الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي والبحث العلمي

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

جامعة 20 اوت1955- سكيكدة

UNIVERSITE 20 AOUT 1955- SKIKDA

Faculté des Sciences

Département d'informatique

Mémoire Présenté en Vue de l'Obtention du Diplôme de Master

Filière :MI

Spécialité:RSD

Intitulé :

SMA pour la détection d'intrusions D'IoT.

Sous la direction de :

DR. Cheikh Mohamed

Présenté par :

Boudheb Imane

Lakehal Abir

Année universitaire 2022/2023

Remerciement :

Avant tout, nous remercions Dieu de nous avoir donné la force et le courage pour réaliser ce travail modeste.

Nous tenons à remercier tout d'abord, le Dr. Mohamed Cheikh, de nous avoir proposé un tel intéressant sujet, pour son encadrement avec patience, ses Précieux conseils, sa disponibilité et son soutien tout au long de ce travail.

Nous remercions les membres de jury : de nous avoir fait l'honneur d'accepter de participer à nos jurys, et aussi ceux qui nous ont aidé à L'aboutissement de ce travail.

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

Mes remerciements à tous ceux qui m'ont aidé de près ou de loin…

Dédicaces

Avec l'aide et la protection D'ALLAH s'est réalisé ce travail ;

J'ai le grand plaisir de dédier ce modeste travail:

A la lumière de ma vie, la source de tendresse, ma première supporteur et mon amour éternelle, ma mère que j'adore Naima.

A mon très cher père Ahcene, pour ses encouragements, son soutien, et surtout pour son amour et son sacrifice afin que rien n'entrave le déroulement de mes études.

A ma sœur Yasmine, qui n'a pas cessé de m'encourager tout au cours de réalisation de ce travail.

A mes frères Oussama, Younes et Mohamed Mehdi.

A mon grand-père, ma grand-mère, mes oncles Kamel et Yassine et toute la famille.

A mes chères amies Miyada, Enfel, Imane et Abir. Merci pour tous les moments inoubliables et de m'a toujours encouragé et m'aimé.

Imane

Dédicaces

Nous remercions ALLAH tout puissant pour nous avoir donné la foi et éclairé. Notre chemin vers la réussite durant toutes nos années d'étude.

Je dédié ce mémoire qui est le fruit de nombreuses années d'étude à toutes les personnes qui ont participé de près et de loin pour mener à bien ce projet et

Plus particulièrement :

A ma mère, la plus belle femme dans le monde «Fatima» qui a œuvré pour ma réussite, de par son amour, son soutien tous les sacrifices consentis et ses précieux conseils pour toute son assistance Et sa présence dans ma vie.

A la mémoire de mon père «Ali» qui serait très fier de moi.

A mon adorable frère «Oussama» qui m'a soutenu dans mes moments les plus difficileset m'a encouragé à être forte.

A mon petite sœur «Nada» que j'aime sans limites.

A ma grande- mère «Aicha», A toutes mes tantes et tous mes oncles.

A ma belle chère binôme «Imane», ma meilleure amie avec laquelle que j'ai partagé tous mes souvenirs et mes années d'étude.

A tous mes ami(s) Manal, Nassira et lesquels que j'ai partagé les bons moments.

Abir

Résumé

L'Internet des objets est l'une des technologies modernes les plus importantes qui a connu une large diffusion dans de nombreux domaines. Cependant, la sécurité du réseau de l'Internet des objets est l'une des nécessités les plus importantes et pourtant elle est aujourd'hui exposée à de nombreuses attaques.

Les systèmes de détection d'intrusion ont leurs limites lorsqu'ils sont appliqués à l'Internet des objets, mais avec la croissance de la nécessité de renforcer la détection des vulnérabilités et la sensibilisation pour empêcher l'accès non autorisé aux ressources importantes, le système de détection d'intrusion (IDS) est responsable de l'inspection. Ainsi, en étudiant cela, nous avons inclus une stratégie basée sur un système multi-agents pour la détection des attaques dans la base UNSW-NB15.Nous avons également basée sur classifications consensuelle, utilisant l'algorithme de Paxos pour prouver l'efficacité de notre système.

Les mots clés : Système de Détection d'intrusion, Système Multi-agents(SMA), Internet des objets, UNSW-NB15.

المخلص :

أنترنت الاشياء هي واحدة من أهم التقنيات الحديثة التي انتشرت على نطاق واسع في العديد من المجالات. ومع ذلك، فإن أمان شبكة انترنت الأشياء هو واحد من أهم الاحتياجات ومع ذلك فهو معرض اليوم للعديد من الهجمات.

لدى أنظمة كشف الاختراق حد أقصى عند تطبيقها على انترنت الأشياء، ولكن مع نمو الحاجة إلى تعزيز كشف الثغرات وزيادة الوعي لمنع الوصول غير المصرح به إلى الموارد الهامة، يتحمل نظام كشف الاختراق (IDS) مسؤولية التفتيش. وبالتالي ، من خلال دراسة هذا ، قمنا بتضمين استراتيجية تعتمد على نظام متعدد العوامل لاكتشاف الهجمات في قاعدة بيانات UNSW-NB15. كما اعتمدنا أيضًا على تصنيفات الإجماع ، باستخدام خوارزمية Paxos لإثبات فعالية نظامنا.

الكلمات الرئيسية: نظام كشف الاختراق (IDS)، نظام متعدد الوكلاء (SMA)، إنترنت الأشياء، UNSW-NB15

Abstract

The Internet of Things (IoT) is one of the most important modern technologies that have seen widespread adoption in various fields. However, the security of IoT networks is a crucialnecessity that is currently susceptible to numerous attacks.

Intrusion detection systems have their limitations when applied to the IoT, but with the increasing need to enhance vulnerability detection and raise awareness to prevent unauthorized access to critical resources, the Intrusion Detection System (IDS) is responsible for inspection. In this study, we have incorporated a strategy based on a multi-agent system for attack detection in the UNSW-NB15 database. We have also relied on consensus-based classifications, using the Paxos algorithm to demonstrate the effectiveness of our system.

Keywords: Intrusion Detection System, Multi-Agent System (MAS), Internet of Things, UNSW-NB15.

Tables de matiere :

Chapitre02 : Le système de détection d'intrusion et les systemes multiagents

Chapitre03 : Conception et Implémentation.

Listes des figures

pages

Liste des tableaux

Liste des acronymes

ACL : langage de communication d'agent.

ADS : Anomalie Système de détection.

AIDE: Advanced Intrusion Detection Environment

ALG: Application Layer Gateway.

ANFIS: Système d'Interface Floue Neuronale Adaptative

BLE: Bluetooth Low Energy.

DDoS: Distributed Denial of Service

HIDS: Host-based intrusion detectionsystem.

IDS: Intrusion Detection System.

IDWG: Intrusion Detection WorkingGroup.

IOT: Internet of Things.

LGP: Programmation Génétique Linéaire

NIDS: Network Intrusion Detection System.

OC: L'objet connecté.

OSSEC: Open Source Security.

RF: Forêts Aléatoires.

SIoT : le concept d'IOT social.

SVM : Support Vector Machine

UIT : Union Internationale des Télécommunication

Introduction générale :

Les ordinateurs ne peuvent plus se passer des réseaux et systèmes informatiques, qui sont devenus essentiels pour le fonctionnement et le développement de la plupart des entreprises. Ces systèmes sont largement utilisés dans divers domaines tels que l'industrie, le marketing, l'assurance, la médecine et l'éducation. Ils ont également joué un rôle majeur dans l'émergence de l'Internet des objets, qui s'est développé rapidement ces dernières années et a facilité les tâches quotidiennes de l'homme. Les différents systèmes liés à l'Internet des objets, tels que les systèmes de sécurité des maisons et des bâtiments, dépendent fortement des systèmes informatiques pour fonctionner efficacement. L'interdépendance croissante entre ces différents systèmes et réseaux les rend accessibles à un groupe diversifié et croissantd'utilisateurs.

Que l'on soit familier ou non avec les réseaux, il n'est pas rare de constater une certaine méfiance envers ces derniers. En effet, ils peuvent être la cible d'attaques malveillantes visant à accéder, lire, modifier ou détruire des informations sensibles, perturbant ainsi leur bon fonctionnement. La sécurisation des réseaux est donc devenue un enjeu crucial pour éviter toute intrusion non autorisée. Cette sécurité peut être mise en place de manière préventive ou réactive, mais il est important de noter que même avec une approche préemptive, il est difficile d'assurer une sécurité totale étant donné la complexité des systèmes et les failles potentielles qui peuvent exister.

Et afin de le préserver de toutes les éventuelles attaques, l'approche interactive est mise en place pour s'en protéger. Cette méthode consiste à détecter rapidement les attaques pour pouvoir y réagir promptement et les éviter. Le système multi-agents est utilisé pour la détection d'intrusion, ce qui en fait un mécanisme spécial de gestion de la sécurité.

Dans ce mémoire, nous nous concentrons sur l'approche de classification consensuelle de telle manière qu'une seule décision est générée à partir des résultats obtenus via différentes techniques. L'agrégation de ces résultats selon une approche consensuelle permet de tirer profit des meilleurs atouts de chaque méthode individuellement.

Ce mémoire est structuré comme suit :

- **Chapitre 1 :** aborde les définitions et généralités sur les notions de base de

l’internet des objets et la fusion d’informations.

- **Chapitre2 :** On détail sur les systèmes de détection d’intrusion, architecture, méthodes, leur différent types, emplacement et avantages, et on parle en générale sur les systèmes multi-agents.

- **Chapitre 3** : On parle sur la conception de modèle et après l’implémentation toute en passant sur la plateforme utilisée, les langages de programmation et les résultats obtenus.

- Le mémoire s'achève par une conclusion générale récapitulant le contexte de recherche de notre étude.

Chapitre 01
L’Internet des objets

Introduction :

Aujourd'hui, l'Internet des objets en anglais the Internet of Things (IoT) est l'une des technologies les plus avancées au monde et grâce aux avancées technologiques et aux dernières recherches scientifiques, l'Internet des objets est devenu une technologie cruciale de notre époque. Cette connectivité généralisée ne se limite pas à la simple communication entre les objets, mais s'étend à de nombreux domaines.

L'IoT fait référence à la connexion d'objets physiques variés à Internet, leur permettant ainsi de communiquer entre eux et avec les utilisateurs. Ces objets peuvent être des appareils électroniques, des capteurs, des véhicules, des machines industrielles ou même des vêtements connectés. La sécurité de l'IoT est primordiale étant donné que cette technologie est omniprésente et a été à l'origine de nombreuses attaques.

Il est donc crucial de garantir la sécurité des données personnelles et d'éviter les attaques potentiellement dangereuses. Les fabricants et les utilisateurs doivent collaborer pour mettre en place des mesures de sécurité efficaces pour les appareils IoT.

1. L'internet des objets (IOT)

1.1 Définition de l'internet des objets

Le terme IoT est apparu la première fois en 1999 dans un discours de l'ingénieur britannique Kevin ASHTON. Il servait à désigner un système ou les objets physiques sont connectés à internet. Il s'agit également de systèmes capables de créer et transmettre des données afin de créer de la valeur pour ses utilisateurs à travers divers services (agrégation, analytique, etc.). Selon l'UIT l'Internet des Objets est d'défini comme (une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolues en interconnectant des objets (physique ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution). Au fil du temps, le terme a évolué et il englobe maintenant tout l'écosystème des objets connectés. Cet écosystème englobe, des fabricants de capteurs, des éditeurs de logiciels, des opérateurs historiques ou nouveaux sur le marché, des intégrateurs, etc. Cet éclectisme en fait sa richesse [1].

1.2 Un objet connecté (OC)

L'objet connecte échange des données, qu'elles soient numériques ou physiques entre eux. Un OC peut interagir avec le monde physique de manière indépendante sans intervention humaine.

Il possède plusieurs contraintes telles que la mémoire, la bande passante ou la consommation d'énergie, etc. Il doit être adopté à un usage, il a une certaine forme d'intelligence, une capacité de recevoir, de transmettre des données avec des logiciels grâce aux capteurs embarqués. Un objet connecté a une valeur lorsqu'il est connecté à d'autres objets et briques logicielles [2].

Par exemple :

Le D-Shirt : signifier un maillot sportif connecté, Ce maillot permet un monitoring en continu et unsuivi des performances de l'utilisateur. Des capteurs, la plupart existant déjà sur le marché actuel, ont été intégrés à un maillot afin de mesurer et d'enregistrer les caractéristiques et les performances des sportifs.On y retrouve par exemple un GPS, un altimètre, un cardio fréquencemètre et un accéléromètre.

Ainsi, le D-Shirt pro propose une solution complète de collecte et de gestion des données. Cette solution repose sur un couplage entre des capteurs intelligents (smart devices) et une plate-forme de type Big Data [3].

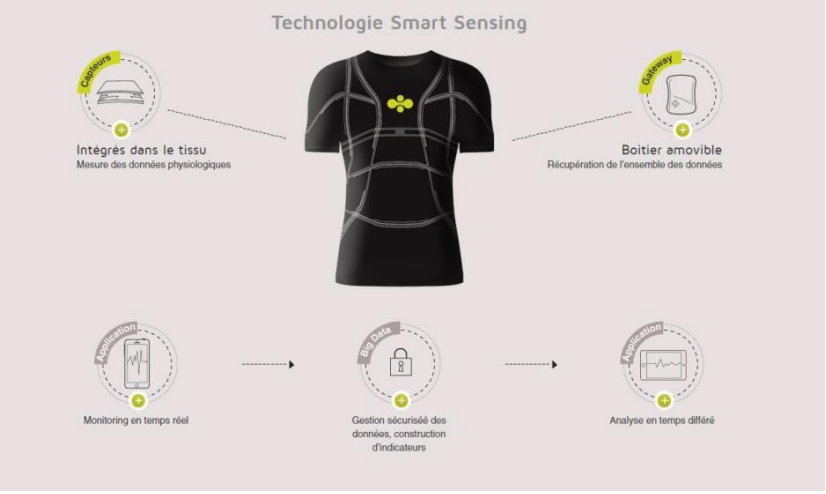

Figure 1: Principe de fonctionnement du D-Shirt.

2. Les Composants de l'internet des objets :

L'IoT est constitué de 05 Cinq composants essentiels. L'objet connecté est d'abord un objet qui a une fonction mécanique et/ou électrique propre, il peut soit être conçu directement connectable, soit il est déjà existant et la connectivité est rajoutée à posteriori. L'objet connecté a pour fonction de collecter des données de capteurs, de traiter ces données et de les communiquer à l'aide de d'une fonction de connectivité et de recevoir des instructions pour exécuter une action. Généralement ces fonctions de l'objet connecté nécessitent une source d'énergie, surtout quand les données sont prétraitées directement dans l'objet [4].

