الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة سعيدة د.مولاي الطاهر

كلية التكنولوجيا

قسم: الإعلام الآلي

Mémoire de Master

Spécialité : Sécurité informatique et Cryptographie

Thème

Conception et réalisation d'un Système de détection d'intrusion entre les Objets Connectés

Présenté par :

Metarfi Mebarka Sara

Tedjini Imene

Dirigé par :

Limam Said

Année universitaire 2022-2023

Dédicaces

Je dédie cet ouvrage a ma mère et mon père, qui m'ont soutenu et encouragé pendant toutes ces années de scolarité. J'espère qu'ils trouveront ici un témoignage de ma profonde gratitude.
À mes frères, sœurs, familles, proches et enseignants.
Merci à tous mes amis qui m'ont toujours encouragé : Halima, chaima, Rashida, chaimaa et Fatima. Je leur souhaite plus de succès.

je rends grâce à mon dieu de m'avoir donné la force , la volonté et la sagesse d'être patiente dans mes études Je dédie ce travail à : Ce qui m'a donné la vie , et de mon courage, mon très cher père merci papa Ma chère maman, que nulle dédicace ne peut exprimer mes sincères sentiments, pour sa patience illimitée, ses encouragement continu et son profond amour. sans oublier mes chers frères ibrahim et iness pour leur grand amour et leur soutien , qu'ils trouvent ici l'expression de ma haute gratitude. A toute la famille de tedjini et bouazza A ma copine binôme sara A toutes mes chers amis Et toutes les personnes que j'ai oublié involontairement .

REMERCIEMENT

Je tiens à exprimer toute ma reconnaissance à mon directeur de mémoire, Dr.SAID LIMAM. Je le remercie de m'avoir encadré, orienté.
J'adresse mes sincères remerciements à tous les professeurs, intervenants et toutes les personnes qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques ont guidé mes réflexions et ont accepté de me rencontrer et de répondre à mes questions durant mes recherches.

Résumé

en raison de leur utilisation excessive dans divers domaines et du faible niveau de sécurité sur Internet et sur les réseaux en général, notre objectif dans ce travail a été d'assurer la sécurité des objets connecté. en même temps pour atteindre une sécurité complète qui englobe tous les aspects. Nous avons utilisé l'apprentissage automatique et l'apprentissage profond et pour y parvenir nous avons proposé une stratégie conçu pour être un système de détection d'intrusion dans l'environnement des objets connectés.

Mots clés : les objets connectés, Systéme de détection d'intrusion,l'apprentissage Automatique ,l'apprentissage profond ,IFogSim

Abstarct

due to their excessive use in various fields and the low level of security on the Internet and on networks in general, our objective in this work has been to ensure the security of internet of things. at the same time to achieve complete security that encompasses all aspects. We have used machine learning and deep learning that are artificial intelligence solutions and to achieve this Our proposed plan is designed to be an intrusion detection system in the environment of internet of things.

Keywords : Internet of things, Intrusion detection system , Machine learning , Deep learning ,IFogSim

ملخص:

نظرا للإفراط في استخدامها في مختلف الميادين وانخفاض مستوى الأمن على شبكة الإنترنت وعلى الشبكات بوجه عام، كان هدفنا في هذا العمل هو ضمان أمن الأجسام المتصلة حيث تطرقنا الى فهم معنى و هيكلة الاشياء المتصلة بالانترنيت .

في نفس الوقت حاولنا تحقيق الامن الكامل الذي يشمل جميع الجوانب. من بين افظل الحلول اخترنا التعلم الالي و التعلم العميق لنصمم به نظام للكشف عن التسلل, حيث اقترحنا استراتيجية مصممة بشكل دقيق لتكون نظام كشف التسلل في بيئة الاشياء المتصلة بالانترنيت.

الكلمات المفتاحية:انترنيت الاشياء , نظام الكشف عن التسلل , التعلم الالي , التعلم العميق

Table de Matières

Introduction Générale

La collecte de données en temps réel aide les entreprises à améliorer leur flux de travail et à réduire les coûts d'exploitation, ce qui permet aux machines de fournir des informations sur l'état afin que les techniciens puissent planifier la maintenance avant que la défaillance n'affecte la production, améliore l'efficacité opérationnelle et contribue à réduire les coûts.

Toutes ces fonctionnalités nous fourni par la technologie moderne sous le soi-disant Internet des objets.

Ces caractéristiques ont permis à différents secteurs d'utiliser l'IoT et de s'y fier pour gérer leurs données, mais cela a eu l'effet contraire, de sorte que l'équipement IoT n'est pas toujours inclus. Assurer la sécurité des données collectées et transmises par les dispositifs IoT est un défi, en particulier lorsque les dispositifs IoT sont utilisés dans des domaines plus sensibles tels que la santé, l'assurance et la défense.

Il existe de nombreux cadres de sécurité pour l'IoT, mais jusqu'à présent il n'y a pas une seule norme acceptable de l'industrie.

Cependant, la simple adoption d'un cadre de sécurité IoT pourrait être utile, Il fournit des outils et des listes de contrôle pour aider les entreprises à créer et à déployer des dispositifs IoT. Parmi les cadres de sécurité figurent les systèmes de détection d'intrusion.

le système de détection d'intrusion **(ids)** est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussie comme échouées des intrusions.

Le système de détection d'intrusion dépend de deux, en savoir plus sur les logiciels malveillants ou la découverte de déviations du modèle qui représente les bons comportements est associée à l'apprentissage automatique et l'apprentissage profond qui sont des nouvelles approches de l'intelligence artificielle et qui a fourni des résultats étonnants dans le domaine de la sécurité grâce à des méthodes de classification.

Notre objective est de réaliser un système de détection d'intrusion dans un environnement IoT, alors on a besoin de connaissions bien notre environnement et leur architecture pour l'emplacement de notre système de sécurité.

Notre mémoire est divis en 4 chapitres, un chapitre d'état de l'art qui présente c'est quoi un objet connecté, comment un environnement IoT basé sur le cloud et le fog computing.

Dans le chapitre 02 nous avons définit la sécurité et les système de sécurité, la détection d'intrusion et comment utilisé pour un environnement IoT.

En suit, le chapitre 03 présente la stratégie que nous avons proposé pour un système de détection d'intrusion, les méthodes que nous avons utilisés et leurs principe de fonctionnement. En fin le chapitre 04 présente les résultats de simulation que nous avons effectué afin d'évaluer notre stratégie.

CHAPITRE 1

Etat de l'art sur les objets connecté IoT et sur le Cloud et le Fog computing

1.1. INTRODUCTION

Depuis son émergence, la technologie a aidé à faciliter la vie humaine grâce à des inventions réelles et pratiques. En particulier, en ce qui concerne Internet, les réseaux publics et privés facilitent la communication et le traitement d'applications numériques telles que la radiodiffusion en direct, la radiodiffusion audio, la messagerie instantanée, etc. En 2010, le concept d'Internet et des télécommunications a été étendu aux objets dits Internet, ces derniers se référant à la communication des personnes et leur capacité à traiter, exploiter, gérer et contrôler des données à distance sans interférence directe. L'application de ce concept englobe différents domaines tels que les soins de santé, les transports, l'industrie automobile et les maisons intelligentes.[1]

1.2. LES OBJETS CONNECTÉS

1.2.1. DÉFINITION

Il est considéré comme une évolution de la soi-disant RFID (identification par radiofréquence), un dispositif de stockage et de récupération de données à distance. Il a donné aux systèmes la possibilité d'augmenter la vitesse de lecture de l'information et de créer des réseaux de capteurs et de nœuds interconnectés qui permettent une plus grande quantité d'information disponible simultanément via une station de base.

Un dispositif électronique se connecte à un dispositif distant par échange de données ou est un système de dispositifs informatiques inter-connectés qui peuvent collecter et transmettre des données par des réseaux sans fil sans interférence humaine, dont certains sont faciles à accepter et à utiliser même par ceux qui ne sont pas familiers avec les nouvelles technologies telles que l'éclairage connecté. Tandis que d'autres sont vraiment des forces technologiques qui permettent à n'importe qui de construire un grand projet de démotique. Le développement de l'IOT comprend de nombreuses questions telles que l'infrastructure, les communications, les interfaces, les protocoles et les normes.[2]

1.2.2. COMMENT FONCTIONNE UN OBJET CONNECTÉ

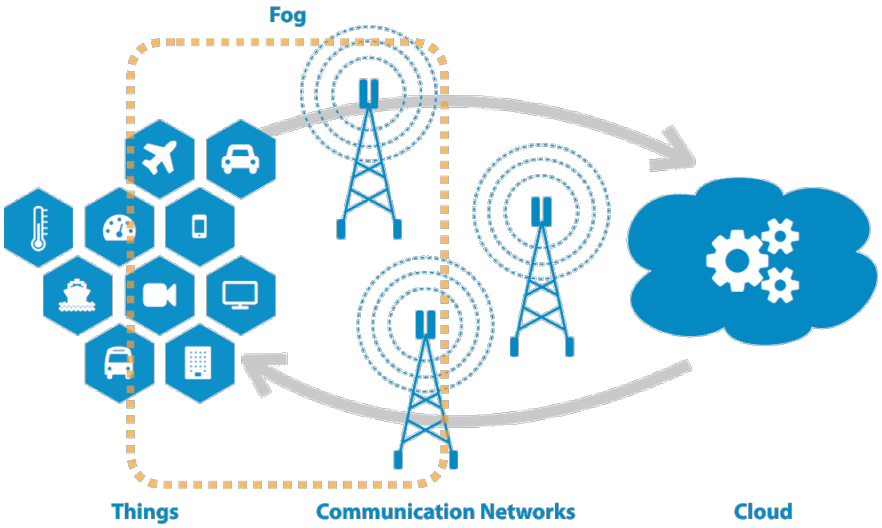

FIGURE 1.1 – *comment fonctionne un objet connecté*

l'Internet des objets fonctionne sur les données collectées par les capteurs, qui sont des dispositifs intelligents soutenus par le Web qui utilisent des systèmes intégrés qui représentent le système des objets connecté, où ils envoient des données de capteur au **cloud** et peuvent même interagir avec d'autres objets sans interférence humaine, bien que les gens puissent interagir avec les appareils - par exemple, pour former ou donner des instructions ou accéder aux données.[2]

