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 :

- BENSASSI SAAD
- LAZREG KHADIDJA

Sur le thème

Apprentissage automatique pour la détection d'intrusions dans l'IoT

Soutenu publiquement le 20 /06/ 2024 à Tiaret devant le jury composé de :

Mr Si Abdelhadi Ahmed	Grade	Université M.C.B	Président
Mr Alem Abdelkader	Grade	Université M.A.A	Encadreur
Mr Daoud Mohamed Amine	Grade	Université M.C.B	Examinateur

Année universitaire 2023 – 2024

Remerciements

Tout d'abord, *nous remercions* ***ALLAH*** *le tout-puissant de nous avoir donné la santé, le courage et la patience nécessaires à mener ce travail à son terme.*

C*'est avec un grand plaisir que nous réservons cette page en signe de gratitude et de profonde reconnaissance à tous ceux qui nous ont aidés de prés ou de loin pour la réalisation de ce modeste travail.*

Nous remercions notre encadreur ***Dr. Alem Abdelkader*** *pour sa précieuse assistance, sa disponibilité, son soutien et l'intérêt qu'il a manifesté pour ce travail, ainsi que pour les discussions, le soutient, la bonne humeur et pour avoir accepté de valider les résultats de notre travail et nous avoir fait partager leurs connaissances.*
Qu'ils trouvent ici l'expression de notre gratitude et tout notre respect.
C*omme nous n'oublions pas* ***Mr. BOUAZZA Abdelhamid*** *pour*
son soutien et son assistance , ainsi que pour les discussions,
le soutient, la bonne humeur.
N*os remerciements aux membres du jury* ***Mr. Si Abdelhadi*** *et* ***Mr. Daoud Mohamed Amine****, d'avoir accepté de juger notre travail.*

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

Dédicaces . . .

A ma reine **ARIAM** et mon prince **ANES**

A Mon CHER Mari ***CHOUKRI***

Je dédie ce travail à ma mère, qui a été mon pilier et ma source d'inspiration tout au long de ma vie. Ton amour inconditionnel et ton soutien constant ont été mes plus grands atouts. Merci d'avoir été là à chaque étape de mon parcours, en m'encourageant et en me poussant à donner le meilleur de moi-même,

À ***ma mère****, qui a été mon pilier et ma source d'inspiration tout au long de ma vie. Ton amour inconditionnel et ton soutien constant ont été mes plus grands atouts. Merci d'avoir été là à chaque étape de mon parcours, en m'encourageant et en me poussant à donner le meilleur de moi-même,*

À ***mon père,*** *dont l'intégrité et la détermination ont été des exemples inspirants. Ton soutien infaillible, tes encouragements et tes précieux conseils m'ont guidé sur le chemin de la réussite, Je vous aime de tout mon cœur et je dédie ce mémoire à vous, mes merveilleux parents,*

À ***mon cher frère Kada****, mon soutien inébranlable et mon partenaire de vie tout au long de cette aventure.*

À *Mes sœurs et frères ,*

À ma belle-famille, pour votre soutien précieux et votre amour inconditionnel tout au long de ce parcours,

À tous ceux qui me sont chers et proches, à tous ceux qui ont semé en moi à tout point de vue, soyez sûrs que ce travail est le résultat de votre confiance en moi. Soyez-en remerciés.

Khadidja

Dédicaces …

En témoignage de ma gratitude et mon amour

Je dédie ce travail

À mes très chers parents, à mes sœurs et frères, à ma cher femme, à mes enfants ,à tous mes proches et mes très chers amis qui m'ont accompagné, soutenu et encouragé tout au long de la réalisation de ce mémoire.

À tous ceux que j'aime ;

Et à tous ceux qui m'aiment ;

Je vous dédie ce travail avec tous mes vœux de bonheur, de santé et de réussite.

Saad

Chapitre II:Intrusion Detection Systems

Chapitre III: Contribution,résultat et discussion

IoT	**: Internet of Things.**
6LoWPAN	**: IPv6 over Low-Power Wireless Personal Area Networks.**
CNN	**: Convolutional Neural Network.**
CoAP	**: Constrained Application Protocol.**
CPS	**: Cyber Physical System).**
DAO	**: DODAG Advertisement Object.**
DDS	**: Data Distribution Service.**
DIO	**: DODAG Information Object.**
DIS	**: DODAG Information Sollicitation.**
DNN	**: Deep Neural Network.**
DODAG	**: Destination Oriented Directed Acyclic Graph.**
ETX	**: Expected Transmission Count.**
HIDS	**: Host Intrusion Detection System.**
IA	**: Intelligence Artificielle.**
IDS	**: Intrusion Detection Systems.**
IDWG	**: Intrusion Detection exchange format Working Group.**
IEEE	**: Institute of Electrical and Electronics Engineers.**
IETF	**: Internet Engineering Task Force.**
IETF	**: Internet Engineering Task Force.**
IPv6	**: Internet ProtocolVersion6.**
KNN	**: k-Nearest Neighbours.**
LR	**: Logistic Regression.**
LSTM	**: Long Short-Term Memory.**
M2M	**: Machine to Machine.**
ML	**: Machine Learning.**
ML	**: Machine Learning.**
MLP	**: Multi-Layer Perceptron.**
NaN	**: Not a Number.**
NFC	**: Near-Field Communication.**

NIDS	**: Network Intrusion Detection Systems.**
OC	**: Objet Connecté.**
OCE	**: Objet Connecté Enrichi.**
OF	**: Objective Function.**
OF0	**: Objective Function Zero.**
OSI	**: Open Systems Interconnection.**
OSVM	**: One-Class Support Vector Machine.**
P2P	**: Peer-to-Peer.**
PCA	**: Principal Component Analysis.**
RFC	**: Random Forest Classifier.**
RFID	**: Radio-Frequency Identification.**
RL	**: Renforcement Learning.**
RNN	**: Recurrent Neural Network.**
ROLL	**: Routing Over Low-power and Lossy**
SMOTE	**: Synthetic Minority Over-sampling Technique.**
SVM	**: Support Vector Machine.**
TN	**: True Negative.**
TP	**: True Positive.**
t-SNE	**: t-distributed Stochastic Neighbor Embedding**
UDP	**: User Data Protocol.**
WLAN	**: Wireless Local Area Network.**
WSN	**: Wireless Sensor Neworks.**
WSN	**: Wireless Sensors Network.**

الملخص

مكن التطور السريع لتكنولوجيا إنترنت الأشياء (IoT) من ربط عدد لا يُحصى من الأجهزة والأنظمة حول العالم. ومع ذلك، نظرًا لعدم وجود تدابير أمنية إلكترونية كافية، أصبحت إنترنت الأشياء هدفًا رئيسيًا للقراصنة والهجمات الخبيثة. لحل هذه المشكلة الحرجة، هناك حاجة إلى شبكة آمنة بالكامل تتيح نشر هذه التكنولوجيا بشكل آمن وفعال. يقدم هذا العمل نموذجًا متطورًا للكشف عن التسلل يعتمد على التعلم العميق ويتكون من مستويين، باستخدام الذاكرة طويلة وقصيرة المدى (LSTM). يشمل النموذج تقنيات ثنائية ومتعددة التصنيف، بالإضافة إلى عمليات التصفية والتجميع القائمة على الوقت، وكلها مصممة لتحسين الأداء. تم تقييم النموذج المقترح باستخدام مجموعتي البيانات UNSW-NB15 وMinerva، حيث أظهر انخفاضًا في معدلات الإنذارات الخاطئة (الإيجابيات الخاطئة) ودقة عالية

الكلمات المفتاحية: إنترنت الأشياء، الأمن، نظام كشف التسلل، التعلم العميق، LSTM، UNSW-NB15، Minerva.

Résumé

La rapide évolution de la technologie de l'Internet des objets (IDO ou IoT en anglais) a permis l'interconnexion d'innombrables appareils et systèmes dans le monde entier. Cependant, en raison de l'absence de mesures de cybersécurité adéquates, l'IoT est devenu une cible privilégiée pour les pirates informatiques malveillants. Pour résoudre ce problème critique, il est nécessaire de mettre en place un réseau entièrement sécurisé, permettant un déploiement sûr et efficace de cette technologie. Ce travail présente un modèle sophistiqué de détection d'intrusion basé sur l'apprentissage profond à deux niveaux, utilisant la mémoire à long et court terme (LSTM), intégrant des techniques de classification binaire et multi classification, ainsi que des processus de filtrage et d'agrégation basés sur le temps, tous conçus pour optimiser les performances. Le modèle proposé a été évalué à l'aide des ensembles de données UNSW-NB15 et Minerva, montrant des taux de fausses alarmes (faux positifs) réduits, ainsi qu'une exactitude et une précision élevées.

Mots clés : Internet des objets, sécurité, système de détection d’intrusion, apprentissage profond, LSTM, UNSW-NB15, Minerva.

Abstract

The rapid expansion of the Internet of Things (IoT) technology has enabled the interconnection of countless devices and systems worldwide. However, due to its lack of adequate cyber security measures, it has become a prime target for malicious hackers. To address this critical issue, a fully secure IoT network must be established, allowing for a safe and efficient deployment of this technology. This paper presents a sophisticated two-level deep learning-based intrusion detection model that uses long-short-term memory (LSTM), incorporating binary and multi-level classification techniques, time-based filtering and aggregation processes, all designed to optimize performance. The proposed model was evaluated using the UNSW-NB15 and Minerva datasets, achieving highly satisfactory results, including reduced false alarm rates (false positives), and high accuracy and precision.

Keywords: Internet of Things, security, intrusion detection system, deep learning, LSTM, UNSW-NB15, Minerva.

Introduction

Introduction générale

L'internet et le réseau informatique ont connu un énorme développement ce qui a fait naître l'internet des objets (connu sous le nom de IoT : Internet of things) et grâce à son avènement, de nombreux dispositifs connectés sont déployés pour faciliter notre vie quotidienne. Cependant, la gestion des communications et du routage au sein de ces réseaux d'objets pose des défis uniques. Le protocole de routage RPL (Routing Protocol for Low-Power and Lossy Networks) a été spécialement conçu pour répondre aux exigences des réseaux à faible consommation d'énergie et présentant des pertes de paquets. Le RPL est largement utilisé dans les réseaux IoT pour permettre une connectivité efficace et fiable entre les nœuds. Il utilise une structure hiérarchique appelée graphe DODAG (Destination Oriented Directed Acyclic Graph) pour organiser les nœuds en fonction de leurs relations de parenté. Cela permet d'optimiser les performances du réseau en termes de consommation d'énergie, de latence et de fiabilité des communications.

Avec la prolifération croissante des dispositifs IoT, l'IoT 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 (IDS) basé sur le Deep Learning (DL) spécifiquement conçu pour détecter les attaques de routage dans (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.

Pour mener à bien notre recherche, le présent travail est organisé en trois chapitres selon le plan méthodologique suivant, la partie théorique se compose de deux chapitres :

Le premier chapitre, intitulé "Internet of Things et le protocole de routage RPL" fait l'objet de la présentation des réseaux IoT, son architecture et sa pile protocolaire. Puis une présentation détaillée du protocole de routage RPL qui fait l'objet de notre étude, et ses différentes attaques ainsi que les contre-mesures existantes pour faire face à ces menaces, en termine avec les mécanismes de sécurité.

Le deuxième chapitre, intitule "Intrusion Detection Systems et le Deep Learning" ce chapitre est dédié à la présentation des IDS (Intrusion Detection Systems). 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. Nous abordons aussi le Deep Learning (DL) et son application dans le domaine de la cybersécurité, nous explorons les concepts fondamentaux du DL, 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.

Le dernier chapitre : "contribution, résultat et discussion" 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.

Et enfin nous terminerons avec une conclusion générale, ainsi que quelques perspectives pour des travaux futurs.

Partie 1

Définitions et concepts de base

Chapitre I

Internet of Things et la sécurité

I .1 Introduction :

Ce premier chapitre permet de définir les notions de base de chaque concept, on commençant par l'objet connecté, l'internet des objets (IoT), après la sécurité dans IoT et on termine avec la sécurité pour la couche de routage de protocole RPL.

I.2 L'objet connecté :

Un objet connecté (OC) est un dispositif dont la principale fonction n'est pas d'être un système informatique ou une interface d'accès à Internet. Par exemple, une machine à café ou une serrure traditionnelle ont été conçues sans avoir intégrer de systèmes informatiques ou de connexion à Internet. Cependant, en ajoutant une connexion Internet à un OC, il devient un OC enrichi (OCE), ce qui lui permet d'offrir davantage de fonctionnalités et d'interagir avec son environnement. Un OC peut interagir avec le monde physique de manière autonome, sans intervention humaine. Il est soumis à diverses contraintes telles que la mémoire, la bande passante ou la consommation d'énergie, qui doivent être prises en compte lors de sa conception **[1].**

Figure 1.1: Objet connecté **[2].**

I.3 C'est quoi l'internet des objets :

Plusieurs définitions ont été données à l'internet des objets ou "Internet of Things (IoT)" en anglais, L'IoT est un réseau intelligent qui connecte tous les objets à l'internet dans le but d'échanger des informations selon des protocoles convenus **[3]**. Ainsi, n'importe qui peut accéder à n'importe quoi, à tout moment et de n'importe où **[4]**. Dans le réseau IoT, les choses ou les objets sont connectes sans fil avec de minuscules capteurs intelligents. Les dispositifs IoT peuvent interagir entre eux sans intervention humaine **[5].**

L'IoT utilise des schémas d'adressage uniques pour interagir avec d'autres objets ou choses et coopérer avec les objets pour créer de nouvelles applications ou de nouveaux services. L'IoT introduit diverses applications telles que les maisons intelligentes, les villes intelligentes, la surveillance de la sante, l'environnement intelligent et l'eau intelligente **[6]**. Avec le développement des applications ido soulevé de nombreuses questions. Parmi les nombreuses autres questions, celle de la sécurité de l'IoT ne peut être ignorée. Les dispositifs IoT sont accessibles de n'importe ou via un réseau non fiable comme l'internet. Les réseaux IoT ne sont donc pas protégés contre un large éventail d'attaques malveillantes.

Si les problèmes de sécurité ne sont pas résolus, les informations confidentielles peuvent être divulguées à tout moment. Le problème de la sécurité doit donc être résolu.

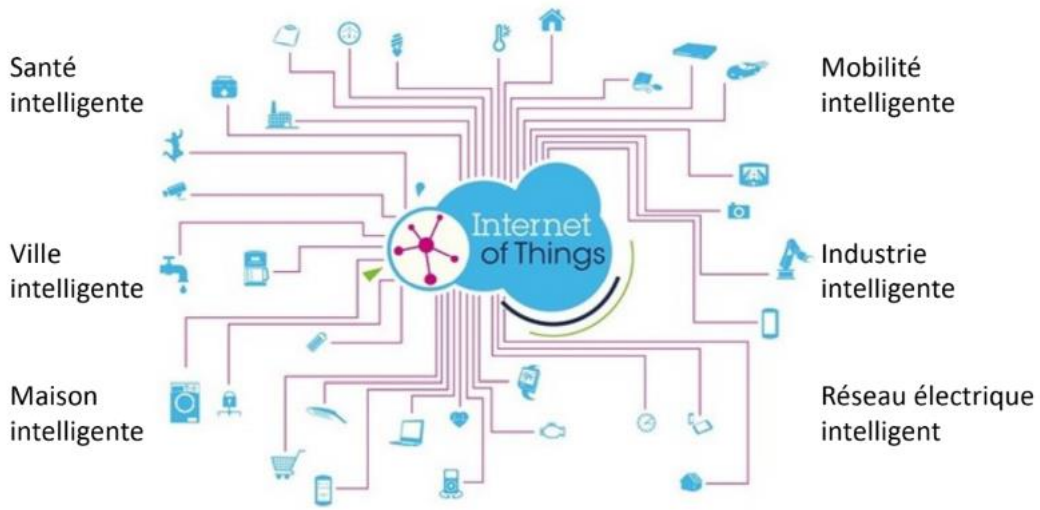

Figure 1.2: Internet des objets **[7].**

I.4 Les composants de l'IoT :

Les composants de l'IoT sont cinq, la composante principale de l'IoT est l'objet connecté, qui peut être conçu pour être connectable ou avoir une connectivité ajoutée ultérieurement. L'objet collecte et traite des données de capteurs, les communique et reçoit des instructions pour exécuter une action. Pour ces fonctions, une source d'énergie est généralement nécessaire, surtout si les données sont prétraitées dans l'objet **: [8]**

1. **Les capteurs :** Un capteur IoT est un dispositif électronique qui transforme une information physique (température, pression, débit...) en un signal électronique, il permet de collecter ces données physiques et les envoyer ensuite à un serveur ou

une plateforme IoT pour être analysées, traitées et utilisées pour prendre des décisions ou pour automatiser des systèmes. Exemples de capteurs : position, proximité, déplacement, accélération, lumière, température, humidité, son, vibration, chimique, gaz, flux, pression, etc.

2. **Les actionneurs :** L'actionneur est un dispositif matériel qui permet de transformer une information digitale en un phénomène physique, d'où sa dénomination. Un actionneur IoT permet de contrôler ou de modifier l'état d'un objet physique dans le monde réel, en fonction des données reçues à partir d'autres dispositifs IoT. Exemple d'actionneurs : Afficheurs, Alarmes, Caméras, Haut-parleurs, Interrupteurs, Lampes, Moteurs, Pompes, Serrures, Vannes, Ventilateur, etc.
3. **Énergie :** La contrainte la plus importante à laquelle les capteurs sont soumis est l'énergie. L'autonomie des nœuds est évaluée en termes d'années.
4. **Réseau de capteurs :** Les capteurs sont équipés de dispositifs sans fil pour émettre et recevoir des données, mais cela ne suffit pas pour rendre un ensemble de capteurs accessible et interopérable. Pour cela, les capteurs doivent s'organiser en un réseau de capteurs, qui est caractérisé par des éléments très petits avec des capacités de transmission sans fil.
5. **La connectivité :** Les objets IoT ont une antenne RF pour se connecter aux réseaux et transmettre des informations telles que leur identité, leur état, des alertes et des données de capteurs. De plus, ils peuvent recevoir les données et des commandes en retour. Le module de connectivité est essentiel à la gestion du cycle de vie de l'objet.

I.5 Domaines d'application :

L'IoT s'est déployé dans de nombreuses applications, comme le montre (**la figure 1.4)**. Elles sont devenues intelligentes et effectuent leur travail de manière robotisée en s'appuyant sur l'internet qui améliorerait le genre de nos vies personnelles, des entreprises et des communautés. Qui touche essentiellement : la domotique, les villes, le transport, la santé et l'industrie. Dans ce qui suit, nous présentons les domaines d'application les plus pertinents.

I.5.1 La domotique et les villes intelligentes :

- **La domotique :** ou maison connectée, représente l'utilisation de l'Internet des Objets dans une maison. Grâce à la domotique, Les humains utilisent de nombreux

appareils électroniques comme : les réfrigérateurs, les fours à micro-ondes, les ventilateurs, les chauffages et les climatiseurs à la maison. Les capteurs sont installés pour détecter les problèmes et les communiquer à l'entreprise de fabrication afin qu'elle les résolve.

- **Les smart cities :** Il existe aussi les villes intelligentes qui permettent d'améliorer la qualité de vie des habitants, en assurant une consommation de ressources minimales grâce à une combinaison intelligente des infrastructures (énergie, transport, communication) aux différents niveaux hiérarchiques (ville, quartier, bâtiment). La ville de Santander, en Espagne, a été l'une des premières, en Europe, à se lancer dans une stratégie smart city à grande échelle.

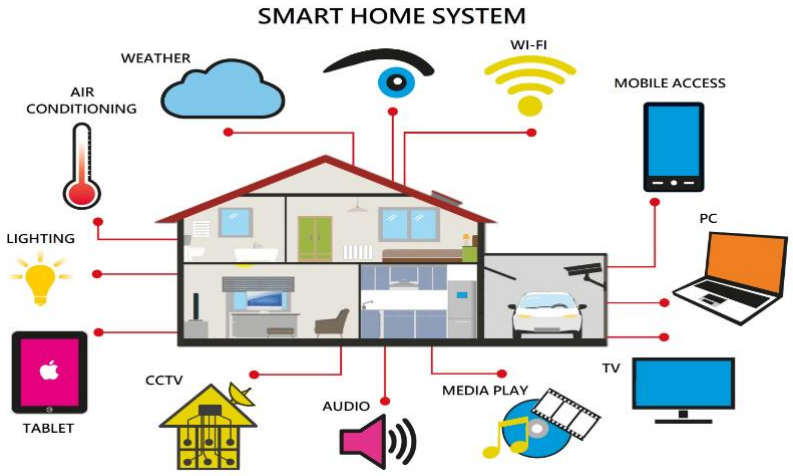

Figure 1. 3 : Système de maison intelligente **[8].**

I.5.2 Le transport :

Il existe plusieurs moyens de transport tels que les voitures, les trains, les bus, etc. Sont actuellement devenus intelligents en leur équipant par des capteurs, actionneurs et une puissance de traitement. L'IoT peut sauver des vies, car il peut réduire le trafic et minimiser l'impact des véhicules sur l'environnement.