- **Capteur :**

Les capteurs sont des dispositifs permettant de transformer une grandeur physique observée (température, luminosité, mouvement etc. …) en une grandeur digitale utilisable par des logiciels. Il existe une très grande variété de capteurs de tous types, les objets connectés ont souvent la fonction de captation de ces grandeurs physiques sur leurs lieux d'utilisation.

Exemple de capteurs : lumière, présence, proximité, position, déplacement, accélération, rotation, température, humidité, son, vibration, électrique, magnétique, chimique, gaz, flux, force, pression, niveau, …etc. [4].

- **Réseaux de capteurs :**

Afin de satisfaire les besoins de communication entre eux, les capteurs sont équipes de dispositifs sans fil pour l'émission et la réception de données. Cela ne suffit cependant pas à rendre un ensemble de capteurs accessibles ou du moins de manière interopérable, transparente et simplifiée pour cela, les capteurs doivent aussi s'organiser ce qui caractérise un réseau de capteurs, c'est que ses éléments sont de très petits appareils, dotes de capacités de transmission sans fil [4].

- **Énergie** :

La plus importante contrainte à laquelle sont soumis les restes aux capteurs concernant l'énergie : L'autonomie temporelle des nœuds s'évalue en termes d'années [4].

- **Actionneurs :**

Les actionneurs sont des dispositifs qui transforment une donnée digitale en phénomène physique pour créer une action, ils sont en quelque sorte l'inverse du capteur. Exemple d'actionneurs : Afficheurs, Alarmes, Caméras, Haut-parleurs, Interrupteurs, Lampes, Moteurs, Pompes, Serrures, Vannes, Ventilateur, Vérins [4].

- **Connectivité :**

La connectivité de l'objet est assurée par une petite antenne Radio Fréquence qui va permettre la communication de l'objet vers un ou plusieurs réseaux (qui sont détaillés dans la section « réseaux IoT »). Les objets pourront d'une part remonter des informations telles que leur identité, leur état, une alerte ou les données de capteurs, et d'autre part recevoir des informations telles que des commandes d'action et des données. Le module de connectivité permet aussi de gérer le « cycle de vie de l'objet », c'est-à-dire, l'authentification et l'enregistrement dans le réseau, la mise en service, la mise à jour et la suppression de l'objet du réseau [4].

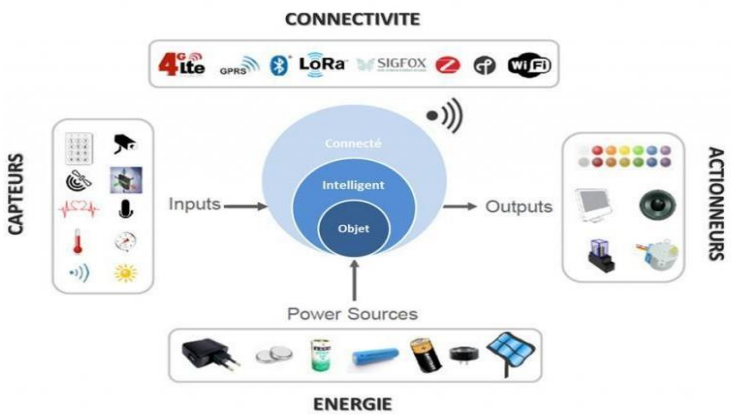

Figure 2 : Les Composants de l'IOT.

3. Les caractéristiques clés de l'internet des objets :

L'Internet des objets est un réseau de dispositifs connectés qui peuvent communiquer entre eux et avec d'autres systèmes informatiques. Les caractéristiques clés de l'IoT comprennent [5] :

- **Inter-connectivité** : l'infrastructure internationale d'information et de communication peut êtreinterconnectée avec n'importe quoi.
- **Services liés aux objets** : tels que la protection de la vie privée et l'uniformité sémantique entreles objets physiques et leurs objets virtuels connectés.
- **Hétérogénéité** : les appareils IoT peuvent se connecter à d'autres appareils via différents réseaux.
- **Changement dynamique** :le changement dynamique de l'état des appareils.
- **Échelle énorme**: les appareils IOT sont beaucoup plus importants que le nombr d'appareilssurInernet

- **Sécurité** : nous devons mettre en place un système de sécurité parmi les créateurs et les destinataires de l'IoT, comme la sécurité des données personnelles et le bien-être physique
- **Connectivité** : permet l'accessibilité et la compatibilité du réseau.

4. Fonctionnement de l'Internet des Objets :

4.1 Etapes de mise en place d IOT :

Les objets connectés sont au sein de l'IOT, mais il est important de pouvoir connecter l'ensemble de ces objets, les faire échanger des informations et interagir au sein d'un même environnement.

La mise en place de l'IOT passe par les étapes suivantes :

- **L'identification** : Rendre possible l'identification de chaque élément connecté (IPV4, IPV6).
- **L'installation de capteurs** : Mise en place de dispositifs nous rapprochant du monderéel.
- **La connexion des objets entre eux** : Etablir une connexion entre tous les objets afinqu'ils puissent échanger des informations (SigFox, LoRa, NFC, Bluetooth).
- **L'intégration** : C'est Intégration des objets pour que les données soient transmisesd'une couche à une autre (middlewares).
- **La connexion à un réseau** : Relier les objets et leurs données au monde informatique via unréseau internet par exemple en utilisant (HTTP, REST, CoAP, MQTT) [6].

4.2 Technologies de l'IOT :

L'IoT permet l'interconnexion des différents objets intelligents via l'Internet. Ainsi, pour son fonctionnement, plusieurs systèmes technologiques sont nécessaires. L'IoT désigne diverses solutions techniques (RFID, TCP/IP, technologies mobiles, etc.) qui permettent d'identifier des objets, capter, stocker, traiter, et transférer des données dans les environnements physiques, mais aussi entre des contextes physiques et des univers virtuels. En effet, bien qu'il existe plusieurs technologies utilisées dans le fonctionnement de l'IoT, nous mettons l'accent seulement sur quelques-unes citées ci-dessous [6].

4.2.1 Les technologies de courte portée :

Bluetooth : Inventé en 1994 par la société suédoise Ericsson, leprotocole Bluetooth est un standard de transfert de données sans fil. Il utilise une faible bande

passante, ce qui ne lui permet de transférer que peu de données à de courtes distances, mais est également très peu énergivore. Inclus à l'immense majorité des téléphones mobiles, afin de réaliser une communication entre deux téléphones, ou entre un téléphone et un objet connecté de nature différente, il possède désormais de nombreuses applications : oreillette de discussion téléphonique sans fil, montre intelligente, moniteur de fréquence cardiaque, etc [6].

Zigbee : C'est un protocole de communication radio développé spécifiquement pour les applications de domotique. D'une portée moyenne de 100 mètres, il utilise une faible bande passante et est idéal pour le transfert de données en faible volume. le dispositif Zigbee convient aux appareils alimentés par une pile ou une batterie, et en particulier aux capteurs [6].

4.2.2 Les technologies de moyenne portée :

- **Wi-Fi** :

Le Wi-Fi désigne un ensemble de protocoles de communications sans fil, permettant des connexions à haut débit sur des distances de 20 à 100 mètres. Il s'agit d'un réseau local sans fil très énergivore, qui ne convient que pour les appareils branchés sur secteur ou dont l'alimentation électrique peut être aisée et fréquente. Il permet de transférer rapidement beaucoup de données [6].

- **Bluetooth Low Energy :**

La technologie BLE est un protocole de réseau personnel sans fil à très basse consommation d'énergie. Comme la technologie Bluetooth originelle, le BLE ne permet de transférer qu'une quantité limitée de données à une distance moyenne de 60 mètres. La différence entre les dispositifs Bluetooth et BLE se situe au niveau de la consommation électrique nécessaire à la communication, qui est dix fois moindre pour BLE [6].

4.2.3 Les technologies de longue portée :

- **Réseaux cellulaires mobiles**

Fournis par les opérateurs de télécommunication, les réseaux cellulaires mobiles**,** basés sur la technologie GSM, permettent de transférer une quantité importante de données à une longue portée. Ils nécessitent l'installation d'une carte SIM dans l'appareil à connecter, afin d'identifier celui-ci sur le réseau de communication [6].

- **Réseaux radio bas-débit**

SigFox : c'est un réseau de communication radio sans fil à bas débit et à basse fréquence, d'une portée moyenne de 10 kilomètres en milieu urbain et de 30 à 50 kilomètres en milieu rural. Ce réseau convient à des appareils à basse consommation, dotés ainsi d'une grande autonomie, qui transfèrent une faible quantité de données [6].

LoRa : c'est un protocole de communication radio à très basse consommation, qui permet de transmettre des données en petite quantité, à des distances de 2 à 5 kilomètres en ville et jusqu'à 45 kilomètres en milieu urbain. À l'instar de SigFox, il s'agit d'un dispositif qui convient particulièrement aux équipements peu énergivores n'émettant que périodiquement, notamment les capteurs [6].

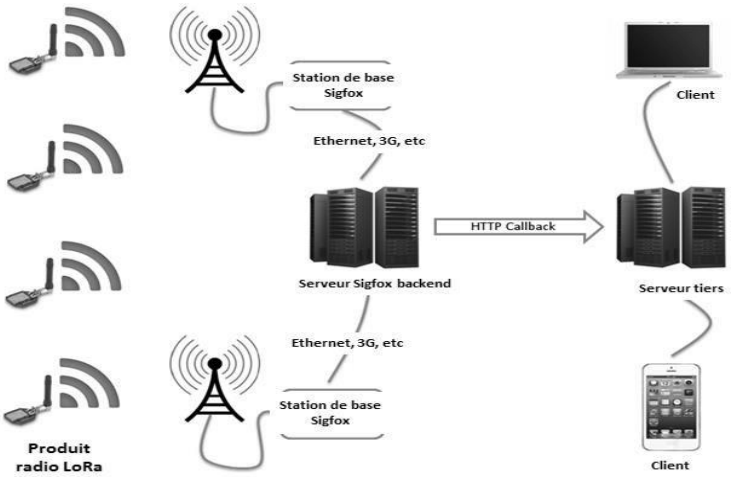

Figure 3 : Les protocoles Sigfox et LoRa.

5 . L'architecture de l'IOT :

L'IOT fait donc référence à un écosystème dans lequel des applications et des services sont pilotés par des données obtenues du monde physique et transmises par des capteurs embarqués dans les objets.

Un dispositif IOT a ainsi la capacité de percevoir son environnement (température, humidité, présence, etc.), de traiter et de transférer les données recueillies dans des applications ou des services (mobilisant notamment des algorithmes d'intelligence

artificielle) et enfin d'aider à la prise de décisions – décisions qui, si le dispositif contient des actionneurs, peuvent s'appliquer au monde physique.

Ces dispositifs mobilisent à la fois des équipements physiques (les capteurs), des réseaux de télécommunication (pour la transmission des données), des équipements pour la mémorisation des données, éventuellement des actionneurs et enfin des couches logicielles pour le traitement des informations réparties sur l'ensemble des éléments identifiés [7].

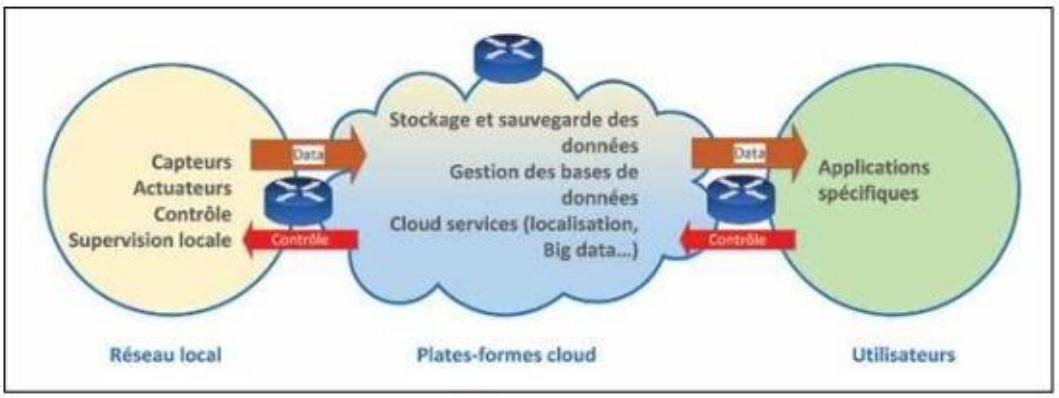

Figure 4: Architecture générale de l'IoT.

Nous distinguons quatre couches logicielles qui permettent de décrire une solution IOT dans son ensemble:

- **Une couche en contact avec les capteurs ou actionneurs de l'objet connecté :** qui récupère les données acquises et transfère les ordres d'actions (brique « objet connecté») ;
- **Une couche réseau** : qui s'appuie sur un service de télécommunication qui peut selon les contraintes opérationnelles être filaire ou sans fil, et présenter des caractéristiques de débit et de portée qui déterminent les types d'application susceptibles d'être utilisées (brique « réseau IOT »).

- **Une couche jouant le rôle d'intergiciel (Middleware) :** dédiée au stockage et au traitement des données collectées (couche « plateforme IOT »).
- **Les applications utilisant ces données et fournissant des services** : proposées aux utilisateurs finaux (applications IOT) [7].

7. Les modèles de communication d'Internet des objets :

- **Périphérique à périphérique** : deux appareils ou plus, qui se connectent directement et communiquent entre eux, plutôt que via un serveur d'applications intermédiaire. Ce modèle utilisede petits paquets d'informations pour la communication entre des appareils avec un débit dedonnées relativement minimum comme dans la domotique (par exemple, le message d'état de verrouillage de la porte ou d'allumer la commande d'éclairage) dans un script domotique [5].

- **Périphérique à Cloud** : Dans ce modèle, le dispositif IoT se rapporte directement à un service cloud Internet comme un fournisseur de services d'application pour échanger des données et contrôler le trafic de messages. Cette méthode tire extrêmement parti des techniques de communication existantes pour établir une liaison entre l'appareil et le réseau IP, qui se connecte finalement au service cloud [5].

- **Périphérique vers passerelle** : Dans ce modèle, le modèle de passerelle de couche de périphérique à application ALG et le périphérique IoT se connectent via un service ALG en tant quecanal pour étendre un service cloud. Cela signifie qu'il existe un logiciel d'application fonctionnant sur un périphérique de passerelle locale, qui agit comme un dispositif entre le périphérique et le service cloud [5].

