**REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE**

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE 20 AOUT 1955 - SKIKDA

FACULTE DES SCIENCES

DEPARTEMENT D'INFORMATIQUE

**Mémoire de fin d'études**

**Pour l'Obtention du Diplôme de Master en Informatique**

**Option** : Systèmes Informatiques

**Thème**

# L'apprentissage profond pour la détection d'attaque DoS dans l'IoT

**Présenté par :**

- Nia Sara
- Soltani Chafia

**Encadré par :**

- Dr. Chikh Ramdane

**Année Universitaire : 2021-2022**

# *Remerciement*

*Au terme de ce travail, on tient à remercier **ALLAH** le tout puissant de nous avoir donné la foi et de nous avoir permis d'en arriver là.*

*On tient à exprimer nous profonde gratitude à notre cher professeur et encadrant **Mr. Chikh Ramdane** pour son suivi et pour son énorme soutien, qu'il n'a cessé de nous prodiguer tout au long de la période du projet. N'adressons aussi nos vifs remerciements aux membres des jurys pour avoir bien voulu examiner et juger ce travail.*

*Nous ne laisserons pas cette occasion passer, sans remercier tous les enseignantes le personnel de l'**université de 20 Aout 1955 Skikda**, et particulièrement ceux de la section de **département d'informatique** pour leur aide et leurs précieux conseils et pour l'intérêt qu'ils portent à nos formation.*

*Enfin, nos remerciements à tous ceux qui ont contribué de près ou de loin au bon déroulement de ce projet.*

# Dédicace

*Je dédie ce travail :*

*A ma chère mère et à mon cher père qui n'ont jamais cessé de me supporter, et m'encourager durant mes années d'études.*

*A mes sœurs, mes frères, qui me donnent de l'amour et de la vivacité.*

*Aux enfants Taim, Maissem et Ilef*

*Vous occupez une place particulière dans mon cœur.*

*A tous ceux qui m'ont aidé - de près ou de loin -*

*A tous mes amis qui m'ont toujours encouragé, et à qui je souhaite plus de succès.*

*Merci!*

**SARA**

# Dédicace

*Je dédie ce travail :*

*A mon père *ALI* qui ma toujours soutenue dans moments difficiles et pour ses sacrifices et ses encouragements dieu me le garde.*

*A ma mère *SAADIA* qui a sacrifié sa vie pour mon bien êtrelui dédie ce modeste mémoire en souhaitant de tout mon cur dieu me la garde.*

*A mes chers frères "Walid, Mokhtar, Bilel"*

*A mes chères sœurs "Amel, Halima, Sihem, Yousra" Auxenfants "DJouri roaa, Assil, Adem, Djoud, Iline"*

*A ma chère amie *Chourouk Boubaissa**

*Mon amie : *Sara*, qui a été mon binôme durant toute notrecursus.*

*A ma grande mère et mes tantes et oncles et tous leurs enfants A toutes*

*mes amies "Romaissa, Kenza, Bouchra, Romiela, Leila, Malek, Roaa,*

*khawla, Ikram"*

*A tous mes camarades de la promotion 2021 : Master Systèmes Informatiques.*

*A tous ceux qui me sont chers et que j'ai involontairement oublié*

*A tous mes professeurs.*

*Merci!*

**CHAFIA**

# Résumé

L'IoT connecte toutes les choses dans le monde à Internet et constitue un moyen intelligent d'envoyer et recevoir des informations. Au fur et à mesure que cettetechnologie progresse, la nécessité d'exploiter la détection et la sensibilisation aux faiblesses augmente pour empêcher l'accès non autorisé aux ressources critiques et aux fonctions commerciales, rendant ainsi le système indisponible. Les attaques par déni de service (DoS) sont aussi communes. Le système de détection d'intrusion (IDS) est le processus qui examine l'activité du système ou du réseau pour trouver d'éventuelles intrusion ou attaques. Nous avons étudié les performances des méthodes d'apprentissage profond (DL) appliquées à la détection des intrusions pour Internet of Things. Ensuite, Nous avons évalué les méthodes proposées avec l'ensemble de données UNSW-NB15 pour la détection des attaques DoS sur IoT. Nous avons également présenté une étude comparative avec les algorithmes d'apprentissage profond, en utilisant différentes mesures appliquées pour l'évaluation des performances d'apprentissage profond (Précision, F1-score). Les résultats expérimentaux ont montré que les performances des algorithmes apprentissage automatique (ML) traditionnels sont supérieures à celles des approches de deep learning (DL) proposées en tant que modèles de détection avec une grande précision.



**Mots clés :** Internet des objets (IoT), Système de détection d'intrusion (IDS), Déni de service (DoS), Apprentissage profond (DL), Apprentissage automatique (ML), UNSW-NB15.

# Abstract

IoT connects everything in the world to the Internet and is a smart way to send and receive information. As this technology advances, the need to leverage vulnerability detection and awareness increases to prevent unauthorized access to critical resources and business functions, thereby rendering the system unavailable. Denial of Service (DoS) attacks is also common. Intrusion Detection System (IDS) is the process that examines system or network activity to find possible intrusions or attacks. We studied the performance of deep learning (DL) methods applied to intrusion detection for Internet of Things. Then, we evaluated the proposed methods with the UNSW-NB15 dataset for the detection of DoS attacks on IoT. We also presented a comparative study with deep learning algorithms, using different measures applied for the evaluation of deep learning performance (Precision, F1-score). The experimental results showed that the performance of traditional machine learning (ML) algorithms is superior to that of deep learning (DL) approaches proposed as detection models with high accuracy.



**Keywords:** Internet of Things (IoT), Intrusion Detection System (IDS), Denial of Service (DoS), Deep Learning (DL), Machine Learning (ML), UNSW-NB15.

# الملخص

تربط إنترنت الأشياء كل الأشياء في العالم بالإنترنت وهي طريقة ذكية لإرسال المعلومات واستلامها. مع تقدم هذه التكنولوجيا، تزداد الحاجة إلى تعزيز اكتشاف الثغرات والوعي لمنع الوصول غير المصرح به إلى الموارد الهامة ووظائف الأعمال، وبالتالي جعل النظام غير متاح. هجمات رفض الخدمة (DoS) شائعة أيضًا. نظام كشف التطفل (IDS) هو العملية التي تفحص نشاط النظام أو الشبكة للعثور على عمليات التطفل أو الهجمات المحتملة. درسنا أداء طرق التعلم العميق (DL) المطبق على كشف التسلل لإنترنت الأشياء. بعد ذلك ، قمنا بتقييم الأساليب المقترحة باستخدام مجموعة بيانات UNSW-NB15 لاكتشاف هجمات DoS على إنترنت الأشياء. قدمنا أيضًا دراسة مقارنة مع خوارزميات التعلم العميق ، باستخدام مقاييس مختلفة مطبقة لتقييم أداء التعلم العميق (الدقة ، درجة F1). أظهرت النتائج التجريبية أن أداء خوارزميات التعلم الآلي التقليدية (ML) يتفوق على أداء مناهج التعلم العميق (DL) المقترحة كنماذج كشف بدقة عالية.

**الكلمات الرئيسية:** إنترنت الأشياء (IoT)، نظام كشف التسلل (IDS)، رفض الخدمة (DoS)، التعلم العميق (DL)، التعلم الآلي (ML)، UNSW-NB15.

# Table des matières

# Liste des figures

# Liste des tableaux

# Liste des abréviations

- **IoT :** Internet of Things.
- **UIT :** L'Union Internationale des Télécommunications.
- **IP :** Internet Protocol.
- **OC :** Objet Connectée.
- **DoS:** Denial of Service attack.
- **DDoS:** Distributed Denial of Service attack.
- **IDS :** Intrusion Detection System.
- **NIDS:** Network Intrusion Detection System.
- **HIDS:** Host Intrusion Detection System.
- **DIDS:** Distributed Intrusion Detection System.
- **IA :** Intelligence Artificial.
- **ML :** Machine Learning.
- **DL :** Deep Learning.
- **DNN :** Deep Neural Network.
- **CNNs :** Convolutional Neural Networks.
- **RNNs :** Recurrent Neural Networks.
- **LSTM:** Long Short-Term Memory.
- **MLP :** Mutli Layer Perceptions.
- **DT :** Decision tree.
- **NB :** Naive Bayes.
- **RF :** Random Forest.
- **GB :** Gradien Boost.

# Introduction générale

## 1. Le contexte de la recherche

Depuis sa création, l'Internet des objets (IoT) a connu une croissance fulgurante en tant que technologie de pointe. En un mot, l'IoT est l'intégration d'appareils et de données de sorte que les processus sont automatisés et centralisés dans une certaine mesure.

La recherche continue de développer des systèmes de détection d'intrusion (IDS) pour sécuriser la cyber-technologie qui résout les problèmes d'attaque dans l'environnement Big Data d'aujourd'hui, l'objectif premier de cette recherche se concentre sur la réalisation d'un IDS dans IoT basé sur la technique DL.

## 2. La problématique

Aujourd'hui, nous vivons dans l'ère la plus technologique de l'histoire de l'humanité. Pas un jour ne passe avant que nous l'appelions un nouveau terme, nous ne savons pas ce que c'est ni d'où il vient. Récemment, l'un des termes est devenu fréquemment répété, qui est l'Internet des objets (Internet of Things).

L'IoT est une description d'un réseau de communication sensoriel, c'est-à-dire composé d'objets tangibles contenant des capteurs, des logiciels et une technologie visant çà connecter différents appareils entre eux pour permettre l'échange d'informations et faciliter nos opérations. En plus, il est devenu le moyen préféré des entreprises car il fournit des informations précises qui leur permettent de prendre des décisions plus réalistes et scientifiques, mais comme tous les autres technologies, il n'est pas sans risques : avec l'augmentation de son acceptation, la multiplication des appareils connectés entre eux, et l'échange abondant d'informations entre les différents appareils, la vie privé et la sécurité se durcissent comme des préoccupations qui hantent les institutions et les particuliers. Parmi certains des risques qui affectent son travail, il y a des attaques appelées DoS, ces attaques sont considérées parmi les attaques qui sont menées en inondant les sites avec un torrent de données inutiles envoyées par des appareils infectés. Pour éviter ces attaques, nous avons mis point avec une solution quiaide à se protéger contre cette attaque.

## 3. Les objectifs

La solution proposée dans ce cadre est la création et le développement de modèles d'apprentissage en profondeur pour les activités normales et anormales afin de construire un IDS basé sur L'approche comportementale. Le développement d'un modèle DL robuste et optimisé nécessiteà nouveau un apprentissage et des tests sur l'ensemble de données actuel basé sur les

intrusions qui doit être constamment mis à jour avec de nouvelles menaces et des modèles DL optimisés.

## 4. L'organisation du manuscrit

Nous avons structuré ce mémoire de la façon suivante :

Le **premier chapitre (Internet des Objets),** sera consacré à la présentation générale de l'Internet of Things ;

Le **deuxième chapitre (La sécurité dans Internet of Things),** ce chapitre présente quelques notions de base sur la sécurité informatique et les attaques, et l'IDS ;

Le **troisième chapitre (description de projet),** sera consacré à la description générale de notre recherche ;

Le **dernier chapitre (Implémentation du système)** concerne l'implémentation de notre système et les outils de développements utilisé, tel que le langage Python, ainsi que quelques images et tableaux qui présentent les graphes et les résultats de notre système ;

Une **conclusion générale** viendra souligner tous les points importants de notre mémoire et nos travaux et perspectives futurs ;

Une **bibliographie** sera également mise à la disposition de la lecture ;

Une **annexe** présente un contenu scientifique détaillé, utilisé dans le développement des solutions proposées.

# Chapitre 01 :
# Internet des Objets

# 1. Introduction

Dans le monde matérialiste d'aujourd'hui, les gens évoluent vers un mode de vie extrêmement intelligent, productif, moins cher et limité dans le temps. Ces besoins de façon exponentielle augmentée la demande d'automatisation. Aujourd'hui, l'automatisation prend rapidement racine dans tous les domaines. [1]

Le concept Internet des Objets a été inventé en 1999 par un membre de la Communauté de développement de l'identification par radiofréquences (RFID), et il est récemment devenu plus pertinent pour le monde réel en raison du développement des appareils mobiles, des communications embarquées et ubiquitaire, du Cloud Computing et l'analyse des données. [2]

L'Internet des Objets (IoT) est une source mondiale d'informations émergentes basées sur une architecture Internet qui facilite l'échange de biens et de services. L'IoT est un système d'appareils informatiques interdépendants, de machines mécaniques et numériques, d'objets, d'animaux ou de personnes qui ont des identifiants uniques et sont capables de transmettre des données sur un réseau sans interaction d'homme à homme ou d'homme à ordinateur. L'Internet des Objet (IoT) connecte n'importe qui, où, quant. Avec le développement de la technologie, nous nous dirigeons vers une société où tout est connecté.

Dans ce chapitre, nous présentons la définition, l'importance, les avantages et les inconvénients de l'IoT (Internet des Objets), les domaines d'application, le modèle en couches, les caractéristique, la plateforme, l'architecture, etc.

# 2. Définition

L'Internet des Objets (IdO) en anglais Internet of Things (IoT) décrit un réseau de terminaux physiques, des objets qui intègrent des capteurs, des softwares et d'autres technologies pour se connecter et échanger des données avec d'autres terminaux et systèmes sur internet. Ces terminaux peuvent aller du simple appareil électroménager à l'outillage industriel très complexe.

Il y a plus de 7 milliards d'appareils IoT connectés aujourd'hui, et les experts prédisent que ce nombre passera à 10 milliards d'ici 2020 et 22 milliards d'ici 2025. Oracle dispose d'un réseau de partenaires d'appareils.

Selon l'UIT[1], l'Internet des Objets (IdO) est une « infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets *(*physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution ». [3] En réalité, la définition de ce qu'est l'Internet des objets n'est pas figée. Elle recoupe des dimensions d'ordres conceptuel et technique.

L'Internet des Objets (IoT) fait référence à un système d'objets interdépendants connectés à Internet, capables de collecter et de transmettre des données sur des réseaux sans fil intervention humaine. Avec l'avènement des puces informatiques super bon marché et la prolifération des réseaux sans fil, tout peut être transformé en une partie d'une parcelle de terrain.

D'autre définition s'en tiennent aux aspects technique de l'IoT (« objet doté d'identités et de personnalités virtuelles qui opèrent dans des espaces intelligents et utilisent des interfaces intelligentes pour se connecter et communiquer dans divers contextes d'utilisation »[4]), d'autres portent sur les usages et les fonctionnalités (« la convergence des identifiants numériques »[5]) stipule qu'il devient possible d'identifier de manière uniforme des éléments d'information numériques (adresses) et des éléments physiques (palettes dans un entrepôt ou animaux dans un troupeau).

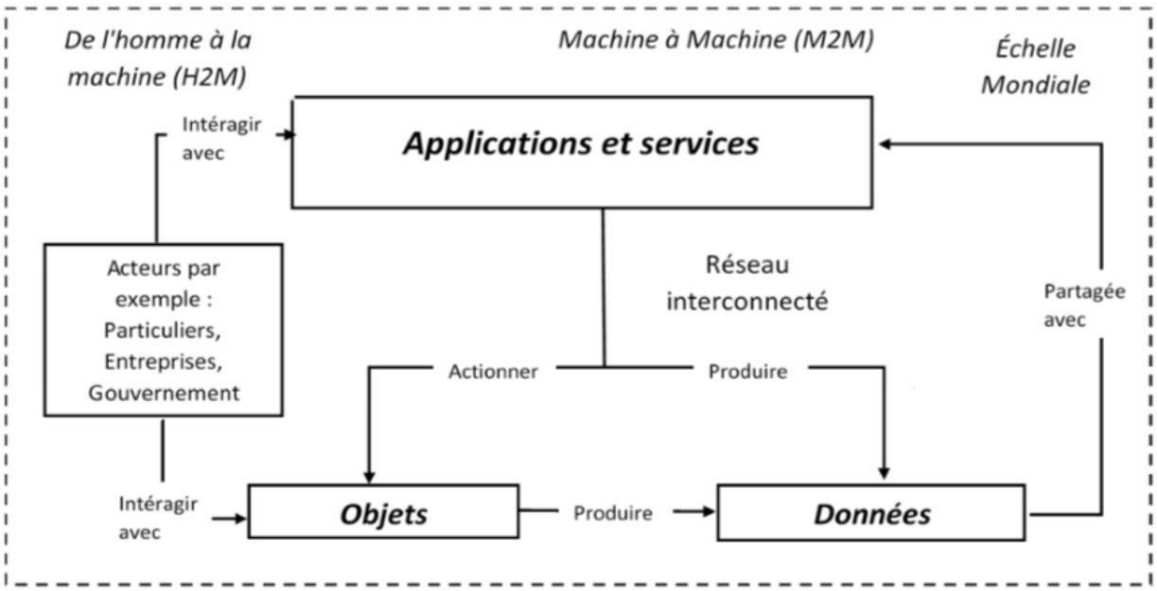



**Figure 1.1 :** Visualisation de la définition d'IoT. [6]

**1** L'Union Internationale des Télécommunications.

## 3. Clés concept de l'IoT

L'Internet des objets décrit le réseau d'objets physiques "choses" intégrant des capteurs, des logiciels et d'autres technologies dans le but de connecter et d'échanger des données avec d'autres appareils et systèmes sur Internet. Les concepts clés de l'IoT sont :

- ✓ **Matériel :** le cœur de l'IoT se compose de milliards d'appareils interconnectés avec des capteurs et des actionneurs connectés qui détectent et contrôlent le monde physique ;
- ✓ **Programmation embarquée :** Les appareils IoT sont des appareils embarqués qui peuvent être prototypés à l'aide de plates-formes de microcontrôleurs standardisées (telles qu'Arduino), et des cartes de circuits imprimés (PCBs) personnalisées développées ultérieurement ;
- ✓ **Sécurité :** La sécurité est l'un des problèmes les plus critiques de l'IoT, étroitement liée à l'éthique des données, à la confidentialité et à la responsabilité. Il doit être intégré à chaque étape de la conception du système ;
- ✓ **Intégration du réseau et du cloud :** La conception et la gestion du réseau sont essentielles dans l'IoT, en raison du grand nombre d'appareils connectés et de l'impact à grande échelle que les décisions de conception du réseau peuvent avoir ;
- ✓ **Analyse et prédiction des données :** Les développeurs doivent ingérer, stocker et interroger de manière sécurisée et fiable de grandes quantités de données hétérogènes à partir de ces appareils ;
- ✓ **Apprentissage automatique et Intelligence Artificielle :** Pour être vraiment intelligent, les analyses de big data doivent appliquer des techniques informatiques cognitives issues de Data Mining, la modélisation, des statistiques, de l'apprentissage automatique, et de l'Intelligence Artificielle.

## 4. Importance

L'importance de l'IoT est devenue assez importante car il s'agissait du premier véritable développement d'Internet. Cela conduira à des applications révolutionnaires qui peuvent profondément changer notre mode de vie, et notre façon d'apprendre, de travailler et de jouer. L'IoT fournit déjà été doté l'Internet de capacités de détection (température, pression, vibration, lumière, humidité, tension). [7]

Lorsqu'un élément est connecté à Internet, cela signifie qu'il peut envoyer ou recevoir des informations, ou les deux. Cette capacité à envoyer et/ou recevoir des informations rend les choses intelligentes, et plus intelligentes, c'est mieux.

## 5. Fonction d'IoT

L'internet des objets fonctionne principalement avec des capteurs et objets connectés placés dans/sur des infrastructures physiques. Ces capteurs vont alors émettre des données qui vont remonter à l'aide d'un réseau sans fil sur des plateformes IoT. [8] Par conséquent, ils peuvent être analysés et enrichis pour en tirer pleinement parti. Ces plateformes de gestion et de visualisation de données sont de nouvelles solutions IoT qui permettent aux territoires, aux entreprises et même aux utilisateurs d'analyser les données et d'en tirer des conclusions afin d'adapter les pratiques et les comportements.

Les éléments fondamentaux de l'IoT sont les appareils qui collectent des données. D'une manière générale, ce sont des appareils qui sont connectés à Internet, ils ont donc chacun une adresse IP [2]. Leur complexité va des véhicules autonomes transportant des produits dans les usines aux simples capteurs surveillant la température dans des bâtiments.

## 6. Composant de l'internet des objets

Le concept d'IoT nécessite la coordination des dispositifs suivants :

- Des balises physiques identifient chaque objet / des balises virtuelles identifient chaque emplacement ;
- Appareils mobiles (téléphones portables, gestionnaires, ordinateurs portables, etc.) équipés de logiciels supplémentaires pour lire les balises physiques ou localiser les balises virtuelles ;
- un réseau sans fil reliant le dispositif portable à un serveur contenant des informations sur l'objet marqué ;
- Les informations sur les objets sont gérées dans les pages Web existantes ;
- Un dispositif d'affichage (écran d'un téléphone mobile) peut demander des informations sur un objet ou un groupe d'objets.

[2] Internet Protocol.

# 7. Avantages et inconvénients d'IoT

## 7.1. Les avantages

Pour les industries, l'IoT représente un virage technologique qui facilite l'automatisation pour un internet industriel prédictif.

- ✓ Augmenter l'efficacité en prenant des décisions plus intelligentes et plus éclairées ;
- ✓ Réduisez vos coûts de maintenance en remplaçant les maintenances inutile par une maintenance prédictive plus efficace et personnalisée ;
- ✓ Optimisez vos processus grâce à une meilleure communication et un contrôle opérationnel à distance pour identifier les risques, les sources de gaspillage et les éventuels goulots d'étranglement ;
- ✓ Limitez vos coûts d'inventaire en réduisant les erreurs humaines et en facilitant la gestion automatisée des stocks pour opérations de logistiques ;
- ✓ Anticipez vos interventions de maintenance sur votre chaîne de production et réduisez fortement les risques de pannes brutales ;
- ✓ Surveillez l'efficacité et la productivité de votre équipement.

## 7.2. Les inconvénients

Chaque technologie doit également répondre à certaines lacunes ou à de nouveaux défis qui nécessitent une attention particulière. Pour l'IoT, les principaux sujets tournent autour des problématiques liées à la sécurité des données et aux cyber-attaques. En effet, à partir du moment où un appareil est connecté, il peut être source de piratage. Par conséquent, des protocoles de sécurité très stricts doivent être mis en place pour empêcher les personnes malveillantes d'accéder aux données hautement sensibles de l'exploitation de votre site industriel. La sécurité, la sauvegarde, l'audit et la surveillance régulière sont vos meilleures défenses.

De plus, nous ne pouvons pas oublier qu'il s'agit d'un objet connecté, donc même avec de nombreuses garanties en place, le risque de protection des données demeure. D'autre part, certaines personnes sont réticentes à mettre en œuvre cette technologie en raison d'un manque de connaissances.

# 8. Domaines d'applications de l'IoT

La technologie IoT peut être utilisée dans tous les domaines de la vie. Il peut être utilisé dans les entreprises, les maisons, les communications, les transports, les hôpitaux, les industries, les systèmes de sécurité, etc.


**Figure 1.2 :** Domaines d'applications d'IoT. [9]

## 8.1. Internet personnel des objets

Les appareils IoT peuvent être utilisés sous les formes suivantes :

- Maisons intelligentes, (par exemple : les applications que nous utilisons dans notre vie quotidienne telles que la télévision, les interrupteurs d'éclairage, les réfrigérateurs, les climatiseurs, le chauffage, les serrures de porte, les serrures de coffres-forts, le verrouillage/déverrouillage de porte, les systèmes de sécurité, et bien d'autres peuvent être contrôlés par Internet des Objets) ;
- Appareils portables, (tels que les Smartphones, les Fitbits, les moniteurs de santé, les montres, etc.) pour vous faciliter la vie. Ces appareils améliorent le divertissement, la connectivité réseau, la santé et la forme physique.

## 8.2. IoT dans les soins de santé

- Les appareils IoT portables permettent aux hôpitaux de surveiller la santé des patients pour obtenir des informations vitales en temps réel ;

- Les lits intelligents aident le personnel à être averti ;
- L'installation de capteurs IoT sur des équipements critiques peut améliorer la entraineune sûreté ou une sécurité accrue de l'équipement, sauvant ainsi des vies ;
- Il est utilisé dans les moniteurs de fréquence cardiaque, les montres intelligentes, surveillance de la glycémie chez les patients diabétiques.

### 8.3. IoT dans la fabrication

- Cela peut impliquer la numérisation de l'usine, la sécurité, la gestion des stocks, le contrôle de la qualité, l'emballage, la logistique et l'optimisation de la chaîne d'approvisionnement ;
- La technologie RFID et GPS peut prendre en charge un suivi des produits commerciaux de l'origine à la destination. L'ensemble de la chaîne d'approvisionnement peut être optimisé du début à la fin. Ces capteurs peuvent collecter des informations sur les temps de trajet, l'état du produit et les conditions environnementales auxquelles le produit est soumis ;
- Les capteurs fixés à l'équipement de l'usine peuvent aider à identifier les goulots d'étranglement dans la chaîne de production, et donc la diminution des déchets de temps ;
- Nous pouvons également suivre les performances des équipements et prévoir quand les machines ont besoin d'entretien pour éviter les pannes.

### 8.4. IoT de détail

- La technologie IoT peut être utilisée en les achats en ligne et en magasin. Il aide l'entrepôt, la robotique et la chaîne d'approvisionnement, la gestion des achats ;
- L'IoT peut aider à analyser le trafic des centres commerciaux afin que les magasins à l'intérieur du les centres commerciaux puissent prendre les mesures nécessaires pour améliorer l'expérience d'achat des clients tout en réduisant les frais généraux ;
- De nombreux avantages pour les détaillants peuvent cibler les clients en fonction des achats passés. En fonction des données fournies via l'IoT, les détaillants peuvent personnaliser les promotions pour leurs clients fidèles.

### 8.5. IoT dans les transports

- La technologie IoT pour les voitures autonomes ;

- Le GPS est un autre exemple d'utilisation de l'IoT pour aider les entreprises de transport à accélérer et à acheminer plus efficacement, ce qui traduit par les délais de livraison plus rapides ;
- Les urbanistes peuvent également utiliser les données pour comprendre les modèles de trafic, la demande de stationnement, ainsi que la construction et entretien des routes.

### 8.6. IoT en agriculture

- Surveille les niveaux d'humidité du sol pour déclencher les pompes d'irrigation, prédire le type et la fertilité du sol et prescrire différents engrais aux agriculteurs ;
- Améliorer le rendement en contrôlant les conditions climatique, l'irrigation intelligente, l'humidité du sol, les nutriments, les systèmes de fertilisation et réduisez les déchets en optimisant ressources limitées. Cela peut révolutionner les anciens métiers. Les gouvernements et les ingénieurs peuvent utiliser l'IoT pour analyser les facteurs complexes de l'urbanisme. Dans des domaines comme gestion du trafic, la gestion de l'énergie, de l'eau le management, le contrôle des déchets, la sécurité urbaine et les urgences ;
- En plus de cela, l'IoT est une aubaine pour le domaine de l'agriculture hydroponique. [10]

L'IoT peut également être utilisé dans l'éducation, l'énergie, la recherche, l'administration, le droit, l'application de la loi, l'environnement, la publicité, la construction de bâtiments, les tests, l'analyse, le marketing, la mode, le style de vie, etc. Il existe d'innombrables applications où de nombreuses technologies peuvent être utilisées.

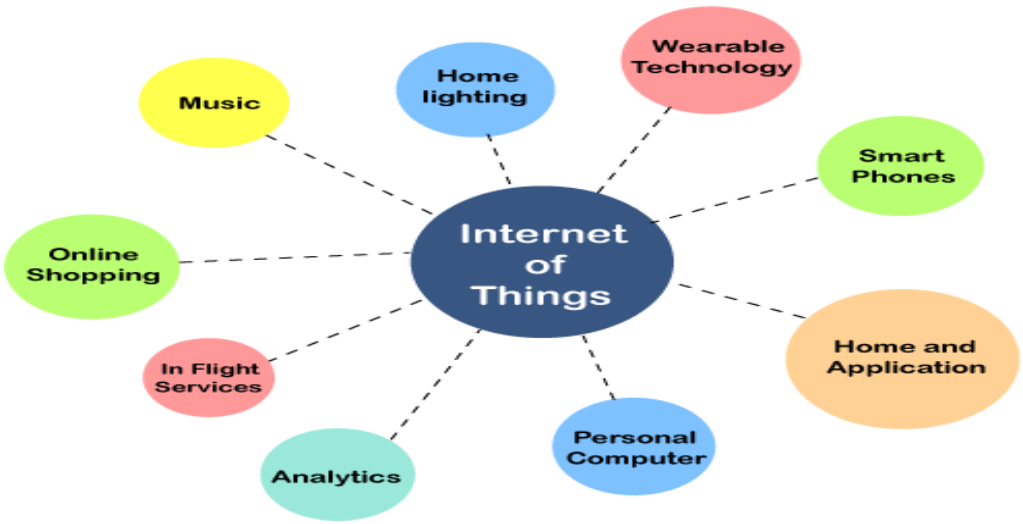



**Figure 1.3 :** Différents application d'IoT.

# 9. Modèle en couche

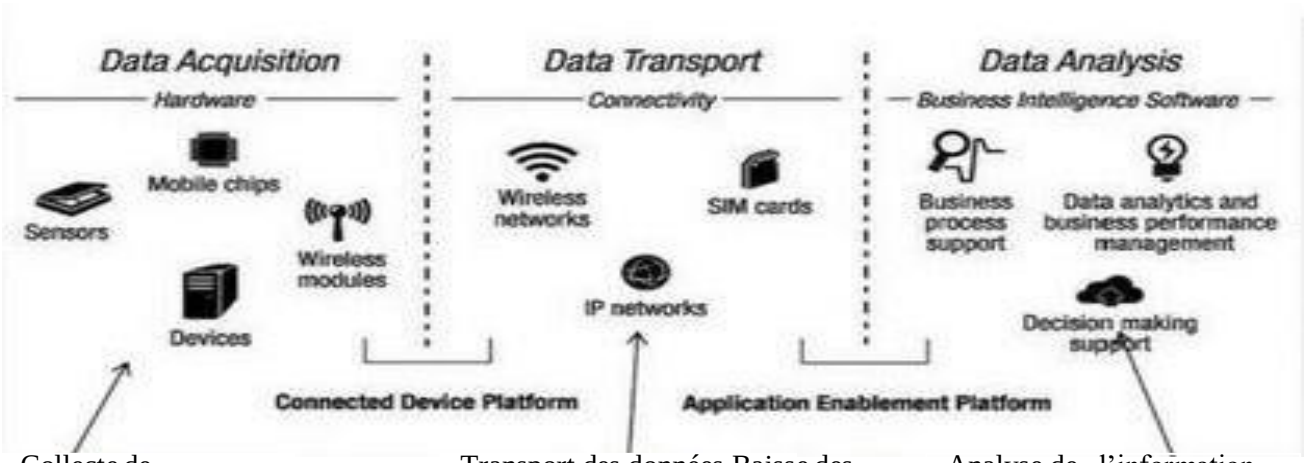



**Figure 1.4 :** Système d'Intégration & Services.

## 9.1. La couche acquisition

Le rôle de cette couche est la collecte des données à partir de l'environnement, les données seront captées à partir de l'environnement physique et converties à des données numériques. Dans cette couche il y a trois rôles clés : l'identification, la position et l'acquisition desdonnées.