Les voitures d'aujourd'hui évoluent pour devenir de véritables ordinateurs qui progressent vers la conduite autonome, comme les véhicules actuellement testés par Google. Bien que nos voitures ne soient pas encore totalement autonomes, elles deviennent de plus en plus autonomes grâce à des systèmes d'automatisation de certaines tâches de conduite, telles que l'allumage des phares ou le freinage automatique.

I.5.3 La santé (Smart Health) :

Dans le domaine de la santé, l'IoT joue un rôle essentiel, il permettra le déploiement de réseaux personnels pour le contrôle et le suivi des signes cliniques, les objets connectés permettent de suivre la tension, le rythme cardiaque, la qualité de respiration ou encore la masse graisseuse grâce à des capteurs et des puces. Ceci permettra ainsi de faciliter la télésurveillance des patients à domiciles notamment pour des personnes âgées pour les éviter de se déplacer jusqu'aux hôpitaux en particulier lorsqu'il s'agit d'une maladie très contagieuse telle que le COVID-19, la télémédecine est très recommandée. De nos jours, il existe aussi ce qu'on appelle les hôpitaux intelligents qui sont dotés de nouvelles technologies.

I.5.4 L'industrie :

Grâce à la technologie IoT, il sera possible d'assurer un suivi complet des produits, de la chaîne de production jusqu'à la chaîne logistique et de distribution, en surveillant les conditions d'approvisionnement. Cela permet aux usines d'améliorer l'efficacité de ses opérations, d'optimiser la production et d'améliorer la sécurité des employés.

I.5.5 L'énergie :

L'IoT facilite l'échange d'informations en temps réel entre les nombreux appareils du réseau électrique, permettant ainsi une distribution et une gestion de l'énergie plus efficace.

I.5.6 Le militaire :

Les objets connectés reliés à Internet offrent de nouvelles opportunités pour une utilisation militaire. En exploitant des technologies innovantes, ils pourraient fournir des solutions utiles dans le domaine militaire. Dans le domaine militaire, une application pertinente consiste à déployer un réseau de capteurs dans des zones stratégiques ou difficiles d'accès pour surveiller les activités des forces ennemies. Cependant, il est crucial de garantir une cybersécurité solide pour assurer l'efficacité de ces systèmes. Des essais concluants ont déjà été menés dans ce domaine par l'armée américaine **[9].**

I.5.7 L'agriculture :

Il utilise les technologies IoT qui permettent une gestion efficace des ressources. Cela peut aider à surveiller le développement des plantes et contrôler en cas de changements drastiques inattendu de l'évolution due à la température ou l'humidité. À l'aide de drones munis d'un système GPS, les exploitants peuvent ainsi recueillir en temps réel des données ou des images pour vérifier l'humidité du sol ou encore l'état des cultures et des plantations.

I.5.8 L'éducation :

Dans les années à venir, la majorité des établissements d'enseignement adopteront progressivement les technologies de l'IoT afin d'améliorer les processus d'apprentissage et l'enseignement à distance. En appliquant l'IoT dans l'éducation, l'efficacité opérationnelle de l'école, la sécurité du campus et la qualité de l'éducation peut être améliorée **[10].**

Voici quelques exemples concrets des applications de l'Internet des objets (IoT) dans le domaine de l'éducation :

• Surveillance des présences.

• Tableaux blancs intelligents et autres médias numériques interactifs.

• Sécurité sur le campus.

• Des cartes d'étudiant intelligentes.

• Capteurs de température et de l'équipement pour le chauffage, la ventilation et l'air conditionné pour réduire la consommation d'énergie **[11].**

I.5.9 Le sport :

L'utilisation de l'IoT dans le domaine sportif est de plus en plus courante, car elle a permis de développer des objets connectés pour les sportifs. Le premier objet qui vient à l'esprit est désormais le bracelet connecté pour but de donner les statistiques à des sessions de sport. D'une façon générale, on peut imaginer que n'importe quel accessoire de sport pourrait devenir un objet connecte comme par exemple : ballons connectés en Bluetooth qui calculent la puissance de frappe, la trajectoire et la rotation, des raquettes de tennis connectées, etc.

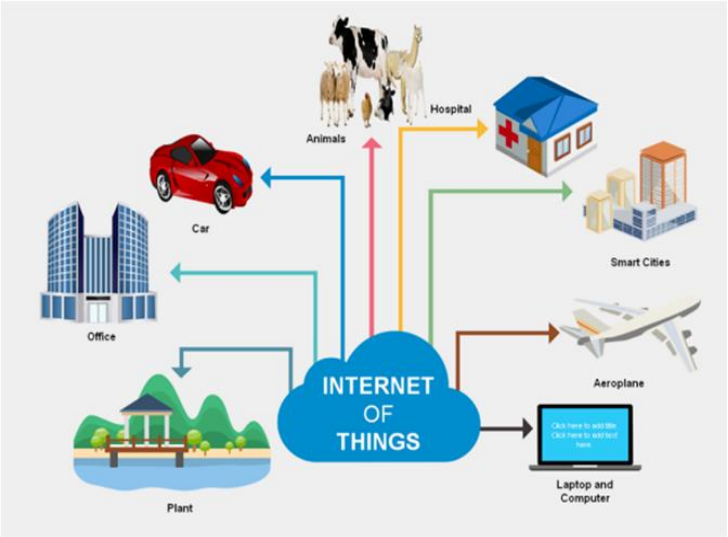

Figure 1.4 : Domaines d'application **[12].**

I.6 Architecture générale de l'IoT :

Différentes architectures ont été proposées. Parmi elles, on trouve les suivantes :

• **La couche de perception :** elle représente la couche physique, car la tâche principale de la couche de perception est de reconnaître les propriétés physiques telles que la température, l'humidité, le niveau de la lumière, la vitesse, etc. À l'aide, des capteurs et des actionneurs afin de recueillir des informations sur l'environnement, ces informations seront envoyées à la couche suivante **[13].**

• **La couche réseau :** également connue sous le nom de "couche de transmission" est une couche responsable de la connexion et la transmission des données reçues de la couche de perception. Elle est également utilisée pour transmettre et traiter les données des capteurs. Les principales technologies utilisées pour réaliser cette couche sont : les technologies cellulaires, WiFi, Bluetooth, Zigbee **[13].**

• **La couche d'application:** est la responsable de la gestion des interactions directe avec les utilisateurs finaux. Elle traite les données reçues de la couche réseau et elle est chargée de fournir à l'utilisateur des services spécifiques et applications intelligentes **[13].**

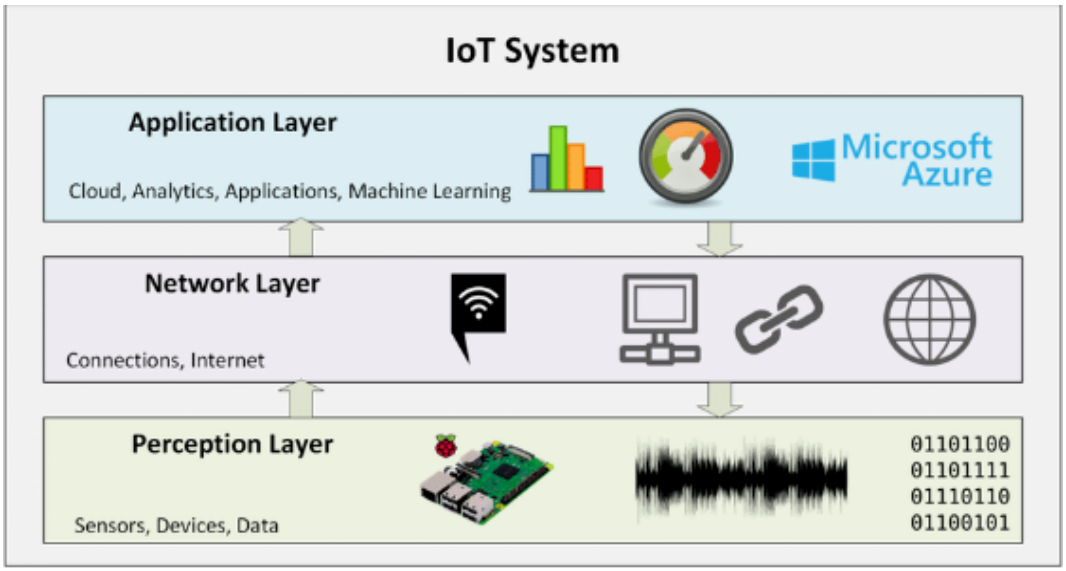

Figure 1.5 : Architecture générale de l'IoT **[14].**

• **Architecture à quatre couches :**

En raison du développement continu de l'Internet des objets, toutes les exigences de l'Internet des objets ne peuvent pas être satisfaites, pour cela une architecture a quatre couches a été proposé, elle comporte trois couches comme l'architecture précédente, mais elle comporte également une couche supplémentaire appelée couche de support. Le but de créer cette couche est la sécurité. Dans une architecture à quatre couches, les informations sont envoyées à la couche network obtenue à partir de la couche perception. La couche de support a deux responsabilités. Elle confirme que les informations sont envoyées par un utilisateur réel et utilise des méthodes d'authentification pour prévenir les menaces. La deuxième responsabilité est d'envoyer des informations à la couche réseau **[13].**

• **Architecture à cinque couches :**

L'architecture à quatre niveaux a joué un rôle important dans le l'évolution de l'IoT. L'architecture à quatre niveaux présentait également des problèmes de sécurité et de stockage. Les chercheurs ont proposé une architecture à cinq niveaux sont, la couche de perception, couche de transport, couche d'application de plus couche processing et couche Business **[13].**

• **La couche processing :**

Elle est connue sous le nom de couche middleware et joue le rôle de collecter les informations provenant de la couche de transport. Elle traite ensuite ces informations collectées et a la responsabilité de supprimer les données superflues **[13].**

• **La couche business :**

Sa responsabilité principale est de prendre en charge la gestion et le contrôle des applications. De plus, il possède la capacité de déterminer les modalités de création, de stockage et de modification des informations **[13].**

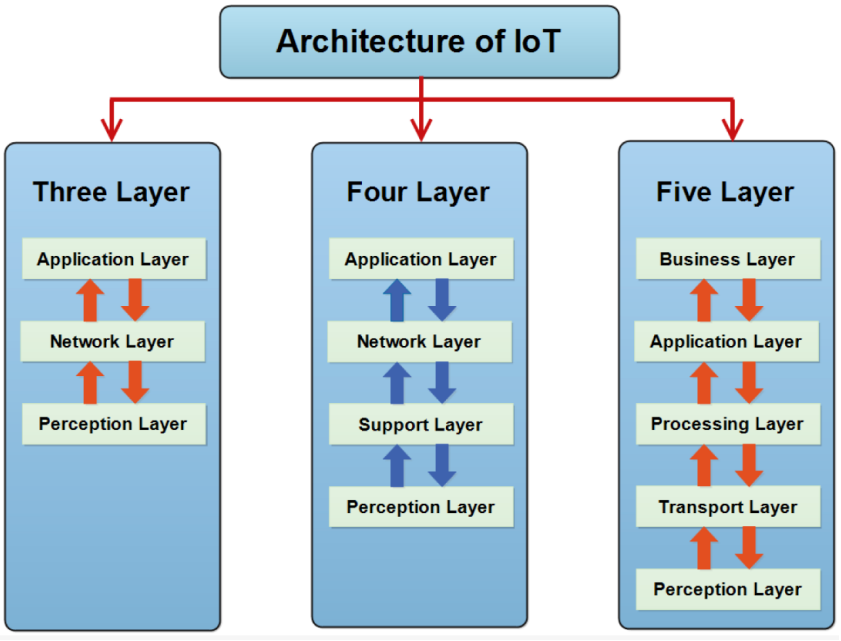

Figure 1.6 : Les architectures en couches de l'IoT (trois, quatre et cinq couches**) [13].**

I.7 Technologies de l'IoT :

Un système IoT réunit de nombreux acteurs et composants technologiques qui assurent le bon fonctionnement d'un système IoT. En effet, bien qu'il existe plusieurs technologies utilisées dans le fonctionnement de l'IoT, nous mettons l'accent seulement sur trois technologies clé, le RFID, WSN et M2M.

I.7.1 RFID :

La RFID est une technologie sans fil qui est utilisée pour l'identification des objets, dans laquelle une étiquette RFID (une petite puce avec une antenne) transporte des données qui sont lues par un lecteur RFID. Elle englobe toutes les technologies qui utilisent les ondes radio pour identifier automatiquement des objets ou des personnes. RFID utilise un ensemble de bandes de fréquences (125 kHz, 13,56 MHz, 433 MHz, 865-868 MHz, 2,45-5,8 GHz et 3,1-10 GHz). Sa portée varie selon la fréquence, elle peut aller jusqu'à des centaines de mètres **[15].**

I.7.2 WSN :

Un réseau de capteurs WSN (Wireless Sensor Network) est un réseau composé d'un ensemble de nœuds-capteurs, ces derniers sont capables de collecter, traiter, analyser et disséminer des informations et communiquent via des ondes radio afin de surveiller des phénomènes précis. Un nœud capteur est composé généralement d'interfaces de capture de

l'information, d'un microprocesseur, d'une unité mémoire, d'une interface de communication et d'une batterie comme source d'énergie **[16].**

I.7.3 M2M :

C'est l'association des technologies de l'information et de la communication avec des objets intelligents. Permettant une communication entre différentes machines ou équipements (véhicules, capteurs, caméras) connectés à différents réseaux sans l'intervention de l'humain. Les applications M2M utilisent différentes interfaces et protocoles pour les échanges entre les différents réseaux mobiles par exemple.

I.8 Protocoles de réseaux IoT :

Il existe des options de connectivité presque distinctes pour s'adapter aux applications modernes. Parmi ces protocoles, on peut citer :

La norme IEEE 802.15.1 / Bluetooth : Inventé en 1994 par la société suédoise Ericsson, le protocole Bluetooth est un standard de transfert de données sans fil. Elle a été standardisée sous la norme IEEE 802.15.1, il utilise une faible bande passante, ce qui ne lui permet de transférer que peu de données à de courtes distances. Inclus à l'immense majorité des téléphones mobiles, afin de réaliser une communication entre deux téléphones, ou entre un téléphone et un objet connecté de nature différente, il possède désormais de nombreuses applications : oreillette de discussion téléphonique sans fil, montre intelligente, moniteur de fréquence cardiaque, station météo, thermostat, domotique intelligente et un système de surveillance du trafic **[17].**

La norme IEEE 802.15.4/ Zigbee : Egalement connue sous le nom de Zigbee, est spécialement conçue pour les réseaux à dimension personnelle (Wireless Personal Area Networks : WPANs). Il permet la transmission de données sur de plus longues distances tout en offrant une faible consommation d'énergie, On retrouve ZigBee dans les contrôles industriels, les applications médicales, les détecteurs de fumée, etc **[17] ...** Elle offre la possibilité de créer des topologies réseau comprenant un très grand nombre de capteurs.

La norme IEEE 802.11x/WiFi : Le Wi-Fi regroupe un ensemble de protocoles de communication sans fil qui permettent des connexions haut débit sur des distances allant de 20 à 100 mètres. Cependant, il est important de noter que le Wi-Fi est un réseau local sans fil qui consomme beaucoup d'énergie, ce qui le rend plus adapté aux appareils alimentés sur secteur ou ayant une alimentation électrique régulière. Il offre la possibilité de transférer rapidement de grandes quantités de données **[17].**

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

SigFox : SigFox est une technologie de communication sans fil à faible consommation d'énergie conçue pour les objets à faible consommation comme les capteurs et les applications M2M. Elle permet de transférer de petites quantités de données sur des distances allant jusqu'à 50 kilomètres. Cette technologie est largement utilisée dans divers domaines tels que les compteurs intelligents, les moniteurs de patients, l'agriculture, les dispositifs de sécurité, l'éclairage public et les capteurs environnementaux **[17].**

Lora : LoRa (Long Range) est un protocole de communication sans fil conçue pour fournir les réseaux étendus de faible consommation et grande portée et une transmission de données sécurisée. La norme LoRa a été développée pour les dispositifs de type IoT dans les réseaux régionaux ou mondiaux **[18].**

I.9 Protocoles applicatifs :

Est un ensemble de règles définissant le mode de communication entre deux applications informatiques. Les protocoles de la couche application sont utilisés pour échanger des données entre les programmes s'exécutant sur les hôtes source et de destination. Il existe des protocoles de la couche application qui permettent la communication dans l'IoT **[19].**

- MQTT (Message Queuing Telemetry Transport)
- CoAP (Constrained Application Protocol)
- AMQP (Advanced Message Queuing Protocol)
- XMPP (Protocole de messagerie et de présence extensible)
- DDS (Data Distribution Service)

I.10 IPv6 et les IoT :

L'IoT englobe un nombre extrêmement élevé de nœuds, et il est essentiel que chaque nœud soit identifiable et accessible par tout utilisateur autorisé, peu importe sa position. Pour résoudre ce défi, l'utilisation de l'adressage IPv6 a été proposée pour l'IoT. Les adresses IPv6 sont représentées par des chiffres binaires de 128 bits, offrant ainsi une capacité suffisante pour identifier tous les objets qui nécessitent une adresse.

I.11 La pile protocolaire de l'IoT :

Différentes entreprises et organisations ont proposé plusieurs piles protocolaires pour L'IoT. La littérature présente des piles protocolaires constituées de trois couches : la couche de détection, la couche réseaux et communications et la couche d'applications, comme proposé par Minerva et al.**[20]**. En revanche, Granjal et al **[21]** ont proposé une pile protocolaire plus complète constituée de cinq couches : la couche physique, la couche MAC, la couche adaptation, la couche réseau et routage, et la couche d'applications.

Dans le contexte des objets connectés, les interfaces de communication sans fil de type 802.15.4 sont couramment utilisées. Ces protocoles radio ont une consommation énergétique très faible, ce qui permet de constituer des réseaux de faible puissance appelés LLN (Low-Power and Lossy Networks) ou LowPAN (LoW Power wireless Area Networks).

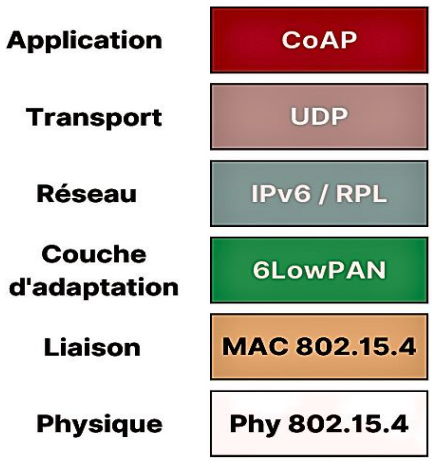

Figure 1.7 : la pile protocolaire de l'IoT **[22].**

Comme le montre la figure ci-dessus le réseau IoT est constitué d'une pile de six couches. Les couches "physique" et "MAC" sont supportées par les normes IEEE 802.15.4 et IEEE 802.15.4e. La couche adaptation utilise 6LoWPAN et la couche réseau utilise principalement le protocole RPL pour le routage. La couche application utilise CoAP pour le transfert web optimisé.

I.11.1 la couche physique :

La couche physique est chargée de gérer le support physique des transmissions. Elle détermine les méthodes de conversion des bits en signaux analogiques et inversement.

I.11.2 La couche MAC :

En plus de gérer la consommation d'énergie, considérée comme l'une des fonctions primordiales dans les réseaux de capteurs sans fil, la couche MAC est également responsable des tâches suivantes : les confirmations de réception, les créneaux horaires dédiés, la découverte des voisins, les balises, l'accès au canal physique, la validation des trames, l'association des nœuds et la sécurité, qui n'est disponible que dans cette couche selon la norme IEEE 802.15 **[21]**.

I.11.3 La couche adaptation :

La couche d'adaptation [6LowPAN] permet de faire passer des trames IPv6 dont le MTU est au minimum de 1280 octets dans des trames 802.15.4 (127 octets). Elle est conçue pour faciliter l'interopérabilité entre différents types de réseaux en IPv6 tels que l'Ethernet, le 802.15.4, le Wifi, la 4G, etc. Cette technologie permet de supporter les communications Internet pour l'IoT et standardise les protocoles de communication IoT ainsi que les communications de bout en bout entre les dispositifs capteurs IoT **[23]**.