- **Modèle de partage de données principal** : Il fait référence à une architecture de communication, qui permet aux utilisateurs d'exporter et d'analyser des données d'objets intelligents à partir d'un service cloud en combinaison avec des données provenant d'autres sources. Il permet également d'agréger et d'analyser les données collectées à partir de flux de données d'appareils IoT uniques. [5]

8. Les Domaines d’application d’Internet des objets :

L’Internet des objets a été appliqué dans de nombreux domaines, et cela est dû au développement rapide de la technologie, et les plus importants de ces domaines sont :

8.1 Les Villes Intelligentes :

Beaucoup de grandes villes ont été soutenues par des projets intelligents, comme Séoul, New York,

Tokyo, Shanghai, Singapour, Amsterdam et Dubaï. Les villes Intelligentes peuvent encore être considérées comme des villes de L'avenir et la vie intelligente, et par le taux d'innovation de la création de villes Intelligentes d'aujourd'hui, il sera devenu très faisable pour entrer la technologie IoT Dans le développement des villes. La demande exige une planification minutieuse à chaque étape, avec l'appui de L'accord des gouvernements, citoyens à mettre en œuvre la technologie d'Internet des Objets dans tous les aspects. Par l'IoT, les villes peuvent être améliorées à plusieurs Niveaux, en améliorant les infrastructures, en améliorant les transports [8].

8.2 Le Smart Grid :

L'un des domaines d'application de l'IoT est le secteur de la distribution d'énergie intelligente, dit « Smart Grid ». En France, ERDF est très actif dans le développement de ce domaine, où un besoin clair en récupération d'information à différents points du réseau électrique est devenue nécessaire pour une meilleure intégration des différentes sources d'énergies et une meilleure gestion de la distribution jusqu'aux utilisateurs finaux [8].

8.3 Les Appareils Intelligents :

Des appareils intelligents dans les soins de santé sont utilisés pour stocker et gérer les paramètres de soins clés et pour gérer les données sur les maladies capturées. Ils sont principalement déployés pour fournir des solutions de conditionnement physique en suivant les activités ciblées et des dispositifs de diagnostic utilisés pour stocker des données de dispositifs. Principalement, ils sont utilisés comme des solutions de fitness pour suivi des activités du patient et des appareils de diagnostic intelligents tels que les dispositifs de tension matérielle, les podomètres, Google verre, etc. utilisé pour capturer les données des capteurs, pour une analyse plus approfondie par le médecin [8].

8.4 La domotique :

La domotique est l'un des domaines les plus fascinants de l'IoT, car elle permet de connecter les équipements domestiques à un réseau. Cela offre plusieurs avantages, notamment la possibilité de contrôler tous les équipements techniques d'une maison depuis une seule interface (comme une tablette ou un téléphone), ainsi que la capacité de les contrôler à distance grâce à des API disponibles sur le web.

La domotique permet d'automatiser de nombreuses tâches quotidiennes : la fermeture de vos volets en fonction de l'ensoleillement, l'ouverture de votre portail lorsque vous approchez en voiture, la gestion de l'éclairage de toutes vos pièces, la préparation d'un café à votre réveil ou à votre retour du travail ou encore la redirection des appels à l'interphone sur votre smartphone afin que le livreur puisse déposer vos colis sur le pas de votre porte d'entrée… En bref, toutes les petites

améliorations de confort que vous pouvez imaginer sont déjà possibles [9].

Figure 5 : La domotique dans une maison.

8.4.1 La maison intelligente :

Une maison intelligente est une installation domestique pratique où les appareils et les dispositifs peuvent être automatiquement contrôlés à distance de n'importe où grâce à une connexion internet utilisant un téléphone portable ou un autre appareil en réseau. Les appareils d'une maison intelligente sont interconnectés par l'internet, ce qui permet à l'utilisateur de contrôler à distance des fonctions telles que l'accès à la maison, la température, l'éclairage et un cinéma maison…. etc.

Les appareils d'une maison intelligente sont reliés entre eux et peuvent être accessibles par un point central – un smart phone, une tablette, un ordinateur portable. Les serrures de porte, les télévisions, les thermostats, les caméras, les lumières et même les appareils tels que le réfrigérateur peuvent être contrôlés par un seul système domotique. Le système est installé sur un téléphone portable ou un autre appareil en réseau, et l'utilisateur peut créer des horaires pour que certains changements prennent effet [9].

Exemple de la maison intelligente :

Somfy : Il permet à l'utilisateur de contrôler les équipements de la maison à la voix en l'associant à un assistant vocal comme Amazon Alexa, Google Home ou Siri.

L'écosystème TaHoma de Somfy est renforcé chaque année par de nouvelles compatibilités grâce au programme So Open, et au développement permanent de solutions innovantes [10].

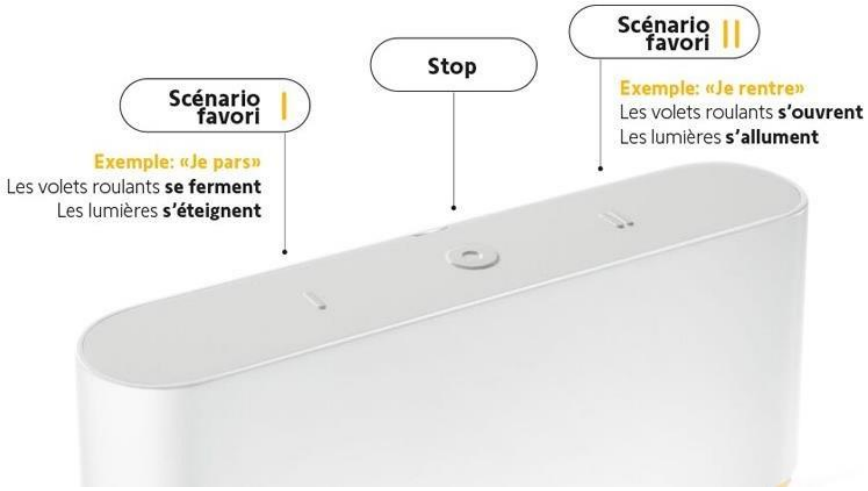

Figure 6: La commande intelligente TaHoma switch.

8.5 Le Transport et La Mobilité Intelligent :

Le développement du transport est l'un des facteurs qui indiquent le bien-être de Pays. Une application de surveillance de l'état des routes et d'alerte est l'un des applications plus importantes de l'IoT. Le processus a besoin de l'identification de l'utilisateur et son trajectoire souhaité dans son application sur son téléphonique intelligents.

Le transport intelligent est confronté à trois conceptions principales ils sont l'analyse des transports, le contrôle des véhicules connectées. L'analyse de transport représente l'analyse de la prédiction de la demande et de détection anomalie. Le routage des véhicules et le contrôle de la vitesse en plus de la gestion du trafic sont tous connu comme le contrôle du transport qu'ils ont réellement étroitement lié aux véhicules connectés [8].

8.6 La Surveillance à Distance Des Patients

Ce domaine d'application est déployé pour surveiller à distance les paramètres essentiels du patient par l'utilisation de capteurs, de dispositifs et les objets qui les entourent. En cela, les données critiques du patient sont transmises et partagées en temps réel entre le patient et les soignants. Sa principale pertinence est la gestion des maladies chroniques telles que le diabète, les maladies cardiaques, asthme, etc. [8].

9. L'importance de l'IOT :

L'internet des objets est devenu une technologie clé dans le monde d'aujourd'hui. Et l'IoT offre de nombreux avantages dans différents domaines.

Les avantages d'IoT dans les applications commerciales et industrielles sont nombreux. La plupart d'entre eux sont centrés sur l'efficacité - non seulement parce que des opérations efficaces permettent de réduire les coûts et de diminuer notre impact sur la planète, mais aussi parce que, dans certains cas, l'efficacité d'un processus donné, ou la transmission d'informations et l'automatisation des processus, sont essentielles. Dans de nombreux cas, des vies en dépendent.

Les avantages que les solutions IoT apportent dans le domaine de l'automatisation de la fabrication comprennent plusieurs capacités que les humains ne peuvent offrir :

Les machines peuvent assembler les pièces avec plus de précision et de rapidité, ce qui réduit les erreurs lors de l'assemblage. L'automatisation permet également à une usine de travailler de plus longues heures sans fatigue, et les robots peuvent détecter très rapidement des défauts qui ne sont pas nécessairement détectés par l'œil humain.

D'autres exemples d'automatisation comprennent gestion intelligente du trafic pour améliorer la fluidité et acheminer rapidement les véhicules d'urgence à travers la ville ; technologie des véhicules connectés qui automatise le comportement et le freinage des véhicules pour la sécurité ; et ventilateurs de gel automatisés dans l'agriculture lorsque le gel est détecté [11].

10. La sécurité dans l'Internet des Objets

10.1Définition de la sécurité informatique :

On peut définir la sécurité informatique comme étant le fait d'assurer le bon fonctionnement d'un système et de garantir les résultats attendus de sa conception. Autrement dit, la sécurité représente l'ensemble de politiques et pratiques adoptées pour prévenir et surveiller l'accès non autorisé, l'utilisation abusive, la modification ou le refus d'une opération informatique. A partir de cette définition, on peut extraire les bases de la sécurité qui sont décrites dans ce qui suit [12].

- **Authentification** :

L'authentification est le mécanisme de sécurité qui permet de prouver l'identité d'une entité.

- **Confidentialité :**

La confidentialité est le mécanisme qui permet de cacher une donnée, et de cacher même l'information de son existence. Ainsi, empêcher toutes entité(s) non autorisée(s) d'avoir accès à cette donnée. Généralement, on assure ce service en utilisant le chiffrement de données. Ce dernier est basé sur des algorithmes mathématiques permettant de déformer un texte en clair est le remettre à sa forme initiale grâce au à une ou plusieurs clés cryptographiques.

- **Intégrité :**

L'intégrité est un mécanisme assurant qu'une donnée ne soit pas : falsifiée, modifiée, altérée ou supprimée par une entité non autorisée. Dans la plupart des cas, ce service est réalisé en utilisant des fonctions de hachages avec des propriétés de signature de données.

- **Disponibilité :**

La disponibilité est le mécanisme qui permet de garantir la bonne exécution d'un service, et le bon fonctionnement du système. Afin de garantir la disponibilité d'un service, on utilise des mécanismes qui le protègent contre les arrêts intentionnels telles que les attaques de dénies de service et dénies de service distribués (*Denial/Distributed Denial of service (Dos/DDos)*), et non intentionnels (ex. les erreurs humaines).

- **Non répudiation :**

Le non répudiation est un mécanisme permettant de garantir qu'une opération ne peut être niée par celui qui l'avait établi. On garantit ce service grâce aux signatures numériques combinées avec des mécanismes qui assurent le non rejeu de données.

- **Non rejeu :**

Est un mécanisme garantissant qu'un message échangé entre deux entités A et B, ne doit pas être réutilisé par une entité non autorisée C. La plupart des systèmes intègrent des compteurs et des numéros de séquence différents au niveau des messages échangés, ce qui fait qu'un message ne peut pas avoir le même numéro de séquence que ses *n* messages précédents (*n* un nombre de message qui varie selon la politique de sécurité utilisée), sinon il sera automatiquement rejeté.

- **La résilience :**

La résilience est une capacité d'un système à surmonter une altération de son environnement.

- **La confidentialité persistante :**

La confidentialité persistante est une caractéristique cryptographique qui garantit que la découverte d'une information secrète (ex. clé privée) d'un objet légitime par un utilisateur malicieux ne compromet pas la confidentialité des communications passées.

- **L'évolutivité :**

L'évolutivité représente l'aptitude d'un système à maintenir des bonnes performances lorsque des ressources (notamment ressources matérielles) lui sont ajoutées.

- **La tolérance aux fautes :**

La tolérance aux fautes est un mécanisme permettant à un système de continuer à fonctionner lorsque l'un de ses composants tombe en panne (ex. en dupliquant les serveurs) [12].

10.2 Définition de la sécurité de l'internet des objets :

La sécurité de l'IoT est le domaine technologique qui concerne la protection des dispositifs et des réseaux connectés dans l'internet des objets (IOT).

L'IoT consiste à ajouter la connectivité internet à un système de dispositifs informatiques interconnectés, de machines mécaniques et numériques, d'objets, d'animaux et/ou de personnes. Chaque « chose » est dotée d'un identifiant unique et de la capacité de transférer automatiquement des données sur un réseau. Permettre à des dispositifs de se connecter à l'internet les expose à un certain nombre de vulnérabilités graves s'ils ne sont pas correctement protégés.

La sécurité de l'IoT est devenue l'objet d'un examen minutieux après un certain nombre d'incidents très médiatisés où un dispositif IoT commun a été utilisé pour infiltrer et attaquer un réseau le plus important. La mise en œuvre de mesures de sécurité est essentielle pour garantir la sécurité des réseaux auxquels sont connectés des dispositifs IoT [13].

10.3 Les différentes attaques dans l'IOT :

Les études ont montré qu'il existe différentes types d'attaque IoT [14] :

- **Les attaques par déni de service (DDoS)**

Les pirates informatiques peuvent utiliser des milliers d'appareils IoT infectés pour envoyer simultanément des demandes à un serveur, le surchargeant et le rendant inaccessible.

- **L'attaque via l'appareil lui-même** :

Dans ce cas, les attaques proviennent d'une partie de l'appareil. Il peut s'agir de sa mémoire, son interface physique ou Web.

- **Les attaques par les canaux de communication** :

Les protocoles utilisés dans les systèmes des objets IoT peuvent présenter des failles. Ce qui engendre des problèmes de sécurité affectant l'ensemble des systèmes. Les attaques réseau entrent aussi dans cette catégorie (déni de service ou DDoS et l'usurpation d'adresse).

- **Les attaques par l'intermédiaire des logiciels et applications** :

Les applications Web ou les logiciels sont aussi des moyens d'attaque de l'IoT. Les hackers peuvent, par exemple, voler les informations sur l'identification de l'utilisateur ou induire à une mise à jour de logiciel malveillant.

Par exemple : Absence de surveillance et de gestion des appareils :

Les objets connectés sont de plus en plus utilisés, surtout avec les nouveaux projets de villes connectées. Ce qui augmente les risques sur la sécurité de l'IoT. D'autant plus lorsqu'il n'y a pas de surveillance ni de gestion des appareils. Par conséquent, en cas d'attaque, l'entité concernée ne peut pas détecter ou répondre correctement. Pour y faire face, il faut instaurer un système de surveillance adéquat [15].

11. Amélioration de la sécurité de l'internet des Objets :

Parmi les problèmes de sécurité de l'IoT évoqués, la plupart peuvent être surmontés par une meilleure préparation, notamment lors du processus de recherche et de développement de tout dispositif IoT destiné aux consommateurs, aux entreprises ou aux industries. L'activation de la

sécurité par défaut est essentielle, tout comme la fourniture des systèmes d'exploitation les plus récents et l'utilisation de matériel sécurisé.