1.2.3. LES PRINCIPALES COMPOSANT D'UN OBJET CONNECTÉ

Comme nous l'avons déjà considérée la définition que les objets Internet sont tous des objets qui peuvent interagir à distance sans intervention humaine dynamiquement et soutenir la communication entre eux. Parmi les facteurs qui interfèrent avec la conception de l'architecture de l'Internet des objets figurent le réseautage, la connectivité, les processus et d'autres facteurs, tout en veillant à ce qu'ils soient décentralisés, hétérogènes, extensibles et interopérables. [3]

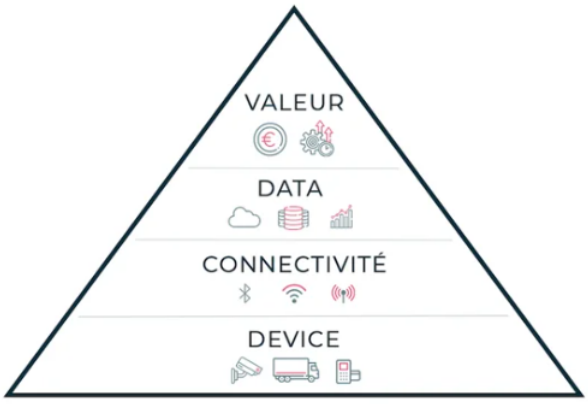

FIGURE 1.2 – *architecture d'un objet connecté*

— les capteurs (devices) : qui captent et collectent les données physiques environnantes. Cela peut être un taux d'humidité, une température, une présence, une pression.

— la connectivité : à savoir, comment cette donnée captée va être communiquée sur le réseau Internet, par exemple le Wifi de votre foyer, le réseau cellulaire de votre téléphone, le Bluetooth de votre voiture, etc.

— la donnée (data) : Les données arrivent à l'état brut. Ce sont des suites de chiffres qui doivent être triées, analysées, stockées.

— la valeur : transformer ces données traitées pour leur donner du sens et de la valeur. par exemple, l'application de votre téléphone qui communique la température de votre maison via les différents thermostats.

1.2.4. L'OBJECTIF DU L'IOT

Les objectifs de l'IoT peuvent être regroupés en plusieurs catégories :

1.2.4.1. L'EFFICACITÉ ET DE LA PRODUCTIVITÉ

De nombreux objets peuvent travailler de manière autonome et communiquer entre eux pour exécuter des tâches et prendre des décisions grâce à l'Internet des objets.

En automatisant certaines tâches et en permettant aux objets de fonctionner de manière plus intelligente et plus coordonnée, cela peut réduire les coûts et améliorer l'efficacité.[4]

1.2.4.2. L'efficacité énergétique

En permettant à certains objets de s'adapter automatiquement aux niveaux de consommation d'énergie et aux conditions environnementales, l'Internet des objets peut être utilisé pour optimiser l'utilisation de l'énergie. Par exemple, un réfrigérateur connecté peut être configuré pour s'éteindre lorsqu'il n'est pas utilisé et pour modifier sa consommation d'énergie en fonction de la température extérieure.[4]

1.2.4.3. Création de nouvelles opportunités d'affaires

En permettant aux entreprises de collecter et d'analyser des données en temps réel sur l'utilisation de leurs produits et services, l'IoT peut créer de nouvelles opportunités d'affaires. Cela peut aider les entreprises à mieux comprendre les besoins de leurs clients et à améliorer les produits et services qu'elles proposent.[4]

1.2.4.4. Amélioration de la sécurité

En permettant à certains objets de détecter et de signaler des situations dangereuses ou suspectes, l'Internet des objets peut être utilisé pour améliorer la sécurité. Par exemple, il est possible de configurer un système de sécurité connecté pour envoyer une alerte en cas de détection d'une intrusion ou d'une fuite de gaz.[4]

notre objective et de améliorer la sécurité entre les objets connectées, donc nous basons sur l'architecture qui définit un environnement de connexion des objets avec des services tiers.

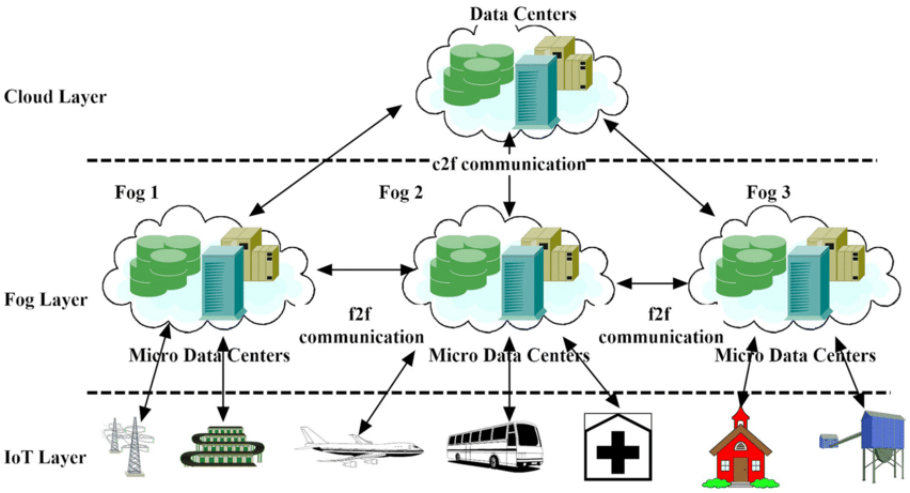

FIGURE 1.3 – *l'architecture d'environnement basé sur les objets connecté*

donc d'après l'architecture il y 3 couches principales :

— **cloud layer**.

— **fog layer**.

— **iot layer** les utilisateurs ou mobiles définit .

Cloud computing et Fog computing

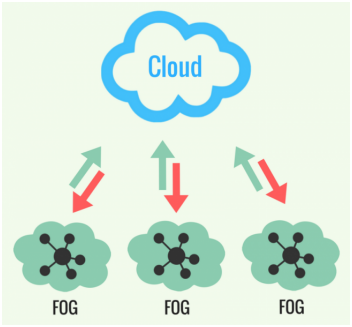

Figure 1.4 – *connectivité entre le Cloud computing et le Fog computing*

1.3. CLOUD COMPUTING

1.3.1. DÉFINITION

Le cloud computing est une infrastructure et une puissance de stockage, où il est accessible via Internet, l'ordinateur et d'autres appareils électroniques ne deviennent dans ce cas qu'un point d'accès pour le fonctionnement uniquement, car l'utilisation du disque dur dans le stockage ou l'utilisation de la suppression du disque dur pour accéder aux applications, l'accès aux Données de n'importe où et à tout moment, il offre également aux utilisateurs toute la sécurité nécessaire et la capacité nécessaire de stockage et de travail en toute simplicité, il dépend de sources externes de données informatiques.

C'est un système informatique qui consiste à utiliser des serveurs distants qui permettent de stocker, de partager et d'accéder aux données Le cloud computing se développe A grande échelle, il fonctionne sur l'Internet des objets et la 5 ème génération.[2]

1.3.2. LES TYPES DES SERVICES CLOUD COMPUTING

1.3.2.1. SOFTWARE -AS-A-SERVICE (SAAS)

Il comprend des prototypes qui aident les utilisateurs et les clients à faire leur travail facilement, et que les applications ne sont pas installées sur leurs appareils.Au lieu de cela, les applications saas sont hébergées sur des serveurs cloud, comme si vous louiez de l'espace pour travailler.[5]

1.3.2.2. PLATFORM-AS-A-SERVICE (PAAS)

Le service PAAS a été développé plus que le service SAAS pour aider les développeurs à développer leur service car il leur permet de créer facilement des applications et de leur fournir tous les outils nécessaires, l'infrastructure, les composants dont ils ont besoin et les systèmes d'exploitation en ligne.[5]

1.3.2.3. INFRASTRUCTURE-AS-A-SERVICE (LAAS)

Le service (laas) consiste à travailler sur l'infrastructure qui permet de louer un espace de stockage auprès de la société serveur et de travailler dessus pour une date précise, après quoi elle peut utiliser cette structure pour développer ses propres applications.[5]

1.3.2.4. NETWORK AS A SERVICE (NAAS)

Naas fournit un (des) réseau (s) virtuel (s) aux utilisateurs, avec NaaS, l'utilisateur peut également avoir des réseaux.[5] hétérogène.

Les modelés de déploiement : Pour faciliter l'utilisation et le développement du cloud computing, puis l'émergence de 4 modèles de cloud computing à ce jour, chaque modèle présente des avantages et des inconvénients comme suit :.[2]

— **Cloud privé**

L'infrastructure de ce modèle se trouve soit au siège de l'organisation, soit à l'extérieur de celle-ci et est utilisée par une organisation.

l'inconvénient du cloud privé est qu'il a besoin d'employés capables de le gérer en termes de développement.

L'avantage est qu'il offre une meilleure visibilité et un meilleur contrôle sur l'infrastructure.

— **Cloud communautaire**

Afin de répondre aux besoins de la communauté puis de créer le cloud communautaire, il fonctionne avec de nombreuses institutions et peut être placé à l'extérieur ou à l'intérieur de l'organisation.

le défaut du cloud communautaire est lié à la sécurité, à l'isolement des données et aux risques d'attaque.

l'avantage, les données restent partiellement fragmentées, sauf pour les zones qui sont dans lesquelles l'accord sur l'accès partagé, ce qui rend le coût moins.