I.11.4 La couche réseau :

La communication entre les nœuds du réseau est gérée par le protocole RPL, qui est un protocole de routage à vecteur de distance adapté aux réseaux peu fiables caractérisés par des pertes de paquets et une faible bande passante. Dans les LLN, où les pertes de paquets sont tolérées, les données sont généralement transportées par UDP, ce qui permet de limiter la taille des en-têtes **[23]**.

I.11.5 La couche application :

Le protocole CoAP (Constrained Application Protocol) est utilisé pour les communications de la couche application dans l'IoT en permettant l'interopérabilité avec l'architecture Web et les communications de bout en bout entre les périphériques IoT et les autres entités Internet. Ce protocole est actuellement limité aux communications UDP sur 6LoWPAN **[23]**.

I.12 Les défis de L'IoT :

L'IoT présente de nombreux défis, le plus important étant la sécurité. La protection des dispositifs IoT contre les cyberattaques est essentielle pour garantir la confidentialité, l'intégrité et la fiabilité des réseaux.

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 **[24]:**

- **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 **[24] :**

- 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.

I.13 Sécurité dans L'IoT :

Étant donné les problèmes de sécurité inhérents à l'IoT, il est impératif d'assurer la sécurité des systèmes IoT. Par conséquent, il est nécessaire de mettre en œuvre un système sécurisé pour l'Internet des objets, les normes et standards ont fixé des exigences de

sécurité qui garantissent la sécurité de l'information et du réseau. Nous présentons ci-dessous un résumé de ces exigences citées dans la littérature **[25]**.

I.13.1 Définition de la sécurité informatique :

La sécurité informatique est un domaine d'expertise utilisant un ensemble de techniques et de méthodes visant à prévenir, à détecter et à protéger les systèmes informatiques, les réseaux, les applications, les données et les utilisateurs contre les menaces qui peuvent les compromettre. Ça peut être un virus, des logiciels malveillants, des attaques par déni de service, des violations de données et des cyberattaques **[26].**

Les mesures de sécurité prisent en compte peuvent inclure l'utilisation de pares-feux, de systèmes de détection d'intrusion, de cryptage des données, de politiques de sécurité, de procédures de gestion des incidents, de formation des utilisateurs, de tests de pénétration et d'audits de sécurité.

- **La confidentialité :** Un attaquant peut facilement intercepter le message passant de l'expéditeur au destinataire, de sorte que la confidentialité peut être divulguée et le contenu modifie **[27].** Le passage de messages sécurisés est donc nécessaire dans l'IoT.
- **L'intégrité :** Le message ne doit pas être altéré en transit ; il doit être reçu au nœud récepteur tel qu'il a été envoyer au nœud émetteur. L'intégrité garantit que le message n'a pas été modifié par des personnes non autorisées pendant la transmission **[27]**.
- **La disponibilité :** Les données ou les ressources doivent être disponibles au moment voulu **[27]**. Les attaquants peuvent inonder la bande passante des ressources pour nuire à la disponibilité.

La disponibilité peut être endommagée par des attaques malveillantes telles que le déni de service (DOS), l'inondation, le trou noir, le brouillage ….etc.

- **L'authentification :** L'authenticité implique la preuve de l'identité. Les utilisateurs doivent être capables d'identifier l'identité des autres avec lesquels ils interagissent. Elle peut être vérifiée par le processus d'authentification afin que l'entité non autorisée ne puisse pas participer à la communication **[28]**.
- **La non-répudiation :** La non-répudiation garantit que l'expéditeur et le destinataire ne peuvent pas nier avoir envoyé et reçu le message respectivement **[29]**.

I.14 Vulnérabilité et Menaces dans L'IoT :

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 **[30] :**

- **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 provient principalement 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 essentiel 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 **[30]**.

I.15 La sécurité pour la couche réseau (Protocole RPL) :

LIETF (Internet Engineering Task Force) à découvert l'importance de créer un nouveau groupe de travail pour trouver une solution de routage IPv6 pour les réseaux d'objets intelligents IP, le nouveau groupe appelé *ROLL (Routing Over Low power and Lossy).*

Le groupe de travail de routage IETF sur des liaisons à faible puissance et avec perte *(ROLL)* a normalisé un protocole de routage indépendant des liaisons basé sur IPv6 pour les nœuds à ressources limitées appelés RPL (Routing Protocol for Low power and Lossy Networks), RPL a été créé pour prendre en charge les exigences de routage minimales grâce à la création d'une topologie robuste sur les liaisons avec perte.

Ce protocole de routage est responsable de : prend en charge des modèles de trafic simples et complexes tels que multipoint à point, point à multipoint et point à point **[31]**.

I.16 Le protocole de routage RPL :

Le protocole RPL est un protocole de routage proactif, et il est le standard recommandé par l'IETF pour les réseaux basse consommation et à faible puissance (LLN) et les réseaux de capteurs 6LoWPAN, il fonctionne sur la norme (IEEE 802.15.4). Il a été mis à jour en mars 2012. RPL offre une connectivité IPv6 à Internet et réduit également le coût pour atteindre la station de base à partir de n'importe quel nœud du LLN. Le protocole RPL est principalement destiné aux réseaux de collecte, où les nœuds envoient régulièrement des mesures à un point de collecte. Il a été spécialement conçu pour s'adapter aux conditions changeantes du réseau et pour fournir des itinéraires de secours en cas d'indisponibilité des itinéraires par défaut **[32].**

I.17 La topologie RPL :

Le protocole RPL établit une structure de routage appelée DODAG (Directed Acyclic Graph) qui est enracinée au niveau de la passerelle. Le DODAG est construit selon un processus de découverte de voisins (Neighbor Dis-covery (ND)). C'est un arbre de routage créé par un nœud racine, il décrit les liens orientés entre les nœuds, se terminant à un ou plusieurs nœuds racines, ou chaque nœud peut transmettre des données à son nœud parent, qui les transmet à son tour vers le haut jusqu'à ce qu'elles atteignent le nœud de destination

ou la passerelle. De même, le nœud de destination peut envoyer un message unicast pour cibler un nœud spécifique dans son réseau **[33].**

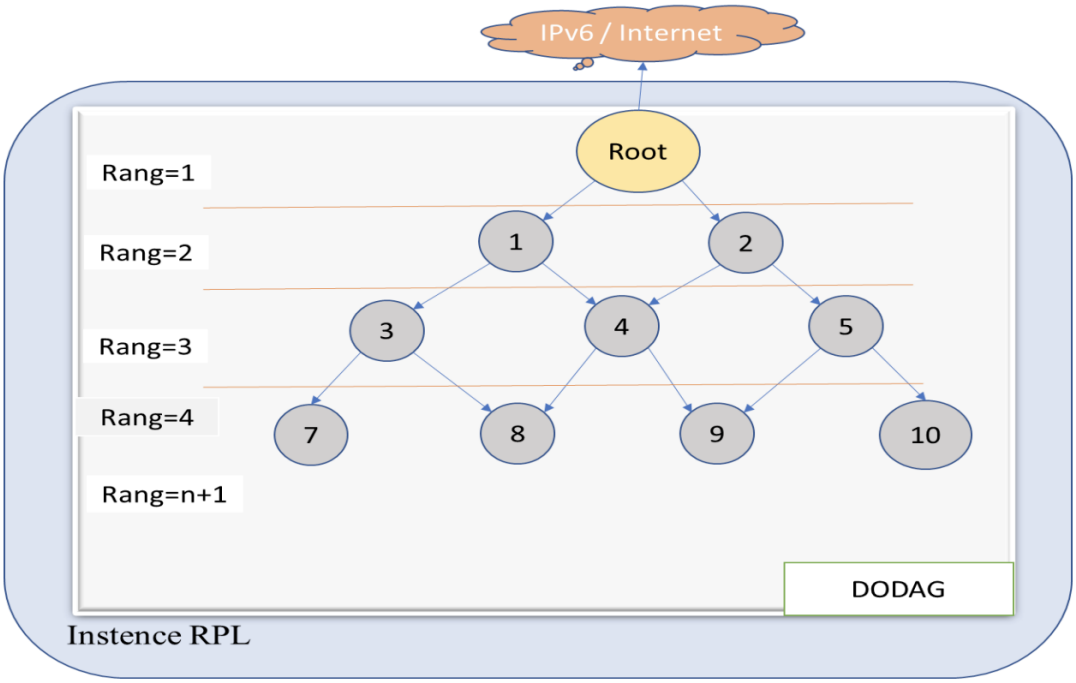

Figure1.8 : Partition de topologie RPL **[34].**

I.18 Taxonomie des attaques sur RPL :

La taxonomie des attaques de routage dans les réseaux IoT est présentée dans **(la figure 1.9)** et se divise en trois catégories principales. Dans cet article, les attaques de routage dans les réseaux IoT ont été largement classées en trois catégories **[42] :**

1. **Attaques contre les ressources du réseau :** celles-ci visent à faire consommer à un nœud légitime ses ressources énergétiques, de traitement ou de mémoire dans le but de perturber la disponibilité du réseau. Ces attaques sont particulièrement dangereuses pour les réseaux contraints, car elles réduisent considérablement la durée de vie des appareils et donc du réseau RPL. On peut distinguer deux grandes catégories d'attaques contre des ressources :

• **Attaques directes :** où le nœud malveillant provoque directement une sur- charge pour perturber le réseau. Par exemple : attaques d'inondation (flooding) et attaques de surcharge de la table de routage (routing table overload).

• **Attaques indirectes :** où le nœud malveillant incite les autres nœuds à générer de la surcharge. Comme les Attaques d'augmentation du rang (increasing rang attack), Attaques d'incohérence de DAG (DAG inconsistency) et les attaques par modification du numéro de version (version number modification).

2. **Attaques contre la topologie du réseau :** ces attaques ont pour objectif de perturber la structure du réseau RPL. Les attaquants cherchent soit à optimiser de manière sub-optimale la topologie du réseau, soit à isoler un groupe de nœuds RPL du reste du réseau. Cette catégorie peut également être classée en deux sous-catégories différentes en fonction des conséquences qui en résultent :

• **La sous-optimisation :** qui signifie que le réseau convergera vers une forme non-optimale, induisant de mauvaises performances, comme : attaque de falsification de table de routage (routing table falsification), Attaque de puit (sinkhole), wormhole et (Routing Information Replay Attacks).

• **L'isolation :** d'un nœud ou un ensemble de nœuds, les coupant du reste de la topologie RPL, y compris du nœud racine. Comme : l'attaque de trou noir (Blackhole) et Les Attaques d'incohérence DAO (DAO Inconsistency Attacks).

3. **Attaques contre le trafic réseau :** cette catégorie concerne les attaques contre le trafic réseau qui vise généralement à capturer les informations transmises par les nœuds. Telles que les attaques de spoofing ou les attaques de tromperie. Cette catégorie se subdivise à nouveau en deux sous-catégories en fonction de l'objectif poursuivi :

• **L'écoute (Eavesdropping Attacks) :** des informations qui sont transmises par le réseau pour recueillir le trafic du réseau comme : sniffing et l'analyse du trafic du réseau.

• **Le détournement :** d'un nœud ou d'un ensemble de nœuds, notamment pour altérer les informations légitimes échangées, comme les attaques du rang diminué (Decreased Rank Attacks) et les Attaques d'identité (Identity Attacks).

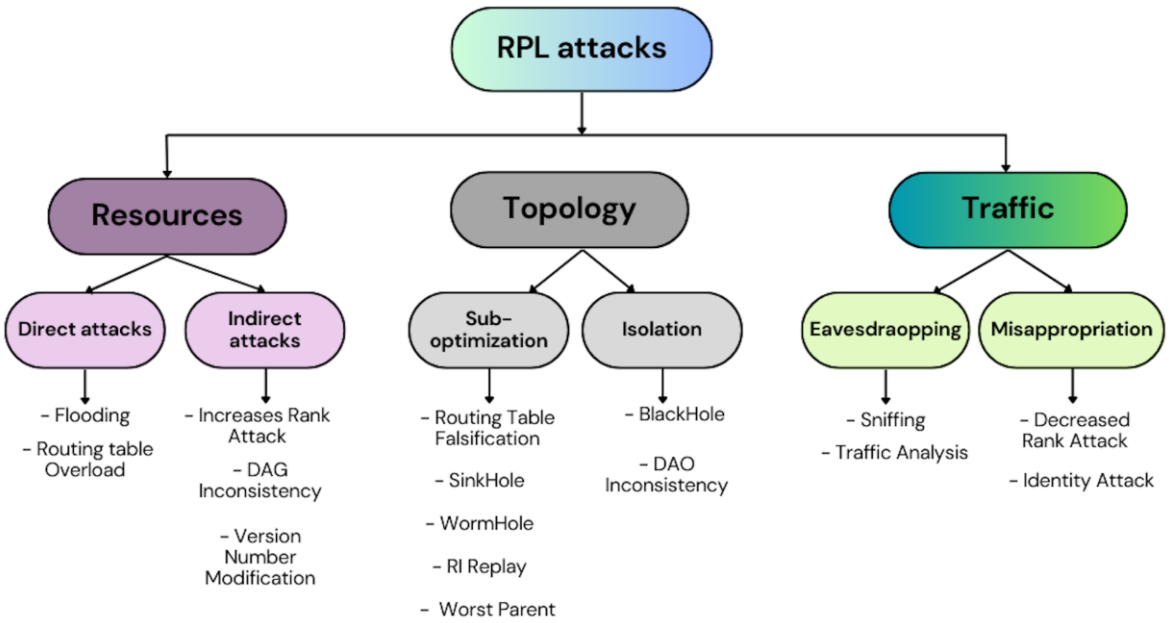

Figure 1.9: Taxonomie des attaques sur le RPL **[42].**

I.19 Attaques sur le protocole RPL :

Le protocole RPL est exposé à diverses attaques de sécurité lors du transfert de paquets de données entre les appareils. Les caractéristiques des réseaux LLN, telles que les ressources limitées, le manque d'infrastructure, la sécurité physique limitée, les topologies dynamiques et les liaisons peu fiables, les rendent particulièrement vulnérables et difficiles à défendre contre les attaques. Ça peut-être bien que spécifique au protocole RPL, il s'applique également aux réseaux de capteurs sans fil, et aux réseaux filaires **[35].** Dans ce qui suit nous présenterons les attaques courantes sur RPL.

I.19.1 Attaques contre les ressources :

- **Attaque DIS**

Des messages de contrôle liés au RPL sont transmis dans le réseau pour construire une structure de transmission optimisée. Les nœuds malveillants internes peuvent attaquer le réseau RPL en envoyant un grand nombre de messages de contrôle inutiles. L'une de ces attaques cible les messages de contrôle DIS envoyés par de nouveaux nœuds pour rejoindre le réseau. Cette attaque est appelée attaque DIS. Lorsqu'un nouveau nœud souhaite rejoindre le réseau, il envoie périodiquement des messages de contrôle DIS pour demander des informations d'autorisation. Les nœuds malveillants peuvent exploiter ce processus en inondant le réseau d'un grand nombre de messages DIS, ce qui affecte négativement les performances du réseau. Cette attaque est conçue pour perturber le fonctionnement normal

des protocoles de routage en augmentant le trafic inutile et en épuisant les ressources du réseau. Les conséquences d'une telle attaque pourraient inclure une congestion du réseau, une consommation d'énergie accrue et une qualité de service réduite **[36].**

- **Version number attack**

Le numéro de version est un champ important de chaque message DIO. Il est propagé sur le graphe DODAG et est incrémenté par la racine seulement, chaque fois, la reconstruction du DODAG est nécessaire, Dans cette attaque, l'attaquant augmente le champ du numéro de version dans les messages DIO et les transmet à ses voisins. En conséquence, la reconstruction inutile d'un nouveau DODAG est forcée, ce qui entraîne la perte de paquets de données, l'encombrement du réseau et l'épuisement des ressources des nœuds en raison de la surcharge des messages de contrôle **[35].**

- **Attaque DOS**

Un attaquant pourrait essayer d'envoyer de nombreux messages pour brouiller un canal réseau. Cela réduit les performances et l'efficacité du réseau. Un attaquant extérieur pourrait lancer une attaque par déni de service (DoS) en envoyant des messages invalides sur le réseau et en exfiltrant les messages des nœuds légitimes. Cela empêche les nœuds légitimes de traiter les messages en raison de messages non-valides provenant d'attaquants. Par rapport aux attaques DoS, les attaques par déni de service distribué (DDoS) sont des attaques plus graves dans lesquelles un groupe de nœuds voyous lancent des attaques contre des nœuds légitimes à différents endroits et à différents moments. Ce type d'attaque consomme des ressources, réduit la capacité du réseau et empêche le réseau de fonctionner correctement ou en temps opportun **[37].**

I.19.2 Attaques contre la topologie :

- **Attaque Sinkhole**

Dans une attaque sinkhole, un nœud compromis achemine intentionnellement tout le trafic provenant de sa zone voisine vers lui-même en diffusant de fausses informations, un attaquant ou un nœud compromis essaie d'inciter d'autres nœuds à envoyer des données en se faisant passer pour les relais les plus attrayants de leur voisinage. Le but de cette attaque est d'intercepter et de manipuler les données lorsqu'elles traversent le réseau **[37].**

- **Attaque Rank**

L'un des principaux éléments de conception de RPL est son mécanisme de classement, qui utilise la propriété de classement pour assurer un routage sans boucle. Un nœud peut changer sa valeur de classement en manipulant les valeurs de rang () des nœuds de manière malveillante et tromper ses nœuds voisins après avoir rejoint un réseau RPL. L'objectif de cette attaque est de créer une topologie sous-optimale, entraînant un trafic de données empruntant des chemins réseau de moindre qualité de service (QoS). Plusieurs nœuds adjacents changeront ultérieurement leur parent préféré actuel. Cela peut alors déclencher plus facilement d'autres attaques, comme les trous noirs et aggraver les choses. L'objectif principal des deux modes d'attaque de classement est de déstabiliser le réseau **[36].**

- **Attaque Wormhole**

Une attaque par trou de ver est une attaque grave qui peut être lancée même lorsque l'authenticité et la confidentialité sont garanties dans toutes les communications. Une attaque par trou de ver est une attaque dans laquelle deux ou plusieurs nœuds attaquants sont connectés par un lien appelé lien de trou de ver, et les nœuds forment un tunnel pour diffuser des paquets de données dans le réseau. Dans le cas d'un réseau sans fil, il est plus facile d'effectuer cette attaque, car un attaquant peut envoyer à travers le trou de ver le trafic qui lui est envoyé ainsi que tout trafic intercepté lors de la transmission sans fil. L'attaque par trou de ver déforme le chemin de routage et est particulièrement problématique pour les réseaux RPL. Si un attaquant transmet des informations à une autre partie du réseau, les nœuds qui sont en fait éloignés se verront comme s'ils étaient dans le même voisinage. En conséquence, ils peuvent générer des routes non optimisées vers la fonction objective. Cela embrouille le réseau et perturbe le processus de communication. **[35].**

- **Attaque Blackhole**

Dans cette attaque, le nœud attaquant prétend qu'il a le chemin le plus court vers la destination le nœud de contrôle (appelé node sink), après avoir illégalement changé son rang. Dans une attaque par trou noir, un intrus malveillant sa seule mission est alors de ne rien transférer, créant une sorte de puits ou de blackhole dans le réseau. Laisse tomber tous les paquets qu'il est censé transmettre. Cette attaque peut être très préjudiciable lorsqu'elle est combinée à une attaque de gouffre **[38],** entraînant la perte d'une grande partie du trafic. Elle peut être considérée comme un type d'attaque par déni de service. Si l'attaquant occupe une position stratégique dans le graphe, il peut isoler plusieurs nœuds du réseau. Il existe également une variante de cette attaque appelée trou gris (ou attaque par transfert sélectif) dans laquelle l'attaquant ne rejette qu'une partie spécifique du trafic du réseau

[35]. Les nœuds doivent communiquer de manière adéquate pour former un DODAG légal sans problème. En outre, lors du lancement d'une attaque par trou noir, le nœud malveillant ne génère aucun message de contrôle **[39].** Une attaque par trou noir peut être orchestrée par un seul nœud malveillant ou par un groupe de nœuds malveillants qui s'entendent pour rendre l'attaque plus difficile à détecter **[40].**

I.19.3 Attaques contre le trafic :

- **Attaque Sybil**

Sybil est également appelée l'attaque « nœud unique avec plusieurs identités ». Le nœud malveillant affiche un identifiant différent et peut se trouver à plusieurs endroits en même temps et il ressemble à un cœur ordinaire. Ce dernier peut exploiter le mécanisme de transmission DIS pour attaquer également le réseau. Si le nœud malveillant génère et multidiffuse un grand nombre de messages DIS superposés avec différentes identités fictives, tous les nœuds récepteurs vont croire que de nouveaux nœuds veulent rejoindre le réseau, puis redémarrer l'algorithme Trickle depuis le début à plusieurs reprises et diffuser un nombre excessif de messages DIO. Cette attaque dégrade les performances du système **[41].**

- **Attaque analyse du trafic**

Permettent d'obtenir des informations sur le routage en analysant les schémas de trafic d'une liaison, même si les paquets sont chiffrés. L'objectif est de collecter des informations sur le réseau RPL, telles qu'une vue partielle de la topologie en identifiant les relations entre les nœuds parents et enfants. Un nœud malveillant peut ensuite utiliser ces informations pour mener d'autres attaques. Si l'attaquant est proche du nœud racine, il peut traiter un volume de trafic plus important et obtenir davantage d'informations que s'il se trouve en périphérie d'un sous-DODAG **[35].**

I.20 Mécanisme de sécurité pour IoT :

Les mécanismes de réponse aux menaces et attaques informatiques sont un ensemble de procédures et d'outils qui permettent de d´détecter, de gérer et de résoudre les incidents de sécurité. On peut distinguer deux approches :

• **Approche réactive :** consiste `à réagir aux problèmes de s´sécurité une fois qu'ils se sont produits. Cela peut inclure **[43] :**

1. **Anti-virus et anti-malware :** ces logiciels sont utilisés pour d´détecter et ´éliminer les virus et les logiciels malveillants.