Les développeurs IoT doivent être attentifs aux vulnérabilités en matière de cyber sécurité à chaque étape du développement, et pas seulement à la phase de conception. Le piratage de la clé de voiture, par exemple, peut être atténué en plaçant le FOB dans une boîte métallique, ou loin des fenêtres et des couloirs [16].

- **ICP et certificats numériques :**

L'ICP est un excellent moyen de sécuriser les connexions client-serveur entre plusieurs appareils en réseau. Grâce à un système de cryptage asymétrique à deux clés, l'ICP est en mesure de faciliter le cryptage et le décryptage des messages privés et des interactions à l'aide de certificats numériques. Ces systèmes permettent de protéger les informations que les utilisateurs saisissent sur les sites web pour effectuer des transactions privées. Le commerce électronique ne pourrait pas fonctionner sans la sécurité de l'ICP [16].

- **Sécurité des réseaux :**

Les réseaux offrent une énorme opportunité de contrôle à distance d'appareils IoT, et donc une menace pour les détenteurs de ces appareils. Étant donné que les réseaux comportent des composants numériques et physiques, la sécurité IoT sur site doit porter sur les deux types de points d'accès. La protection d'un réseau IoT consiste notamment à assurer la sécurité des ports, à désactiver la redirection des ports et à ne jamais ouvrir de ports lorsque cela n'est pas nécessaire, à utiliser des antimalwares, des pare-feu et des systèmes de détection et prévention des intrusions, à bloquer les adresses IP (Internet Protocol) non autorisées et à s'assurer que les systèmes sont patches et à jour [16].

- **Sécurité des API :**

Les API sont l'épine dorsale de la plupart des sites web sophistiqués. Elles permettent aux agences de voyage, par exemple, de regrouper les informations sur les vols de plusieurs compagnies aériennes en un seul endroit. Malheureusement, les pirates peuvent compromettre ces canaux de communication, ce qui rend la sécurité des API nécessaire pour protéger l'intégrité des données envoyées par les appareils IoT aux systèmes dorsaux et pour s'assurer que seuls les appareils, développeurs et applications autorisés communiquent avec les API. La violation de données de T-Mobile en 2018 est un parfait exemple des conséquences d'une mauvaise sécurité des API. En

raison d'une "fuite d'API", le géant de la téléphonie mobile a exposé les données personnelles de plus de 2 millions de clients, notamment les codes postaux de facturation, les numéros de téléphone et les numéros de compte, entre autres données [16].

Pour protéger les appareils IoT contre les attaques, il est important de prendre plusieurs mesures de sécurité. Cela peut inclure l'utilisation de mots de passe forts et uniques pour chaque appareil, la mise à jour régulière du firmware et du logiciel pour corriger les vulnérabilités connues, et l'utilisation d'une connexion sécurisée telle que le chiffrement SSL/TLS.

En outre, il est important que les fabricants d'appareils IoT prennent également en compte la sécurité dès la conception et la fabrication des produits. Cela peut inclure l'utilisation de protocoles de sécurité standardisés tels que le protocole HTTPS pour les communications en ligne et l'inclusion d'une fonctionnalité permettant aux utilisateurs de désactiver les fonctionnalités non essentielles qui pourraient être vulnérables aux attaques

12. Conclusion :

Dans le premier chapitre de notre travail en a abordé tout d'abord la définition de l'internet des objets et un objet connecté, en détaillant ses composants et ses caractéristiques, ses fonctionnementset ses architectures. Par la suite, on a examiné également les domaines d'application de cette technologie et leur importance. Et vers la fin de ce chapitre on a aussi essayé de mettre la lumière sur la sécurité informatique et la sécurité de l'internet des objets.

Chapitre 02

Le système de détection d’intrusion et les systèmes multi agents

1 Introduction

Les systèmes multi-agents prennent aujourd'hui une place de plus en plus importante en informatique, particulièrement dans le domaine de l'intelligence artificielle, la sécurité et plusieurs domaines.

L'utilisation de SMA dans les IDS offre une approche innovante pour améliorer la sécurité informatique en permettant une collaboration efficace entre les agents autonomes pour détecter et prévenir les intrusions.

2 Généralité sur le système de détection d'intrusion :

2.1 Définitions :

On peut associer plusieurs termes à la sécurité liée à l'intrusion sont les suivantes :

2.2 Intrusion :

Une intrusion est une action malveillante ou non autorisée visant à accéder, à altérer ou à perturber un système informatique, un réseau ou une application. Les intrusions peuvent être effectuées par des personnes malveillantes ou des pirates informatiques pour voler des données confidentielles, endommager des systèmes ou des réseaux, installer des logiciels malveillants ou nuire à la réputation d'une organisation.

2.2.1 Détection d'intrusion :

La détection d'intrusion est le processus de surveillance et d'analyse de l'activité sur un réseau ou un système informatique pour détecter les tentatives d'accès non autorisées, les activités malveillantes ou les failles de sécurité. Les outils de détection d'intrusion peuvent être utilisés pour surveiller les journaux système, les fichiers de configuration, les connexions réseau et les comportements suspects des utilisateurs. Les systèmes de détection d'intrusion peuvent détecter des anomalies dans le trafic réseau ou le comportement des utilisateurs en fonction de règles préétablies, de signatures de logiciels malveillants connus ou d'algorithmes d'apprentissage automatique. La détection des intrusions est un élément important de la sécurité informatique et peut aider à arrêter les attaques avant qu'elles ne causent des dommages importants.

2.2.2 Systèmes de détection d'intrusion :

Un système de détection d'intrusion (IDS) est un matériel, un logiciel ou une combinaison des deux, utilisé pour surveiller les activités du réseau ou du système afin de détecter les signes de malveillance. En matière de sécurité informatique, concevoir un système de détection d'intrusion robuste est l'un des problèmes les plus fondamentaux et importants. La fonction principale du système est de détecter les intrusions et d'émettre des alertes lorsque l'utilisateur tente de s'introduire de manière opportune. Lorsque l'IDS détecte une intrusion, il envoie un message d'alerte à l'administrateur du système [14].

2.3 Architecture de système de détection d'intrusion :

Quel que soit le niveau des moyens techniques mis en place pour la prévention d'attaques dans un système informatique, il peut succomber face à un adversaire endurant, utilisant des techniques plus évoluées ou des moyens plus avancés. De ce fait, il faudra qu'en dessous de toute couche de prévention, qu'il ait une couche de détection d'intrusion. C'est le fondement du développement des systèmes de détection d'intrusion, plus connus sous le nom d'IDS) [2].

La **figure 1**, proposée par l'IDWG présente le processus générique des systèmes de détection d'intrusion.

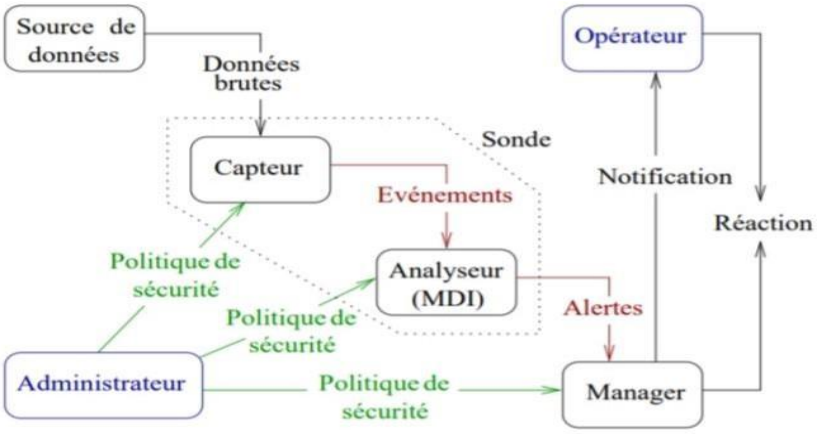

Figure 7: Modèle générique de la détection d'intrusions proposé par l'IDWG.

L'administrateur configure les différents composants (capteur(s), analyseur(s), manager(s)). Les capteurs accèdent aux données brutes, les filtrent et les formatent pour ne renvoyer que les événements intéressants à un analyseur. Les analyseurs utilisent ces événements pour décider de la présence ou non d'une intrusion et envoient le cas échéant une alerte au manager (qui notifie

l'opérateur humain). Une réaction éventuelle peut être menée automatiquement par le manager ou manuellement par l'opérateur [16] [15].

2.4 Les méthodes de détection d'intrusion :

2.4.1 La détection basée sur les signatures (signature-based detection) :

Sont une classe de systèmes qui exploitent une base de données de "signatures" d'attaques connues. Les signatures des activités en cours sont extraites, et des méthodes de correspondance et/ou de vérification de la conformité des protocoles sont ensuite utilisées pour comparer ces signatures à celles de la base de données. Si une correspondance est trouvée, une alarme est déclenchée. Ces systèmes peuvent fonctionner à la fois en mode en ligne, en surveillant directement les hôtes et en déclenchant des alarmes en temps réel, et en mode hors ligne, où les journaux des activités du système sont analysés. Cette classe d'IDS est également connue dans la littérature sous le nom de détection d'utilisation abusive ou de détection basée sur la connaissance [17]. L'extraction des signatures de trafic peut être une tâche fastidieuse et longue à réaliser, en fonction du nombre et des types de "caractéristiques" de trafic considérées. En effet, les signatures sont souvent élaborées manuellement par des experts ayant une connaissance détaillée des exploits que le système est censé détecter [18].

2.4.2 La détection d'anomalie (anomaly detection):

Ce type d'IDS est également connu publiquement comme une anomalie Système de détection (ADS). L'IDS dépend de la variation comportement normal. L'IDS ne s'appuie pas sur modèles d'attaque définis. Cependant, IDS peut différencier entre le trafic réseau normal et anormal selon un seuil prédéfini. Ainsi, ADS peut détecter invisible avant attaques, contrairement aux PEID [19], [20]. La figure 2 montre les types d'IDS [21].

2.4.3 La détection hybride (hybride detection):

Il est composé à la fois de composants NIDS et HIDS de manière efficace en utilisant des agents mobiles. Les agents mobiles se déplacent vers chaque hôte et effectuent des vérifications de journal système, tandis qu'un agent central vérifie le trafic réseau global pour détecter l'existence d'anomalies [22].

2.5 Les types de système détection d'intrusion:

2.5.1 Les IDS réseaux (Network-based IDS) :

Le système de détection d'intrusion réseau (NIDS) surveille le trafic réseau et analyse le trafic en cours pour détecter les attaques. Lorsqu'une attaque est identifiée ou qu'un comportement anormal est détecté, une alerte peut être envoyée à l'administrateur. Les NIDS peuvent détecter 4 types majeurs d'attaques : les dénis de service, les sondes, les utilisateurs à privilèges élevés et les connexions distantes aux utilisateurs [23].

2.5.2 Les IDS hôtes (Host-based IDS):

Un IDS basé sur l'hôte détecte les comportements d'intrusion en scannant les journaux et les enregistrements d'audit. Ce type d'IDS est généralement utilisé sur des hôtes importants pour protéger la sécurité de l'hôte dans toutes les directions. L'avantage de l'IDS basé sur l'hôte est qu'il fournit des informations plus détaillées, des taux de fausses alarmes plus faibles et une complexité moindre que l'IDS basé sur le réseau. Cependant, il réduit l'efficacité du système d'application et repose excessivement sur les données de journalisation et la capacité de surveillance de l'hôte [24].

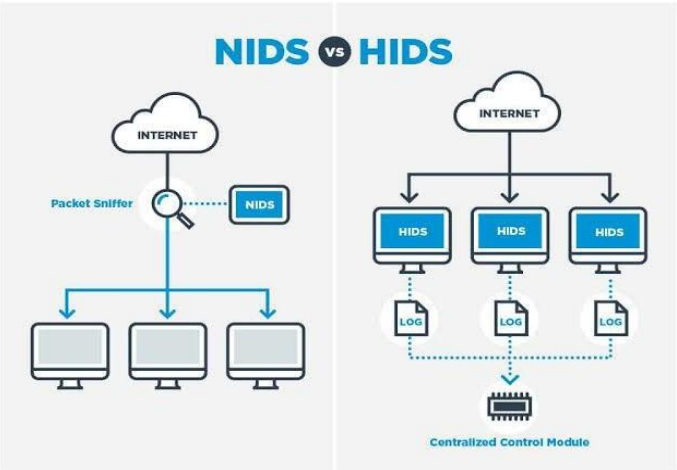

Figure 8: Les Types D'IDS.

2.6 Emplacement de l'IDS :

Il est très important de faire un bon travail dans le positionnement du système de détection d'intrusion, cela nécessite d'identifier les ressources à protéger et les ressources les plus susceptibles d'être attaquées, puis de les mettre en place avec soin dans les zones appropriées. Il existe plusieurs

emplacements stratégiques où les IDS doivent être placés [25]12. La figure 3 illustre un réseau local et trois positions au sein desquelles un IDS peut occuper:

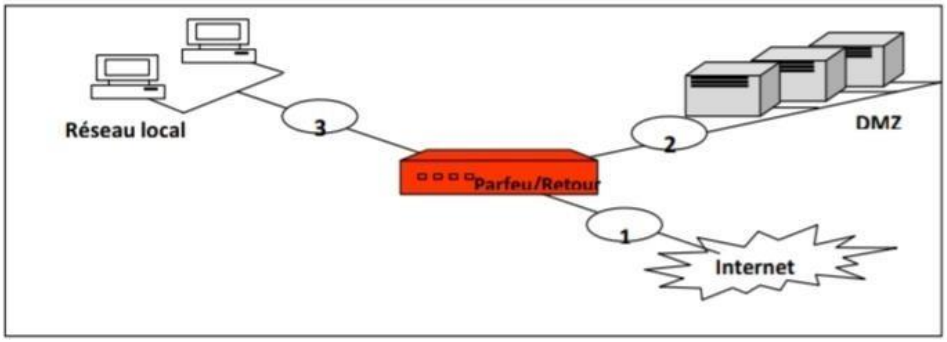

Figure 9: Emplacements des IDS.

- **Position (1)** : Dans cette position, l'IDS détecte toutes les attaques frontales de l'extérieur vers le pare-feu. Dans ce cas, de nombreuses alertes seront remontées, ce qui rendra les logs difficilement consultables.
- **Position (2) :** L'IDS placé sur la DMZ4 sert à détecter les attaques non filtrées par le pare-feu et appartenant à un certain niveau de compétence. Il sera plus clair de consulter les journaux ici car aucune attaque bénigne ne sera répertoriée.
- **Position(3) :** le but de l'IDS à cet emplacement est de signaler les attaques internes à partir du réseau local de l'entreprise. Considérant le fait que 80% des attaques viennent de l'intérieur, il serait peut-être judicieux d'en placer un ici.