## 9.2. La couche transport

La couche transport c'est-à-dire qui va transmettre l'information à partir des capteurs Giscard la partie stockage donc dans la partie transport en distingue deux types de technologies :

- Technologie de transmission au niveau local : LANs, PAN, Zigbee, Bluetooth ;
- Technologie des transmissions à grande distance : les services internet, réseau cellulaire.

## 9.3. La couche analyse

Cette couche analyse les données collectées, dans cette couche il y a deux composantes :

- Une composante de stockage (Cloud) : en stocke toutes les informations ;

- Une composante qui prend la décision selon les données collectes et les paramètres enregistrés.

## 10. Caractéristique d'IoT

Les caractéristiques fondamentales de l'IoT sont les suivantes : [11]

- **Inter connectivité :** En ce qui concerne l'IoT, tout objet peut être connecté à l'infrastructure mondiale d'information et de communication.
- **Services liés aux objets :** l'IoT est capable de fournir des services liés aux objets dans le cadre de ses exigences inhérentes, telles que la protection de la vie privée et la cohérence sémantique entre les objets physiques et leurs objets virtuels associés. Pour que de tels services puissent être fournis dans le respect de ces exigences, les technologies utilisées doivent évoluer dans le monde physique et de l'information.
- **Hétérogénéité** : Les dispositifs utilisés dans l'IoT sont hétérogènes puisqu'ils ne sont pas basés sur les mêmes plates-formes matérielles ni sur les mêmes réseaux. Ils peuvent interagir avec d'autres appareils ou plates-formes de service par l'intermédiaire de réseaux déférents.
- **Dynamiques :** L'état des dispositifs (par exemple veille/réveil, connecté/déconnecté) et l'environnement dans lequel ces appareils fonctionnent (emplacement, vitesse, etc.) changent de manière dynamique. D'autre part, le nombre d'appareils peut également être modifié dynamiquement.

## 11. Classification d'IoT

L'Internet des objets est un terme générique qui couvrant différentes avancées fondamentales uniques qui relient des éléments physiques et leur représentations virtuelles dans le but d'exploiter cette connexion pour améliorer les services et les idées de communication. [12] Le cadre de classification est basé sur une analyse des scénarios générés. Il manifeste des capacités spécifiques partagées par les scénarios IoT qui doivent être prises en compte afin de comprendre des scénarios de haut niveau ou de mettre en œuvre des scénarios à l'avance. [13] Dans le premier et le plus important composant architectural de l'IoT est la couche de perception. Il collecte des données à l'aide de capteurs, qui sont les plus moteurs essentiels de l'Internet des objets. [14]

Il y a différents types de capteurs utilisés dans diverses applications IoT. Les capteurs les plus couramment disponibles actuellement sont les téléphones intelligents. Les Smartphones eux-mêmes on de nombreux types de capteurs intégrés, tels que des caméras, des capteurs de lumière, des microphones, des capteurs de proximité, des capteurs de localisation (GPS), des capteurs de mouvement (accéléromètres, gyroscopes), et des magnétomètres.

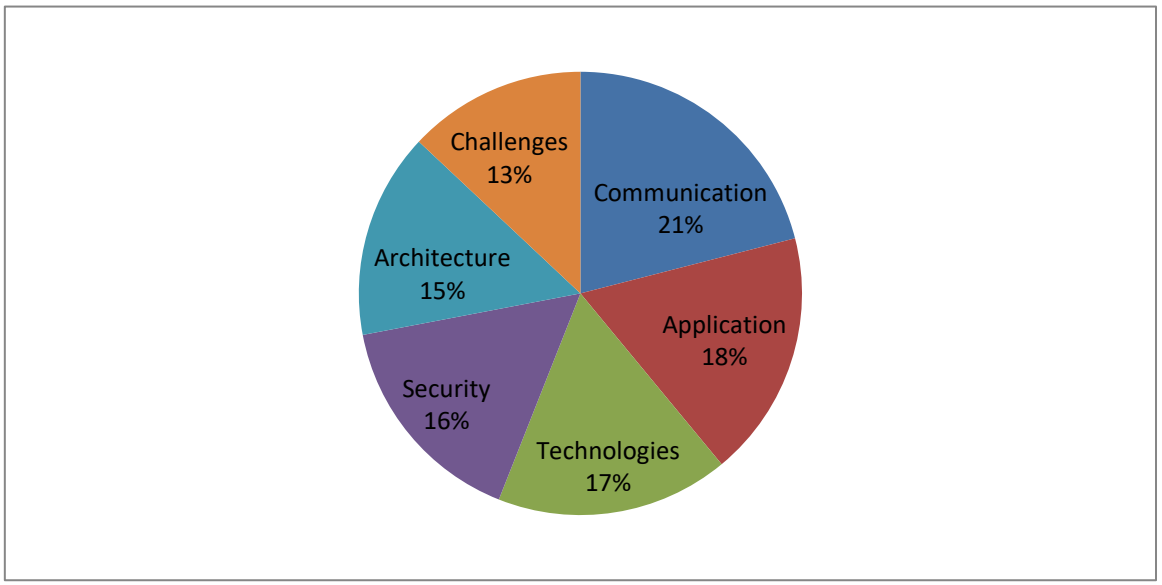



**Figure 1.5 :** Pourcentage de classification pour les revues IoT 2010-2019. [15]

| **Range** | | **Pouvoir** | | **Taux ou Débit** | | **Latence** | |
|---|---|---|---|---|---|---|---|
| **court** | **langue** | **Bas** | **haut** | **bas** | **haut** | **bas** | **Haut** |
| RF-ID<br>BLE<br>ZigBee<br>ANT<br>Z-wave<br>6LPWA<br>DASH 7<br>… | LoRa<br>Sigfox<br>LRLP (802.11)<br>… | ZigBee<br>LoRa<br>Ingenu<br>Sigfox<br>Telensa<br>EC-GSM-IoT<br>NB-IoT<br>Wirepas<br>Weightless(N/PW)<br>… | | ZigBee<br>LoRa<br>Ingenu<br>Sigfox<br>Telensa<br>NB-IoT<br>DASH 7 | BLE<br>Wirepas<br>… | DASH 7<br>Wirepas<br>… | NB-IoT<br>… |

**Tableau 1.1 :** IoT classification et exemple.

## 12. Étapes et technologies de l'écosystème IoT

L'OC [3] est au cœur de l'IoT, mais il est important de pouvoir connecter tous ces objets, leur permettant d'échanger des informations et d'interagir dans le même environnement. La mise en œuvre de l'IoT passe par les étapes suivantes : identification, installation de capteurs, objets se connectant entre eux, intégration et connexion au réseau. [16]

| **Identifier** | **Capteur** | **Connecter** | **Intégrer** | **Mettre en réseaux** |
|---|---|---|---|---|
| Permet d'identifier chaque élément connecté. | La mise en place du dispositif nousrapprochant du monde réel. Les fonctions de base des objets (le capteur de température pour lethermomètre par exemple). | Établissez une connexion entre tous les objets afin qu'ils puissent parler et échanger des données. | Disposer d'un moyen de communication rattachant les objetsau monde virtuel. | Connectez des objets et leurs données au monde informatique viaun réseau, tel qu'Internet. |
| IPv4, IPv6, 6loWPAN. | MEMS, RF MEMS, NEMS. | Sigfox, LoRa. | RFID, NFC, Bluetooth, B LE, ZigBee, Wi-Fi, réseaux cellulaires. | CoAP, MQTT, AllJoyn, REST HTTP. |

**Tableau 1.2:** Les étapes et les technologies pour la mise en place de l'IoT. [16]

## 13. Technologies d'IoT

L'IoT exploite principalement les technologies de mise en réseau et protocoles standards. Cependant, les technologies et protocoles IoT les plus importantes [17] sont RFID, NFC, Zigbee, Bluetooth, code de produit électronique (EPC), base énergie sans fil, code-barres, LTE-A, Intelligence Artificielle (IA), Réseaux de capteurs sans fil (WSN) et Wifi-Direct. [18]Contrairement au réseau unifié standard du système universel, ces technologies prennent en charge des fonctions réseau spécifiques requises par les systèmes IoT. [17]

[3] Objet Connectée.

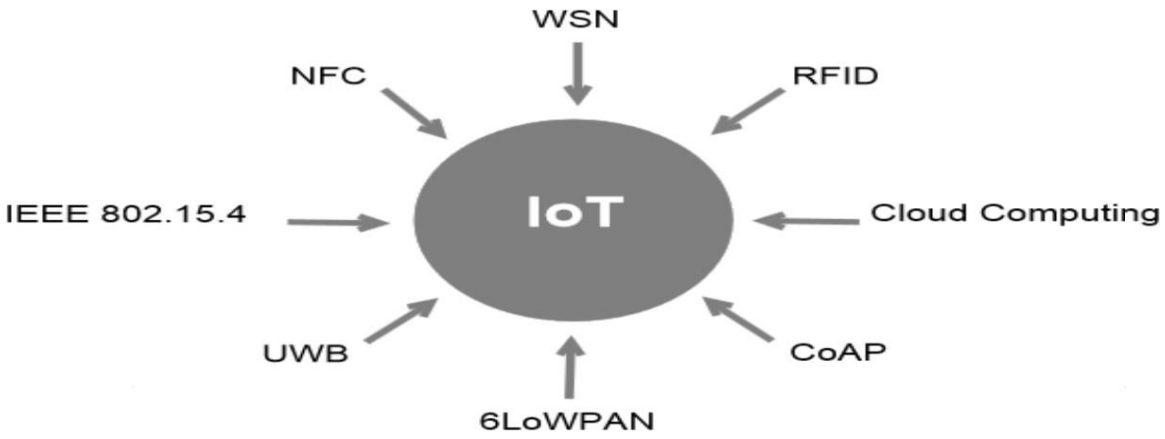



**Figure 1.6 :** Technologie d'IoT.

## 13.1. Identification par radio fréquence (RFID)

La RFID est une forme de communication sans fil qui utilise une combinaison de couplage électromagnétique ou électrostatique dans la partie radiofréquence du spectre du champ électromagnétique pour identifier avec précision des objets, c'est-à-dire des personnes. Une étiquette peut être lue à plusieurs mètres de distance et n'a pas besoin d'être dans une ligne droite de lecture pour suivre. Les principaux composants de la RFID sont les étiquettes, les antennes, les contrôleurs d'accès, les logiciels et les lecteurs de services, qui sont plus réels et efficaces.


**Figure 1.7 :** Déploiement de la technologie de RFID.

## 13.2. Communication de fichiers en champ proche (NFC)

Le NFC est un ensemble de technologie sans fil 13,56 MHz qui nécessite généralement une distance de 4 cm. [19] Les tags NFC sont des dispositifs passifs. Ils stockent des données qui peuvent être récupérées par des appareils NFC actifs.

La communication en champ proche, qui transmet des données via des champs radio électromagnétiques, est la technologie derrièreles services de paiement comme Apple Pay et Google Wallet. Cet appareil doit contenir une puce NFC pour effectuer des transactions NFC. Il fonctionne également dans des environnements sales, aucune ligne de mire requise, méthode de connexion simple et sans prétention.


**Figure 1.8 :** La technologie NFC.

### 13.3. Zigbee

Le Zigbee est une technologie sans fil basée sur des normes conçue pour permettre une connexion sans fil de machine à machine à faible coût et à faible consommation d'énergie.

Machines et réseaux IoT. Zigbee fonctionne selon la spécification IEEE 802.15.4 et est utilisé pour créer des réseaux qui nécessitent de faibles taux de transfert de données, des réseaux sécurisés et une efficacité énergétique. [20] Il est utilisé dans de nombreuses applications telles que les commandes de chauffage et de refroidissement, les systèmes d'automatisation des bâtiments, les commandes de chauffage et de refroidissement et les équipements médicaux.

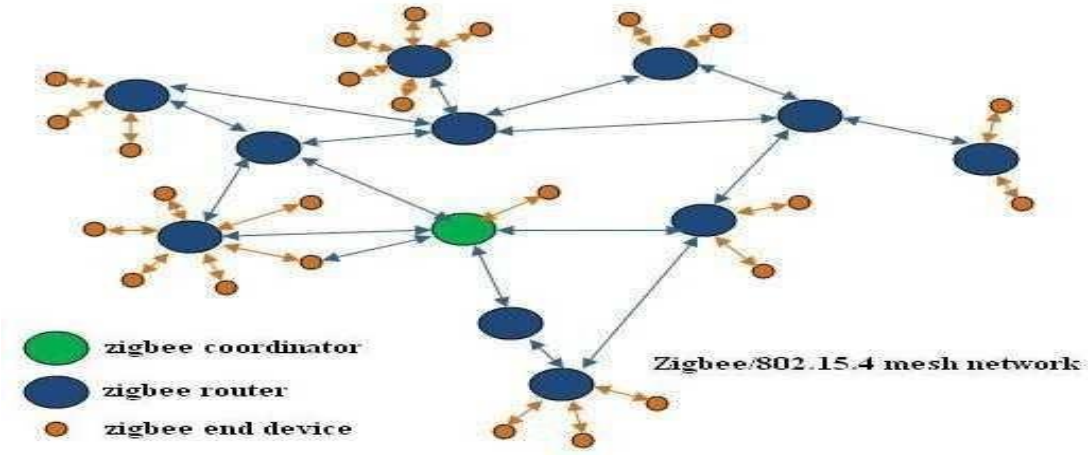



**Figure 1.9 :** Présentation du réseau Zigbee.

### 13.4. Bluetooth

Bluetooth est une technologie de communication sans fil à courte portée qui permet aux appareils (ordinateurs, téléphones portables et périphériques) de transmettre sans fil des données ou de la voix sur de courtes distances.

Le but de Bluetooth est de remplacer les câbles qui connectent normalement les appareils, tout en gardant les communications entre les appareils sécurisées. [21]

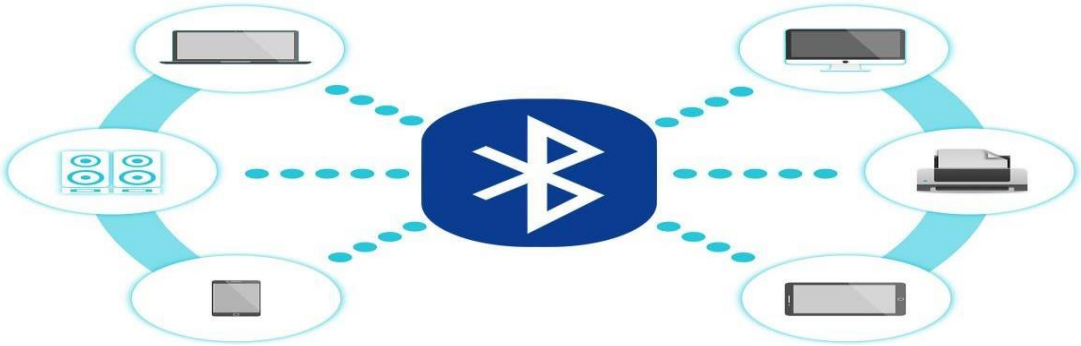


**Figure 1.10 :** La technologie Bluetooth.

### 13.5. Code de produit électronique (EPC)

Un code de produit électronique (EPC) est un numéro unique qui identifie un article spécifique dans la chaîne d'approvisionnement. Les EPC peuvent être associés à des données dynamiques, c'est-à-dire l'origine d'un article ou sa date de fabrication. [22] Tout comme un numéro d'identification de véhicule (VIN) ou un article commercial mondial (GTIN), les EPC sont essentiels au fonctionnement des systèmes d'information qui font partie d'un réseau mondial d'EPC. Un code EPC peut stocker des informations sur le type EPC, le numéro de série unique du produit, ses spécifications, des informations sur le fabricant, etc.

### 13.6. Sans fil à faible consommation

Cette technologie remplace l'aspect le plus gourmand en énergie d'un système IoT. Cependant, les capteurs et autres éléments peuvent être désactivés pendant de longues périodes et la liaison de communication doit rester en mode d'écoute. [23] Avec une faible consommation d'énergie, le sans-fil peut non seulement réduire la consommation, mais également prolonger la durée de vie de l'appareil grâce à une utilisation moindre.

### 13.7. Code à barre

Un code-barres se compose de barres et d'espaces et est une représentation codée lisible par machine de chiffres et de caractères. Aujourd'hui, emballages des produits vendus dans les supermarchés, les dépanneurs et d'autres magasins sont visibles partout. Ce sont des codes- barres. [24] Il existe 3 types de codes-barres de 2 dimensions (2D), numériques et alphanumériques. Les codes-barres sont conçus pour être lisibles par machine et lisibles à l'aide de lecteurs de codes-barres optiques, ils peuvent également être lus à l'aide de caméras.

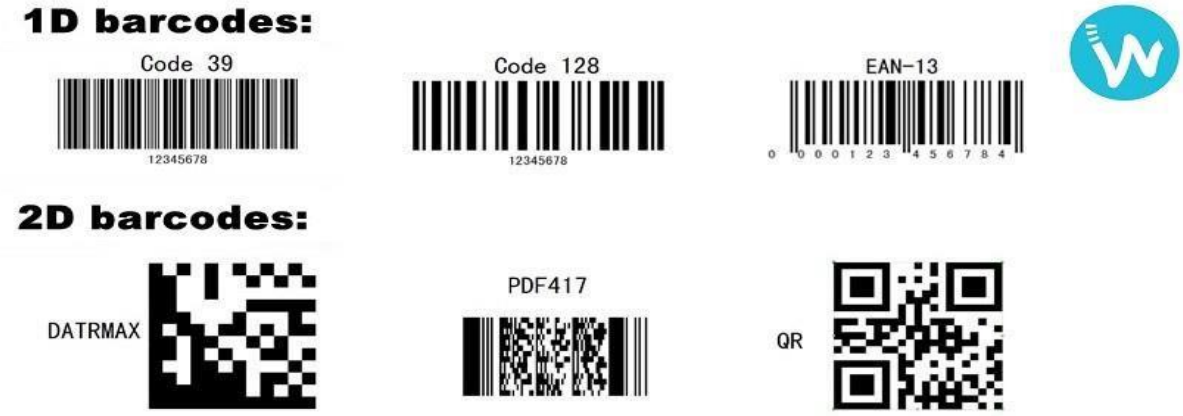



**Figure 1.11 :** Différences Codes-barres.

### 13.8. LTE-A

LTE-A signifie LTE-Advanced qui combine de nombreuses nouvelles technologies pour permettre aux systèmes de fournir des débits de données plus élevés, ainsi que d'excellentes performances, en particulier autour des bords des cellules et d'autres zones où les performances n'aurait normalement pas été aussi sain. [25] LTE-A, offre une mise à niveau essentielle de la technologie du LTE en étendant sa couverture, mais aussi sa latence et en augmentant son débit.

### 13.9. Intelligence Artificiel IA

Les processus d'IA créent des systèmes qui peuvent apprendre à utiliser leur expérience antérieure pour simuler des tâches humaines sans aucune intervention humaine. (Fondamentalement des systèmes intelligents !). D'autre part, l'IoT est un réseau de divers appareils connectés sur Internet et qui peuvent collecter et échanger des données entre eux. L'intelligence artificielle fait référence aux environnements électroniques sensibles et responsables de la présence des personnes.

Dans un global, monde du renseignement, les dispositifs fonctionnent de concert pour accompagner les personnes dans la réalisation de leurs actes de la vie quotidienne pratique, [26] façon naturelle d'utiliser l'information et l'intelligence cachée dans les appareils connectés au réseau. [27]

### 13.10. Réseau de capteurs sans fil RCSF

Les réseaux de capteurs sans fil RCSF : (Wireless Sensor Network, WSN) Un RCSF se compose de nombreux Nœuds de Capteurs qui ont des fonctionnalités de capturer et traiter/transmettre des données.

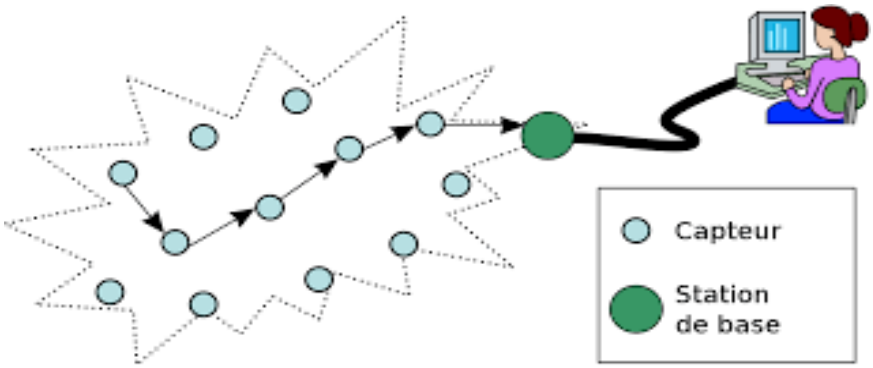



**Figure 1.12 :** Réseau de capteur sans fil.

### 13.11. Wifi

Le Wifi est un type de technologie de réseau sans fil utilisé pour se connecter à Internet. Les fréquences sur lesquelles le Wifi fonctionne sont 2.4Ghz ou 5GHz, assurant une transmission sans interférence des antennes TV, radio, téléphones portables et les radios bidirectionnelles. [28]

Le Wifi fonctionne sur de plus longues distances que le Bluetooth ou l'infrarouge, et est une technologie discrète à faible consommation d'énergie, ce qui la rend adapté aux appareils portables tels que les ordinateurs portables et les ordinateurs de poche. Cette technologie inclut tout type de produit WLAN qui prend en charge IEEE 802.11 avec double bande, 802.11a, 802.11b, 802.11g et 802.11n.


**Figure 1.13 :** La technologie Wifi dans IoT.

### 13.12. Wifi direct

Le Wifi Direct est une technologie créée par la Wifi Alliance. Elle n'est pas nouvelle mais avec la montée en puissance du "tout connecté", il est bon de savoir à quoi elle sert. Elle permet tout simplement de mettre en relation sans fil deux appareils compatibles pour effectuer du transfert de données ou du streaming.

Wifi, autorise directement deux appareils à établir une connexion directe, connexion peer-to-Wifi peer-to-peer, aucun routeur sans fil requis. Le Wifi devient une méthode de communiquer sans fil comme Bluetooth, mais avec moins de latence. [29]

Le Wifi direct est potentiellement compatible avec les Smartphones, les tablettes, les ordinateurs, les télévisions, les appareils photos, les imprimantes et bien d'autres périphériques. Il reprend la sécurité du Wifi classique et il est possible de sécuriser ses transferts avec une clé de sécurité comme sur un réseau classique.

## 14. Plateforme d'IoT

Une plateforme IoT est un logiciel qui gère la connexion et le contrôle des objets connectés dans le Cloud pour collecter, stocker, corréler, analyser et exploiter leurs données tout en assurant leur gestion. Selon la publication du rapport IoT, il y aura plus de 620 plates-formes IoT dans le monde.

Les plateformes IoT permettent de contrôler plusieurs objets et réseaux connectés. Une vue d'ensemble de cette « agrégation de données » est indispensable pour tous les services souhaitant gérer leurs objets.

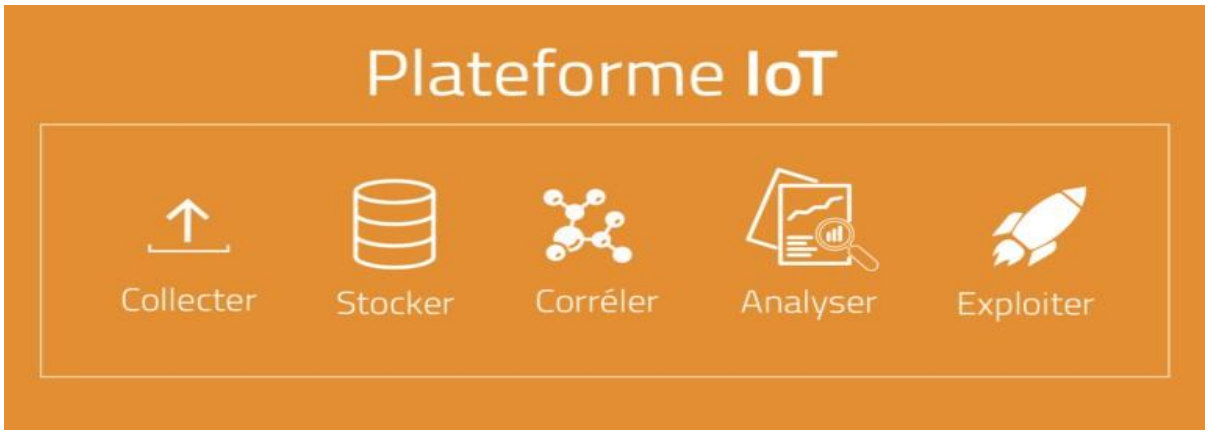



**Figure 1.14 :** Plateforme d'IoT.

On peut distinguer 5 types de plateformes IoT :

- ✓ **Plates-formes de connectivité :** Les plateformes de connectivité sont des services centrés sur les composants réseau du système IoT. Ils fournissent toutes les ressources (logiciels, matériaux, réseaux, intégrations, données, etc.) nécessaires pour garantir la fiabilité de la connexion du système ;
- ✓ **Plates-formes de gestion des objets connectés :** Les plates-formes de gestion des objets connectés sont conçues pour assurer toutes les tâches liées aux dispositifs IoT. Ils garantissent que votre groupe d'appareils connectés soit fonctionnel et sécurisé. De telles plateformes assurent le monitoring de votre appareil et vous avertissent lorsqu'une anomalie ou une panne est détectée ;

  **Plateformes Cloud :** Les plateformes Cloud exploitent le Cloud Computing pour vous fournir une infrastructure centralisée pour héberger, configurer et gérer vos systèmes IoT. Ce type de plateforme est parfait pour les entreprises qui ont besoin de flexibilité, car le système peut facilement évoluer en fonction des besoins de l'organisation et peut supporter l'intégration de millions d'objets connectés simultanément ;
- ✓ **Plateformes de bout en bout :** Ces plateformes IoT sont des solutions complètes qui offrent aux utilisateurs tout ce dont ils ont besoin pour mettre en place leur système. Ils sont préconfigurés de toutes les applications, réseaux, API et autres matériaux indispensables pour lancer un projet IoT, ce qui réduit le temps et les efforts nécessaires à la configuration et au déploiement des éléments du système ;
- ✓ **Plateformes de données :** Toutes les plateformes IoT doivent capacités d'analyse de données plus ou moins avancées. Ce qui différencie les plateformes de données des autres, c'est l'utilisation de solutions sophistiquées de traitement et d'analyse des données. Nous parlons spécifiquement de big data, d'intelligence artificielle et d'apprentissage automatique. Ce type de plate-forme est mieux adapté aux systèmes qui collectent et analysent de grandes quantités de données complexes.

## 15. Architecture de l'IoT

L'architecture d'IoT se compose de différentes couches de technologie prenant en charge l'IoT, à savoir la perception, la couche applicative, la couche métier, la couche réseau et la couche middleware. [30] Il sert à illustrer les relations entre différentes technologies et à communiquer l'évolutivité, la modularité et la configuration des déploiements IoT dans différents scénarios. La figure 1.15 représente l'architecture des couches IoT.