2. **IDS :** Un système de d´détection d'intrusion est un système de s´sécurité informatique qui surveille les activités du réseau ou d'un système informatique pour d´détecter toute activité malveillante ou non autorisée.

• **Approche préventive :** consiste à mettre en place des mesures pro-actives pour réduire les risques de s´sécurité avant qu'ils ne surviennent. Cela inclut des mesures tels que **[43] :**

1. **Pare-feu :** un pare-feu est une barrière de s´sécurité qui bloque le trafic non autorisé entre un réseau privé et Internet**.**
2. **Cryptographie** : la cryptographie permet de chiffrer les données afin qu'elles ne soient pas accessibles à des tiers non autorisés**.**
3. **Contrôle d'accès :** le contrôle d'accès permet de définir les autorisations d'accès à un système ou à des données pour les utilisateurs et les groupes**.**
4. **Sécurité physique :** la sécurité physique comprend des mesures telles que la surveillance vidéo, les portes à serrure électronique et les barrières pour empêcher l'accès non autorisé aux locaux**.**
5. **Gestion des identités et des accès :** la gestion des identités et des accès (IAM) permet de gérer les identités des utilisateurs et leur accès aux systèmes et aux données**.**
6. **Tests de pénétration :** les tests de pénétration sont des tests effectués pour évaluer la sécurité d'un système en simulant une attaque**.**

I.21 Conclusion :

En conclusion, l'Internet des objets (IoT) représente une avancée majeure dans le domaine de la connectivité et de la technologie et offre un potentiel énorme pour améliorer notre vie quotidienne. Au cours de ce chapitre, nous avons examiné les généralités de l'IoT, en comprenant ses composants essentiels, ses applications diverses et ses implications pour l'avenir. Nous allons approfondir notre compréhension de la sécurité dans les réseaux IoT utilisant le protocole RPL, ainsi que des différentes attaques auxquelles ils sont susceptibles d'être confrontés. Le chapitre suivant se concentrera sur les systèmes de détection d'intrusions (IDS).

Chapitre II

Intrusion Detection Systems

II.1 Introduction :

Le système de détection d'intrusion (IDS) est une invention qui répond à ces exigences de sécurité. Il est adopté pour le but d'empêcher toutes les menaces imminentes de violation des politiques de sécurité, des réseaux et des systèmes informatiques. Le noyau de ce système est un module de reconnaissance des intrusions efficaces, robustes et évolutifs. Il est aussi l'élément clé de tout produit de cybersécurité.

II.2 Intrusion :

Action (ou tentative d'action) qui a pour conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité d'une ressource (violation de la politique de sécurité) **[44].**

II.3 Détection d'intrusions :

Les techniques de détection d'intrusion tentent de faire la distinction entre une utilisation normale du système et une tentative d'intrusion, tout en émettant des alertes. En règle générale, les données d'audit du système sont analysées à la recherche d'intrusions connues ou de signatures comportementales inhabituelles. La détection peut se faire en temps réel, auquel cas un programme IDS peut déclencher une alerte et un personnel qualifié peut tenter de remédier à l'intrusion en coupant la liaison ou en se mettant en piste **[45].**

II.4 Définition d'un système de détection d'intrusions :

On appelle système de détection d'intrusion, en anglais **I**ntrusion **D**etection **S**ystem ou (IDS), tout système combinant logiciel et matériel, qui permet d'écouter le trafic du réseau de manière furtive et en temps réel afin de repérer les tentatives d'intrusion sur un réseau interne ou sur un ordinateur hôte pour permettre une prévention contre les intrusions qui visent à compromettre la **confidentialité** (Pour chaque information, on définit l'ensemble d'utilisateurs autorisés à y accéder), **l'intégrité** des données (Les données n'ont pas été modifiées) et la ***disponibilité*** (les services du système doivent être opérationnels et accessibles) **[46]**.

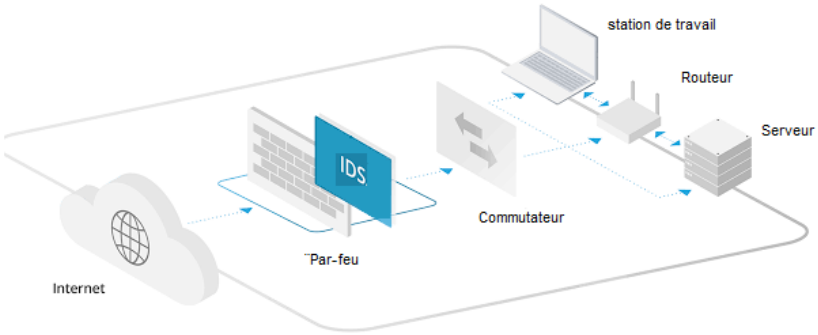

Figure 2.1: L'emplacement d'un IDS

Certains termes sont souvent employés quand on parle d'IDS :

• **Faux positif** : une alerte provenant d'un IDS, mais qui ne correspond pas à une attaque réelle (Fausse alerte).
• **Faux négatif** : une intrusion réelle qui n'a pas été détectée par l'IDS.
• **Vrai négatif et Vrai positif** : correspondent aux comportements souhaités.

II.5 Architecture de base d'un système de détection d'intrusions :

Le groupe IDWG (**I**ntrusion **D**etection exchange format **W**orking **G**roup) de l'IETF (**I**nternet **E**ngineering **T**ask **F**orce) **[47],** a proposé une architecture de base d'un système de détection d'intrusion.

Cette architecture définit un format d'échange de message pour les IDS : Intrusion Detection Message Exchange Format (IDMEF), qui contient implicitement un modèle de données.

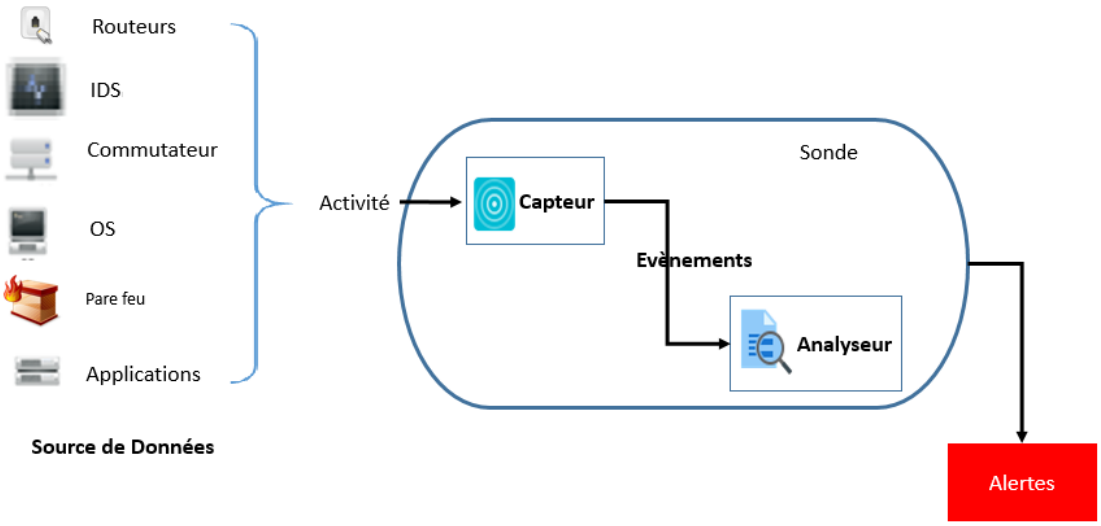

Figure 2.2: Modèle générique de la détection d'intrusions proposé par l'IDWG **[48].**

Cette architecture est composée des modules suivants :

- **Source de données** : Appelée aussi sonde de capture, c'est l'interface entre le système surveillé et l'IDS, c'est la collecte d'informations sur les activités non autorisées du système. Sa position joue un rôle stratégique dans la détection des intrusions.
- **Capteur** : charge de collecter et filtrer les informations brutes envoyées par la source de données. Le résultat de ce traitement sera un message formaté, appelé évènement, après il fait le transfert des évènements à l'analyseur.
- **Analyseur** : il est responsable de l'analyser des évènements générés par le capteur. Et en cas de détection d'une activité indésirable il le signale à l'administrateur de sécurité. Dans cette architecture, le capteur et l'analyseur forment ensemble une sonde.
- **Manager (Alerte)** : en plus de la notification des **alertes**, il offre à l'administrateur la possibilité de configurer une sonde et de gérer des rapports.
-

II.6 Classification des IDS :

Plusieurs critères de classification des IDS ont été proposés. Dans **[49],** Debar propose une taxonomie qui utilise plusieurs critères pour la classification des IDS **(voir la figure 2.3)**: les méthodes de détection (comportemental ou par scénario), les sources

d'informations, la réaction après détection, la fréquence d'utilisation ou bien la stratégie de contrôle.

1. **Méthode de détection :**

Il existe deux principes de détections :

- L'approche comportementale modélise le comportement normal des utilisateurs, du système informatique et de l'activité réseau. Ensuite, toute action suspecte par rapport à la normale constitue un événement suspect.
- L'approche, appelée détection par connaissances, recherche explicitement les signatures des attaques connues dans les fichiers de sécurité et le trafic réseau.

2. **Source d'information** :

- Les données analysées divisent les systèmes de détection d'intrusions en deux catégories : les systèmes de détection d'intrusions réseaux et les systèmes de détection d'intrusions hôtes : La première catégorie des IDS filtre le trafic réseau et se déploie généralement dans des endroits précis du réseau, par exemple dans la zone démilitarisée, un brin réseau contenant des serveurs internes ou juste avant ou/et après un pare feu.
- La deuxième catégorie des IDS analyse les données des journaux de sécurité établis par les systèmes d'exploitation et les applications qui tournent sur les machines. Ces IDS sont déployés directement sur les hôtes du réseau.

3. **Réponse des IDS** : les systèmes de détection d'intrusions émettent des réponses active qui influent directement la source d'attaque, comme ils peuvent se restreindre à des réponses passives qui inscrivent l'événement suspect.
4. **Paradigme de détection** : la détection d'intrusions s'effectue en analysant l'état courant du système ou en supervisant les transitions des états normaux aux états dangereux. Durant ces deux types d'inspection, l'IDS récupère les informations en interrogeant directement le système ou en écoutant passivement les événements.
5. **Mode de supervision** : l'analyse assurée par un système de détection d'intrusions peut être continue ou périodique dans le temps.

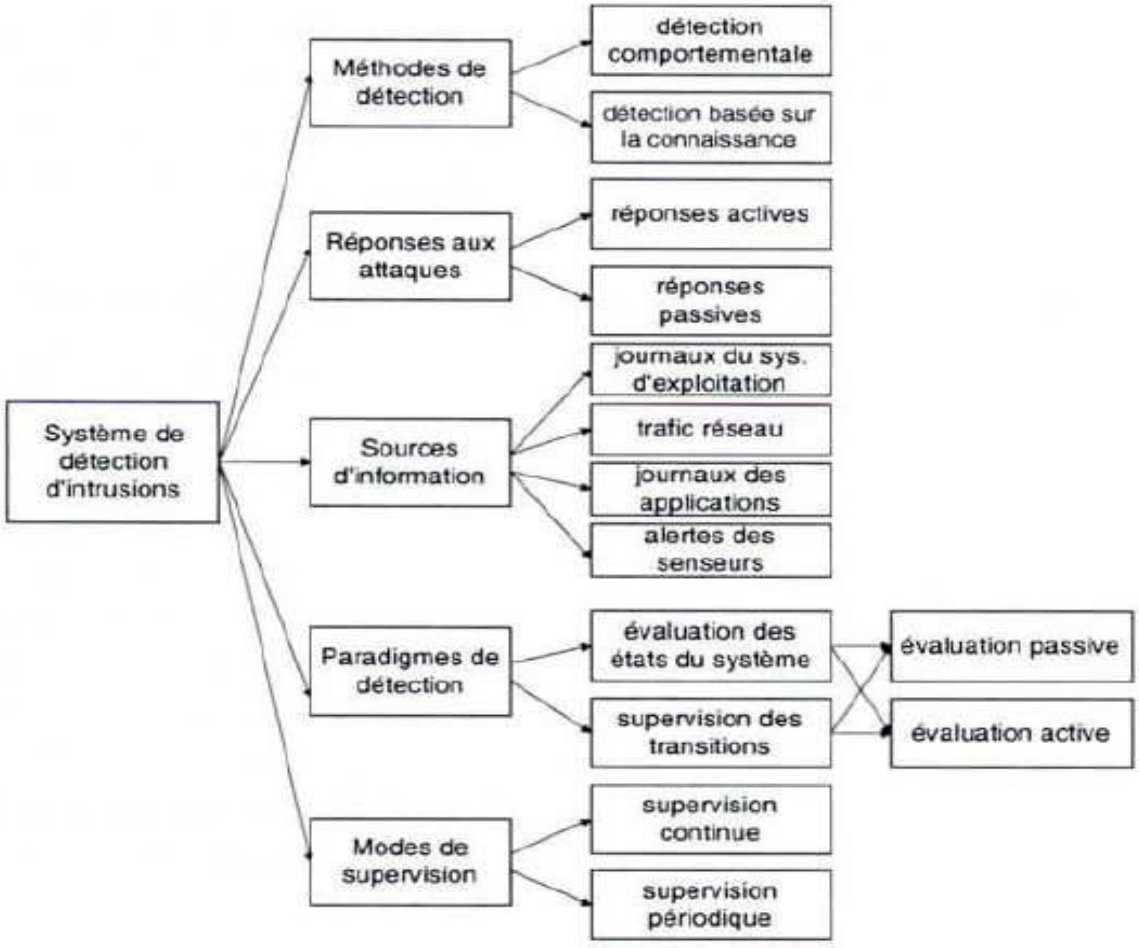

Figure 2.3: Classification IDS **[49].**

II.7 Les types d'IDS :

Il existe deux grandes familles d'IDS **[50]** :

- Les **N**etwork based **I**nusion **D**etection **S**ystem ou NIDS pour la sécurité au niveau réseau.
- Les **Host** based **I**nusion **D**etection **S**ystem ou HIDS pour la sécurité au niveau des hotes.

II.7.1 Systèmes de détection d'intrusion réseau (NIDS) :

Les NIDS (**N**etwork based **I**nusion **D**etection **S**ystem) sont utilisés pour contrôler les paquets circulant sur un ou plusieurs réseaux, dans le but de découvrir une intrusion. Un IDS réseau opère au niveau des couches réseau, transport et application. Ce système place les cartes d'interface réseau du système qu'on veut protéger en mode promiscuité (appelé aussi mode promiscuous). Ces cartes sont en mode **f**urtif. Ce genre de sondes sont placés à

l'extérieur du réseau pour analyser les tentatives d'attaque et à l'intérieur afin d'analyser les requêtes traversant le pare-feu ou dirigées depuis l'intérieur **[50].**

- **Les avantages de NIDS :**

- Surveillance discrète du réseau donc invisible pour les attaquants.
- Détecte plus facilement les scans grâce aux signatures.
- Filtration du trafic
- Pas besoin d'une base d'attaque
- Peu de faux négatif
- Assurer la sécurité contre les attaques puisqu'il est invisible.

- **Les limites des NIDS :**

- Impossible de détecter des attaques dans un trafic chiffré.
- Problème de bande passante si le trafic réseau est important.
- NIDS est tolérant aux faux positifs, En cas de profonde modification dans le système surveillé, déclenchement d'un flot ininterrompu d'alertes.
- Une NIDS mal positionné peut ne pas être efficace.

II.7.2 Systèmes de détection d'intrusions hôtes (HIDS) :

Les systèmes (HIDS) sont installés sur un hôte (poste de travail, serveur, etc.). Le HIDS analyse les captures des paquets réseaux entrant et sortant de la machine, et les informations particulières, au seins des journaux de traces (syslog, lastlog,wtmp,..), dans le but de constater une intrusion (déni de service, porte dérobée, chevaux de Troie, tentatives d'accès non autorisées, exécution du code malicieux, attaques par débordement de tampons…) **[51].**

- **Les avantages de HIDS :**

- La détection des attaques dans un trafic chiffré.
- Ils peuvent empêcher les attaques de causer des dommages, donc une meilleure réaction aux attaques.
- Une observation avec précision des activités du système.
- Les HIDS sont un outil de "dernière ligne de défense" utilisé pour conjurer les attaques manquées par le NIDS.

- **Les limites des HIDS :**
  - Vulnérable aux attaques du type DOS (Denie of service).
  - Consommation de ressources matérielles (CPU, etc…)
  - Difficultés à détecter les scans.

II.8 Les autres IDS :

II.8.1 Les IDS Hybrides :

Un IDS hybride est une combinaison des caractéristiques des HIDS et NIDS. Il fait la surveillance pour les réseaux et les hôtes on se basant sur une architecture distribuée **[52].**

II.9 Méthode de détection d'intrusions :

Deux méthodes sont principalement utilisées par les systèmes de détection d'intrusion : la reconnaissance de signatures et la détection d'anomalies **[53]**.

- **L'approche par signature ou par scenario :**

La reconnaissance de signatures est une approche consistant à rechercher dans l'activité de l'élément surveillé les signatures (ou empreintes) d'attaques connues.

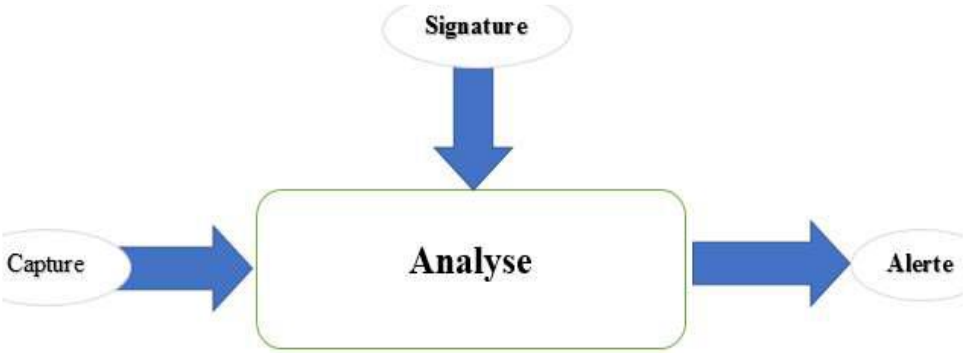

Figure 2.4 : Approche par signature

- **L 'approche comportementale ou par anomalie :**

Pour sa part, la détection d'anomalies se fait grâce à l'analyse de statistiques du système : changement de mémoire, utilisation excessive de l'unité centrale, comportement inhabituel des utilisateurs, etc.

