République Algérienne Démocratique et Populaire

Ministère d'Enseignement Supérieur et de la Recherche Scientifique

Université ABBES LAGHROUR-Khenchela-

Département MI

Mémoire

Présenté en vue d'obtenir le diplôme de

Master en Informatique(LMD)

Détection des intrusions pour les systèmes IoT en utilisant des techniques d'apprentissage

Encadrer Par :

Mr. Zianou Ahmed Seghir

Présenter Par :

Dridi Halima

Hamdani Nacira

Année Universitaire

2020-2021


بسم الله الرحمن الرحيم

Remerciement

Nous tenons tout d'abord à remercier Dieu le tout puissant qui nous a aidé et nous a donné la patience pour finir ce travail malgré tout. Notre haute gratitude nous exprimons nos remerciements à notre encadreur Mr. ZIANOU AHMED SEGHIR pour l'assistance qu'il nous a témoigné, pour sa disponibilité, pour ses orientations et conseils sans lesquels ce projet ne verra pas le jour, qu'elle trouve ici l'expression de notre gratitude.

Nous jamais oubliant nos enseignants qui tout au long du cycle d'étude à l'université ABBES LAGHROUR, nous ont transmis leur savoir.

Enfin, Nous remercions aussi tous nos amis et collègues qui nous ont soutenu et tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

Un grand merci à tous

DÉDICAC

C'est avec une grande émotion et un immense plaisir que je dédie ce modeste travail :

À ma famille, elle qui m'a doté une éducation digne, son amour a fait de moi je que je suis aujourd'hui.

A mes très chers parents, que Dieu les garde, qui étaient toujours là pour moi.

A mon époux Ali.

A mon petit sourire Massil.

À ma force et mon soutien dans la vie : mes chères sœurs : Rawia, Ratiba et Fadwa.

Je vous remercie pour tout ce que vous avez fait pour moi.

À mes adorables frères : Amir, Ismail.

À mes chers neveux et nièces que le Dieu vous protège.

À mes amies proches qui ont toujours été à mes côtés : Khaoula et Hiba.

Nacira

DÉDICAC

Après Bismillah et Et que les prières et la paix soient sur le Messager de Dieu,je dédie ce travail,

- ✓ ***Aux âmes des martyrs d'Algérie***
- ✓ ***A l'âme de mon cher père, il a fait sa dernière demeure au paradis iin sha' allah***
- ✓ ***A la bougie qui éclaire mon chemin, ma mère bien-aimée***
- ✓ ***A mon compagnon, cher mari Azzedine***
- ✓ ***A la lumière de mon chemin, mes filles, Nauruane et Soundous,***
- ✓ ***A celui qui m'a rendu plus fort, mon cher fils Luqman***
- ✓ ***A mes frères et mes sœurs, mon soutien dans la vie***
- ✓ ***A celui qui m'a donné la force de continuer, mon collègue Nassira***
- ✓ ***A tous mes professeurs et ceux qui m'ont appris***
- ✓ ***A tous mes étudiants et à tous mes amis, amis d'études et de travail***
- ✓ ***A tout les étudiant***

HALIMA

Résumé

La nature ouverte de l'Internet a créé la possibilité de connecter des appareils, des applications et des services à une ampleur qui transforme la façon dont nous interagissons avec notre environnement et notre société.

L'Internet des Objets a un énorme potentiel pour changer notre monde pour le mieux, en même temps, avec des milliards d'appareils, d'applications et de services IdO déjà utilisés, et de plus en plus nombreux à venir en ligne, la sécurité de l'IdO est devienne plus importante, Les appareils et services IdO mal sécurisés peuvent servir de points d'entrée pour les cybers attaques.

Avec le grand volume des données, les méthodes classiques de détection des intrusions deviennent insuffisantes.

Dans cette thèse, on va proposer un système de détection d'intrusions pour les internet des objets on se basant sur le machine learning, afin d'aboutir une forte sécurité contre les attaque et les intrusions inconnu.

Summary

The open nature of the Internet has created the possibility of connecting devices, applications and services on a scale that is transforming the way we interact with our environment and our society.

The Internet of Things has enormous potential to change our world for the better, at the same time, with billions of IoT devices, applications and services already in use, and more and more coming online, the IoT security is becoming more important. Poorly secured IoT devices and services can serve as entry points for cyber-attacks.

With the large volume of data, conventional methods of intrusion detection become insufficient. In this thesis, we will propose an intrusion detection system for the Internet of Things based on machine learning, in order to achieve strong security against unknown attacks and intrusions.

Table des matières

Table des figures :

Introduction générale :

Les réseaux et les systèmes informatiques sont devenus des outils indispensables au fonctionnement des entreprises. Ils sont aujourd'hui déployés dans tous les secteurs professionnels : les universités, les banques, les assurances ou encore le domaine militaire.

L'informatique gérée par ces systèmes fait l'objet de convoitises. Elle peut être exposée à des attaques qui exploitent des éléments vulnérables du système d'information. La détection des actions malveillantes est rapidement devenue une nécessité.

Les mesures de prévention se sont révélées insuffisantes et ont amené la création de systèmes de détection d'intrusions (IDS : Intrusion Détection systèmes).

Une intrusion est définit comme étant toute tentative pouvant nuire à l'intégralité, la confidentialité ou la disponibilité dans le réseau ainsi que toute tentative visant à contourner les dispositifs de sécurité mis en place sur le réseau ou une machine. Ces tentative d'intrusions peuvent être bénignes comme extrêmement dangereuses et préjudiciable pour l'entreprise.

Le domaine de la détection d'intrusion est encore jeune mais en plein développement .Nous dénombrons a l'heure actuelle environ une centaine de systèmes de détections d'intrusions (ou IDS pour Intrusion Detection System), que ce soit des produits commerciaux ou du domaine public .Ces systèmes de surveillance du réseau sont devenus pratiquement indispensables dû à l'incessant accroissement en nombre et en dangerosité des attaques réseaux depuis quelques années.[1]

Dans notre travail on s'intéresse sur les différentes systèmes utilisées dans la détection d'intrusion, généralement ces dernières sont des systèmes de datamining ou de machine Learning et technique statique.

Organisation du mémoire

Notre mémoire est organisé comme suit :

Le premier chapitre est consacré à l'internet des objets. Le deuxième chapitre est axé à la présentation des systèmes de détection des intrusions. Le troisième chapitre est fondé sur le machine learning (apprentissage automatique). Le quatrième chapitre parle de différents systèmes de détection d'intrusion pour les IOT basés sur le machine learning. On termine notre étude par la conception et la réalisation de notre application.

Chapitre 01 : Introduction à l'internet des objets.

1.1 Introduction

Un nouveau paradigme appelé Internet des Objets a rapidement gagné du terrain ces dernières années. L'IdO fait référence à "un réseau mondial d'objets interconnectés adressables de manière unique, basé sur des protocoles de communication standard" dont le point de convergence est l'Internet. L'IdO repose sur la présence omniprésente, autour des personnes, d'objets, capables de mesurer, déduire, comprendre, et même modifier leur environnement. Il repose sur des nœuds (objets) intelligents et interconnectés dans une infrastructure de réseau dynamique et globale. Il est généralement caractérisé par de petits objets du monde réel, distribués largement, avec une capacité de stockage et de traitement limitée, ce qui implique des problématiques de fiabilité, de performance, de sécurité et de confidentialité. Il est alimenté par les progrès récents de divers appareils et technologies de communication. Il ne concerne pas seulement des appareils complexes comme les téléphones mobiles, mais aussi des objets simples utilisés tous les jours comme les montres, les thermostats, les vêtements, etc.

Ces objets, agissants comme des capteurs ou des actionneurs, sont capables d'interagir les uns avec les autres.

La principale conséquence de l'IdO est, sans aucun doute, son impact sur la vie quotidienne des utilisateurs potentiels. L'IdO a des effets remarquables à la fois dans la maison et le travail où il jouera un rôle déterminant dans un avenir proche (santé, transport intelligent, domotique, vie assistée, etc.). Des retombées importantes sont également attendues pour les entreprises (transport de marchandises, sécurité, logistique, automatisation industrielle, etc.). Selon ces considérations, le Conseil national de renseignement des États-Unis a déclaré que l'IdO était l'une des six technologies qui auront un impact potentiel sur les intérêts américains à l'horizon

Dès 2011, le nombre de dispositifs interconnectés avait dépassé le nombre de personnes sur Terre .En 2018, le nombre d'appareils interconnectés a été estimé à 30 milliards, et il devrait atteindre la valeur de 50 milliards d'ici 2020 soit 6.58 objets par personne. Ces chiffres suggèrent que l'IdO sera l'une des principales sources de données volumétriques.[1]

1.2 Internet des objets : définitions

Avant de définir les concepts d'IdO, il est important de définir l'objet connecté qui est un dispositif dont la finalité première n'est pas d'être un système informatique ni une interface d'accès au web, exemple, un objet tel qu'une machine à café ou une serrure était conçue sans intégration de systèmes informatiques ni connexion à Internet.

Définiion1 : *L'Internet des Objets (IdO) se définit comme un réseau mondial de services interconnectés et d'objets intelligents de toutes natures destinés à soutenir les humains dans les activités de la vie quotidienne grâce à leurs capacités de détection, de calcul et de communication. Leurs aptitudes à observer le monde physique et à fournir des informations pour la prise de décision, seront partie intégrante de l'architecture de l'Internet du futur.*

Définition2 : *Est l'extension d'internet à des choses et à des lieux du monde physique. Elle représente les échanges d'informations et de données provenant de dispositifs présents dans le monde réel vers le réseau internet.*

Définition3 : *Est un réseau qui permet, via des systèmes d'identification électronique normalisés et sans fils, d'identifier et de communiquer numériquement avec des objets physiques afin de pouvoir mesurer et échanger des données entre les mondes physiques et virtuels.*

Toutes ces définitions traduisent que L'**Internet des Objets**, communément appelé en anglais **Internet of Things (IoT)** désigne une technologie d'avant-garde, où les objets traditionnellement non connectés qui nous entourent (comme des lampes, machines, vêtements, etc.), qu'ils soient physiques ou virtuels, ont désormais la capacité de communiquer entre eux en temps réel. Ce réseau d'objets là permet le partage de leurs données par l'intermédiaire d'une plateforme *Cloud* et ce, sans intervention humaine. Grâce à l'optimisation des interactions entre les humains et les machines et à la multiplication des flux de données, que les objets connectés offrent la possibilité de définir les besoins précis d'un individu, de sorte à lui offrir un bien ou un service unique. [2]

1.3 Domaines d'utilisation (exemples d'application).

On n'en entendait à peine parler il y a quelques années, et ils sont maintenant partout. Les objets connectés ont envahi notre quotidien sans même que nous y prêtions attention.

De la télé intelligente à la voiture connectée, nos loisirs, nos déplacements sont facilités par ces nouveaux outils qui augmentent grandement notre confort.

Le potentiel des objets connectés est énorme. Une étude de 2016 du cabinet Gartner prévoit qu'en 2020, plus de la moitié des outils et process métiers feront appels à l'Internet des Objets. Les applications sont variées et recouvrent de nombreux domaines : industrie, sciences, santé,… Les Jeudis vous proposent dix applications de l'IdO qui transforment le paysage sociétal. [3]

1.3.1 L'IoD dans le domaine de la santé

Machines à rayons X et imagerie, moniteurs connectés, compteurs d'énergie… 60 % des hôpitaux mondiaux utilisent déjà l'Internet des Objets pour augmenter leur productivité et améliorer les soins apportés aux patients. L'étude d'Arubanetworks montre que d'ici 2019, c'est presque 90 % des services de santé qui auront intégré les objets connectés dans leur matériel médical.

Les objets connectés sont utilisés au quotidien pour :

- La surveillance au sein des établissements médicaux et la maintenance
- Les opérations chirurgicales et le contrôle à distance
- Les services de géolocalisation

La normalisation de l'Internet des Objets dans le domaine de la Santé va permettre de créer de nouveaux modèles de fonctionnement qui augmenteront la productivité des employés, mais aussi la collaboration entre soignants ainsi que la communication avec les patients.

1.3.2 La révolution numérique en réponse aux impératifs énergétiques

L'intelligence artificielle est une véritable plus-value dans le domaine énergétique, qui pourrait dans les années à venir représenter un investissement écologique décisif dans l'avenir de notre société. Les enjeux sont également économiques, et les entreprises l'ont bien compris.

L'IoD, dans le cadre de l'énergie, répond à des problématiques majeures :

- Appauvrissement des ressources naturelles
- Accroissement des besoins énergétiques à l'échelle mondiale
- Instabilité des prix du marché
- Manque de main d'œuvre humaine

La révolution numérique est entrée dans le débat des secteurs énergétiques par la gestion des ressources : compteurs énergétiques, réseau intelligent mais aussi l'Internet des Objets à domicile, avec la maison intelligente.

1.3.3 La domotique ou maison connectée

Appelée également domotique, la maison intelligente est en train de se normaliser. Une étude du cabinet Juniper Research prévoit d'ailleurs un accroissement de 200 % du nombre d'objets connectés à l'intérieur des habitations d'ici fin 2021.

