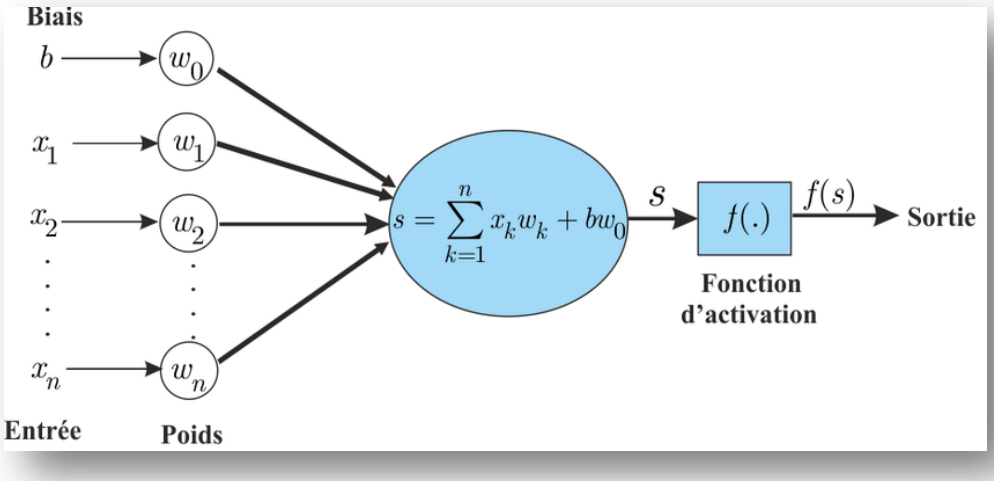

Figure 21: Lastructure d'un neurone artificiel.

L'objectif d'un réseau de neurones est de transformer les entrées en sorties significatives.

Le neurone calcule la valeur de sortie en appliquant une fonction d'activation à une somme pondérée des valeurs d'entrée.

Et fondamentalement, chaque neurone d'un réseau peut être implémenté comme indiqué ci-dessus et il est possible de constater que le neurone artificiel est composé de six éléments de base, à savoir :

- **Entrées** : cela représente les caractéristiques et essentiellement l'ensemble de données entrant dans les réseaux.
- **Poids** : cela représente la dimension ou la force de la connexion entre les unités. Si le poids du nœud 1 au nœud 2 a une quantité plus élevée, alors le neurone 1 a une influence plus considérable sur le neurone 2.
- **Biais** : c'est la même chose que l'interception ajoutée dans une équation linéaire. C'est un neurone spécial ajouté à chaque couche dans le réseau neuronal, qui stocke simplement la valeur de 1 dont la tâche est de modifier la sortie ainsi que la somme pondérée de l'entrée vers l'autre neurone.
- **Somme nette** : elle calcule la somme totale.
- **Fonction d'activation** : un neurone peut être activé ou non, ce qui est déterminé par une fonction d'activation. La fonction d'activation calcule une somme pondérée et ajoute en plus le biais pour donner le résultat [33].
- **Sortie** : elle consiste en la valeur finale produite par le neurone pour un ensemble particulier de signaux d'entrée [34].

3.4 Les couches d'un Réseau de neurone:

En général, un réseau neuronal artificiel peut être divisé en trois parties appelées couches, qui sont connues sous le nom de [34].

- **Couche Entrée: (InputLayer)** c'est l'ensemble de neurones qui porte le signal d'entré du réseau, et par la suite tous les neurones de cette couche sont reliés à la couche suivante.
- **Couche cachée: (Hiddenlayers)** elles peuvent être une ou plusieurs, c'est ici où les relations entre les variables vont être mises en exergue. Le choix du nombre de couches et de neurones est intuitif et nécessite de l'expérience venant de l'expert.
- **Couche sortie: (OutputLayer)** elle représente le résultat du réseau de neurones c'est ce qu'on appelle la prédiction.

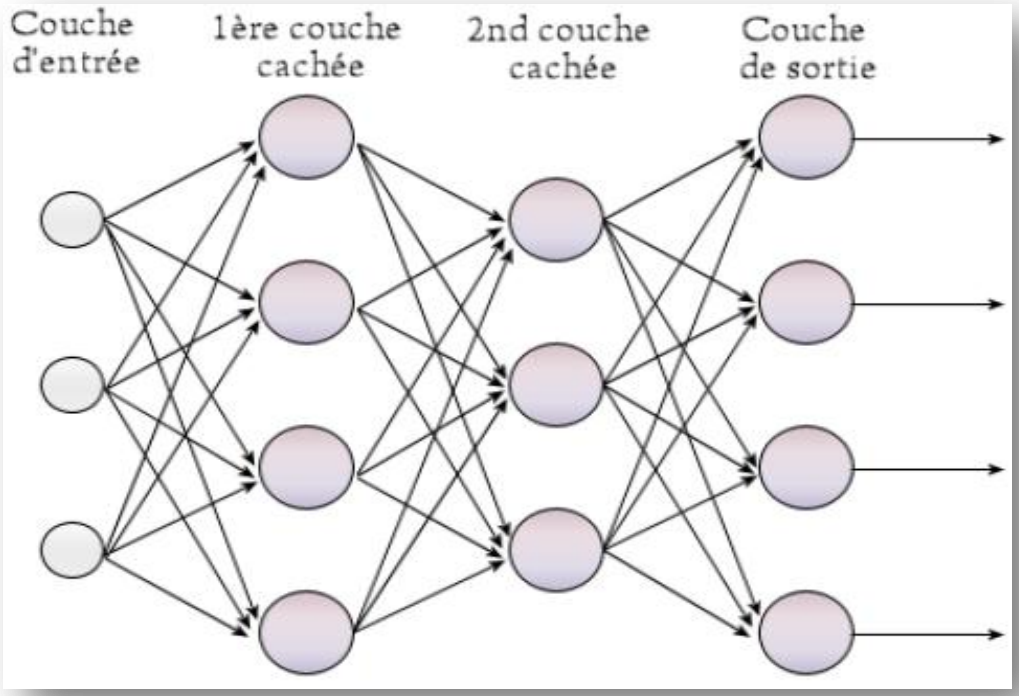

Figure 22 :L'architecture d'un modèle Deep Learning.

3.5Les fonctions d'activations :

Les fonctions d'activation sont des équations mathématiques qui déterminent la sortie d'un réseau neuronal. La fonction est attachée à chaque neurone du réseau, et détermine s'il doit être activé ("déclenché") ou non, en fonction de la pertinence de l'entrée de chaque neurone pour la prédiction du modèle. Les fonctions d'activation aident également à normaliser la sortie de chaque neurone dans une plage entre 1 et 0 ou entre -1 et 1 :

- **Fonctiond'activationbinaire**

  Une fonction d'activation binaire est une fonction d'activation basée sur un seuil. Si la valeur d'entrée est supérieure ou inférieure à un certain seuil, le neurone est activé et envoie un signal identique au prochain niveau. Le problème avec une fonction de seuil est qu'elle ne permet pas de sorties à valeurs multiples - par exemple, elle ne peut pas prendre en charge la classification des entrées en plusieurs catégories [33].