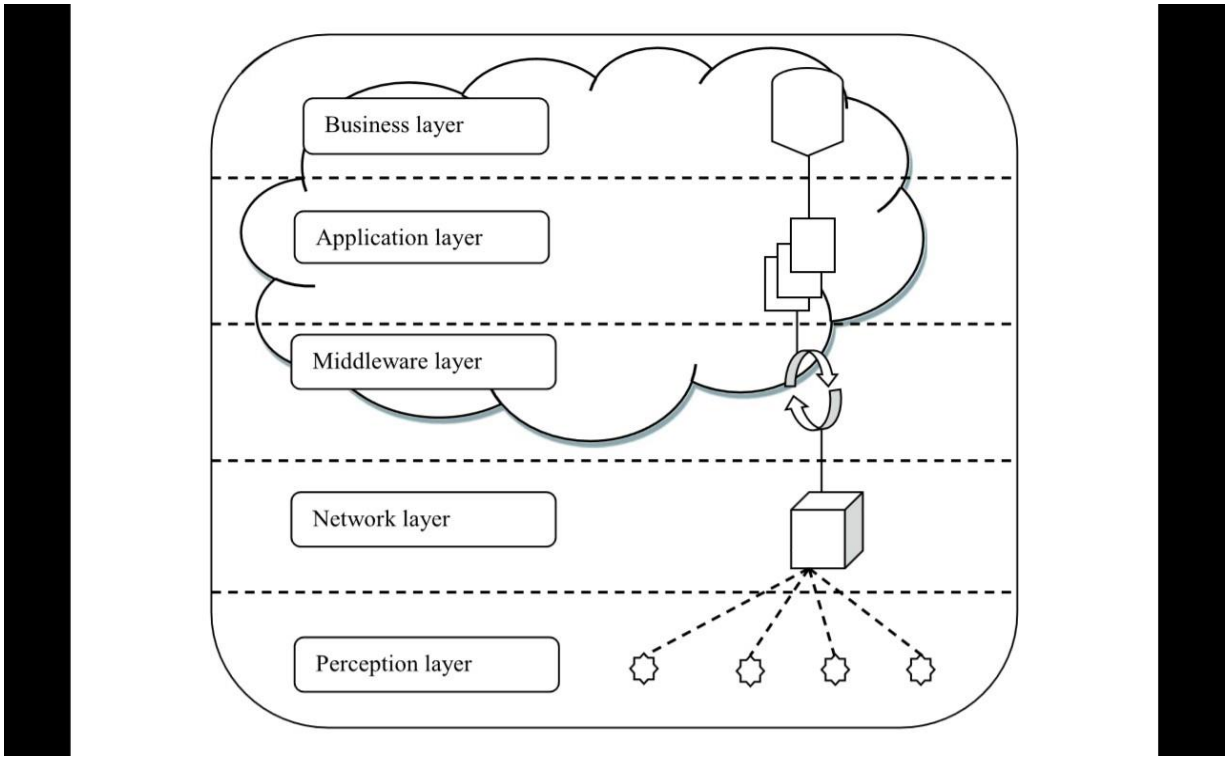



**Figure 1.15 :** l'architecture à 5 couches d'IoT. [1]

- ✓ **La couche de perception :** est la couche au niveau le plus bas du diagramme d'architecture. Il existe des capteurs et des actionneurs qui détectent et collectent des informations environnementales, de sorte que l'objectif principal de la couche de perception est de recevoir des informations du réseau environnemental. Cependant, le processus de détection et de collecte de données est effectué dans la couche de perception. De plus, des entités telles que des étiquettes RFID, des caméras, des GPS, des étiquettes à code-barres et des capteurs sont situées sur cette couche. Avec les instances, le rôle clé de cette couche est de collecter des données et de trouver des objets ou des choses dans l'environnement réseau. [1]

- ✓ **La couche réseau :** qui regroupe les informations de la couche de perception en bas. La fonction de la couche réseau est similaire à celle de la couche transport et réseau dans l'interconnexion du système ouvert (OSI). Cependant, la couche réseau est utilisée pour collecter les informations la couche la plus basse et la transmettre à Internet. Par conséquent, cette couche ne comprend que la passerelle qui a une seule interférence qui est liée au réseau de capteurs ainsi que aux autres réseaux. [1] Dans certains scénarios, la couche réseau inclut des informations centre de traitement et centre de gestion du réseau, est responsable de la connexion, du, transport et du traitement des données issues des capteurs et actionneurs.
- ✓ **La couche traitement :** La couche intermédiaire reçoit les informations de la couche réseau. Cependant, le l'objectif principal de la couche middleware est de stocker les données et d'exécuter des processus de gestion des services. De plus, la couche middleware effectue le traitement du système d'information et prend automatiquement des décisions en fonction des résultats. La couche middleware génère la sortie et la transmet à la couche suivante appelée couche application. [1] A des fonctions avancées telles que le stockage, le calcul, le traitement et les capacités de prise d'action. Il stocke tous les ensembles de données et, en fonction de l'adresse et du nom de l'appareil, fournit à l'appareil les données appropriées.
- ✓ **La couche d'application :** est utilisée pour effectuer l'arrangement final des informations. Cette couche reçoit des données de la couche middleware précédente et fournit une application de gestion globale qui restitue les données en fonction des données passant par la couche middleware. Cependant, la couche d'application définit les informations sur l'intelligence domestique, le suivi intelligent des véhicules, la santé intelligente, l'intelligence agricole, la transformation intelligente et les villes intelligentes. [1]
- ✓ **La couche business :** Dans la couche métier, les données reçues de la couche application précédente sont transformées en informations significatives, qui sont ensuite générés à partir des données existantes dans d'autres services de haut niveau. De plus, les données sont traitées sous forme de connaissances, ce qui rend les données plus efficaces et peut être utilisée par les prestataires de service pour gagner de l'argent.

L'IoT fonctionne sur la base d'une communication machine-à-machine (M2M), Donc M2M signifie une communication qui se produit entre deux machines différentes sans aucune intervention humaine. Par conséquence, dans l'IoT réseau, les unités non connectées deviennent l'art de l'IoT à travers la transmission de données périphérique, tel que les étiquettes RFID et les codes à barre, et se connectent enfin à Internet. Cependant, les objets non intelligents appelés choses deviennent des nœuds de communicants dans la terminologie IoT. [1] Le succès de tout appareil est déterminé non seulement par la technologie utilisée, mais aussi par la manière dont il est livré aux consommateurs. La gestion exécute ces tâches pour l'appareil. Cela implique la création d'organigrammes, de diagrammes, l'analyse des résultats, etcomment amélioré l'équipement, etc.

## 16. Infrastructures pour l'IoT

L'infrastructure est un ensemble d'éléments, d'ouvrages ou d'installations interdépendants qui supportent en partie ou en totalité une structure ou un réseau. Le terme est souvent utilisé d'une façon très abstraite. Par exemple, les outils d'ingénierie informatique sont quelquefois décrits comme une partie de l'infrastructure d'un environnement de développement, et le terme capital d'infrastructure en économie peut être trop large, comme il inclut l'habillement jusqu'au système de canaux qui s'étend sur un continent. Il faut aussi pondérer avec la notion de robustesse dans un environnement fluide.

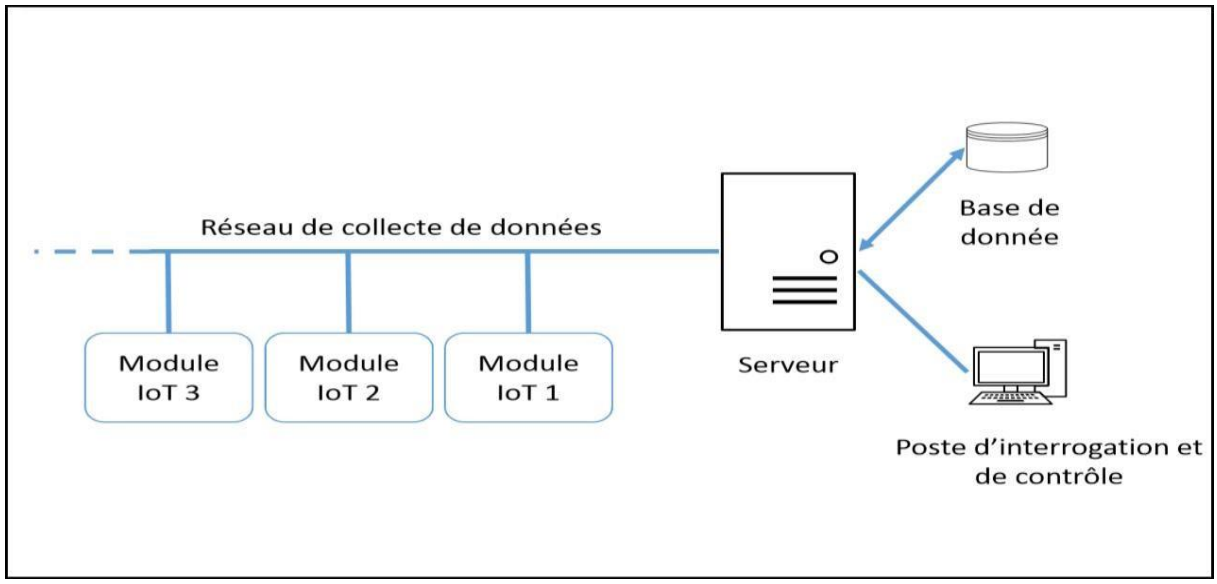



**Figure 1.16 :** Infrastructure élémentaire. [31]

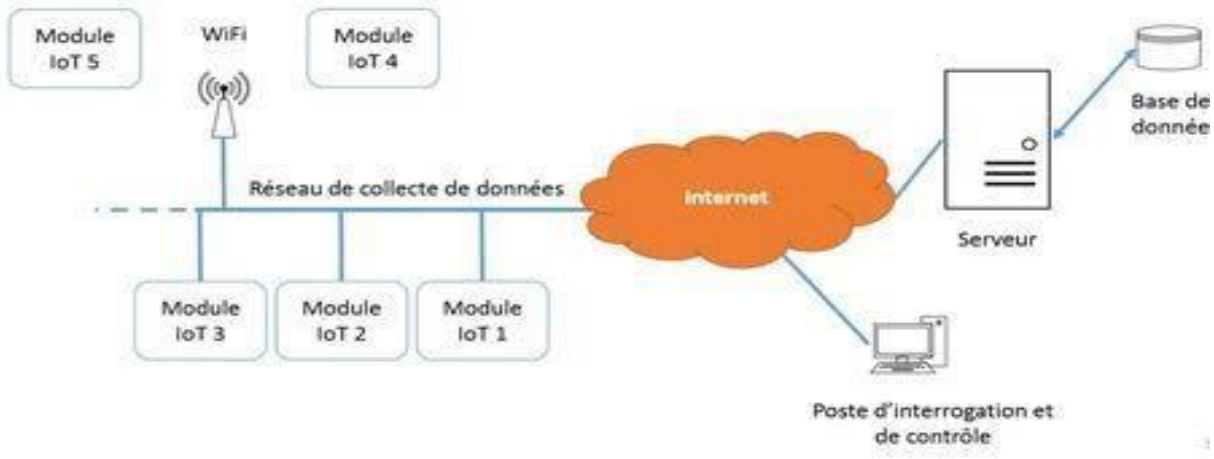



**Figure 1.17 :** Exploitation du réseau internet. [31]

## 17. Défait d'IoT

Cependant, plusieurs obstacles peuvent ralentir les progrès de l'IoT, notamment le déploiement du protocole IPv6, l'alimentation des capteurs et la définition de normes. [7]

- **Déploiement du protocole IPv6 :** Nous avons atteint le nombre maximum d'adresses IPv4 en février 2010. Si cela n'a pas d'impact notable sur le public, le développement de l'IoT pourrait ralentir, car chaque milliard de nouveaux capteurs potentiels devront avoir leur propre adresse IP. De plus, le protocole IPv6 facilite la gestion du réseau grâce à la configuration automatique et offre des fonctions de sécurité améliorées.
- **Alimenter les capteurs :** pour que l'IoT atteigne son plein potentiel, les capteurs doivent pouvoir être autonomes. Imaginez devoir remplacer les batteries de milliards d'appareils déployés dans le monde et même dans l'espace. Évidemment, ce n'est pas possible. Par conséquent, nous devons trouver un moyen de générer de l'électricité en exploitant l'environnement, comme les vibrations, la lumière et le flux d'air.
- **Normes :** l'espace des normes a parcouru un long chemin, mais il reste encore beaucoup à faire, en particulier dans les domaines de la sécurité, de la confidentialité, de l'architecture et des communications. Tout comme l'IEEE, de nombreuses organisations s'efforcent de relever ces défis en veillant à ce que les paquets IPv6 puissent être acheminés via différents types de réseaux.

## 18. Amélioration de la résilience, la sécurité et l'assurance de l'IoT

Alors que nous nous appuyons de plus en plus sur les nouveaux services créés par l'IoT, sa résilience face aux défaillances partielles de l'infrastructure ou aux défaillances des sous-systèmes devient critique.

Les déploiements IoT impliquent des architectures de systèmes distribués de plus en plus complexes, La résilience « by design » est un enjeu majeur. Le degré de fiabilité est également important en matière de sécurité et de sécurité IoT.

Jusqu'à présent, le cyber sécurité a été considéré comme relevant principalement du cyberespace : protection des informations numériques, respect de la « nétiquette » (bonnes pratiques d'utilisation d'Internet), etc. Avec l'IoT, le cyber sécurité va au-delà de l'espace virtuel vers l'espace physique : il s'agit désormais de garantir son intégrité physique et de protéger son environnement dans le monde réel.

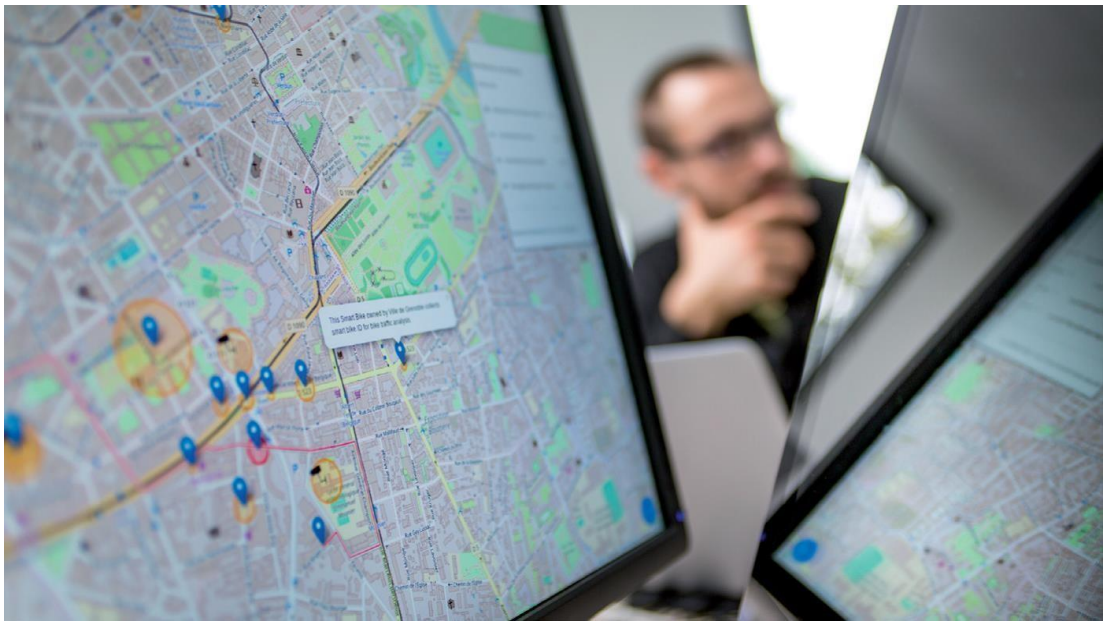


**Figure 1.18 :** Map of Things : collecte des données et information des usagers d'objets connectés.

À quels nouveaux risques sommes-nous confrontés en matière de sécurité IoT ? Quels sont lesavantages ? Un simple "gadget" IoT peut ne pas valoir les risques qui l'accompagnent.

De nouveaux modèles doivent être développés pour comprendre qui est les attaquants potentiels et les problèmes de sécurité dans les environnements IoT complexes.

À partir de ces modèles, nous pouvons ensuite développer de nouveaux mécanismes d'assurance pour les logiciels, le matériel et les communications des appareils IoT, prolongeant l'ensemble du cycle de vie à des décennies. Un nouveau maillon faible dans ce milieu.

## 19. Conclusion

Ce chapitre vise à décrire les concepts fondamentaux de l'IoT et comment son impact sur lavie quotidienne humaine crée beaucoup de confort et de dépendance à une plus grande automatisation des processus.

L'Internet of Things est une nouvelle révolution de l'Internet. En raison de ses domaines d'application diversifiés et des combinaisons hétérogènes de diverses communications et technologies embarquées dans son architecture, c'est un sujet de recherche clé pour leschercheurs dans le domaine des sciences de l'information et des technologies de l'informatiqueembarquée.

L'IoT est un sujet de grand intérêt et d'excitation, en grande partie justifié. À l'heure actuelle,le grand monde d'Internet compte régulièrement 2,9 billions d'octets de sources de données chaque jour. Selon les statistiques, la proportion de données au cours des deux dernières années est de 92%. L'Internet des objets (IoT) promet d'avoir un impact majeur en ajoutant de nouvelles dimensions à la façon dont les gens interagissent avec les choses qui les entourent.

L'Internet of Things se développe de jour en jour et la standardisation des modèles d'interconnexion pour les réseaux avec du matériel et des appareils hétérogènes est l'avenir de l'IoT.

# Chapitre 02 :
# La sécurité dans Internet of Things

# 1. Introduction

La sécurité est un enjeu majeur des technologies numériques modernes. L'infrastructure de télécommunication, les réseaux sans fils (Bluetooth, Wifi, WiMax), l'Internet, les systèmes d'informations, les routeurs, les systèmes d'exploitation et les applications informatiques, toutes ces entités présentent des vulnérabilités : faille de sécurité, défaut de conception ou de configuration.

L'Internet des objets (IoT) est une technologie adoptée à l'échelle mondiale Système de réseau automatisé. La croissance rapide de l'Internet des objets (IoT) a introduit des milliards d'appareils compatibles Internet dans notre vie quotidienne, les rendant plus intelligents en comblant le fossé entre les mondes physique et virtuel. Par conséquent, une partie de l'adoption de l'IoT consiste à anticiper ce que la technologie apporte d'autre aux environnements auxquels elle est appliquée, notamment les problèmes de sécurité qui peuvent donner lieu à des attaques réussies contre les systèmes et appareils IoT.

Dans ce chapitre, nous présentons la sécurité de l'Internet des Objets, la détection d'intrusions, et les attaques.

Dans les systèmes IoT, les protocoles utilisés peuvent présenter des failles de sécurité [32] Peut avoir des effets à l'échelle du système. Les appareils IoT sont cibles vulnérables pour les cybercriminels et les attaquants car Ils manquent de protocoles de sécurité de base. Ça signifie Ils peuvent être piratés et attaqués par des botnets qui utilisent lancer une attaque DDoS contre une organisation. [33]

# 2. La sécurité dans l'Internet of Things

## 2.1. Définition de la sécurité informatique

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire les vulnérabilités d'un système contre les menaces accidentelles ou intentionnelles. [61] Ces systèmes informatiques et leurs réseaux d'interconnexion sont également la proie de vandales, des égoïstes malveillants, des terroristes et un éventail d'individus. Outre ces attaques intentionnelles sur les systèmes informatiques, il existe d'innombrables façons dont les erreurs involontaires peuvent endommager ou détruire la capacité d'un système à s'acquitter de ses fonctions prévues.

## 2 .2. La sécurité d'IoT

La sécurité IoT est le domaine de la technologie qui implique la sécurisation des appareils connectés et des réseaux dans l'Internet des objets (IoT).

L'Internet des objets est l'ajout de la connectivité Internet à des systèmes d'appareils informatiques interconnectés, de machines mécaniques et numériques, d'objets, d'animaux et/ou de personnes. Chaque "chose" a un identifiant unique et est capable de transmettre automatiquement des données sur le réseau. Autoriser les appareils à se connecter à Internet les expose à de nombreuses vulnérabilités graves s'ils ne sont pas correctement sécurisés.

La sécurité de l'IoT a fait l'objet d'un examen minutieux à la suite de plusieurs incidents très médiatisés liés à l'utilisation d'appareils IoT courants pour infiltrer et attaquer les réseaux les plus critiques. La mise en œuvre de mesures de sécurité est essentielle pour garantir la sécurité du réseau auquel les appareils IoT sont connectés.

L'examen minutieux de la sécurité IoT a considérablement augmenté en raison de l'augmentation des applications et des services IoT. La sécurité rend la vie d'un pirate plus difficile car elle protège le système contre le piratage. La sécurité réduit la probabilité que les collations soient gâtées ou réduit les risques pour la sécurité.

L'objectif de la sécurité IoT n'est pas seulement de protéger les actifs, mais également de garantir la confidentialité des communications, la disponibilité des données et l'intégrité dans l'écosystème IoT. Par conséquent, la sécurité de l'IoT a récemment suscité l'intérêt des chercheurs, utilisant des simulateurs, des simulateurs et analysant les plates-formes disponibles pour étudier les vulnérabilités, [34] les défenses, [35] les attaques [36] et les atténuations. [37]

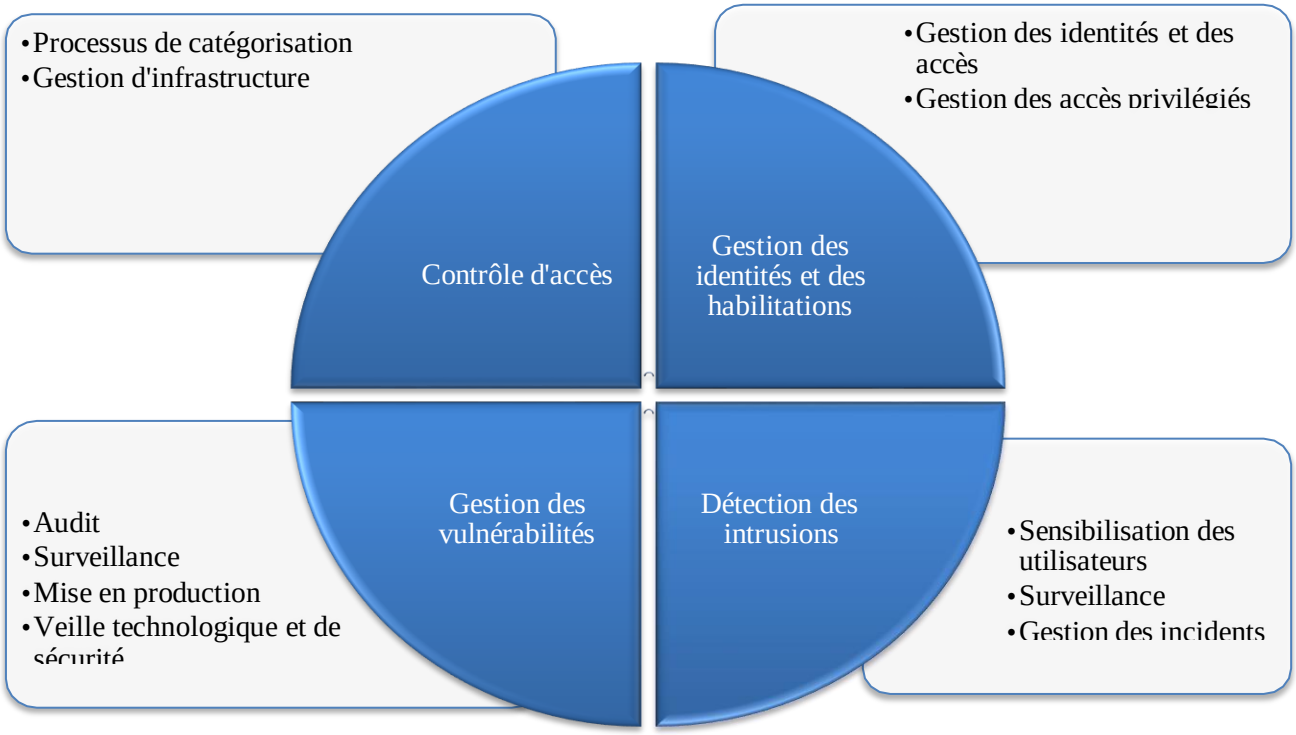



**Figure 2.1 :** Processus de sécurité.

La figure ci-dessous montre les 4 catégories d'examen de la sécurité IoT, à savoir l'attaque, la vulnérabilité, la défense et l'atténuation. Les attaques et les vulnérabilités sont interdépendantes ; par conséquent, des recherches sont nécessaires pour effectuer des tests d'intrusion ou des tests d'éthique afin d'identifier les vulnérabilités possibles.

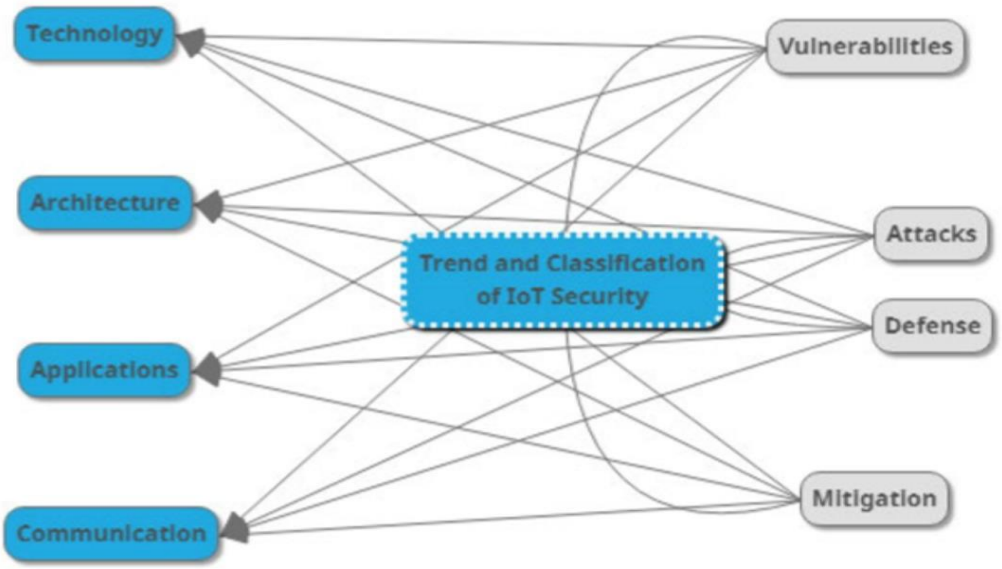



**Figure 2.2 :** Classification des revues de sécurité IoT.

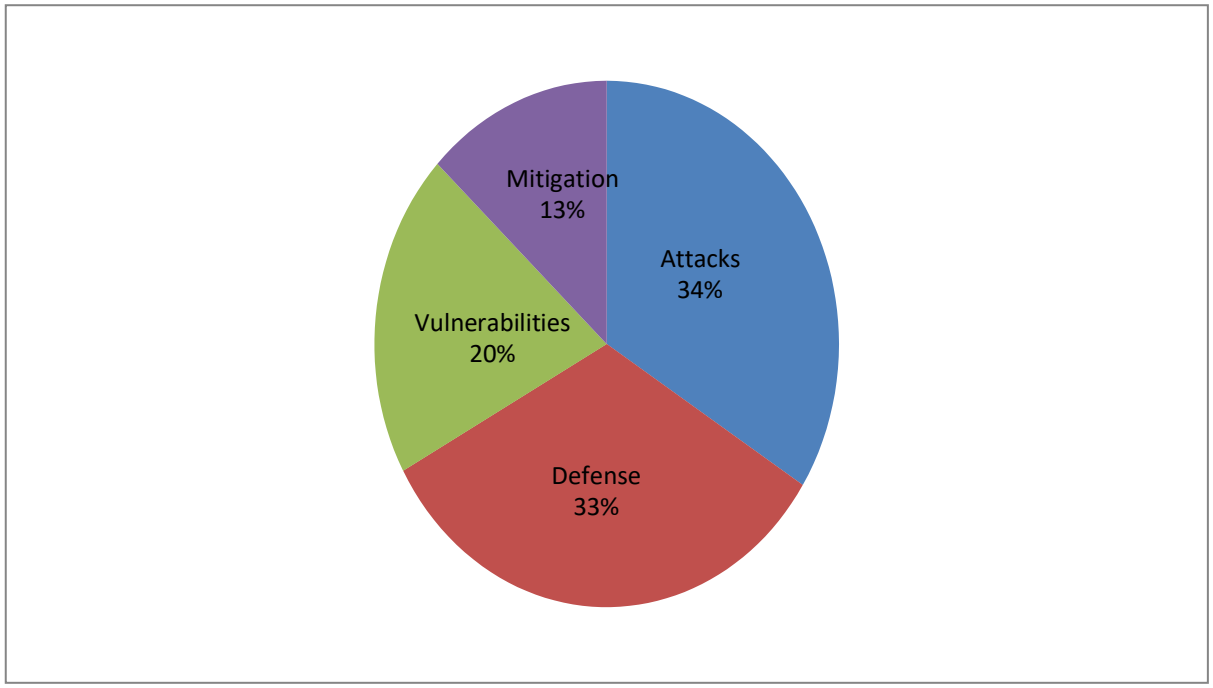



**Figure 2.3 :** Tendance des revues de sécurité IoT. [15]

La sécurité de l'IoT doit tenir compte des caractéristiques dynamiques, hétérogènes et interopérables de l'IoT. Les recherches futures devraient également envisager des communications légères ou des réseaux légers centrés sur l'information avec des réseaux de communication spécifiques centrés sur les données, ainsi capables de minimiser les menaces et les attaques de réseau ou de communication.

## 2.3. Échecs de sécurité IoT

- L'économie favorise une sécurité faible ;
- La sécurité est difficile, surtout pour les nouvelles entreprises ;
- Les systèmes IoT sont complexes et chaque partie doit être sécurisée ;
- Le support de sécurité n'est pas toujours maintenu ;
- Sensibilisation insuffisante des consommateurs à la sécurité IoT : les consommateurs ont une connaissance limitée de la sécurité IoT, ce qui peut affecter leur capacité à l'intégrer dans leurs habitudes d'achat ou à configurer et maintenir la sécurité dans leurs systèmes IoT;

- Les utilisateurs peuvent avoir des difficultés à détecter ou à résoudre les incidents de sécurité : dans de nombreux cas, l'impact d'un produit ou d'un service mal sécurisé n'est pas apparent pour les utilisateurs. Par exemple, un réfrigérateur peut continuer à bien faire son travail même s'il a été compromis et fait partie d'un botnet effectuant une attaque DDoS ;
- Les mécanismes de responsabilité légale existants peuvent ne pas être clairs.

## 2.4. Les étapes de la sécurité de l'IoT

- **Secure Boot** : Garantit que seules les mises à jour logicielles authentifiées et signées par le fabricant sont autorisées**,** Cibler Secure Boot aurait empêché l'accès au réseau deTarget via les sociétés HVAC fournisseur, où le voleur a pu installer un logiciel malveillant qui a accédé à des données précieuses ;
- **Authentification :** Authentification des données et gestion de l'identité des appareils, Mirai a éliminé Amazon, Spotify et Twitter dans une attaque DDOS ;
- **Ports protégés :** Renforcez et contrôlez l'accès aux ports d'E/S pour empêcher les intrusions locales. Les attaquants ayant un accès physique à votre appareil signifient que ce n'est plus votre appareil ;
- **Stockage sécurisé** : Chiffrement des données au niveau du système de fichiers pour le stockage des informations sensibles. Des pirates ont volé 100 millions d'euros à la banque centrale du Bangladesh en pénétrant dans le stockage flash non sécurisé de **SWIFT**.
- **Connexions sécurisées :** Les protocoles de cryptage pour les données en mouvement et en direct (OTA) garantissent l'intégrité des données, en envoyant des messages sans fil soigneusement conçus sur le réseau interne du véhicule, les chercheurs en sécurité ont pu pirater une Jeep en mouvement. Oui.