II.10 Positionnement de L'IDS dans l'IoT :

L'emplacement d'un IDS (Système de Détection d'Intrusion) dans l'IoT dépend de plusieurs facteurs, tels que les objectifs de sécurité, les contraintes de performance, les

caractéristiques du réseau IoT et les types de menaces ciblées. Voici quelques options d'emplacement possibles pour un IDS dans l'IoT **[54] :**

- **Emplacement au niveau du périphérique (End-point)** : L'IDS est directement intégré dans les périphériques IoT pour surveiller les activités et d´détecter les comportements anormaux. Cela permet une détection précoce des intrusions au niveau des périphériques individuels, mais peut n´nécessiter des ressources matérielles et logicielles suffisantes.
- **Emplacement au niveau de la passerelle (Gateway) :** L'IDS est déployé sur une passerelle IoT, qui agit comme un point d'entrée centralisé pour les périphériques connectés. Cela permet de surveiller et d'analyser le trafic entrant et sortant de l'IoT, offrant une visibilité et une protection globales.
- **Emplacement au niveau du réseau :** L'IDS est positionné au sein du réseau IoT, surveillant le trafic entre les périphériques, les passerelles et les serveurs IoT. Cela permet de détecter les activités suspectes ou les anomalies au niveau du réseau, mais peut nécessiter une infrastructure réseau adaptée pour l'inspection du trafic.
- **Emplacement dans le cloud :** L'IDS est hébergé dans le cloud, où il analyse le trafic provenant de multiples sources IoT. Cela offre une évolutivité et une centralisation des fonctions d'analyse, mais nécessite une connexion Internet fiable et peut soulever des préoccupations de confidentialité des données. Il est important de noter que le choix de l'emplacement de l'IDS dans l'IoT dépendra des besoins spécifiques en matière de sécurité, de performance et de gestion du réseau. Une approche hybride combinant plusieurs emplacements peut ´également être envisagée pour une protection complète de l'IoT.

Dans ce qui suit une figure qui illustre une des possibilités de l'emplacement d'un IDS dans le contexte de l'IoT :

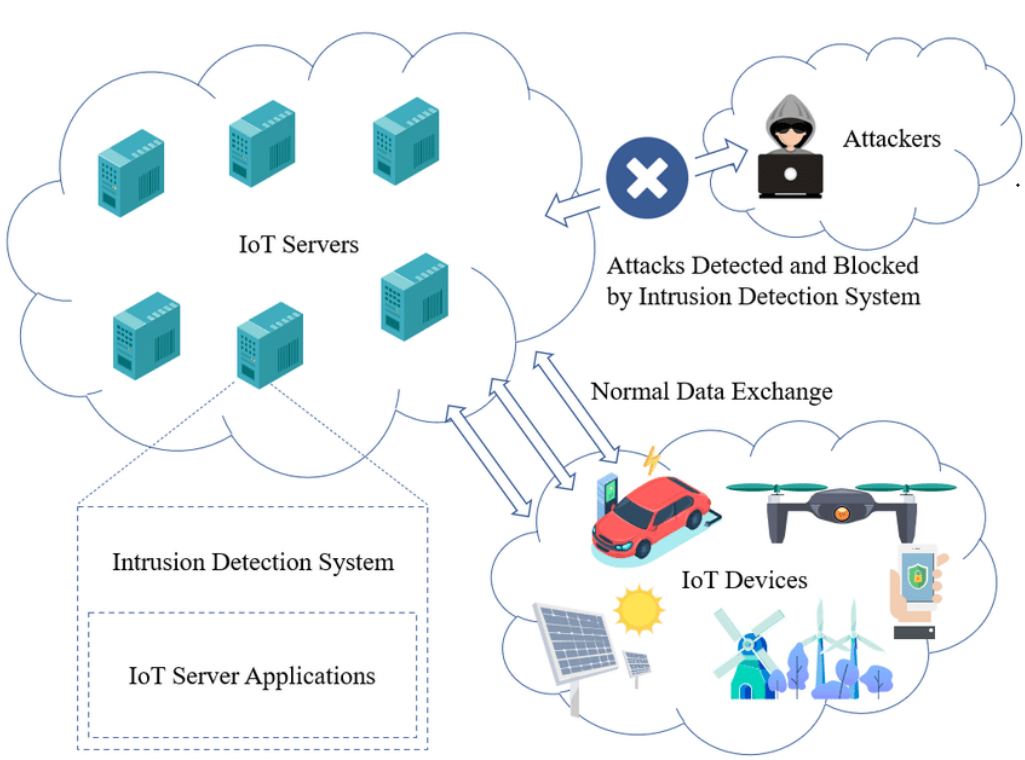

Figure 2.5: IDS pour les Serveurs IoT **[54].**

II.11 Deep Learning :

II.11.1 Définition d'intelligence artificielle :

L'intelligence artificielle (IA) 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 **[55].**

II.11.2 Définition d'apprentissage automatique :

L'apprentissage automatique est un sous-domaine de l'(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 **[56].**

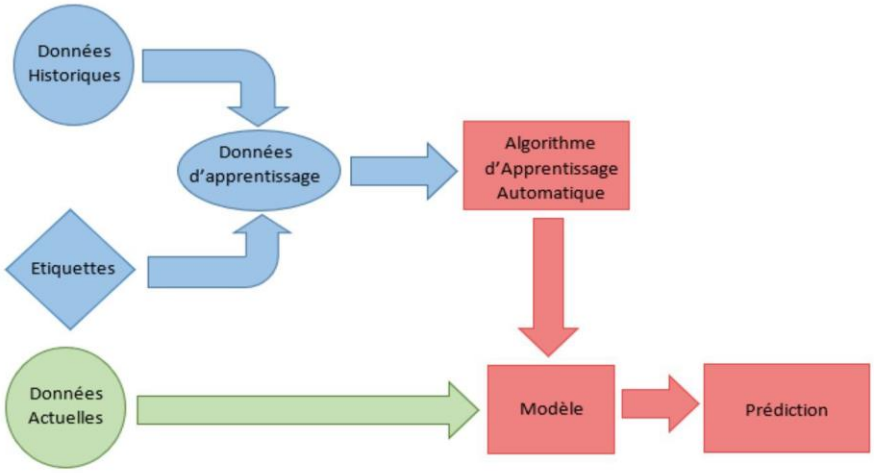

Figure 2.6: Méthodes permettant d'apprendre et de prédire des données.

II.11.2.1 Types des systèmes de l'apprentissage automatique :

Il existe plusieurs types de systèmes de ML qu'on peut les classer selon différentes catégories majeures :

• Selon l'effectuation de l'apprentissage progressivement, au fur et à mesure ou non (Apprentissage en ligne, Apprentissage groupe).

• Selon s'il compare uniquement les nouvelles données à des données connues ou qu'il d´détecte les ´éléments de structuration dans les données d'entraînement et construit un modèle prédictif comme un scientifique (Apprentissage à partir d'observation, Apprentissage à partir d'un modèle).

• Selon l'effectuation de l'apprentissage avec ou sans supervision humaine (Apprentissage non-supervisé, Apprentissage semi-supervisé, Apprentissage supervisé, Apprentissage par renforcement).

- **Apprentissage non-supervisé :** Dans l'apprentissage non supervisé, l'environnement ne fournit que des données d'entrée sans objectifs souhaités. Il n'a pas besoin de données étiquetées, le système tente d'apprendre sans professeur et peut étudier les similitudes entre les données non étiquetées et classer les données en différents groupes. Les méthodes classent les objets sans besoin d'une base de données **[57].** On distingue plusieurs types à savoir le clustering qui permet de regrouper les données similaires, la réduction de dimension, etc…
- **Apprentissage semi-supervisé :** l'apprentissage semi-supervisé se situe entre l'apprentissage supervisé et celui non supervisé, il utilise à la fois des données labellisées et non labellisées pour s'adapter à un modèle.

- **Apprentissage supervisé :** L'apprentissage automatique peut être supervisé dans le cas où des étiquettes sont associées à des données d'apprentissage, et vous essayez de prédire des étiquettes pour des données futures. Autrement dit les méthodes consistent à classer les objets à partir d'une base de données dite d'apprentissage.

Avec le Supervised Learning on peut d´développer des modèles pour résoudre deux types de problèmes : les problèmes de Régression ou les problèmes de Classification **[57].**

II.11.3 Définition d'apprentissage profond :

L'apprentissage profond ou le deep learning (DL) est une technique de l'apprentissage automatique qui utilise des réseaux de neurones artificiels pour apprendre `à partir de données. Les réseaux de neurones sont des modèles mathématiques qui simulent le fonctionnement du cerveau humain en apprenant à partir de données brutes et en effectuant des tâches de classification, de reconnaissance d'images, de traitement du langage naturel et bien plus encore **[58].** Le DL est également utilisé dans de nombreux domaines de recherche, notamment en biologie, en physique, en astronomie et en économie, où il est utilisé pour extraire des informations `à partir de données massives.

II.12 Comparaison entre l'apprentissage automatique et l'apprentissage profond : [59]

On a résumé la comparaison entre les deux types d'apprentissage dans le tableau suivant :

	Apprentissage profond	**Apprentissage automatique**
Exigences en matière de données	Nécessite de grandes quantités des données	Peut s'entrainer sur moins de données
Précision	Fournit une grande précision	Donne moins de précision
Temps de l'exécution	Prend plus de temps pour s'entrainer	Prend moins de temps pour s'entrainer
Dépendance matérielle	Nécessite un GPU pour s'entrainer correctement	Trains sur CPU
Réglage de hyperparamètres	Peut être réglé de différentes manières	Capacités de réglage limitées

Tableau 2.1 : Comparaison entre l'apprentissage profond et l'apprentissage automatique.

II.13 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.

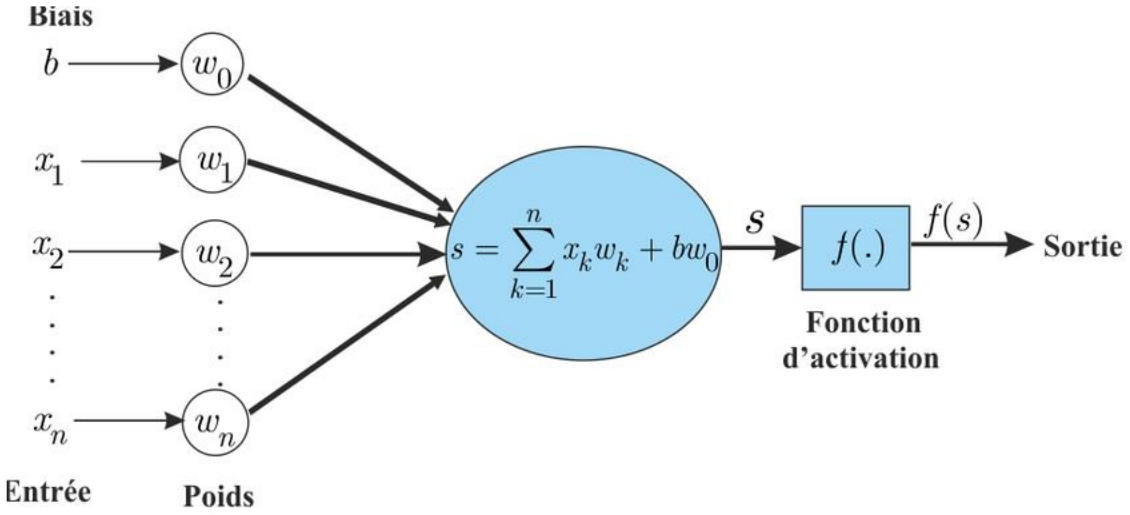

Figure 2.7 : La structure d'un neurone artificiel.

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 **[60].**

• **Sortie** : elle consiste en la valeur finale produite par le neurone pour un ensemble particulier de signaux d'entrée **[61].**

II.14 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 **[61].**

- **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.

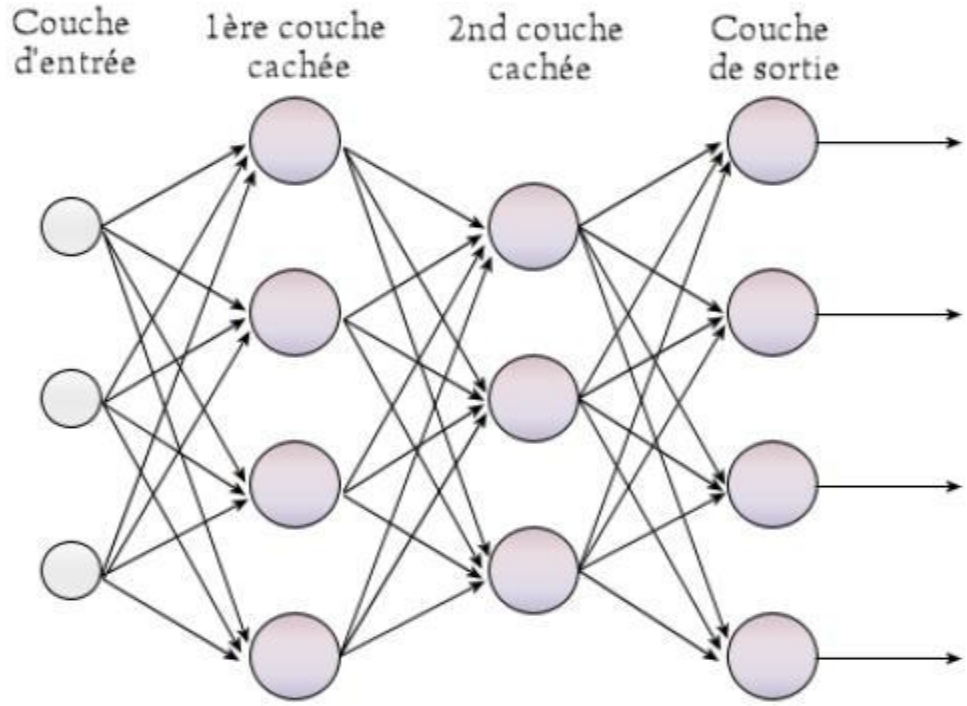

Figure 2.8 : L'architecture d'un modèle Deep Learning.

II.15 Les 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 :

• Fonction d'activation binaire

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 **[60].**

• Fonction d'activation linéaire

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, une fonction d'activation linéaire a deux problèmes majeurs :

• 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 **[60].**

•Fonctions d'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 **[60].**

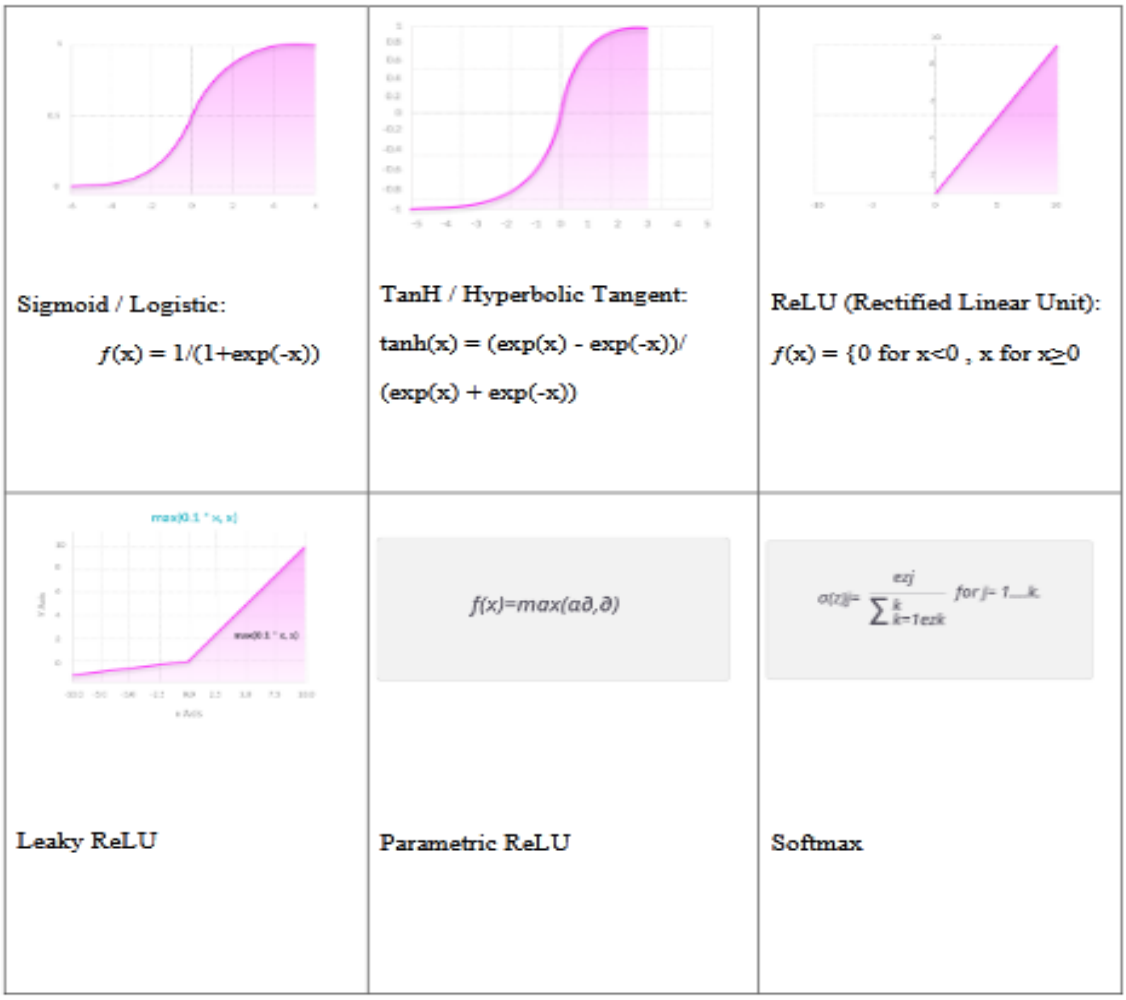

Figure 2.9: Les fonctions d'activation **[60].**

II.16 Les Modèles du Deep Learning :

II.16.1 Le réseau neuronal profond (deep neuronal 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 **[47].**

Le concept de base du perceptron a été introduit par Rosen blatt en 1958 **[60].** 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 :

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

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.

II.16.2 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 **[61] [53].** La structure générale d'un réseau CNN est représentée dans **(la figure 2.10) :**

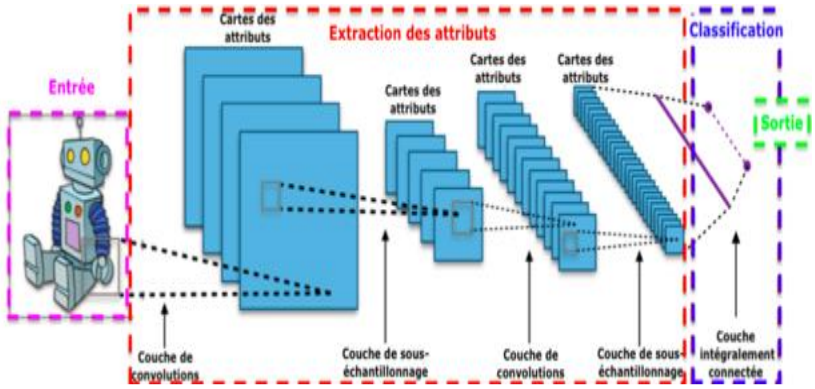

Figure 2.10: La topologie CNN.

- **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].

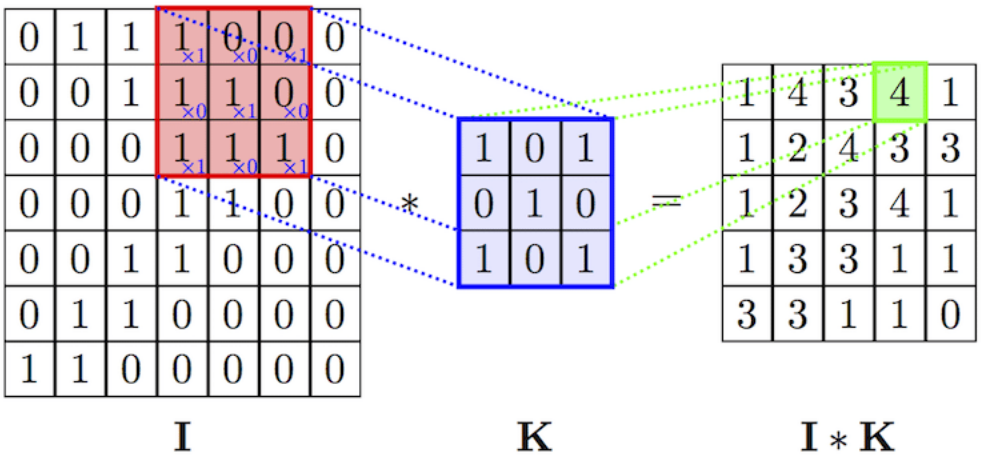

Figure 2.11: Traitement de la matrice d'image.

- **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 existe diffèrent types de pooling **[61] :**

▪ 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.