- **Fonctiond'activationlinéaire**

  Une fonction d'activation linéaire prend la forme: **A = cx.** Elle prend les entrées, multipliées par les poids pour chaque neurone, et crée un signal de

sortie proportionnel à l'entrée. Dans un sens, une fonction linéaire est meilleure qu'une fonction de seuil car elle permet plusieurs sorties, pas seulement oui ou non. Cependant, unefonctiond'activationlinéaire a deuxproblèmesmajeurs:

- Il n'est pas possible d'utiliser la rétropropagation du gradient pour entraîner le modèle, la dérivée de la fonction est une constante et n'a aucune relation avec l'entrée **X.** Il n'est donc pas possible de revenir en arrière et de comprendre quels poids dans les neurones d'entrée peuvent fournir une meilleure prédiction.
- Toutes les couches du réseau neuronal se réduisent à une seule avec des fonctions d'activation linéaires, peu importe le nombre de couches dans le réseau neuronal, la dernière couche sera une fonction linéaire de la première couche (car une combinaison linéaire de fonctions linéaires est toujours une fonction linéaire). Ainsi, une fonction d'activation linéaire transforme le réseau neuronal en une seule couche [33].

- **Fonctionsd'activation non linéaires**

  Les modèles de réseaux de neurones modernes utilisent des fonctions d'activation non linéaires. Elles permettent au modèle de créer des mappages complexes entre les entrées et les sorties du réseau, qui sont essentiels pour apprendre et modéliser des données complexes telles que des images, des vidéos, de l'audio et des ensembles de données non linéaires ou à haute dimensionnalité. Presque tous les processus imaginables peuvent être représentés sous forme de calcul fonctionnel dans un réseau de neurones, à condition que la fonction d'activation soit non linéaire. Les fonctions non linéaires résolvent les problèmes d'une fonction d'activation linéaire.

  - Elles permettent la rétropropagation du gradient car elles ont une fonction dérivée qui est liée aux entrées.
  - Elles permettent l'empilement de plusieurs couches de neurones pour créer un réseau neuronal profond. De multiples couches cachées de neurones sont nécessaires pour apprendre des ensembles de données complexes avec des niveaux élevés de précision [33].

Les fonctions d'activation non linéaires courantes [33]

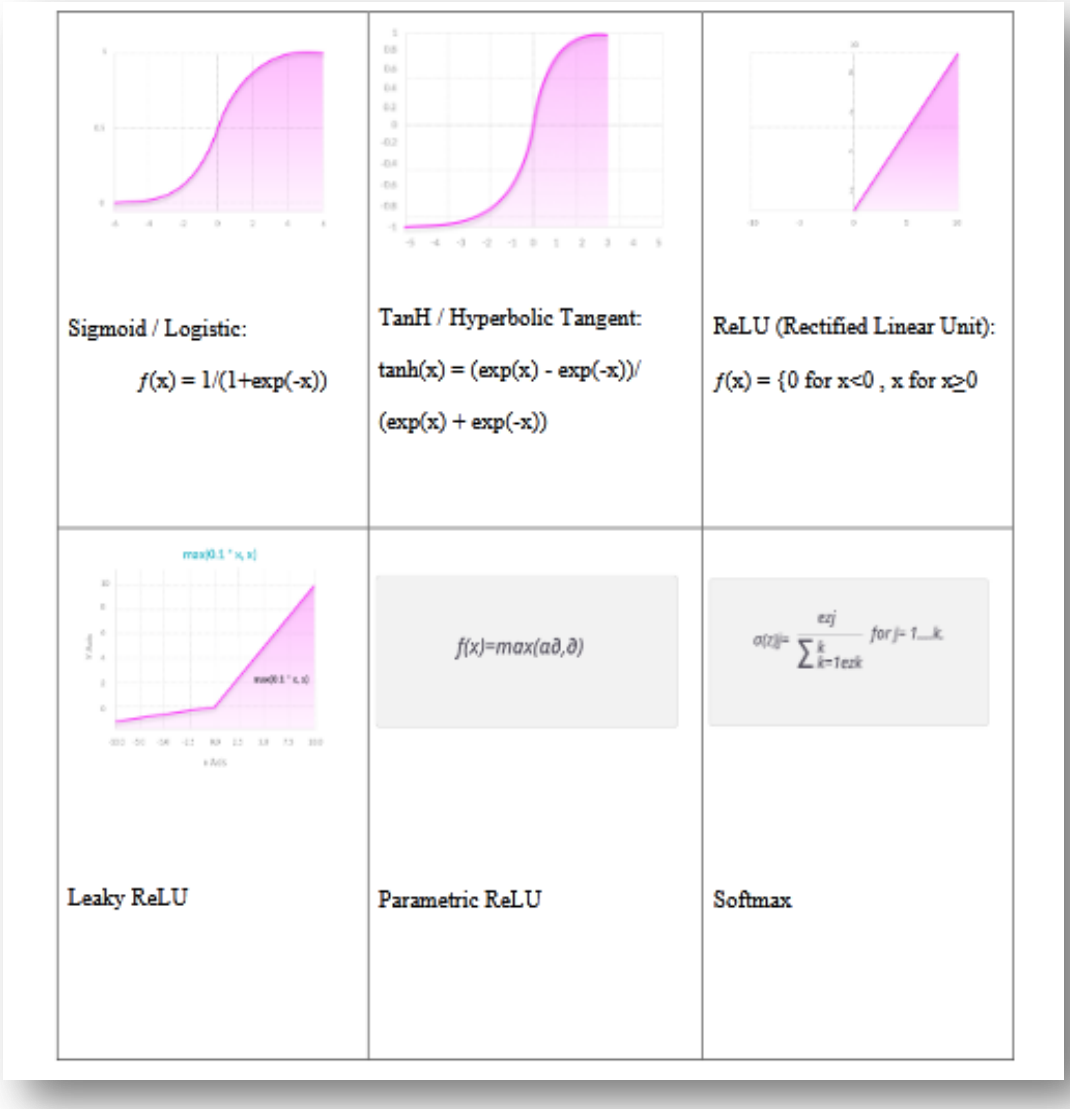

Figure 23: Les fonctions d'activation[33] .

4 TOPOLOGIES DES RESEAUX DE NEURONES:

4.1 Propagation avant (forward propagation) :

Cela est réalisé en fonction des valeurs des sorties à travers les entrées. Ce processus est effectué à l'aide de l'une des équations d'activation (Sigmoid, Relu, Tanh, Softmax, etc.). Certaines valeurs de theta sont imposées avant le début.

4.2 Back propagation :

Les valeurs de poids sont calculées de manière inverse. Cela se fait en trouvant la différence entre la valeur attendue et la valeur réelle, suivie d'une différenciation partielle. Cela est utilisé pour modifier les valeurs de poids supposes.

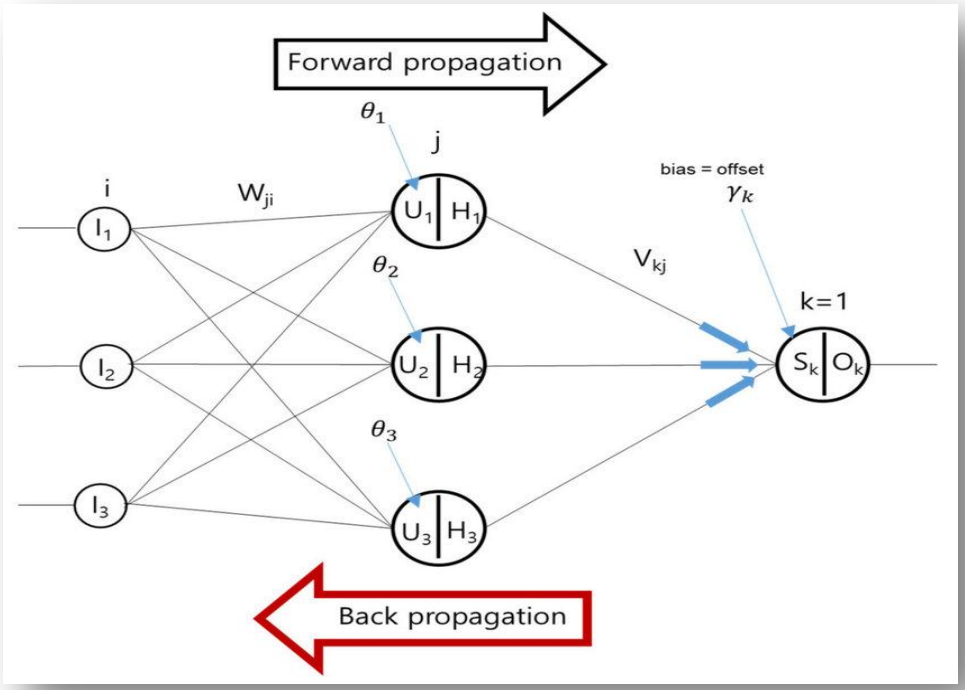

Figure 24 : Topologies des réseaux de neurones:

5 LES MODELS DU DEEP LEARNING :

5.1 Le réseau neuronal profond(deep neural network(DNN)) :

Les réseaux neuronaux profonds (DNN), également appelés réseaux de neurones profonds, sont composés d'un ensemble de neurones organisés en plusieurs couches, appelées perceptrons multicouches (MLP). Ils se distinguent des réseaux neuronaux traditionnels (Artificial Neural Network) par leur profondeur et le nombre de couches et de neurones qui les composent. Lorsqu'un ANN possède deux couches cachées ou plus, il est connu sous le nom de réseau neuronal profond. Leur objectif est de modéliser des données avec des architectures complexes en combinant différentes transformations non linéaires [34].

Le concept de base du perceptron a été introduit par Rosenblatt en 1958 [33]. Le perceptron calcule une sortie unique à partir de multiples entrées réelles (xi) en

effectuant une combinaison linéaire en fonction de ses poids d'entrée (w), puis en appliquant une fonction d'activation non linéaire. Mathématiquement, cela peut être exprimé comme suit :

$$\mathbf{y = \delta(\Sigma n=1\ Wixi + b) = \delta(WT\ X + b)}$$

où :

- **W** : vecteur des poids

- **X** : vecteur des entrées

- **b** : biais

- **δ** : fonction d'activation

Un MLP typique comprend une couche d'entrée constituée de nœuds sources, une ou plusieurs couches cachées contenant des nœuds de calcul, et une couche de sortie composée de nœuds. Le signal d'entrée se propage de couche en couche dans le réseau.

Les réseaux DNN sont généralement utilisés dans des problèmes d'apprentissage supervisé. La formation du modèle (apprentissage) consiste à ajuster tous les poids et les biais à leurs valeurs optimales.

5.2 Le réseau neuronal convolutif (CNN) :

Le terme "réseau neuronal convolutif fait référence à l'utilisation par le réseau d'une procédure mathématique connue sous le nom de convolution. Les réseaux convolutifs sont un type de réseau neuronal qui remplace la multiplication générale de matrices dans au moins une couche par une convolution. Le CNN est l'un des meilleurs algorithmes d'apprentissage pour effectuer l'opération de convolution, ce qui facilite l'extraction de caractéristiques pertinentes à partir de points de données localement connectés. La sortie des noyaux convolutifs est ensuite transmise à la fonction d'activation (une unité de traitement non linéaire) qui prend en charge à la fois l'apprentissage des abstractions et l'introduction de non-linéarité dans l'espace des caractéristiques. Cette non-linéarité génère divers motifs d'activation, ce qui facilite l'apprentissage des différences de signification dans les images. La topologie CNN est divisée en plusieurs étapes d'entraînement qui comprennent des couches convolutives, des unités de traitement non linéaires et des couches de réduction d'échantillonnage

[34] [35]. La structure générale d'un réseau CNN est représentéedans la figure 25 :

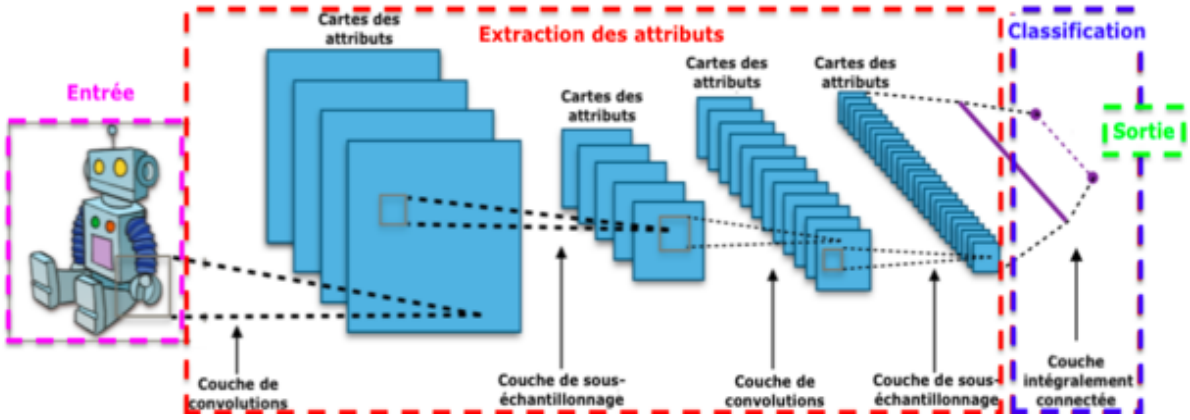

Figure 25 : La topologie CNN.

• **Couche de convolution :**pour extraire des caractéristiques d'une image d'entrée. La convolution maintient l'association entre les pixels en apprenant les caractéristiques de l'image via les données d'entrée de petits carrés. Cette opération mathématique a deux entrées, à savoir un noyau ou filtre et une matrice d'image [37].

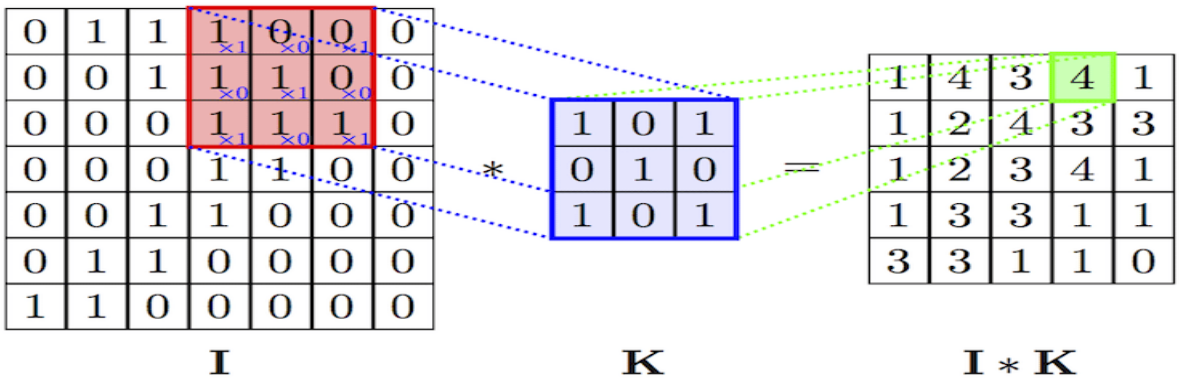

Figure 26 : traitement de la matrice d'image

• **Couche de Pooling :** fait référence à la méthode de sous-échantillonnage de l'entrée qui est généralement positionnée entre deux couches de convolution. Les couches de pooling diffèrent des couches de convolution en n'ayant pas de valeurs pondérées. Le sous-échantillonnage de l'image aide à soulager la charge de calcul du CNN. L'objectif est de réduire la dimensionnalité d'une représentation d'entrée. Le pooling agit uniquement pour agréger des valeurs avec différentes fonctions d'agrégation. Il exist different types de pooling [36]:

- le maximum pooling qui prend le pixel ayant la valeur maximale parmi tous les pixels de la sélection.
- l'averagepooling qui prend les pixels ayant la valeur moyenne de tous les

pixels de la sélection.