— **Cloud hybride**

Le cloud hybride est une solution unique pour les utilisateurs car il permet la possibilité de transférer des applications et des données, car il relie l'infrastructure avec la même technologie.

l'avantage est de travailler facilement entre le public et le privé et la possibilité d'accès au travail et non de fixer des limites. Quant au défaut de celui-ci, c'est dans la sécurité des transports et des données entre le public et le privé..[2]

1.4. FOG COMPUTING

1.4.1. DÉFINITION

Le Fog Computing offre une meilleure sécurité car les données sensibles sont traitées localement et dans un temps très court qui peut prendre quelques secondes ou minutes au lieu de les envoyer dans le cloud pour analyse, ce qui aide les utilisateurs à surveiller les appareils, ce qui les rend plus sûrs lorsqu'ils collectent, analysent et stocke les données.[6]

industries utilisée les fog computing Avec le développement et la prospérité du fog computing, une expansion significative est connue de tous les magasins,

en particulier les institutions et les industries qui ont besoin d'analyses à la périphérie du réseau, utilisent des ressources informatiques et nécessitent une analyse rapide des données, telles que la santé, l'agriculture, le gouvernement, pétrole, gaz, routes, etc.

1.4.2. LES AVANTAGES DU FOG COMPUTING

— le temps de latence : les données sont traitées en un temps très court, quelques millisecondes de notre part apportent une réponse efficace et le réseau fog peut traiter une grande quantité de données avec moins de retard.

— conservation de la bande passante du réseau : puisque les données est traité localement en fog computing Il consomme le moins de bande passante réseau possible.

— Analyse en temps réel : Certains événements nécessitent des données et une réponse efficace en peu de temps, et le fog computing y est parvenu.

— Accès en ligne et hors ligne : Fog computing stocke les données localement et ne les envoie pas au Cloud uniquement en cas de besoin, ce qui les rend disponibles lorsqu'il n'y a pas de connexion Internet pour envoyer des données.[6]

1.4.3. INCONVÉNIENTS DU FOG COMPUTING

— Risques pour la sécurité et la confidentialité :

Si tous les appareils connectés les uns aux autres ne sont pas sécurisés, il peut y avoir des failles que le pirate peut exploiter pour accéder à la confidentialité et aux données en utilisant vos appareils contre vous Comme si le contrat collectait des informations sensibles provenant des appareils des utilisateurs

— consommation d'énergie :

Plus le nombre de nœuds est élevé, plus la consommation d'énergie de l'entreprise est importante.

— la complexité du réseau :

Le Fog computing fonctionne à la fois avec les réseaux traditionnels et le cloud computing, ce qui rend leur combinaison complexe ou difficile et plus vulnérable aux attaques et compliqué en le sécurisant.[6]

1.4.4. DIFFÉRENCE ENTRE LE CLOUD COMPUTING ET FOG COMPUTING

1.4.4.1. CLOUD COMPUTING

Il est utilisé pour stocker et traiter des données via Internet.
Il peut être travaillé sans posséder d'infrastructure.
Vous devez payer une redevance pour le travail.
Accessible à tous, tout utilisateur peut louer un espace et y travailler.
Il contient des formulaires d'aide en échange de payer ce que vous en utilisez.
Il a une structure centralisée.[2]

1.4.4.2. FOG COMPUTING

Fournit des services aux utilisateurs sur le réseau périphérique.
Maintient les ressources informatiques entre la source de données et le cloud.
Les dispositifs de couche de brouillard effectuent des opérations liées au réseau.
Fournit des services fiables à grande échelle.
Plus proche des utilisateurs que des serveurs cloud efficaces.
Architecture décentralisée.[2]

1.5. CONCLUSION

Dans ce chapitre nous avons défini les infrastructures cloud et fog computing qui présente l'architecture et les composantes principales d'un environnement IoT.

Nous avons vu dans ce chapitre comment l'environnement permet de connecter des données et de les passer à partir des objets aux services cloud..

CHAPITRE 2

La sécurité et les système de détection d'intrusion

INTRODUCTION

La sécurité informatique est une matière essentielle dans le domaine de la technologie. Elle doit être développée et travaillée d'avantage afin de sécuriser les données, les utilisateurs et les informations. Sur elle, toutes les attaques, quels que soient leur type et leur complexité, doivent être découvertes. Les développeurs travaillent pour trouver des solutions afin de convoyer l'adversaire et ne lui donner aucune opportunité et ne laisser aucune brèche, il est donc nécessaire d'avoir un système de détection d'intrusion et de le faire évoluer à chaque fois au besoin. Dans ce chapitre nous allons pésenter le role de la sécurité dans le fog computing et la définition des différents types de sécurité et leur principe de fonctionnement.

2.1. LA SÉCURITÉ EN GÉNÉRALE

2.1.1. DÉFINITION

La sécurité est la protection, la prévention et les procédures prises pour éviter les erreurs et les dangers afin de sécuriser et de protéger les utilisateurs, leur vie privée et leurs données contre le vol ou toute modification des informations, et de protéger le réseau informatique et ses données contre les attaques ou les brûlures. , et il est très important dans la protection des appareils.[7]

2.1.2. LES TYPES DE SÉCURITÉ

— **Sécurité du réseau**

Protéger le réseau contre les pirates malveillants et les empêcher d'atteindre leur cible.

— **Sécurité Internet**

Internet est utilisé de manière terrible et durable, rendant toutes les données vulnérables, donc les murs de protection assurent la sécurité Internet.

— **Sécurité du cloud**

Avec le développement et l'expansion de la technologie, la sécurité du cloud est une nécessité, car les données sont maintenant traitées et stockées directement dans le cloud. Les applications SASS doivent donc être sécuritaires et l'utilisation du cloud public doit être sécuritaire.[7]

2.2. LA SÉCURITÉ AU NIVEAU DE FOG COMPUTING

En raison de l'expansion rapide et à grande échelle du calcul du brouillard et du traitement d'un grand nombre de données en un temps court et efficace, l'adoption de la technologie FC selon le consortium openfog en tant que un intermédiaire entre le cloud et les appareils finaux, car elle fournit des services de stockage plus proches du travail en temps réel et de l'adaptation aux données de IOT.
Ce nouveau modèle informatique assure la sécurité grâce à sa collaboration avec le cloud computing et l'infrastructure portable.
Mais avec le passage du temps, les options de confidentialité des données ne sont plus traditionnelles et la sécurité dans le cloud computing est adaptée pour protéger d'énormes données.
il a donc été décidé de reconsidérer les problèmes de sécurité comme ils sont les plus sensibles dans le fog computing tout en trouvant de nouvelles solutions et méthodes pour détecter et réduire les risques de sécurité dans les fog computing.[8]

2.3. LES SYSTÈME DE DÉTECTION D'INTRUSION

Le système de détection d'intrusion (IDS) fonctionne pour détecter les attaques et les intrusions dans le système afin d'assurer la sécurité, le processus d'analyse a lieu soit sur le réseau (NIDS), soit sur l'hôte (HIDS).[9]

Le processus d'analyse du réseau (NIDS) est le plus étendu car il fonctionne pour détecter le trafic réseau dans recherche de toute intrusion suspectée.

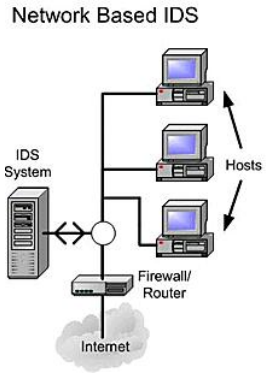

FIGURE 2.1 – *IDS sur le réseau*

Alors que les systèmes basés sur l'hôte (HIDS) surveillent l'activité et les processus des utilisateurs sur l'appareil afin de détecter les attaques.

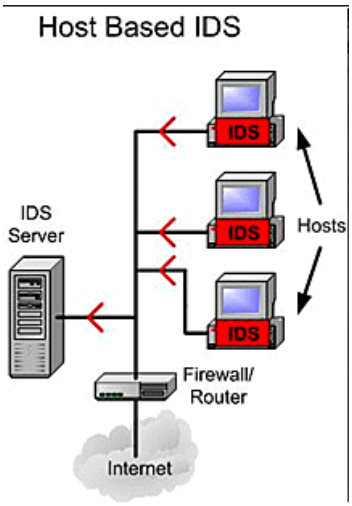

FIGURE 2.2 – *IDS sur l'hote ou les systèmes*

2.3.1. LES IDS BASÉ SUR LA SIGNATURE

La détection signature travaille sur l'étude et la collecte d'un ensemble de signatures, puis les étudie au préalable et vérifie qu'il s'agit d'attaques, donc les intrusions sont détectées en faisant correspondre les données avec les

signatures.Si le résultat est positif, elles sont considérées comme des attaques. Enfin, après avoir été étudiées, elles sont placées comme nouvelles signatures dans la base de signatures connues.[9]

2.3.2. LES IDS BASÉ SUR L'ANOMALIE

Dans ce chapitre, la sécurité en général, ses types et son importance dans le fog computing, sa fonctionnalité et ses connaissances sur les systèmes de détection d'infiltration et leur pertinence dans ce domaine sont présentés à travers sa détection quotidienne d'attaques très complexes et de méthodes innovantes. Les menaces à la sécurité des systèmes informatiques sont diverses et en augmentation terrible et complexe menaçant la sécurité du système, ce qui a conduit les chercheurs à améliorer et développer des méthodes de détection à tous les niveaux pour assurer la sécurité des utilisateurs.[9]

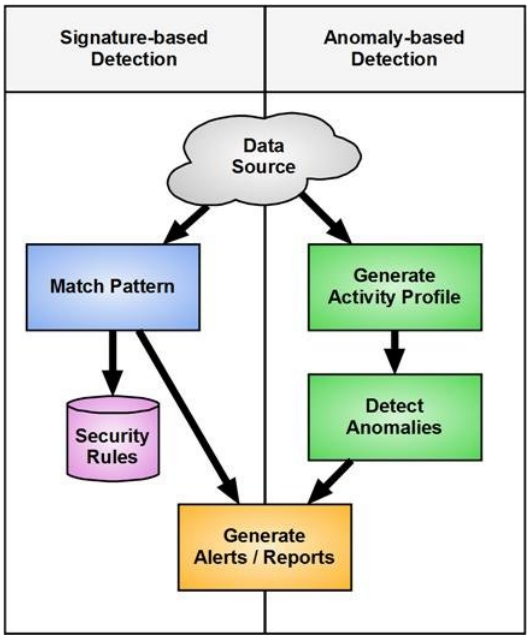

FIGURE 2.3 – *la différence entre IDS basé sur la signature et les IDS bsé sur l'anomalie*

2.3.3. LES IPS

Un IPS est une plateforme logicielle qui examine le contenu du trafic réseau afin de trouver et de traiter les vulnérabilités. On l'appelle souvent un système de détection et de prévention des intrusions ou IDPS.