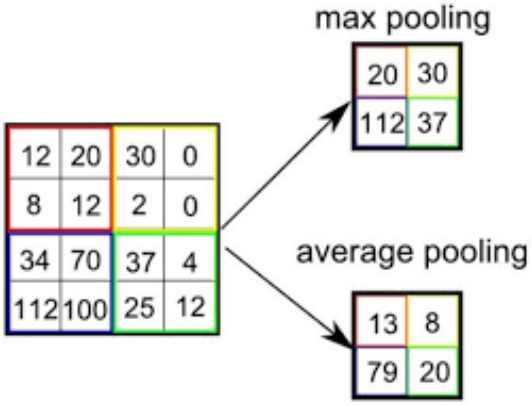

Figure 2.12: les deux différents types de pooling.

- **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 **[54].** 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	• 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.

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 des modèles coûteux en termes de ressources de calcul et de temps 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.

Tableau 2.2 : Avantages et Inconvénient de CNN.

II.16.3 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) **[50].**

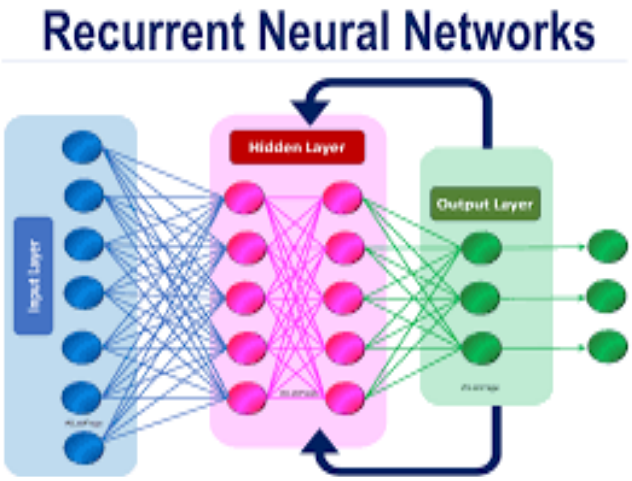

Figure 2.13: la topologie RNN **[54].**

II.16.4 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 **[50].** Le schéma suivant illustre les transformations appliquées à l'état caché au pas de temps t :

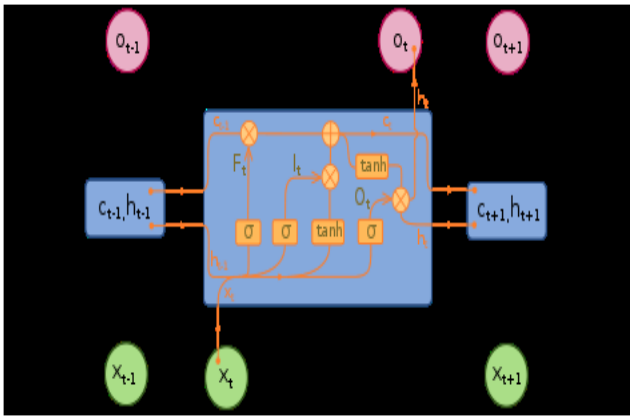

Figure 2.14: la topologie LSTM **[50].**

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 **[51] :**

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

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 **[51].**

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 **[51].**

II.17 Principes clés 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 **[52].**

II.18 Métriques D’évaluation :

Les modèles proposés sont évalués à l'aide de mesures d'évaluation, telles que l'exactitude, la précision, le rappel et le score F1, couramment utilisées dans divers domaines, y compris la détection des menaces. Les sections suivantes décrivent chaque mesure, suivie de formules et de justifications mathématiques.

- **L’exactitude :** Le terme "précision" fait référence au degré d'exactitude des prédictions d'un modèle. Le taux de précision est la proportion d'instances correctement classées (y compris les vrais positifs et négatifs) par rapport au nombre total d'instances. Il est calculé à l'aide de l'équation **[64].**

$$\text{Exactitude} = \frac{\text{VP+VN}}{\text{VP+VN+FP+FN}}$$

- Vrai positif (VP) : Nombre d'instances correctement identifiées comme positives (c'est-à-dire comme des menaces).

- Vrai négatif (VN) : Nombre d'instances correctement identifiées comme négatives (c'est-à-dire comme des menaçantes).

- Faux positif (FP) : Nombre d'instances incorrectement classées comme positives (c'est-à-dire non-menaces classées à tort comme menaces).

- Faux négatif (FN) : Nombre d'instances incorrectement classées comme négatives (c'est-à-dire non-menaces classées à tort comme non-menaces).

- **Précision :** Le concept de précision fait référence au degré d'exactitude des

prédictions positives. Le taux de vrais positifs est la proportion d'instances positives prédites avec précision par rapport au nombre total d'instances positives prédites, y compris les vrais et les faux positifs. La formule de la précision est la suivante **[65] :**

$$\textbf{Précision} = \frac{\mathrm{TP}}{\mathrm{TP+FP}}$$

- **Rappel :** Le rappel, également connu sous le nom de sensibilité ou de taux de vrais positifs, mesure le nombre d'instances positives prédites avec précision (vrais positifs) par rapport à toutes les instances positives réelles (vrais positifs et faux négatifs).

  L'expression mathématique est donnée par l'équation **[66].**

  $$\textbf{Rappel} = \frac{\mathrm{TP}}{\mathrm{TP+FN}}$$

- **F1 Score :** Le score F1 est une mesure qui combine la précision et le rappel. Cela permet d'atteindre un équilibre entre les deux mesures. La moyenne de la précision et du rappel est utile lorsque la précision et le rappel ont des choix inégaux. Elle est fréquemment utilisée en ML et en analyse statistique pour évaluer les performances d'un modèle de classification. L'expression mathématique est illustrée par l'équation [**67] :**

  $$\textbf{F1 Score} = \frac{2.(Précision.Rappel)}{\mathrm{Précision+Rappel}}$$

Le F1 score fournit une valeur unique qui met en évidence les performances combinées de la précision et du rappel.

II.19 Conclusion :

Dans ce chapitre, nous avons parlé particulièrement des systèmes de détection d'intrusion (IDS). Nous avons commencé par définir les IDS et présenter leurs concepts de base ainsi que leurs différents types. Ensuite, nous avons abordé l'utilisation de l'intelligence artificielle (IA) comme méthodologie pour les IDS, en explorant différentes architectures telles que les DNN, CNN et LSTM. Dans la deuxième partie, nous expliquerons comment nous réaliserons notre travail, notamment la création de notre modèle IDS robuste pour les réseaux IoT.

Partie 2

Contribution, résultat et discussion

Chapitre III

Contribution, résultat et discussion

III.1 Introduction :

Après avoir exposé toute la théorie nécessaire, nous abordons maintenant la deuxième partie afin de présenter notre travail.

Dans ce chapitre, nous présenterons notre travail d'implémentation. Tout d'abord, nous introduirons les outils et les langages employés pour mettre en œuvre notre modèle, notamment le simulateur Cooja pour la simulation des attaques dans un environnement IoT. Nous détaillerons le principe de fonctionnement et expliquerons toutes les étapes nécessaires pour réaliser notre contribution. La méthode proposée est évaluée à l'aide des ensembles de données UNSW-NB15 et Minerva, en expliquant comment ils ont été générés. Ensuite, nous détaillerons les différentes étapes du prétraitement sur l'ensemble des données, du nettoyage à la normalisation et à l'équilibrage.

Enfin, nous présenterons notre modèle IDS basé sur un modèle hiérarchique utilisant LSTM ainsi que les différents résultats expérimentaux.

III.2 Travaux Connexes:

Il existe plusieurs études sur l'attaque des protocoles de routage pour l'IoT en utilisant IDS :

1. Dans les recherches de Mridula Sharma, Haytham Elmiligi, Fayez Gebali et Abhishek Verma (2019) au titre **[68]: Simulating Attacks for RPL and Generating Multi-class Dataset for Supervised Maching:**

    - Leur document se concentre sur l'analyse des menaces à la sécurité en matière de RPL et sur les attaques qui pourraient affecter le réseau du CPS (Cyber Physical System)

    - Ils présentent un nouveau Framework pour simuler les attaques RPL en utilisant le contiki-Cooja.et ils avaient simulés quatre attaques différentes à l'aide de ce Framework.

    - Pour les mises en œuvre de l'expérimentation, ils choisissent d'utiliser quatre attaques différentes : l'attaque "hello flood", l'attaque "DODAG Information Solicitation" (DIS), l'attaque "increased version" et l'attaque "reduced rank".

- Ils analysent les caractéristiques extraites des paquets de trafic du réseau et propose un nouveau modèle d'apprentissage machine. En utilisant plusieurs techniques de réduction des caractéristiques, le nombre de caractéristiques requises pour la classification des attaques est réduit de 58 à 21, soit une réduction de 63,7% à économiser l'énergie de traitement et de communication.

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

Leurs résultats expérimentaux montrent qu'ils pouvaient atteindre une précision de classification de 99,33% en utilisant le classificateur Random-forest.

2. Dans les recherches de: Yavuz, F. Y., Devrim, & Ensar, G. Ü. L. (2018) au titre **[69]: Deep learning for detection of routing attacks in the internet of things. International Journal of Computational Intelligence Systems, 12(1), 39-58.**

   - Cette étude est une preuve de concept vers l'application d'apprentissage approfondi pour la sécurité de l'IoT.

   - Ils proposent une méthode de détection des attaques de routage pour l'IoT basée sur l'apprentissage approfondi.

   - Le principal problème dans ce domaine est le manque d'ensembles de données et la qualité des données disponibles. Nos ensembles de données sur les attaques sont produites par simulation, en utilisant le code d'un capteur réel et l'implémentation du protocole RPL de Contiki-RPL.

   - Dans leur étude, ils utilisent le simulateur Cooja-IoT, afin de générer des données d'attaque hautement précises dans des réseaux IoT dont la taille allant de 10 à 1000 nœuds.

   - Ils proposent une méthodologie de détection d'attaques nettement évolutive et basée sur l'apprentissage approfondi pour la détection des attaques de routage IoT qui sont des attaques de catégorie restreinte, de type "hello-flood" et de modification de numéro de version, avec une grande précision et exactitude.

- Ils notent que l'application de l'apprentissage approfondi à la cybersécurité dans l'IoT nécessite la disponibilité de données consistantes sur les attaques IoT.

- Ils ont construit en outre, un réseau neuronal profond des modèles formés à l'aide des ensembles de données de l'IRAD avec les informations d'évaluation : l'exactitude, la précision et les taux de rappel.

- Ils parviennent enfin, à obtenir jusqu'à 99%, sur la base des Scores F1 et le score du test AUC.(Yavuz et al., 2018).

3. Asongo et al. **[79]** ont proposé un IDS basé sur les réseaux neuronaux récurrents (RNN) qui a permis d'obtenir une grande précision dans la détection des intrusions dans le réseau. Le modèle le plus performant a enregistré une classification avec une précision réelle de 88,16 %, un score F1 (F1S) de 90,45 % et une précision de vérification de 94,32 %. L'étude a montré que l'utilisation de la méthode GRU permettait d'obtenir une précision de test plus élevée que les techniques RNN et LSTM simples sur l'ensemble de données UNSW-NB15. Cependant, en termes de temps de formation, le RNN simple était plus rapide. En outre, l'article souligne l'importance de la procédure de normalisation des caractéristiques et introduit l'algorithme XGBoost pour la sélection des caractéristiques.
4. Dong et al. **[80]** ont proposé le modèle MCA-LSTM, qui utilise le gain d'information (GI) pour la sélection des caractéristiques, et l'algorithme de corrélation multiple (MCA) pour construire une matrice de carte de zone triangulaire (TAM). Ensuite, ils appliquent la LSTM pour l'apprentissage des caractéristiques à partir de la matrice TAM, ce qui permet d'améliorer la précision de la classification. Les résultats expérimentaux indiquent que la précision de test du modèle proposé sur une tâche de classification en 5 étapes utilisant l'ensemble de données NSL-KDD atteint 82,15 %. Sur une tâche de 10 classifications utilisant l'ensemble de données UNSW-NB15, elle atteint 77,74 %.
5. Kabir et al. **[81]** ont proposé un système de détection des intrusions utilisant une approche basée sur l'apprentissage automatique combinée avec l'ensemble de données UNSW-NB15. Les chercheurs souhaitent améliorer la précision des systèmes de détection des intrusions dans les réseaux (NIDS) en expérimentant diverses combinaisons d'ensembles d'algorithmes (XGBoost et Random Forest) et

un algorithme supervisé simple (K-Nearest Neighbors, ou KNN). Leurs conclusions indiquent que l'approche par empilement dépasse les modèles individuels, se traduisant par une précision supérieure de 96,24 %.

III.3 Environnement de développement :

III.3.1 Langages de programmation et bibliothèques :

- ✓ **Google Colab:**

Google Colab est un environnement de développement en ligne basé sur Jupyter Notebook, 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 **[70].**

- ✓ **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.

- ✓ **Définition de langage de programmation :**

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.

Nous avons utilisé comme bibliothèque pour notre projet :

- ✓ **Panda:**

Pandas est un package Python open source qui est le plus largement utilisé pour la science et l'analyse des données **[71].**

- ✓ **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 **[72].**

- ✓ **Scikit learn:**

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.

- ✓ **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 **[73].**

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 **[73].**

III.3.2 Ensemble de données utilisées :

L'une des étapes les plus importantes pour évaluer et valider les approches de détection d'attaques basées sur l'apprentissage automatique en IoT est le choix des datasets à utiliser.

Le principal problème dans ce domaine est le manque d'ensembles de données IoT disponibles. Cependant l'accès à ces données peut s'avérer difficile à obtenir en vue de leur confidentialité. Dans le tableau ci-dessous nous allons présenter quelques ensembles de données utilisées pour la détection des intrusions réseaux **[74] :**

Dataset	Type d'attaque	Année
KDD Cup	NON	1999
NSL-KDD	NON	2009
CTU-13	NON	2011
UNSW-NB15	OUI	2015
CICDDoS2018	NON	2018
CICDDoS2019	NON	2019
UNSW-NB15 V2	OUI	2021
CICIDS001	NON	2022

Tableau 3.1: Datasets référentielles sur les intrusions.

Nous avons utilisé un ensemble de données IoT **[75]** qui a été générer en 2020 par BOUAZZA Abdelhamid et CHAABI Aissa à l'Université d'Ibn Khaldoun - Tiaret.

III.3.2.1 Génération de Dataset Minreva :

Le dataset Minreva qu'il été générer en 2020 par BOUAZZA Abdelhamid et CHAABI Aissa à l'Université d'Ibn Khaldoun – Tiaret.

Cet ensemble de données d'attaque est produits par simulation, en utilisant des scénarios réels et 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 :

- **Capture de trafic:**

• Ils ont capturé tout le trafic qui passait par le réseau IoT avec différents scénarios en tant que fichier PCAP à l'aide de Wireshark avec l'aide d'un outil prêt dans le simulateur Cooja appelé radio messages. Le fichier PCAP est converti en fichier csv.

• Chaque seconde, un certain nombre de paquets est capturé dans la simulation qui est divisée en fenêtres de temps de 1000 ms.

• Les ensembles de données brutes comprennent des types de données qui ne peuvent pas être traités par l'algorithme d'apprentissage automatique, tels que les adresses IP, ce qui peut fausser le modèle (sur justement). Pour éviter ce problème, les adresses source et de destination sont converties de l'IPv6 à l'identifiant de nœud. Par exemple, l'adresse IPv6

2001 :0db8 :3c4d :0015 :0000 : d234::3eee :0011 peut être abrégée en 11 et l'adresse IP de diffusion ff02::1a est convertie en 99.

- **Générer de nouvelles fonctionnalités**:

Toutes les étapes précédentes ont généré un total de 13 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.

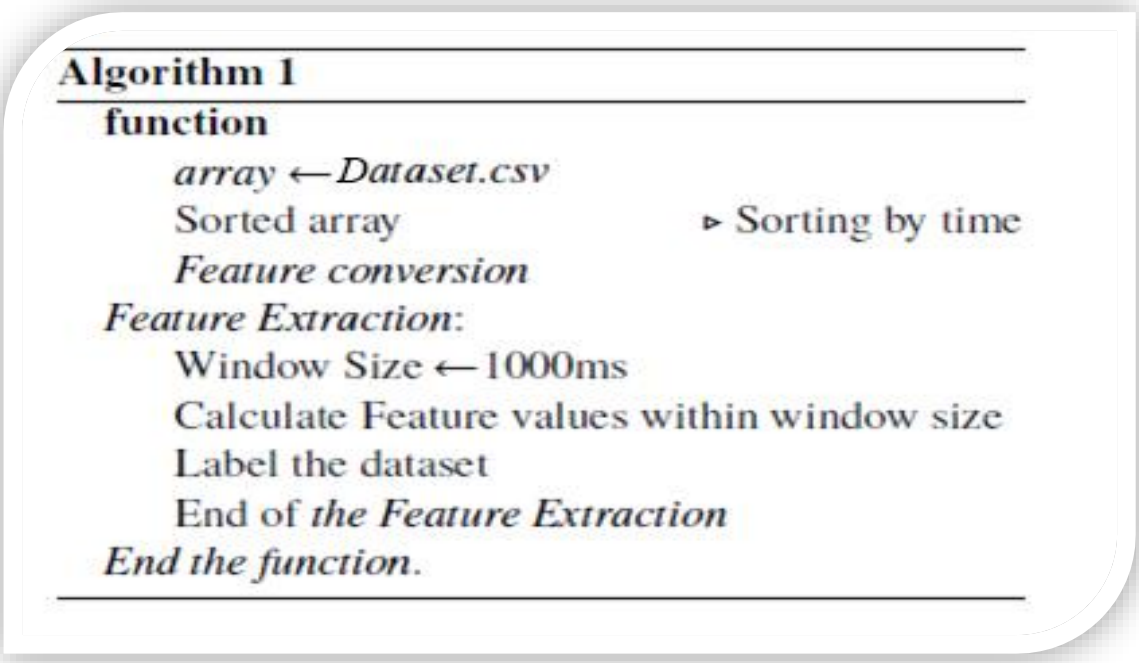

Figure 3.1 : L'algorithme d'extraction des caractéristiques.

- **Suivi de l'énergie:**

Ils ont suivi la consommation d'énergie des nœuds sans attaques et ont constaté que les attaques consommaient beaucoup d'énergie des nœuds. À l'aide du simulateur, quatre

propriétés ont été déduites : l'énergie (ON), le mode d'émission (radio TX), le mode de réception (radio RX) et enfin INT (radio interférencée).

- **Suivi de la position et du rang :**

En modifiant la position (X, Y) et le rang (rank) des nœuds, ils ont observé que les nœuds malveillants occupent toujours une position géographique importante et sont proches du nœud racine pour couvrir et influencer autant de nœuds que possible.