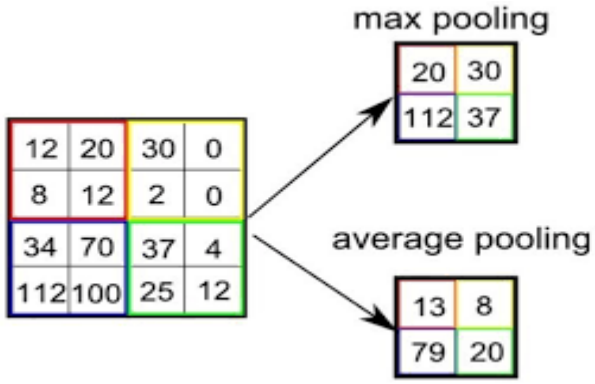

Figure 27 : les deux different types de pooling

• **Couche integralement connectée :** Dans les modèles conventionnels, la couche FC "fullyconnected" est équivalente au réseau entièrement connecté. , la sortie de la première phase (contenant la convolution et le sous-échantillonnage répétitif) est transmise à la couche FC, et l'opération de produit entre le vecteur de poids et le vecteur d'entrée est calculée pour donner la sortie finale [37]. Le réseau neuronal convolutif présuppose que les entrées et sorties du modèle sont indépendantes les unes des autres. Cependant, comme les données acquises sont dépendantes du temps, des informations temporelles doivent être incluses dans les données d'entrée dans certaines applications.

Avantage	Inconvénient
• **Les CNN sont capables de traiter des images de grande taille avec des ressources de calcul limitées grâce à l'utilisation de couches de sous-échantillonnage et de pooling.** • **Les CNN sont hautement parallélisables, ce qui leur permet d'être entraînés efficacement sur des architectures de calcul modernes, telles que les GPU et les TPU.** • **Les CNN ont été largement étudiés et développés ces dernières années, ce qui signifie que des modèles pré-entraînés de haute qualité sont disponibles pour une grande variété de tâches.**	• **Les CNN peuvent être sensibles aux variations d'éclairage, de positionnement et de résolution des images, ce qui peut affecter les performances du modèle.** • **Les CNN sont des modèles à architecture fixe, ce qui signifie qu'ils ne sont pas flexibles pour traiter des entrées de tailles et de formes différentes.** • **Les CNN peuvent être des modèles coûteux en termes de ressources de calculet detemps d'entraînement, en particulier pour les tâches de vision par ordinateur les plus complexes.** • **Les CNN peuvent être sujets à des problèmes de sur-apprentissage s'ils sont entraînés sur des ensembles de données trop petits ou mal équilibrés.**

5.3 Réseaux de Neurones Récurrents (RNN) :

Les réseaux récurrents sont fréquemment utilisés lorsqu'il y a une entrée séquentielle. Ces entrées sont couramment rencontrées lors du traitement de texte ou de la voix. Au lieu de traiter complètement un seul exemple, avec des problèmes séquentiels, seule une partie du problème peut être traitée à la fois. Par exemple, pour construire un réseau qui écrit des pièces de théâtre shakespeariennes, l'entrée serait naturellement les pièces existantes de Shakespeare. Ce que le réseau doit apprendre à faire, c'est de prédire le mot suivant de la pièce. Pour ce faire, il doit se souvenir du texte qu'il a vu jusqu'à présent. Les réseaux récurrents proposent un mécanisme pour cela. Ils permettent également de construire des modèles qui fonctionnent naturellement avec des entrées de longueurs variables (comme des phrases ou des morceaux de discours, par exemple) [38]

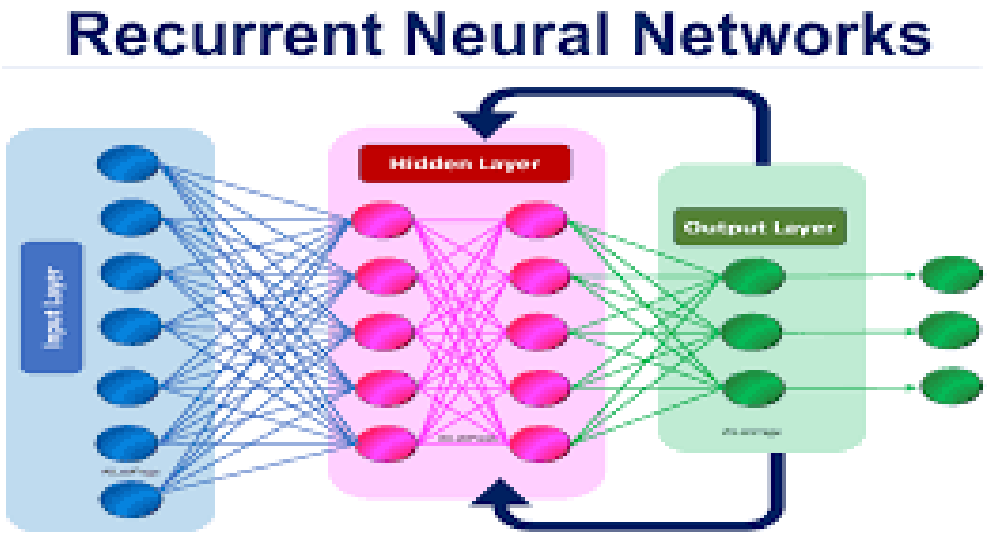

Figure 28 : la topologie RNN[37]

Avantage	Inconvénient
• **Capacité à modéliser des dépendances temporelles :** Les RNN sont conçus pour capturer les dépendances séquentielles à travers le temps, ce qui les rend particulièrement adaptés au traitement de données séquentielles telles que le langage naturel, la parole et les séries temporelles. • **Mémoire à court terme :** Les RNN disposent d'une mémoire à court terme qui leur permet de prendre en compte les informations récentes lors de la prédiction des séquences futures. • **Flexibilité de la taille de l'entrée :** Les RNN peuvent gérer des séquences de longueurs variables, ce qui les rend adaptés à des tâches où la longueur de la séquence varie, telle que la traduction automatique. • **Modèles pré-entraînés :** Comme les RNN sont largement utilisés, il existe de nombreux modèles pré-entraînés disponibles, qui peuvent être utilisés comme point de départ pour des tâches spécifiques.	• **Problème du gradient qui disparaît ou explose :** Les RNN peuvent rencontrer des difficultés lors de l'entraînement en raison du problème du gradient qui disparaît ou explose, ce qui peut rendre l'apprentissage de dépendances à long terme difficile. • **Complexité computationnelle :** Les RNN peuvent être plus lents à entraîner et à évaluer que d'autres architectures de réseaux neuronaux en raison de leur nature récurrente, ce qui peut rendre le processus de développement plus coûteux en termes de temps et de ressources. • **Difficulté de parallélisation :** En raison de leur nature récurrente et de leurs dépendances séquentielles, les RNN sont plus difficiles à paralléliser sur des architectures de calcul modernes, telles que les GPU, par rapport à d'autres architectures comme les CNN. • **Sensibilité à l'ordre des données :** Les RNN sont sensibles à l'ordre des données d'entrée, ce qui signifie que des séquences de données mélangées ou désordonnées peuvent affecter leurs performances

5.4 Long Short Team Memory (LSTM) :

Le Long Short Term Memory (LSTM) est une variante de RNN capable d'apprendre des dépendances à long terme. Il a été démontré comment les RNN vanilla utilisent l'état caché du pas de temps précédent et l'entrée actuelle dans une couche tanh pour mettre en œuvre la récurrence. Les LSTM mettent également en œuvre la récurrence de manière similaire, mais au lieu d'une seule couche tanh, il y a quatre couches interagissant de manière très spécifique [38]. Le schéma suivant illustre les transformations appliquées à l'état caché au pas de temps t :

