République Algérienne Démocratique

Ministère de l'enseignement supérieur et de la

Recherche scientifique

Université Larbi Tébessi - Tébessa

Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie

Département : Mathématiques et Informatique

Mémoire de fin d'étude

Pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique

Filière : Informatique

Option : Réseaux et sécurité d'information

Thème

Détection des attaques de déni de service par une approche basée Deep learning

Réalisé par :

Mohammed BELGUIDOUM

Devant le jury :

Dr. Mekhaznia T	MCA	Univérsité Larbi Tébessi	Président
Mr. Tag S	MAA	Univérsité Larbi Tébessi	Examinateur
Dr. Souahi MS	MCB	Univérsité Larbi Tébessi	Encadreur

Date de soutenance : 14/06/2022

Résumé

Les attaques par déni de service sont l'une des plus graves en cybersécurité, La diversité de ses attaques et l'utilisation de nombreuses méthodes difficiles à détecter et même à arrêter sont encore aujourd'hui l'une des principales préoccupations de la cybersécurité.

Les méthodes élaborées de détection des attaques par déni de service sont très importantes en cybersécurité pour assurer la sécurité du réseau, Récemment, il a fait l'objet de nombreuses recherches et a utilisé beaucoup d'apprentissage automatique de nombreuses façons pour détecter les attaques par déni de service.

Notre objectif dans ce travail est de modéliser ce système pour aider les administrateurs de cybersécurité à détecter et identifier diverses attaques. Dans ce travail, nous étudions des méthodes d'apprentissage automatique (ML) pour la détection d'intrusion, puis nous appliquons une technique de techniques d'apprentissage profond, Convolution Neural Network (CNN) et il a été testé sur l'ensemble de données de travail CICDDoS2019 composé de plus de 60 millions de trafic et enregistrant 14 types de cyberattaques, nous avons évalué les méthodes proposées en utilisant différentes mesures appliquées pour évaluer les performances de l'apprentissage automatique (précision, recall, score F1) .

Les résultats obtenus montrent que l'apprentissage profond fourni est meilleur que les algorithmes traditionnels d'apprentissage automatique (ML)

Mots clés : Apprentissage automatique, Apprentissage profond, Déni de service, CNN, CICDDoS2019

Abstract

Denial of service attacks are one of the most serious in cybersecurity. The diversity of its attacks and the use of many methods that are difficult to detect and even stop are still today one of the main concerns in cybersecurity.

Elaborate denial-of-service attack detection methods are very important in cybersecurity to ensure network security, recently it has been extensively researched and used a lot of machine learning in many ways to detect denial-of-service attacks. denied service.

Our objective in this work is to model this system to help cybersecurity administrators detect and identify various attacks. In this work, we study machine learning (ML) methods for intrusion detection, then we apply a technique of deep learning techniques, Convolution Neural Network (CNN) and it has been tested on the set of CICDDoS2019 working data consisting of more than 60 million traffic and recording 14 types of cyberattacks, we evaluated the proposed methods using different metrics applied to evaluate machine learning performance (Précision, Recall, F1 score).

The results obtained show that the deep learning provided is better than traditional machine learning (ML) algorithms

Keywords: machine learning, deep learning, denial of service, CNN, CICDDoS2019

ملخص

تعد هجمات رفض الخدمة من اكثر و اخطر الهجمات في الامن السيبراني ، في بكثرة تنوع هجماتها و استخدام اساليب عديدة يصعب اكتشافها و حتى ايقافها فهيا لا تزال ليومنا هذا احد الاهتمامات الرئيسية في الامن السيبراني

فطرق المتعبرة لكتشاف هجمات رفض الخدمة مهمة جدا في الامن السيبراني لضمان امن الشبكة . في الاونة الاخيرة كانت موضعا للكثير من الابحاث و استخدام الكثير من تعلم الالة بطرق كثيرة لكتشاف هجمات رفض الخدمة