Outre les objets de divertissement comme les télés intelligentes ou les enceintes connectées, la domotique a pensé également la sécurité et l'économie d'énergie au sein de l'habitat :

- Centrale domotique : contrôle et programmation de différentes interventions à l'intérieur du foyer
- Capteurs d'informations (système d'alarme, variations de température, etc.)
- Actionneurs, qui permettent la programmation et le contrôle des différents appareils électroniques du foyer, même à distance

1.3.4 L'industrie connectée

L'industrie n'est pas en reste sur l'usage de l'Internet des Objets et des bénéfices que celui-ci lui apporte. Dans le cadre des problématiques rencontrées dans le domaine industriel, l'usage des objets connectés est très spécifique et répond à des besoins :

- D'optimisation (chaîne logistique)
- De transformation des processus d'entreprise
- D'amélioration de l'efficacité et de la productivité
- De traçabilité et de sécurité

La révolution digitale est aussi l'opportunité pour certains types d'industrie de se renouveler et d'apporter une plus-value sur un terrain en perte de popularité. C'est par exemple le cas avec SNCF Fret, qui retrouve doucement ses lettres de noblesse en lançant sa locomotive connectée, qui permet une meilleure traçabilité de ses wagons, et une plus grande sécurité pour le client.

1.3.5 L'Internet des objets dans l'agriculture

La croissance rapide de la population mondiale, les changements d'habitudes alimentaires, les perturbations climatiques sont trois grands facteurs, parmi d'autres, qui font de l'agriculture moderne un défi au quotidien.

D'ici 2050, la productivité agricole devra avoir augmenté de 70 % pour répondre à la demande mondiale. Plus qu'un défi technologique, il s'agit d'un enjeu humanitaire. Les céréaliers et maraîchers ont d'ores et déjà mis à profit les drones afin de de récolter en temps réel des informations essentielles à la gestion de l'exploitation :

- Humidité de la terre
- État des plantations
- Climat, etc.

Les données récoltées sont transférées aux tracteurs connectés (parfois autonomes). Cela permet de doser finement le niveau d'engrais et d'arrosage sur telle ou telle parcelle et de réduire les coûts, tant financiers qu'énergétiques.

1.3.6 Les objets connectés dans les élevages

Traceurs GPS pour le bétail, recueillement des habitudes alimentaires des bovins, les objets connectés ne sont pas seulement utiles aux agriculteurs, mais également aux éleveurs qui peuvent surveiller plus finement l'état de santé de leurs bêtes.

Avez-vous déjà entendu parler des vaches connectées ? Fait amusant, il s'agit de l'animal le plus connecté au monde ! Son collier doté de nombreux capteurs permet une meilleure traçabilité mais aussi d'avoir des informations en temps réel sur son état de santé et son comportement.

1.3.7 Smart retail : des supermarchés branchés

Le commerce physique subit aussi les transformations de l'ère digitale. Fortement concurrencées par le e-commerce et m-commerce, les boutiques de vente au détail veulent tirer profit de la popularité de l'IdO en alliant l'e-commerce à la vente traditionnelle.

Les boutiques physiques ont donc elles aussi pris le pas de la révolution numérique et sont de plus en plus nombreuses à proposer des fonctionnalités ludiques et interactives afin de renforcer l'expérience de vente et accroître le taux de conversion.

On retrouve, parmi les concepts de « smart retail », la technologie d'identification par radiofréquence (RFID) qui permet de renforcer l'expérience client en offrant un parcours client ultra personnalisé. Outre les applications mobiles, des concepts de caddies connectés ont déjà été pensés pour faciliter les courses en supermarché :

- Liste de courses intégrée
- Parcours guidé pour optimiser le temps de course
- Calcul automatique du montant du panier,…

Les commerçants investissent également dans les applications mobiles pour fidéliser et attirer les clients vers les boutiques physiques, par le biais, par exemple, de notifications sur les promotions / soldes en cours lors du passage d'un client près d'une boutique.[1]

1.4 Architecture de l'internet des objets

L'architecture d'un système IoT est composée de plusieurs niveaux qui communiquent entre eux pour relier le monde tangible des objets au monde virtuel des réseaux et du cloud. Tous les projets n'adoptent pas une architecture formellement identique, néanmoins il est possible de schématiser le parcours de la donnée.

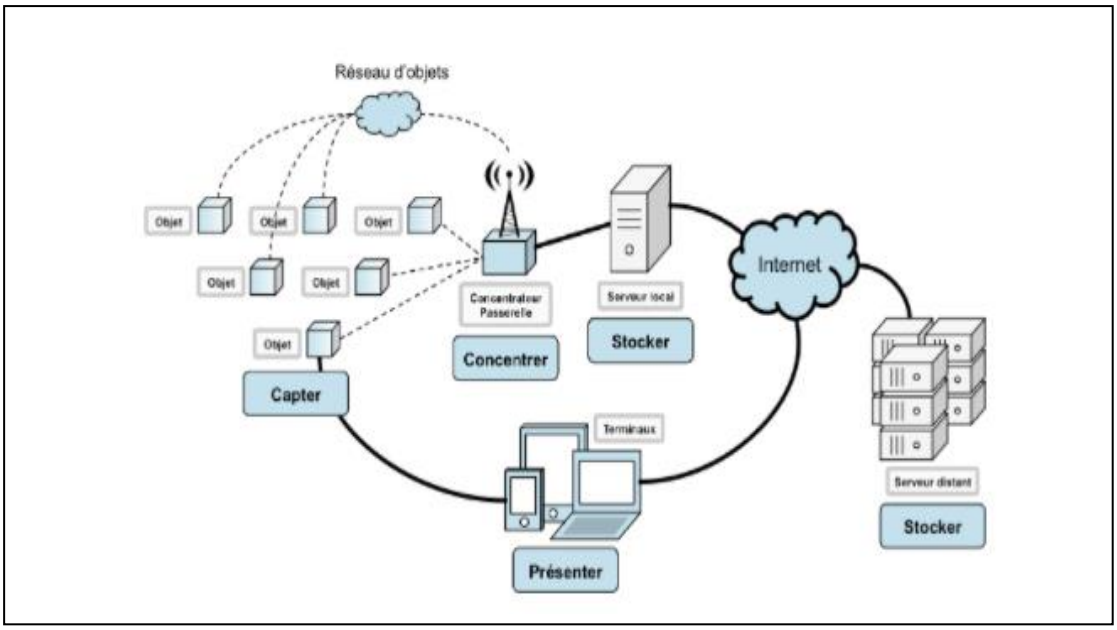


Figure 1.1 : Architecture de l'IoD. [3]

Précisons le rôle des différents processus présentés sur ce schéma :

- **Capter** désigne l'action de transformer une grandeur physique analogique en un signal numérique.
- **Concentrer** permet d'interfacer un réseau spécialisé d'objet à un réseau IP standard (e.g. WiFi) ou des dispositifs grand public.
- **Stocker** qualifie le fait d'agréger des données brutes, produites en temps réel, méta taguées, arrivant de façon non prédictible.

Enfin, **présenter** indique la capacité de restituer les informations de façon compréhensible par l'Homme, tout en lui offrant un moyen d'agir et/ou d'interagir.

Deux autres processus n'apparaissent pas sur le schéma, car ils sont à la fois transverses et omniprésents :

- **Le traitement des données** est un processus qui peut intervenir à tous les niveaux de la chaîne, depuis la capture de l'information jusqu'à sa restitution. Une stratégie pertinente, et commune quand on parle d'Internet des objets, consiste à stocker l'information dans sa forme intégrale. On collecte de manière exhaustive, « big data », sans préjuger des traitements qu'on fera subir aux données. Cette stratégie est possible aujourd'hui grâce à des architectures distribuées type NoSQL, capables d'emmagasiner de grandes quantités d'information tout en offrant la possibilité de réaliser des traitements complexes en leur sein (Map/Reduce par exemple).
- **La transmission des données** est un processus qui intervient à tous les niveaux de la chaîne. Deux réseaux, supports des transmissions, cohabitent généralement :
- **Réseau local de concentration :** On utilise alors des technologies comme ANT, NFC ou Bluetooth.
- **Réseau WAN :** permettant d'interconnecter les réseaux spécialisés et de les interfacer avec des fermes de serveur. On utilise alors WiFi, les réseaux cellulaires (GSM, UMTS, LTE) ou encore les connexions physiques standard (Ethernet, fibre optique). Ces réseaux sont généralement connectés à Internet.

Les technologies de transmission utilisées dépendent essentiellement de l'application et du contexte. La transmission peut par exemple exploiter le Push reposant sur Comet ou WebSocket. Les canaux peuvent être bidirectionnels si l'application autorise une rétroaction. Dans certains cas, ces canaux devront transmettre les données en temps réel, dans d'autres cas, le temps ne sera pas un facteur déterminant.[3]

1.5 Conclusion

Nous pouvons penser que l'intégration de nombreux objets du monde réel sur Internet nécessitera de créer de nouvelles interactions intuitives de haut niveau avec le monde physique et sera au cœur de l'Internet des Objets. Du fait de leur complexité croissante, l'intégration d'un maximum d'automatismes dans les architectures de l'IdO ne sera que bénéfique à leurs utilisations. S'il est nécessaire que les objets, de natures différentes, collaborent entre eux, nous devons faire face aux problèmes d'hétérogénéité, d'interopérabilité et de sécurité. Les applications conçues pour l'IdO sont aujourd'hui trop monolithiques, trop adaptées à un contexte particulier ce qui freine toute personnalisation, toute réutilisation.

En ce qui concerne la sécurité, nous notons que le domaine de l'IdO ouvert, hétérogène et mobile est vulnérable. Il présente des risques importants en termes de sécurité. Les limites du système sont plus perméables depuis que le système a été étendu : de l'objet intelligent à la passerelle, puis au nuage. En outre, le fait qu'une application IdO peut, par exemple, générer des informations susceptibles d'être facturées ou que certains objets nécessitent une vérification de leur intégrité, cela nous oblige à fournir un environnement d'exécution sécurisé et de confiance pour l'exécution des applications de haute sécurité. [4]

Chapitre 2 : Système de détection des intrusions

2.1 Définition :

Un système de détection d'intrusions (« Intrusion Detection Systems » ou IDS) est un appareil ou une application qui alerte l'administrateur en cas de faille de sécurité, de violation de règles ou d'autres problèmes susceptibles de compromettre son réseau informatique.

Les systèmes de détection d'intrusions surveillent et analysent les activités d'un réseau, analysent ses configurations et ses vulnérabilités, et vérifient l'intégrité des fichiers. Ils peuvent reconnaître des schémas d'attaque classiques. Pour ce faire, ils analysent les comportements anormaux et suivent les violations de règles par les utilisateurs. Certains systèmes industriels de détection d'intrusions peuvent également réagir à des menaces détectées.

Un système IDS est en général à double détente. La première étape, que l'on peut qualifier de passive, intervient sur la machine. Il s'agit de l'inspection des fichiers de configuration du réseau, notamment pour détecter les paramètres déconseillés et les violations de règles. La seconde étape, que l'on peut qualifier d'active, intervient sur le réseau. Ici, les mécanismes réutilisent des méthodes d'attaque identifiées et enregistrent les réactions.[5]

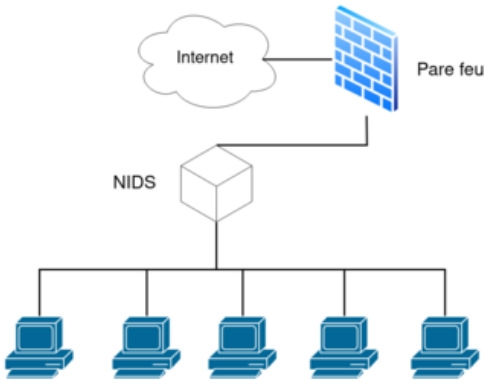


Figure 2.1 : Placement d'un NIDS en amont d'un pare-feu.

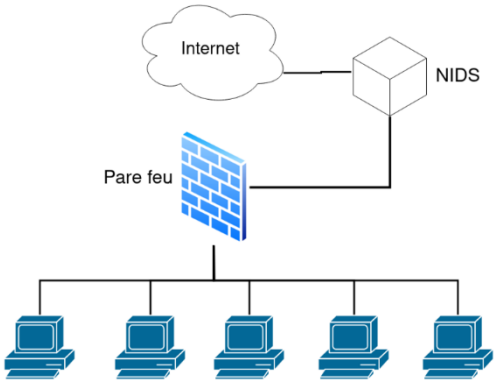


Figure 2.2 : Placement d'un NIDS en aval d'un pare-feu.

2.2 Les composants d'un système de détection d'intrusion :

On peut distinguer trois couches nécessaires pour un IDS :

2.2.1 La surveillance du système d'information :

La couche de surveillance du système d'information est chargée d'enregistrer toutes les actions. Les actions viennent soit :

- Du trafic réseau (NIDS) ;
- Du Système d'exploitation (HIDS).

Ces actions peuvent être de différentes sortes (lectures, écriture de fichiers, authentification...) et sont ensuite enregistrées en logs, qui sont envoyés à la couche surveillance afin d'être

3.1.1. Le scannage des sources d'informations :

La couche de monitoring va analyser les logs. Son but est d'évaluer les menaces pesant sur le système d'information en recherchant des événements notables. Les logs sont regroupés afin de distinguer des motifs permettant de distinguer une action connue, qui est alors évaluée. Ces événements sont alors classés en événements notables ou non.

Dans le cas où les événements sont notables, l'IDS va évaluer la menace du système d'information.

Après avoir identifié la menace de notre Système d'Information, il va alors indiquer son jugement sur la sécurité du réseau ou des systèmes et transmettre sa décision à la couche décision [4].