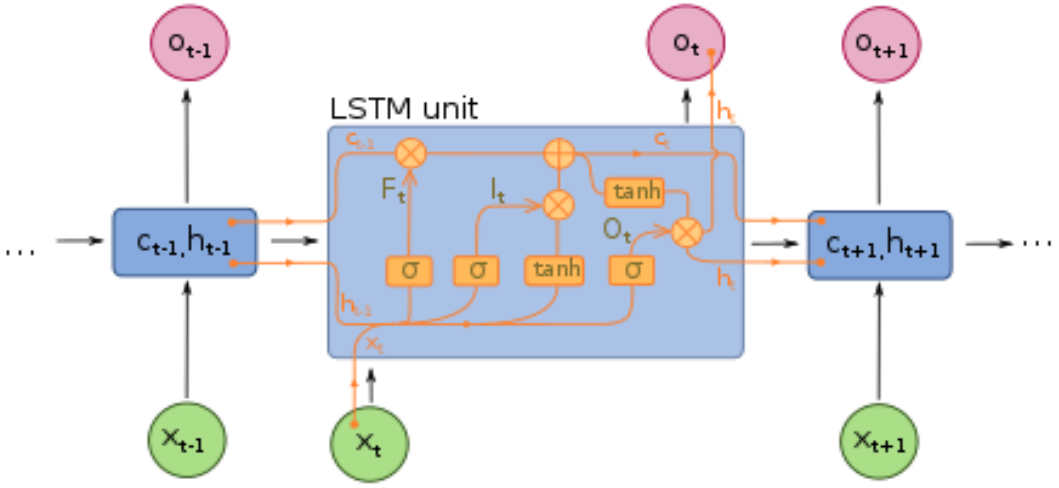

Figure 29 : la topologie LSTM[38]

L'état de cellule c représente la mémoire interne de l'unité. L'état caché ht, les portes i, f, o et g sont le mécanisme par lequel le LSTM travaille sur le problème du gradient qui disparaît. Pendant l'entraînement, le LSTM apprend les paramètres de ces portes. Pour avoir une compréhension plus approfondie de la façon dont ces portes modulent l'état caché du LSTM, considérons les équations qui montrent comment il calcule l'état caché ht au temps t à partir de l'état caché ht−1 au pas de temps précédent [39] :

$$
\begin{aligned}
i &- \sigma(U_i x_t + V^i h_{t-1}) \\
f &- \sigma(U_f x_t + V^f h_{t-1}) \\
o &- \sigma(U_o x_t + V^o h_{t-1}) \\
g &- \tanh(U_g x_t + V^g h_{t-1}) \\
c_t &- c_{t-1} \otimes f + g \otimes i \\
h_t &- \tanh(c_t) \otimes o
\end{aligned}
$$

Ici, i, f et o sont les portes d'entrée, d'oubli et de sortie. Elles sont calculées en utilisant les mêmes équations mais avec des matrices de paramètres différentes. La fonction sigmoïde module la sortie de ces portes entre zéro et un, de sorte que le vecteur de sortie produit peut être multiplié élément par élément avec un autre vecteur pour définir la quantité du deuxième vecteur qui peut passer à travers le premier [39].

La porte d'oubli définit la quantité de l'état précédent ht−1 qu'on souhaite laisser passer. La porte d'entrée définit la quantité de l'état nouvellement calculé pour l'entrée actuelle xt qu'on veut laisser passer, et la porte de sortie définit la quantité de l'état interne qu'on veut exposer à la couche suivante. L'état caché interne g est calculé en

fonction de l'entrée actuelle xt et de l'état caché précédent ht−1. Remarquez que l'équation pour g est identique à celle pour le RNN vanilla.

Étant donné i, f, o et g, l'état de la cellule ct à l'instant t peut maintenant être calculé en termes de ct−1 à l'instant t-1 multiplié par la porte d'oubli et l'état g multiplié par la porte d'entrée i. Ainsi, cela permet de combiner la mémoire précédente et la nouvelle entrée en réglant la porte d'oubli à 0 pour ignorer l'ancienne mémoire et en réglant la porte d'entrée à 0 pour ignorer l'état nouvellement calculé [39]

6 PRINCIPES CLES DE CONCEPTION POUR L'IDS SUR LE DEEP LEARNING DANS L'IOT :

Les principes clés de conception pour les solutions de détection d'intrusion basées sur l'apprentissage en profondeur dans l'IoT sont les suivants :

- **Gestion de l'overfitting** : l'overfitting se produit lorsque le modèle s'adapte bien aux données d'entraînement, mais ne généralise pas bien sur des données inconnues. En apprentissage profond, l'overfitting peut être évité en utilisant les méthodes suivantes :
    - l'application de la régularisation, qui ajoute un coût à la fonction de perte du modèle pour les poids élevés ;
    - l'utilisation de couches de dropout, qui suppriment de manière aléatoire certaines fonctionnalités en les fixant à 0.
- **Équilibrage des données** : le déséquilibre des données se réfère à une distribution disproportionnée des classes dans un ensemble de données. Si un modèle est entraîné sur un ensemble de données déséquilibré, il deviendra biaisé, c'est-à-dire qu'il favorisera les classes majoritaires de l'ensemble de données, ce qui affectera négativement l'efficacité du modèle.
- **Ingénierie des fonctionnalités** : elle permet de réduire le coût du flux de travail d'apprentissage en profondeur en termes de consommation de mémoire et de temps. Elle permet également d'améliorer l'exactitude du modèle en supprimant les fonctionnalités non pertinentes et en appliquant une transformation des fonctionnalités pour améliorer l'exactitude du modèle d'apprentissage.
- **Optimisation du modèle** : l'objectif de l'optimisation du modèle est de minimiser une fonction de perte, qui calcule la différence entre la sortie

prédite et la sortie réelle. Cela est réalisé en ajustant itérativement les poids du modèle. En appliquant un algorithme d'optimisation tel que SGD et Adam, l'efficacité du modèle sera améliorée.

- **Test sur des ensembles de données IoT** : une solution de détection d'intrusion basée sur l'apprentissage en profondeur pour l'IoT doit être testée sur un ensemble de données IoT pour obtenir des résultats qui reflètent le trafic réel de l'IoT[40].

CONCLUSION :

Dans ce chapitre, nous avons discuté des algorithmes de Deep Learning et de la plupart des architectures de réseaux neuronaux, et dans le chapitre suivant nous allons discuter de notre sujet IOT et comment fonctionne avec le Deep Learning.

Chapitre4 :Réalisation et implémentation

INTRODUCTION

Après avoir donné toute la théorie que nous voyons nécessaire pour le développement de notre système, on se penche maintenant sur la deuxième partie dans le but de présenter notre travail.

Dans ce chapitre, nous présentons notre contribution ainsi que les différents outils utilisés. Tout d'abord, nous utilisons le simulateur Cooja pour simuler des attaques au sein d'un environnement IoT et générer notre ensemble de données. Cooja est un simulateur largement utilisé dans la recherche sur l'Internet des objets (IoT) permettant de créer des scénarios d'attaques réalistes.

Ensuite, nous détaillons le jeu de données (Data-set) utilisé dans notre contribution, connu sous le nom de Minerva-IDS.

Enfin, nous présentons notre modèle IDS (Système de détection d'intrusion) fondé sur les réseaux LSTM (Long Short-Term Memory) et exposons les différents résultats de nos expérimentations.