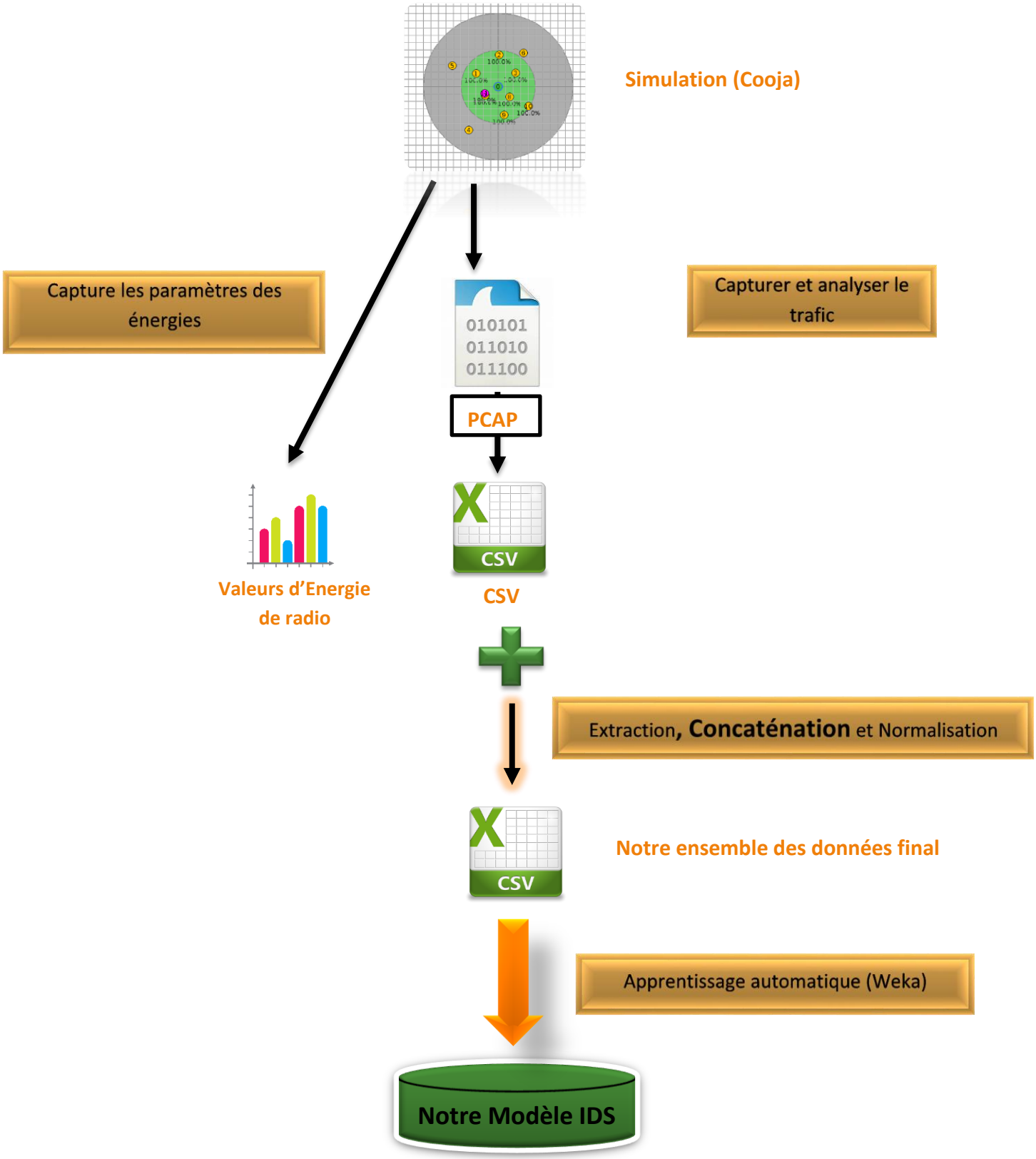

Figure 3.2: Les différentes étapes pour construire dataset.

Notre RPL contient 24 caractéristiques et 48024 échantillons. Dans les tableaux ci-dessous, nous décrirons tous les détails :

- **Description de l'ensemble de données Minreva :**

N°	Nom de la fonctionnalité	Description
1	J	Temp
2	Src	Source
3	Dst	Destination
4	Protocole	Le protocole de couche supérieur décodé
5	Dure_tr	Temp de transmission pendant une fenêtre horaire
6	Moy_tr	Supports de transmission
7	Longueur_tr	Taille de paquet transmis
8	DIStr	Numéro DIS transmis
9	DIO_tr	Numéro DIO transmis
10	DAO tr	Numéro DAO transmis
11	Dure_rec	Temp de réception pendant une fenêtre horaire (14)
12	Moy_rec	Supports de reception
13	Longueur_rec	Taille du paquet reçu
14	DIS_rec	Numéro DIS reçu
15	DIO_rec	Numéro DIO reçu
16	DAO_rec	Numéro DAO reçu
17	SUR	Energie
18	TX	Energie d'émission
19	RX	Energie de reception
20	INT	Radio brouillée
21	Pos_x	Position géographique X sur l'axe X
22	Pos_y	Position géographique Y sur l'axe Y
23	A sonné	Rang de nœud dans DODAG
24	Classe	Classe d'attaque

Tableau 1.2: Description de Minreva.

Normale /Attaque	Catégorie	Nombre
Attaque	Decreased Rank	9367
	Version Number	3196
	Black Hole	1493
	Hello Flooding	5064
Normal		28922

Tableau 3.3 : Les statistiques de Minerva.

III.3.2.2 L'ensemble de données UNSW-NB15 :

L'ensemble de données UNSW-NB15 est une collection complète de données sur le trafic réseau, conçue explicitement pour évaluer les systèmes de détection d'intrusions (IDS). Créé par des chercheurs du Centre australien pour la cyber-sécurité (ACCS), il contient à la fois du trafic standard et du trafic anormal, ce qui est crucial pour le développement et le test des modèles IDS.

Cet ensemble de données comprend 2 540 044 enregistrements, chacun avec 49 caractéristiques différentes. Ces caractéristiques couvrent divers attributs de protocole, des informations au niveau des paquets et des statistiques au niveau des flux. Le dataset comprend 10 types d'attaques : Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, et Worms.

Les étiquettes d'attaques de l'ensemble des données ont été générées à l'aide d'un outil développé en interne appelé NUSW-NB IDS, permettant aux chercheurs de contrôler les types et les taux d'attaque pendant le processus de collecte des données. L'ensemble de données UNSW-NB15 a été largement utilisé dans la recherche sur les IDS, en particulier pour le développement et l'évaluation de modèles d'apprentissage automatique et profond.

III.4 Notre contribution :

Dans cette section, nous présentons notre modèle LSTM hiérarchique, qui se compose de deux niveaux. Au premier niveau, nous utilisons une LSTM pour la classification binaire afin d'identifier le trafic anormal du trafic normal. Ensuite, au deuxième niveau, nous

effectuons une classification multi-classes à l'aide d'un modèle LSTM pour détecter le type d'attaque.

Nous évaluons le modèle proposé sur les ensembles de données UNSW-NB15 et Minerva, qui sont des ensembles de données de trafic réseau conçus explicitement pour évaluer les systèmes de détection d'intrusion en IoT. Ces ensembles de données nécessitent un prétraitement considérable avant d'être utilisés pour l'entraînement du modèle proposé. Nous évaluons le modèle proposé à l'aide de différentes mesures.

L'objectif final est de créer un système de détection d'intrusion précis et efficace pour les environnements IoT.

III.4.1 Le modèle proposé :

Pour obtenir des résultats précis et fiables dans la détection des anomalies, il est important d'obtenir un niveau élevé de précision et de réduire le nombre de faux positifs. Plusieurs niveaux de classification sont souvent utilisés pour améliorer le fonctionnement de la détection. Nous avons utilisé une architecture hiérarchique à deux niveaux de classification **(voir figure 3.3).**

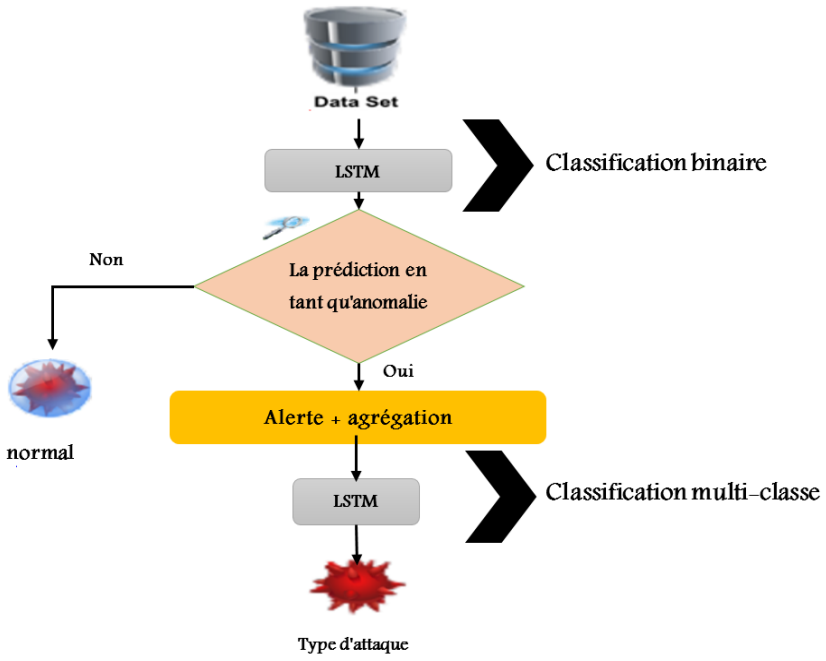

Figure 3.3 : L'architecture globale de notre modèle.

Le premier niveau est une classification binaire qui utilise la LSTM pour détecter le trafic anormal avec précision. Nous avons choisi d'utiliser la LSTM, car elle est très efficace pour identifier les dépendances à long terme et les modèles temporels dans les données séquentielles, ce qui est essentiel pour l'analyse du trafic réseau. La classification binaire avec LSTM est plus performante que la classification multi-classes avec LSTM. Le niveau de classification binaire de notre architecture hiérarchique permet de détecter le trafic susceptible de contenir des anomalies, qui peuvent ensuite être analysées en détail au deuxième niveau de notre modèle par multi-classification. En d'autres termes, le trafic susceptible d'être normal est filtré. Le deuxième niveau de classification peut alors se concentrer sur le trafic restant et détecter des anomalies plus subtiles. Une telle stratégie réduit le nombre de faux positifs avec le premier modèle binaire LSTM, ce qui nous permet de détecter le trafic anormal avec une grande précision.

Ensuite, nous appliquons un filtre sur le résultat du premier niveau pour identifier le trafic anormal avant d'utiliser une LSTM multi-classes pour déterminer le type d'attaque. L'architecture globale du modèle LSTM multi-classes est similaire à celle de la LSTM binaire, sauf dans la couche de sortie de la multi-classification. Afin de rendre la LSTM multi-classes plus précise, nous utilisons un processus appelé « agrégation temporelle » sur l'ensemble des données. En évaluant plusieurs fenêtres temporelles, la méthode permet d'atteindre les meilleures performances.

De nombreuses études ont utilisé cette technique, généralement au niveau du prétraitement des données, pour améliorer les performances des modèles. Dans notre étude, nous employons une technique utilisant un modèle de base à base de LSTM qui se concentre sur les effets de l'agrégation temporelle. La nouveauté de notre approche consiste à positionner l'agrégation et à traiter la fenêtre temporelle comme une variable dépendante de l'ensemble des données et du modèle, ce qui permet d'obtenir des performances supérieures à celles du modèle de base. Notre approche fournit une solution flexible et puissante pour traiter les ensembles de données de séries temporelles.

III.4.2 Prétraitement :

Le prétraitement des données est une technique d'exploration des données qui transforme les données brutes en formats compréhensibles, en s'attaquant à des problèmes tels que l'incomplétude, l'incohérence et les erreurs dans les grands ensemblesde données **[76].**

III.4.3 Nettoyage des données :

Le nettoyage des données consiste à identifier et à traiter les erreurs, les structures inadéquates, les doublons ou les valeurs manquantes dans l'ensemble de données. La duplication des données ou la classification incorrecte peut se produire de diverses manières lors de l'intégration de différentes sources de données **[77].**

III.4.4 Encodage

Le codage est une technique que nous utilisons pour représenter les variables catégorielles sous forme de valeurs numériques dans un modèle d'apprentissage automatique **[78].**

III.4.5 Normalisation des données :

La plupart du temps, en machine Learning, les Data Set proviennent avec des ordres de grandeurs différents. Cette différence d'échelle peut conduire à des performances moindres. Pour pallier à cela, des traitements préparatoires sur les données existent. Notamment le **Feature Scaling** qui comprend la **Standardisation** et la **Normalisation**.

Min-Max Scaling peut être appliqué quand les données varient dans des échelles différentes. A l'issue de cette transformation, les features seront comprises dans un intervalle fixe [0,1]. Le but d'avoir un tel intervalle restreint est de réduire l'espace de variation des valeurs d'une feature et par conséquent réduire l'effet de valeurs aberrantes.

La normalisation peut être effectuée par la technique du **Min-Max Scaling**.

III.4.6 Equilibrage :

En complément du choix d'un critère pertinent, il peut être intéressant de tenter de ré-équilibrer l'échantillon pour aider les algorithmes à mieux détecter les individus de la classe minoritaire. Les méthodes classiques consistent à créer de nouvelles observations de la classe minoritaire (oversampling) et/ou supprimer des individus de la classe minoritaire (undersampling).et SMOTE pour Synthetic Minority Over- Sampling Technique consiste à sur-échantillonner en se basant sur les proches voisins de la classe minoritaire **[70].**

Le problème des données déséquilibrées se pose lorsque la distribution des échantillons entre les différentes classes est inégale. Il en résulte un ensemble de données asymétrique, où une classe est déséquilibrée et peut donner lieu à un modèle biaisé. Les données d'apprentissage subissent généralement un rééchantillonnage avant la classification, ce qui

augmente le nombre d'échantillons appartenant à la classe minoritaire, et un sous-échantillonnage, qui réduit le nombre d'échantillons de la classe majoritaire. Les problèmes de classification déséquilibrée sont fréquemment rencontrés dans divers ensembles de données, car la classe minoritaire ne dispose généralement pas de suffisamment de données. Une approche pour rectifier le déséquilibre des classes consiste à synthétiser des données supplémentaires provenant de la classe minoritaire, ce qui permet d'atténuer le problème de la disponibilité limitée des données.

La technique de sur échantillonnage des minorités synthétiques (SMOTE) est une approche largement utilisée pour générer des échantillons supplémentaires dans l'ensemble de données. La méthodologie repose sur le développement de paquets de données qui connectent un point donné à ses K points voisins les plus proches **[78].** La technique SMOTE génère de nouveaux échantillons à partir de l'ensemble de données existant afin d'obtenir un ensemble de données équilibré. Elle est utilisée pour augmenter le nombre d'instances des catégories minoritaires. En outre, une analyse est menée pour évaluer l'impact de divers facteurs, notamment la réduction de la dimensionnalité, la taille de l'ensemble de formation et le nombre de voisins (K) sur la précision du système. En outre, une analyse qualitative évalue les variables qui affectent les résultats. Voici les étapes utilisées pour effectuer l'analyse SMOTE dans le cadre de cette recherche.

III.4.7 Étape de Split :

Dans cette étape, nous divisons l'ensemble des données en 60 % de données d'entraînement, 20 % de données de validation et 20 % de données de test.

Nos modèles sont ensuite évalués à l'aide des ensembles de données de validation. La précision atteinte par chaque modèle est mesurée à l'aide de l'ensemble des données de test.

III.5 Implémentation :

Pour mettre en œuvre notre approche LSTM pour la détection d'intrusion dans l'IoT, le cadre architectural proposé comprend les étapes suivantes :

Étape 1 :

- **Prétraitement des données :** cette étape implique le nettoyage, la normalisation, le traitement des données manquantes, l'encodage, puis l'application de SMOTE pour équilibrer les classes.

Étape 2 :

- **Classification binaire basée sur la LSTM :** au premier niveau de l'architecture proposée, nous utilisons un modèle de classification binaire basé sur la LSTM. Ce modèle tente de distinguer le trafic réseau normal du trafic anormal. Cette approche binaire conduit à un mécanisme de détection plus efficace et plus ciblé dans la phase initiale, offrant un avantage par rapport à la classification multi-classes, comme le montre le tableau 1. Après la détection initiale, la sortie du classificateur binaire, qui est effectivement pré-filtrée en ne rendant que les anomalies potentielles, est ensuite transférée au deuxième niveau de l'architecture. Cette méthodologie garantit un processus de détection des intrusions plus précis grâce à l'utilisation de la classification binaire.

Classification	**Exactitude**	**précision**	**F1-score**
Binary classification	97.43 %	98.19 %	97.98%
Multi classification	84.99 %	84.53 %	83.85%

Tableau 3.4: Performance de la classification binaire vs multi-classification sur l'ensemble de test unsw-nb15.

Étape 3 :

- **Filtre et agrégation temporelle:** après la phase de classification initiale, nous appliquons une stratégie appelée « agrégation temporelle » pour identifier le type de trafic anormal. Cette stratégie, mise en œuvre sur des fenêtres temporelles définies, permet une analyse temporelle précise du comportement de l'anomalie. Dans le cadre du processus d'agrégation temporelle, les instances sont regroupées en fonction de leur étiquette « Type d'attaque ». Ensuite, nous calculons des

statistiques sommaires pour chaque groupe identifié sur la fenêtre temporelle désignée, en utilisant l'attribut « Time » dans l'ensemble des données. Cette approche permet d'obtenir une vue globale du comportement de l'anomalie.

La durée de la fenêtre temporelle sélectionnée pour l'agrégation peut être fixe ou variable en fonction des besoins spécifiques et des caractéristiques inhérentes à l'ensemble des données.

Étape 4 :

- **La classification multiple par LSTM :** une fois que les données ont été agrégées dans le temps, elles passent par un deuxième niveau de classification à l'aide d'un modèle LSTM à classification multiple. Ce modèle est spécifiquement conçu pour identifier le type d'attaque.

Étape 5 :

- **L'évaluation du notre modèle :** enfin, le modèle est évalué à l'aide d'un ensemble de données de test. Nous mesurons la précision du modèle et apportons les ajustements nécessaires à l'architecture du modèle ou au processus de formation afin d'améliorer les performances. Ces ajustements peuvent inclure la modification de la taille de la fenêtre temporelle pour l'agrégation, un paramètre qui peut avoir un impact significatif sur les performances du modèle.

III.6 Résultats et discussion :

Dans cette partie, nous présentons les résultats de l'évaluation de notre modèle. Les résultats présentés sont basés sur les hyper paramètres du modèle LSTM décrits dans **le tableau 3.5**

Nom	***Paramètre***
Couche 1 de LSTM	Unités: 512
Couche 2 de LSTM	Unités: 256
Couche 3 de LSTM	Unités: 64
Couche de sortie	Unités: Nombre de classes, Activation: softmax
Dropout	0.2
Batch size	32
Epochs	1000
Optimizer	Adam
Loss Function	Sparce categorical crossentropy

Tableau 3.5 : Les hyper paramètres de notre modèle LSTM.

Nous avons utilisé dans l'architecture Batch Normalization et Dropout, qui sont des techniques complémentaires. Batch Normalization stabilise et accélère l'apprentissage tout en réduisant les risques d'instabilité, tandis que Dropout prévient le sur apprentissage en introduisant de la régularisation et en rendant le modèle plus robuste. Ces deux techniques contribuent à améliorer la performance générale et la capacité de généralisation des réseaux neuronaux.

III.7 Métriques d'évaluation :

Nous avons évalué les performances de notre modèle en nous concentrant sur trois mesures : l'exactitude, la précision, le rappel et le f1-score.

III.8 L'impact de l'agrégation temporelle sur la multi-classification :

Le tableau 3.6 montre comment le processus d'agrégation rend la LSTM multi-classes plus précise pour différents intervalles de temps. En examinant les données du réseau à différents moments, vous pouvez observer comment l'attaque a affecté le réseau et son comportement, ce qui facilite sa détection. Cela permet d'obtenir une classification plus fiable et plus précise.

0 s	**84.99 %**	**84.53 %**	**83.85%**
0.15 s	89.34 %	85.43 %	86.59 %
0.3 s	94.16 %	90.11 %	92.16%
1s	95.19 %	96.20 %	95.27 %

Tableau 3.6 : Performance globale du LSTM Multi-classes avec différents temps d'agrégation sur l'ensemble de test unsw-nb15.

Le processus d'agrégation dans notre IDS consiste à combiner les données du trafic réseau sur un certain intervalle de temps afin d'identifier des modèles et de détecter des anomalies. Nos résultats montrent que l'augmentation de l'intervalle de temps dans le processus d'agrégation peut améliorer les performances du modèle. En effet, un long intervalle de temps fournit plus de données au modèle, lui permettant de les analyser et d'identifier les attaques potentielles avec plus d'exactitude et de précision.

La comparaison de la précision de notre modèle en fonction de différents intervalles de temps montre que, par exemple, en utilisant un temps d'agrégation de 1 seconde, la précision du modèle atteint 95,19 %, ce qui améliore considérablement les performances par rapport au modèle sans agrégation, qui a une précision de 84,99 %.

Cela signifie que lorsque l'agrégation est utilisée, la précision du modèle augmente significativement de 10 %. Il est important de noter que le temps d'agrégation est crucial pour obtenir une précision aussi élevée. Ces résultats montrent que notre approche est très efficace pour détecter différents types d'attaques dans les réseaux IOT.

III.9 L'évaluation de notre modèle avec l'ensemble de données Minerva :

Après avoir examiné les résultats de l'application de la LSTM sur notre ensemble de données UNSW-NB15, nous avons suggéré d'appliquer le même modèle sur un ensemble de données Minerva pour évaluer davantage notre approche. Le tableau suivant illustre les résultats obtenus.

Classifier	Exactitude	Précision	Faux alarme rate	Rappel	F1-Score
Notre modèle	**0.99**	**0.99**	**0.001**	**0.99**	**0.99**

Tableau 3.7 : La performance de notre modèle avec l'ensemble de données Minerva.

III.10 Etude comparative :

1. Sur l'ensemble de données Minerva :

Pour évaluer les performances de notre approche, nous avons comparé ses résultats avec ceux de travaux connexes (Yavuz et al., 2018) et (Sharma et al., 2019). Le résultat de cette étude comparative est résumé dans le tableau suivant.