3.1.2. Les décisions prises lors de l'évaluation positive d'une intrusion :

Si la couche surveillance juge que le système a été compromis, l'IDS peut prendre plusieurs décisions :

- La première est de prévenir l'administrateur du système d'information afin qu'il puisse prendre les décisions qui s'imposent ;
- la deuxième est d'effectuer une action définie à l'avance par l'administrateur système afin d'empêcher l'intrusion (ou la ralentir).

Remarque : Selon les choix effectués lors de la conception d'un IDS, certaines parties de l'architecture peuvent changer. Les systèmes de détection d'intrusion distribués (DIDS) combinent les contraintes des systèmes distribués et des IDS.

La technique d'analyse des données peut éventuellement modifier l'architecture en ajoutant la couche de traitement des données propre à la technologie utilisée. Par exemple, lors de l'utilisation de réseaux neuronaux, les données doivent être traduites en données compréhensible pour le réseau et le résultat doit être traduit.

On peut ensuite considérer que le cloud computing pose de nouvelles contraintes sur l'architecture d'un IDS, notamment pour la détection d'intrusion. [5]

3.2. Caractéristiques souhaitées d'un IDS :

- Il doit fonctionner de manière continue avec une présence humaine minimum.
- Il doit être tolérant aux fautes c'est-à-dire qu'il doit être capable de retrouver son état initial de fonctionnement après un crash causé soit par une manipulation accidentelle soit par des activités émanant de personnes malintentionnées.
- Il doit résister à la subversion. L'IDS doit être capable de se contrôler lui-même et de détecter s'il a été modifié par un attaquant.
- Il doit imposer une supervision minimale du système sur lequel il tourne afin de ne pas interférer avec ses opérations normales.
- Il doit être configurable d'après les politiques de sécurité du système qu'il supervise.
- Il doit également être capable de s'adapter aux changements des systèmes et des comportements des utilisateurs au cours du temps (par exemple installation de nouvelles applications, transfert des utilisateurs d'une activité vers une autre et du coup transfert des ressources du système).

  Lorsque le nombre de systèmes à superviser augmente et donc que les attaques potentielles augmentent également, nous pouvons alors attendre de l'IDS les caractéristiques suivantes :

- Il doit être capable de superviser un nombre important de stations tout en fournissant des résultats de manière rapide et précise.

- Il doit fournir "un service minimum de crise" c'est-à-dire que si certains composants de l'IDS cessent de fonctionner, les autres composants doivent être affectés le moins possible par cet état de dégradation.
- Il doit autoriser des reconfigurations dynamiques. Si un grand nombre de stations est supervisé, il devient pratiquement impossible de redémarrer l'IDS sur tous les hôtes lorsque l'on doit effectuer un changement. [4]

3.3. Principes de détection :

Nous classons les IDS en deux grandes catégories de principe de détection d'intrusion :

2.4.1 Approche par scénario

Les systèmes à base de signatures qui consistent à rechercher dans l'activité de l'élément surveillé les signatures (empreintes) d'attaques répertoriées et donc connues. Ce principe de détection d'intrusion est réactif et pose plusieurs contraintes, en effet il ne détecte que les attaques répertoriées dont il possède l'empreinte. De ce fait il nécessite des mises à jour fréquentes. Ce principe de détection implique aussi que les pirates peuvent contourner celui-ci en maquillant leurs attaques, il modifie en fait la signature connue par les IDS et de ce fait l'attaque devient invisible par l'IDS.

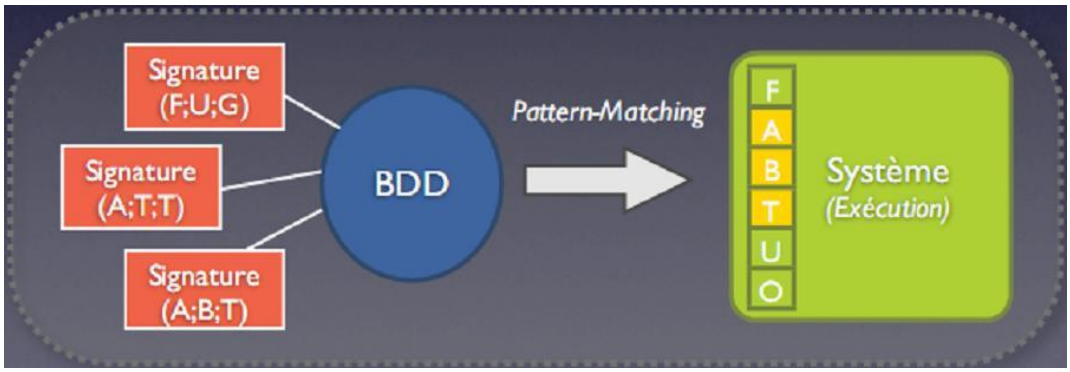


Figure 2.3.:Approche par scénario

Cette approche fournit un diagnostic clair, il est donc possible de réagir et de contre attaquer, si la politique de sécurité est celle-là. Par contre ils ne peuvent détecter que les attaques contenues dans la base de connaissances. Il faut en permanence maintenir à jour cette base. Il est possible de rendre inactif un IDS utilisant cette approche par une attaque en déni de service.

2.4.2 Approche comportementale :

Chapitre 2 : Système de détection des intrusions

Les systèmes à approche comportementale consistent à détecter les différentes anomalies sur le réseau. C'est l'administrateur qui définira le fonctionnement "normal" des éléments surveillés, il y a donc une phase d'apprentissage pour fixer ce niveau. Par la suite l'IDS sera en mesure de signaler à l'administrateur toute situation qui divergera du niveau de fonctionnement de référence. Le fonctionnement de référence peut être élaboré par différentes analyses statistiques de l'élément à surveiller. Ce système de détection présente un avantage par rapport au précèdent : il détecte les nouveaux types d'attaques. Cependant il faudra faire parfois des ajustements afin que le fonctionnement de référence corresponde au mieux à l'activité normale des utilisateurs et ainsi réduire les fausses alertes qui en découleraient.

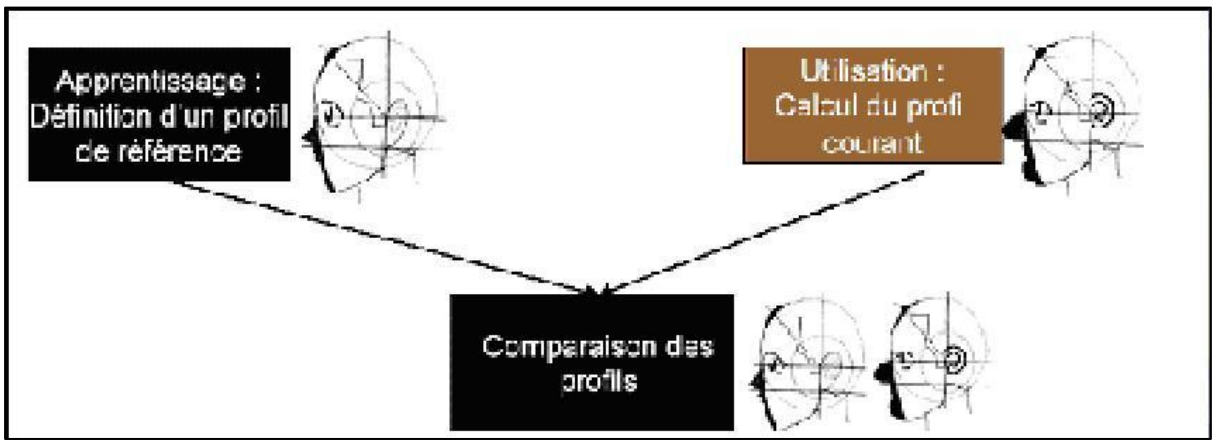


Figure 2.4 : Approche comportementale.

Cette approche a l'avantage de ne pas avoir besoin d'une base de signature. Elle permet donc, en théorie, de détecter des attaques inconnues. Cependant, elle a des inconvénients assez importants.

Que se passe-t-il s'il y a une attaque pendant l'apprentissage ? Celle-ci est considérée comme un comportement normal, et ne sera jamais détectée. De même il n'y a aucune interprétation de l'attaque, on ne sait pas quelle attaque a été déclenchée. On ne sait donc pas réagir. Il est très difficile d'effectuer un apprentissage complet.[6]

Méthodologie de détection :

Les systèmes de détection d'intrusion sont généralement classifiés en deux catégories, les systèmes de détection d'intrusion par signatures et les systèmes de détection d'intrusion par anomalies.

2.4.3 Systèmes de détection d'intrusion par signatures :

Les systèmes de détection d'intrusion par signature (ou SIDS : Signature-based Intrusion Detection System), reposent sur des bibliothèques de description des attaques (appelées signatures). Au cours de l'analyse du flux réseau, le système de détection d'intrusion analysera chaque événement et une alerte sera émise dès lors qu'une signature sera détectée. Cette signature peut référencer un seul paquet, ou un ensemble. Cette méthodologie de détection se révèle être efficace uniquement si la base de signatures est maintenue à jour de manière régulière. Dans ce cas, la détection par signatures produit peu de faux-positifs. Cependant, une bonne connaissance des différentes attaques est nécessaire pour les décrire dans la base de signature8. Dans le cas d'attaques inconnues de la base, ce modèle de détection s'avérera inefficace et ne générera donc pas d'alertes. La base de signature est donc très dépendante de l'environnement (système d'exploitation, version, applications déployées, …).pour effectuer une détection par signature, on peut utiliser, Les arbres ou les systèmes de transition d'états.

2.4.4 Systèmes de détection d'intrusion par anomalies *:*

Contrairement aux SIDS, les systèmes de détection d'intrusion par anomalies (ou AIDS : Anomaly-based Intrusion Détection System) ne se reposent pas sur des bibliothèques de description des attaques. Ils vont se charger de détecter des comportements anormaux lors de l'analyse du flux réseau. Pour cela, le système va reposer sur deux phases :

- Une phase d'apprentissage, au cours de laquelle ce dernier va étudier des comportements normaux de flux réseau.

- Une phase de détection, le système analyse le trafic et va chercher à identifier les événements anormaux en se basant sur ses connaissances.

Cette méthode de détection repose sur de nombreuses techniques d'apprentissage supervisé, telles que :

- ✓ Les réseaux de neurones artificiels.
- ✓ Le modèle de Markov caché.
- ✓ Les machines à vecteurs de support.

En 2019, la détection d'intrusion par anomalies est reconnue par la communauté comme étant très efficace. En effet, selon les méthodes d'apprentissage implémentées, l'exactitude des résultats peut rapidement atteindre plus de 90% de détection.

2.4.5 Hybride *:*

Cette méthodologie de détection consiste à reposer à la fois sur un système de détection par signatures et sur un système de détection par anomalies. Pour cela, les deux modules de détection, en plus de déclencher des alertes si une intrusion est détectée, peuvent communiquer leurs résultats d'analyse à un système de décision qui pourra lui-même déclencher des alertes.

2.4.6 Temporalité de détection :

Il existe deux types de temporalité dans les systèmes de détection d'intrusion. La détection en temps réel (système temps réel), et la détection post-mortem (analyse forensique). Le plus souvent, l'objectif est de remonter les alertes d'intrusion le plus rapidement possible à l'administrateur système. La détection en temps réel sera donc privilégiée. Cette temporalité de détection présente des défis de conception pour s'assurer que le système puisse analyser le flux de données aussi rapidement qu'il est généré. il est aussi envisageable d'utiliser un système de détection d'intrusion dans le cadre d'analyse post-mortem. Dans ce cas, ce dernier permettra de comprendre le mécanisme d'attaque pour aider à réparer les dommages subis et réduire le risque qu'une attaque du même genre se reproduise.

2.4.7 Corrélation des alertes :

La corrélation des alertes a pour objectif de produire un rapport de sécurité de la cible surveillée . Ce rapport sera basé sur l'ensemble des alertes produites par les différentes sondes de détection

d'intrusion disséminées sur l'infrastructure. Pour cela, il est nécessaire de différencier deux composants :

- les sondes : chargées de récupérer les données depuis les sources concernant leurs cibles (fichiers de logs, paquets réseaux,…) et de générer, si nécessaire, des alertes.

- les composants d'agrégation et de corrélation : chargés de récolter les données des sondes et des autres composants d'agrégation et de corrélation afin de les corréler et produire le rapport de sécurité transmis à l'administrateur.

Les corrélations peuvent être décrites en deux types :

- les corrélations explicites : ces corrélations sont utilisées lorsque l'administrateur peut exprimer une connexion entre des événements connus.

- les corrélations implicites : celles-ci sont utilisées lorsque les données ont des relations entre elles et que des opérations sont nécessaires pour mettre en valeur certains événements. [5]

2.5 Étude et choix d'une solution de détection d'intrusion :

Concernant la source de données, la première chose à considérer lors de l'étude d'une solution de détection d'intrusion est le choix d'une sonde de détection : HIDS et NIDS (Network-based Intrusion Detection System). L'évaluation des sondes pourra s'appuyer sur une grille de notation intégrant les critères suivants :

- Méthodes et capacités de détection.
- Performance en conditions de charge élevées.
- Résistance aux techniques d'évasion.
- Exploitation des données à traiter.
- Ergonomie des interfaces d'administration et d'exploitation.
- Coûts de la solution.