Ces solutions comprennent également des réponses automatisées, telles que le blocage de l'adresse de la source du trafic, le dépôt de colis dangereux et l'envoi d'alertes aux utilisateurs. Fondamentalement, la solution IPS n'est pas seulement un outil de diagnostic qui identifie les menaces de sécurité réseau, mais aussi une plateforme qui peut y répondre. C'est la différence avec le système de détection d'intrusion IDS.[10]

2.4. CONCLUSION

Les menaces à la sécurité des systèmes informatiques sont variées et terribles, complexes et menaçantes. Cela a amené les chercheurs à améliorer et à développer des méthodes de détection à tous les niveaux pour assurer la sécurité des utilisateurs. Dans ce chapitre, la sécurité a été présentée en général, ses types et son importance au niveau de fog computing, et la pertinence des systèmes de détection d'intrusion dans ce domaine grâce à leur détection quotidienne d'attaques très complexes et de méthodes innovantes.

CHAPITRE 3

La stratégie proposé

3.1. INTRODUCTION

Dans les chapitres précédent, nous avons discuté sur la sécurité en général et de la sécurité dans un environnements d'objets connecté, sorte que la solution idéale est un système de détection d'intrusion.

D'après l'architecture d'un environnement IoT que nous avons a présenté precedemment, cette architecture est constituée de trois niveaux (cloud computing, Fog computng, usé) notre système de détection d'intrusion sera place au niveau de la couche fog computing.

Dans ce chapitre nous allons présenter notre stratégie globale pour la détection d'intrusion, ainsi nous détaillons trois solutions différentes dans la phase d'analyse.

3.2. Notre système de détection d'intrusion propos

L'architecture globale

L'architecture globale de notre système de détection d'intrusion propos est compose de 3 phases principales : la sélection des attributs, l'analyse et la validation.

La figure suivante présente l'architecture globale de notre système de détection d'intrusion propos :

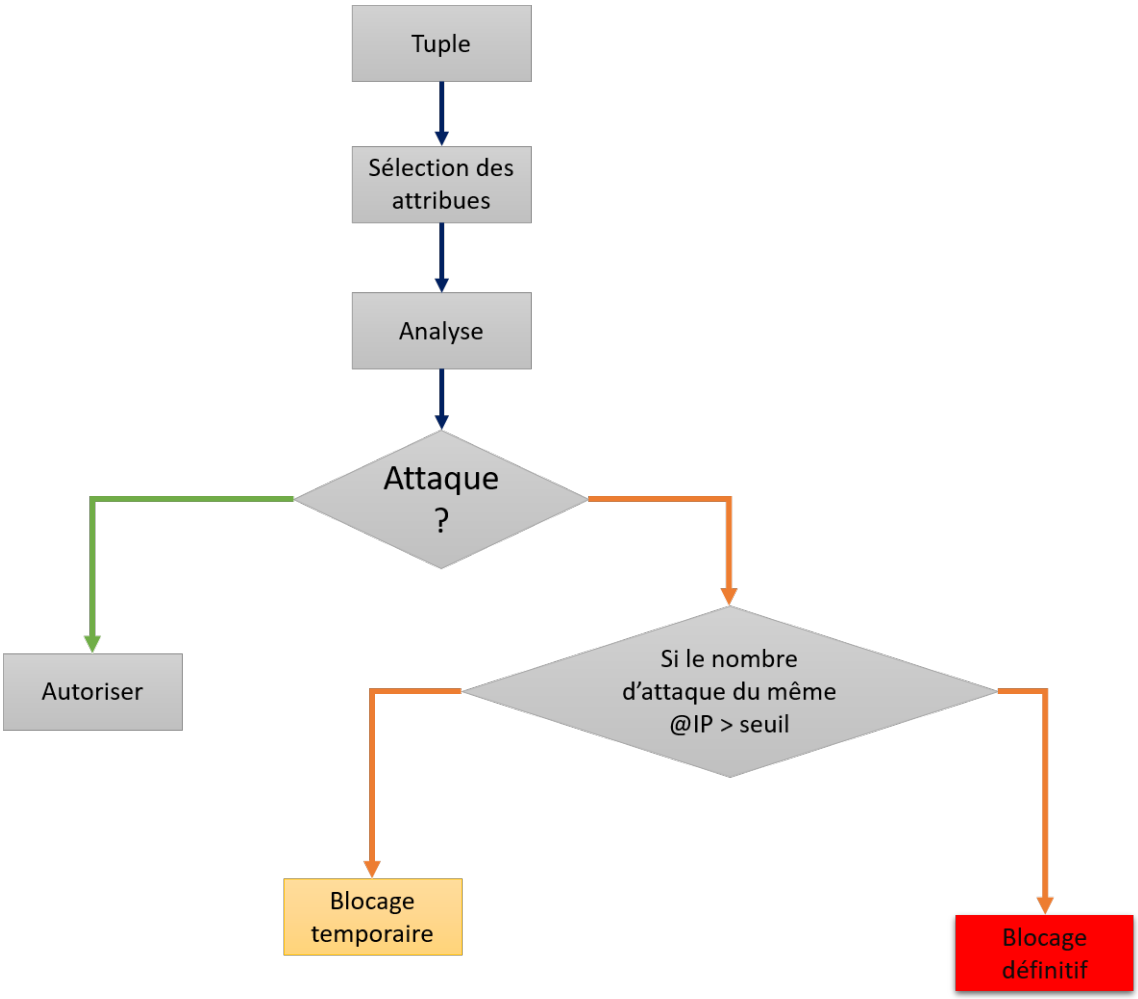

FIGURE 3.1 – *L'architecture de notre stratégie proposé*

3.2.1. LA SÉLECTION DES ATTRIBUTS

C'est le processus de détection des caractéristiques pertinentes et de suppression des données non pertinentes, redondantes ou bruyantes. Les caractéristiques non pertinentes sont celles qui ne fournissent aucune information utile.[11]

d'après l'arrivée d'un paquet (dans notre cas nous parlerons d'un Tuple qui représente un requete d'un IoT un noeud fog), nous sélectionnons les paramètres les plus importants afin de réduire la quantité d'informations analyser et aussi dans le but d'accélérer le processus de détection.

3.2.2. L'analyse

Comme nous définissions dans le chapitre précédent les système de détection d'intrusion sont basés sur deux méthodes : les IDS basé sur la signature et les IDS basé sur l'anomalie.

La phase d'analyse permet de traiter et de classifier les requêtes des utilisateurs en requêtes normales ou des attaques.
Nous avons propose une nouvelle approche basée sur l'apprentissage automatique ou l'apprentissage profond pour analyser les Tuples envoyés par les IoTs.

3.2.3. la validation

Après la phase d'analyse les tuples des IoT sont classes en deux groupes : Tuple d'attaque /Tuple non attaque, la phase de validation permet aux Tuples non attaques de continuer leur exécution d'une façon normale. Par contre les Tuples d'attaque seront bloqué par le système. Nous avons utilisé deux types de blocage, un blocage temporaire et un blocage définitif. Si un IoT envoie un Tuple et ce dernier est considéré par notre système comme un Tuple d'attaque, le système pass l'attaque dans une liste de blocage.

le problème suggérer si cette adresse est une adresse d'un victime donc on ne peut pas bloqué cette utilisateur, qu'est ce qu'on a fait ?, on a vérifier le nombre d'accès pour cette adresse s'il est dépassé un nombre précise donc est un attaquant et on a bloquer définitivement sinon si ne dépasse pas alors est un victime et on a bloquer temporairement.

3.3. Les méthodes proposés

— **L'apprentissage**

Il s'agit d'un processus qui permet à l'apprenant de créer en lui la connaissance nécessaire pour penser et agir, comme Beillerot (1989) à définit.

Ce concept a été appliqué à la machine de sorte que l'apprenant ici est la machine ou l'ordinateur et ce concept est appelé apprentissage automatique.

L'apprentissage automatique est une forme d'intelligence artificielle fondée sur des concepts mathématiques et statistiques qui permettent à un ordinateur d'apprendre à partir de données qui n'utilisent pas de programmation explicite.

Diverses techniques d'apprentissage automatique ont été développées pour créer des algorithmes qui peuvent apprendre et s'améliorer indépendamment, appelées techniques **d'apprentissage profond (deep learning en anglais)**.

Ces techniques comprennent les réseaux neuronaux artificielle. L'apprentissage profond dépend de ces algorithmes, ainsi que des technologies telles que la reconnaissance d'image et la vision automatisée.[12]

Les méthodes 01 et 02 : machine learning/l'apprentissage automatique Dans les deux méthodes que nous allons présenter maintenant sera l'étape de la sélection des caractéristiques d'une manière classique pour déterminer et équiper notre environnement que nous voulons analyser. donc nous allons appliquons ce qu'ont appelé la normalisation des données.

— la normalisation des données : est la mise à l'échelle des données en variables numériques de 0 à 1. la formule :

$$x_{new} = \frac{x - x_{min}}{x_{max} - x_{min}}$$

donc, on va explique seulement la partie d'analyse. les deux méthodes suivantes sont des algorithmes d'apprentissage automatique.

3.3.1. MÉTHODE 01 : K-MEANS

3.3.1.1. K-MEANS CLUSTERING

est algorithme d'apprentissage automatique non supervisé utilise des caractéristiques plutôt que des catégories prédéfinies pour catégoriser les données

non étiquetées de façon non supervisée. Le nombre de groupes ou de catégories produits est indiqué par la variable K.