هدفنا من هذا العمل هو نمذجة هذا النظام لمساعدة المسؤولين عن الامن السيبراني لكتشاف و تحدد الهجمات المتنوعة ، في هذا العمل قمنا بدراسة طرق تعلم الالة (ML) لكشف التسلل بعدها طبقنا تقنية من تقنيات التعلم العميق ، شبكة عصبية تلافيفية (CNN) و تم اختباره على مجموعة بيانات CICDDoS2019 التي تم العمل عليها و المتكونة من اكثر من 60 مليون حركة مرور ، و سجلت 14 نوع من الهجمات السبرانية ، لقد قمنا بتقييم الطرق المقترحة باستخدام مقاييس مختلفة مطبقة لتقييم اداء التعلم الالي (الدقة ، الاسترجاع ، درجة F1)

تظهر النتائج المتحصل عليها ان تعلم العميق المقدم افضل من خوارزميات تعلم الالة التقليدية (ML) ان النموذج المقترح كشف بدقة عالية ومعدل الكشف علي الدقة و معدل الخسارة منخفضة

الكلمات الرئيسية: تعلم الالة ،التعلم العميق ، رفض الخدمة ، CNN ، CICDDoS2019

.

Dédicace

Je remercie Allah de m'avoir donné le courage pour accomplir ce modeste travail que je dédie :

À mes très chers parents,

Aucune dédicace ne peut exprimer l'amour, l'appréciation, le dévouement et le respect que j'ai toujours pour vous, Ce travail est le fruit des sacrifices que vous avez consentis pour m'enseigner au fil des années, je vous en suis reconnaissant toute ma vie.

A ma belle sœur

Lorsque la mer représentait ma tristesse tu m'as appris à nager

A mes chers frères,

Je leur souhaite du succès dans leur vie personnelle et académique.

A Mes chers amis :

Merci pour tous les souvenirs intemporels dans nos cœurs, je les remercie pour leur soutien et pour m'avoir accompagné.

Remerciements

Nous remercions en premier lieu au DIEU pour nous avoir donné la force de réaliser ce travail.

Aussi mes remerciements les plus sincères aux personnes qui m'ont apporté leur aide et qui ont contribué à l'élaboration de ce travail ainsi qu'à la réussite de cette formidable année académique.

Je remercie également Monsieur Souahi Mohamed Salah pour sa générosité et la grande patience dont elle a fait preuve malgré ses responsabilités professionnelles.

Nous remercions également tous les membres du jury d'avoir accepté à participer à l'évaluation de notre travail.

Nous aimerons exprimer aussi à toute l'équipe pédagogique et administrative du master académique en Informatique spécialité :

Administration et sécurité des réseaux.

Enfin, j'adresse mes plus sincères remerciements à tous mes proches et amis, qui m'ont toujours soutenue et encouragée au cours de la réalisation de ce mémoire.

Liste des tableaux

Liste des figures

Table des matières

Introduction Générale

Aujourd'hui, nous vivons la période de la technologie et l'Internet est la base des nations et de la civilisation. Aujourd'hui, l'Internet est essentiel pour apprendre, travailler ou communiquer par messagerie instantanée et de nombreuses autres technologies émergentes telles que les véhicules autonomes avec la conduite à distance, la vente de machines et d'autres technologies de l'information. La diffusion de tous ces outils d'information dans le monde a créé de nouvelles lacunes en matière de sécurité.

L'évolution des réseaux d'information dans le monde a fait face à des menaces réelles, délibérées ou accidentelles. Nous n'avons presque pas une journée sans publier une histoire de piratage, d'atteinte à la vie privée, d'espionnage, de fraude et de cybersécurité. Il y a un certain nombre de défis et de menaces en matière de cybersécurité que la cybersécurité doit aborder et mettre fin récemment, du 15 au 16 février 2022, à la guerre de Ruissa. L'Ukraine a été victime d'une attaque par déni de service contre toutes les institutions militaires et financières en Ukraine dans laquelle les pirates russes ont continué d'attaquer les sources d'information ukrainiennes sans s'arrêter, inondant les serveurs ukrainiens de trafic. C'est un défi de cybersécurité.