Un HIDS aura un impact sur le serveur en termes de performance, car il va consommer une partie des ressources de ce serveur. Concernant l'installation d'un ou plusieurs NIDS, il

faudra tenir compte de la disponibilité de points de raccordements permettant d'écouter le réseau. Le positionnement d'une sonde de détection dépend des contraintes propres à l'architecture. À l'extérieur du pare-feu (côté WAN), la sonde NIDS est plus proche des attaquants, mais va lever un volume important d'alertes en raison d'attaques classiques (e.g. balayage de port) qui seront très certainement bloquées par le pare-feu. Une sonde NIDS à l'intérieur d'un pare-feu (côté LAN), sera moins exposée aux bruits de fond résiduels et aux faux-positifs qui en résultent.

Par ailleurs, il peut être nécessaire de configurer la sonde NIDS avec deux interfaces réseaux. La première effectuera une surveillance en mode « promiscuous ». Dans ce mode, on capture tous les paquets qui passent par le lien réseau, qu'ils soient ou non adressés à la sonde. La seconde sera placée sur un VLAN (Virtual Local Area Network) dédié pour communiquer avec le système de gestion des événements et la console de gestion. En ce qui concerne les sondes HIDS, elles devront être déployées sur les serveurs critiques. [7]

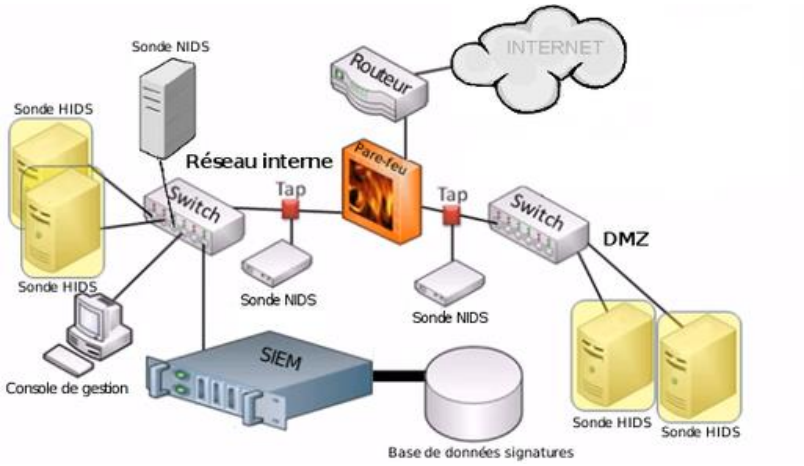


Figure.2.5 : Positionnement des sondes de détection d'intrusion dans une architecture réseau simplifiée.[7]

2.6 Les défis liés à la détection d'intrusions :

La sécurité de l'information ne se limite plus à une approche purement technique. Aujourd'hui, certaines entreprises ont conscience que quelques briques technologiques, logicielles ou matérielles, ne suffisent plus à protéger leurs informations critiques. Désormais, ces entreprises s'orientent vers le management de la sécurité, dans une approche globale, aussi bien organisationnelle, technologique que juridique.

Chapitre 2 : Système de détection des intrusions

L'étude du cabinet d'audit Price Waterhouse Coopers auprès de 3 877 entreprises dans 78 pays « fait ressortir que plus d'une entreprise sur deux déclare que le Directeur des Systèmes d'Information est, in fine, propriétaire des risques de cybercriminalité. Seulement, une entreprise sur cinq (5 % en France) déclare ainsi que cette responsabilité est, in fine, du ressort de la Direction Générale ou du Conseil d'Administration » .Or, un facteur déterminant dans la réussite d'un projet de sécurité de l'information, s'intégrant ou non dans un système de gestion de la sécurité de l'information (ISMS ou *Information Security Management System*), est l'engagement réel et affiché de la structure dirigeante et des managers intermédiaires de l'organisation.

La prise en compte de la gestion des risques au sein du SI permet de considérer la sécurité de l'information comme un processus métier transverse et une réelle composante de la stratégie d'entreprise.

Ainsi, un projet de détection des intrusions qui s'inscrit dans un contexte de gestion des risques, dépasse la seule compétence des équipes techniques, du RSSI. [8]

Le processus de la gestion des risques de sécurité des SI peut être résumé en six phases principales :

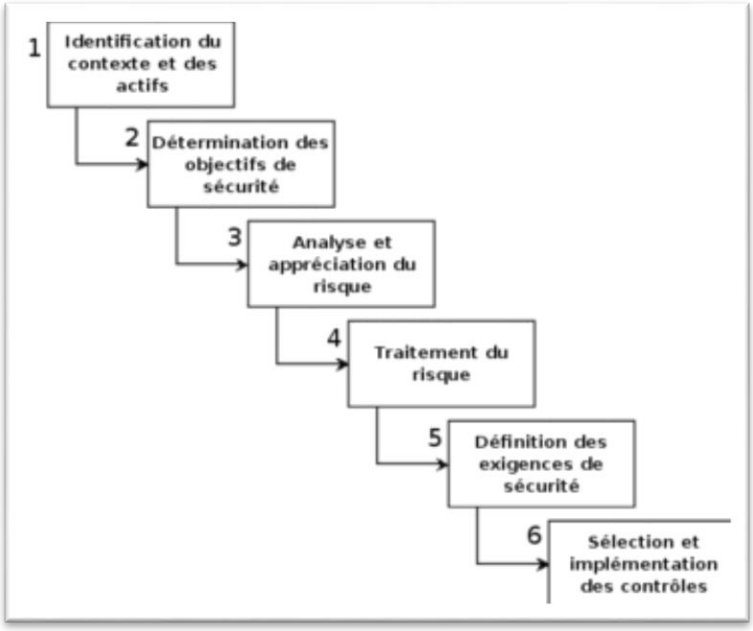


Figure 2.6 : Le processus de gestion des risques de sécurité.

Les trois premières phases conduisent à identifier, analyser et apprécier les risques de sécurité.

En phase 4, nous pouvons les accepter et ne rien faire, ou les transférer en externalisant une activité par exemple, voire les réduire en agissant sur leurs origines ou leurs conséquences.

En phase 5, des exigences de sécurité peuvent alors être déterminées afin de réduire le risque. Nous choisissons des mesures à mettre en œuvre pour atteindre ces objectifs de sécurité et elles vont être le fondement de la politique de sécurité. Par exemple, des contrôles techniques peuvent être choisis comme la détection des intrusions sur le réseau du SI.

Un système de détection d'intrusion qui s'inscrit dans ce contexte de gestion du risque, devra être perçu et accompagné par des moyens humains et financiers nécessaires à sa mise en œuvre.

En premier lieu, l'approche purement financière dans le choix de la conduite ou non d'un projet de détection des intrusions est un élément déterminant. Beaucoup de projets n'aboutissent pas, car aucune évaluation du retour sur investissement en sécurité informatique (ROSI ou *Return On Security Investment*) par les DSI ou les RSSI n'est réalisée. Selon les secteurs d'activités, la ligne budgétaire consacrée à la sécurité de l'information est assimilée à un centre de coût et non de profit. Dans un second lieu, l'approche « évaluation des risques » moins financière et plus qualitative est un argument important, mais non suffisant. La mise en place de solutions de détection des intrusions doit s'accompagner d'une évaluation du ROSI.

Le CLUSIF propose un état de l'art autour d'un modèle de coût et de la notion de ROSI. Mais il n'y a pas de consensus clair autour de la définition de ROSI. La définition orientée incidents de sécurité est celle que nous retiendrons.

Toute la difficulté est de pouvoir estimer la valeur exacte de chaque incident de sécurité lié à une intrusion et sa probabilité d'occurrence. La réalisation préalable d'une analyse des risques de sécurité des systèmes d'information facilitera ce travail, car elle intègre une évaluation des actifs du SI, du facteur d'exposition du système (EF ou *Exposure Factor*) et des vulnérabilités d'une infrastructure globale pouvant être exploitées par une ou plusieurs menaces connues ou inconnues.

Enfin, réagir de manière appropriée à une intrusion est surtout une question d'organisation et de procédures qui doivent être définies et appliquées par les équipes informatiques en réponse aux incidents.

Comment traiter l'alerte, comprendre l'incident et le clôturer ? Quelles sont les mesures conservatoires à prendre ? Qui alerter (le responsable sécurité, le CERT, la direction métier, la direction générale, la gendarmerie, etc.) ?

Les activités relatives à la détection d'intrusion doivent s'appuyer sur des actions précises et des rôles alloués à chacun, des outils dont l'informaticien a besoin et les résultats qu'il doit produire sous conditions de présentation, de contraintes de réactivité ou d'astreinte.

Les éléments collectés lors de la phase de détection et la qualification de l'intrusion ne suffisent pas eux seuls. Il est également nécessaire d'évaluer une stratégie de réponse en fonction de la criticité du système compromis et de l'impact d'une interruption de service du système.

- activation d'une cellule de crise.
- délai de remise en production.
- implication des relations publiques et communication appropriée.
- volonté de répondre à une attaque.
- volonté de poursuivre légalement l'attaquant. [6]

2.7 Conclusion

Les outils de détection d'intrusions sont apparus depuis quelques années maintenant et leur usage se répand dans les systèmes d'information et les réseaux. Ils sont sortis du domaine militaire et commencent à être intégrés à la définition des architectures de systèmes d'information commerciaux. Ces systèmes font pour la plupart de l'analyse de trafic (réseau, requêtes) envoyé à un système d'information, et recherchent dans leurs bases de connaissances des éléments identifiant ce trafic comme dangereux. L'évolution naturelle de ces systèmes conduit à prendre en compte des descriptions génériques des mécanismes d'attaque, plutôt que la détection d'attaques spécifiques sur des vulnérabilités connues. Dans un deuxième temps, il pourra apparaître sur le marché des systèmes de détection d'intrusions utilisant des notions de politique de sécurité pour détecter des actions non conformes à celle-ci, même si l'attaque sous-jacente n'est pas explicitement identifiée. [5]

Chapitre 03 : Machine learning (apprentissage automatique)

3.1. Introduction

Le machine learning est un domaine captivant. Issu de nombreuses disciplines comme les statistiques, l'optimisation, l'algorithmique ou le traitement du signal, c'est un champ d'études en mutation constante qui s'est maintenant imposé dans notre société. Déjà utilisé depuis des décennies dans la reconnaissance automatique de caractères ou les filtres anti-spam, il sert maintenant à protéger contre la fraude bancaire, recommander des livres, films, ou autres produits adaptés à nos goûts, identifier les visages dans le viseur de notre appareil photo, ou traduire automatiquement des textes d'une langue vers une autre. Dans les années à venir, le machine learning nous permettra vraisemblablement d'améliorer la sécurité routière (y compris grâce aux véhicules autonomes), la réponse d'urgence aux catastrophes naturelles, le développement de nouveaux médicaments, ou l'efficacité énergétique de nos bâtiments et industries. Le but de ce chapitre est d'établir plus clairement ce qui relève ou non du machine learning, ainsi que des branches de ce domaine dont ce chapitre traitera. [9]

3.2. Aperçu sur l'apprentissage automatique

Un bref historique dans le domaine d'apprentissage automatique aussi communément appelé (Machine Learning, en anglais), nous amènent à parler des trois grandes époques de l'ordinateur, plus précisément, au tout début de l'informatique, de son évolution, au fil du temps et enfin au monde d'aujourd'hui et de demain.

De nos jours, nous pouvons constater et ce n'est qu'un point de vue, que l'évolution de l'informatique s'est faite principalement sur deux axes :

- Gain en capacité à cumuler de l'information et à sa diffusion dans des domaines tels que les fouilles de données (Data Mining), les entrepôts de données, les réseaux et services web, sans oublié leurs applications sous-jacentes sous Smartphones.
- Gain en intelligence des systèmes informatique, en particuliers, les domaines liés à l'intelligence artificielle

La discipline de l'apprentissage automatique (AA) possède de riches fondements théoriques. On sait, désormais, répondre à des questions comme :

- Quelles méthodes d'apprentissage sont les plus efficaces pour résoudre tel ou tel types de problèmes ?
- Combien d'exemples d'entraînement faut-il fournir à un programme d'apprentissage pour être certain qu'il apprenne avec une efficacité donnée ? [10]

3.3 Définition du machine learning

Qu'est-ce qu'apprendre, comment apprend-on, et que cela signifie-t-il pour une machine ? La question de l'apprentissage fascine les spécialistes de l'informatique et des mathématiques tout autant que neurologues, pédagogues, philosophes ou artistes.

- *Une définition qui s'applique à un programme informatique comme à un robot, un animal de compagnie ou un être humain est celle proposée par Fabien Benureau (2015) : « L'apprentissage est une modification d'un comportement sur la base d'une expérience ».*
- *Dans le cas d'un programme informatique, qui est celui qui nous intéresse dans ce chapitre, on parle d'apprentissage automatique, ou machine learning, quand ce programme a la capacité d'apprendre sans que cette modification ne soit explicitement programmée.*
- ***L'apprentissage automatique** (en anglais Machine Learning) est un type d'intelligence artificielle qui confère aux ordinateurs la capacité d'apprendre sans être explicitement programmés. Il consiste à la mise en place d'algorithmes ayant pour objectif d'obtenir **une analyse prédictive** à partir de données, dans un but précis.* [11]

Exemple

Supposons qu'une entreprise veuille connaître le montant total dépensé par un client ou une cliente à partir de ses factures. Il suffit d'appliquer un algorithme classique, à savoir une simple addition : un algorithme d'apprentissage n'est pas nécessaire. Supposons maintenant que l'on veuille utiliser ces factures pour déterminer quels produits le client est le plus susceptible d'acheter dans un mois. Bien que cela soit vraisemblablement lié, nous n'avons manifestement pas toutes les informations nécessaires pour ce faire. Cependant, si nous disposons de l'historique d'achat d'un grand nombre d'individus, il devient possible d'utiliser un algorithme de machine learning pour qu'il en tire un modèle prédictif nous permettant d'apporter une réponse à notre question. [12]

3.4 Ingrédients de la machine learning

Le machine learning repose sur deux piliers fondamentaux :

- ✓ d'une part, les données, qui sont les exemples à partir duquel l'algorithme va apprendre
- ✓ d'autre part, l'algorithme d'apprentissage, qui est la procédure que l'on fait tourner sur ces données pour produire un modèle. On appelle entraînement le fait de faire tourner un algorithme d'apprentissage sur un jeu de données.