L'objectif est de diviser les données en grappes distinctes K et de donner l'emplacement du centre de masse de chaque grappe.

Un cluster (classe) peut alors être attribué à un nouveau point de données basé sur le centre de masse fermé.

Cette méthode a l'avantage majeur d'éliminer le biais humain de l'analyse. L'ordinateur construit ses propres grappes plutôt que de demander à un chercheur d'utiliser des preuves empiriques plutôt que des conjectures. [14]

— L'algorithme fonctionne comme suit :

Tout d'abord,on donnons un nombre de clusters, ensuite nous initialisons aléatoirement les clusters par des point aléatoire appelé moyenne ou centroid.

Nous classons chaque élément à sa moyenne la plus proche et nous mettons à jour les coordonnées de la moyenne, qui sont les moyennes des éléments classés dans ce groupe jusqu'à présent.

Nous répétons le processus pour un nombre donné d'itérations et à la fin, nous avons nos clusters.[14]

3.3.2. MÉTHODE 02 : PCA (ANALYSE DES PRINCIPALES COMPOSANTES)

PCA est une technique d'apprentissage automatique dans le but de réduction de dimension, qui permet de convertir des variables très corrélées en nouvelles variables décorrélées les unes des autres.

Le principe est simple : il s'agit en fait de résumer l'information contenue dans une grande base de données en un certain nombre de variables synthétiques appelées composants principales.

Évidemment, la perte d'informations est synonyme de réduction de dimension. C'est l'essentiel de l'analyse en composantes principales. Il est nécessaire de pouvoir réduire la taille de nos données tout en conservant le plus d'informations possible.[15]

— L'algorithme fonctionne comme suit :

Normaliser la gamme des variables initiales continues.

Calculer la matrice de covariance pour identifier les corrélations.

Calculer les vecteurs propres et les valeurs propres de la matrice de covariance pour identifier les principaux composants.

Créer un vecteur de fonctionnalité pour décider quels composants principaux garder.

Refonte des données sur les principaux axes de composantes.[15]

— comparaison entre **les auto-encoder** et **les PCAs** :

On peut dire que les auto-encoders et les pca sont des généralisations des composantes principaux. auto-encoder peut également faire la même chose que l'analyse des composantes principaux. Mais Auto-encoder peut faire plus parce qu'il peut faire du mappage non linéaire plutôt que linéaire. Alors que dans le cas des PCAs, nous n'avons que la cartographie linéaire.

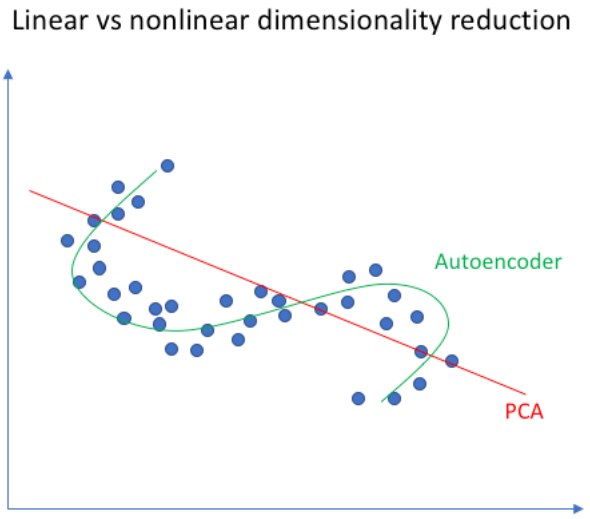

FIGURE 3.2 – *autoencoders-vs-principal-component-analysis*

3.3.3. MÉTHODE 03 : DEEPLEARINING OU L'APPRENTISSAGE PROFOND

Le deep learning est une branche des technologies de l'intelligence artificielle, principalement basée sur des réseaux de neurones artificiels multicouches.

Des techniques de deep learning ont été utilisées dans le domaine de la détection d'intrusion. La documentation que nous avons adoptée dans le cadre de nos recherches a fourni de nombreuses approches de l'IDS en utilisant différents réseaux de neurones profonds pour répondre aux préoccupations en matière de vie privée et aux menaces à la sécurité.[16]

Notre méthode proposée est une combinaison des méthodes utilisées dans la littérature afin que la détection d'intrusion sera plus rapide et plus pécise.

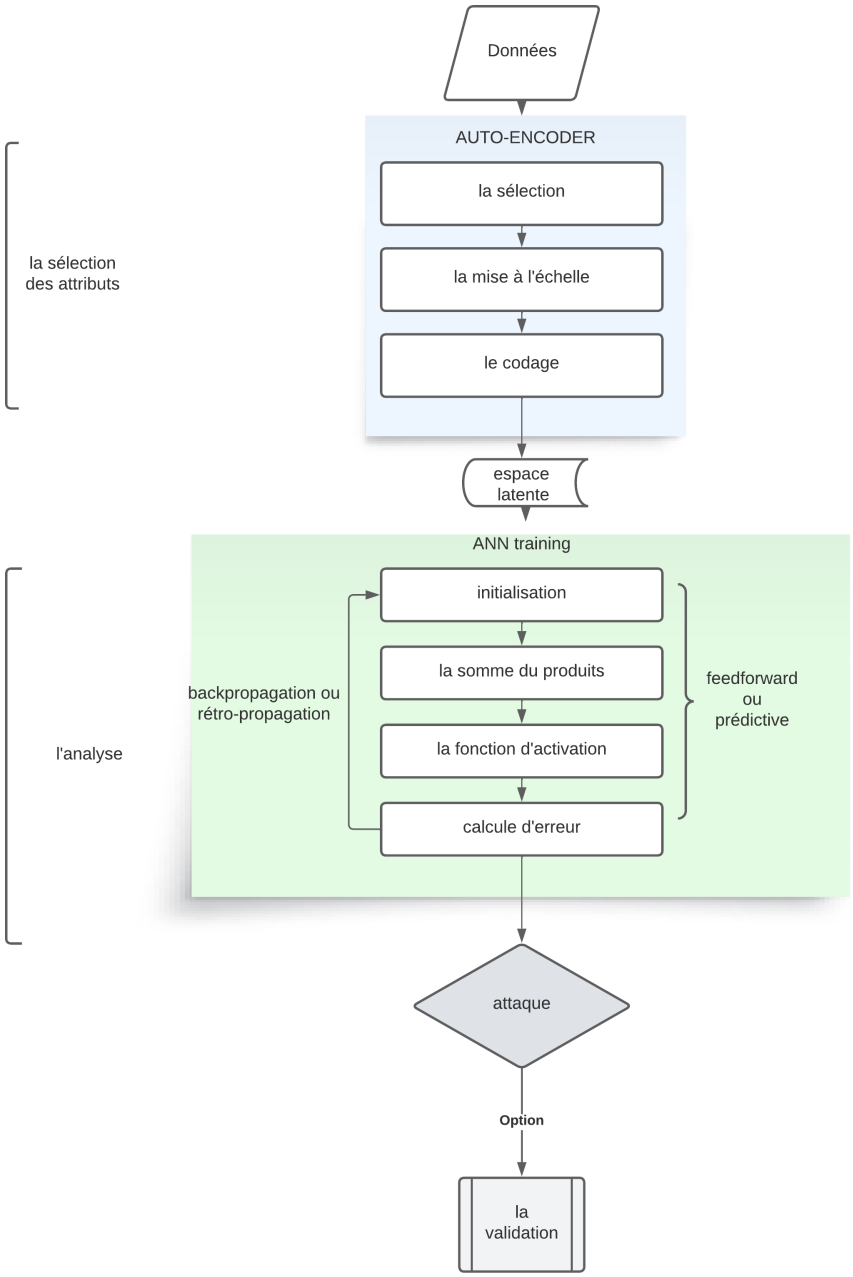

FIGURE 3.3 – *L'architecture de la méthode 01 deep learning*

3.3.3.1. La sélections des attributs

Dans l'architecture globale de notre système de détection d'intrusion propose, la première phase est la sélection des attributs : nous avons utilisé le **Auto-Encoder** .

Auto-Encoder : est une sorte de réseau neuronal multiple couches où la sortie cible est la même entrée avec une certaine quantité d'erreur de reconstruction. utilise le AE apprentissage non supervisé pour décoder ou reconstruire Par codage. Pour réduire les dimensions de propriétés, extraire les propriétés pertinentes, les compresser et les supprimer bruit des images, prédiction des séquences, détection des anomalies [17].

Il se compose de 4 éléments importants : chiffrement, la zone latente,L'erreur de reconstruction et déchiffrement :

Le chiffrement : permet de réduire et d'identifier les données importantes et de fournir des données de type numérique .

La zone latente : contient uniquement les données extraites et chiffrées des données originales.

Le déchiffrement : démantèle les données de code en essayant d'accéder aux mêmes données originales.

L'erreur de reconstruction : après avoir essayé de déchiffrer il y a une différence entre les données original et les données résultantes, si la proportion d'erreur est grande, elle affecte et remet en question la valeur des données et peut être considérée comme une attaque.[17]

Dans notre système de détection d'intrusion propose, nous avons travaillé qu'avec le chiffrement et l'espace latent pour représenter la première phase (la sélection des attributs)

Les fonctions proposées à cette étape :

1. sélection
   - `Coefficient de corrélation de Pearson` est une statistique descriptive, c'est-à-dire qu'il résume les caractéristiques d'un ensemble de données. Plus précisément, il décrit la force et la direction de la relation linéaire entre deux variables quantitatives.