2.7 Les avantages des systèmes de détection d'intrusion :

Les systèmes de détection d'intrusion (IDS) offrent de nombreux avantages pour aider à protéger les réseaux, les systèmes et les données contre les attaques malveillantes. Voici quelques-uns des avantages des systèmes de détection d'intrusion : [26]

- **Déjouer les attaques attendues sur le réseau :** Les IDS protègent les systèmes contre les attaques réseaux par : détection de porte dérobée, détection d'usurpation d'adresse IP, Dos, les vers, les chevaux de Troie, virus, Botnet, rootkit, Spyware, et autres menaces qui pourraient nuire au réseau, Les IDS actifs prennent des mesures automatiques contre les menaces de sécurité et les risques auxquels font face.
- **Avertis Administrateur réseau d'alerte pour les événements de sécurité potentiels :** la fonction de base des systèmes de détection d'intrusions est de générer des avertissements là où existent des menaces externes, internes ou de violations de la politique de sécurité réseau, et aussi

de fournir à l'administrateur des informations détaillées sur le mouvement des données au sein du réseau.

- **Gagnez du temps :** L'utilisation des IDS fournit beaucoup de temps et d'effort pour connaitre de ce qui se passe dans le réseau, peut aussi tourner en permanence sans superviseur humain.
- **Contrôle des Programmes utilisés par les employés pour surveiller l'Internet :** IDS peut aider à découvrir les programmes qui traitent de l'internet, cela permet de mieux contrôler et de protéger le réseau.
- **Avoir la confiance des clients :** Les IDS aident les organisations de protéger les données de ses clients contre le vol et la violation de la sécurité, Cela permet d'avoir la confiance des clients et partenaires et garder une bonne réputation sur l'organisation.
- **Économisez de l'argent :** Grace aux IDS les organisations peuvent déterminer les mouvements suspects dans le réseau et signaler les responsables pour prendre des mesures proactives en protéger le réseau et gagner l'argent qui sera dépensé si la violation de la sécurité est arrivé dans le réseau ou si le vol de renseignements personnels a eu lieu.

3 Les systèmes multi agents :

3.1 Définition :

Un agent est un système informatique situé dans un environnement, capable d'effectuer de manière autonome une action afin de remplir des objectifs **(Foukia, 2001)**. Dans le contexte de la détection d'intrusion, un système multi-agent est un ensemble de plusieurs agents qui peuvent réduire considérablement la charge de travail dans le réseau en répartissant les responsabilités entre les agents. Selon **(Achbarou, 2018)**, un agent peut être caractérisé par certaines propriétés :

• **Autonomie :** les agents peuvent agir et coopérer sans intervention externe. Ils ont la capacité de contrôler leur comportement et leurs actions.

• **Communication :** les agents échangent des messages entre eux afin de collaborer et de coordonner leurs actions. Le protocole de communication d'agent le plus populaire est le langage de communication d'agent (ACL).

• **Sociabilité :** les agents interagissent et collaborent les uns avec les autres pour atteindre un objectif commun.

• **Réactivité :** les agents peuvent modifier leur comportement grâce à l'apprentissage afin d'agir en fonction des changements externes dans l'environnement.

• **Proactivité :** les agents ont la capacité de prendre des initiatives pour atteindre un objectif [27].

3.2 Domaines d'application SMA :

Les Systèmes Multi-Agents ont de nombreuses applications dans différents domaines, notamment :

- **Intelligence artificielle** : Les SMA sont utilisés dans le développement d'agents intelligents capables de résoudre des problèmes complexes.
- **Robotique** : Les SMA sont utilisés pour la coordination de robots autonomes dans des environnements dynamiques.
- **Sciences sociales :** Les SMA sont utilisés pour modéliser et simuler des systèmes sociaux complexes tels que les marchés financiers, les systèmes de vote ou encore les comportements de foule.
- **Informatique distribuée :** Les SMA sont utilisés pour résoudre des problèmes de coordination et de communication entre des agents autonomes dans des environnements distribués.
- **Jeux vidéo :** Les SMA sont utilisés pour modéliser l'intelligence artificielle des personnages non-joueurs dans les jeux vidéo.
- **Logistique :** Les SMA sont utilisés pour la gestion de la chaîne logistique et l'optimisation des processus de production.
- **Sécurité :** Les SMA sont utilisés pour la surveillance et la sécurité des réseaux informatiques, la détection de menaces et la prévention d'attaques.

4 Les travaux connexes :

Dans cette section, nous mettons en évidence un certain nombre d'études qui ont appliqué les Systèmes Multi-Agents pour la détection d'intrusion dans IOT. [28] [23]

Dans [19], en 2005, construit un NIDS basé sur une approche de détection comportementale utilisant plusieurs classificateurs capables de détecter différents types d'attaques**. Un deuxième travail [17], en 2008**, concerne également l'utilisation de plusieurs classificateurs, de sorte que chacun puisse modéliser un groupe particulier de protocoles et de services réseau similaires. D'autres techniques comme les forêts aléatoires sont utilisées dans [27] [33] [16].

Dans [27], les auteurs proposent une architecture d'IDS multi-classes basée sur les forêts aléatoires. Au lieu d'utiliser l'attribut de classe pour prédire la classification, ils choisissent l'attribut de type de service (HTTP, FTP, etc.) comme classe à prédire. Cet attribut est choisi exclusivement pour détecter les valeurs aberrantes.

Dans [33], les auteurs proposent la combinaison d'un ensemble de classificateurs : LGP, ANFIS et RF. Le vote pondéré est également utilisé dans ce travail pour la prise de décision. Le classificateur Random Forest est également utilisé pour construire un modèle de système de détection d'intrusions dans [16]. Les résultats obtenus indiquent que le modèle présenté est efficace avec un faible taux de fausses alarmes et un taux élevé de détection [38].

D'autres auteurs [43], [28], [48] utilisent des techniques collaboratives pour améliorer leurs systèmes de détection. Dans [28], les auteurs développent un nouvel algorithme collaboratif pour la détection d'intrusions de logiciels malveillants basé sur les SVM. Dans ce travail, seulement quelques échantillons étiquetés sont nécessaires, tandis que les résultats de détection sont de haut niveau. Les expériences prouvent l'efficacité de ce modèle.

Dans [43], un nouveau cadre collaboratif d'IDS a été proposé pour le Cloud. Ce cadre intègre Snort pour détecter les attaques connues en utilisant la correspondance de signatures. Pour détecter les attaques inconnues, un système de détection d'anomalies (ADS) est construit en utilisant un classificateur d'arbres de décision et une machine à vecteurs de support (SVM). La corrélation des alertes et la génération automatique de signatures réduisent l'impact des attaques DoS et DDoS et augmentent les performances et la précision de l'IDS. Cependant, cela nécessite un temps d'apprentissage élevé [48]. Sur le même thème, un autre travail [48] propose un Système Collaboratif de Détection d'Intrusions Réseau (C-NIDS) pour détecter les attaques réseau dans le Cloud en surveillant le trafic réseau, tout en offrant une grande précision en abordant de nouveaux défis, notamment la détection d'intrusions dans les réseaux virtuels, la surveillance d'un trafic élevé, la scal-abilité et la capacité de résistance. De plus, dans ce cadre, les capteurs NIDS déployés dans le Cloud fonctionnent de manière collaborative pour faire face aux attaques coordonnées contre l'infrastructure du Cloud et la base de connaissances reste à jour. Cependant, ce travail manque de résultats permettant de valider le modèle proposé.

En 2017, Bostani [20] a proposé un cadre de découverte d'intrusion non supervisé et hybride pour reconnaître les attaques de transfert sélectif et de piège de données pour l'IoT.

Yulong et al. Ont proposé d'utiliser une technique de détection d'intrusion moderne pour l'environnement IoT, en accord avec une démonstration d'automatisation [21].Yulong et al. En comparant les flux d'activité préoccupés, cette IDS peut parfaitement identifier les jam-attaques, les fausses attaques et les attaques de réponse dans les réseaux IoT. Cette stratégie distingue trois types d'attaques IoT : fausses attaques, jam-attaques et attaques de réponse.

Kapitnov et al. [22] proposent un protocole potentiellement compatible avec les agents autonomes. Ils ont proposé un protocole architectural pour intégrer la communication à travers une technologie blockchain Ethereum dans les réseaux connectés peer-to-peer.

Calvaresi et al. [23] Déclarent que les comportements des agents sont des comportements autonomes et dépendants des utilisateurs. Ils ont conçu et mis en œuvre un système intégrant MAS, basé sur le Java agent development framework (JADE), et BTC, basé sur Hyperledger Fabric.

En 2018, Calvaresi et al. Les systèmes multi-agents combinés à la technologie blockchain pourraient faire face plus efficacement aux défis des environnements interconnectés sophistiqués. [24] examiné les systèmes multi-agents et les technologies de chaîne de blocs.

En 2018, Diro et al.ont proposé un IDS pour l'IdO où l'apprentissage profond est utilisé pour la détection des anomalies [26]. Cela s'est avéré efficace pour identifier les attaques d'organisation IoT Fog par rapport aux IDS classiques.

Casado-Vara et al. [28] Les architectures de bout en bout existantes sont optimisées par l'architecture hybride proposée. Une autre partie de cette architecture hybride est la gestion des données.

En 2019, Li et al. En utilisant l'apprentissage de la migration profonde, le IDS proposé peut surmonter l'absence d'ensembles de formation appropriés et résoudre les erreurs de classification des échantillons et les contraintes spatiales des problèmes de regroupement de données, en optimisant le modèle de détection des intrusions et en améliorant l'efficacité. Proposé un moyen d'extraction des données IoT et un nouveau IDS pour les villes intelligentes basé sur l'apprentissage de la migration profonde [29].

Un autre modèle d'apprentissage profond pour la détection des intrusions dans les réseaux a été proposé par **Le et al** [30]. Le processus d'apprentissage a eu lieu en utilisant plusieurs méthodes d'apprentissage profond, par exemple, les réseaux neuronaux récurrents (RNN).

Un autre travail notable présenté par **Arshad et al. [31]** en **2019** a proposé un nouveau cadre de détection d'intrusion pour les dispositifs IoT à ressources limitées [31]. Ce cadre vise à séparer la détection d'intrusion entre les dispositifs IoT et le routeur de bordure.

Anthi et al. Cette architecture IDS a été évaluée en utilisant des informations d'action organisées à partir d'un véritable banc d'essai et des scripts pour lancer des attaques multi-niveaux qui représentent le comportement d'un assaillant. En **2019**, ils ont proposé une conception IDS à

trois niveaux pour distinguer un comportement malveillant en temps réel dans les appareils domestiques IoT [32].

Ils préconisent une expérimentation plus approfondie, combinant les IDS avec de nouveaux modèles d'apprentissage automatique. La réponse à une enquête menée par Chaabouni et al.

En 2019 indique que les techniques d'apprentissage automatique sont efficaces en termes de sécurité et de confidentialité des réseaux [33].

5 Conclusion

La première partie de ce chapitre, nous avons tout d'abord commencé par la définition de système de détection d'intrusion, son architecture, ses types, puis nous avons présenté l'emplacement d'IDS, et nous citons quelques avantages.
Dans la deuxième partie nous avons défini le SMA et aussi les domaines SMA. Dans le prochain chapitre, nous présenterons une présentation plus au moins détaillée de la conception du système.

Chapitre 03
Conception et Implémentation

1 Introduction :

Ce chapitre est divisé en deux parties : la conception et l'implémentation des agents, et la description de l'application ainsi que l'exposé des résultats expérimentaux. Nous commencerons tout d'abord par la conception du système, en fournissant une description complète du projet, en fixant les objectifs, en présentant le modèle proposé et l'algorithme appliqué. D'abord, la Conception du système, nous détaillerons la conception du système en fournissant les informations suivantes : Description complète du projet .Nous expliquerons en détail le contexte et les motivations de notre projet, en soulignant les problèmes existants et la nécessité d'une solution améliorée.

Objectifs : Nous énumérerons les objectifs spécifiques que nous cherchons à atteindre avec notre système amélioré, en mettant l'accent sur les améliorations attendues par rapport aux systèmes existants.

Modèle proposé : Nous présenterons en détail le modèle que nous avons développé, enexpliquant son architecture, ses composants clés et son fonctionnement global. Nous justifierons également les choix de conception que nous avons faits.

Algorithme appliqué : Nous décrirons l'algorithme que nous avons utilisé dans notre système, en fournissant les détails de sa mise en œuvre et en expliquant comment il contribue à l'amélioration des performances. Ensuite, Implémentation des agents, nous expliquerons comment nous avons implémenté les agents dans notre modèle. Nous avons utilisé la base de test UNSW-NB15 pour évaluer l'efficacité de notre système proposé. Les outils suivants ont été utilisés pour l'implémentation : Eclipse, JADE et Weka.

Enfin, la description de l'application et résultats expérimentaux, nous présenterons en détail l'application développée en utilisant notre système amélioré. Nous expliquerons les fonctionnalités clés de l'application et comment elle résout les problèmes identifiés dans la conception initiale.

Ensuite, nous exposerons les différents résultats des expérimentations que nous avons menéespour évaluer les performances de notre système.

Pour conclure ce chapitre, nous effectuerons une analyse approfondie des résultats obtenus. Nous discuterons des performances de notre système par rapport aux objectifs fixés, en soulignant les points forts et les limites identifiés lors des expérimentations. Nous aborderons également les implications pratiques de nos résultats et les perspectives d'amélioration futures.

2 Conception

2.1 Objectif :

L'objectif de ce travail et le suivant :

Mettre en œuvre un système de détection d'intrusion basé sur le comportement des internet des objets et reposant sur les systèmes multi agents.

Pour faire ça nécessaire de réaliser les objectifs suivants :

- Comprendre les caractéristiques de l'Internet of Things.
- Création d'un système de sécurité permettant de détecter les attaques dans IOT.

Dans notre mémoire, nous utilisons le travail préalablement réalisé par M. Cheikh [52] dans son thèse intitulé "Exploitation de la visualisation et de la classification consensuelle à base d'agents pour l'amélioration de la détection d'intrusion" en 2018. Ce travail repose sur une approche de classification consensuelle qui utilise l'algorithme de Paxos. Le modèle proposé utilise un ensemble d'agents (classifieurs) capables d'assumer différents rôles dans l'algorithme Paxos, en fonction de leur capacité de classification. Cette approche a été validée en utilisant la base de données KDD. Toutefois, dans notre étude, nous avons remplacé les classifieurs de travail effectué par déautres (IBK, NaiveNet, J48graft...etc) afin d'obtenir de meilleurs résultats, en adoptant la détection d'intrusion dans l'IoT en utilisant la base de données UNSW-NB15.