Ces deux piliers sont aussi importants l'un que l'autre. D'une part, aucun algorithme d'apprentissage ne pourra créer un bon modèle à partir de données qui ne sont pas pertinentes c'est le concept garbage in, garbage out qui stipule qu'un algorithme d'apprentissage auquel on fournit des données de mauvaise qualité ne pourra rien en faire d'autre que des prédictions de mauvaise qualité. D'autre part, un modèle appris avec un algorithme inadapté sur des données pertinentes ne pourra pas être de bonne qualité.

Remarque

Bien que l'usage soit souvent d'appeler les deux du même nom, il faut distinguer l'algorithme d'apprentissage automatique du modèle appris : le premier utilise les données pour produire le second, qui peut ensuite être appliqué comme un programme classique.

Un algorithme d'apprentissage permet donc de modéliser un phénomène à partir d'exemples. Nous considérons ici qu'il faut pour ce faire définir et optimiser un objectif. Il peut par exemple s'agir de minimiser le nombre d'erreurs faites par le modèle sur les exemples d'apprentissage.

Quelques exemples :

- ➢ Un vendeur en ligne peut chercher à modéliser des types représentatifs de clientèle, à partir des transactions passées, en maximisant la proximité entre clients et clientes affectés à un même type.
- ➢ Une compagnie automobile peut chercher à modéliser la trajectoire d'un véhicule dans son environnement, à partir d'enregistrements vidéo de voitures, en minimisant le nombre d'accidents
- ➢ Des chercheurs en génétique peuvent vouloir modéliser l'impact d'une mutation sur une maladie, à partir de données patient, en maximisant la cohérence de leur modèle avec les connaissances de l'état de l'art
- ➢ Une banque peut vouloir modéliser les comportements à risque, à partir de son historique, en maximisant le taux de détection de non solvabilité. [11]

Chapitre 3 : Machine learning (Apprentissage Automatique)

L'intelligence artificielle et le machine learning

Le machine learning peut être vu comme une branche de l'intelligence artificielle. En effet, un système incapable d'apprendre peut difficilement être considéré comme intelligent. La capacité à apprendre et à tirer parti de ses expériences est en effet essentielle à un système conçu pour s'adapter à un environnement changeant. L'intelligence artificielle, définie comme l'ensemble des techniques mises en œuvre afin de construire des machines capables de faire preuve d'un comportement que l'on peut qualifier d'intelligent, fait aussi appel aux sciences cognitives, à la neurobiologie, à la logique, à l'électronique, à l'ingénierie et bien plus encore.

Pourquoi utiliser l'apprentissage automatique ?

Le machine learning peut servir à résoudre des problèmes que l'on ne sait pas résoudre (comme dans l'exemple de la prédiction d'achats ci-dessus), que l'on sait résoudre, mais dont on ne sait formaliser en termes algorithmiques comment nous les résolvons (c'est le cas par exemple de la reconnaissance d'images ou de la compréhension du langage naturel), que l'on sait résoudre, mais avec des procédures beaucoup trop gourmandes en ressources informatiques (c'est le cas par exemple de la prédiction d'interactions entre molécules de grande taille, pour lesquelles les simulations sont très lourdes).

Le machine learning est donc utilisé quand les données sont abondantes (relativement), mais les connaissances peu accessibles ou peu développées. Ainsi, le machine learning peut aussi aider les humains à apprendre : les modèles créés par des algorithmes d'apprentissage peuvent révéler l'importance relative de certaines informations ou la façon dont elles interagissent entre elles pour résoudre un problème particulier. Dans l'exemple de la prédiction d'achats, comprendre le modèle peut nous permettre d'analyser quelles caractéristiques des achats passés permettent de prédire ceux à venir. Cet aspect de la machine learning est très utilisé dans la recherche scientifique : quels gènes sont impliqués dans le développement d'un certain type de tumeur, et comment ? Quelles régions d'une image cérébrale permettent de prédire un comportement ? Quelles caractéristiques d'une molécule en font un bon médicament pour une indication particulière ? Quels aspects d'une image de télescope permettent d'y identifier un objet astronomique particulier ? [10]

3.5 Types d'apprentissage :

Les algorithmes d'apprentissage peuvent se caractériser selon le mode d'apprentissage qu'ils emploient :

3.5.1 Apprentissage supervisé :

- Dans ce type d'apprentissage, on cherche à définir une règle de prédiction $R : \mathcal{X} \rightarrow \mathcal{Y}$ d'un variable à prédire Y en fonction de variables prédictives X. On dispose pour cela de données pour lesquelles à la fois X et Y sont observés et on cherche, parmi une famille de règles possibles, celle qui optimise un critère de qualité à définir. Le but est ensuite de pouvoir appliquer $\mathscr{R}$ à de nouvelles données pour lesquelles seules X est connu afin d'en déduire une prédiction $Ypred = (X)$.
- On dispose d'un ensemble d'objets et pour chaque objet une valeur cible associée, il faut apprendre un modèle capable de prédire la bonne valeur cible d'un objet nouveau.

Il existe deux types de sous-problèmes en apprentissage supervisé numérique :

- Régression : lorsque la valeur cible à prédire est continue.
- Classement, classification ou catégorisation : lorsque la valeur cible à prédire est discrète.

Exemple : un diagnostic médical est une règle d'apprentissage supervisé (X sont les symptômes, Y le diagnostic).

Parmi les méthodes d'apprentissage supervisé on trouve :

3.5.1.1 Les arbres de décision :

Les arbres de décision, un moyen **d'apprentissage supervisé** qui permet de séparer des individus dans des groupes selon des règles ou de prévoir la valeur d'une variable (cible) à partir de variables en entrée.

Un arbre de décision est composé de :

- ✓ Un ensemble de nœuds internes : un nœud interne correspond à un test sur un attribut.
- ✓ Un ensemble de branches : une branche correspond à un résultat d'un test (la valeur de l'attribut).
- ✓ Un ensemble de Feuilles : une feuille correspond à une classe ou bien à une valeur de la variable cible.

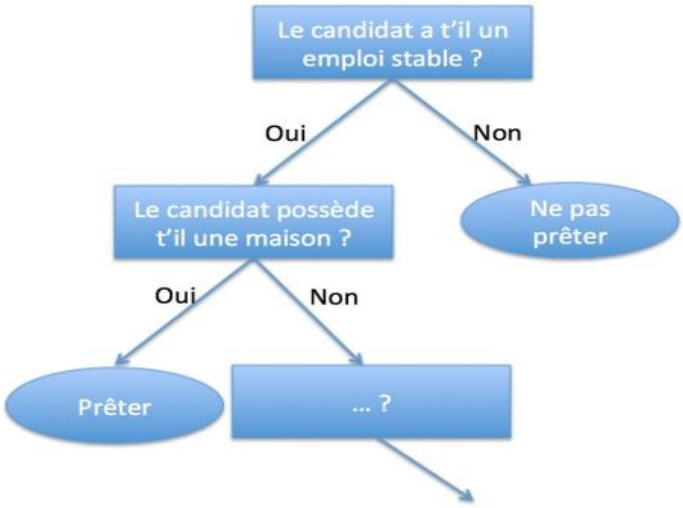


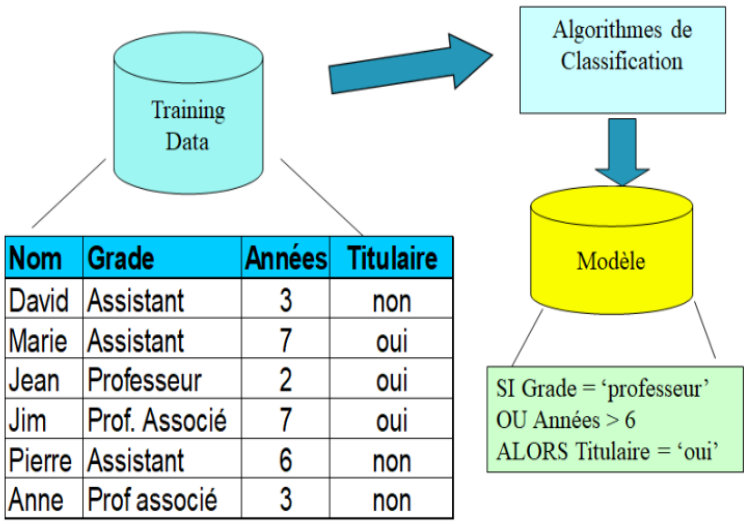
Figure 1.1: Exemple d'arbre de décision. [11]

Le fonctionnement de la classification par arbre de décision se décompose en deux phases :

1. la **phase d'apprentissage**
2. la **phase de classification**

1. La phase d'apprentissage.

Dans cette phase, les approches de classification utilisent un jeu d'apprentissage (Training Data) dans lequel tous les objets sont déjà associés aux classes de références connues. L'algorithme de classification apprend du jeu d'apprentissage et construit un modèle.



Nom	Grade	Années	Titulaire
David	Assistant	3	non
Marie	Assistant	7	oui
Jean	Professeur	2	oui
Jim	Prof. Associé	7	oui
Pierre	Assistant	6	non
Anne	Prof associé	3	non

Figure 3.2: Exemple de phase d'apprentissage.

2. La phase de classification

Consiste à :

1) Tester le modèle appris (arbre générer) sur un échantillon d'instances classées (jeu de teste).

2) Appliquer le modèle sur des instances non classées.

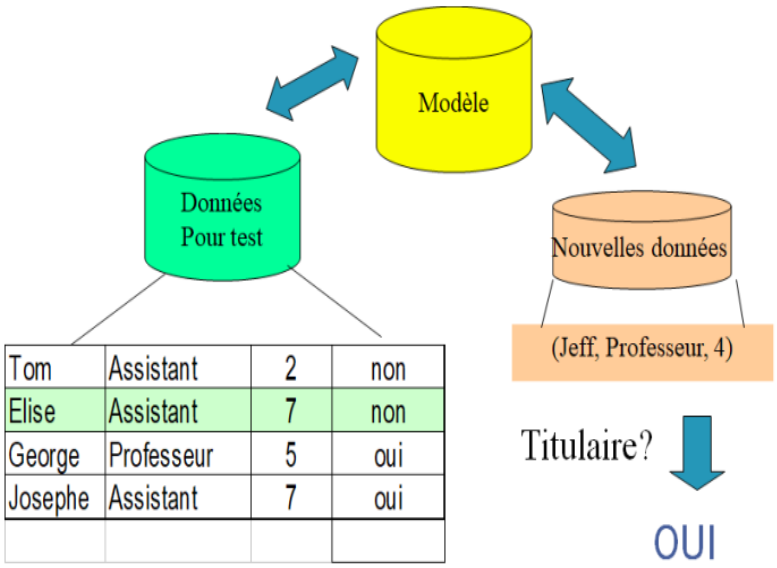


Figure 3.3: Exemple de phase de classification.

3.5.2 Apprentissage non supervisé :

- Dans ce second type d'apprentissage, on dispose de variables observées X dont on souhaite apprendre une caractéristique structurelle. Le but n'est alors pas de prédire une autre variable Y mais une caractéristique inconnue de la matrice X. La famille la plus couramment utilisée d'algorithmes d'apprentissage supervisé est celle des algorithmes de classification (clustering) dont le but est de créer des groupes d'individus rassemblés sur la base de la proximité de leurs valeurs de X.
- on dispose d'un ensemble d'objets sans aucune valeur cible associée, il faut apprendre un modèle capable d'extraire les régularités présentes au sein des objets pour mieux visualiser ou appréhender la structure de l'ensemble des données.

Exemple : Identifier des groupes de documents ayant un sujet similaire, sans les avoir au préalable étiquetés par sujet. Cela permet d'organiser de larges banques de textes.

3.5.3 Apprentissage semi-supervisé :

On dispose d'un petit ensemble d'objets avec pour chacun une valeur cible associée et d'un plus grand ensemble d'objets sans valeur cible ; il faut tirer profit à la fois des données avec et sans valeurs cibles pour résoudre des tâches d'apprentissage supervisé ou non-supervisé.

3.5.4 Apprentissage par renforcement :

On dispose d'un ensemble de séquences de décisions (politiques ou stratégiques) dans un environnement dynamique, et pour chaque action de chaque séquence une valeur de récompense (la valeur de récompense de la séquence est alors la somme des valeurs des récompenses des actions qu'elle met en œuvre) ; il faut apprendre un modèle capable de prédire la meilleure décision à prendre étant donné un état de l'environnement. [10]

3.6 Quelques exemples d'application.

Exemples de problèmes de régression :

- Prédiction du montant des ventes d'une entreprise compte tenu du contexte économique. Prédiction du prix de vente d'une maison en fonction de plusieurs critères.
- Prédiction de la consommation électrique dans une ville étant donnée des conditions météorologiques. . .