     Bien que les interprétations de la force de la relation (également

connue sous le nom d'ampleur de l'effet) varient d'une discipline à l'autre.(3scribbr) la formule de la méthode coefficient de corrélation de pearson est le suivant ?? :

$$r = \frac{n\Sigma xy - (\Sigma x)(\Sigma y)}{\sqrt{[n\Sigma x^2 - (\Sigma x)^2][n\Sigma y^2 - (\Sigma y)^2]}}$$

2. **la mise à l'échelle**
   - `MinMaxScaler` : Transformer les caractéristiques en les adaptant à une range donnée.
     Cet estimateur met à l'échelle et traduit chaque caractéristique individuellement de sorte qu'elle se situe dans la range donnée de l'ensemble de formation, c.-à-d. entre zéro et un.[19]

$$x_{scaled} = \frac{x - x_{min}}{x_{max} - x_{min}}$$

3. **codage :**
   - `one-hot-encoding` : est utilisé pour représenté les données catégorique d'une datasets sous forme numérique.
     La plupart des datasets de la vie réelle que nous rencontrons pendant l'élaboration de notre projet de science des données comportent des colonnes de type de données mixtes. datasets sont composés de colonnes à la fois catégoriques et numériques. Cependant, divers modèles d'apprentissage automatique ne fonctionnent pas avec des données catégoriques et pour les intégrer dans le modèle d'apprentissage automatique, il faut les convertir en données numériques [20].

3.3.3.2. L'ANALYSE

A cette étape du deep learning, la machine est formée pour donner des résultats précis.

Parmi les méthodes d'entraînement, les réseaux neuronaux artificielle (ANN) qui modélisent le cerveau humain Les réseaux neuronaux artificielle sont constitués de neurones semblables à des cellules cérébrales humaines reliées entre elles par certaines coefficients.

Pendant l'entraînement, l'information est distribuée à ces points de contact.

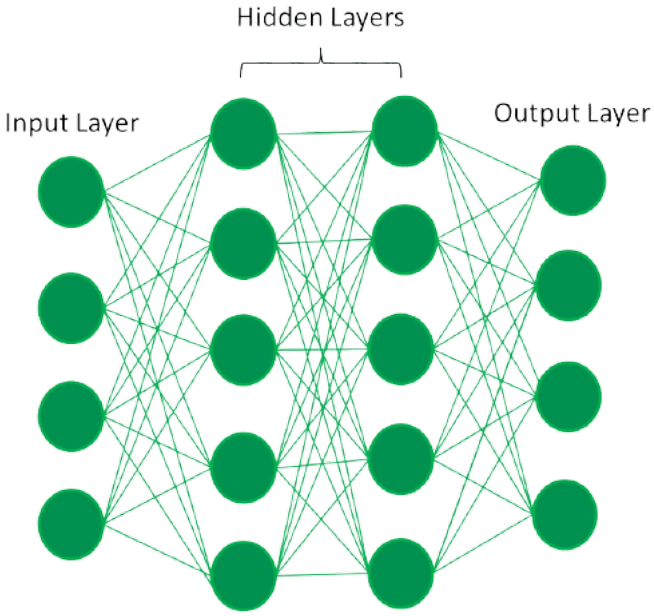

FIGURE 3.4 – *réseaux neuronaux artificielle*

ANN utilise ce qu'on appelle des couches caché. ce dernière ressemble à des neurones, de sorte que chacune de ces couches cachées est une forme transitoire avec un comportement probable.

Cette couche cachée sert de lien entre les intrants, c'est-à-dire les données que nous fournissons à ANN et les extrants où les résultats finaux sont fournis pour faciliter la classification.

Lorsque les données sont entrées dans la couche d'entrée, elles reçoivent des poids aléatoires. Ces données passent au couche suivant qui est les couches cachés (le nombre peut varier).

Il applique certains calculs à toutes les entrées avec des poids à partir des quels la fonction d'activation permet au signal de passer ou de ne pas passer selon la fonction d'activation utilisée et quelle entrée provient de la couche précédente. cette partie appelé prédictive, **feedforward** en anglais.

Les résultats finaux de cette partie sont comparés aux résultats attendus par ce qu'on appelle **calcule d'erreur**. Si ne donne pas de résultats approximatifs, recalculés en changeant les poids d'entrées et des biasis, Cette partie s'appelle rétro-propagation, **backpropagation** en anglais.[21]

les calcules appliqué :

— la somme des produits :

  est la somme des données entrantes multiplié par ses poids sommé par une autre données entré appeler bias cette entré d'une valeur égal à 1 et un poids, son rôle est similaire au seuil et il détermine si le neurone est activé ou non ??.

  la formule : $som = \Sigma_{i=0} \quad w_i * x_i + b;$

  ou : x : données entrants , w : poids des données , b : bias

— la fonction d'activation :

  Une fonction sigmoïde est une fonction qui a une courbe S, aussi appelée courbe sigmoïde.La fonction d'activation décide si un neurone doit être activé ou non. L'exemple le plus courant est la fonction logistique, qui est calculée par la formule suivante :

$$f(x) = \frac{1}{1 + e^{-x}}$$

La fonction d'activation a pour but d'introduire la non-linéarité dans la sortie d'un neurone. La transformation non linéaire de l'entrée est effectuée par la fonction d'activation, ce qui la rend capable d'apprendre et d'effectuer des tâches plus complexes.

— calcule d'erreur :

La performance du modèle de réseau neuronal est mesurée dans une tâche particulière, généralement la régression ou la classification par fonction de perte.

La fonction de perte d'erreur carrée moyenne est sélectionnée pour les tâches de régression lorsque nous voulons que le réseau prédise des données continues.

la fonction de perte d'erreur quadratique moyenne (**mean squared error** en anglais) est sélectionnée pour les tâches de régression lorsque nous voulons que le réseau prédise des données continues.

l'erreur quadratique moyenne (MSE) est une fonction de perte qui calcule l'erreur quadratique moyenne entre la valeur désiré et la valeur prédit.

Afin d'améliorer le réseau neuronal, nous devons réduire la valeur de la fonction de perte pendant la phase de rétro-propagation.

la formule de MSE est la suivante :

$$E = \frac{1}{2}(yd - yp)^2$$

ou : yd : la valeur de sortie désiré , yp : la valeur de sortie prédit

— la retro-propagation :

Nous devons choisir un ensemble spécifique de poids pour lesquels la valeur de la fonction de perte est aussi basse que possible puisque la perte dépend des poids.

La descente en gradient est une technique mathématique que nous utilisons pour ce faire.

La descente en gradient :

est un processus d'optimisation itératif qui recherche la valeur optimale d'une fonction objectif. L'une des méthodes les plus courantes pour modifier les paramètres d'un modèle pour réduire une fonction de coût dans les projets d'apprentissage automatique est cette méthode.

L'objectif principal de la descente de gradient est d'identifier les paramètres du modèle qui fournissent la précision maximale sur les ensembles de données d'apprentissage et de test.

Elle met à jour individuellement les paramètres de chaque exemple d'apprentissage. comme avantages il est plus accélérer par rapport à la descente de gradient par lots. et que les mises à jour fréquentes nous permettent d'avoir un taux d'amélioration assez détaillé.

la formule suivante présenté la stochastique gradient de descente :

$$w_{new} = w_{old} - \eta * \frac{\delta l}{\delta w_{old}}$$

ou : w : les poids , η : taux d'apprentissage, l : l'erreur.

3.4. CONCLUSION

L'apprentissage automatique et l'apprentissage profond sont des nouvelles approches qui offrent l'intelligence artificielle et jouent un rôle dans la sécurité grâce à des méthodes de classification qui aident à prédire et à détecter les anomalies et les intrusions.

Nous les avons utilisés pour proposer des nouvelles méthodes de détection des intrusions, notamment au niveau de toutes les objets connecté à Internet (iot) qui sont maintenant les plus utilisables dans divers services.

Nous avons utilisé le AUTO-ENCODER, ANN, K-MEANS, PCA pour notre stratégie proposé, nous avons donné une explication détaillée du fonctionnement de chacun et de la façon dont cela nous aide dans le processus de classification.

CHAPITRE 4

La simulation

4.1. INTRODUCTION

dans le chapitre précédent nous avons présente notre système de détection d'intrusion et nous choisissions la troisième méthode (deeplearning) pour l'implémenter et l'évaluer.

dans ce chapitre nous allons présenter le langage de programmation Java et l'environnement de développement Eclipse et le simulateur IFogSim et ses classe principales. en plus, en expliquer les configuration que nous faisons sur le simulateur avant le lancement de notre méthode proposé.

4.2. L'ENVIRONNEMENT DE DÉVELOPPEMENT

Pour l'implémentation de notre méthode de détection d'intrusion au niveau de Fog computing nous avons développer le simulateur IfogSim afin de supporter notre stratégie, et pour un environnement de travail on utilise :

— caractéristique matérielles et logicielles d'ordinateur utilisé :

Nous avons développe notre application sur une machine avec un processeur Intel(R) Core(TM) i3-4005U CPU @ 1.70GHz et d'une capacité mémoire de 4Go. Le simulateur est sous Windows10 64 bits.

— simulateur utilisé : IFogSim

— langage utilisé : Java

— ide utilisé : Eclipse

4.2.1. LE LANGAGE DE PROGRAMMATION JAVA

Java est un langage de programmation à usage général, évolué et orienté objet dont la syntaxe est proche du C. Ses caractéristiques ainsi que la richesse de son écosystème et de sa communauté lui ont permis d'être très largement utilisé pour le développement d'applications de types très disparates. Java est notamment largement utilisé pour le développement d'applications d'entreprises et mobiles.

Il n'y a pas de compilation spécifique pour chaque plate forme. Le code reste indépendant de la machine sur laquelle il s'exécute. Il est possible d'exécuter des programmes Java sur tous les environnements qui possèdent une Java Virtual Machine. Cette indépendance est assurée au niveau du code source grâce à Unicode et au niveau du bytecode.

FIGURE 4.1 – *java-logo*

4.2.2. L'ÉDITEUR ECLIPSE

Eclipse est capable de gérer de nombreux types de projets, en particulier des projets complexes avec plusieurs sous-projets contenant de nombreux fichiers sources.

Eclipse comprend aussi des systèmes de construction de code (build) comme Maven ou Gradle, pour créer et maintenir des projets plus complexes. Il peut aussi vous aider à mettre en place une base de projet, grâce aux assistants, ou wizards, afin de ne pas partir d'un fichier vide à chaque fois

Eclipse simplifie le développement Java, en particulier pour les gros projets dans un contexte professionnel. Voyons donc à quoi ressemble cet IDE, à travers un tour rapide de l'outil.