2.2 L'algorithme de Paxos :

En informatique distribuée, Paxos est une famille de protocoles permettant de résoudre le consensus dans un réseau de nœuds faillibles, c'est-à-dire susceptible d'avoir des pannes. Le consensus désigne ici le fait que les différents nœuds se mettent d'accord sur un résultat [53],et c'est une opération difficile quand les nœuds ou leurs moyens de communications ont des pannes [54]

Paxos adopte une approche optimiste : c'est un algorithme best-effort. Comme le terme l'indique, il tente de faire 'au mieux'. Cela signifie qu'il garantit toujours la cohérence du système, c'est-à-dire la condition d'accord, mais ne garantit la terminaison du protocole que dans le cas où le système se comporte suffisamment bien et sur une période suffisante [121][52].

- L'algorithme Paxos est divisé en deux phases [56] :

2.2.1 La phase de lecture :

Un proposant envoie une proposition sous forme de requête « prepare » à un groupe d'accepteurs. Chaque requête est associée à un numéro de scrutin, choisi de manière croissante par les proposants et ordonné avec les numéros des autres scrutins choisis. Lorsqu'un accepteur reçoit une requête avec un numéro de scrutin plus grand que tous ceux déjà rencontrés, il répond avec un message d'acquittement et la dernière valeur acceptée. Il promet également de ne pas accepter de proposition avec un numéro de scrutin plus petit que celui reçu.

2.2.2 La phase d'écriture :

Un proposant permet de soumettre une proposition à un groupe d'accepteurs. Si la proposition est acceptée par une majorité d'accepteurs, le proposant envoie une requête accepte incluant la valeur de la proposition à tous les accepteurs. Si un accepteur reçoit une requête accepte incluant une proposition avec un numéro de scrutin, il accepte la valeur incluse dans la proposition à condition qu'il n'ait pas déjà répondu à un proposant suite à la réception d'une requête prépare d'une proposition avec un numéro de scrutin strictement plus grand que celui-ci.

• Le problème du consensus dans Paxos est exprimé en termes de trois ensembles d'agents : (cf.Figure1) [52]:

1. Proposers (les auteurs de proposition) qui peuvent proposer des valeurs.

2. Acceptors (les acceptants) qui choisissent une seule valeur.

3. Learners (les apprenants) qui vont apprendre quelle valeur a été choisie.

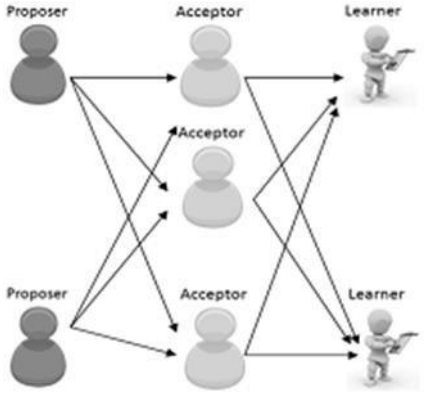

Figure 10: Architecture de Paxos.

2.3 Modèle proposé:

Dans le modèle SMA proposé, chaque agent représente un classifieur. Lorsqu'un agent client envoie un paquet, la recherche d'un consensus est déclenchée. Chaque agent prend une décision initiale (classe) en réponse à la requête et propose sa décision pour démarrer le processus de consensus. Ensuite, les agents entament la recherche du consensus en vue d'élire une classe commune "C", qui doit être l'une des classes initialement proposées par l'un des agents. Une fois le consensus atteint, la décision consensuelle "C" est envoyée en tant que réponse finale à l'agent client. [52]

2.4 Facteurs de détection de système :

2.4.1 Le facteur de confiance (FC) :

Le facteur de confiance représente par la valeur maximale du vecteur de distribution, qui est liée à la prédiction de classification.

2.4.2 Le facteur de performance (FP) :

La mesure est déterminée en utilisant la fonction F-Measure , ce qui permet de condenser les performances du classifieur en une seule valeur, selon la formule suivant : [52]

$$\text{F-measure}=\frac{2*Recall*precision}{Recall+precision}$$

- Precision représente le rapport entre le nombre de Tp et la somme des Tp et des FP.

Precision= $\frac{TP}{TP+FP}$

- Racall est définie comme le rapport entre le nombre de Tp et la somme des Tp et des FN

Recall= $\frac{TP}{TP+FN}$

3 Implémentation :

3.1 Environnement de programmation :

Parler de l'implémentation revient à détailler l'aspect matériel, l'environnement de développement et les différents outils qui ont été utilisé pour réaliser l'application.

3.1.1 Aspect matériel :

Notre projet a été développé sur un pc :

- Type : système d'exploitation 64bits.
- Processeur : Intel(R) Core (TM) 2 Duo CPU T6600 @2.20 GHz 2.20GHz.
- RAM: 4.00 Go.

3.2 Environnement de développement :

Dans cette section, nous présentons les outils et les logiciels que nous avons utilisés : Eclipse IDE, JADE (Java Agent Développement Framework) et Weka.

3.2.1 Eclipse:

Eclipse est un environnement de développement intégré libre extensible, universel et polyvalent, permettant de créer des projets de développement mettant en œuvre n'importe quel langage de programmation. Eclipse IDE est principalement écrit en Java (à l'aide de la bibliothèque graphique SWT, d'IBM), et ce langage, grâce à des bibliothèques spécifiques, est également utilisé pour écrire des extensions.La spécificité d'Eclipse IDE (IntegratedDevelopmentEnvironement) vient du fait de son architecture totalement développée autour de la notion de plugin : toutes les fonctionnalités de cet atelier logiciel sont développées en tant que plug-in [57]

Figure 11 : Le logo d'éclipse.

3.2.2 JADE :

JADE (Java Agent Development Framework) estun framework logiciel entièrement implémenté en langage Java. Il simplifie la mise en œuvre de systèmes multi-agents grâce à un middleware conforme aux spécifications FIPA et à un ensemble d'outils graphiques prenant en charge les phases de débogage et de déploiement [58].

Figure 12: Le logo de JADE.

3.2.3 Weka :

Weka est une collection d'algorithmes d'apprentissage automatique pour les tâches d'exploration de données. Il contient des outils pour la préparation des données, la classification, la régression, le clustering, l'exploration des règles d'association et la visualisation [59].

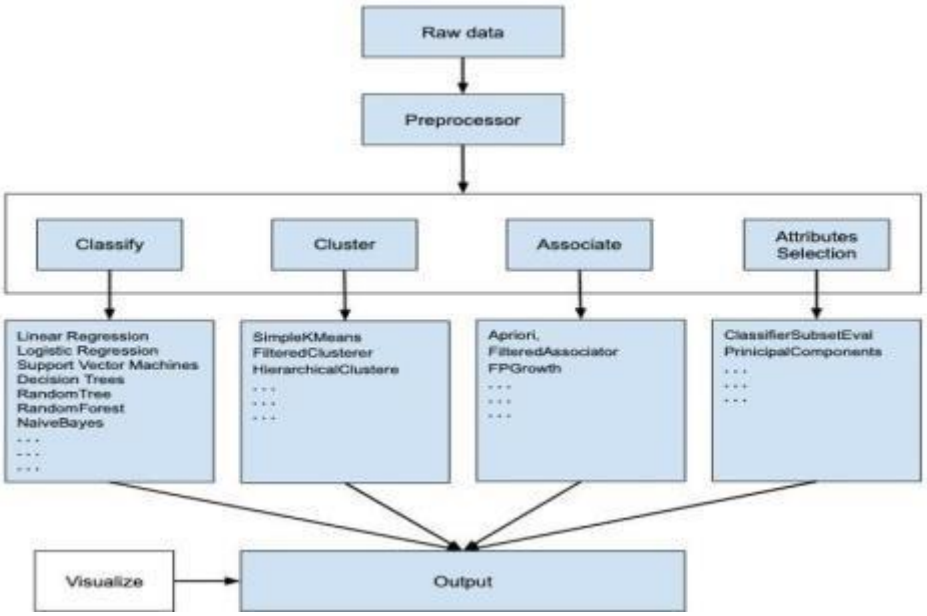

Figure 13: Diagramme de weka.

Si vous observez le début du flux de l'image, vous comprendrez qu'il y a de nombreuses étapes dans le traitement du Big Data pour le rendre adapté à l'apprentissage automatique. Tout d'abord, vous commencerez par les données brutes recueillies sur le terrain. Ces données peuvent contenir plusieurs les valeurs nulles et les champs non pertinents. Vous utilisez les outils de prétraitement des données fournis dans WEKA pour nettoyer les données. Ensuite, vous enregistrerez les données prétraitées dans votre stockage local pour appliquer ML algorithmes.

Ensuite, selon le type de modèle ML que vous essayez de développer, vous sélectionnerez l'une des options telles que Classer, Regrouper ou Associer. La sélection d'attributs permet de sélection automatique d'entités pour créer un jeu de données réduit.

A noter que sous chaque catégorie, WEKA propose l'implémentation de plusieurs algorithmes. Vous sélectionneriez un algorithme de votre choix, définiriez les paramètres souhaités et l'exécuteriez sur l'ensemble de données. Ensuite, WEKA vous fournirait la sortie statistique du traitement du modèle. Il vous fournit un outil de visualisation pour inspecter les données. Les différents modèles peuvent être appliqués sur le même jeu de données. Toi peut ensuite comparer les sorties de différents modèles et sélectionner le meilleur qui répond à votre objectif.

Ainsi, l'utilisation de WEKA se traduit par un développement plus rapide de modèles d'apprentissage automatique sur la totalité. Maintenant que nous avons vu ce qu'est WEKA et cqu'il fait, dans le chapitre suivant, apprenons

Comment installer WEKA sur votre ordinateur local [60].

- **Interface utilisateur graphique de WEKA :**

- **Explorer** : Un environnement pour explorer les données avec WEKA (la suite de cette documentationtraite de cette application plus en détail).

- **Expérimentateur** : un environnement pour effectuer des expériences et effectuer des tests entre les schémas d'apprentissage.

- **Knowledge Flow** : cet environnement prend essentiellement en charge les mêmes fonctions que Explorer mais avec une interface glisser-déposer. L'un des avantages est qu'il prend en charge apprentissage.

- **Simple CLI** : Fournit une interface de ligne de commande simple qui permet l'exécution directe de Commandes WEKA pour les systèmes d'exploitation qui ne fournissent pas leur propre ligne de commande interface.

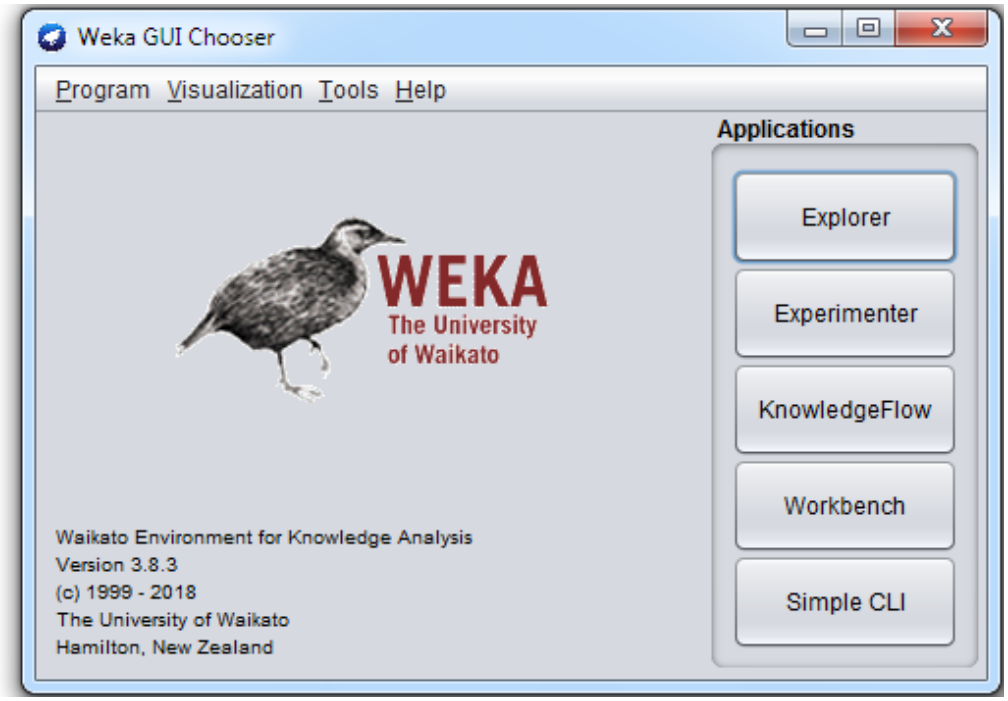

Figure 14: Interface graphique Weka.

Nous ne décrirons que le premier composant "Explorer".

- **Explorateur** : Les fenêtres de l'Explorateur WEKA affichent différents onglets en commençant par le prétraitement.
- Initialement, l'onglet de prétraitement est actif, car l'ensemble de données est d'abord prétraité avantd'être appliqué algorithmes et exploré le jeu de données. Les onglets sont les suivants :
- **Preprocess** : Choisissez et modifiez les données chargées.
- **Classifier** : appliquer des algorithmes d'entraînement et de test aux données qui seront classifiées et régressées les données.
- **Cluster** : Formez des clusters à partir des données.
- **Associer** : extrayez la règle d'association pour les données.
- **Sélectionner les attributs** : les mesures de sélection des attributs sont appliquées.
- **Visualiser** : la représentation 2D des données est visible.
- **Barre d'état** : la section la plus basse de la fenêtre affiche la barre d'état. Cette section montre ce qui se passe actuellement sous la forme d'un message, tel qu'un fichier est en cours chargé. Faites un clic droit dessus, les informations sur la mémoire peuvent être vues, et également Run ramasse-miettes pour libérer de l'espace peut être exécuté.
- **Bouton Log** : il stocke un journal de toutes les actions dans Weka avec l'horodatage. Les journaux sont affichés dans une fenêtre séparée lorsque le bouton Log est cliqué.
- **Icône d'oiseau WEKA** : présente dans le coin inférieur droit montre l'oiseau WEKA avec représente le nombre de processus exécutés simultanément (par x.). Lorsque le processus est courir l'oiseau se déplacera [60].