1 TRAVAUX CONNEXES :

Dans cette section, nous présentons un aperçu de certaines recherches sur la détection des attaques de routage dans l'Internet des objets (IoT) à l'aide de systèmes de détection d'intrusion (IDS).

1. Yavuz, F. Y., Devrim, et Ensar, G. Ü. L [40]. Cette étude est une preuve de concept de l'application de l'apprentissage profond à la sécurité dans l'Internet des objets.

• Ils ont proposé une méthode de détection des attaques de routage pour l'IoT basée sur l'apprentissage profond.

• Le principal problème dans ce domaine est le manque d'ensembles de données et la qualité des données disponibles. Leurs ensembles de données d'attaque sont produits par simulation, en utilisant le code d'un capteur réel et la mise en œuvre du protocole Contiki-RPL RPL.

• Ils proposent une méthodologie de détection d'attaque clairement évolutive basée sur l'apprentissage approfondi pour la détection des attaques de routage IoT de catégorie

restreinte, de type inondation d'hello et de modification du numéro de version, avec une grande précision et exactitude.

• De plus, ils ont construit un réseau neuronal profond de modèles formés à l'aide d'ensembles de données IRAD avec des informations d'évaluation : taux de précision, de précision et de rappel.

2. Mridula Sharma, HaythamElmiligi, FayezGebali et AbhishekVerma [42]

• Ils ont introduit un nouveau cadre (Framework) pour simuler des attaques RPL en utilisant Contiki-Cooja et ont simulé quatre attaques différentes à l'aide de ce cadre.

• Pour la mise en œuvre de l'expérience, ils ont choisi d'utiliser quatre attaques différentes : l'attaque "hello flood", l'attaque "DODAG Information Solicitation" (DIS), l'attaque "increased version" et l'attaque "reducedrank".

• Ils analysent les caractéristiques extraites des paquets de trafic réseau et proposent un nouveau modèle d'apprentissage automatique. En utilisant plusieurs techniques de réduction des caractéristiques, le nombre de caractéristiques nécessaires pour la classification des attaques est réduit de 58 à 21, ce qui représente une réduction de 63,7 % de l'économie d'énergie de traitement et de communication.

• L'ensemble de caractéristiques sélectionné montre une efficacité accrue dans la détection de différentes attaques à l'aide de trois classificateurs différents, à savoir Naive Bayes, RandomForest et C4.5.

Leurs résultats expérimentaux montrent qu'ils ont pu atteindre une précision de classification de 99,33 % en utilisant le classificateur Random Forest.

3. Kasongo et al [43]. ont proposé un cadre basé sur les Réseaux de Neurones Récurrents (RNN) pour détecter les intrusions réseau. Ce cadre a atteint une grande précision dans les tâches de détection d'intrusion.

L'évaluation du cadre a été réalisée en utilisant les ensembles de données de référence NSL-KDD et UNSW-NB15. Pour les tâches de classification binaire sur l'ensemble de données NSL-KDD, le modèle XGBoost-LSTM a atteint une précision de test (TAC) de 88,13 % et une précision de validation (VAC) de 99,49 %, avec un temps

d'entraînement de 225,46 secondes. Sur l'ensemble de données UNSW-NB15, le modèle XGBoost-Simple-RNN s'est avéré être le meilleur avec une TAC de 87,07 %.

L'évaluation a également inclus des tâches de classification multiclasse. Le modèle XGBoost-LSTM a obtenu une TAC de 86,93 % sur l'ensemble de données NSL-KDD, tandis que le modèle XGBoost-GRU a atteint une TAC de 78,40 % sur l'ensemble de données UNSW-NB15.

Dans l'ensemble, le cadre de détection d'intrusion proposé a démontré son efficacité pour renforcer la sécurité des systèmes réseau. L'intégration d'un algorithme de sélection des caractéristiques basé sur XGBoost a en outre amélioré la précision du cadre.

2 NOTRE CONTRIBUTION :

Nous avons utilisé un dataset simuler avec le simulateur Cooja et on a fait un prétraitement (avec balancement des données),

3 PREPARATION DES DONNEES:

Nous avons utilisé un ensemble de donnéesIoT [43]qui a été publié en 2020 par BOUAZZA Abdelhamid et CHAABI Aissa à l'Université d'Ibn Khaldoun - Tiaret. Le principal problème dans ce domaine est le manque d'ensembles de données et la qualité des données disponibles. Leurs ensembles de données d'attaque sont produits par simulation, en utilisant des scénarios réels en utilisant le code d'un capteur réel et la mise en œuvre du protocole Contiki-RPL

Toutes les étapes de création de l'ensemble de données sont résumées comme suit

3-1 Capture de trafic :

• Tout le trafic qui passait par le réseau IoT a été capturé avec différents scénarios en tant que fichier PCAP à l'aide de Wireshark et un outil prêt dans le simulateur Cooja appelé radio messages. Le fichier PCAPest converti en fichier csv.

3-2 Générer de nouvelles fonctionnalités :

Toutes les étapes précédentes ont généré un total de 3 fonctionnalités à partir de 6 fonctionnalités au départ.

• Le temps de transmission et de réception de chaque paquet est calculé. Il s'agit du temps total de la durée de chaque paquet de transmission et de réception sur 1000 ms. Ensuite, ils ont calculé le temps de transmission et de réception moyen pour chaque nœud. Le nombre de paquets de contrôle transmis par chaque nœud (concernant les paquets de contrôle : DAO, DIO et DIS) est calculé dans une fenêtre de taille 1000 ms. Ces valeurs ont un impact sur la détection des attaques telles que le Hello Flooding, car dans cette attaque, le taux de transmission doit être plus élevé. Le pseudo-code de l'algorithme d'extraction de fonctionnalités est fourni ci-dessous.

4 METRIQUES ET EVALUATION :

Dans cette section, nous avons évalué les performances des classificateurs IDS, nous sommes concentrés sur trois mesures d'exactitude, de précision et de taux de fausses alarmes.

7 ETUDES COMPARATIVES :

Pour évaluer les performances de LSTM_IDS, nous avons comparé ses performances avec des travaux connexes :

8ENVIRONNEMENT D'EXECUSSION :

Google Colab :

Google Colab est un environnement de développement en ligne basé sur JupyterNotebook, qui offre la possibilité d'écrire, d'exécuter et de partager du code Python. Il fournit un accès gratuit à des ressources de calcul puissantes, y compris des unités de traitement graphique (GPU) et des unités de traitement tensoriel (TPU) pour accélérer l'exécution des tâches d'apprentissage automatique et de calcul intensif[48].

Définition du langage Python en informatique :

Python est le langage de programmation open source le plus employé par les informaticiens. Ce langage s'est propulsé en tête de la gestion d'infrastructure, d'analyse de données ou dans le domaine du développement de logiciels. En effet, parmi ses qualités, Python permet notamment aux développeurs de se concentrer sur ce qu'ils font plutôt que sur la manière dont ils le font. Il a libéré les développeurs des contraintes de formes qui occupaient leur temps avec les langages plus anciens. Ainsi, développer du code avec Python est plus rapide qu'avec d'autres langages.

Définition jupyter :

Jupyter se présente comme un outil extrêmement simple à mettre en œuvre qui vous permettra de transformer vos Jupyter Notebooks en applications web ou en Dashboard quasiment automatiquement.

Panda :

Pandas est un package Python open source qui est le plus largement utilisé pour la science et l'analyse des données[45].

Numpy :

Le terme Numpy est en fait l'abréviation de « Numerical Python ». Il s'agit d'une bibliothèque Open Source en langage Python. On utilise cet outil pour la programmation scientifique en Python, et notamment pour la programmation en Data Science, pour l'ingénierie, les mathématiques ou la science[46].