## 3. Les attaques

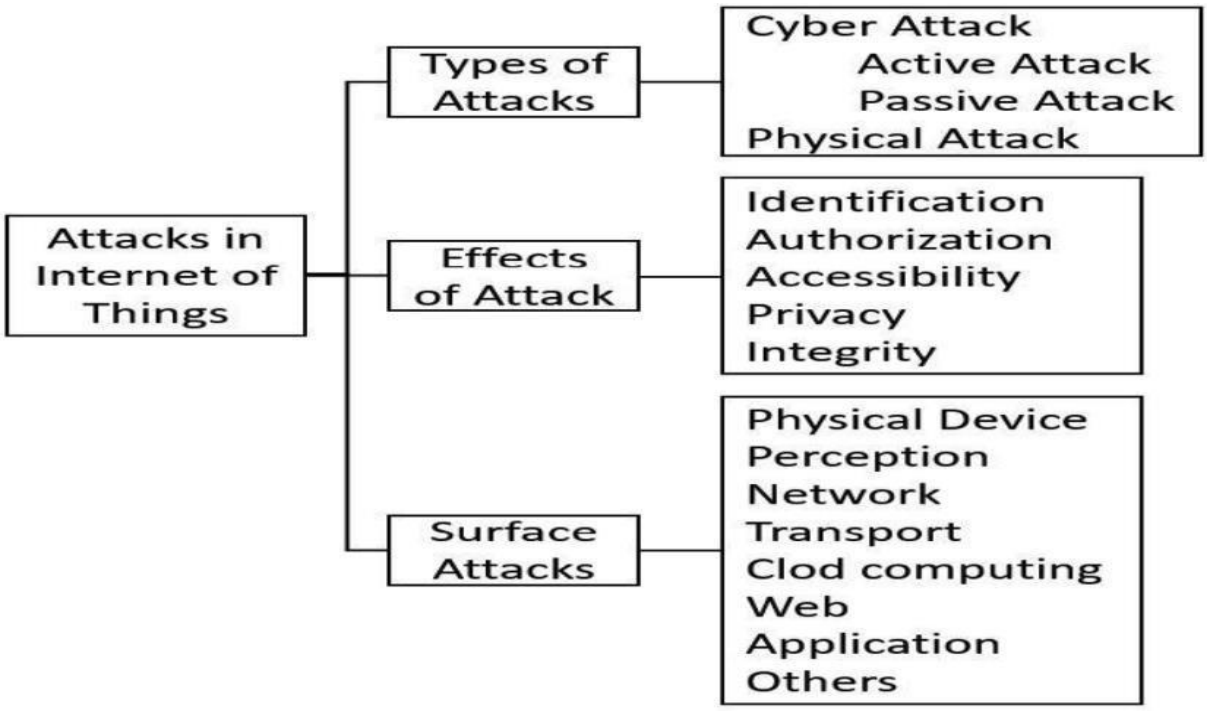



**Figure 2.4 :** Catégories d'attaques dans l'internet des objets. [57]

### 3.1. Les surfaces d'attaque de l'IoT

Dans le cadre de son projet Internet des objets, l'Open Web Application Security Project (OWASP) a publié une ébauche de liste détaillée des zones de surface d'attaque IoT, ou des zones des systèmes et applications IoT où des menaces et des vulnérabilités peuvent exister. Vous trouverez ci-dessous un résumé des zones de surface d'attaque IoT :

- **Dispositifs**. Les appareils peuvent être le principal moyen par lequel les attaques sont lancées. Les parties d'un appareil dont les vulnérabilités peuvent provenir sont sa mémoire, son micro logiciel, son interface physique, son interface Web et ses services réseau. Les attaquants peuvent également profiter de paramètres par défaut non sécurisés, de composants obsolètes et de mécanismes de mise à jour non sécurisés, entre autres ;
- **Canaux de communication.** Les attaques peuvent provenir des canaux qui connectent les composants IoT entre eux. Les protocoles utilisés dans les systèmes IoT peuvent avoir des problèmes de sécurité qui peuvent affecter l'ensemble des systèmes. Les systèmes IoT sont également sensibles aux attaques de réseau connues telles que le déni de service (DoS) et l'usurpation d'identité ;

- **Applications et logiciels.** Les vulnérabilités des applications Web et des logiciels associés pour les appareils IoT peuvent compromettre les systèmes. Les applications Web peuvent, par exemple, être exploitées pour voler les informations d'identification des utilisateurs ou pousser des mises à jour de micro logiciel malveillant.

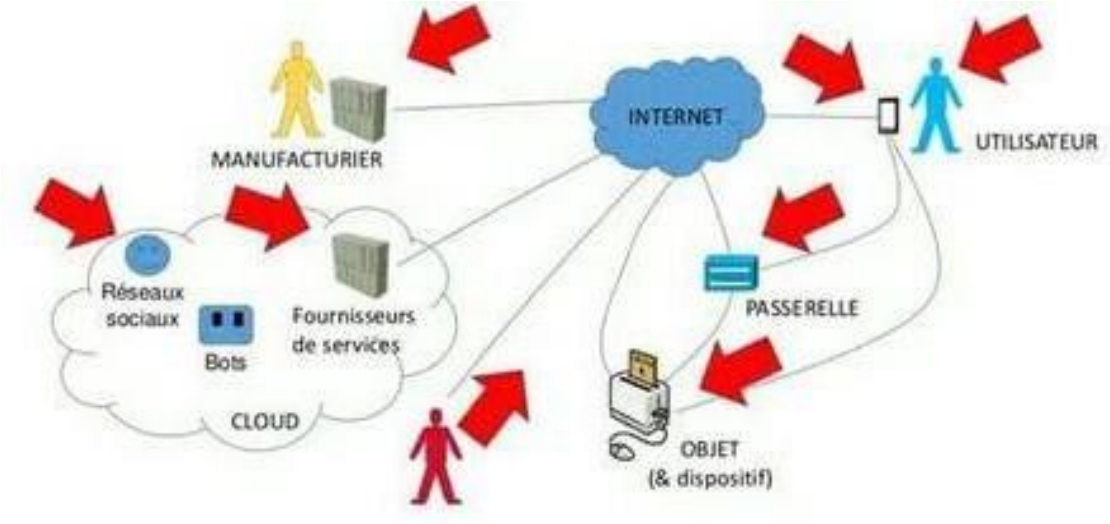



**Figure 2.5 :** Les surfaces d'attaque.

## 3.2. Les types d'attaques

Un cyber attaque est tout type d'action offensive contre un système, une infrastructure ou un réseau informatique, voire un ordinateur personnel, utilisant diverses méthodes pour voler, modifier ou détruire des données ou des systèmes informatiques.

Aujourd'hui, nous allons décrire les 10 types de cyber attaques les plus courants : [38]

1) **Attaques par déni de service (DoS) et par déni de service distribué (DDoS) :** Les attaques par déni de service submergent les ressources du système, ce qui rend le système incapable de répondre aux demandes de service. Les attaques DDoS ciblent également les ressources système, mais sont lancées par de nombreux autres hôtes infectés par des logiciels malveillants contrôlés par l'attaquant.
2) **Attaque de l'homme au milieu (MitM) :** Une attaque de l'homme du milieu est un pirate qui s'insère dans les communications entre un client et un serveur.
3) **Attaque d'hameçonnage et de harponnage :** l'hameçonnage est l'envoi d'e-mails qui semblent provenir d'une source fiable dans le but d'obtenir des informations personnelles ou d'inciter un utilisateur à faire quelque chose. Cette technique combine ingénierie sociale et stratégies techniques.

Il peut s'agir d'une pièce jointe à un e-mail qui charge des logiciels malveillants sur votre ordinateur. Il peut également utiliser des liens vers des sites Web illégaux pour vous inciter à télécharger des logiciels malveillants ou à transmettre vos informations personnelles.

4) **Attaque par téléchargement** : les attaques par téléchargement furtif sont une méthode courante de propagation des logiciels malveillants. Les pirates trouvent des sites Web dangereux et insèrent des scripts malveillants dans le code HTTP ou PHP de l'une des pages. Ce script peut installer des logiciels malveillants directement sur les ordinateurs des visiteurs du site ou rediriger les visiteurs vers des sites contrôlés par des pirates. Des téléchargements furtifs peuvent se produire lors de la visite de sites Web ou de la visualisation d'e-mails ou de fenêtres contextuelles.
5) **Attaque par mot de passe :** étant donné que les mots de passe sont le mécanisme le plus couramment utilisé pour authentifier les utilisateurs de systèmes informatiques, l'obtention de mots de passe est une méthode d'attaque courante et efficace.
6) **Attaque par injection SQL :** L'injection SQL est devenue un problème courant affectant les sites Web exploitant des bases de données. Cela se produit lorsque les criminels exécutent des requêtes SQL sur la base de données avec des données entrantes du client vers le serveur.
7) **Attaque XSS (Cross-site Scripting) :** Les attaques XSS utilisent des ressources réseau tierces pour exécuter des scripts dans le navigateur Web ou l'application inscriptible de la victime.
8) **Attaque d'écoute clandestine :** l'écoute clandestine est le résultat de l'interception du trafic réseau. Ils permettent aux attaquants d'obtenir des mots de passe, des numérosde carte de crédit et d'autres informations confidentielles que les utilisateurs envoient sur le réseau.
9) **Attaque d'anniversaire :** Les attaques d'anniversaire sont lancées contre des algorithmes de hachage qui vérifient l'intégrité des messages, des logiciels ou des signatures numériques. Une attaque d'anniversaire fait référence à la probabilité de trouver deux messages aléatoires qui génèrent le même résumé lorsqu'ils sont traités par une fonction de hachage.
10) **Attaque par des logiciels malveillants :** Un logiciel malveillant peut être décrit comme un logiciel indésirable installé dans votre système sans votre consentement. Il peut s'attacher à un code légitime et se propager, se cacher dans des applications utiles ou se reproduire sur Internet.

### 3.3. Les attaques Dos et DDoS

Une attaque par déni de service (abréviation. DoS attack pour Denial of Service attack en anglais) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. À l'heure actuelle la grande majorité de ces attaques se font à partir de plusieurs sources, on parle alors d'attaque par déni de service distribuée (abréviation. DDoS attack pour Distributed Denial of Service attack). Une attaque DDoS est une arme de cyber sécurité visant à perturber le fonctionnement des services ou à extorquer de l'argent aux organisations ciblées. Ces attaques peuvent être motivées par la politique, la religion, la concurrence ou le profit. [67]

On appelle « attaque par déni de service » toutes les actions ayant pour résultat la mise hors ligne d'un serveur. Techniquement, couper la connexion entre un serveur et un client, dans un but malfaisant, peut être considéré comme une attaque par déni de service. Dans les faits, les attaques par déni de service sont opérées en saturant la bande passante d'un serveur défini.

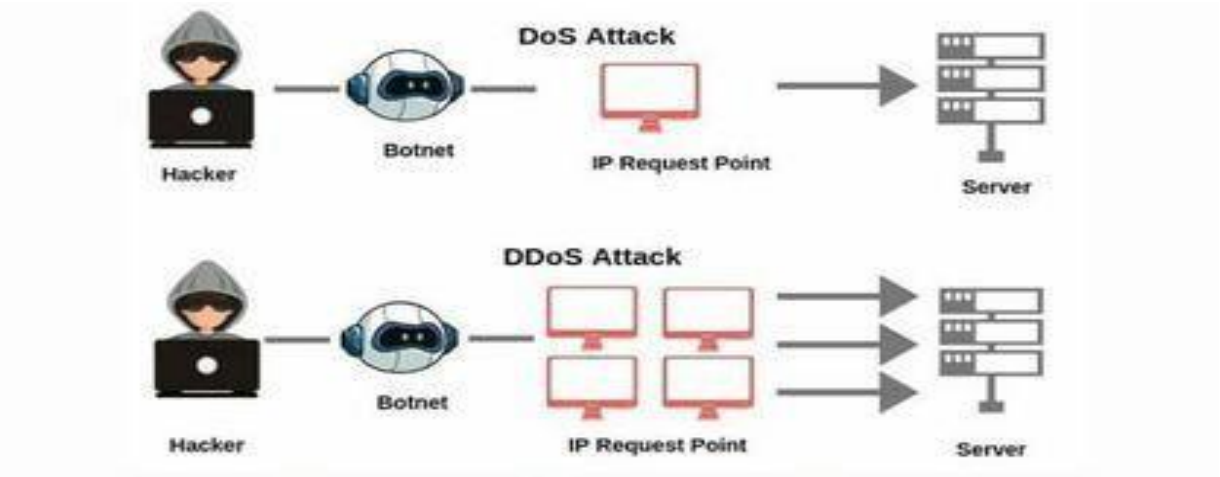



**Figure 2.6 :** Représentation des attaques DoS et DDoS.

Les attaques DoS empêchent les utilisateurs ciblés d'accéder à un ordinateur ou à un réseau. Les pirates utilisent activement les attaques Dos pour perturber le fonctionnement normal des systèmes informatiques. Une approche distribuée est l'un des moyens les plus efficaces de mettre fin à une approche. Il existe différentes attaques DoS. Les attaques volumétriques reposent sur l'inondation du réseau avec des demandes d'écho pour utiliser toute sa capacité de bande passante. Une attaque Syn Flood est similaire à une attaque Flood en ce sens qu'elle inonde le réseau avec un flot de requêtes ; cependant, l'attaquant crée rapidement un lien vers le service sans le terminer.

Les attaques par fragmentation visent à empêcher la capacité du réseau cible à se réorganiser. Les attaques de la couche application ciblent les failles de programmation cachées dans une application ou un réseau en inondant la cible de requêtes. Enfin, les attaques de phlashing DoS envoient de fausses demandes de mise à jour et injectent des logiciels malveillants sur le réseau cible, ce qui fait que les attaques distribuées sont les attaques les plus courantes. Les pirates infectent le réseau des appareils liés avec des logiciels malveillants et commencent à les inonder de demandes pour inonder le réseau.

En raison de leur popularité croissante, les échanges de crypto-monnaie sont souvent la cible d'attaques DDoS. Plusieurs attaques DDoS ont été tentées par certains grands échanges de crypto-monnaie depuis 2020. Les botnets sont des réseaux constitués de millions de systèmes infectés par des logiciels malveillants et contrôlés par des pirates informatiques afin d'effectuer des attaques DDoS. Ces bots ou systèmes zombies sont utilisés pour effectuer des attaques contre les systèmes cibles, souvent en submergeant leur bande passante et leurs capacités de traitement. Ces attaques DDoS sont difficiles à tracer, car les botnets sont disséminés dans des lieux géographiques différents. Les botnets peuvent être atténués par : [38]

- **le filtrage RFC3704**, qui bloque le trafic provenant d'adresses usurpées et contribue à assurer la traçabilité du trafic vers son véritable réseau source. Le filtrage RFC3704 supprime par exemple les paquets provenant d'adresses figurant sur la liste Bogon ;
- **Le filtrage par trous noirs**, qui élimine le trafic indésirable avant qu'il n'entre dans un réseau protégé. Lorsqu'une attaque DDoS est détectée, l'hôte BGP (Border Gateway Protocol) doit envoyer des mises à jour de routage aux routeurs des FAI, afin qu'ils acheminent tout le trafic à destination des serveurs victimes vers une interface null0 lors du saut suivant.

Avec l'utilisation croissante de la technologie blockchain, un nouveau type d'attaque DoS, l'attaque blockchain DoS, a émergé. Ces attaques ciblent les blockchains qui utilisent le processus de consensus PoW. Cette nouvelle attaque DoS cible le système de récompense des mineurs. La méthode de consensus PoW repose sur les mineurs pour valider les nouveaux blocs, et la validation des blocs s'arrête si les mineurs ne sont pas payés. Une attaque DoS réussie sur un réseau décentralisé est plus difficile. Contrairement aux réseaux traditionnels, les attaques DoS reposent sur la nature centralisée du réseau, ce qui n'est pas le cas des réseaux basés sur la blockchain. Les attaquants envoient de fausses preuves à la blockchain revendiquant un avantage minier afin de perturber le processus minier. Cela empêche les autres mineurs d'effectuer des tâches de vérification

ce qui ralentit la puissance de traitement de la blockchain. Pourtant, jusqu'à présent, les attaques DDoS ont été extrêmement rares et infructueuses.

### 3.4. Différence entre les attaques DoS et DDoS

La principale différence entre DoS et DDoS est que le premier est une attaque système à système, tandis que le second implique plusieurs systèmes attaquant un seul système. Cependant, il existe d'autres différences, impliquant leur nature ou leur détection, notamment : [59]

- **Facilité de détection/atténuation :** étant donné que le DoS provient d'un seul endroit, il est plus facile de détecter son origine et de rompre la connexion. En fait, un pare-feu compétent peut le faire. D'autre part, une attaque DDoS provient de plusieurs emplacements distants, déguisant son origine.
- **Vitesse d'attaque :** étant donné qu'une attaque DDoS provient de plusieursemplacements, elle peut être déployée beaucoup plus rapidement qu'une attaque DoS provenant d'un seul emplacement. L'augmentation de la vitesse d'attaque rend sadétection plus difficile, ce qui signifie une augmentation des dégâts ou même un résultat catastrophique.
- **Volume de trafic :** une attaque DDoS utilise plusieurs machines distantes (zombies ou bots), ce qui signifie qu'elle peut envoyer des quantités de trafic beaucoup plus importantes à partir de différents emplacements simultanément, surchargeant rapidement un serveur d'une manière qui échappe à la détection.
- Mode d'exécution : une attaque DDoS coordonne plusieurs hôtes infectés par des logiciels malveillants (bots), créant un botnet géré par un serveur de commande et de contrôle (C&C). En revanche, une attaque DoS utilise généralement un script ou un outil pour mener l'attaque à partir d'une seule machine.
- Traçage de la ou des sources : l'utilisation d'un botnet dans une attaque DDoS signifie que le traçage de l'origine réelle est beaucoup plus compliqué que le traçage de l'origine d'une attaque DoS.

### 3.5. Types d'attaques DoS et DDoS

Les attaques DoS et DDoS peuvent prendre de nombreuses formes et être utilisées pour divers moyens. Il peut s'agir de faire perdre des affaires à une entreprise, de paralyser un concurrent, de détourner l'attention d'autres attaques ou simplement de causer des problèmes ou de faire une déclaration. Voici quelques formes courantes prises par de telles attaques. [59]

**1. Attaque en larme**

Une attaque en forme de larme est une attaque DoS qui envoie d'innombrables fragments de données IP (Internet Protocol) à un réseau. Lorsque le réseau essaie de recompiler les fragments dans leurs paquets d'origine, il n'y parvient pas.

Par exemple, l'attaquant peut prendre de très gros paquets de données et les décomposer en plusieurs fragments pour que le système ciblé les réassemble. Cependant, l'attaquant modifie la façon dont le paquet est désassemblé pour confondre le système ciblé, qui est alors incapable de réassembler les fragments dans les paquets d'origine.

**2. Inondation Attaque**

Une attaque par inondation est une attaque DoS qui envoie plusieurs demandes de connexion à un serveur mais ne répond pas pour terminer la poignée de main.

Par exemple, l'attaquant peut envoyer diverses demandes pour se connecter en tant que client, mais lorsque le serveur tente de communiquer en retour pour vérifier la connexion, l'attaquant refuse de répondre. Après avoir répété le processus un nombre incalculable de fois, le serveur devient tellement inondé de demandes en attente que les vrais clients ne peuvent pas se connecter, et le serveur devient "occupé" ou même plante.

**3. Attaque de fragmentation IP**

Une attaque par fragmentation IP est un type d'attaque DoS qui délivre des paquets réseau modifiés que le réseau récepteur ne peut pas réassembler. Le réseau s'enlise avec des paquets volumineux non assemblés, épuisant toutes ses ressources.

**4. Attaque volumétrique**

Une attaque volumétrique est un type d'attaque DDoS utilisée pour cibler les ressources de bande passante.

Par exemple, l'attaquant utilise un botnet pour envoyer un volume élevé de paquets de requêtes à un réseau, submergeant sa bande passante avec des requêtes d'écho ICMP (Internet Control Message Protocol). Cela entraîne un ralentissement ou même une interruption complète des services.

**5. Attaque de protocole**

Une attaque de protocole est un type d'attaque DDoS qui exploite les faiblesses des couches 3 et 4 du modèle OSI.

Par exemple, l'attaquant peut exploiter la séquence de connexion TCP, envoyer des requêtes mais ne pas répondre comme prévu ou répondre avec une autre requête en utilisant une adresse IP source usurpée. Les requêtes sans réponse épuisent les ressources du réseau jusqu'àce qu'il devienne indisponible.

### 6. Attaque basée sur les applications

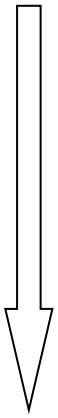
Une attaque basée sur les applications est un type d'attaque DDoS qui cible la couche 7 du modèle OSI.

Un exemple est une attaque Slow loris, dans laquelle l'attaquant envoie des requêtes HTTP (HyperText Transfer Protocol) partielles mais ne les termine pas. Des en-têtes HTTP sont périodiquement envoyés pour chaque demande, ce qui entraîne une immobilisation des ressources réseau. L'attaquant continue l'assaut jusqu'à ce qu'aucune nouvelle connexion ne puisse être établie par le serveur.

Ce type d'attaque est très difficile à détecter car plutôt que d'envoyer des paquets corrompus, il en envoie des partiels et utilise peu ou pas de bande passante.

Le tableau, ci-dessous, qui représente le modèle OSI. Ceux qui ont pris des cours d'informatique, et qui ont une bonne mémoire, savent de quoi je parle. La couche 7 du modèle OSI c'est la couche Application. Les couches 3 et 4, donc Réseau et Transport, sont utilisées pour effectuer des attaques DDoS traditionnelles. Ces dernières sont les plus populaires.

| | **Protocol Data Unit (PDU)** | **Couche** | |
|---|---|---|---|
| **Couches Hautes** | Donnée | 7 | Application |
| | | 6 | Présentation |
| | | 5 | Session |
| | Segments / Datagramme | 4 | Transport |
| **Couches Matérielles** | Paquet | 3 | Réseau |
| | Tram | 2 | Liaison de données |
| | Bit | 1 | Physique |



Transmissiondes données

**Tableau 2.1 :** les sept couches du modèle OSI (Open Systems Interconnection). [60]

## 3.6. Classification des attaques IoT DoS/DDoS basée sur une structure en couches

### 3.6.1. Couche de perception

- **Vulnérabilités de sécurité :** Cette couche, parfois appelée « couche de détection », dépend des ressources physiques faisant partie de l'IoT. Il utilise plusieurs technologies et dispositifs de détection pour collecter des données, les transformer en signaux numériques et les transmettre à la couche réseau. [39] Les technologies de la couche de perception comprennent les étiquettes RFID, les caméras, le réseau de capteurs sans fil (WSN), le GPS et le Bluetooth. Ces appareils sont choisis en fonction des fonctionnalités des applications IoT. Types d'attaques célèbres sur cette couche : [56]
  - ✓ **Attaque de brouillage RF :** Étant donné que la plupart des appareils sans fil utilisent des signaux de radiofréquence (RF) pour communiquer avec d'autres, ce signal peut être brouillé avec d'autres signaux plus puissants. L'attaquant intercepte et nie la communication entre le capteur, ou l'étiquette, et le lecteur des données transmises ; [40] [41]
  - ✓ **Écoute clandestine :** affecte principalement la partie confidentialité de l'appareil IoT. Il s'agit d'une attaque dangereuse, car l'attaquant peut lire et collecter des informations secrètes entre la balise et le lecteur de données, et tirer parti des informations recueillies. [42][41] Ces informations confidentielles peuvent être des appels téléphoniques, des SMS, des vidéoconférences. [43]
- **Solution de sécurité au niveau de la couche de perception :** Les auteurs [41] parlent des contre-mesures possibles contre les attaques RFID, WSN. Dans le document, une contre-mesure proposée contre le brouillage consiste à réguler la puissance transmise et le spectre étalé à sauts de fréquence (FHSS). C'est une solution puissante pour éviter les interférences et les évanouissements multi-trajets (distorsion), il diminue également les interférences à bande étroite, augmente la capacité du signal et améliore le rapport signal sur bruit. [44]

### 3.6.2. Couche réseau

- **Vulnérabilités de sécurité au niveau de la couche réseau :** Cette couche fonctionne de la même manière que la couche réseau TCP/IP et est également confrontée aux mêmes problèmes de sécurité typiques des réseaux de communication qui affectent la confidentialité, la disponibilité et l'intégrité des données. [45][46]

Il est chargé de transmettre les données collectées à partir des dispositifs et capteurs de la couche de perception. [43] Types d'attaques bien connus à cette couche : [56]

- ✓ **Attaques par inondation :** Dans ce type d'attaques, de nombreux trafics inutiles sont envoyés sur le réseau, rendant le système cible inaccessible. Plus précisément, le drain du système se fait par un grand nombre de requêtes de l'attaquant, [48] par exemple, UDP flood. L'attaquant inonde différents paquets UDP (User Datagram Protocol) sur différents ports de la victime, par conséquent, l'hôte du serveur inspectera ces ports pour les demandes entrantes encore et encore, provoquant l'épuisement des ressources de la victime ; [48]
- ✓ **Attaques par inondation basées sur la réflexion :** l'attaquant, dans ce type d'attaques, intercepte la connexion authentique et envoie de fausses requêtes répétées aux réflecteurs. Ces réflecteurs répondent en même temps au système cible le rendant inaccessible. [48]

❖ **Solution de sécurité au niveau de la couche réseau :** Comme pour l'IPv6 traditionnel, il existe un moyen testé de sécuriser les réseaux normaux appelés IP sec. Depuis que les appareils IoT ont été ajoutés à Internet à l'aide d'IPv6 sur des réseaux personnels sans fil à faible consommation (6LoWPAN), Raza et al. [49] ont introduit un moyen de sécuriser l'IoT basé sur l'extension IP sec testée ajoutée à 6LoWPAN. De plus, les techniques ESP (Encapsulation Security Payload) et Authentication Header (AH) sont utilisées pour sécuriser la communication entre les dispositifs de la coucheapplication et la couche réseau.

### 3.6.3. Couche middleware

❖ **Vulnérabilités de sécurité au niveau de la couche middleware :** Cette couche est responsable de la manipulation des données et des décisions intelligentes basées sur le calcul et le traitement. Le traitement est effectué sur une quantité massive de données collectées à partir de capteurs et de balises. Ces données sont stockées dans une base de données, la technologie informatique en nuage pourrait également être utilisée dans cette couche. [50][55] Différentes attaques et menaces de sécurité sont associées àcette couche, en raison de l'accumulation d'une grande quantité de données et de l'utilisation du Cloud Computing. [46] L'objectif principal de ces attaques est les données cloud pour détruire la vie privée des utilisateurs. [51] Types d'attaques célèbres sur cette couche : [56]

- ✓ **Signature Wrapping Attack :** pour les services cloud XML, les signatures sont utilisées pour vérifier l'authenticité de la connexion avec un autre service. L'attaquant peut modifier les messages écoutés et exécuter des commandes arbitraires au nom d'un utilisateur légitime, sans aucune modification de la signature. De même, Amazon Elastic Cloud Computing (EC2) utilise l'interface SOAP (Simple Object Access Protocol) pour contrôler la machine déployée. Les attaquants exploitent la faiblesse de cette interface et modifient les messages envoyés ou exécutent des commandes arbitraires ; [51]
- ✓ **Attaque par inondation dans le cloud :** les attaquants épuisent les ressources du service cloud en envoyant des requêtes étendues. Le système cloud peut transférer les services concernés vers un autre serveur, provoquant l'épuisement d'un autre serveur. Ceci affectant principalement la qualité de service [51].

❖ **Solution de sécurité au niveau de la couche middleware :** Shafagh et al. [54] ont proposé un mécanisme appelé Encrypted Query Processing Approach, qui permet aux utilisateurs de lancer des requêtes cryptées sur la base de données en utilisant un schéma cryptographique. De cette manière, la couche middleware peut stocker des données en toute sécurité sur la base de données et cela est faisable dans les appareils à faible consommation d'énergie.

### 3.6.4. Couche d'application

❖ **Vulnérabilités de sécurité au niveau de la couche application :** Cette couche est considérée comme la couche supérieure ; il est responsable de la partie logique de l'application IoT. [56] Cette couche est confrontée à différents défis de sécurité, par exemple, les autorisations d'accès et l'authentification sont très susceptibles d'être piratées, car elles sont difficiles à maintenir au sein de différents types d'applications et d'utilisateurs. [45] De plus, les pirates peuvent exploiter les vulnérabilités de la couche application, telles que le dépassement de mémoire tampon, les scripts intersites et l'injection SQL, ce qui rend difficile le maintien de la confidentialité et de la protection des données. [48] Types d'attaques célèbres sur cette couche : [56]

- ✓ **Attaque de reprogrammation :** l'attaquant peut modifier le code du programme s'il dispose d'un accès non autorisé, ce qui entraîne une fuite de données. Ayant accès au code source du programme, ils peuvent modifier le code à l'usage. De plus, s'ils utilisent une boucle infinie dans le code, cela conduira à l'épuisement des ressources du serveur ; [48]

- ✓ **Attaque DoS basée sur le chemin :** Cette attaque appelée attaque PDoS, qui est effectuée en inondant les chemins de communication de bout en bout multi-sauts avec des paquets de données. [52]

❖ **Solution de sécurité au niveau de la couche application :** Pour le problème d'authentification dans la couche application, Cirani et al. [53] ont proposé un cadre d'autorisation basé sur l'intégration avec un service d'autorisation ouvert (OAS) externe. L'ensemble de la solution désignée par IoT-OAS, qui cible les services HTTP et CAP (Constrained Application Protocol). Cette méthode offre une intégration flexible et facile avec les services existants, en plus de réduire la charge de traitement. [56]

## 3.7. Amélioration de la protection contre les attaques DoS etDDoS

Voici quelques bonnes pratiques de haut niveau pour la protection DoS et DDoS :

- Surveillez votre réseau en permanence : Ceci est bénéfique pour identifier les modèles de trafic normaux et essentiel pour une détection et une atténuation précoces ;
- Exécutez des tests pour simuler des attaques DoS : cela aidera à évaluer les risques, à exposer les vulnérabilités et à former les employés au cyber sécurité ;
- Créez un plan de protection : créez des listes de contrôle, formez une équipe d'intervention, définissez les paramètres d'intervention et déployez la protection ;
- Identifiez les systèmes critiques et les modèles de trafic normaux : le premier aide à planifier la protection, et le second aide à la détection précoce des menaces ;
- Fournir une bande passante supplémentaire : cela n'arrêtera peut-être pas l'attaque, mais cela aidera le réseau à faire face aux pics de trafic et à atténuer l'impact de toute attaque.

Les attaques DDoS évoluent, deviennent de plus en plus sophistiquées et puissantes. Les entreprises ont donc besoin de solutions qui utilisent des stratégies complètes, telles que des outils de rapports et d'analyse avancés, pour surveiller simultanément d'innombrables paramètres de menace. Pour protéger une organisation contre les attaques connues et se préparer à d'éventuelles attaques zero-day, une protection DDoS multicouche, telle que FortiDDoS, est nécessaire.

FortiDDoS inclut l'Appliance d'atténuation des attaques DDoS Fortinet, qui fournit une évaluation continue des menaces et une protection de sécurité pour les couches 3, 4 et 7 (Tableau 2.1).

# 4. Les système de détection d'intrusions

Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une action de prévention et d'intervention sur les risques d'intrusion. Afin de détecter les attaques que peut subir un système (réseau informatique), il est nécessaire d'avoir un logiciel spécialisé dont le rôle est de surveiller les données qui transitent sur ce système, et qui est capable de réagir si des données semblent suspectes.