Exemples de problèmes de catégorisation :

- Prédiction de l'état sain/malade d'un patient par rapport à une maladie et compte tenu de différents facteurs.
- Prédiction de l'accord ou du refus d'un crédit à un client d'une banque en fonction de ses caractéristiques.

Prédiction du chiffre correct à partir d'une image scannée d'un chiffre écrit à la main. [11]

3.7 Conclusion

Nous avons défini dans ce chapitre la notion de L'apprentissage automatique (en anglais machine learning) ou apprentissage statistique est un champ d'étude de l'intelligence artificielle qui se fonde sur des approches statistiques pour donner aux ordinateurs la capacité d'apprendre à partir de données, c'est-à-dire d'améliorer leurs performances à résoudre des tâches sans être

explicitement programmés pour chacune. Plus largement, cela concerne la conception, l'analyse, le développement et l'implémentation de telles méthodes..

Chapitre 4 : Systèmes de détection d'intrusion de l'IoT basés sur le machine learning

4.1 Obtention des données

La première étape est l'obtention des données. Lors de la phase d'apprentissage, ces informations permettent de connaître les habitudes des utilisateurs ou les différents types d'attaques de manière générale. Lors de la phase d'exécution, ils permettent de détecter une attaque. Néanmoins, la question est de savoir s'il existe une mesure de la quantité de données nécessaire pour avoir un modèle correct, c'est-à-dire qui respecte un certain taux d'erreur accepté. Cette question est encore ouverte à ce jour. Toutefois, le choix des informations à prendre en compte dépendra du type d'apprentissage. [12]

4.2 Supervisé ou non supervisé

Les apprentissages supervisés utilisent généralement des datasets représentant des attaques connues.

Les apprentissages non supervisés se basent uniquement sur les comportements des utilisateurs pour détecter une variation par rapport aux comportements normaux qui représentent une attaque.

Les algorithmes supervisés réalisent d'excellents résultats pour des intrusions connues, ils sont meilleurs que les algorithmes non supervisés. Inversement, pour des agressions inconnues, les algorithmes supervisés voient une réduction drastique de leur efficacité contrairement aux algorithmes non supervisés. Ceci peut s'expliquer par le fait que, puisque les algorithmes non supervisés ne font que partitionner des données, les attaques leur sont toujours inconnues. En e et, étant donné que ces derniers ne font que regrouper des données proches, ils ne savent pas quand elles représentent une attaque. Bien que les algorithmes supervisés et non supervisés obtiennent des résultats semblables pour des attaques inconnues, les modèles non supervisés sont préférés pour leur robustesse.

En effet, ceux-ci ne changent pas drastiquement leur taux de réussite selon que l'intrusion est connue ou non. De plus, ils n'ont pas d'oracle leur disant à quelle classe appartient telle donnée. Ils réalisent solitairement les classes. Ils sont donc plus indépendants que les

techniques supervisées qui ont besoin d'un oracle. Leur point fort est la classification d'attaques appartenant à un label inconnu. En effet, on ne doit pas leur présenter l'ensemble des labels. De plus, il est parfois très dur de classifier univoquement une information dans une classe. C'est pourquoi cette méthode est parfois préférée pour les IDS.

4.3 Hypothèse

Dans le cas des algorithmes supervisés, une hypothèse difficile à respecter lors de l'apprentissage est qu'il n'y a pas d'attaque contenue dans les informations modélisant le comportement normal des programmes qui peuvent pourtant avoir beaucoup d'irrégularités. En effet, dans le cas con- traire, on insérerait des propriétés d'une attaque comme comportement normal. Par conséquent, cette dernière ne sera pas détectée.

Inversement, comme précisé dans ce chapitre, un algorithme non supervisé peut lever cette hypothèse en nettoyant les données pour enlever les informations d'attaque. Pour cela, on recherche un ensemble d'enchaînement, appelé motif, de système call fortement présent dans le système et on les range suivant leur dangerosité d'attaquer le système. Par après, on regarde l'ensemble des séquences des systèmes calls présentes pour les comparer aux motifs découverts précédemment, réalisant ainsi une sorte d'empreinte des différentes séquences de système calls par rapport aux motifs qu'ils contiennent. Par après, on regarde la distance de toutes les empreintes par rapport à une autre a n d'avoir un graphique unique pour l'ensemble. Ceci nous permet de mieux visualiser celles de même nature (qui sont donc très proches les unes des autres) par rapport à celles très différentes. Ainsi, un espacement très grand entre deux groupes d'empreintes où l'un en contient beaucoup et l'autre très peu permet de supposer que l'un en est une attaque alors que l'autre ne l'est pas. De plus, comme on suppose qu'il y a moins d'empreintes d'attaques que de non-attaques, on retrouve facilement l'ensemble de celles d'attaques. C'est pourquoi on utilise un algorithme non supervisé offline pour détecter les anomalies dans les données.

Par après, un algorithme supervisé peut utiliser ces données nettoyées pour concevoir et implémenter le modèle.

4.4 Implémentation

Une méthode généralement utilisée, qui est basée sur l'approche comportementale, est la prise d'empreintes des utilisateurs, c'est-à-dire de leur comportement, et de regarder quand elle ne lui correspond pas sur le système. Ainsi, on peut détecter un comportement anormal et donc une attaque éventuelle. Inversement, on peut prendre l'empreinte de certains pirates connus pour les détecter. Cette dernière peut être apprise par le machine learning.

Toutefois, une autre méthode, basée sur l'approche par scénario, est l'utilisation de données représentant des attaques. Pour que cela soit réaliste, il faut que l'IDS soit suffisamment rapide, efficace et flexible aux petits changements normaux des utilisateurs, sans toutefois permettre de dévier vers une situation d'attaque. Dans le cas contraire, soit elle ne sera pas détectée soit le nombre de faux positifs pourrait exponentiellement augmenter. De manière globale, on réalise un tel IDS en trois étapes.

On modélise tous les comportements normaux de chaque utilisateur ou les signatures des attaques, on le donne au machine learning pour qu'il l'apprenne et ensuite on regarde si le comportement dévie de l'habituel ou s'approche d'une situation offensive.

Dans certains cas, il est intéressant de savoir le type de l'attaque et non seulement si elle a eu lieu. Pour cela, on peut demander au réseau neuronal de nous donner par exemple [0,0,0] s'il n'y a pas d'attaque, [0,0,1] s'il y a une attaque de type 1, [0,1,0] s'il y a une attaque de type 2 et [1,0,0] s'il y a une attaque de type 3. Si le réseau nous donne [0,1,1] on peut vérifier si il y a eu deux attaques simultanées ou si le réseau n'a pas réussi à déterminer correctement ce qui s'est passé.

Une dernière implémentation est la gestion d'un grand nombre d'alertes venant des IDS par du machine learning. Ainsi, cette méthode est une sorte de filtre de ces dernières permettant de se focaliser sur les alarmes les plus importantes.

En effet, un IDS peut générer un nombre volumineux de fausses alertes, ce qui rend la tâche des administrateurs système impossible. Ceci est donc un complément aux IDS et non un remplacement de ceux-ci. Comme vu précédemment, il existe des NIDS et des HIDS.

HIDS Pour modéliser le comportement d'un utilisateur, on peut regarder l'ensemble des commandes qu'il a utilisées durant une période, comme ce qui a été fait dans l'article [12],

ce qui donne un HIDS offline. Cette méthode est justifiable puisque la plupart des personnes n'utilisent pas le système dans le même but ni de la même manière.

Pour un HIDS semblable mais online, la machine apprend à reconnaître les commandes futures selon les k dernières utilisées.

Néanmoins, leur ordre n'est pas révélateur pour savoir si une attaque a lieu ou pas. Il semble plus significatif de regarder l'ensemble des commandes utilisées durant une période. L'inconvénient majeur est la non-prise en compte des arguments des system calls.

Ainsi, il est intéressant de prendre en compte les valeurs de retour, les statuts d'erreur et d'autres arguments pour détecter des attaques.

En effet, prenons l'exemple des system calls suivants exécutés par un simple utilisateur : open, read, write. Ces trois systèmes calls peuvent sembler inoffensifs puisque c'est une simple ouverture, lecture et écriture dans un chier. Néanmoins, la situation change si on regarde l'argument de ces system calls et que celui-ci est le chier passade. Une autre méthode est l'apprentissage des programmes et non des utilisateurs. Ainsi, la machine apprend le fonctionnement normal des logiciels sur une machine.

NIDS Pour ce qui est du NIDS, il est nécessaire de bien comprendre l'ensemble des variables d'un paquet, ainsi que du protocole, pour comprendre le fonctionnement normal du système. Essayons de partitionner les paquets TCP 8 . Pour cela, on peut d'abord voir les attributs qui ne changeront sans doute jamais entre ceux-ci : Version du protocole + les arguments réservés. D'autres attributs permettent de les partitionner : adresse source/destination + protocole utilisé.

Ces deux propriétés sont généralement utilisées par les rewalls pour filtrer les paquets. Enfin, certains attributs pourraient être différents dans une même partition : taille du header, identificateur, TTL,. . . Ce sont ceux qui sont généralement utilisés pour détecter une anomalie, regarder les valeurs de ces attributs pour déterminer une anomalie n'est pas une bonne manière de faire.

Ainsi, on regarde la moyenne de certaines valeurs, le pourcentage d'événements selon la valeur d'un attribut, le pourcentage de paquets ayant telle valeur.

Il faut donc s'assurer d'avoir suffisamment de paquets lors de la phase d'apprentissage pour garantir qu'aucun comportement normal non présent dans ces paquets ne soit oublié. [13]

4.5 Problématiques des modèles

- **Non périodicité** :

La non-périodicité de certains phénomènes peut avoir des répercussions problématiques. Prenons l'exemple de la rédaction d'un mémoire. Il y a une période où l'étudiant réalise beaucoup de recherches et une autre période où l'étudiant écrit son mémoire. Durant ces deux phases, c'est toujours le même étudiant qui travaille sur la même machine. Néanmoins, les demandes de ressources ne sont pas égales, ce qui pourrait faire croire à la machine learning qu'il y a quelque chose d'inhabituel. Semblablement, une augmentation de fréquentation sur un site web ne signifie pas pour autant une attaque contre ce site web. Réaliser un détecteur d'intrusion qui ralentirait cette augmentation aurait une conséquence négative. Pour contrer ce problème, il est conseillé de mélanger un grand nombre de paramètres pour réaliser le profil de l'utilisateur et de donner la possibilité à l'administrateur de considérer si c'est un cas non voulu.

- **Espacement des attaques** :

Une attaque difficilement visible est une attaque réalisée en un temps très espacé. Pour les contrer.

4.6 Optimisation

Il y a une forte volonté de réduire le temps d'apprentissage pour pouvoir mettre en œuvre une solution commerciale. Propose une manière de réduire le temps d'apprentissage ainsi que la taille de la structure. Pour être encore plus performant, on peut définir la structure de l'ensemble des réseaux neuronaux utilisés dans l'IDS. En voici quelques-unes :

Une première boîte contenant un filtre d'information suivie par une autre contenant le réseau neuronal.

Une première boîte contenant un filtre d'information suivie par n boites de réseaux neuronaux suivies par une dernière qui va jouer le rôle d'arbitre en déterminant ce qui se passe sur le réseau selon les informations reçues par les n boîtes de réseaux neuronaux. Chacune d'entre elles reconnaît un type d'attaque (DOS, U2R, R2L, scan,. . .). Ceci est aussi appelé la méthode Boo Sting.

Trois premières boîtes suivies d'une dernière. L'entraînement se fait ainsi :

On entraîne la première boîte avec un certain nombre d'informations. On prend au hasard des nouvelles informations et on entraîne une deuxième. - On prend des nouvelles informations et on regarde la réaction des deux premières. Si ces deux boîtes ne convergent pas vers la même idée, on prend cette information et on la met comme entraînement pour la troisième. [11]

4.7 Conclusion

Dans ce chapitre, nous avons présentés les différentes techniques utilisées pour la détecter d'intrusions des IoD basées sur le machine learning, en se basant sur les méthodes d'implémentation et approches d'utilisations.

Chapitre 4 : Systèmes de détection d'intrusion pour les IOT basés sur le machine learning

Chapitre 5 : Conception et réalisation

5.1 Introduction

Ces dernières années, la diffusion des appareils IoT dans le monde a progressé rapidement. Les objets connectés sont désormais déployés dans tous les domaines tels que la santé, les villes intelligentes, l'éducation, etc. Pour intégrer ce flux de commercialisation rapide, peu d'attention a été accordée à la sûreté et à la sécurité des appareils et des réseaux IoT qui mettent en danger les utilisateurs IoT et à leur tour perturbe l'ensemble de l'écosystème connecté à Internet, y compris les sites Web, les applications, les réseaux sociaux et les serveurs. De plus, les vecteurs d'attaques de sécurité ont évolué dans les deux sens, en termes de complexité et de diversité. Par conséquent, une plus grande attention doit être accordée à l'analyse de ces attaques, à leur détection, ainsi qu'à la prévention des infections et à la récupération du système après les attaques.

Dans cette thèse, nous avons étudié et proposé un système de détection et de prévention des intrusions (IDPS) basé sur le Machine Learning (ML) pour l'écosystème IoT afin de détecter et de répondre immédiatement aux menaces potentielles dès qu'elles se produisent. Il représente un cadre cohérent avec un workflow de sécurité complet, de la collecte de données à détection des menaces et activation des actions appropriées.