Scikitlearn :

Scikit-learn est une bibliothèque en Python qui offre de nombreux algorithmes d'apprentissage supervisé et non supervisé. Elle repose sur des technologies que vous connaissez peut-être déjà, telles que NumPy, pandas et Matplotlib.

Les fonctionnalités fournies par scikit-learn comprennent :

- Régression, compris la régression linéaire et logistique.

- Classification, compris les voisins les plus proches (K-Nearest Neighbors).

- Sélection de modèles.

- Prétraitement, compris la normalisation Min-Max.

Scikit-learn est une puissante bibliothèque qui facilite l'implémentation de diverses techniques d'apprentissage automatique dans vos projets Python.

Tenssorflow :

TensorFlow est une bibliothèque open-source de logiciels pour le flux de données et la programmation différentielle, utilisée pour diverses tâches. De la même manière, TensorFlow est utilisé dans l'apprentissage automatique par les réseaux neuronaux. Développé par Google en 2011 sous le nom de DistBelief, TensorFlow a été officiellement publié en 2017 gratuitement. La bibliothèque est capable de s'exécuter sur plusieurs CPU et GPU, et est disponible sur différentes plateformes, compris les appareils mobiles. Le nom vient des tableaux multidimensionnels appelés tenseurs, qui sont couramment utilisés dans les réseaux neuronaux[47].

TensorFlow est une bibliothèque puissante qui permet de créer et d'entraîner des modèles d'apprentissage automatique avancés. Grâce à sa compatibilité avec différentes plates-formes et à sa capacité de tirer parti des ressources matérielles, TensorFlow offre une grande flexibilité pour les projets de machine learning.

Keras :

Keras est une bibliothèque open-source de composants de réseaux neuronaux écrits en Python. Keras est capable de s'exécuter sur TensorFlow, Theano, PlaidML et d'autres plates-

formes. Cette bibliothèque a été développée pour être modulaire et conviviale, mais elle a initialement débuté en tant que projet de recherche pour le système d'exploitation intelligent neuro-électronique à réponse ouverte (ONEIROS). L'auteur principal de Keras est François Chollet, un ingénieur de Google qui a également créé le modèle de réseau neuronal profond XCeption. Bien que Keras ait été officiellement lancé, il n'a été intégré à la bibliothèque principale TensorFlow de Google qu'en 2017. Un support supplémentaire a également été ajouté pour l'intégration de Keras avec le Microsoft Cognitive Toolkit.

Keras simplifie le processus de création et d'entraînement de réseaux neuronaux en fournissant une interface conviviale et une abstration des détails complexes. Avec son intégration dans différentes bibliothèques de calcul numérique, Keras offre une flexibilité et une compatibilité étendues pour les projets d'apprentissage profond.

CONCLUSION :

En conclusion, notre modèle LSTM_IDS représente une avancée importante dans le domaine de la détection d'intrusions dans l'Internet des objets. Grâce à son utilisation de l'apprentissage profond et à l'utilisation de tous les attributs disponibles dans les ensembles de données, notre modèle offre une solution prometteuse pour assurer la sécurité des systèmes IoT. Les performances obtenues, combinées à une faible

incidence de fausses alarmes, permettent aux utilisateurs de détecter rapidement les intrusions et de prendre les mesures nécessaires pour protéger leurs systèmes. Dans un monde de plus en plus connecté, notre modèle LSTM_IDS offre une approche solide pour garantir la sécurité des systèmes IoT et leur bon fonctionnement.

Conclusion Générale

CONCLUSION GENERALE :

Avec l'augmentation du nombre d'appareils connectés à l'Internet des objets, leur sécurité devient le premier obstacle. Lorsque nous parlons de l'Internet des objets, cela signifie des données partout, et c'est plus dangereux. Il existe de nombreuses recherches dans le domaine de la sécurisation de ces réseaux, mais peu d'entre elles correspondent à l'environnement réel de l'Internet des objets et aux scénarios réels auxquels ils sont exposés.

Notre travail de recherche s'est concentré sur la sécurité de l'Internet des objets (IoT) et plus spécifiquement sur les attaques visant le protocole de routage RPL. Dans cette optique, nous avons développé un modèle de détection d'intrusion basé sur l'apprentissage en profondeur afin de repérer ces attaques.

Nous avons effectué une étude approfondie des attaques les plus significatives ciblant le protocole de routage RPL dans l'IoT, en mettant l'accent sur la sécurité et les défis spécifiques de ce domaine. Pour mener nos recherches, nous avons utilisé l'ensemble de données Minerva, créé à l'aide du simulateur Cooja, qui intègre des attaques réalistes et des caractéristiques importantes telles que la localisation des nœuds et la gestion de l'énergie.

Le modèle de détection d'intrusion que nous avons développé repose sur l'algorithme LSTM (Long Short-Term Memory), qui est un type de réseau de neurones récurrents spécialement conçu pour traiter des séquences de données. Nous avons minutieusement optimisé les hyperparamètres du modèle afin d'obtenir des performances de détection optimales.

Dans le cadre de l'évaluation de notre IDS, nous avons comparé notre modèle à d'autres architectures de réseaux neuronaux, ainsi qu'à des travaux récents dans le domaine de la détection d'intrusion IoT. Les résultats obtenus démontrent clairement l'efficacité et la robustesse de notre modèle LSTM-IDS, qui a réussi à détecter avec précision les attaques ciblant les systèmes IoT.

Cette validation approfondie confirme que notre modèle est une solution prometteuse pour renforcer la sécurité des dispositifs IoT en détectant de manière fiable les activités suspectes et les comportements malveillants. Ces résultats

encourageants ouvrent la voie à de nouvelles améliorations et à de futures recherches visant à perfectionner encore davantage notre système de détection d'intrusion.

Pour les travaux futurs, nous suggérons d'enrichir l'ensemble de données en y ajoutant de nouvelles attaques récentes pour améliorer sa diversité. De plus, l'utilisation d'une approche combinant différents algorithmes d'apprentissage en profondeur tels que le LSTM, le CNN et le RNN pourrait permettre d'améliorer encore les performances de l'IDS et de détecter un plus large éventail d'attaques.

En conclusion, notre travail a contribué à renforcer la sécurité de l'IoT en proposant un système de détection d'intrusion basé sur l'apprentissage en profondeur. Il reste encore des défis à relever, mais notre recherche ouvre la voie à de futures améliorations dans ce domaine critique de la cybersécurité.

BIBLIOGRAPHIE

[1] Gubbi, J., Buyya, R., Marusic, S., &Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

[2] Atzori, L., Iera, A., &Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.

[3] Stankovic, J. A. (2014). Research directions for the Internet of Things. IEEE Internet of Things Journal, 1(1), 3-9.

[4] Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. Computer Communications, 54, 1-31.

[5] Botta, A., De Donato, W., Persico, V., &Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. Future Generation Computer Systems, 56, 684-700.

[6] Finkenzeller, K. (2010). RFID handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication (3rd ed.). John Wiley & Sons.

[7] IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). IEEE Std 802.15.4-2015.

[8] IEEE Standard for Local and Metropolitan Area Networks—Part 15.4:Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std.802. 15. 4-2011, 2011.

[9] Near Field Communication, White paper, ECMAinternational, December 2003

[10] J. W. Hui and D. E. Culler, “Extending IP to low-power, wireless personal area networks,” IEEE Internet Comput., vol. 12, no. 4, pp. 37–45,Jul./Aug. 2008.

[11] T. Clausen, U. Herberg, and M. Philipp, “A critical evaluation of theIPv6 routing protocol for low power and lossy networks (RPL),” in Proc.IEEE 7th Int. Conf. WiMob, 2011, pp. 365–372.