## 4.1. Les différentes catégories d'IDS

### 4.1.1. Systèmes de détection des intrusions réseau (NIDS)

Un NIDS (Network Intrusion Detection System) est un IDS orienté réseau. Il permet de d'analyser le trafique qui circule au niveau IP (couche réseau) pour détecter d'éventuelles intrusions. Il est composé de sondes (capteurs) qui capturent le trafique acheminées sur le réseau et d'un moteur pour analyser ce trafique.

Le NIDS offre l'avantage de la furtivité et n'ajoute aucune surcharge au réseau en terme de trafique. La figure 2.7 montre l'architecture d'un réseau contenant un NIDS.

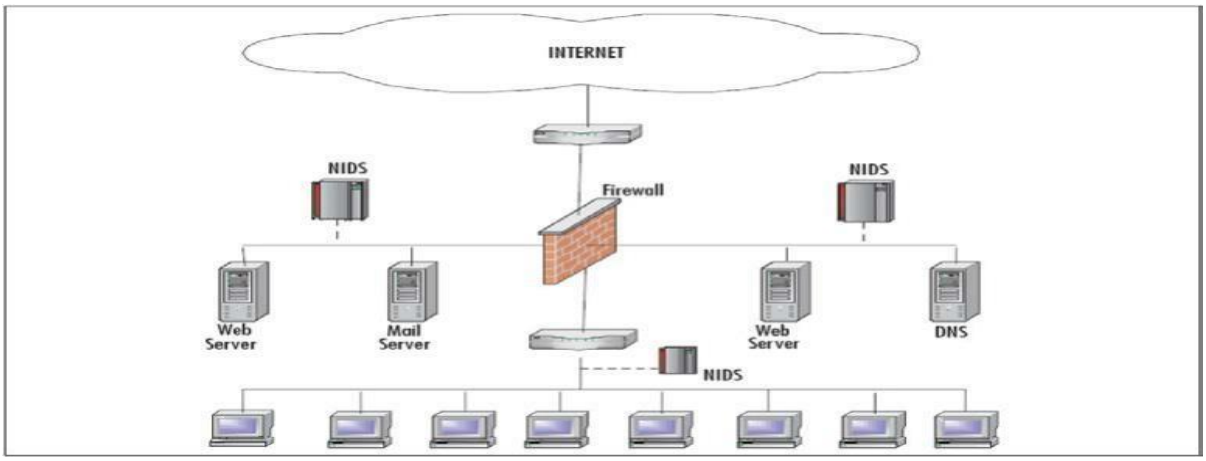



**Figure 2.7 :** Modèle d'architecture pour NIDS proposé par le groupe IDWG [58]

### 4.1.2. Système de détection d'intrusion hôte (HIDS)

Un HIDS (Host Intrusion Detection System) est un agent logiciel installé sur la machine à protéger afin d'analyser en temps réel les flux de trafique de cette machine ainsi que les fichiers journaux. Contrairement à un NIDS, un HIDS ne protège donc que le système local. Un HIDS est capable de détecter les changements dans les fichiers et dans le systèmed'exploitation de la machine hôte. La figure 2.8 montre l'utilisation de l'HIDS dans un réseau.

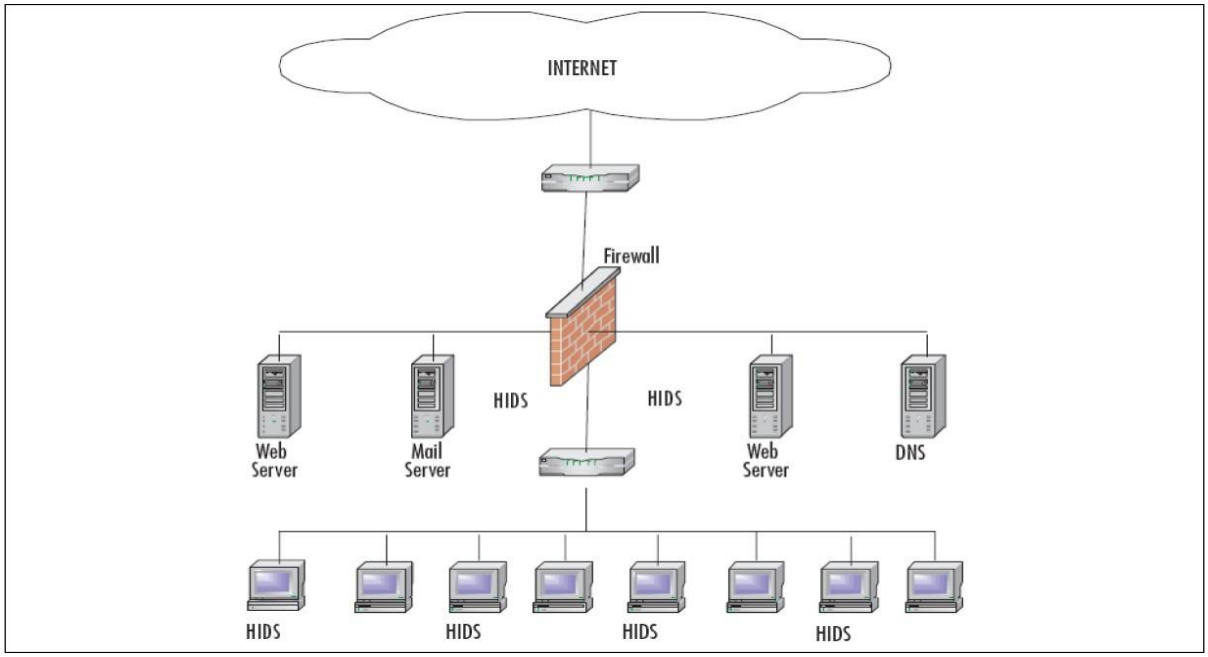



**Figure 2.8 :** Réseau HIDS [58]

### 4.1.3. Système de détection d'intrusion distribué (DIDS)

Un DIDS (Distributed Intrusion Detection System) est obtenu en faisant collaborer plusieurs types d'IDS (NIDS, HIDS, senseurs) distribués dans un même réseau local. Chacun de ces IDS rapporte son analyse vers un même système de corrélation central. Cependant, la gestion des informations recueillies par les différents senseurs ne se traite pas de la même façon car, chaque senseur peut avoir ses propres règles. Ainsi, les alertes renvoyées vers le système de corrélation centrale sont traitées en prenant en considération les spécificités de chaque type d'alerte. La figure 2.9 représente une vue globale d'un DIDS.

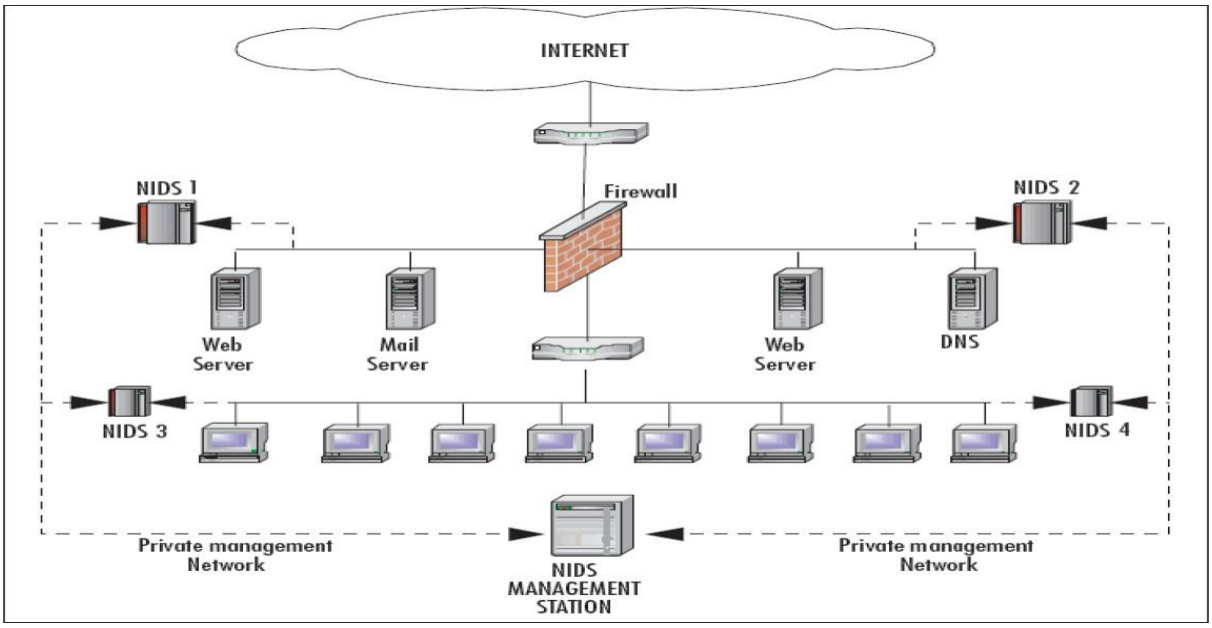



**Figure 2.9 :** Schéma global d'un DIDS [58]

## 4.2. Fonctionnement d'un IDS

### 4.2.1. Méthodes de détection

Deux stratégies majeures sont largement employées pour distinguer, quel trafic est malicieux ou non. La première stratégie se base sur le comportement passé du système pour distinguer si un trafic est bon ou mauvais (malicieux). Elle permet de détecter toutes les activités inhabituelles comparées à celles qui sont préalablement définies. Anderson dans [68] a utilisé des études statistiques pour classifier et déterminer le comportement d'un utilisateur, mais, généralement la connaissance et la distinction d'un tel comportement peuvent se font par apprentissage. Après cette phase le trafic est catégorisé en bons (de même type que celui rencontré durant la phase d'apprentissage) ou malicieux (dévie par rapport au trafic considéré comme normal).

Cependant, cette stratégie rend l'IDS tributaire de la qualité du trafic analysé durant la phase d'apprentissage et souvent la prédiction n'est pas précise et le système génère alors beaucoup de faux positifs et de faux négatifs. La deuxième technique pour la détection d'intrusion est connue sous le nom « Rule-based / Signature-based analysis ». Cette technique se base sur la comparaison du trafic généré par l'activité des utilisateurs dans le réseau avec une base de données de patrons de trafic connus pour être malicieux Elle consiste à identifier seulement les scénarios d'attaque qui ont un comportement anormal dans une base de scénarios d'attaques prédéfinis.

La détection par signatures est l'approche la plus utilisée dans la technologie des IDSs commerciaux car elle donne de meilleurs résultats comparativement à l'approche comportementale.

### 4.2.2. Analyse des attaques

L'analyse du trafic peut différer d'une architecture à une autre, nous pouvons distinguer deux types d'analyses : l'analyse locale centralisée et l'analyse distribuée. L'analyse peut aussi être périodique ou continue. Pour analyser un trafic, nous pouvons distinguer quatre tâches différentes :

- **Agrégation des données :** permet de faire la collecte d'informations et la normalisation du format des données pour faciliter le traitement ;
- **Réduction des données :** permet de filtrer les données inutiles, trouver les redondances et éliminer les données erronées ;
- **Corrélation des données :** permet d'identifier les relations entre les alertes dans le butde les regrouper (Clustering) en fonction de différentes variables (temps, évènement, port destination, protocole, contenu du message, etc.) ;
- **Induction des données :** essayer de comprendre de nouvelles données, découvrir de nouveaux patrons ou identifier des nouvelles attaques.

| | **Vrai** | **Faux** |
|---|---|---|
| **Positif** | Une alerte est générée et une condition présente doit e révélée. | Une alerte et générée et aucune condition présente n'est révélée. |
| **Négatif** | Une alerte n'est pas générée et aucune condition présente n'est pas révélée. | Une alerte n'est pas générée et une condition présente doit est révélée. |

**Tableau 2.2 :** Vrai/Faux, Positif/Négatif. [69]

### 4.2.3. Réaction et comportement après une attaque

La qualité de la réaction d'un IDS dépend souvent des règles mises par l'administrateur lors de l'installation et de la configuration du système. Nous pouvons distinguer deux approches pour la réaction d'un IDS :

- **Approche passive :** l'IDS ne fait aucune réaction se contentant d'informer l'administrateur par une alerte sous forme d'un courriel ou un message SMS ;

- **Approche active :** l'IDS envoie des alertes en plus d'autres réactions contre cette attaque comme, par exemple, réinitialiser la connexion, bloquer du trafic, supprimer tous les processus du système attaquant, etc.

Nous distinguons deux modes pour une alerte : le mode complet donnant une alerte plus détaillée et un mode réduit donnant quelques informations essentielles (Full Mode Alert, Fast Mode Alert).

### 4.3. Architecture des IDS

Un IDS est essentiellement constitué d'un sniffer couplé avec un moteur qui analyse le trafic et entreprend des actions suivants les règles définies dans l'IDS. Ces règles décrivent le comportement de l'IDS selon le trafic analysé trafic : Alertes, journalisation des événements dans des fichiers logs.

Un IDS peut analyser les couches suivantes :

- Couche Réseau (IP, ICMP) ;
- Couche Transport (TCP, UDP) ;
- Couche Application (HTTP, Telnet).

Selon le type de trafic, l'IDS accomplit certaines actions définies dans les règles. 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 négative :** une intrusion réelle qui n'a pas été détectées par l'IDS.

Le shéma suivante illutre le fonctionnement et les caractéristiques d'un IDS

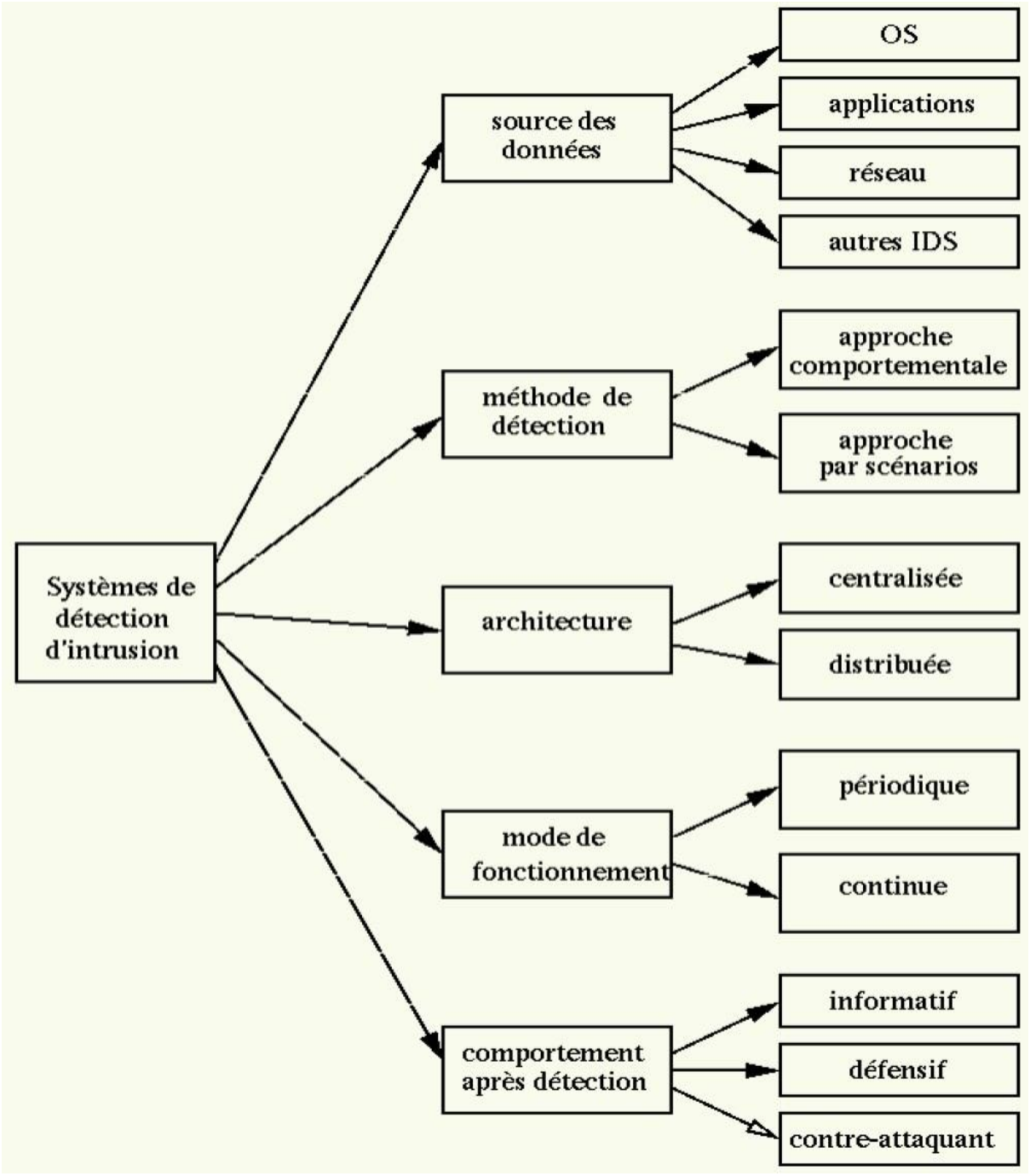



**Figure 2.10 :** Caractéristiques et Fonctionnement des IDS.

### 4.4. Critères de Choix D'un IDS

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

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

- **Fiabilité :** Les alertes générées doivent être justifiées et aucune intrusion ne doitpouvoir lui échapper ;
- **Réactivité :** Un IDS doit être capable de détecter les nouveaux types d'attaques le plus rapidement possible ; pour cela il doit rester constamment à jour. Des capacités de mise à jour automatique sont indispensables ;
- **Facilité de mise en œuvre et adaptabilité :** Un IDS doit être facile à mettre en œuvre, surtout s'adapter au contexte dans lequel il doit opérer. Il est inutile d'avoir un IDS émettant des alertes en moins de 10 secondes si les ressources nécessaires à une réaction ne sont pas disponibles pour agir dans les mêmes contraintes de temps ;
- **Performance :** la mise en place d'un IDS ne doit en aucun cas affecter les performances des systèmes surveillés.

De plus, il faut toujours avoir la certitude que l'IDS a la capacité de traiter toute l'information à sa disposition (par exemple un IDS réseau doit être capable de traiter l'ensemble du flux pouvant se présenter à un instant donné sans jamais supprimer de paquets) car dans le cas contraire il devient trivial de masquer les attaques en augmentant la quantité d'information.

# 5. Apprentissage automatique pour la détection desintrusions IoT

## 5.1. Définition de l'apprentissage automatique

L'apprentissage automatique est un processus systématique d'obtention des modèle de connaissances à partir des entrées bien définies sans faire toute procédure algorithmique pour les sorties rationalisées. IoT est un produit inévitable de notre vie quotidienne.

Le Machine Learning ou apprentissage automatique est un domaine scientifique, et plus particulièrement une sous-catégorie de l'intelligence artificielle. Elle consiste à laisser des algorithmes découvrir des " patterns ", à savoir des motifs récurrents, dans les ensembles de données. Ces données peuvent être des chiffres, des mots, des images, des statistiques, etc.

Les algorithmes de Machine Learning apprennent de manière autonome à effectuer une tâche ou à réaliser des prédictions à partir de données et améliorent leurs performances au fil du temps. Une fois entraîné, l'algorithme pourra retrouver les patterns dans de nouvelles données. [62] Appliquer l'intelligence à Internet de choses par l'approche artificielle, est l'une des méthodes pour minimiser la demande de travail intensive pour chaque processus. [63] En tant que prototype, les gadgets Internet des objets peuvent être utilisés pour divers fins et installer à divers endroits en fonction des cas d'utilisation. [57] Celles-ci la taille des gadgets peut varier de minuscule à énorme lors du déploiement, ce qui entraîne les informations les plus cruciales et les plus sensibles à travers tous les sens mode d'activités de la vie quotidienne. [64]

## 5.2. Application de l'apprentissage automatique à l'IoT

Aujourd'hui, il existe plusieurs algorithmes ML appliqués dans l'IoT. Ces applications ML dépendent fortement du domaine appliqué. Il existe plusieurs raison pour lesquelles l'apprentissage automatique influence l'IoT. Mais d'abord, que se passe-t-il si l'IoT est mis en œuvre sans ML ? L'IoT doit faire face aux conséquences suivantes lorsqu'il est uniquement mis en œuvre sans ML. Cela inclut l'intégration de données provenant de plusieurs sources, la gestion des appareils, la gestion d'un énorme volume de données et le contrôle des versions des applications. [65]

Applications d'apprentissage automatique plus larges dans tous les domaines de l'Internet des objets, il présente de nombreux avantages La réduction des coûts par l'apprentissage automatique joue un rôle essentiel sur les applications de l'industrie.

Une partie mondialement connue de l'apprentissage automatique façonne l'avenir sur la base de la recommandation, où se composent de nombreux exemples comme Amazon, YouTube, Netflix, etc., ayant une plus grande dans l'entreprise ne se limite pas à la mesure [66].

En figure. 2.11, dispose des données pour montrer la tendance de l'interconnexion avec l'Internet des objets et Machine Learning sur la projection mondiale au cours des cinq dernières années.

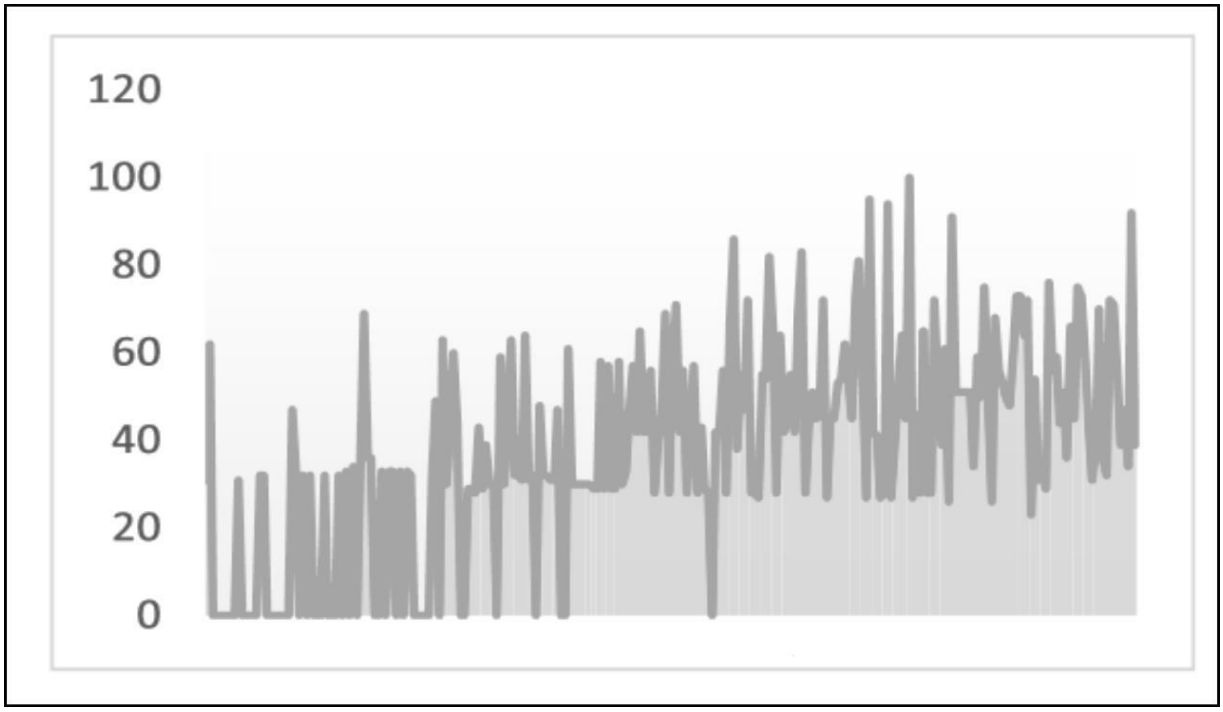



**Figure 2.11 :** Utilisation de l'apprentissage automatique IoT (Google Trends). [57]

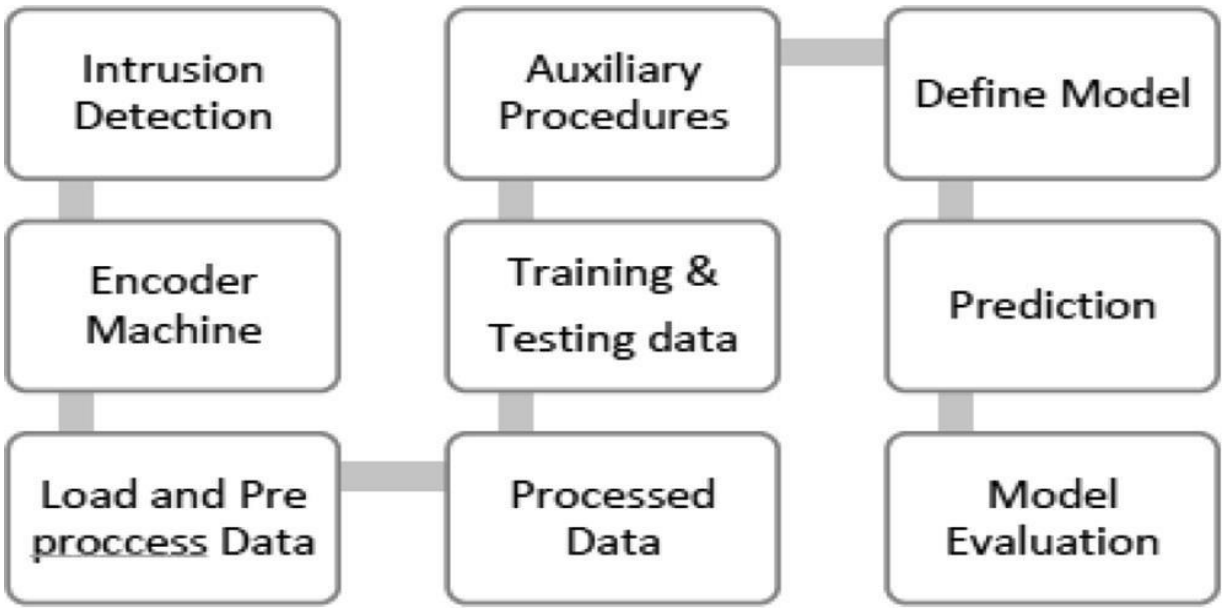



**Figure 2.12 :** Modèle d'application de Machine Learning pour le système de détection d'intrusion. [57]

## 6. Conclusion

Le deuxième chapitre vis à donner une description globale de la sécurité dans Internet of Things. Ainsi son développement remarquable ces dernières années qui suscite de plus en plus l'intérêt des différents utilisateurs de l'internet et de l'informatique. Ensuite nous avons passé à la description des différentes attaques, et la détection d'intrusion, l'apprentissage automatique.

Les réseaux Internet of Things sont vulnérables à différentes attaques les fabricants et développeurs mondiaux de gadgets exigent plus de prudence dans cette session une discussion détaillée des attaques et telles que la surface attaque, les effets de l'attaque et les types d'attaque dans Internet des Choses.

Pour appliquer l'algorithme d'apprentissage automatique à l'Internet des choses réseau système les attaques sur le réseau vont identifier par méthode de détection d'intrusion. Cette méthode de détection applique le algorithme d'apprentissage automatique sur le réseau avec limite de seuil définit l'attaque comme anormale ou normale [71]. La détection d'intrusion était un comportement anormal survenu dans le réseau, qui est classés en trois aspects principaux sur le modèle de signature, modèle d'anomalie et modèle de spécification. Dans la signature système de détection d'intrusion modèle essayez de trouver les modèles dans connecté réseau similaire à celui de la base de données de signatures existante.

Les applications sur Machine Learning ne peuvent pas être limitées, ce qui agit en tant que procédure universelle pour une grande variété d'applications industrielles et technologiques streamers avec les systèmes IoT. Cela favorise la recherche et l'entreprise propulsera avec des décisions précises et une action limitée planifier des analyses. Dans le monde numérique, l'Internet des objets fait interconnexion de tous les appareils ou gadgets en un seul système, qui permet le moyen le plus simple d'accéder n'importe où, n'importe quand avec sécurité.

# Chapitre 03 :
# Description de projet

# 1. Introduction

Les systèmes de détection d'intrusion sont l'une des considérations les plus importantes en matière de sécurité réseau, aidant à repérer les intrusions avant et/ou après une attaque. Il joue un rôle important en tant que mécanisme de défense pour les réseaux et les systèmes. Nous présenterons ici quelques méthodes d'apprentissage en profondeur qui ont été appliquées dans le domaine de la détection d'intrusion dans IoT.

Dans Ce chapitre nous ferons une description compète du projet, fixant les objectifs, l'architecture du système, dataset utilisée, nous avons également étudié et analysé divers travaux de détection d'intrusion basés sur le deep learning.

# 2. Objectif

L'objectif de ce travail et la suivante :

Mettre en œuvre un système de détection d'intrusion basé sur le comportement des internet des objets et reposant sur la technique de deep learning.

Pour fair ca nécessaire de réaliser les objectifs suivants :

- Comprendre les caractéristiques de l'Internet of Things ;
- Développer un système de détection basé sur le comportement qui utilise un algorithme d'apprentissage en profond ;
- Analyser et apprendre le comportement de l'attaque DoS et ainsi détecter une attaque par son comportement ;
- Identifier et implémenter des attaques sur objets connectés étudiés ;
- Tester la performance de la solution de ce système.

En résumé, l'objectif de cette étude est d'implémenter une méthode de détection d'intrusion en se basant sur les approches de Deep Learning. Nous utilisons une dataset DoS, qui reprisent un trafic réseau réel contenant plusieurs types des attaques DoS malveillantes les plus répandus.

## 3. Architecture du système

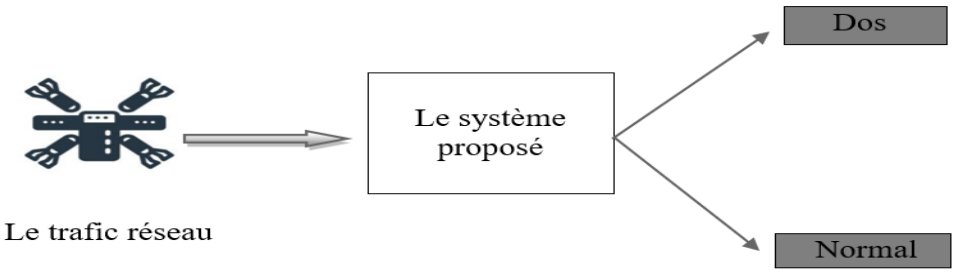



**Figure 3.1 :** L'architecture du système.

## 4. Travaux connexes

Dans cette section, nous mettons en évidence un certain nombre d'études qui ont appliqué des algorithmes deep learning, pour la détection d'intrusion.