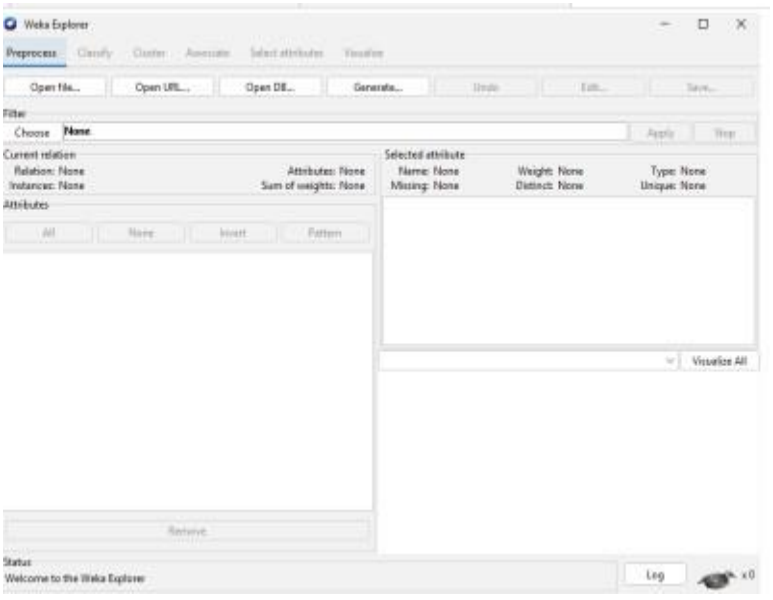

Figure 15 : Interface de l'explorateur weka.

3.3 Dataset UNSW-NB15 :

L'ensemble de données de sécurité du réseau informatique UNSW-NB15 a été publié en 2015 (Moustafa &Slay, 2015). Cet ensemble de données comprend 2 540 044 données normales et anormales modernes réalistes (également appelées comme attaque) les activités du réseau. Ces enregistrements ont été collectés par le générateur de trafic IXIA à l'aide de trois Serveurs virtuels. Deux serveurs ont été configurés pour distribuer le trafic réseau normal et le troisième l'un a été configuré pour générer le trafic réseau anormal [61].

Data set UNSW-NB15 est un ensemble de données de détection d'intrusion réseau qui contient divers types d'attaques et un trafic normal. Data set 10 % est un sous-ensemble de l'ensemble de données d'origine, contenant environ 175 000 instances. Il comprend à la fois des paquets réseau bruts et des fonctionnalités prétraitées extraites des paquets. Les attaques dans l'ensemble de données sont classées en quatre catégories principales : Fuzzers, Analyse, Portes dérobées et DoS. Le trafic normal comprend à la fois le trafic bénin et le trafic de fond. L'ensemble de données est couramment utilisé pour évaluer les systèmes de détection d'intrusion et les algorithmes d'apprentissage automatique pour les applications de sécurité réseau.

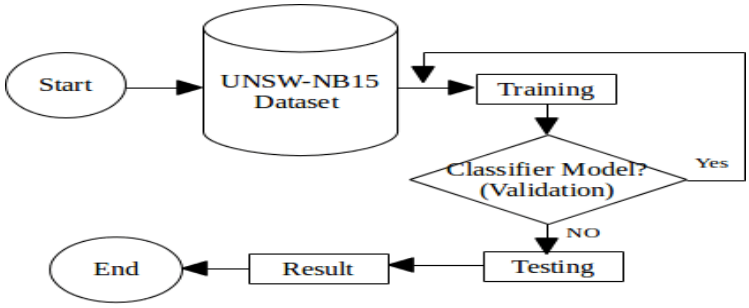

Figure 16 : Base de test UNSW_NB15

L'UNSW-NB15 est subdivisé en plusieurs ensembles de données principaux : UNSW-NB15-TRAIN, qui est utilisé pour entraîner différents modèles, et UNSW-NB15-TEST (100 %), qui est utilisé pour tester les modèles entraînés. Dans notre travail, nous avons également divisé UNSW-NB15-TRAIN en deux partitions suivantes : UNSW-NB15-TRAIN-1 (75 % de l'ensemble d'entraînement complet) pour l'entraînement et UNSW-NB15-VAL (25 % de l'ensemble d'entraînement complet) pour la validation avant le test. Cette deuxième partition est utilisée comme vérification de la cohérence des résultats obtenus pendant le processus d'entraînement. Lorsque

cette stratégie est utilisée, il est crucial d'éviter que le modèle s'entraîne sur l'ensemble d'évaluation ou de test, car cela pourrait conduire à un phénomène connu sous le nom de fuite de données. La fuite de données se produit pendant le processus d'entraînement lorsqu'un modèle voit des informations qu'il ne devrait pas voir, introduisant ainsi un biais dans le modèle final. Cela conduit à une mauvaise performance du modèle sur des données précédemment non vues [62].UNSW-NB15 contient des instances avec les catégories suivantes d'attaques réseau : Backdoor, Shellcode, Reconnaissance, Worms, Fuzzers, DoS, Generic, Analyse, Shellcode et Exploits. De plus, le Tableau 1 fournit les détails et la distribution des valeurs de chaque classe d'attaque dans les sous-ensembles de données. [63].

Types des attaques	**UNSW-NB15**	**UNSW-NB15-Val**	**UNSW-NB15-Train**	**UNSW-NB15-Test**
Normal	56000	14089	41911	14089
Generic	40000	9919	30081	9919
Exploits	33393	8359	25034	8356
Fuzzers	18184	4576	13608	4576
Dos	12264	3027	9237	3027
Reconnaissance	10491	2616	7875	2616
Analysis	2000	523	1477	523
Backdoor	1746	416	1330	416
Shellcode	1133	279	854	279
worms	130	31	99	31
Total	**175351**	**43835**	**131505**	**82332**

Tableau 1: Instances de répartition UNSW-NB15 [63].

3.3.1 Convertir les données csv en arrf :

- Ouvrez Weka. Si vous travaillez dans Weka, vous disposez d'un outil intégré qui convertira vosfichiers .CSV au format .ARFF. Vous trouverez généralement Weka dans le dossier.
- Cliquez sur le menu « Tools ». C'est dans la barre de menu en haut de la fenêtre Weka.
- Cliquez sur « ArffViewer ». Cela ouvre une fenêtre vide appelée ″ARFF-Viewer.″
- Cliquez sur le menu « File ». Il se trouve en haut de la fenêtre ARFF-Viewer.
- Cliquez sur « Open ». Une fenêtre de navigateur de fichiers apparaîtra.
- Accédez au dossier contenant le fichier .CSV
- Sélectionnez CSV data files (*.csv) dans le menu ″Files of Type″. Vous devriez maintenant voirle fichier .CSV que vous devez convertir dans la fenêtre.
- Sélectionnez-le .CSV et cliquez sur « Open ». Cela ouvre le fichier dans la visionneuse.
- Cliquez sur le menu « File ».
- Cliquez sur « Save As ».
- Nommez le fichier. Le nom du fichier doit se terminer par ″.ARFF″ (par exemple, mydata.ARFF).[64]

3.4 Choix des classifieurs :

Nous avons initié nos tests en utilisant un ensemble de classifieurs (IBK, J48, Bayes Net, Naive Byes, J48graft) pour adapter le système de détection d’intrusion. Le Tableau 2 représente les calssifieurs utilisés :

Agents	Classifieurs
Agent1	J48
Agent2	Bayes Net
Agent3	J48 graft
Agent4	Naive Baye
Agent5	IBK

Tableau2:classifieur sutilisés.

3.4.1 J48 :

Ross Quinlan [65] a développé l'algorithme C4.5 qui est utilisé pour générer un arbre de décision. Les arbres de décision sont produits à partir de J48, c'est-à-dire une implémentation Java Open Source de la version C4.5 dans l'outil de fouille de données WEKA [66]. Il s'agit d'un algorithme standard d'arbre de décision. L'un des algorithmes de classification en fouille de données est l'induction d'arbre de décision. L'algorithme de classification [67] est appris par induction pour construire un modèle à partir d'un ensemble de données pré-classifiées. Chaque élément de données est défini par des valeurs des caractéristiques ou des fonctionnalités. La classification peut être considérée comme une correspondance entre un ensemble de fonctionnalités et une classe particulière [68].

3.4.2 Naive Bayes :

Les classifieurs NaiveBayes sont famille de classificateurs probabilistes simples basés sur de fortes hypothèses d'indépendance entre les caractéristiques. Un classificateur Naive Bayes prétend que la présence (ou l'absence) d'un attribut spécifique d'une classe n'est pas associée à la présence (ou l'absence) d'autres caractéristiques. La classification bayésienne fournit des algorithmes d'apprentissage pratiques et les connaissances a priori et les données observées peuvent être combinées. La classification bayésienne offre une perspective utile pour comprendre et évaluer de nombreux algorithmes d'apprentissage. Elle calcul des probabilités explicites pour les hypothèses et est robuste au bruit dans les données d'entrée. L'entraînement est rapide car seule la probabilité de

chaque classe et la probabilité de chaque classe donnée différentes valeurs d'entrée (x) doivent être calculées. Aucun coefficient n'a besoin d'être ajusté par des procédures d'optimisation [69].

3.4.3 J48 graft :

Le greffon J48 est un algorithme basé sur les arbres de décision, c'est l'implémentation Java de l'algorithme C4.5 introduit par Ross Quinlan. Son objectif principal est de fonctionner sur l'apprentissage supervisé, la classification pour produire un arbre de décision. La technique de greffe ajoute des nœuds à un arbre de décision existant dans le but de réduire les erreurs de prédiction. J48 Graft utilise le concept suivant, mais le principal qu'il utilise est le ratio d'information gain comme critère de division. Il se concentre principalement sur la gestion des attributs de valeur qui sont continus ainsi que des attributs de valeur discrets. J48 Graft Normalized information gain ratio utilise des critères de division. J48 Graft est utilisé pour sélectionner les meilleures caractéristiques qui partitionnent l'ensemble de données en sous-ensembles contenant soit une classe, soit l'autre. L'objectif principal est de trouver les régions et branches feuillues existantes qui correspondent le mieux aux coupes pour créer de nouvelles feuilles avec d'autres classifications que l'original. L'arrêt se fait pendant le processus de division, ce qui amène le nombre d'instances à diviser en dessous d'un certain seuil [69].

3.4.4 IBK :

C’est une approche très simple et directe. Elle ne nécessite pas d’apprentissage mais simplement le stockage des données d’apprentissage. Son principe est le suivant. Une donnée de classe inconnue est comparée à toutes les données stockées. On choisit pour la nouvelle donnée la classe majoritaire parmi ses K plus proches voisins (Elle peut donc être lourde pour des grandes bases de données) au sens d’une distance choisie [70].

3.4.5 BayesNet :

Est une classe largement utilisée de modèles graphiques probabilistes. Ils se composent de deux parties : une structure et des paramètres. La structure est un graphe acyclique dirigé (DAG) qui exprime les indépendances conditionnelles et les dépendances entre les variables aléatoires associées aux nœuds. Les paramètres consistent en des distributions de probabilité conditionnelles associées à chaque nœud. Un réseau bayésien est une représentation compacte, flexible et interprétable d'une distribution de probabilité conjointe. C'est aussi un outil utile dans la découverte de connaissances car les graphes acycliques dirigés permettent de représenter les relations causales entre les variables. En général, un réseau bayésien est appris à partir de données [71].

3.5 Les mesures de performances :

Nous commencerons par exposer quelques mesures permettant d'évaluer les performances des IDS. L'efficacité d'une technique de détection d'intrusion est évaluée en fonction de sa capacité à effectuer des détections correctes. Selon la concordance entre la réalité d'un événement donné et la prédiction de la technique utilisée, il existe quatre possibilités (voir Tableau 3) [53].

		Prédiction de la valeur	
	Type	Attaque	Normal
Valeur actuelle	Attaque	TP	FN
	Normal	FP	TN

Tableau 3: La matrice de confusion.

Il existe quatre mesures pour évaluer les performances des IDS. L'évaluation de l'efficacité d'une technique de détection d'intrusion repose sur sa capacité à effectuer des détections correctes [53] :

- Les vrais-positifs (TP) correspondent aux situations où l'IDS génère une alerte pour un événement qui est effectivement une attaque légitime.
- Les faux-positifs (FP) se produisent lorsque l'IDS génère une alerte pour un événement qui n'est pas une véritable attaque.
- Les vrais-négatifs (TN) se produisent lorsque l'IDS ne génère pas d'alerte pour un événement qui n'est pas une attaque.

• Les faux-négatifs (FN) correspondent aux situations où l'IDS ne génère pas d'alerte pour un événement qui est pourtant une attaque.

3.6 **Résultats** :

Le tableau suivant représente les résultats obtenus à partir de taux de classification correct atteint par les différents classificateurs que nous avons utilisés pour détecter les intrusions.

Agents	Taux de ClassificationCorrecte
Agent A1 : (J48)	**95.94 %**
Agent A2 : (BayesNet)	**88.44%**
Agent A3 : (J48graft)	**95.77%**
Agent A4 :(NaiveBayes)	**80.49%**
Agent A5 : (IBK)	**95.98%**
Consensus	**96.85%**
Max_Function	**94.20%**

Tableau 4:Résultats relatifs aux Taux de Classification Correcte.

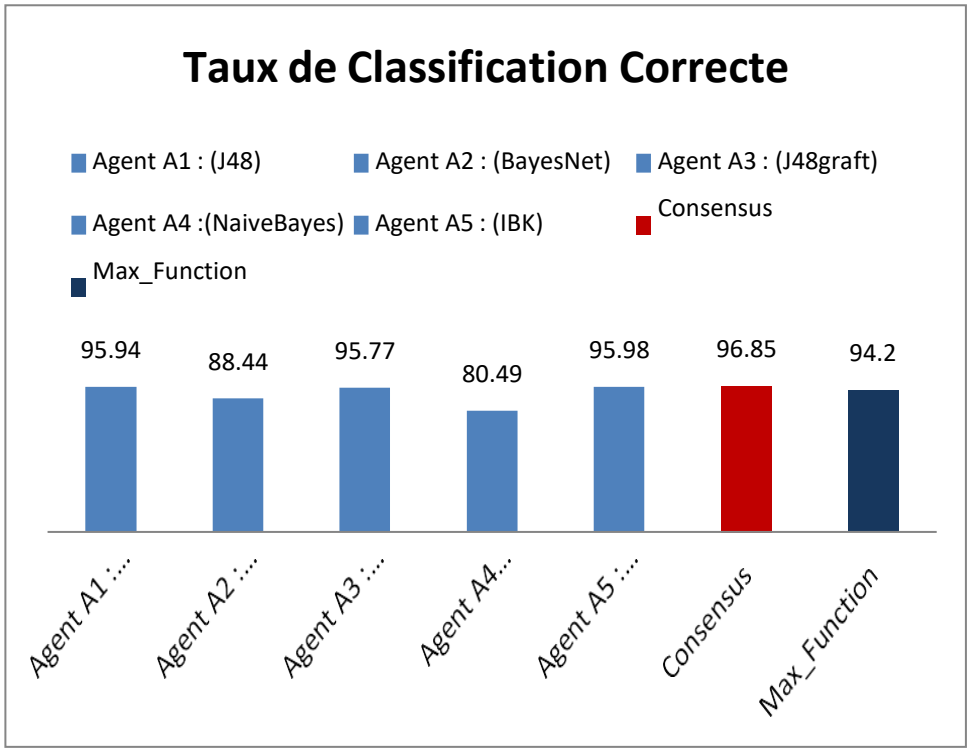

Figure 17: Graphiques à barres montrant le pourcentage de TCC.