	Minerva-IDS	(Yavuz et al., 2018)	(Sharma et al., 2019
Simulation	**Oui/cooja**	**Oui/cooja**	**Oui/cooja**
Type attaques	**4**	**3**	**4**
Type data	**PCAP filles, Energie, posotion**	**PCAP files**	**PCAP files**
Nbre d'attributs	**23**	**18**	**21**

Tableau 3.8 : Comparaison des data-set entre les IDS proposés.

	Modèle	Rappel	F1-Score	Exactitude	Precision
(Yavuz et al., 2018)	MLP	0.957	0.957	/	0.957
(Sharma et al., 2019)	Random farest	0.993	/	99.330	0.994
Notre travail	LSTM	1.000	0.999	1.000	0.999

Tableau 3.9 : La comparaison des mesures de performances entre les IDS proposés.

Notre modèle a atteint un taux de rappel de 1.000, un F1-Score de 0.999, une précision de 0.999 et une exactitude de 1.000. Ces résultats indiquent que notre modèle IDS basé sur LSTM a obtenu des performances supérieures par rapport aux modèles précédents, avec une détection d'intrusion plus précise et un taux de rappel parfait.

Ces résultats démontrent l'efficacité de notre approche basée sur LSTM pour la détection d'intrusion dans les systèmes IoT. Notre modèle offre une meilleure sécurité et une protection accrue contre les attaques, grâce à sa capacité à détecter avec précision les intrusions et à minimiser les faux positifs.

2. Sur l'ensemble de données UNSW NB15 :

Méthode	**Exactitude**
*XGBoost-LSTM **[79]***	73.29%
*MCA-LSTM **[80]***	94.90%
*XGBoost +KNN and RF **[81]***	96.24%
Our Model	95.19%

Le tableau 3.10 montre une autre comparaison entre notre modèle et les travaux connexes sur l'ensemble de données UNSW-NB15.

Le modèle XGBoost-LSTM **[79]** a présenté les performances les plus faibles, avec une précision de 73,29 %. En revanche, le modèle MCA-LSTM **[80]** a obtenu de bien meilleurs résultats, avec une précision de 94,90 %. Les meilleurs résultats ont été obtenus par le

modèle d'ensemble de **[81],** qui a utilisé XGBoost et KNN comme classificateurs de base et RF comme méta-classificateur, atteignant une précision de 96,24 %. Notre modèle a suivi de près cette approche d'ensemble, avec une précision de 95,19 %, ce qui indique ses solides performances pour la détection des intrusions dans les réseaux IoT.

Bien que le modèle d'ensemble de **[81]** ait démontré des performances supérieures grâce à la variation des multiples classificateurs utilisés, notre modèle a obtenu des résultats très proches en utilisant uniquement une architecture basée sur LSTM. Ce résultat est principalement dû à la caractéristique unique de notre modèle : l'inclusion d'une variable de fenêtre temporelle, qui permet un réglage fin et une optimisation supplémentaire. Cette caractéristique distinctive pourrait potentiellement permettre à notre modèle de surpasser même les performances optimales obtenues dans l'étude **[81]** lors des itérations futures.

De plus, les classificateurs d'apprentissage automatique peuvent rencontrer des problèmes de performance lorsqu'ils traitent de grands ensembles de données, tandis que les architectures d'apprentissage profond, telles que LSTM, sont très efficaces avec n'importe quel type d'ensemble de données.

III.11 Conclusion :

En conclusion, nous avons proposé un modèle hiérarchique de détection des intrusions qui utilise la mémoire à long terme (LSTM) en IoT. L'efficacité du modèle a été évaluée sur l'ensemble des données UNSW-NB15 et Minerva. Le modèle hiérarchique comprend deux niveaux. Le premier niveau utilise un modèle LSTM de classification binaire conçu spécifiquement pour détecter le trafic anormal. Le deuxième niveau utilise un modèle LSTM multi-classe pour classer le type exact d'attaque.
Ce processus d'agrégation temporelle a été introduit pour améliorer les performances du modèle. Les résultats de l'étude soulignent l'efficacité des modèles à base de LSTM avec agrégation temporelle dans la détection des intrusions, apportant ainsi une contribution précieuse au domaine de la recherche.

Conclusion

Conclusion générale

Avec l'augmentation du nombre d'appareils connectés à l'Internet des objets (IoT), leur sécurité devient un enjeu majeur. L'IoT implique la présence omniprésente de données, ce qui accroît les risques. Bien que de nombreuses recherches se concentrent sur la sécurisation de ces réseaux, peu d'entre elles prennent en compte les environnements réels de l'IoT.

, Dans ce travail, nous avons étudié les attaques les plus importantes contre les protocoles de routage dans l'IoT et leur fonctionnement. La sécurité dans l'IoT suscite plus d'intérêt que dans tout autre environnement, car elle implique des composants sensibles. L'objectif de ce travail était de construire un système de détection d'intrusion (IDS) contre les attaques dans l'IoT, basé sur des algorithmes d'apprentissage profond. Pour entraîner notre modèle, nous avons utilisé un ensemble de données d'attaques de routage appelé Minerva. Cet ensemble de données a été créé avec un simulateur Cooja et était basé sur des recherches récentes. Il contenait quatre attaques principales (blackhole, decreased rank, modification du numéro de version, inondation de Hello) ainsi que des caractéristiques importantes telles que la position des nœuds et l'énergie.

Nous avons proposé un modèle hiérarchique de détection des intrusions utilisant la mémoire à long terme (LSTM) pour l'IOT. L'efficacité du modèle a été évaluée sur les ensembles de données UNSW-NB15 et Minerva. Le modèle hiérarchique comprenait deux niveaux : le premier niveau utilisait un modèle LSTM de classification binaire conçu pour détecter le trafic anormal, et le deuxième niveau utilisait un modèle LSTM multi-classes pour classer le type exact d'attaque. Ce processus d'agrégation temporelle a été introduit pour améliorer les performances du modèle. Notre modèle a montré des taux de fausses alarmes (faux positifs) réduits, ainsi qu'une exactitude et une précision élevées. Les résultats de l'étude ont souligné l'efficacité des modèles basés sur LSTM avec agrégation temporelle dans la détection des intrusions, apportant ainsi une contribution précieuse à la recherche dans ce domaine.

Pour les travaux futurs, il serait intéressant d'ajouter d'autres attaques récentes à l'ensemble des données, ainsi que de combiner certains algorithmes d'apprentissage profond pour obtenir de meilleurs résultats. De plus, l'ajout de PCA pourrait réduire le temps d'apprentissage des IDS, les rendant ainsi plus efficaces contre la plupart des attaques. Le thème traité est un thème de recherche qui nécessite une continuité.

REFERENCES BIBLIOGRAPHIQUES

[1] Alexis Bitaillou, Benoît Parrein et Guillaume Andrieux. “Synthèse sur les protocoles de communicationpourl’Internetdesobjetsdel’industrie4.0”. Thèse de doct.LS2N, Université de Nantes ; IETR, UniversitédeNantes,2019.

[2] url : https://www.12h15.fr/notice-quest-ce-quun-objet-connecte/ (consulté le 22/02/2024).

[3] Shanzhi CHEN et al. ≪ A vision of IoT: Applications, challenges, and opportunities with china perspective ≫. In: IEEE Internet of Things journal 1.4 (2014),
p. 349-359.

[4] Raja BENABDESSALEM, Mohamed HAMDI et Tai-Hoon KIM. ≪ A survey on security models, techniques, and tools for the internet of things ≫. In: 2014 7th International Conference on Advanced Software Engineering and Its Applications. IEEE. 2014, p. 44-48.

[5] Shancang LI, Li Da XU et Shanshan ZHAO. ≪ The internet of things: a survey ≫.
In: Information systems frontiers 17.2 (2015), p. 243-259.

[6] P Gokul Sai SREERAM et Chandra Mohan Reddy SIVAPPAGARI. ≪ Development of Industrial Intrusion Detection and Monitoring Using Internet of Things ≫. In : International Journal of Technical Research and Applications (2015).

[7] Arnaud Rosay < Détection d’intrusions dans les objets connectés par des techniques d’apprentissage automatique : étude dans les domaines de l’éducation et des voitures connectées> Le Mans Université 5 décembre 2022 <https://theses.hal.science/tel-03937132 > consulté le (26 /04 /2024).

[8] url : http://visioforce.com/smarthome.html/ (visité le29/04/2024).

[9] Haniche Malika et Tabrait Nabila. “Internet des objets dans le domaine de l’agri-culture dedemain.”Thèsededoct.UniversitéMouloudMammeri,2019.

[10] url : https://www.al-enterprise.com/-/media/assets/internet/documents/ iot-for-education-solutionbrief-fr.pdf (visité le29/04/2024).

[11] Hicham El Mrabet et aitmoussa Abdelaziz. L’INTERNET DESOBJETSET LES TICE:Vers une école intelligente. Mai2017.

[12] Muhammad Burhan et al. “IoT elements,layered architectures and securityissues: A comprehensivesurvey”.In: sensors 18.9 (2018),p.2796.

[13] Muhammad Burhan et al. “IoTElements,LayeredArchitecturesandSecurity Issues :AComprehensiveSurvey”.In: Sensors 18 (2018).

[14] Younes Abbassi et Habib Benlahmer. “Unaperçusurlasécuritédel’internet des objets (IOT)”. In : ColloquesurlesObjetsetsystèmesConnectés-COC’2021. 2021.

[15] Alexis Bitaillou, Benoît Parrein et Guillaume Andrieux. “Synthèse sur les protocoles de communication pour l’Internet des objets de l’industrie 4.0”. Thèse de doct.LS2N, Université de Nantes ; IETR, Université de Nantes,2019.

[16] Muhammad Burhan et al. “IoT elements, layered architectures and security issues: A comprehensive survey”. In: sensors 18.9 (2018), p.2796.

[17] Shadi Al-Sarawi et al. “Internet of Things (IoT)communication protocols». In: 2017 the International conference on information technology(ICIT). IEEE.2017, p. 685-690.

[18] Tara Salman et Raj Jain. “A survey of protocols and standards for internet of things». In: arXiv preprintarXiv:1903.11549 (2019).

[19] Jasenka Dizdarević et al. “A survey of communication protocols for internet of things and related challenges of fogand cloud computing integration”. In: ACM Computing Surveys (CSUR) 51.6 (2019), p.1-29.

[20] Abiy Biru Chebudie, Roberto Minerva et Domenico Rotondi. “Tow ardsadefinition of the Internet of Things (IoT)”. Thèsededoct.Août2014.

[21] Jorge Granjal, Edmundo Monteiro et Jorge Sá Silva. “Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues». In IEEE Communications Surveys Tutorials 17 (juil.2015),p.1-1.

[22] url : https://connect.ed-diamond.com/open-silicium/os-019/mise-en- place-d-un-reseau-iot-avec-riot (visité le01/04/2023).

[23] Pallavi Sethi et SmrutiR Sarangi. “Internet of things: architectures, protocols, and applications». In: Journal of Electrical and Computer Engineering 2017 (2017).

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

[25] Younes Abbassi et Habib Benlahmer. “Unaperçusurlasécuritédel’internet des objets (IOT)”. In : ColloquesurlesObjetsetsystèmesConnectés-COC’2021. 2021.

[26] Godwin Thomas et Mary-Jane Sule. "A service lens on cybersecurity continuity and management for organizations' subsistence and growth". In: Organizational Cybersecurity Journal: Practice, Process and People (2022).

[27] Manish M PATEL et Akshai AGGARWAL. ≪ Security attacks in wireless sensor networks: A survey ≫. In: 2013 International Conference on Intelligent Systems and Signal Processing (ISSP). IEEE. 2013, p. 329-333.

[28] Shyam Nandan KUMAR. ≪ Review on network security and cryptography ≫. In:International Transaction of Electrical and Computer Engineers System 3.1 (2015), p. 1-11.

[29] VU CHEZHIAN, Dr RAMAR et Zaheer Uddin KHAN. ≪ Security requirements in mobile ad hoc networks ≫. In: International Journal of Advanced Research in computer and communication engineering 1.2 (2012), p. 45-49.

[30] 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.

[31] J. Vasseur, N. Agarwal, J. Hui, Z. Shelby, P. Bertrand, and C. Chauvenet, "RPL: The IP routing protocol designed for low power and lossy networks," *Internet Protoc. Smart Objects Alliance*, vol. 36, 2011.

[32] Tim Winter et al. RPL: IPv6 routing protocol for low-power and lossy networks. Rapp. Tech.2012.

[33] Harith Kharrufa, HayderAA Al-Kashoash et AndrewH Kemp. "RPL-based routing protocolsinIoTapplications:Areview".In: IEEE SensorsJournal 19.15 (2019), p.5952-5967.

[34] Oana Iova, Fabrice Theoleyre et Thomas Noel. "Usingmultiparentroutingin RPL toincreasethestabilityandthelifetimeofthenetwork". In: AdHocNetworks 29 (2015), p.45-62.

[35] Anthéa Mayzaud, Rémi Badonnel et Isabelle Chrisment. "ATaxonomyof Attacks in RPL-based Intrnet of Things". In: International journal of network security 18.3 (mai2016),p.459-473.

[36] Ghada Aljufair, Mohammed Mahyoub et AbdulazizS Almazyad. "OnMiti- gating DIS Attacks in IoT Networks». In: 2023 18thWirelessOn-DemandNetwork Systems and Services Conference (WONS). IEEE.2023, p.104-109.

[37] Avleen Malhi, Shalini Batra et Husanbir Pannu. “Security of Vehicular Ad-hoc Networks: A Comprehensive Survey». In: Computers Security 89 (nov.2019), p. 101664.

[38] Abhishek Verma et Virender Ranga. “Analysis of routing attacks on RPL based 6LoWPANnetworks”.In: International Journal of Gridand Distributed Computing 11.8 (2018),p.43-56.

[39] A Krari, A Hajami et E Jarmouni. “Study and Analysis of RPL Performance Routing ProtocolUnderVariousAttacks”. In: International Journal on “Technical and Physical Problems of Engineering” (IJTPE) 13.49 (2021), p.152-161.

[40] Rajasekar Ramalingam et Rajkumar Soundrapandiyan. “AnalysisofBlackhole AttackinRPL-based6LoWPAN Network: ACaseStudy”. In: nov.2021, p.1-6.

[41] Cong Pu. “Sybil Attack in RPL-Based Internet of Things: Analysis and Defenses”. In: IEEE Internet of Things Journal 7.6 (2020), p.4937-4949.

[42] Divya Sharma, Ishani Mishra et Sanjay Jain. “A detailed classification of routing”. In: International Journal of Advance Research, Ideas and Innovations in Technology 3.1 (2017), p.692-703.

[43] HARROUZ AHMED AMINE AMIRA BOUBAKEUR. “Utilisation des métaheuristiques pour la résolution du problème de sélection d’attributs : Application `a la détection d’intrusions”. In : (2013).

[44] Bourouba, Hadjer,et Ouidad Chaouche.Optimisation des IDS du Cloud Computing par les techniques de machines Learning .Université Ibn Khaldoun-Tiaret-,2020 .dspace.univ-tiaret.dz,http://dspace.univ-tiaret.dz :80/handle/123456789/5364

[45] D.E Denning. ‖An intrusion dection model‖ In: proccedings of the IEEE Transactions on software engineering, Septembre 2007.

[46] David J. Brooks and Michael Coole, Security Science, School of Science, Edith Cowan,

University, Perth, WA, Australia: Intrusion Detection Systems. DOI: https://doi.org/10.1007/978-3-

319-69891-5_161-1

[47] Alzahrani, A.O.; Alenazi, M.J.F. Designing a Network Intrusion Detection SystemBased on Machine Learning for Software Defined Networks. Future Internet **2021**, 13,111.

[48] Bourouba, Hadjer,et Ouidad Chaouche.Optimisation des IDS du Cloud Computing par les techniques de machines Learning .Université Ibn Khaldoun-Tiaret-,2020 .dspace.univ-tiaret.dz,http://dspace.univ-tiaret.dz :80/handle/123456789/5364

[49] Stefan Axelsson, Department of Computer Engineering, Chalmers University of Technology Goteborg, Sweden, Intrusion Detection Systems: A Survey and Taxonomy.

[50] Alzahrani, A.O.; Alenazi, M.J.F. Designing a Network Intrusion Detection System Based on Machine Learning for Software Defined Networks. Future Internet **2021**, 13,111.

https://doi.org/10.3390/fi 13050111

[51] Kanth, Vikram K. Monterey, CA; Naval Postgraduate School « BLOCKCHAIN FOR USE IN COLLABORATIVE INTRUSION DETECTION SYSTEMS » 2019-09

[52] ChiragModi DhirenPatel Bhavesh Borisaniya Hiren Patel Avi Patel Muttu Krishnan Rajarajan A survey of intrusion detection techniques in Cloud https://doi.org/10.1016/j.jnca.2012.05.003

[53] Hung-Jen Liao Chun-HungRichardLin Ying-ChihLin Kuang-YuanTung Intrusion detection

system: A comprehensive review http://dx.doi.org/10.1016/j.jnca.2012.09.004 http://hdl.handle.net/10945/63465

[54] Ming Zhong, Yajin Zhou et Gang Chen. “Sequential model-based intrusion detection system for IoT servers using deep learning methods”. In: Sensors (2021).

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

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

[57] Hacene BELLAHMER. ”Implémentation et évaluation d’un modèle d’apprentissage automatique pour l’estimation de la valeur marchande de propriétés immobilières”. In :(2020).

[58] Dietmar PF Moller. “Machine Learning and Deep Learning”. In: Guide to Cybersecurity

in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. Springer, 2023, p. 347-384.

[59]/ [60] "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 Aurélien Géron

[61]"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.

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

[63] Khan, A., Sohail, A., Zahoora, U., Qureshi, A. S. (2020). A survey of the recent architectures of deep convolutional neural networks. Artificial intelligence review, 53(8), 5455-5516.

[64] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, A. Razaque, Deep recurrent neural network for IoT intrusion detection system, Simul. Model. Pract. Theory 101 (2020)102031.

[65] O. Jullian, B. Otero, E. Rodriguez, N. Gutierrez, H. Antona, R. Canal, Deep-learning based detection for cyber-attacks in IoT networks: A distributed attack detection framework,J. Netw. Syst. Manage. 31 (2) (2023) 33.

[66] Y.K. Saheed, A.I. Abiodun, S. Misra, M.K. Holone, R. Colomo-Palacios, A machine learning-based intrusion detection for detecting internet of things network attacks, Alex. Eng. J.
61 (12) (2022) 9395–9409.

[67] S. Dadkhah, H. Mahdikhani, P.K. Danso, A. Zohourian, K.A. Truong, A.A. Ghorbani, Towards the development of a realistic multidimensional IoT profiling dataset, in: 2022 19th
Annual International Conference on Privacy, Security & Trust (PST), IEEE, 2022, pp. 1–11.

[68] 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.

[69] 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.

[70] 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

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

[72] « 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.

[73] Tensor Flow. ‖ https://www.tensorflow.org/ (accessed Sep. 1, 2021).

[76] Johnny. « Prétraitement des données dans l'apprentissage automatique ». Blog ARC Optimizer, 7 octobre 2022, https://blog.arcoptimizer.com/pretraitement-des-donnees-dans-lapprentissage-automatique.

[77] « One Hot Encoding in Machine Learning ». *GeeksforGeeks*, 12 juin 2019, https://www.geeksforgeeks.org/ml-one-hot-encoding-of-datasets-in-python/.

[78] Rouvière, Laurent. Chapitre 7 Données déséquilibrées | Machine learning. lrouviere.github.io, https://lrouviere.github.io/TUTO_ML/dondes.html. Consulté le 20 juin 2023.

[79]: S. M. Kasongo, "A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework," Comput Commun, vol. 199, pp. 113–125, Feb. 2023, doi:

10.1016/j.comcom.2022.12.010.

[80]: R. H. Dong, X. Y. Li, Q. Y. Zhang, and H. Yuan, "Network intrusion detection model based on multivariate correlation analysis - long short time memory network," IET Inf Secur, vol. 14, no. 2, pp. 166–174, Mar. 2020, doi: 10.1049/iet-ifs.2019.0294

[81]: M. H. Kabir, M. S. Rajib, A. S. M. T. Rahman, M. M. Rahman, and S. K. Dey, "Network Intrusion Detection Using UNSW-NB15 Dataset:Stacking Machine Learning Based Approach," in 2022 International Conference on Advancement in Electrical and Electronic Engineering, ICAEEE 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICAEEE54957.2022.9836404.