**SaiSindhuTheja et Shyam. [71]** ont proposé un nouveau système de détection d'attaque par déni de service (DoS) utilisant un algorithme de recherche Crow (CSA) modifié pour la sélection des fonctionnalités. L'Opposition Based Learning (OBL) est associé au CSA pour booster ses performances. Ensuite, le réseau de neurones récurrent (RNN) est appliqué comme classificateur. Les résultats de l'évaluation ont confirmé les performances compétitives de la méthode de sélection de caractéristiques proposée utilisant la CSA améliorée et la haute précision de classification du RNN avec la CSA.

**Dans [72],** la colonie d'abeilles artificielles (ABC) a été utilisée pour améliorer le classificateur afin de détecter et de lutter contre les attaques par déni de service (DOS) dans le cloud. Les résultats de prédiction ont été améliorés en appliquant l'algorithme ABC par rapport à la technique d'optimisation des essaims de particules d'inspiration quantique (QPSO), avec un taux de détection moyen de 72,4 %.

**Dans [73],** les auteurs ont proposé un algorithme DL pour améliorer la détection des cyberattaques imprévues sur un environnement Internet of Medical Things (IoMT) et pour établir un IDS fiable et productif. Le système proposé, basé sur Deep Neural Network (DNN), a obtenu les meilleures

performances par rapport aux propositions ML existantes. L'évaluation des performances montre une amélioration de la précision de 15% et une réduction du temps de calcul de 32%.

**Dans [74],** les auteurs ont proposé l'utilisation de deux architectures pour détecter les attaques IoT en temps réel : le traitement d'événements complexes associé à la régression linéaire ou vectorielle de support, et le ML basé sur l'apprentissage supervisé. Les architectures proposées ont été appliquées à un réseau IoT de santé pour valider la détection des attaques MQTT.

**Ciklabakkal et al. [75]** ont présenté un IDS pour l'IoT nommé ARTEMIS. L'ARTEMIS traite les données des appareils IoT via ML pour trouver le comportement normal du système et générer des alertes en cas d'anomalies. Les auteurs ont généré un ensemble de données contenant des attaques pour MQTT.

**Saljoughi et al. [76]** ont proposé un schéma de détection d'intrusion d'attaque pour le cloud computing utilisant un modèle combiné d'apprentissage en profondeur et d'intelligence en essaim. Ils ont utilisé un réseau de neurones MLP (Multi layer Perceptron) et un algorithme d'optimisation des essaims de particules (PSO) pour les attaques et la détection des intrusions. Les ensembles de données KDD-CUP et NSL-KDD ont été appliqués dans les expériences d'évaluation, et le schéma proposé a montré une précision accrue dans les attaques et la détection des intrusions.

**Nazir et Khan. [77]** ont proposé une nouvelle sélection de fonctionnalités utilisant l'algorithme Tabu Search (TS) pour former le classificateur Random Forest (RF) afin de construire un système de détection d'intrusion robuste. Le système proposé, appelé TS-RF, a été évalué à l'aide de l'ensemble de données UNSW-NB15. Les résultats de l'évaluation ont montré que le TS surpassait plusieurs méthodes de sélection de caractéristiques, et le TS-FS proposé améliorait la précision de la classification.

**Mayuranathan et al. [78]** ont proposé un système de détection d'intrusion amélioré avec une nouvelle technique de sélection de caractéristiques utilisant l'algorithme d'optimisation Random Harmony Search (RHS). Les machines Boltzmann restreintes ont été appliquées comme classificateur pour la détection de déni de service distribué (DDoS). L'évaluation a été mise en œuvre avec les ensembles de données KDD'99, et le système proposé a obtenu des performances significatives.

**Fatani et al. [79]** ils ont développé une nouvelle méthode de sélection de caractéristiques (FS)pour améliorer la classification IDS en utilisant une nouvelle variante de l'optimisation de recherche transitoire (TSO) et les résultats ont étaient que les valeurs de FPR pour le TSODE sont meilleures que d'autres algorithmes dans le binaire. Et les cas de classification multi- classes parmi les quatre

ensembles de données testés (c'est-à-dire KDDCup-99, NSL-KDD, BoT-IOT et CICIDS-2017). Cela indique que les fonctionnalités sélectionnées utilisant le TSODE proposé améliorent les performances de détection du classifier sur chaque classe par rapport aux autres méthodes.

**De plus, Alsaedi et al. [80]** ont proposé un nouveau jeu de données, appelé TON_IoT. Ils ont utilisé plusieurs méthodes de classification pour évaluer les ensembles de données collectés et ont constaté que RF et les arbres de classification et de régression (CART) obtenaient les meilleurs résultats, tandis que LSTM et KNN arrivaient au deuxième rang par rapport aux autres méthodes de classification.

**Dans [81],** les auteurs ont présenté une méthode de détection d'anomalies qui utilise des instantanés de l'activité du réseau et des encodeurs profonds pour prédire toute anomalie. Pourcela, ils ont créé un réseau IoT et les ont infectés à l'aide des botnets Mirai et BASHLITE. Sur la base des fonctionnalités agrégées via les adresses IP source/destination, les adresses MAC, etc., ils créent un auto-encodeur profond pour chaque appareil séparément.

**Dans l'article [82],** les auteurs ont proposé un mécanisme de défense basé sur l'apprentissage profond contre les attaques DDoS. Ils ont nommé leur système de détection d'intrusion Deep Défense, qui est basé sur un modèle de réseau neuronal récurrent formé sur l'ensemble de données ISCX2012. Leur modèle a montré qu'il réduisait le taux d'erreur d'une grande fraction, mais un inconvénient est que l'ensemble de données est ancien et n'est pas bien mis àjour.

**Geethapriya et al. [83]** ont construit un module MLAD (détection d'anomalies basée sur l'apprentissage automatique) basé sur un réseau de croyances profondes (DBN) qui est une variante de DNN et ont testé leur modèle dans leur propre banc d'essai créé.

**M. Zeeshan et al. [91]** ont proposé en classification binaire, basée sur LSTM modèle d'apprentissage en profondeur non supervisé (PB-DID) atteint des précisions de classification supérieures à 99 % pour les valeurs non anormales vs paquets anormaux (non anormaux vs DDOS et non anormaux vs DOS). Pour une classification binaire entre DDOS et DOS, c'est- à-dire une classification correcte du type d'attaque, ils ont classé non anormal, Trafic DoS et DDoS en utilisant le DL technique et atteint une précision de 96,3% en couvrant presque les deux ensembles de données dans leur intégralité.

**Ferrag et al. [92]** ont proposé des modèles de détection d'intrusion d'apprentissage profond dans le contexte de l'agriculture 4.0. Ils ont évalué les performances de leurs réseaux qui impliquent des structures DNN, CNN et RNN basées sur des classifications binaires et multi classes. Ils ont formé leurs modèles à l'aide de TON_IoT et CIC-DDoS2019 pour diverses attaques DDoS.

**Devrim Akgun. [93]** ont proposé un nouveau système de détection d'intrusion basé sur des modèles d'apprentissage en profondeur pour les attaques DDoS. Ils ont utilisé le jeu de données CIC-DDoS 2019, selon les résultats des tests, le modèle suggéré a atteint des valeurs de précision de 99,30 % pour la classe multi et de 99,99 % pour la classe binaire. Le modèle proposé détecte avec succès divers types d'attaques pour la classification multi-classes et binaires.

## 5. Machine learning

Pour répondre quel est le machine learning, est-il nécessaire de la définition suivant donnée par Bostjan Kaluza (20016) : [84]

- Le ML est sous-domaine du un intelligence artificielle.
- Est aider les ordinateurs apprendre et agir comme être humains avec l'aide d'algorithmes et données.
- Etant données ensemble de données, un algorithme de ML.
- Apprendre différent propriétés et déduire les propriétés des données qui peuvent être présenté dans le futur.

D'après la définition ci-dessus, il on peut en déduire que l'objectif de le ML consiste à développer systèmes qui permettent aux ordinateurs apprendre, généraliser comportements.

Comment vous le verrez, ML est un domaine diversifié et dynamique qui comprend d'autres sous-domaines. Puisque les données (au les règles) sont si importantes dans ML, il s'agit typiquement de l'un des types suivants :

- Apprentissage supervisé : beaucoup de données étiquetées ;
- Apprentissage semi-supervisé : beaucoup de données étiquetées ;
- Apprentissage non supervisé : beaucoup de données, Clustering ;
- Apprentissage de renforcement : essai, feedback, et amélioration.

Selon Andrew Ng (cofondateur de Coursera), « 99% de ML est supervisé ». En plus de catégoriser les données, les algorithmes d'apprentissage automatique peuvent être classés dans les principaux types suivants :

- Classificateurs : pour les images, les spams, les fraudes, etc.
- Régression : prix des actions, prix de l'immobilier, etc.
- Clustering : classificateurs non supervisés.

## 5.1. Deep learning

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

### 5.1.1. Définition de l'apprentissage profond

L'apprentissage profonde (Deep learning ou DL) appartient à une classe de techniques d'apprentissage automatique (machine learning ou ML), il obtient un grand succès dans de nombreuses tâches de l'intelligence artificielle (IA) par rapport aux algorithmes de ML classiques. Les architectures des modèles profondes sont relativement récentes où de nombreuses étapes de traitement non linéaire de l'information sont exploitées, dans lesquelles les informations sont traitées en couches hiérarchiques, chacune recevant et interprétant les informations de la couche précédente pour l'apprentissage des représentations de données. [85] Alors que l'apprentissage automatique implique des MLP (perception multicouches), l'apprentissage profond introduire des réseaux neuronaux profonds, avec de nouveaux algorithmes et de nouveaux architectures (par exemple. réseaux de neurones convolutionnels, RNN et LSTM).

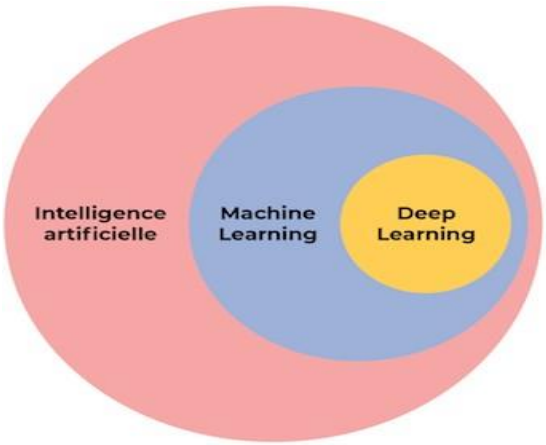



**Figure 3.2 :** Apprendre le deep learning.

### 5.1.2. Quelques méthodes d'apprentissage profond

Les réseaux neuronaux profonds sont un ensemble de neurones organisés en une séquence de couches interconnectés. Ce qui les différencies, c'est l'architecture du réseau (la manière dont les neurones sont organisés dans le réseau et la manière dont ils se fonctionnent. Parmi de nombreuses implémentions de modèles d'apprentissage profond :

- **Deep Neural Network (DNN)**

Les Deep Neural Networks (DNN) sont un ensemble de neurones organisés en une séquence de couches multiples appelée Multi layer Perceptrons (MLP). Ils se distinguent des réseaux neuronaux traditionnels (Artifical Neural Network) par leur profondeur et le nombre de couches, de nœuds (neurones) qui composent le réseau. Lorsqu'un ANN possède deux couches cachées ou plus, il est connu sous le nom de réseau neuronal profond. Ils tentent à modéliser des données contenant des architectures complexes en combinant différentes transformations non linéaires. [86]

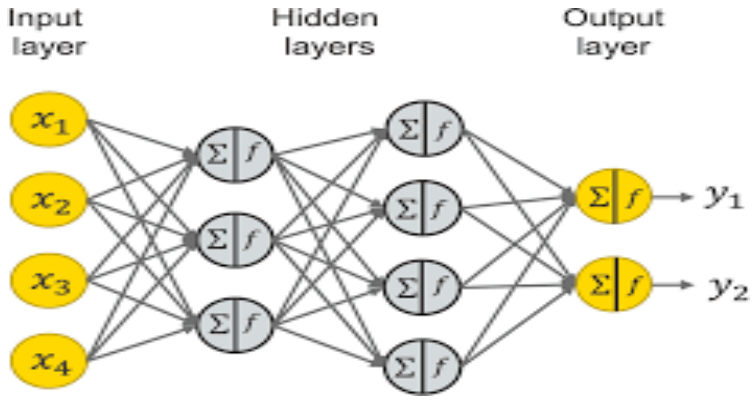



**Figure 3.3 :** Description de deep neural networks.

- **Convolutional neural networks (CNNs)**

Un réseau neuronal convolutionnel ou CNN est une extension des réseaux de feed forward traditionnels (FFN) dans le cadre de l'inspiration des facteurs biologiques [87]. Ceux-ci ont été initialement étudiés pour le traitement d'images dans lesquelles des motifs répétitifs peuvent être trouvés – par exemple, une image avec des bords répétitifs et d'autres motifs. Les CNNs surpassent tous les autres algorithmes ML classiques et fait un grand succès dans les tâches de traitement de vision par ordinateur (Computer Vision Tasks), ils ont des larges applications dans le traitement d'image et vidéo, le traitement du langage naturel (NLP), les systèmes de recommandation …etc.

Les réseaux convolutifs sont particulièrement efficaces grâce à plusieurs types de couches spéciales : des couches de convolution, des couches groupement (Pooling) et de couches entièrement connectées [88].

- **Recurrent neural networks (RNNs)**

Les réseaux neuronal s'inspirent du fonctionnement des neurones biologiques du cerveau humain, ces neurones sont considère comme le centre de réflexion, et parfois ils doivent mémoriser certains évènements pour les utilisé ultérieurement avant de prendre la décision.

Les réseaux neuronal traditionnel n'ont pas ce propriété, alors le fonctionnement d'un réseau de neurones récurrents (RNN) est motivé par le fait qu'un être humain raisonne en s'appuyant sur les connaissances qu'il a acquises et qui qu'il a mémorisé précédemment [89].

Les réseaux RNNs sont des réseaux de type Feed-Forward ayant un état interne (ou mémoire) qui prennent en compte tout ou partie des données vues précédemment (déjà fournies au réseau), en plus de la donnée vue actuellement pour adapter leur décision.

L'idée clé de base de ces réseaux est le déploiement d'un calcul récurrent grâce aux boucles dans l'architecture du réseau. La sortie de réseau est une combinaison de son état interne (mémoire d'entrées) et le dernier l'entrée, au même temps, l'état interne change pour intégrer cette nouvelle donnée saisie. Recurrent neural networks (RNNs) les réseaux neuronal s'inspirent du fonctionnement des neurones biologiques du cerveau humain, ces neurones sontconsidère comme le centre de réflexion, et parfois ils doivent mémoriser certains évènements pour les utilisé ultérieurement avant de prendre la décision.

Les réseaux neuronal traditionnel n'ont pas ce propriété, alors le fonctionnement d'un réseau de neurones récurrents (RNN) est motivé par le fait qu'un être humain raisonne en s'appuyant sur les connaissances qu'il a acquises et qui qu'il a mémorisé précédemment [89].

Les réseaux RNNs sont des réseaux de type Feed-Forward ayant un état interne (ou mémoire) qui prennent en compte tout ou partie des données vues précédemment (déjà fournies au réseau), en plus de la donnée vue actuellement pour adapter leur décision.

L'idée clé de base de ces réseaux est le déploiement d'un calcul récurrent grâce aux boucles dans l'architecture du réseau. La sortie de réseau est une combinaison de son état interne (mémoire d'entrées) et le dernier l'entrée, au même temps, l'état interne change pour intégrer cette nouvelle donnée saisie.

- **Long Short-Term Memory (LSTM)**

La mémoire longue à court terme (LMTS en anglais) est un réseau de neurones artificiels utilisé dans les domaines de l'intelligence artificielle et de l'apprentissage en profondeur. Contrairement aux réseaux de neurones à anticipation standard, LSTM a des connexions de rétroaction. LSTM est un type particulier de réseau neuronal récurrent capable de gérer les dépendances à long terme.

Long Short Term Memory Network est un RNN avancé, un réseau séquentiel, qui permet aux informations de persister. Il est capable de gérer le problème de gradient de fuite auquel est confronté RNN. Un réseau de neurones récurrent est également connu sous le nom de RNN et est utilisé pour la mémoire persistante. Disons qu'en regardant une vidéo, vous vous souvenez de la scène précédente ou en lisant un livre, vous savez ce qui s'est passé dans le chapitre précédent. De même, les RNN fonctionnent, ils se souviennent des informations précédentes et les utilisent pour traiter l'entrée actuelle. Le défaut de RNN est qu'ils ne peuvent pas se souvenir des dépendances à long terme en raison du gradient de fuite. Les LSTM sont explicitement conçus pour éviter les problèmes de dépendance à long terme. [90] À un niveau élevé, LSTM fonctionne très bien comme une cellule RNN. Voici le fonctionnement interne du réseau LSTM. Le LSTM se compose de trois parties, comme indiqué dans l'image ci-dessous et chaque partie remplit une fonction individuelle.

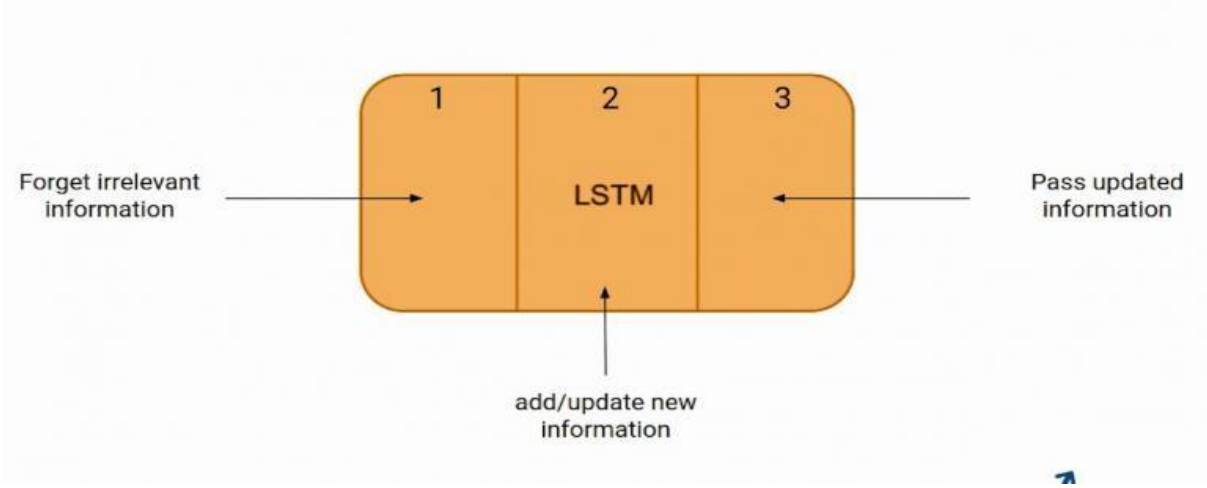



**Figure 3.4 :** Architecture LSTM.

La première partie choisit si les informations provenant de l'horodatage précédent doivent être mémorisées ou sont non pertinentes et peuvent être oubliées. Dans la deuxième partie, la cellule essaie d'apprendre de nouvelles informations à partir de l'entrée de cette cellule. Enfin, dans la troisième partie, la cellule passe les informations mises à jour de l'horodatage courant à l'horodatage suivant.

Ces trois parties d'une cellule LSTM sont appelées portes. La première partie est appelée Forget gate, la deuxième partie est connue sous le nom de Input gate et la dernière est la Output gate.

## 6. Dataset UNSW-NB15

L'ensemble de données a été publié par Moustafa et al. [94] en 2015. Cet ensemble de données est simulé avec plus de 2,5 millions de réseaux paquets. Cet ensemble de données se compose de neuf types d'attaques (Exploits, Reconnaissance, DoS, Generic, Shellcode, Fuzzers, Portes dérobées, vers et analyse)) avec non-anormal les paquets aussi. Plus de 87 % des paquets sont de nature non anormale type qui rend l'ensemble de données fortement déséquilibré.

Dans notre mémoire les données à classifier sont issue UNSW-NB 15. Les paquettes réseau bruts de l'ensemble de données UNSW-NB 15 ont été créé par l'outil IXIA PerfectStorm dans le Cyber Range Lab du centre australien pour la cybersécurité (ACCS) pour générer un hybride d'activité normales modernes réelles et de comportement d'attaque contemporains synthétiques. Cet ensemble de données est composé d'une sélection de attaques DoS, adaptésà utiliser pour tester les systèmes de l'ensemble de données contient 109353 attaques sur lesquels il y a 93000 Normal, et 16353 DoS attaques.

| **Classes** | **Nombre** | **Label** |
|---|---|---|
| **Normal** | 93000 | 0 |
| **DoS** | 16353 | 1 |

**Tableau 3.1 :** Nombre de classes dataset.

| **Totale** | **Train** | **Test** |
|---|---|---|
| **Normal/ DoS** | 76547 | 32806 |

**Tableau 3.2 :** Train/Test dataset.

## 7. Mesures de la performance de modèle d'apprentissage automatique

Il existe quatre métriques principales pour mesurer la précision d'un modèle d'apprentissage automatique. Ces mesures sont l'exactitude, la précision, le rappel et le F-Score (ou F Score). Dans cet article, nous expliquerons comment calculer chacune de ces mesures et à quoi elles servent. Avant d'apprendre ce que sont toutes ces mesures, nous devons d'abord couvrir la matrice de confusion. Lorsque votre modèle d'apprentissage automatique fait une prédiction, il peut avoir raison ou tort. Une matrice de confusion permet de savoir si le modèle a prédit correctement ou non la classe donnée.

### ❖ Matrice de confusion

La matrice de confusion est une matrice qui permet de visualiser les performances des modèles d'apprentissage automatique de classification. Grâce à cette visualisation, vous pouvez avoir une meilleure idée des performances de votre modèle d'apprentissage automatique.

Après avoir créé un modèle d'apprentissage automatique, la précision est une métrique utilisée pour évaluer le modèle d'apprentissage automatique. D'un autre côté, vous ne pouvez pas utiliser la précision dans tous les cas, car cela induirait en erreur. Parce que la précision de99% peut sembler bonne en pourcentage, mais considérez un modèle d'apprentissage automatique utilisé pour la détection de fraude ou la détection de consommation de drogue.

### ❖ Score de précision

La précision du modèle est une métrique de performance du modèle d'apprentissage automatique qui est définie comme le rapport des vrais positifs et des vrais négatifs à toutesles observations positives et négatives. En d'autres termes, la précision nous indique à quelle fréquence nous pouvons nous attendre à ce que notre modèle d'apprentissage automatique prédise correctement un résultat sur le nombre total de fois qu'il a fait des prédictions. Par exemple : supposons que vous testiez votre modèle d'apprentissage automatique avec un ensemble de données de 100 enregistrements et que votre modèle d'apprentissage automatique prédise correctement ces 90 instances. La métrique de précision, dans ce cas, serait : (90/100) = 90 %. Le taux de précision est excellent, mais il ne nous dit rien sur les erreurs que nos modèles d'apprentissage automatique font sur de nouvelles données que nous n'avons jamais vues auparavant. Mathématiquement, il représente le rapport de la somme des vrais positifs et des vrais négatifs sur toutes les prédictions.

***Score de précision = (TP + TN)/ (TP + FN + TN + FP).***

❖ **F1-Score**

Le score du modèle F1 représente le score du modèle en fonction de la précision et du score de rappel. Le F-score est une métrique de performance du modèle d'apprentissage automatique qui donne un poids égal à la fois à la précision et au rappel pour mesurer ses performances en termes de précision, ce qui en fait une alternative aux métriques de précision (elle ne nous oblige pas à connaître le nombre total d'observations). Il est souvent utilisé comme une valeur unique qui fournit des informations de haut niveau sur la qualité de sortie du modèle. Il s'agit d'une mesure utile du modèle dans les scénarios où l'on essaie d'optimiser la précision ou le score de rappel et, par conséquent, les performances du modèle en souffrent. Ce qui suit représente les aspects liés aux problèmes d'optimisation de la précision ou du score de rappel. Mathématiquement, il peut être représenté comme une moyenne harmonique de précision et de score de rappel.

*Score F1 = 2* Score de Précision * Score de Rappel/ (Score de Précision + Score de Rappel/).*

# 8. Conclusion

Dans ce chapitre nous avons présenté le processus général du système de détection d'intrusion, différentes méthodes et architectures d'apprentissage en profondeur ont été appliquées pour la détection d'intrusion. Ces algorithmes d'apprentissage en profondeur proposés ont des performances différentes en fonction des ensembles de données et des fonctionnalités sélectionnés entrée. Cependant, l'utilisation des mêmes méthodes et techniques d'apprentissage ne garantit pas toujours les mêmes résultats d'un cours à l'autre, différentes attaques possibles.

# Chapitre 04 :
# Implémentation du système

# 1. Introduction

Dans ce chapitre nous présentons une application réalisée sur la base du modèle proposé dans le chapitre précédent, pour la détection d'attaque dans IoT utilisant DL. Nous commençons le chapitre par l'introduction l'environnement de programmation, le choix du langage de programmation, avant de passer, par la suite, à la description de l'application, et à l'exposé des différents résultats des expérimentations menées. Nous terminons le chapitre par une analyse et une discussion des résultats obtenus.

# 2. Python

Python est un langage de programmation open source créé par le programmeur Guido van Rossum, ça a été depuis 1991 (plus longtemps que Java), et est régulièrement dans le top 10 des plus populaires langages informatiques. Les gens sont payés pour écrire des programmes Python, des trucs sérieux qui que vous utilisez tous les jours, comme Google, YouTube, Dropbox, Netflix et Hulu. Je l'ai utilisé pour des applications de production aussi variées qu'un appareil de recherche de courrier électronique et un commerce électronique site Internet. Python a une réputation de productivité qui plaît aux organisations en évolution rapide. [95]

## ❖ Principales fonctionnalités de Python

- ✓ Python est l'un des langages les plus faciles à utiliser en programmation, et c'est ce qui en fait un langage très adapté aux débutants ;
- ✓ Il contient un ensemble de phrases simples et simples, ainsi que des mots simples en anglais ;
- ✓ La chose la plus importante qui le distingue est également que ses sources sont disponibles gratuitement et que vous n'avez pas besoin de payer pour les obtenir, leurs mises à jour sont également disponibles, et elles peuvent être obtenues et connaître les derniers développements qui les suivent ;
- ✓ Les programmeurs développent ce langage jour après jour ;
- ✓ Il est également très rapide dans le processus de développement de diverses applications.

## 3. Environnement de travail

Anaconda est une distribution libre et open source, c'est la plate-forme de distribution Python la plus populaire au monde avec plus de 20 millions d'utilisateurs dans le monde [96]. Il est utilisé pour la science des données, l'apprentissage automatique, l'apprentissage en profondeur, etc. Avec la disponibilité de plus de 300 bibliothèques pour la science des données adaptés pour Windows, Linux et MacOS, [97] il devient assez optimal pour tout programmeur de travailler sur anaconda pour la science des données. Anaconda aide à simplifier la gestion et le déploiement des packages. La figure 4.1 représente l'environnement Anaconda.

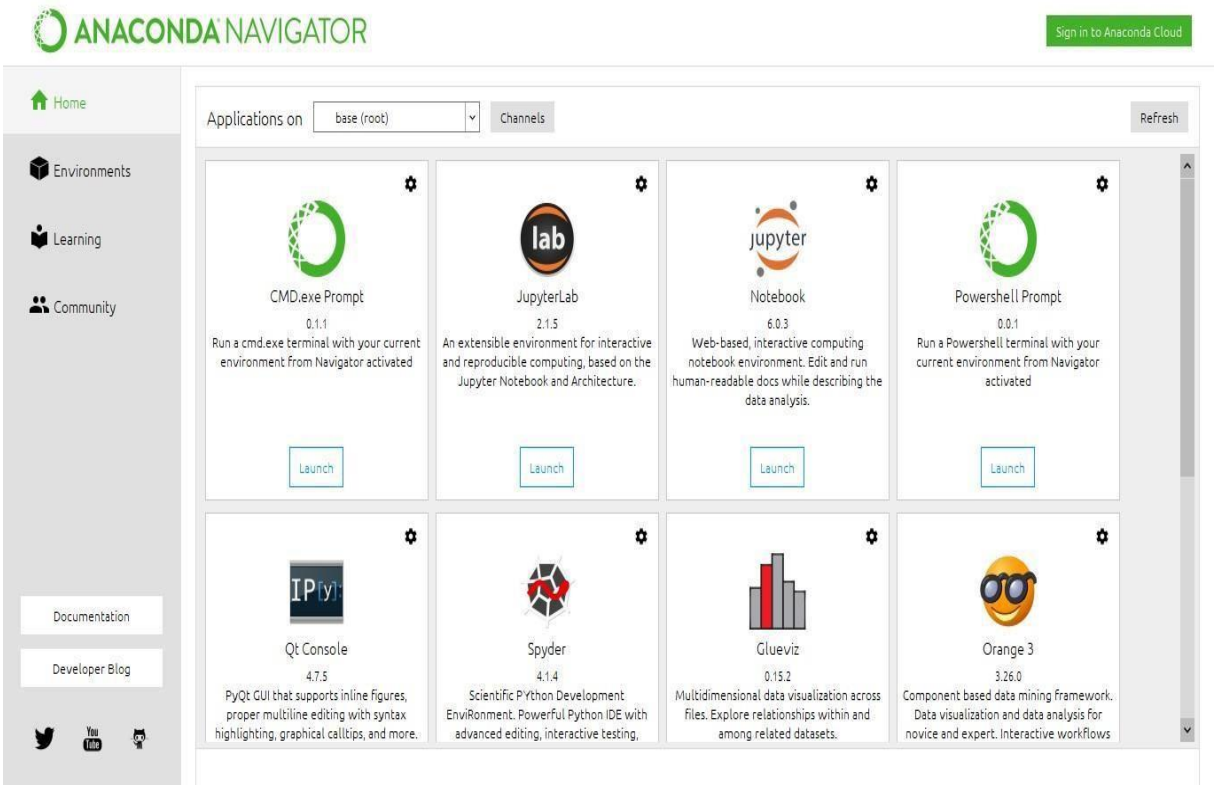



**Figure 4.1 :** Navigateur ANACONDA.

### 3.1. Spyder

Spyder est un environnement scientifique gratuit et open source écrit en Python, pour Python, et conçu par et pour des scientifiques, des ingénieurs et des analystes de données. Il présente une combinaison unique de fonctionnalité avancée d'édition, d'analyse, de débogage et de profilage d'un outil de développement compte avec l'exploration de données, l'exécution interactive, l'inspection approfondie et les belles capacités de visualisation d'un package scientifique. [98]

Pour notre système, nous avons utilisé l'éditeur Spyder (Python 3.9), qui est l'un des éditeurs offerts par Anaconda comme Jupyter et Notebook. La figure 4.2 représente la fenêtre de Spyder.