Les attaques par déni de service sont l'un des risques les plus dangereux pour la sécurité de Serani. Les attaques par déni de service sont des attaques caractérisées par leur diversité d'attaques pour noyer

La problématique

Avec le développement du monde et l'impératif de construire l'infrastructure des technologies de l'information dans le monde entier. Les systèmes de détection d'intrusion sont confrontés à de nombreux défis nécessaires pour protéger les systèmes, Le système doit améliorer le taux de détection d'attaque correct, améliorer le temps et le type de détection d'attaque et réduire le taux de fausses alarmes

Le but de travail

Notre objectif dans cette étude est d'aider à améliorer les systèmes de détection d'intrusion dans le sens où les administrateurs réseau, en particulier les administrateurs de cybersécurité des systèmes de détection d'intrusion, améliorent la détection et la détection de nombreux types d'attaques par déni de service, et il est donc généralement nécessaire mettre en œuvre de nombreuses méthodes de détection d'intrusion basées sur des méthodes d'apprentissage en profondeur dans un jeu de données réel.

CHAPITRE 1 : Les systèmes IDS et les attaques DoS

La détection d'intrusion d'une attaque par déni de service est un composant essentiel des systèmes de protection et de sécurité. Avec l'apparition quotidienne de nouvelles cyberattaques, les systèmes de détection d'intrusion (IDS) jouent un rôle majeur dans l'identification des cyberattaques potentielles sur un réseau ou un système approprié et fourni. IDS doit s'adapter au mieux à ces nouvelles menaces (cyberattaques) et à leurs tactiques, tout en continuant à évaluer. De nombreux outils sur le marché permettent aujourd'hui plusieurs niveaux de détection d'intrusion. Certaines solutions utilisent des signatures pour surveiller les attaques connues. Certaines plates-formes permettent la surveillance et la journalisation du réseau, en choisissant des méthodes de détection d'intrusion, nous avons préservé nos ressources réseau et les avons protégées contre les attaques indésirables. Dans ce chapitre, nous expliquerons comment fonctionne une attaque par déni de service avec un système de détection d'intrusion. Ensuite, nous décrivons les types de systèmes de détection d'intrusion. Les techniques d'attaque par déni de service ont été discutées, avant l'introduction des techniques de détection des systèmes de détection d'intrusion et la conclusion du chapitre.

1.1. Les attaques par déni de service ?

Une attaque par déni de service est une attaque contre un appareil connecté à un réseau qui fournit un service à des utilisateurs légitimes[1] , avec cette attaque, vous bloquez le service et le rendez indisponible par exemple la saturation de la bande passante du réseau (c'est ce qu'on appelle les attaques volumétriques) [2] , ces attaques peuvent entraîner des pertes financières importantes en perturbant le service pour des cibles non préparées., ça il est difficile de le détecter, car dans de nombreux cas, le trafic est similaire au trafic légitime [3].

Il existe trois catégories d'attaque DoS[1] et DDoS [2] et DRDOS [3]

[1] Dos : Déni de service, de l'anglais' Denial of service'
[2] DDoS : Distribué déni de service, de l'anglais' Distributed denial of service'
[3] DRDOS : Réflexion distribuée déni de service, de l'anglais' Distributed Reflection Denial of Service'

1.2. Catégories des attaques de déni de service

Dans les attaques par déni de service, il existe trois types de catégories importantes dans la cybersécurité DoS et DDoS et DRDoS

1.2.1. L'attaque par déni de service (DoS)

C'est une attaque simple qui utilise une seule machine source pour lancer l'attaque, par deux méthodes, la première exploite une vulnérabilité logicielle pour inonder une cible de fausses requêtes pour épuiser les ressources du serveur (cible). L'objectif est de mettre hors ligne un serveur soit en saturant sa connexion Internet, soit le serveur lui-même.[1]