[12] L. Wallgren, S. Raza, and T. Voigt, “Routing attacks and countermeasures in the RPL-based internet of things,” Int. J. Distrib. Sens. Networks, vol. 2013, 2013, doi:10.1155/2013/794326.

[13] A. Mayzaud , R. Badonnel , I. Chrisment , A taxonomy of attacks in RPL - based internetof thing , Int . J. Netw .Secur . 18 (3) (2016) 459-473 .

[14] A., Mayuri, etSudhir T. « Internet of Things: Architecture, Security Issues and Countermeasures ». International Journal of Computer Applications 125, no 14 (17 septembre 2015): 1-4. https://doi.org/10.5120/ijca2015906251.

[15] Claire Kago, (Avril 2020), « 10 conseils pour gérer l'ex- plosion de l'IoT à venir », https://www.journaldu- net.com/ebusiness/internet-mobile/1490765-10-conseils pour-gerer-l-explosion-de-l-iot-a-venir

[16] AXELSSON, S. Aspects of the modelling and performance of intrusion detection. Department of Computer Engineering, Chalmers University of Technology, 2000.

[17]DABOUR, I., & HADJI, I. (). Etude et mise en place d’un système de détectionprévention d’intrusion (IDSIPS) réseau. Etude de cas SNORT.

[18]technologies, Entreprises. « IDS, qu’est ce qu’un système de détection d’intrusions ». La Revue Tech, 24 novembre 2022, https://larevuetech.fr/ids-quest-ce-quun-systeme-de-detection-dintrusions/.

[19] Les sondes de sécurité IDS/IPS. http://igm.univmlv.fr/~dr/XPOSE2009/Sonde_de_securite_IDS_IPS/IDS.html#type. Consulté le 16 mai 2023.

[20]Abdelhalim Zaidi. Recherche et détection des patterns d'attaques dans les réseaux IP _a hauts débits. Réseaux et télécommunications [cs.NI]. Université d'Evry-Val d'Essonne, 2011.

[21]N. M. Shanono, N. A. Abu, and W. Mohamed, “Intrusion Detection System Architecture : Issues and Challenges,” Glob. J. Comput. Sci. Technol., vol. 62, no. 7, 2020.

[22] Bidan, C., Hiet, G., Mé, L., Morin, B., & Zimmermann, J. (2006). Vers une détection d’intrusions à fiabilité et pertinence prouvables. REVUE DE L ELECTRICITE ET DE L ELECTRONIQUE, 9, 75.

[23]Dacier, M., Debar, H., &Wespi, A. (1999). A Revised Taxonomy for Intrusion-Detection Systems.Techmical Report Computer Science Mathematics.

[24]El Rab, M. G. (2008). Evaluation des systèmes de détection d’intrusion.

[25] Majorczyk, F. (2008). Détection d’intrusions comportementale par diversification de COTS: application au cas des serveurs web.

[26]A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion

detection systems: techniques, datasets and challenges,” Cybersecurity, vol. 2, no. 1, pp. 1–22, 2019.

[27] Cédric Michel, Langage de description d'attaques pour la détection d'intrusions

par corrélation d'événements ou d'alertes en environnement réseau hétérogène, Université de Rennes 1,2003.

[28]R. G. Bace and P. Mell, “Intrusion detection systems.” US Department of

Commerce, Technology Administration, National Institute of …, 2001.

[29]« Appréhendez le Deep Learningoul’apprentissageprofond ». OpenClassrooms, https://openclassrooms.com/fr/courses/6417031-objectif-ia-initiez-vous-a-lintelligence-artificielle/6823506-apprehendez-le-deep-learning-ou-lapprentissage-profond.

[30]“Deep Learning | Coursera.” https://www.coursera.org/specializations/deep-learning (accessed .june 20, 2021).

[31]C. Llorens, L. Levier, D. Valois, B. Morin, ―Tableaux de bord de la sécurité réseau,‖ Paris, France, Editions Eyrolles, 2010.

[32]/[33] "Pattern Recognition and Machine Learning" par Christopher Bishop

"Machine Learning: A Probabilistic Perspective" par Kevin P. Murphy "Hands-On Machine Learning with Scikit-Learn and TensorFlow" par AurélienGéron

[34]"Semi-Supervised Learning" par Olivier Chapelle, Bernhard Schölkopf, et Alexander Zien"Introduction to Semi-Supervised Learning" par Xiaojin Zhu et Andrew B. Goldberg "Semi-Supervised Learning with Deep Generative Models" par Diederik P. Kingma et Danilo J. Rezende.

[35] D. H. S. R. A. F. L. H. B. L. ,. S. F. d. R. A. Ivan Nunes da Silva, Artificial

Neural Networks A Practical Course. Springer International Publishing Switzerland., 2017.

[36] Khan, A., Sohail, A., Zahoora, U., Qureshi, A. S. (2020).A survey of the recent

architectures of deep convolutional neural networks. Artificialintelligence review, 53(8), 5455-5516.

[37] Jarrett, K., Kavukcuoglu, K., Ranzato, M. A., LeCun, Y.(2009,September). What

is the best multi-stage architecture for object recognition?. In 2009IEEE 12th international conference on computer vision (pp. 2146-2153). IEEE

[38] Conceptual understanding of convolutional neural network-adeep learning approach.

[39] DouweOsinga. Deep Learning Cook book. O'Reilly Media,Inc, 2018.

[40] Antonio Gulli and Sujit Pal. Deep Learning with Keras.Packt Publishing,2017.

[41] A. Derhab, A. Aldweesh, A. Z. Emam, and F. A. Khan, “Intrusion Detection

Systemfor Internet of Things Based on Temporal Convolution Neural Network and EfficientFeature Engineering,” Wirel. Commun.Mob.Comput., vol. 2020, no. April, 2020, doi:10.1155/2020/6689134.

[42] F. Y. Yavuz, D. Ünal, and E. Gül, “Deep learning for detection of routing attacks

in the internet of things,” Int. J. Comput. Intell. Syst., vol. 12, no. 1, pp. 39–58, 2018, doi: 10.2991/ijcis.2018.25905181.

[43]M. Sharma, H. Elmiligi, F. Gebali, and A. Verma, “Simulating Attacks for RPL

and Generating Multi-class Dataset for Supervised Machine Learning," 2019 IEEE 10th Annu. Inf. Technol. Electron. Mob.Commun. Conf. IEMCON 2019, pp. 20–26, 2019, doi: 10.1109/IEMCON.2019.8936142.

[44]S. M. Kasongo, « A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework » Computer Communications , vol.199,pp. 113-125, Feb, 2023, doi :10.1016/j.comcom.2022.12.010.

[45] S. Kotsiantis, D. Kanellopoulos, and P. Pintelas, "Handling imbalanced datasets: A review," GESTS Int. Trans. Comput. Sci. Eng., vol. 30, no. 1, pp. 25–36, 2006

[46]La bibliothèque Python Pandas – Très Facile. https://www.tresfacile.net/la-bibliotheque-python-pandas/. Consulté le 17 juin 2023.

[47]« Appréhendez le Deep Learning ou l'apprentissage profond ». OpenClassrooms, https://openclassrooms.com/fr/courses/6417031-objectif-ia-initiez-vous-a-lintelligence-artificielle/6823506-apprehendez-le-deep-learning-ou-lapprentissage-profond.

[48] "TensorFlow." https://www.tensorflow.org/ (accessed Sep. 1, 2021).

[49]fuat. « Google Colab Free GPU Tutorial ». Deep Learning Turkey, 20 juin 2021, https://medium.com/deep-learning-turkey/google-colab-free-gpu-tutorial-e113627b9f5d.