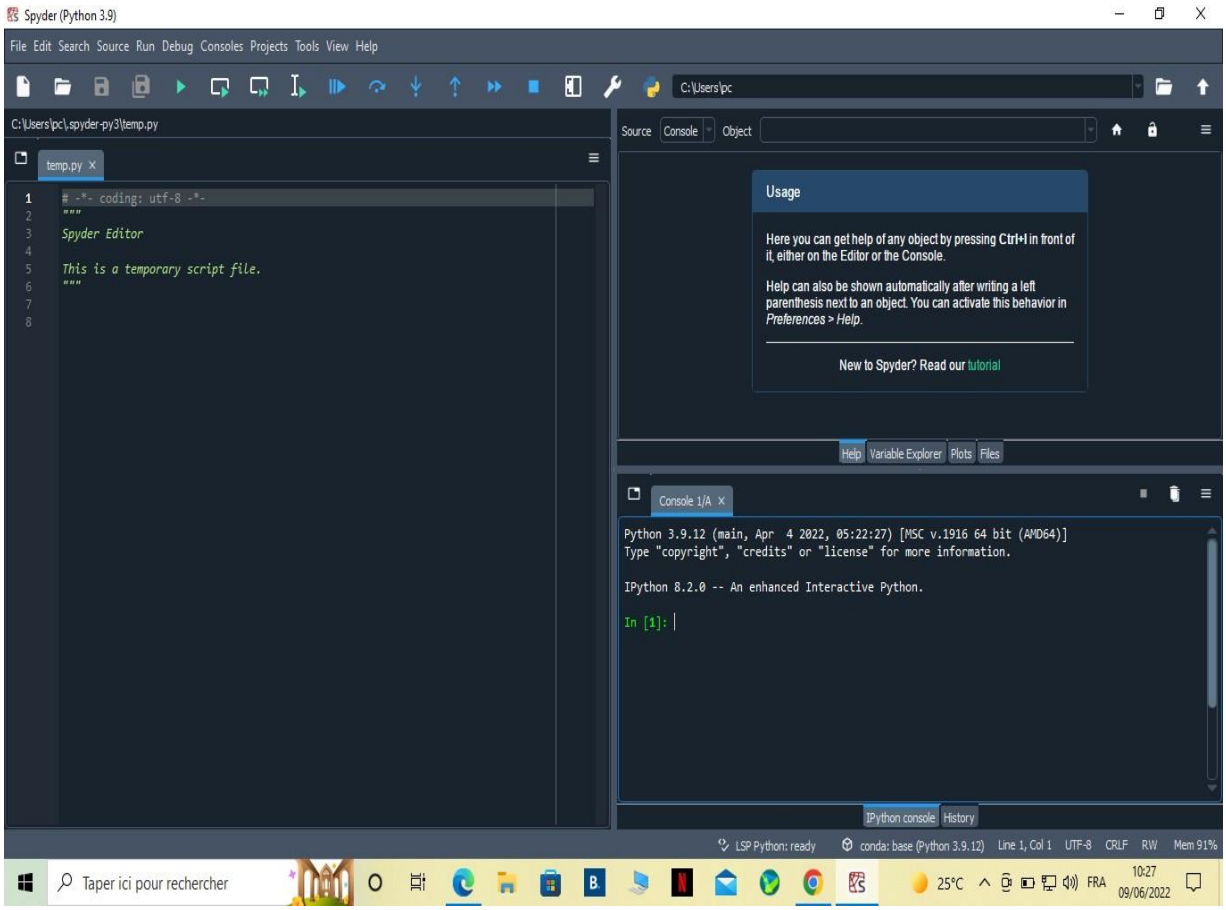



**Figure 4.2 :** Fenêtre de Spyder.

### 3.2. Google Colab

En utilise aussi Google Colab qui est également connu sous le nom de Collaboratory, est de plus en plus utilisé dans l'éducation et l'éducation, car cela. Le projet vise à diffuser l'enseignement et la recherche en apprentissage automatique (Randlesi Pasquetto, Golshan, & Borgman, 2017). Dans cette fonctionnalité, vous pouvez ajouter des blocs-notes, et vous pouvez ensuite commenter le code comme s'il était une sorte de Google Docs (outil d'édition de texte de Google). En outre, les utilisateurs sont autorisés à collaborer et à partager ces bloquer et aider au développement de code développé dans le langage de programmation Python. [99]

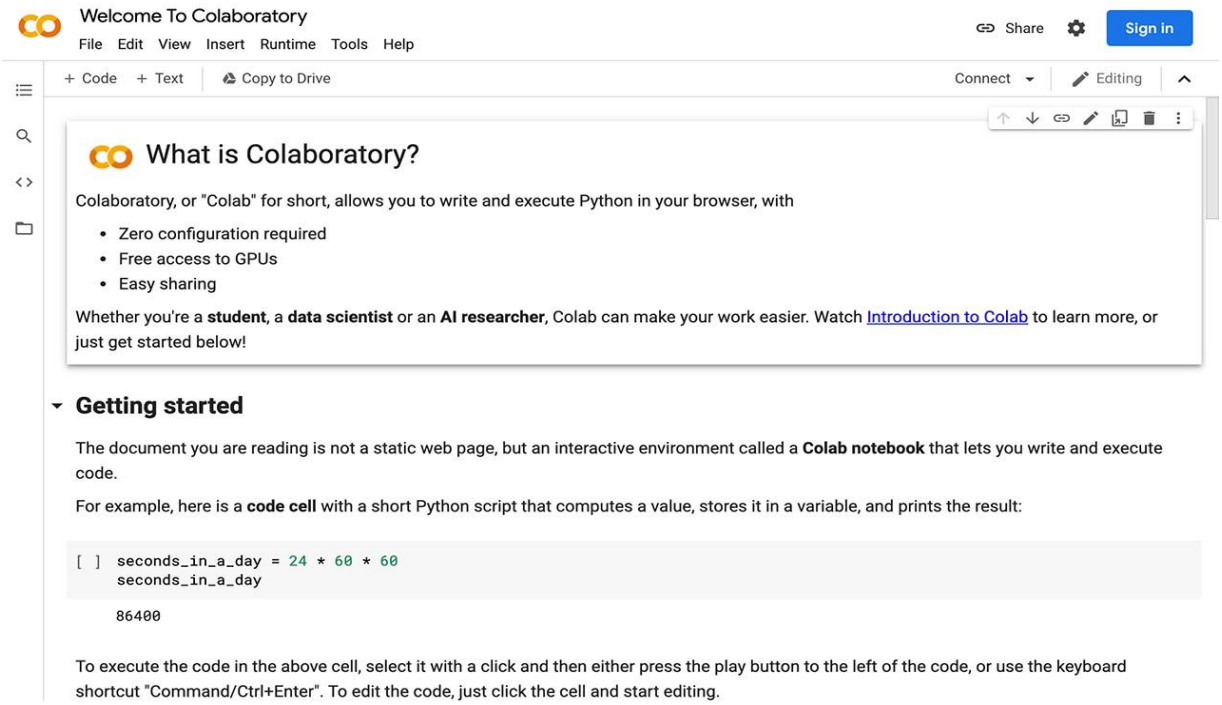



**Figure 4.3 :** Représentation de Colab.

Les caractéristiques de la machine sur laquelle le modèle est implémenté et testé sont résumées dans le tableau suivant :

| Composantes | Valeurs |
|---|---|
| **Processeur** | Intel® Core(TM) i3-6006U CPU @ |
| **Nome de l'ordinateur** | LAPTOP-56JUATBH |
| **Fréquence de processeur** | 2.00GHZ |
| **Mémoire** | 4.00 GO |
| **Système d'exploitation** | Windows 10 – 64 bits |

**Tableau 4.1 :** Spécifications techniques de l'ordinateur utilisé pour les expérimentations.

## 4. Résultats et discussions

Dans le processus d'évaluation, l'exactitude de la classification et d'autres des mesures ont été utilisées pour montrer l'efficacité de notre système par rapport aux modèles peu profonds dans l'IoT distribué au niveau du brouillard. La comparaison de la formation distribuée à l'approche centralisée dans l'exactitude est également l'un de nos critères d'évaluation.

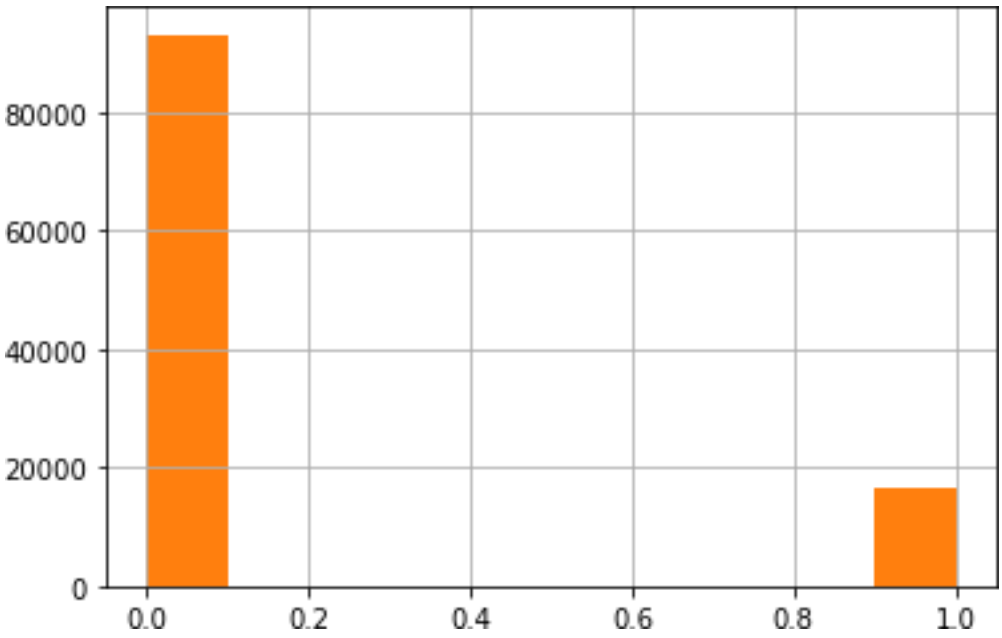



**Figure 4.4 :** Distribution du flux entre attaque DoS et normal.

| Layer(Type) | Output Shape | Param # |
|---|---|---|
| dense_15 (Dense) | (None, 50) | 2250 |
| dense_15 (Dense) | (None, 30) | 1530 |
| dense_17 (Dense) | (None, 25) | 775 |
| dense_18 (Dense) | (None, 20) | 520 |
| dense_19 (Dense) | (None, 2) | 42 |

**Tableau 4.2 :** Paramètre des dense RNN.

| Layer(Type) | Output Shape | Param # |
|---|---|---|
| lstm (LSTM) | (None, 44, 40) | 6720 |
| lstm_1 (LSTM) | (None,10) | 2040 |
| dropout (Dropout) | (None, 10) | 0 |
| dense_9 (Dense) | (None, 5) | 55 |
| dense_10 (Dense) | (None, 1) | 6 |

**Tableau 4.3 :** Paramètre des dense LSTM.

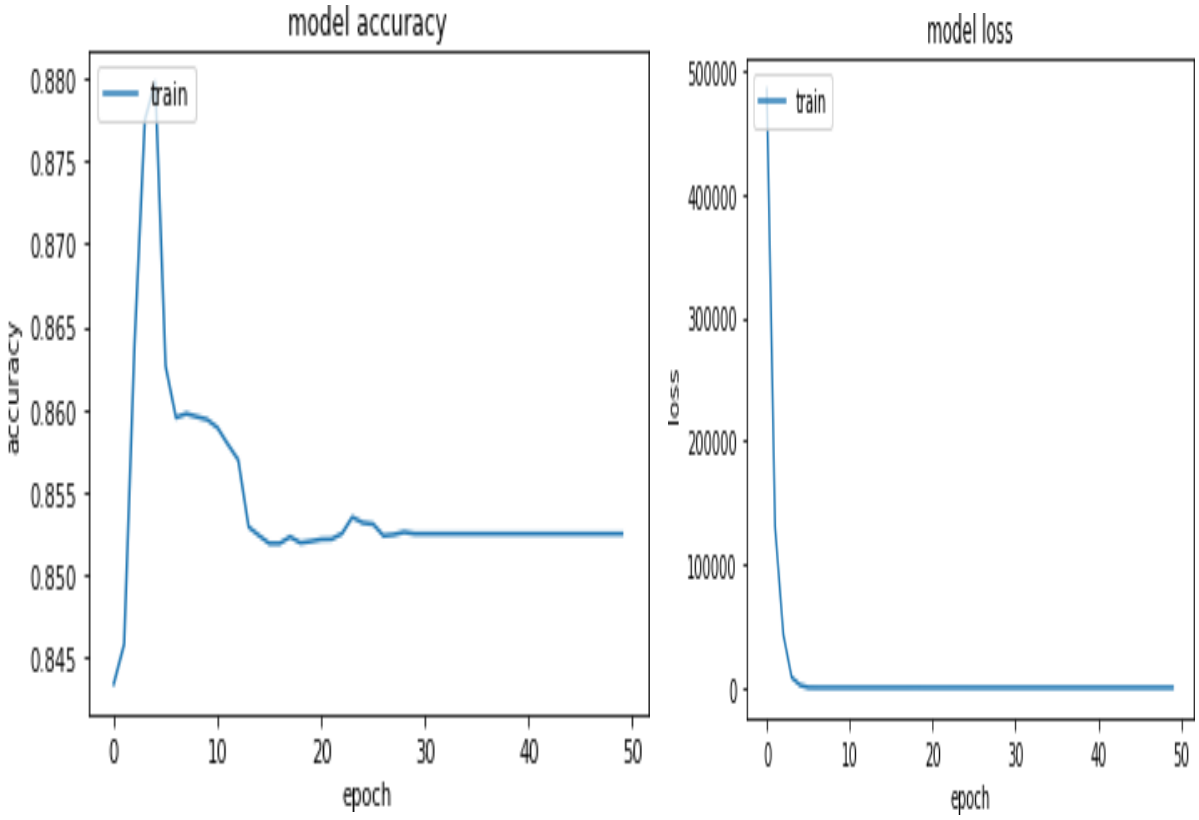



**Figure 4.5 :** Représentation de training accuracy, loss de ANN

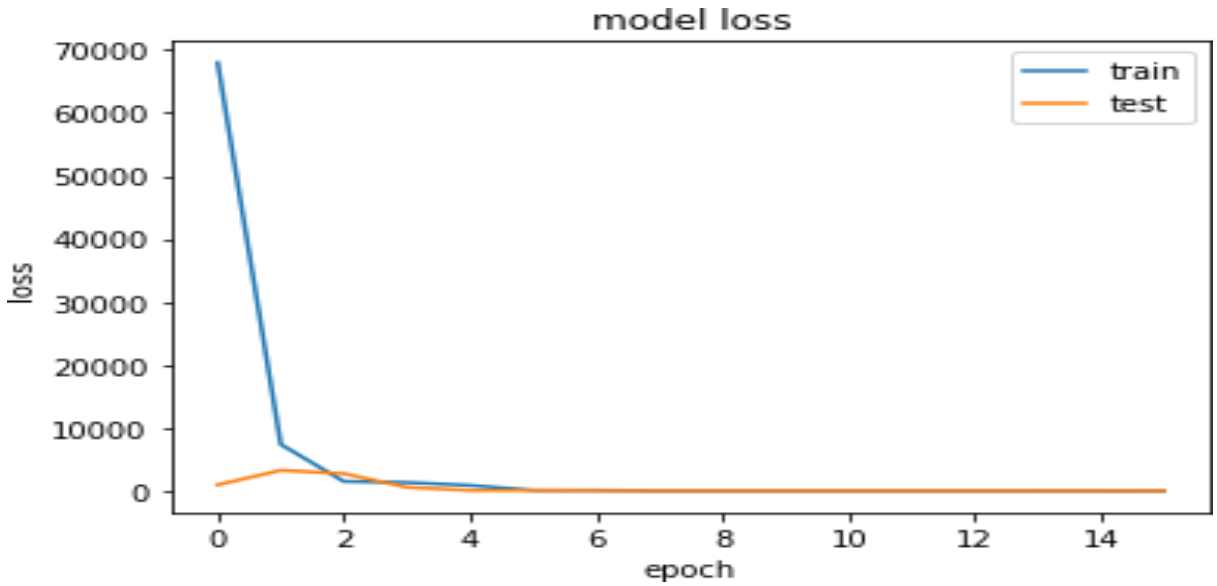



**Figure 4.6:** Train/test loss de RNN.

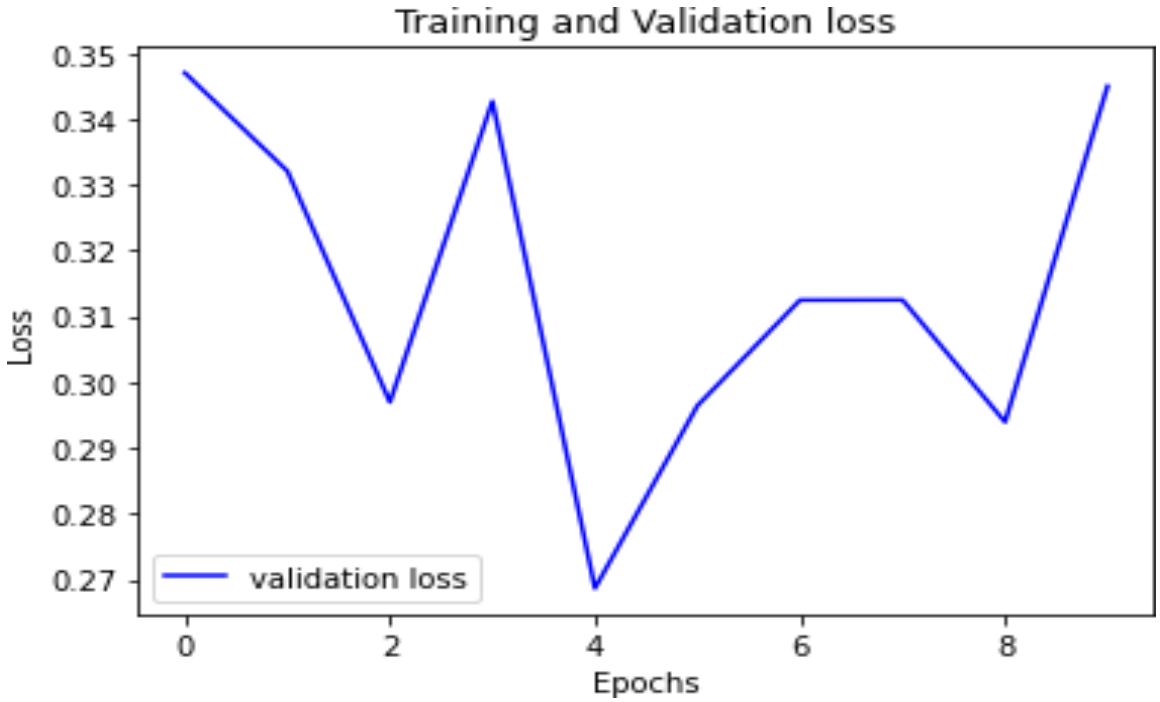



**Figure 4.7:** validation loss de RNN.

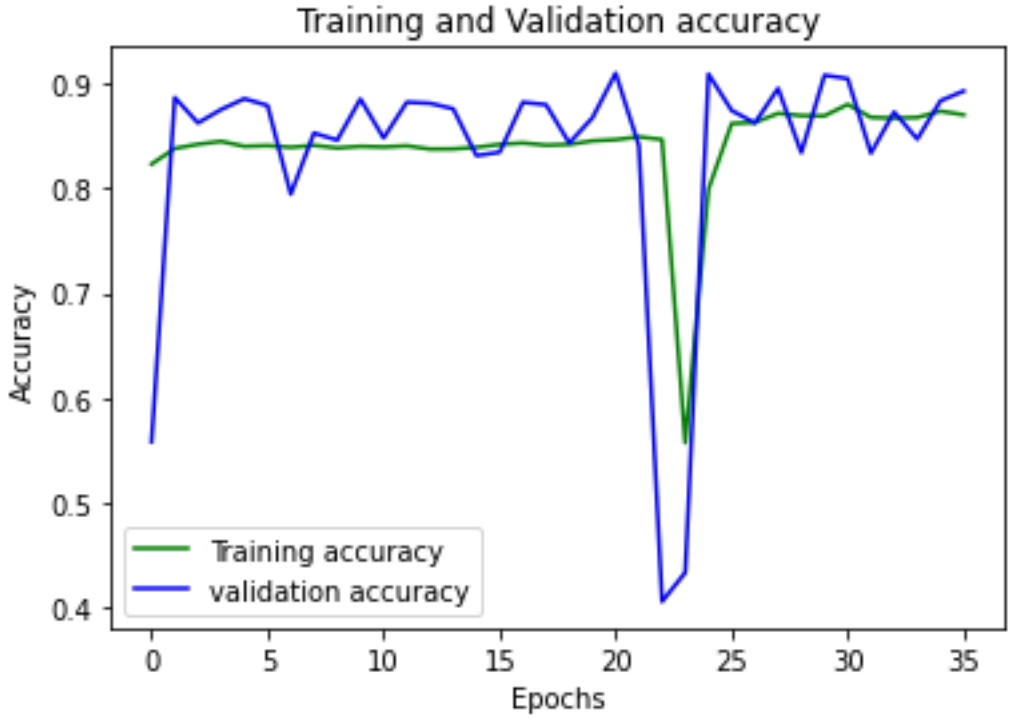



**Figure 4.8 :** Train/validation précision de RNN.

La figure 4.8 représente le graphique de le score de précision de la formation par rapport à accuracy de la validation sur le nombre d'époques.

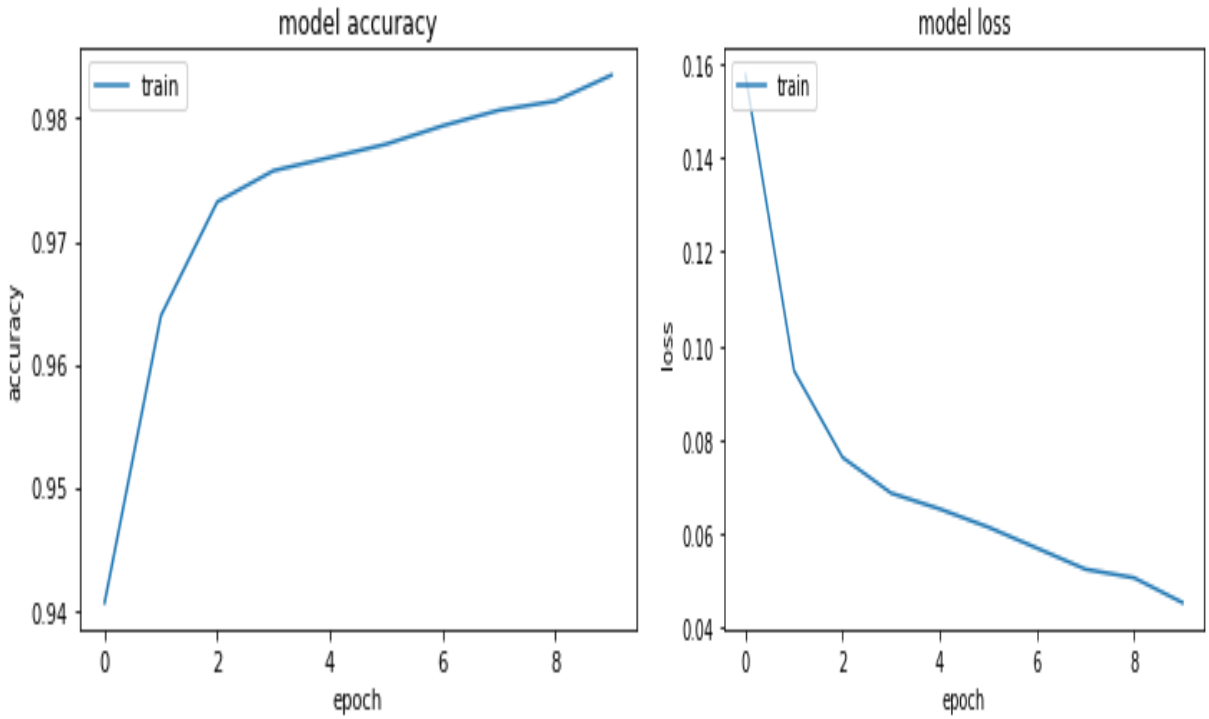



**Figure 4.9 :** Représentation loss, accuracy modèle de LSTM.

| Classifier | Accuracy | F1_Score | Train Time | Test Time |
|---|---|---|---|---|
| **ANN** | 85.10 | 0.78 | 203.86 | 2.18 |
| **RNN** | 88.59 | 0.89 | 62.54 | 1.75 |
| **MLP** | 90.20 | 0.9 | 107.65 | 0.02 |
| **LSTM** | 85.17 | 0.78 | 3124.02 | 924.83 |
| **DT** | 99.26 | 0.99 | 36.47 | 0.35 |
| **NB** | 87.13 | 0.87 | 97.78 | 0.02 |
| **RF** | 99.58 | 0.99 | 135.40 | 0.04 |
| **GB** | 97.05 | 0.96 | 145.38 | 0.02 |

**Tableau 4.4 :** Comparaison des performances des classificateurs sélectionnés utilisant UNSW-NB15 dataset avec train test split méthode.

Les résultats de tableau 4.4 montrent que le classificateur RF est meilleur que les autres classificateurs sur l'ensemble de données UNSW en fonction des paramètres sélectionnés. La précision du classificateur RF est de 99,58%.

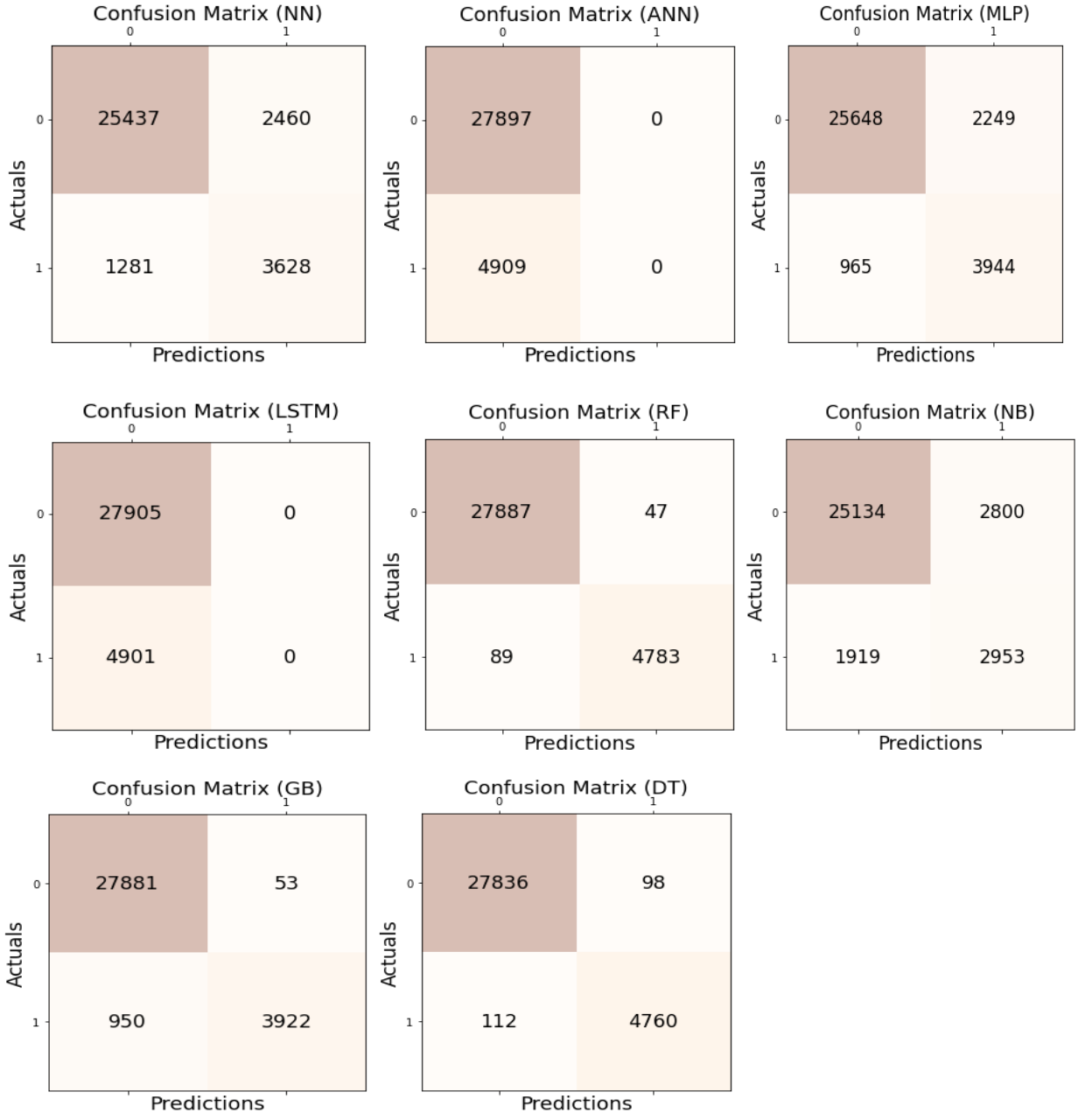



**Figure 4.10 :** Matrice de confusion représentant les prédictions par rapport aux donnéesréelles sur les données de test.

## 5. Conclusion

Dans ce chapitre, nous avons présenté les résultats des différentes expérimentations de notre système de détection, en utilisant UNSW-NB15 dataset pour la détection des attaques DoS.

À l'avenir, ce travail pourra être étendu aux attributs sélectifs et à la classification multi classe pour la détection d'intrusion.

Le score de précision (Accuracy) est utilisé pour mesurer les performances du modèle en termes de mesure du rapport de la somme des vrais positifs et des vrais négatifs sur toutes les prédictions faites.

Le score F1 est une moyenne harmonique de la précision et du score de rappel et est utilisé comme mesure dans les scénarios où le choix du score de précision ou de rappel peut entraîner un compromis en termes de modèle donnant respectivement des faux positifs et des faux négatifs élevés.

# Conclusion générale

# 1. Conclusion

En conclusion, nous fournissons un bref résumé de tout ce qui est développé dans cette lettre qui vise à réaliser un système de détection d'attaques basé sur l'analyse comportementale.