FIGURE 4.2 – *eclipse-logo*

4.2.3. IFOGSIM

IFogSim est un outil de simulation open source basé sur Java pour simuler des scénarios de brouillard. Il est développé par Harshit Gupta et l'équipe du *Cloud Computing and Distributed Systems (CLOUDS) Lab University of Melbourne Australie*.

L'iFogSim fournit des classes intégrées pour créer des nœuds de fog, des capteurs et des actionneurs. Il s'occupe également de l'affectation des ressources et des politiques de gestion.

4.2.3.1. Les classes principaux d'iFogSim

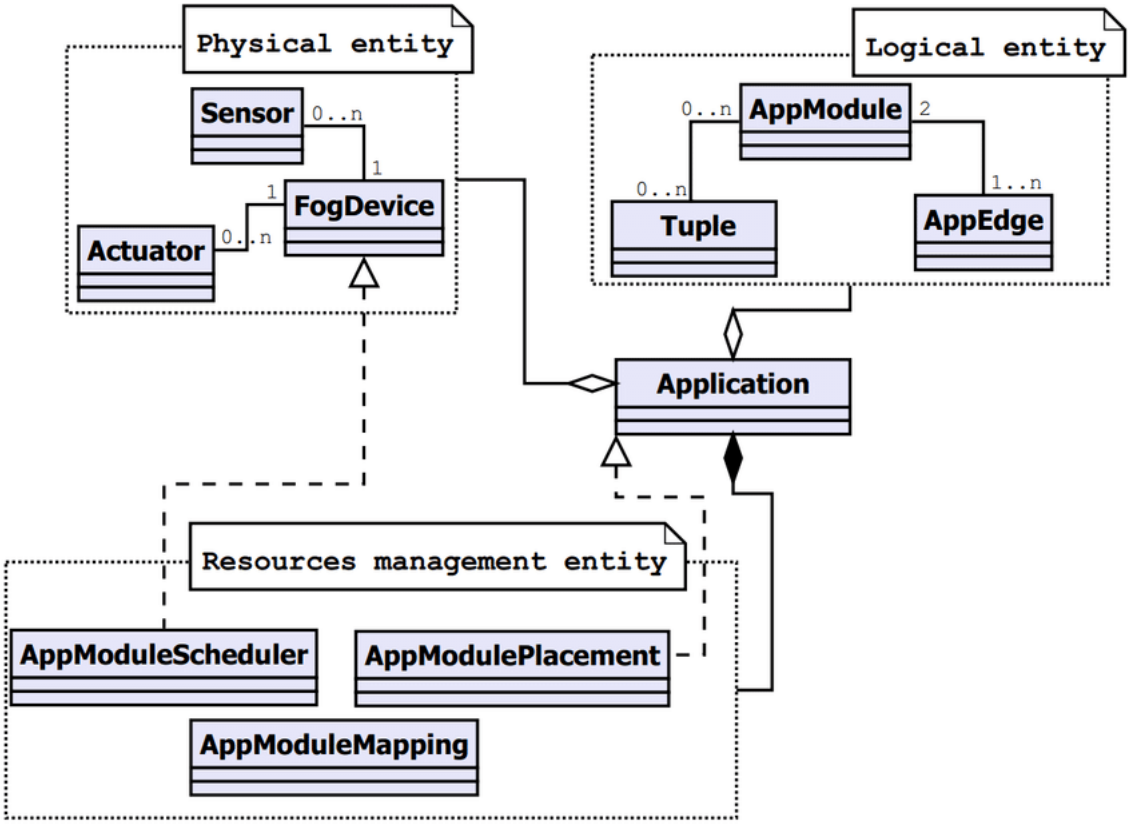

Figure 4.3 – *Les principales composantes de ifogsim*

Les classes suivantes seront utilisées pour créer un environnement iot dans iFogSim.

— **FogDevice**

Cette classe spécifie les caractéristiques matérielles des appareils Fog et leurs connexions à d'autres appareils, capteurs et actionneurs Fog. Réalisés par extension de la classe PowerDatacenter dans CloudSim, les attributs majeurs de la classe FogDevice sont la mémoire accessible, le processeur, la taille de stockage, les bandes passantes montantes et descendantes (définissant la capacité de communication des appareils Fog).Les méthodes de cette classe définissent la manière dont les ressources d'un périphérique Fog sont planifiées entre les modules d'application exécutés sur celui-ci et

la manière dont les modules sont déployés et désactivés sur ceux-ci. Le remplacement de ces méthodes permet aux développeurs de plug-in des politiques personnalisées pour les fonctions mentionnées ci-dessus.

— **Sensor** Les instances de la classe sensor sont des entités qui agissent comme des capteurs IoT décrits dans l'architecture. La classe contient des attributs représentant les caractéristiques d'un capteur, allant de sa connectivité aux attributs de sortie. La classe contient un attribut de référence à l'appareil passerelle Fog auquel le capteur est connecté et la latence de connexion entre eux. Plus important encore, il définit les caractéristiques de sortie du capteur et la distribution du temps inter-transmission ou inter-arrivée de tuple - qui identifie le taux d'arrivée de tuple à la passerelle.

— **Tuple**

Les tuples forment l'unité fondamentale de communication entre les entités dans le brouillard. Les tuples sont représentés comme des instances de la classe Tuple dans iFogSim, qui est héritée de la classe Cloudlet de CloudSim. Un tuple est caractérisé par son type et les modules d'application source et destination. Les attributs de la classe spécifient les exigences de traitement (définies en millions d'instructions (MI)) et la longueur des données encapsulées dans le tuple.

4.2.3.2. Actionneur

Cette classe modélise un actionneur en définissant ses propriétés de connexion réseau. Un attribut de la classe fait référence à la passerelle à laquelle l'actionneur est connecté et à la latence de cette connexion. La classe définit une méthode pour effectuer une action à l'arrivée d'un tuple d'un module d'application.

— **Application**

Une application est modélisée sous la forme d'un graphe orienté, les sommets du DAG représentant les modules qui effectuent le traitement des données entrantes et les arêtes indiquant les dépendances de données entre les modules. Ces entités sont réalisées à l'aide des classes suivantes :

1. **AppModule** Les instances de la classe AppModule représentent les éléments de traitement des applications Fog. AppModule est implémenté en étendant la classe PowerVm dans CloudSim. Pour chaque tuple entrant, une instance AppModule le traite et génère des tuples de sortie qui sont envoyés aux modules suivants dans le DAG. Le nombre de tuples de sortie par tuple d'entrée est décidé à l'aide d'un modèle de sélectivité - qui peut être basé sur une sélectivité fractionnaire ou un modèle en rafales.
2. **AppEdge** Une instance AppEdge indique la dépendance des données entre une paire de modules d'application et représente un bord dirigé dans le modèle d'application. Chaque arête est caractérisée par le type de tuple qu'elle transporte, qui est capturé par l' attribut tupleType de la classe AppEdge ainsi que les exigences de traitement et la longueur des données encapsulées dans ces tuples. IFogSim prend en charge deux types de bords d'application - périodiques et basés sur des événements. Les tuples sur un AppEdge périodique sont émis à intervalles réguliers. Un tuple sur un bord basé sur des événements=(tu, v)est envoyé lorsque le module sourcetu reçoit un tuple et le modèle de sélectivité detupermet l'émission de tuples portés pare
3. **AppLoop** AppLoop est une classe supplémentaire, utilisée pour spécifier les boucles de contrôle de processus qui intéressent l'utilisateur. Dans iFogSim, le développeur peut spécifier les boucles de contrôle pour mesurer la latence de bout en bout. Une instance AppLoop est fondamentalement une liste de modules commençant à l'origine de la boucle jusqu'au module où la boucle se termine.

4.2.3.3. Les classes modifier

Nous avons modéfié dans les classes FogDevice. Sensor,vrgame.

- **Sensor :** dans cette classe nous ajoutons les attributs ip addresse source, ip addresse distination,port,protocole et la taille d'un tuple pour préparer nos données
- **FogDevice :** nous applicons dans cette classe la stratégie proposé pour le traitement des donneés.
- **Vrgame :** nous utilisons la fonction rundom() pour donner des données différent pour chaque tuple.

4.2.3.4. Modèle d'application

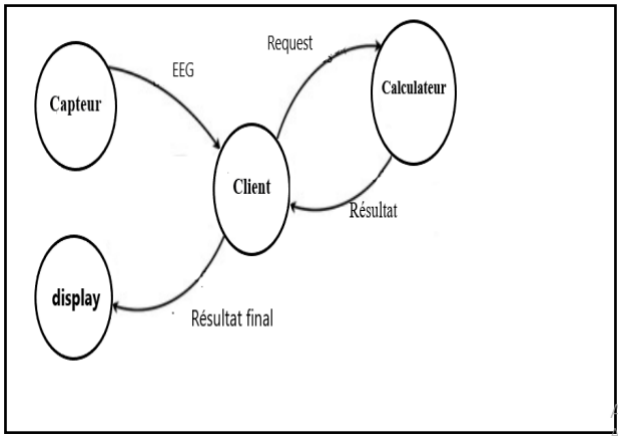

Figure 4.4 – *Modèle d'application*

Pour notre application, nous avons créé un modèle simple. Ce modèle se compose de deux modules : le module Client et le module Calculateur. Le module Client est déployé sur le mobile et le module Calculateur est placé au niveau Fog. Le module client recueillit des informations à partir d'un capteur et effectuer un traitement préliminaire avant de le transmettre au module Calculateur. Le module Calculateur traite les données du mobile et envoie les résultats au module Client pour les afficher sur l'affichage du mobile.

La classe AppModule est utilisée pour modéliser les modules d'application dans iFogSim.

La classe AppEdge dans iFogSim est utilisée pour modéliser les dépendances entre les modules.