5.2 Environnement d’exécution

5.2.1 L’éditeur choisi :

PyCharm Community Edition 2021.1.1

Pycharm est un environnement de développement intégré utilisé pour programmer en Python. Il permet l'analyse de code et contient un débogueur graphique. Il permet également la gestion des tests unitaires, l'intégration de logiciel de gestion de versions, et supporte le développement web avec Django.

Développé par l'entreprise tchèque JetBrains, c'est un logiciel multiplateforme qui fonctionne sous Windows, Mac OS X et Linux. Il est décliné en édition professionnelle, diffusé sous licence propriétaire, et en édition communautaire diffusé sous licence Apache.

PyCharm fournit la saisie automatique de code intelligente, des inspections de code, la mise en évidence d'erreur à la volée et des correctifs rapides, en plus de refacturations de code automatisées et de riches capacités de navigation.

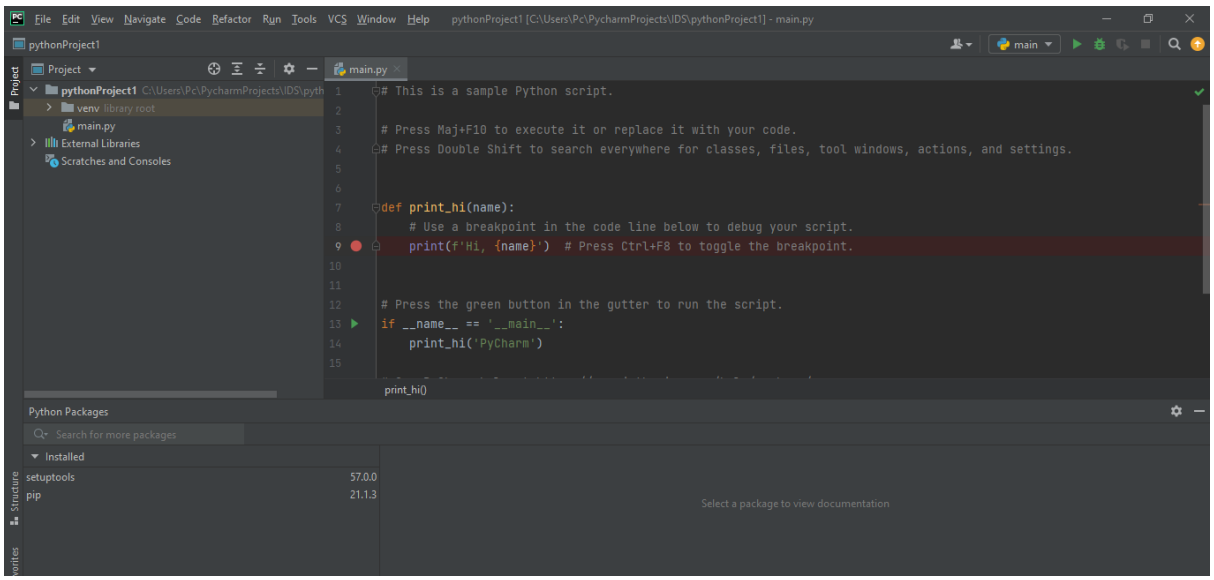


Figure 5.1: PyCharm 2021.1.1.

5.2.2 Le langage de programmation utilisé :

Python 3.8.0 :

Python est un langage de programmation puissant et facile à apprendre. Il dispose de structures de données de haut niveau et permet une approche simple mais efficace de la programmation orientée objet. Parce que sa syntaxe est élégante, que son typage est dynamique et qu'il est interprété, Python est un langage idéal pour l'écriture de scripts et le développement rapide d'applications dans de nombreux domaines et sur la plupart des plateformes.

L'interpréteur Python et sa vaste bibliothèque standard sont disponibles librement, sous forme de sources ou de binaires, pour toutes les plateformes majeures depuis le site Internet https://www.python.org/ et peuvent être librement redistribués. Ce même site distribue et pointe vers des modules, des programmes et des outils tiers. Enfin, il constitue une source de documentation.

5.3 Dataset

L'ensemble de données d'intrusion choisi pour cette étude c'est IOT-2019 data-set, fourni par laboratoire de recherche sur le piratage et les contre-mesures (HCR Lab) de Corée du Sud [17], Les divers types d'attaques réseau ont été créés dans l'environnement Internet des objets (IoT) à des fins académiques. Deux appareils domestiques intelligents typiques - SKT NUGU (NU

100) et caméra Wi-Fi EZVIZ (C2C Mini O Plus 1080P) - ont été utilisés. Tous les appareils, y compris certains ordinateurs portables ou téléphones intelligents, étaient connectés au même réseau sans fil.

L'ensemble de données se compose de 42 fichiers de paquets réseau bruts (pcap) à différents moments.

* Les fichiers de paquets sont capturés en utilisant le mode moniteur de l'adaptateur réseau sans fil.

* Toutes les attaques à l'exception la catégorie Mirai Botnet sont des paquets capturés lors de la simulation d'attaques à l'aide d'outils tels que Nmap. Dans le cas de la catégorie Mirai Botnet, les paquets d'attaque ont été générés sur un ordinateur portable puis manipulés pour le faire apparaître comme s'ils provenaient de l'appareil IoT.

Catégorie	Sous-categorie	Nombre de paquets
Normal	Normal	1756276
Scanning	Host Discovery	2454
Scanning	Port Scanning	20939
Scanning	OS/Version Detection	1817
Man in the Middle (MITM)	ARP Spoofing	101885
Denial of Service (DoS)	SYN Flooding	64646
Mirai Botnet	Host Discovery	673
Mirai Botnet	Telnet Bruteforce	1924
Mirai Botnet	UDP Flooding	949284
Mirai Botnet	ACK Flooding	75632
Mirai Botnet	HTTP Flooding	10464

5.4 Algorithme d'apprentissage pour la détection d'intrusion

Dans cette étude quatre algorithme d'apprentissage sont utilisés

5.4.1 La classification naïve bayésienne (Gaussian Naive Bayes)

```
from sklearn.naive_bayes import GaussianNB
model1 = GaussianNB()
```

5.4.2 Arbre de décision (Decision Tree)

```
from sklearn.tree import DecisionTreeClassifier
model2 = DecisionTreeClassifier(criterion="entropy", max_depth=4)
```

5.4.3 Forêt d'arbres décisionnels (RANDOM FOREST)

```
from sklearn.ensemble import RandomForestClassifier
model3 = RandomForestClassifier(n_estimators=30)
```

5.4.4 Machine à vecteurs de support (SUPPORT VECTOR MACHINE)

```
from sklearn.svm import SVC
model4 = SVC(gamma='scale')
```

5.4.5 Régression logistique (LOGISTIC REGRESSION)

```
from sklearn.linear_model import LogisticRegression
model5 = LogisticRegression(max_iter=1200000)
```

5.5 Résultat et Discussion

5.5.1 Les mesures d'évaluation des modèles

La matrice de confusion est utilisée pour mesurer les performances des algorithmes précédents. Ceci fournit une visualisation de la performance du classificateur sur le jeu de données en entrée. Un certain nombre de mesures de performance différentes, y compris le rappel et la précision, sont dérivées de la matrice de confusion.

La figure 4.1 montre la structure de cette matrice. Les 4 cas possibles sont :

Vrai positif (VP) : une attaque correctement détectée par le test.

Faux positif (FP) : une activité normale détectée comme attaque par le test.

Vrai négatif (VN) : une activité normale correctement détectée par le test.

Faux négatif (FN) : une attaque détectée comme activité normale par le test.

- **TP (True Positives)** : les cas où la prédiction est positive, et où la valeur réelle est effectivement positive. Exemple : le médecin vous annonce que vous êtes malade, et vous êtes malade.
- **TN (True Negatives)** : les cas où la prédiction est négative, et où la valeur réelle est effectivement négative. Exemple : le médecin vous annonce que vous n'êtes pas malade, et vous n'êtes effectivement pas malade.
- **FP (False Positive)** : les cas où la prédiction est positive, mais où la valeur réelle est négative. Exemple : le médecin vous annonce que vous êtes malade, mais vous n'êtes pas malade.
- **FN (False Negative)** : les cas où la prédiction est négative, mais où la valeur réelle est positive. Exemple : le médecin vous annonce que vous n'êtes pas malade, mais vous êtes malade.

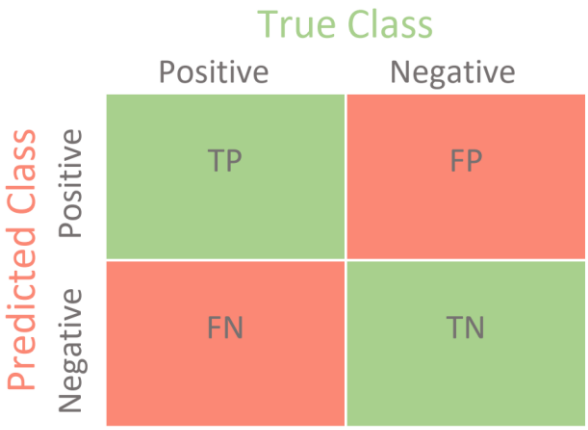


Figure 5.2 – Matrice de confusion.

5.5.1.1 La précision

Cette métrique, également relative à chaque catégorie, renseigne sur la probabilité qu'une prédiction d'une catégorie donnée soit correcte.

Précision = ***TP/(TP+FP)*100%***

5.5.1.2 Le taux de détection (Rappel)

C'est le rapport entre le nombre d'intrusions correctement détectées et le nombre total d'intrusions. Et décrit par la formule :

Rappel =***TP/(TP+FN)*100%***

5.5.1.3 Le taux de faux positif (FP)

Le taux des fausses alertes est calculé comme le rapport entre les nombres de trafic normal qui sont incorrectement classés comme intrusions et le nombre total de trafic normal.

FP=*FP/(TN+FP)*100%*

5.5.1.4 Le taux de réussite (Accuracy)

Nous avons évalué cet algorithme en utilisant le taux de réusite comme métrique de performance. L'exactitude, dans ce cas, représente le taux de précision globale de la classification de l'ensemble de données de testes. Elle traduit le rapport entre les détections correctes et les détections totales obtenues. Elle est donné par :

Accuracy *=(TP+TN)/(TP+TN+FP+FN)*100%*

5.5.1.5 Micro-moyenne (Micro-averaged):

agrégera les contributions de toutes les échantillons pour calculer la métrique moyenne. Afin de montrer comment calculer le micro-moyenne, on prend l'exemple de la table suivante:

	TP	FP	FN	Precision	Number of samples
bird	1	0	1	1	2
cat	4	1	0	0.8	4
dog	2	1	1	0.667	3
TOTAL	7	2	2		

Tableau 5.1 – exemple

La formule suivante calcule le micro-moyenne de la précision

$$\text{Micro-averaged Precision} = \frac{TP_{total}}{TP_{total} + FP_{total}} = \frac{7}{7+2} = 0.7777$$

5.5.1.6 Macro-moyenne (Macro-averaged):

calcule la métrique indépendamment pour chaque classe, puis prend la moyenne (donc toutes les classes sont traitées de manière égale) voir la formule suivante:

$$\text{Macro-averaged Precision} = \frac{1}{3}Precision_{birds} + Precision_{cats} + Precision_{dogs} = \frac{1}{3}(1 + 0.8 + 0.6666) = 0.8222$$

5.5.1.7 Moyenne pondérée (Weighted-averaged):

la contribution de chaque classe à la moyenne est pondérée par sa taille (moyenne pondérée est la moyenne d'un certain nombre de valeurs affectées de coefficients). Cette formule permet de calculer la moyenne pondérée de la précision de l'exemple précédent

$$\text{Weighted-averaged Precision} = \frac{Precision_{birds} * N_{birds} + Precision_{cats} * N_{birds} + Precision_{dogs} * N_{birds}}{\text{Total number of samples}}$$

$$= \frac{1 * 2 + 0.8 * 4 + 0.6666 * 3}{2 + 4 + 3} = 0.8$$

5.5.1.8 F1-score:

combine la précision et le rappel en une seule mesure. Mathématiquement, c'est la moyenne harmonique de la précision et du rappel. Il peut être calculé comme suit :

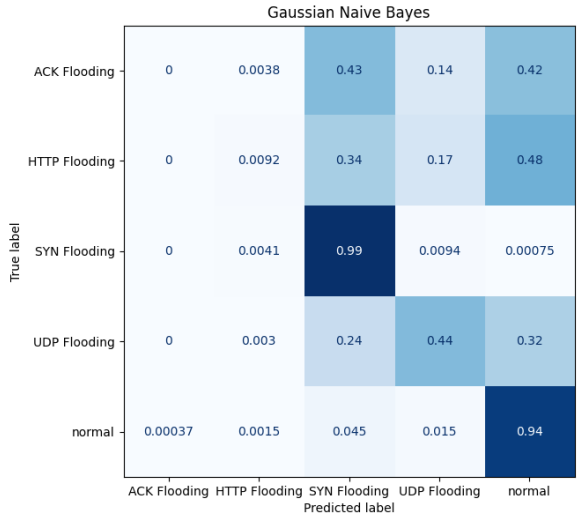
$$F_1\text{−score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = \frac{2\text{TP}}{2\text{TP} + \text{FP} + \text{FN}}$$

5.5.2 Discussion et analyse

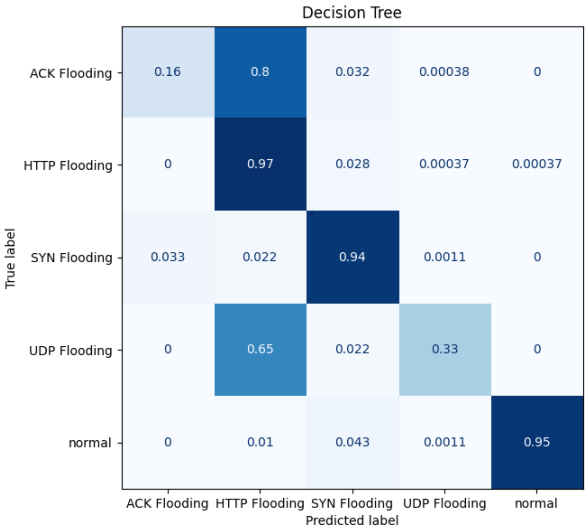
Les modèles de classification naïve bayésienne (NB), Arbre de décision (DT), Forêt d'arbres décisionnels (RF), machine à vecteurs de support (SVM) et régression logistique (LR) ont été testés pour la classification des 4 classes d'attaques avec la classe **normal**. Les tableaux 4.2, 4.3, 4.4, 4.5 et 4.6 donne les résultats obtenus. La meilleure précision obtenue est 82% du modèle arbre de décision. La matrice de confusion normalisée de figure 4.2 ci-dessous montre que la classe **normal** a été bien prédite avec d'autres classes d'attaques qui ont été prédites convenablement. Cependant, certains types d'attaques comme : ACK Flooding et UDP Flooding ont été mal classé, cela signifie que ces attaques ayant des comportements similaires

et partagent certaines propriétés entre eux ce qui rendent la tache de reconnaissance de ces derniers plus difficiles.