Au début, nous avons présenté un aperçu de l'Internet des objets, de son importance et du danger auquel il est exposé par le biais d'attaques électroniques. Par conséquent, les attaques électroniques ciblent ces appareils dans la plupart des cas, sauf pour des raisons de sécurité et de confidentialité, en raison à la nature de l'Internet des objets.

Dans cette mémoire, notre travail est important car la technologie d'apprentissage en profond proposé peut être utilisée pour permettre aux appareils IoT de se protéger dans son environnement dynamique et ad hoc.

# 2. Travaux futurs et perspectives

Avant de clôturer ce mémoire, nous tenons à donner certaines perspectives qui peuvent faire suite de ce travail :

- ✓ Utiliser un Dataset contenant un plus grand nombre de fichiers.
- ✓ Introduire d'autres types d'attributs tels que les chaines de caractères.
- ✓ Dans ce travail, nous avons utilisé que les classifieurs alors qu'il existe d'autre méthodes peuvent être utilisé pour combiner les classifieurs comme OneagainstOne ou OneagainstAllet qui peuvent mener à une meilleure précision.
- ✓ Utiliser d'autres méthodes pour se protéger contre les attaques comme l'apprentissage autodidacte, IDS hybride, SVM…etc.

# Bibliographies


[1] Kumar Pani, Santosh (2021). Internet of Things: Enabling Technologies, Security and Social Implications (-98-1158620-9, 978--98-1158620-0). Singapore: Springer Singapore.

[2] Kevin Ashton, "That 'Internet of Things' Thing", RFID Journal, 22 June 2009. https://www.ida.gov.sg/~/media/files/infocomm%20Landscape/Technology/TechnologyRoadmap/InternetOfThings.pdf.

[3] Livre Blanc . Préparer la Révolution de l‟Internet des Objets Document No 1 – Une cartographie des enjeux. 7 novembre 2016, (PDF , 46 p).

[4] (en) Anonyme. 2008. Internet of Things in 2020. Roadmap for the Future, 1.1 ed.: 27: Infso D.4 Networked Enterprise & RFID; Infso G.2 Micro & Nanosystems in co-operation with the working group RFID of the EPOSS. p. 4.

[5] S. Le Pallec, http://2005.jres.org/paper/70.pdf.

[6] E. Siow, Efficient querying for analytics on Internet of Things databases and streams. PhD thesis, University of Southampton, UK, 2018 .

[7] DAVE, Evans. L'Internet des objets Comment l'évolution actuelle d'Internet transforme-t-elle le monde ?. Avril 2011, 12 p. (Cisco Internet Business Solutions Group (IBSG)).

[8] https://www.synox.io/actualites-sectorielle/4-choses-a-savoir-sur-linternet-des-objets/

[9] https://wikimemoires.net/2019/09/domaines-d-applications-de-l-iot/

[10] N. Suma, S.R. Samson, S. Saranya, G. Shanmugapriya, R. Subhashri, IOT based smart agriculture monitoring system. Int. J. Recent Innov. Trends Comput. Commun. 5(2), 177–181 (2017).

[11] ITUT Rec. Y. 2060 (06/2012),". Overview of the Internet of things (IoT)," June, 2012.

[12] Matthias Thoma ; Sonja Meyer ; Klaus Sperner ; Stefan Meissner ; Torsten Braun ," On IoT-services: Survey.

[13] Classification and Enterprise Integration ", IEEE International Conference on Green Computing and Communications, INSPEC Accession Number: 13372142, Besancon, France , Nov. 2012.

[14] Bruno Dorsemaine ; Jean-Philippe Gaulier ; Jean- Philippe Wary ; Nizar Kheir ; Pascal Urien ," Internet of Things: A Definition & Taxonomy", 9th International Conference on Next Generation

Mobile Applications, Services and Technologies, IEEE, Print ISBN: 978-1-4799-8660-6 , Cambridge, UK, Sept. 2015, DOI: 10.1109/NGMAST.2015.71.

[15] A. H. Mohd Aman et al.: Survey on Trend and Classification of IoT Reviews.

[16] ROXIN, I., BOUCHEREAU A., "Ecosystème de l'Internet des Objets", dans Bouhaï N. et Saleh I., (dir.) "Internet des objets : Evolutions et Innovations ", ISTE Editions Londres, Mai 2017 p. 73 .

[17] Feng Chen, Changrui Ren , Jin Dong , Qinhua Wang , Jinfeng Li , Bing Shao ," IEEE International Conference on Web Services", INSPEC Accession Number: 12219345, Washington, DC, USA, July 2011.

[18] Simon Jiang," Fifteenth International Conference on Advances in ICT for Emerging Regions (ICTer)", IEEE, INSPEC Accession Number: 15700870, Colombo, Sri Lanka, Aug. 2015.

[19] Mark Coates, Mike Rabbat, "Sensor Networks Part 2: ZigBee and IEEE 802.15.4".

[20] D. Martin-Sacristan, J. F. Monserrat, J. Cabrejas-Peñuelas, D. Calabuig, S. Garrigas, N; Cardona, "On the Way Towards Fourth-generation Mobile: 3GPP LTE and LTE-advanced", EURASIP Journal on Wireless Communicationsand Networking, pp. 4:1-4:10, Mar. 2009.

[21] Yusuf Perwej , Kashiful H., Uruj J., Sharad S., "Some drastic improvements found in the analysis of routing protocol for the Bluetooth technology using scatternet" International Conference on Computing, Communications and Information Technology Applications (CCITA-2010) , Ubiquitous Computing and Communication Journal (UBICC) Seoul, South Korea, ISSN Online 1992-8424, ISSN Print 1994-4608, Volume CCITA-2010, Number 5, pages 86-95, 2010;

[22] R. Want, "Enabling Ubiquitous Sensing with RFID", Computer, vol. 37, no. 4, pp. 84-86, 2004.

[23] Leong et al., the Sun EPC network architecture a technical white paper, 2004.

[24] A. C. W. Wong, M. Dawkins, G. Devita, N. Kasparidis, A. Katsiamis, O. King, F. Lauria, J. Schiff, A. J. Burdett, "A 1 V 5 mA multimode IEEE 802.15.6/Bluetooth lowenergy WBAN transceiver for biotelemetry applications", IEEE J. Solid-State Circuits, vol. 8, no. 1, pp. 186-198, 2013.

[25] F. Lassabe, P. Canalda, P. Chatonnay, F. Spies, "Indoor Wi-Fi positioning: techniques and systems" in Annals of Telecommunications, Paris:Springer, vol. 64, no. 9, pp.651-664, 2009.

[26] Arampatzis, T., et al. (2005) A Survey of Security Issues in Wireless Sensors Networks, in Intelligent Control. Pro-ceeding of the IEEE International Symposium on, Mediterrean Conference on Control and Automation, 719-724.

[27] Richard Boire,"Artificial intelligence (AI), automation, and its impact on data science", IEEE International Conference on Big Data (Big Data), Boston, MA, USA, Dec. 2017.

[28] Felix von Reischach ; Stephan Karpischek ; Florian Michahelles ; Robert Adelmann ," Internet of Things (IOT)", Tokyo, Japan, Dec. 2010, DOI: 10.1109/IOT.2010.5678457.

[29] Yusuf Perwej , Firoj Parwej, "A Neuroplasticity (Brain Plasticity) Approach to Use in Artificial Neural Network", International Journal of Scientific & Engineering Research (IJSER), France , Vol.3, Issue 6, June 2012, Pages 1- 9, ISSN 2229 – 5518. DOI: 10.13140/2.1.1693.2808.

[30] J. Shi, J. Wan, H. Yan, H. Suo, A survey of cyber-physical systems, in IEEE International Conference on Wireless Communications and Signal Processing (2011).

[31] https://www.lirmm.fr/~seriai/uploads/Enseignement/iot.pdf.

[32] Shaker Alanazi, Jalal Al-Muhtadi, Abdelouahid Derhab, Kashif Saleem, Afnan N. AlRomi, Hanan S. Alholaibah, Joel J.P.C. Rodrigues, On resilience of Wireless Mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications, in: 2015 17th International Conference on E-Health Networking, Application & Services, HealthCom, IEEE, 2015, pp. 205–210.

[33] Nimbalkar, P., & Kshirsagar, D. (2021). Feature selection for intrusion detection system in internet-of-things (iot). ICT Express, 7(2), 177-181.

[34] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, ``Machine learning-based network vulnerability analysis of industrial Internet of Things," IEEE Internet Things J., vol. 6, no. 4, pp. 6822_6834, 2nd Quart., 2019.

[35] H. Lin, Z. Yan, Y. Chen, and L. Zhang,``A survey on network security-related data collection technologies," IEEE Access, vol. 6, pp. 18345_18365, 2018.

[36] B. Pourghebleh, K.Wakil, and N. J. Navimipour, ``A comprehensive study on the trust management techniques in the Internet of Things," IEEE Internet Things J., vol. 6, no. 6, pp. 9326_9337, 2019.

[37] V. Nguyen, P. Lin, and R. Hwang, ``Energy depletion attacks in low power wireless networks," IEEE Access, vol. 7, pp. 51915_51932, 2019.

[38] https://blog.netwrix.fr/2018/07/04/les-10-types-de-cyberattaques-lespluscourants/#Attaques%20phishingq%20etspear%20phishing.

[39] H. Ning and H. Liu, "Cyber-Physical-Social Based Security Architecture for Future Internet of Things," Adv. Internet Things, vol. 02, no. 01, pp. 1–7, 2012, doi: 10.4236/ait.2012.21001.

[40] A. Roohi, M. Adeel, and M. Ali Shah, "DDoS in IoT: A Roadmap Towards Security & Countermeasures," in DDoS in IoT: A Roadmap Towards Security & Countermeasures, 2019, no. September, pp. 5–7.

[41] P. Rani and G. S. Lakshmi, "IoT Vulnerabilities and Security," vol. 2, no. 6, pp. 1–3, 2017, [Online].

Available
http://www.ijasret.com/VolumeArticles/FullTextPDF/166_IJASRET_IoT_Vulnerabilities_and_Security.pdf;
[42] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, “Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models: A Survey,” IEEE Commun. Surv. Tutorials, vol. 18, no. 4, pp. 2546–2590, 2016, doi: 10.1109/COMST.2016.2582841.
[43] I. Cvitić, M. Vujić, and S. Husnjak, “Classification of security risks in the iot environment,” Ann. DAAAM Proc. Int. DAAAM Symp., vol. 2015-Janua, no. 2016, pp. 731–740, 2015, doi: 10.2507/26th.daaam.proceedings.102.
[44] O. El Mouaatamid, M. Lahmer, and M. Belkasmi, “Internet of Things Security : Layered classification of attacks and possible Countermeasures,” Electron. J. Inf. Technol., no. 9, pp. 66–80, 2016.
[45] N. Hossein, “Frequency Hopping Spread Spectrum: An Effective Way to Improve Wireless Communication Performance,” Adv. Trends Wirel. Commun., 2011, doi: 10.5772/15482.
[46] J. Y. Khan, “Introduction to IoT,” Internet of Things (IoT), no. January 2019, pp. 1–24, 2019, doi: 10.1201/9780429399084-1.
[47] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, “PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications,” Int. J. Distrib. Sens. Networks, vol. 2014, 2014, doi: 10.1155/2014/357430.
[48] L. Hu et al., “Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things,” IEEE Internet Things J., vol. 5, no. 1, pp. 219–228, 2018, doi: 10.1109/JIOT.2017.2778185.
[49] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, “Securing the Internet of Things (IoT): A Security Taxonomy for IoT,” Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018, no. August, pp. 163–168, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00034.
[50] K. Somasundaram and K. Selvam, “IOT – Attacks and Challenges,” Int. J. Eng. Tech. Res., vol. 8, no. 9, pp. 9–12, 2018, doi: 10.31873/ijetr.8.9.67.
[51] K. Sonar and H. Upadhyay, “A survey on ddos in Internet of Things,” Int. J. Eng. Res. Dev., vol. 10, no. 11, pp. 58–63, 2014.
[52] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, “Secure communication for the Internet of Things-a comparison of link-layer security and IPsec for 6LoWPAN,” Secur. Commun. Networks, vol. 7, no. 12, pp. 2654–2668, 2014, doi: 10.1002/sec.406.

[53] S. Kraijak and P. Tuwanut, “A SURV EY ON INTERNET OF THINGS A RCHITECTURE , PROTOCOLS , POSSIBLE A PPLICATIONS , SECURITY , PRIVA CY , REAL-WORLD IMPLEMENTATION A ND,” pp. 26–31, 2015.

[54] H. Shafagh, A. Hithnawi, A. Dröscher, S. Duquennoy, and W. Hu, “Poster: Towards encrypted query processing forn the Internet of Things,” in MobiCom '15: Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, September 2015, New York: Association for Computing Machinery, 2015, pp. 251–253.

[55] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. K. Bashir, “A survey of security and privacy issues in the Internet of Things from the layered context,” arXiv, no. March, 2019;

[56] R. Khader and D. . Eleyan, “Survey of DoS/DDoS attacks in IoT”, Sustainable Engineering and Innovation, vol. 3, no. 1, pp. 23-28, Jan. 2021.

[57] K. Mandal, M. Rajkumar, P. Ezhumalai et al., Improved security using machine learning for IoT intrusion detection system, Materials Today: Proceedings, https://doi.org/10.1016/j.matpr.2020.10.187.

[58] A. Raven, B. Jacob, D. Adam, C. F. James, K, Toby, R. Michael, Snort 2.1 Intrusion Detection, Syngress second edition, ISBN-13: 978-1931836043, (juin 2004).

[59] https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos.

[60] https://www.ya-graphic.com/wordpress-exploite-pour-des-attaques-par-ddos-layer-7/.

[61] Lescop Yves. «La sécurité informatique.1. Principes de la sécurité ». 2007.

[62] https://datascientest.com/machine-learning-tout-savoir.

[63] M.F. Mridha, M.A. Hamid, M. Asaduzzaman, ‘‘Issues of Internet of Things (IoT) and an intrusion detection system for IoT using machine learning paradigm”. In Proceedings of International Joint Conference on Computational Intelligence, (2020)395-406). Springer, Singapore.

[64] S. Zeadally, M. Tsikerdekis, ‘‘Securing Internet of Things (IoT) with machine learning”. International J. Commun. Syst., 33(1)(2020) e4169.

[65] https://iotworlds.com/fr/what-is-the-role-of-machine-learning-in-iot/.

[66] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, X. Bellekens, ‘‘Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study”. arXiv preprint arXiv:2006.15340, 2020 .

[67] https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service.

[68] J.P. Anderson, Computer Security Threat Monitoring and Surveillance, Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, (1980).

[69] Bouzayani, Hatem (2012). Modèle quantitatif pour la détection d'intrusion : une architecture collaborative IDS-HONEYPOT. Mémoire. Gatineau, Université du Québec en Outaouais,

Département d'informatique et d'ingénierie, p. 30 https://di.uqo.ca/id/eprint/508/.

[70] K. Sonar, H. Upadhyay, ‘‘An approach to secure Internet of Things against DDOS”, In Springer proceedings of international conference on ICT for sustainable development, (2016) 367–376.

[71] R. SaiSindhuTheja and G. K. Shyam, "An efficient Metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment", Appl. Soft Comput., vol. 100, Mar. 2021.

[72] S. Sharma, A. Gupta and S. Agrawal, "An intrusion detection system for detecting denial-of-service attack in cloud using artificial bee colony", Proc. Int. Congr. Inf. Commun. Technol, pp. 137-145, 2016.

[73] S. P. RM, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, et al., "An Effective Feature Engineering for DNN using Hybrid PCA-GWO for Intrusion Detection in IoMT Architecture", Computer Communications, vol. 160, pp. 139-149, 2020.

[74] J. Roldán, J. Boubeta-Puig, J. L. Martínez and G. Ortiz, "Integrating Complex Event Processing and Machine Learning: An Intelligent Architecture for Detecting IoT Security Attacks", Expert Systems with Applications, vol. 149, pp. 113251, 2020.

[75] E. Ciklabakkal, A. Donmez, M. Erdemir, E. Suren, M. K. Yilmaz and P. Angin, "ARTEMIS: An Intrusion Detection System for MQTT Attacks in Internet of Things", Proceedings of the 38th Symposium on Reliable Distributed Systems (SRDS), pp. 369-3692, 2019.

[76] A. Shokuh Saljoughi, M. Mehrvarz and H. Mirvaziri, "Attacks and intrusion detection in cloud computing using neural networks and particle swarm optimization algorithms", Emerg. Sci. J., vol. 1, no. 4, pp. 179-191, Jan. 2018.

[77] A. Nazir and R. A. Khan, "A novel combinatorial optimization based feature selection method for network intrusion detection", Comput. Secur., vol. 102, Mar. 2021.

[78] M. Mayuranathan, M. Murugan and V. Dhanakoti, "Best features based intrusion detection system by RBM model for detecting DDoS in cloud environment", J. Ambient Intell. Hum. Comput., vol. 12, no. 3, pp. 3609-3619, 2019.

[79] A. Fatani, M. Abd Elaziz, A. Dahou, M. A. A. Al-Qaness and S. Lu, "IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization," in IEEE Access, vol. 9, pp. 123448-123464, 2021, doi: 10.1109/ACCESS.2021.3109081

[80] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems", IEEE Access, vol. 8, pp. 165130-165150, 2020.

[81] Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Shabtai A, Breitenbacher D, Elovici Y. N-

baiot network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Comput. 2018;17(3):12–22.

[82] Yuan X, Li C, Li X. DeepDefense: Identifying DDoS attack via deep learning. In: 2017 IEEE international conference on smart compting (SMARTCOMP), Hong Kong; 2017. Pp. 1-8. https://doi.org/10.1109/SMARTCOMP.2017.7946998.

[83] Ibitoye O, Shafiq O, Matrawy A. Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks. In: IEEE global communications conference (GLOBECOM). IEEE. 2019; 2019. pp. 1–6.

[84] B. Kaluza, Machine Learning in Java. 2016.

[85] Li Deng. A tutorial survey of architectures, algorithms, and application for deep learning. APSIPA Transactions on Singal and Information Processing, 3, 2014;

[86] Hassan Hadi Al-Maksousy, Michel C Weigle, and Cong Wang. Nids: Neural network based intrusion detection system. In 2018 IEEE International Symposium on Technologies for Homeland Security (HST), pages 1-6. IEEE, 2018;

[87] Yann LeCun et al. Generalization and network desing strategies. Connectionism in perspective, 19:143-155, 1989.

[88] Jiuxiang Gu, Zhenhua Wang, Jason Kuen, Lianyang Ma, Amir Shahroudy, Bing Shuai, Ting Liu, Xingxing Wang, Gang Wang, Jianfie Cai, et al. Recent advances in convolutional neural networks. Pattern Recognition, 77 :354-377, 2018.

[89] Clément Dalloux, Natalia Grabar, and Vincent claveau. Détection de negation: corpus français et apprentissage supervise. Revue des Sciences et Technologies de l'Information-Séri TSI : Technique et Science Informatiques, pages 1-21, 2019.

[90]:https://www.analyticsvidhya.com/blog/2021/03/introduction-to-long-short-term-memory-lstm/ .

[91] Zeeshan, M., Riaz, Q., Bilal, M. A., Shahzad, M. K., Jabeen, H., Haider, S. A., & Rahim, A. (2021). Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets. IEEE Access, 10, 2269-2283.

[92] Ferrag, M.A., Shu, L., Djallel, H., Choo, K.-K.R., 2021. Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. Electronics 10 (11), 1257. doi: 10.3390/electronics10111257.

[93] AKGUN, D., HIZAL, S., & CAVUSOGLU, U. (2022). A New DDoS Attacks Intrusion Detection Model Based on Deep Learning for Cybersecurity. Computers & Security, 102748;

[94] N. Moustafa and J. Slay, ``UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in Proc. IEEE Military Commun. Inf. Syst.

Conf. (MilCIS), Nov. 2015, pp. 1_6.

[95] Python, R. (2019). Python. Python Releases for Windows, 24.

[96] "ANACONDA: Individual Edition", 2020, https://www.anaconda.com/products/individual.

[97] Christine Doig, "Anaconda for R users: SparkR and rBokeh", sur Developer Blog, Continuum Analytics, 1er février 2016.

[98] https://www.spyder-ide.org.

[99] Alves, F. R. V., & Vieira, R. P. M. (2019). The Newton fractal's Leonardo sequence study with the Google Colab. International Electronic Journal of Mathematics Education, 15(2), em0575.

# ANNEXE

Dans cette annexe, nous mettrons sous forme de images de notre système de détection des attaques Dos dans Iot :

### a. Mountez Google Drive sur Google Colab

```
from google.colab import drive
drive.mount('/content/drive')
```

### 2. Lire et extraire des informations de dataset

```
dftrain = pd.read_csv("/content/drive/MyDrive/UNSW-NB15-global.csv")
print('----------------------------------------Dataset information----------------------------------------')
display(pd.DataFrame(dftrain))
```

### 3. la formation et les tests de concaténation , le filtrage des données normales et dos, la suppression de la colonne d' étiquette

```
# Concatenation training and testing,filtiring normal and dos data,remove label columm
df = pd.concat([dftrain])
classes=dftrain['label']
classes.hist()

df=df.drop(columns=['label'])
print('--------------------number classes and size of each one---------------------')
print(' Number classes : ',dftrain['label'].value_counts().count())
print(dftrain['label'].value_counts())
classes=dftrain['label']

print('-----------------------------------dataset info-----------------------------')
df.info()
print('-------------------------null values-------------------------')
print(df.isnull().sum())
```

### 4. Créer un jeu de données d'entraînement.

```
cat_columns = df.select_dtypes(['category']).columns
df[cat_columns] = df[cat_columns].apply(lambda x: x.cat.code)
x_columns = dftrain.columns.drop('label')
x = dftrain[x_columns]
y = dftrain['label']

print("---------------Ready to generate train and test dataset---------------")
x_train, x_test, y_train, y_test = train_test_split(x, y, test_size=0.3, random_state=4)

print("x_train, x_test, y_train, y_test" + str(x_train.shape) + "" +str(y_train.shape) +
      "" +str(x_test.shape) + "" + str(y_test.shape))
```

## 5. Méthode pour la comparaison des performances

### 5.1 Artificial Neural Networks

```
ANN_model = Sequential()
ANN_model.add(Dense(32, input_dim=44, activation='relu'))
ANN_model.add(Dense(12, activation='relu'))
ANN_model.add(Dense(6, activation='relu'))
ANN_model.add(Dense(1,activation='sigmoid'))
ANN_model.summary()
print("---------------Starting ANN---------------")
start = time.time()
ANN_model.compile(loss='binary_crossentropy',optimizer='adam',metrics=['accuracy'])
monitor = EarlyStopping(monitor='val_loss', min_delta=1e-3, patience=5, verbose=1, mode='auto')
#Fitting ANN
ANN_History=ANN_model.fit(x_train,y_train,batch_size=32,epochs = 50)
end = time.time()
diff = end-start
print("Training time: " + str(diff))
starttest = time.time()
y_pred_ANN = ANN_model.predict(x_test)
y_pred_ANN = np.argmax(y_pred_ANN,axis=1)
endtest =time.time()
difftest = endtest-starttest
print("Test time: " + str(difftest))

print("Artificial Neural network, accuracy: " + str(metrics.accuracy_score(y_test, y_pred_ANN)) +
      " F1 score:" + str(metrics.f1_score(y_test, y_pred_ANN,average='weighted')))
matrixANN = confusion_matrix(y_test,y_pred_ANN)
# Creating a dataframe for a array-formatted Confusion matrix,so it will be easy for plotting.
print(matrixANN)
```

### 5.2 Recurrent neural network

```
print("---------------Starting RNN---------------")
model = Sequential()
model.add(Dense(50, input_dim=x_train.shape[1], kernel_initializer='normal', activation='relu'))
model.add(Dense(30, input_dim=x_train.shape[1], kernel_initializer='normal', activation='relu'))
model.add(Dense(25, input_dim=x_train.shape[1], kernel_initializer='normal', activation='relu'))
model.add(Dense(20, kernel_initializer='normal'))
model.add(Dense(2,activation='sigmoid'))
model.compile(loss='sparse_categorical_crossentropy', optimizer='adam', metrics=['accuracy'])
monitor = EarlyStopping(monitor='val_loss', min_delta=1e-3, patience=5, verbose=1, mode='auto')
history = model.fit(x_train,y_train,validation_data=(x_test,y_test),callbacks=[monitor],verbose=2,epochs=50,batch_size=32)
end = time.time()
diff = end-start
print("Training time: " + str(diff))
starttest = time.time()
y_pred_NN = model.predict(x_test)
y_pred_NN = np.argmax(y_pred_NN,axis=1)
endtest =time.time()
difftest = endtest-starttest
print("Test time: " + str(difftest))
print(model.summary())

print("Neural network, accuracy: " + str(metrics.accuracy_score(y_test, y_pred_NN)) +
      " F1 score:" + str(metrics.f1_score(y_test, y_pred_NN,average='weighted')))
matrixNN = confusion_matrix(y_test,y_pred_NN)
print(matrixNN)
```

### 5. 3 Multi layer perceptron

```
print("--------------Starting MLP---------------")
model = MLPClassifier( max_iter=130, batch_size=32, alpha=1e-4,
                       activation = 'relu',solver='adam', verbose=10, tol=1e-4, random_state=None)
model.fit(x_train, y_train)
end = time.time()
diff=end-start
print("Training time: " + str(diff))
starttest = time.time()
y_pred_MLP = model.predict(x_test)
endtest =time.time()
difftest = endtest-starttest
print("Test time: " + str(difftest))
print("Multi Layer Perceptron, accuracy: " + str(metrics.accuracy_score(y_test, y_pred_MLP)) +
      " F1 score:" + str(metrics.f1_score(y_test, y_pred_MLP,average='weighted')))
matrixMLP = confusion_matrix(y_test,y_pred_MLP)
print(matrixMLP)
```

### 5.4 Decision tree

```
#Decision tree
print("---------------Starting Decision tree----------------")
clf = DecisionTreeClassifier()
clf = clf.fit(x_train,y_train)
end = time.time()
diff=end-start
print("Training time: " + str(diff))
starttest = time.time()
y_pred_dt = clf.predict(x_test)
y_pred_dt_roc = clf.predict_proba(x_test)
endtest =time.time()
difftest = endtest-starttest
print("Test time: " + str(difftest))
print("Decision Tree, accuracy: " + str(metrics.accuracy_score(y_test, y_pred_dt)) +
      " F1 score:" + str(metrics.f1_score(y_test, y_pred_dt,average='weighted')))
matrixdt = confusion_matrix(y_test,y_pred_dt)
print(matrixdt)
```

### 5.5 Random forest

```
#RandomForest
print("---------------Starting Random forest---------------")
classifier = RandomForestClassifier(verbose=2,random_state=None)
classifier.fit(x_train, y_train)
end = time.time()
diff=end-start
print("Training time: " + str(diff))
starttest = time.time()
y_pred_random = classifier.predict(x_test)
endtest =time.time()
difftest = endtest-starttest
print("Test time: " + str(difftest))
print("Random Forest, accuracy: " + str(metrics.accuracy_score(y_test, y_pred_random)) +
      " F1 score:" + str(metrics.f1_score(y_test, y_pred_random,average='weighted')))
matrixrf = confusion_matrix(y_test,y_pred_random)
print(matrixrf)
```

### 5.6 Gradient boost

```
#Gradient boost
print("---------------Starting Gradient boost---------------")
model = GradientBoostingClassifier(n_estimators=20, random_state=None,verbose=2)
model.fit(x_train, y_train)
end = time.time()
diff=end-start
print("Training time: " + str(diff))
starttest = time.time()
y_pred_gradient = model.predict(x_test)
endtest =time.time()
difftest = endtest-starttest
print("Test time: " + str(difftest))
print("GradienBoost, accuracy: " + str(metrics.accuracy_score(y_test, y_pred_gradient)) +
      " F1 score:" + str(metrics.f1_score(y_test, y_pred_gradient,average='weighted')))
matrixgb = confusion_matrix(y_test,y_pred_gradient)
print(matrixgb)
```

### 5.7 Long short-term memory

```
267  from keras.models import Sequential
268  from keras.layers import Dense
269  from keras.layers import LSTM
270  from keras.layers import Dropout
271  # Reshape data To use with LSTM
272  print("---------------Starting LSTM---------------")
273  data_size=(x_train.shape[1],x_train.shape[2])
274  LSTM_model = Sequential()
275  LSTM_model.add(LSTM(40,return_sequences = True , input_shape=data_size))
276  LSTM_model.add(LSTM(units=10, activation="relu"))
277  LSTM_model.add(Dropout(0.1))
278  LSTM_model.add(Dense(5, activation="relu"))
279  #model.add(Dropout(0.5))
280  LSTM_model.add(Dense(1, activation="sigmoid"))
281  LSTM_model.summary()
282  start = time.time()
283  LSTM_model.compile(optimizer = 'adam', loss = 'binary_crossentropy', metrics=['accuracy'])
284  LSTM_History = LSTM_model.fit(x_train,y_train,verbose=2,epochs=10,batch_size=32)
285  end=time.time()
286  print(end-start)
287  LSTM_model.evaluate(x_test, y_test, verbose=2)
288  LSTM_model.evaluate( x_train,y_train, verbose=2)
289
290  y_pred_LSTM = LSTM_model.predict(x_test)
291  y_pred_LSTM = np.argmax(y_pred_LSTM,axis=1)
292  endtest =time.time()
293  difftest = endtest-starttest
294  print("Test time: " + str(difftest))
295  print("LSTM, accuracy: " + str(metrics.accuracy_score(y_test, y_pred_LSTM)) +
296          " F1 score:" + str(metrics.f1_score(y_test, y_pred_LSTM,average='weighted')))
297  matrixLSTM = confusion_matrix(y_test,y_pred_LSTM)
298  # Creating a dataframe for a array-formatted Confusion matrix,so it will be easy for plotting.
299  print(matrixLSTM)
300
```

### 6. Créer un classificateur bayes naif

```
#Create Naive Bayes Classifier
print("---------------Starting Naive Bayes---------------")
gnb = GaussianNB()
gnb.fit(x_train, y_train)
end = time.time()
diff=end-start
print("Training time: " + str(diff))
starttest = time.time()
y_pred_nb = gnb.predict(x_test)
endtest =time.time()
difftest = endtest-starttest
print("Test time: " + str(difftest))
print("Naive Bayes, accuracy: " + str(metrics.accuracy_score(y_test, y_pred_nb)) +
      " F1 score:" + str(metrics.f1_score(y_test, y_pred_nb,average='weighted')))
matrixnb = confusion_matrix(y_test,y_pred_nb)
print(matrixnb)
```