4.2.4. RÉSULTATS EXPÉRIMENTEAUX

4.2.4.1. Fonction de perte :

La fonction de la perte représente l'erreur ou l'écart entre la production prévue du modèle et les valeurs cibles réelles pendant la formation. Nous avons utilisé la fonction de perte d'erreur quadratique moyenne

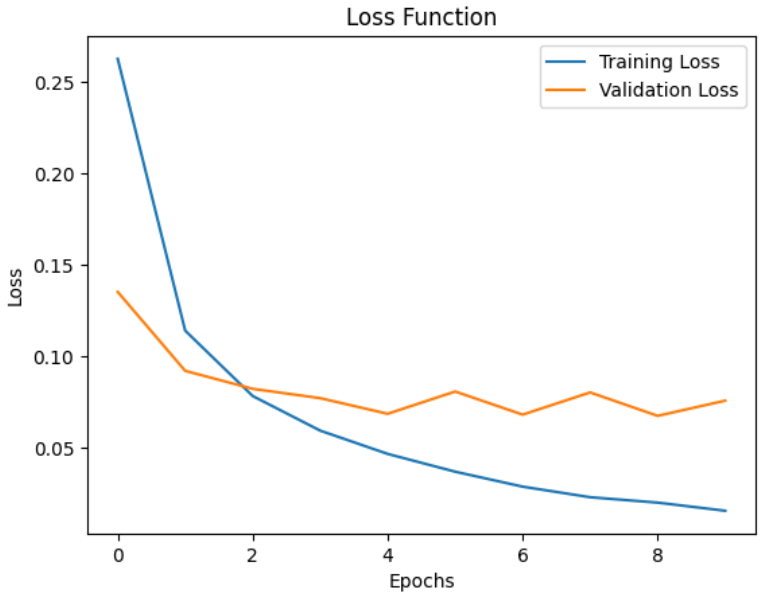

Figure 4.5 – *fonction de perte*

— Blue Ligne nous montre la perte de formation que nous voyons ici qu'elle a diminué progressivement et en général et cela nous indique que notre modèle apprend à réduire les erreurs et cela décrit l'adéquation du modèle aux données de formation au fil du temps.

— La ligne orange indique la perte de vérification, nous voyons qu'elle a d'abord diminué, puis s'est stabilisée. À partir de là, nous concluons que le modèle fonctionne bien sur de nouvelles données.

4.2.4.2. Précision (accuracy) :

L'exactitude représente le pourcentage d'étiquettes correctement attendues par le modèle pendant la formation.

$$accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN}$$

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

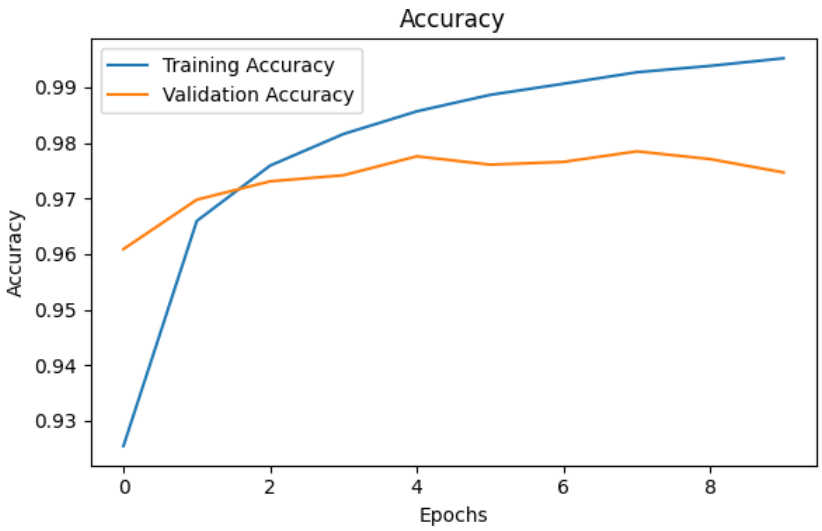

Figure 4.6 – *fonction de précision*

— La ligne bleue la voit augmenter rapidement à mesure que le modèle apprend, puis commence à s'installer. Cela reflète la capacité du modèle à améliorer ses prévisions avec des marques de données de formation.

— La ligne orange représente l'exactitude de la vérification que nous voyons qu'elle augmente initialement légèrement puis se stabilise, ce qui explique

la qualité que notre modèle circule même sur des données invisibles.

— En examinant la fonction des complots de perte et d'exactitude, nous avons pu mieux comprendre le rendement et le comportement de notre modèle pendant la formation.

— Nos résultats ont montré que la perte de formation et la perte de validation diminuent tandis que la précision de la formation et la précision de la vérification augmentent, ce qui indique que le modèle apprend et circule bien

4.3. Conclusion

Le simulateur ifogsim facilite la gestion des données des capteurs pour simplifier la connectivité à les services de cloud et fog computing à travers des différentes classes, parmi les classes nous avons choisissant la classe fog device pour l'analyse des données capturées par un objet connecté au niveau de fog avant de d'envoyer aux niveau cloud ou de répondre aux utilisateurs finaux afin que les actionneurs donne des actions.

Conclusion générale

L'intelligence artificielle a fourni de nombreux outils pour résoudre les problèmes les plus difficiles en informatique, notamment en matière de sécurité. Il a fourni des résultats étonnants pour la sécurité de l'information grâce à l'analyse précise de diverses données telles que des images, audio, données en temps réel et même des données de capteurs. Ces solutions consistaient en des algorithmes et des techniques avancés dans leur étude et analyse des données. D'autre part, des systèmes de détection d'infiltration sont en place comme méthodes contre les risques de sécurité.

Notre proposition était donc de concevoir un système de détection d'intrusion utilisant des techniques de deep learning et de machine learning dans l'environnement associé à l'IoT. Nous avons appliqué le système de détection d'intrusion proposé au simulateur IFogSim qui nous permet d'acquérir et de gérer l'environnement IoT, de la réception des données par les sensors aux couches de Fog cmputing qui représentaient l'emplacement de notre système de détection, Notre système de détection des intrusions a donné de bons résultats en matière de classification et de détection, ainsi que de vérification et de prévention des intrusions détectées.

Bibliographie

[1] INRIA.Mis à jour le 25/10/2022. https ://www.inria.fr/fr/internet-des-objets.

[2] f.z.Fagroud,eh.Benlahmar,s.Filali,h.Toumi(2019).IOT et Cloud computing : etat de l'art., Institut Universitaire de Technologie d'Aix-Marseille (France), Jun 2019, CASABLANCA, Maroc. ffhal-02298881

[3] f.M.Serrat,k.Hammadi,g.Bourgoin.groupe Wireless Logic, leader européen dans la fourniture de cartes SIM multi-opérateurs et de services M2M/IoT industriels.

[4] SYSRESEAU.2 JANVIER 2023.https ://sysreseau.net/iot-internet-des-objet.

[5] j.Nareen,p.Deepika,s.k.Sowmya(2014)Layers of Cloud – IaaS, PaaS and SaaS : A Survey. (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4477-4480

[6] b.Bachari Rad,a.SHareef(2017).Fog Computing : A Short Review of Concept and Applications.IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.11, November 2017

[7] zebraconseils.17 juin 2023.https ://www.zebraconseils.fr/quelle-sont-les-types-de-securite-6794

[8] Mithun Mukherjee ; Rakesh Matam ; Lei Shu ; Leandros Maglaras ; Mohamed Amine Ferrag.10.1109/ACCESS.2017.2749422

[9] ILLY Poulmanogo(25 Avril 2018).1Les systèmes de détection d'intrusion (IDS)Rapport de recherche pour le cours IFT6271-Sécurité informatique.

[10] Marion Karle,Nicolas Baudoin(2003-2004).NT Réseaux IDS et IPS.

[11] BENHAMMADA Sadek(2006-2007).Etude comparative de méthodes de sélection decaractéristiques en apprentissage automatique.Proposition d'une variante

[12] LES CONCEPTIONS DE L'APPRENTISSAGE CHEZ LES FUTURS ENSEIGNANTS. UNIVERSITÉ DU QUÉBEC À MONTRÉAL.NAEYC, 2009 ; Fullan, 2013 ; ministère de l'Éducation de l'Ontario, 2014.

[13] Steeven JANNY - Solal NATHAN – Wenqi SHUQUARTIER(24/05/2022).Introduction à l'apprentissage automatique Ludovic DE MATTEIS

[14] Jake Lever, Martin Krzywinski,Naomi Altman(29 June 2017).Principal component analysisNat Methods 14, 641–642 (2017). https ://-doi.org/10.1038/nmeth.4346

[15] Sidharth Mishra,Uttam Sarkar,Subhash Taraphder,Menalsh Laishram.Multivariate Statistical Data Analysis- Principal Component Analysis (PCA).nternational Journal of Livestock Research eISSN : 2277-1964 NAAS Score -5.36

[16] Roberts, Daniel A., Yaida, Sho, Hanin, Boris. Machine Learning (cs.LG) ; Artificial Intelligence (cs.AI) ; High Energy Physics - Theory (hep-th) ; Machine Learning (stat.ML)

[17] Kishwar Sadaf1 and Jabeen Sultana1.Digital Object Identifier 10.1109/ACCESS.2017.Doi Number Intrusion Detection based on Autoencoder and Isolation Forest in Fog Computing

[18] Shaun Turney(May 13, 2022).https ://www.scribbr.com/statistics/pearson-correlation-coefficient

[19] Jason Brownlee(June 10, 2020).https ://machinelearningmastery.com/standardscaler-and-minmaxscaler-transforms-in-python

[20] Lekhana.Ganji,https ://www.geeksforgeeks.org/ml-one-hot-encoding-of-datasets-in-python

[21] JESUS PACHECO , VICTOR H. BENITEZ , LUIS C. FÉLIX-HERRÁN , AND PRATIK SATAM.Artificial Neural Networks-Based Intrusion Detection System for Internet of Things Fog Nodes.Received March 17, 2020, accepted March 30, 2020, date of publication April 15, 2020, date of current version May 1, 2020.

Table des figures