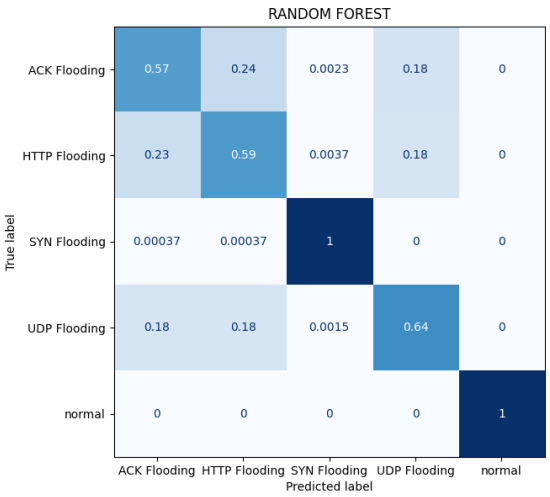
Le taux de réussite (Accuracy) et le temps d'exécution de la phase de teste et d'apprentissage respectivement schématisés dans les figures 4.3 et 4.4 montre que le modèle machine à vecteurs de support a le meilleur taux de réussite et plus grand temps d'exécution.



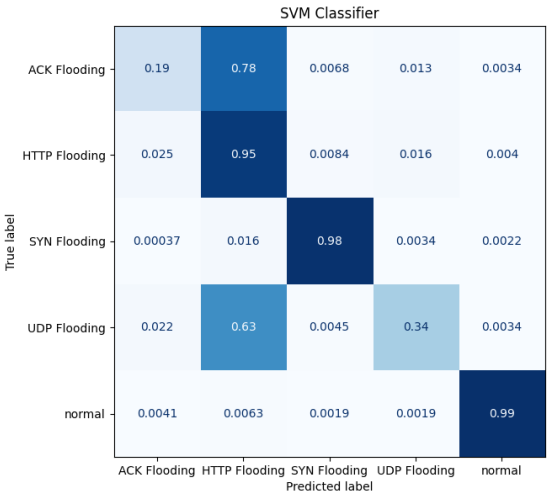
(a)



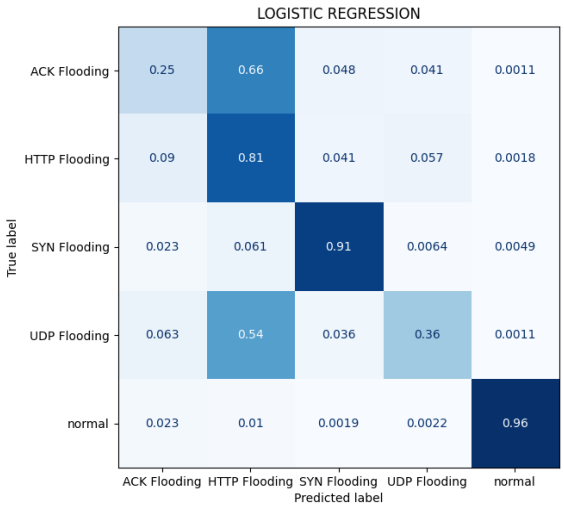
(b)



(c)



(d)



(e)

Figure 4.2 : Matrice de confusion: (a) classification naïve bayésienne (b) Arbre de décision(c) Forêt d'arbres décisionnels (d) Machine à vecteurs de support (d) Régression logistique

	precision	Recall	f1-score
ACK Flooding	0.00	0.00	0.00
HTTP Flooding	0.43	0.01	0.02
SYN Flooding	0.48	0.99	0.65
UDP Flooding	0.57	0.44	0.49
Normal	0.44	0.94	0.59
accuracy			0.47
macro avg	0.38	0.47	0.35
weighted avg	0.38	0.47	0.35

Tableau 4.2 : Le rapport de classification avec la classification naïve bayésienne

	precision	recall	f1-score
ACK Flooding	0.83	0.16	0.27
HTTP Flooding	0.40	0.97	0.57
SYN Flooding	0.88	0.94	0.91
UDP Flooding	0.99	0.33	0.49
normal	1.00	0.95	0.97
accuracy			0.67
macro avg	0.82	0.67	0.64
weighted avg	0.82	0.67	0.65

Tableau 4.3 : Le rapport de classification avec l'**Arbre de décision**

	precision	recall	f1-score
ACK Flooding	0.58	0.57	0.58
HTTP Flooding	0.59	0.59	0.59
SYN Flooding	0.99	1.00	1.00
UDP Flooding	0.64	0.64	0.64
normal	1.00	1.00	1.00
accuracy			0.76
macro avg	0.76	0.76	0.76
weighted avg	0.76	0.76	0.76

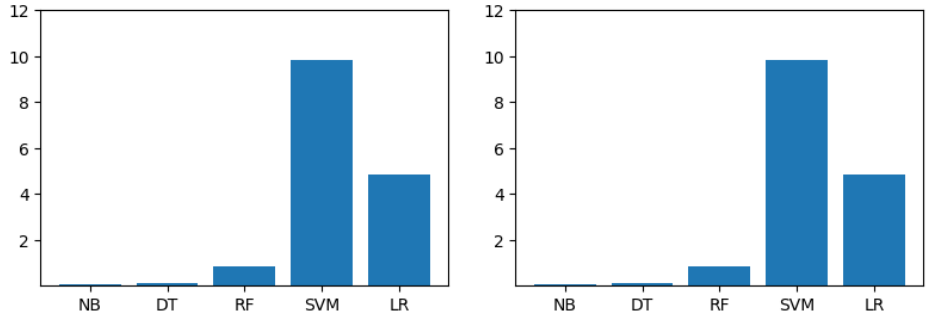
Tableau 4.4 : Le rapport de classification avec la **Forêt d'arbres décisionnels**

	precision	recall	f1-score
ACK Flooding	0.79	0.19	0.31
HTTP Flooding	0.40	0.95	0.57
SYN Flooding	0.98	0.98	0.98
UDP Flooding	0.91	0.34	0.50
normal	0.99	0.99	0.99
accuracy			0.69
macro avg	0.81	0.69	0.67
weighted avg	0.81	0.69	0.67

Tableau 4.5 : Le rapport de classification avec la **Machine à vecteurs de support**

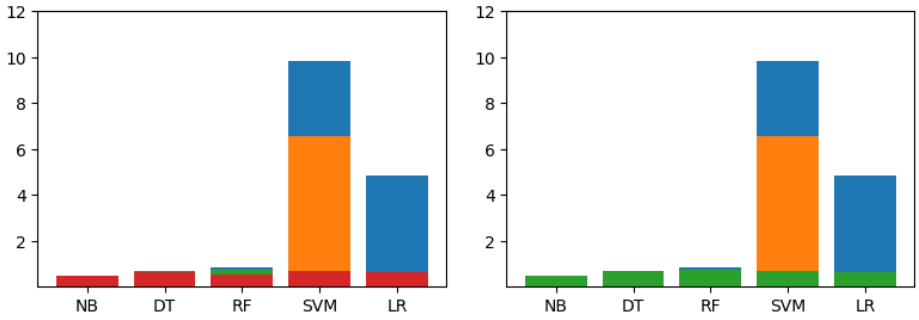
	precision	recall	f1-score
ACK Flooding	0.55	0.25	0.34
HTTP Flooding	0.39	0.81	0.53
SYN Flooding	0.88	0.91	0.89
UDP Flooding	0.77	0.36	0.49
normal	0.99	0.96	0.98
Accuracy			0.66
macro avg	0.72	0.66	0.65
weighted avg	0.72	0.66	0.65

Tableau 4.6 : Le rapport de classification avec la **Régression logistique**



(a) (b)

Figure 5.3 : Le taux de réussite (Accuracy) de (a) la phase de teste (b) la phase d'apprentissage.



(a) (b)

Figure 5.3 : Le temps d'exécution de (a) la phase de teste (b) la phase d'apprentissage.

4.8. Conclusion

Dans ce chapitre, nous avons testé la performance de quelques algorithmes d'apprentissage sur la base IOT-2019 data-set, fourni par laboratoire de recherche sur le piratage et les contre-mesures (HCR Lab) de Corée du Sud. Le taux de réussite obtenu par l'algorithme machine à vecteurs de support en phase d'apprentissage est le meilleur en aux autres comparant au algorithmes, d'autre part, son temps d'exécution est le plus grand.

Conclusion générale

Conclusion générale

Le machines learning est utilisé pour reconnaitre des attaques difficilement représentables via une simple signature ou pour en découvrir des cachées. Pour cela, il faut d'abord obtenir les données qui permettent d'en détecter une.

Dans ce travail, on a télécharger la base de donnees IOT-2019 data-set , cette base de données est composes de 42 paquettes , Pour ouvrir ces packages, nous avons utilisé wireshark

on s'est intéressé aux techniques de détection d'intrusion des internet des objets, nous avons précisé sur la technique de machine Learning ainsi que on a fait la comparaison entre les méthodes de ce dernier. Cette comparaison est basée sur le taux de précisions à la base de données. Nous avons utilises les algorithmes :Gaussian Naive Bayes,algorithme Decision Tree',RANDOM FOREST', SVM Classifier','LOGISTIC REGRESSION ,

Nous avons utilisé Python pour implémenter ces algorithmes, les codes Python sont généralement très simples à lire., python possède une plateforme très active, PyPi, pour le dépôt des librairies (plus de 70000 librairies recensées).

Malgré que la période est courte mais nous avons appris le programme Python et les techniques de détection d'intrusion, on arrive a aussi a utiliser la bibliothèque tkinter pour faire des interfaces graphique.

Liste des références bibliographiques

[1]: yassine haddab, introduction à l'internet des objets, 2014.

[2]: Imed Saleh, Internet of things, Laboratoire Paragraphe, Université Paris8, imad.saleh@univ-paris8.fr, 2017.

[3] : Mekriou Ryma, Mazari Walid, Introduction à l'internet de l'objet et réalisation D'un système domotique, Université de Bejaïa 2016.

[4] : https://www.fondation-mines-telecom.org/wp-content/uploads/2016/01/2011-Linternet-des-objets.

[5] : Tarek ABBES, Doctorat de l'université Henri Poincaré - Nancy 1, Laboratoire Lorrain de Recherche en Informatique et ses Applications, le 14 décembre 2004.

[6] : M. Tran Van Tay, LE SYSTÈME DE DÉTECTION DES INTRUSIONS ET LE SYSTÈME D'EMPÊCHEMENT DES INTRUSIONS (ZERO DAY), Montréal, Février 2005.

[7]: Melle BEN BRAHIM EMBARKA, Melle AMICHE SELYNA, Mise en place d'une solution de détection d'intrusion,2017.

[8]: https://connect.ed-diamond.com/MISC/MISC-072/La-detection-d-intrusion-une-approche-globale

[9] : https://moodle.insa-rouen.fr/course/view.php?id=92.

[10]: Eloïse Berthier, comment les machines apprennent, une introduction au machine learning, vendredi 8 mars 2019.

[11] : Julien Ah-Pine, (julien.ah-pine@univ-lyon2.fr), apprentissage automatique, université lyon 2, 2019/2020

[12] : Chloé-Agathe Azencott, Introduction au Machine Learning, 2003.

[13] : Nadia Chaabouni, Intrusion detection and prevention for IoT systems using machine learning, submitted on 29 sep 2020.

[14] Hyunjae Kang, Dong Hyun Ahn, Gyung Min Lee, Jeong Do Yoo, Kyung Ho Park, Huy Kang Kim, September 27, 2019, "**IoT network intrusion dataset**", IEEE Dataport, doi: https://dx.doi.org/10.21227/q70p-q449

Hyunjae Kang, Dong Hyun Ahn, Gyung Min Lee, Jeong Do Yoo, Kyung Ho Park, and Huy Kang Kim, "IoT Network Intrusion Dataset.", http://ocslab.hksecurity.net/Datasets/iot-network-intrusion-dataset, 2019.