- Le classifieur consensus est supérieur à tous les autres détecteurs (les cinq classifieurs et Max_ Function) car il tire parti des points forts de chaque classificateur.

Conclusion

Dans ce chapitre, nous avons introduit un modèle SMA pour la classification consensuelle qui repose sur l'algorithme Paxos. Notre modèle permet à un agent de jouer différents rôles en fonction de sa capacité en termes de classification. Pour parvenir à une décision consensuelle, nous avons utilisé l'algorithme Paxos comme base.

Nous avons validé le modèle proposé en effectuant une simulation basée sur 10% de l'UNSW-NB15. Les résultats de la simulation, comparés aux techniques de détection classiques, démontrent la supériorité de notre méthode de classification.

Conclusion générale :

Les systèmes multi-agents de détection d'intrusions pour l'IoT (Internet des objets) offrent une approche prometteuse pour sécuriser les environnements connectés. Ces systèmes tirent parti de l'intelligence collective et de la collaboration entre plusieurs agents pour détecter les menaces.

Le travail présenté dans ce mémoire s'inscrit dans le domaine de la sécurité informatique et plus précisément dans les systèmes de détection d'intrusion dans l'IoT. Nous nous sommes concentrés sur un algorithme qui a déjà été proposé dans le cadre de [52].

Nous avons utilisé le travail réalisé par [52] dans notre recherche, en remplaçant les classifieurs traités dans le travail précédent [référence] par d'autres classifieurs tels que : IBK, BayesNet, NaiveBayes, J48, J48graft. Nous avons également utilisé l'ensemble de données UNSW_NB15 pour la détection des attaques. Notre objectif était d'explorer la détection de ces attaques dans l'IoT.

Après l'analyse des résultats, nous avons obtenu de meilleurs résultats, ce qui nous a permis d'améliorer le système et de résoudre les problèmes identifiés précédemment. Ces résultats démontrent l'efficacité des classifieurs utilisés et l'applicabilité de notre système pour la détection d'intrusions dans l'IoT.

Cependant, il convient de noter que notre travail ne se limite pas à l'exploration des classifieurs, mais comprend également d'autres aspects importants tels que la préparation des données, la sélection des caractéristiques et l'évaluation des performances. Ces éléments ont été abordés de manière approfondie dans notre étude et ont contribué à l'amélioration globale du système de détection d'intrusion.

En conclusion, notre recherche a permis de renforcer les fondements des systèmes multi-agents de détection d'intrusions pour l'IoT et de proposer un système plus performant grâce à l'utilisation de différents classifieurs. Ces résultats ouvrent de nouvelles perspectives pour la sécurisation des environnements connectés et constituent une avancée significative dans le domaine de la sécurité informatique.

Bibliographie

[1] DJOGHMA Younes, Reconstruction d'architecture pour les systèmes IOT, Master académique en informatique, Spécialité : Génie Logiciel et Systèmes Distribués (GLSD) 2021 – 2022. (PDF, page 9)

[2] Imad Saleh Laboratoire Paragraphe à l'Université de Montpellier, Introduction à l'internet des Objets (IdO) : Concepts, Enjeux, Défis et Perspectives, February 2018.(PDF, page 02) DIO :21494.OP.2018.0229

[3] https://blog-mdce.fr/le-vetement-sportif-connecte/

[4] Mr. BELHADJ Naceur et Mr. ABBAD Abdelhak , La sécurité de l'Internet des Objets (IoT),(PDF, Page 1 , page 7)

[5] A.-B. Mohamed et R. Ehab, «Internet of things in smart education environment: Supportive framework in,» Wiley, vol. 10, pp. 2-11, 2018.

[6] Melle LARRAS Melissa et Melle KHALFOUNI Djamila, Défis de sécurité de l'Internet des Objets Problèmes et solutions, Master académique en informatique, Spécialité : Système Informatique (SI).

[7] France STRATEGIE,Le monde de l'Internet des objets :des dynamiques à maîtriser,RAPPORT FEVRIER 2022(PDF ,page 39 jusqu'à page 42)

[8] Hadjaj Walid , Etude de Cas sur un système médical domotique controler par unSMA (PDF, page 13jusqu'a page 24) , 13/06/2018.

[9] AFOUF Oussama, Développement d'un Système d'IoT (Internet of Things) dansle cadre de Smart University 2020,(PDF, page 25,page 27)

[10] https://www.somfy.fr/produits/automatismes-et-maison-connectee/maison- connectee

[11] https://fr.digi.com/blog/post/the-benefits-of-iot-real-world-examples

[12] Mohamed Tahar HAMM ,Thèse de doctorat de l'Université Paris-Saclay

préparée à Télécom Paristech , Sécurisation de l'Internet des objets, Spécialité de doctorat: Réseaux et sécurité informatique. le 17 Septembre 2018.

[13] https://easypartner.fr/blog/comment-renforcer-la-securite-des-donnees-dans-liot.

[14] https://www.objetconnecte.com/surface-dattaque-iot-quelles-menaces-comment- les-resorber/

[15] https://www.objetconnecte.com/risques-securite-iot/#google_vignette

[16] https://easypartner.fr/blog/comment-renforcer-la-securite-des-donnees-dans-liot

[17] A survey on anomaly based host intrusion detection system. Shijoe Jose, D.Malathi,Bharth Reddy,Dorathi Jayaseeli. 2018 2018, Jornal of Physics, p. 1.
[18] Rapport final, Les systèmes de détection d'intrusion (IDS). 2018.
[19] cédric Michel. Langage de description d'attaques pour la détection d'intrisions par coorélation d'événements ou d'alerts en environnement réseau hétérogéne. Université Rennes 1: s.n., 2003.
[20] Ansam,khraisat, Iqbal, Gondal et Peter, Vamplew.An Anomaly Intrusion Detection System Using C5 Decision Tree Classifier. 2018. pp. 146-155.
[21] Spadaccino, pierto et Cuomo, Francesca. INTRUSION DETECTION SYSTEMS FOR IOT: OPPORTUNITIES AND CHALLENGES OFFERED BY EDGE COMPUTING AND MACHINE LEARNING. University of Rome,Italy : s.n. pp. 2-3.
[22] A. Aldweesh, A. Derhab, and A. Z. Emam, ``Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," Knowl.- Based Syst., vol. 189, Feb. 2020, Art. no. 105124, doi: 10.1016/J.KNOSYS.2019.105124.
[23] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, ``A survey of deep learning-based network anomaly detection," Cluster Comput., vol. 22, pp. 949961, Sep. 2017, doi: 10.1007/s10586-017-1117-8.
[24] Applicability of Intrusion Detection System on Ethereum Attacks: A Comprehensive Review,ARKAN HAMMOODI HASAN KABLA, MOHAMMED ANBAR , SELVAKUMAR MANICKAM, TAIEF ALAA AL-AMIEDY, PETERSON BERNABE CRUSPE , AHMED K. AL-ANI , et SHANKAR KARUPPAYAH .2022
[25] Chaima KOUIDR, Intrusion Detection System with Grey WolfOptimizer (GWO), International Journal of Informatics and Applied Mathematicse-ISSN: 2667-6990.
[26] A. Pharate, H. Bhat, V. Shilimkar, N. Mhetre, "Classification of Intrusion Detection System", International Journal of Computer Applications (0975 – 8887), Volume 118 – No. 7, May 2015
[27] Chao Liang, Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems,2020
[28] Beneddine Mustapha et Mohamed Amine Abid Malika , "Conception d'un IDS basé sur le Deep Learning et RBN" ,Memoire MASTER, Spécialité : Réseaux et Télécommunications, UNIVERSITE IBN KHALDOUN – TIARET, 2020-2021.
[29] Beneddine Mustapha Mohamed Amine,Abid Malika ,Conception d'un IDS basésur le Deep Learning et RBN, à Tiaret ,2020-2021

[30] Tesnim Younes, Farah Jemili," a Multi-Agent-Based System For Intrusion detection ", 2021.
[31] Chao Liang, Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems.
[32] F.Roli G.Giacinto, R.Perdisci. 2005. Network Intrusion Detection by Combining One-class Classifiers. International Conference on Image Analysis and Processing,ICIAP,
[33] M. Del Rio F. Roli G. Giacinto, R. Perdisci. 2008. Intrusion detection in computer networks by a modular ensemble of one-class classifiers. Inf. Fusion, vol. 9, no 1, Elsevier Science Publishers (2008), p. 69âĂŞ82.
[34] M.ZULKERNINE J.ZHANG. 2006.. Anomaly based network intrusion detection with unsupervised outlier de tection. Proc. of the IEEE ICC, 2388–2393.
[35] S.Shamsuddin A Zainal M. Maarof. 2009. Ensemble Classifiers for Network Intrusion Detection System. Journal of Information Assurance and Security, vol. 4(2009).
[36] N. Farnaaz and M. A. Jabbar. 2016. Random Forest Modeling for Network Intrusion Detection System. In Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016).
[37] S. Zainudin O. F. Rashid, Z. A. Othman. 2017. A Novel DNA Sequence Approach for Network Intrusion Detection System Based on Cryptography Encoding Method.International journal on advanced science engineering information technology, Vol 7, ISSN:2088-5334 (2017), pp. 459–464.
[38] B. Bhavesh M. Chirag S. Dinesh, P. Dhiren. 2016.. Collaborative IDS Frameworkfor Cloudtext. In International Journal of Network Security.18. 699–709.
[39] Y. Wang X. Zhu H. Wang K. Zhang, C. Li. 2017. Collaborative Support Vector Machine for Malware Detectiontext. In In Procedia Computer Science, Volume 108, ISSN 1877-0509. Pages 1682–1691.
[40] A.Mamouni Z. Al Haddad, H. Mostafa. 2016. A collaborative network intrusion detection system (C-NIDS) in cloud computingtext. International Journal of Communication Networks and Information Security (IJCNIS),Vol.8, (2016), 130–135./
[41] Bostani, H.; Sheikhan, M. Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach. Comput. Commun. 2017, 98, 52–71
[42] Fu, Y.; Yan, Z.; Cao, J.; Koné, O.; Cao, X. An Automata Based IntrusionDetection Method for Internet of Things. Mob. Inf. Syst. 2017, 2017, 1750637.

[43] Kapitonov, A.; Lonshakov, S.; Krupenkin, A.; Berman, I. Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs. In Proceedings of the Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), Linkoping, Sweden, 3–5 October 2017; pp. 84–89.
[44] Calvaresi, D.; Calbimonte, J.P.; Dubovitskaya, A.; Mattioli, V.; Piguet, J.G.; Schumacher, M. The Good, the Bad, and the Ethical Implications of Bridging Blockchain and Multi-Agent Systems. Information 2019, 10, 363.
[45] Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. Future Gener. Comput. Syst. 2018, 82, 761–768. [CrossRef]
[46] Casado-Vara, R.; Prieta, F.D.L.; Prieto, J.; Corchado, J.M. Blockchain frameworkfor IoT data quality via edge computing. In Proceedings of the BlockSys'18: 1st Workshop on Blockchain-enabled Networked Sensor System 2018, Shenzhen, China, 4 November 2018.
[47] Li, D.; Deng, L.; Lee, M.; Wang, H. IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. Int. J. Inf. Manag. 2019, 49, 533–545.
[48] Le, T.-T.-H.; Kim, Y.; Kim, H. Network Intrusion Detection Based on Novel Feature Selection Model and Various Recurrent Neural Networks. Appl. Sci. 2019, 9, 1392.
[49] Arshad, J.; Azad, M.A.; Abdeltaif, M.M.; Salah, K. An intrusion detection framework for energy constrained IoT devices. Mech. Syst. Signal Process. 2020, 136, 106436.
[50] Anthi, E.; Williams, L.; Slowinska, M.; Theodorakopoulos, G.; Burnap, P. A Supervised Intrusion Detection System for Smart Home IoT Devices. IEEE Internet Things J. 2019, 6, 9042–9053.
[51] Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Commun. Surv. Tutor. 2019, 21, 2671–2701.
[52] Cheikh Mohamed, Exploitation de la visualisation et de la classification consensuelle à base d'agents pour l'amélioration de la détection d'intrusion, Université Constantine 2 Mehri Abdelhamid, 2018.
[53] L. Lamport, «Lower Bounds for Asynchronous Consensus,» Distributed Computing 19, 2 (2006), 79-103, 2006.

[54] M. Pease, «Reaching Agreement in the Presence of Faults,» Journal of the Association for Computing Machinery, vol. 27, no 2, 1980.
[55] C. Pira, «Une méthodologie pour appréhender la décision collective dans des systèmes multiagents sujets aux défaillances,» thèse de doctorat de l'Université Pierre et Marie Curie, Paris VI, Paris, 2009.
[56] L. Lim, «Gestion de groupe partitionnabledans les réseaux mobiles spontanés,» Thèse de doctorat, Telécom SudParis et Université d'Evry-Val-d'Essonne , Evry-Val- d'Essonne, 2012.
[57] https://munier.perso.univ-pau.fr/temp/M4207C/TP1%20Intro%20Eclipse.pdf

[58] https://jade.tilab.com

[59] https://www.cs.waikato.ac.nz/ml/weka/

[60] www.tutorialspoint.com.

[61]

62 Shabtai A, Elovici Y, Rokach L. A survey of data leakage detection and prevention solutions. Berlin: Springer; 2012
63 Sydney M. Kasongo and Yanxia Sun, Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset, 2020, https://doi.org/10.1186/s40537-020-00379-6.
[64] https://www.wikihow.tech/Convert-CSV-to-ARFF.

[65] Quinlan, J. R. C4.5: Programs for Machine Learning. Morgan Kaufmann Publishers, 1993.
[66] http://en.wikipedia.org/wiki/C4.5_algorithm

[67]Report from Pike research, http://www.pikeresearch.com/research/smartgrid-dataanalytics
[68]Jehad Ali1, Rehanullah Khan2, Nasir Ahmad3, Imran Maqsood, Random Forests and Decision Trees, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 3, September 2012.
[69] Gaurav Meena, Ravi Raj Choudhary, A Review Paper on IDS Classification using KDD 99 and NSL KDD Dataset in WEKA,2017.

[70] Faïcel Chamroukhi, Classification supervisée, Les K-plus proches voisins, Université de Caen ,Lab of Mathematics Nicolas Oresme.
[71] https://www.uib.no/en/rg/ml/119695/bayesian-networks.