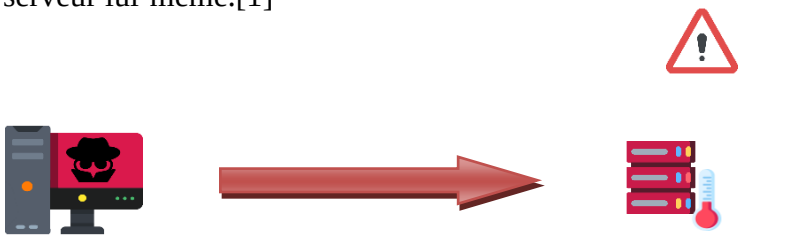


Figure 1-1: L'attaque par déni de service (DoS)

1.2.2. L'attaque par distribué déni de service (DDoS)

Une attaque DDoS, également une attaque par déni de service, est une technique de piratage qui inonde les serveurs de sites Web de (trop) de fausses connexions, rendant le site Web inaccessible. Cela est fait par moi (les pirates) en utilisant des botnets[4], qui sont une grande collection de machines infectées qui envoient des requêtes en boucle, c'est-à-dire tout ce qui peut se connecter à un site Web, et de plus en plus ces botnets. [4] [5]

[4]Botnets : Il s'agit d'appareils endommagés par un virus ou similaire dans le but d'une attaque intrusive ou similaire

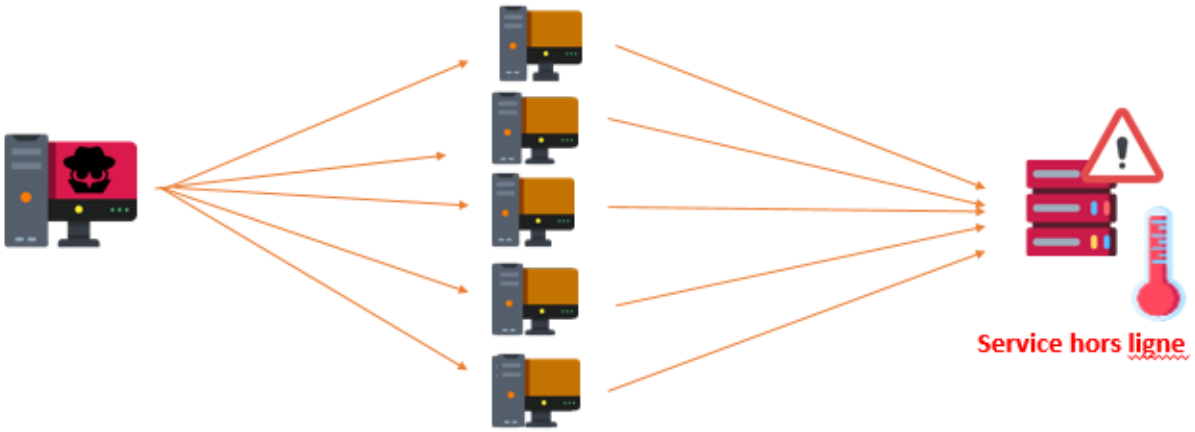


Figure 1-2 : L'attaque par distribué déni de service (DDoS)

1.2.3. L'attaque par distribué réflexion déni de service (DrDoS)

L'attaque DrDoS diffère de son prédécesseur, l'attaque DDoS, car elle étend l'attaque DDoS en incluant l'usurpation d'adresse IP tout en rendant l'attaque complexe.. L'attaque DoS par réflexion distribuée se compose de deux phases : la première est l'usurpation d'adresse IP pour masquer les attaquants à l'aide du réflecteur et la seconde est l'amplification utilisée pour maximiser la taille des réponses par rapport aux tailles de la demande. La principale caractéristique de l'attaque DrDoS, qui différencie ce type de l'attaque DDoS, est qu'elle n'attaque pas directement la destination mais envoie plutôt des paquets à la demande via un intermédiaire, un « réflecteur » exploitable qui consiste également à usurper l'adresse IP de l'expéditeur [6] [7].

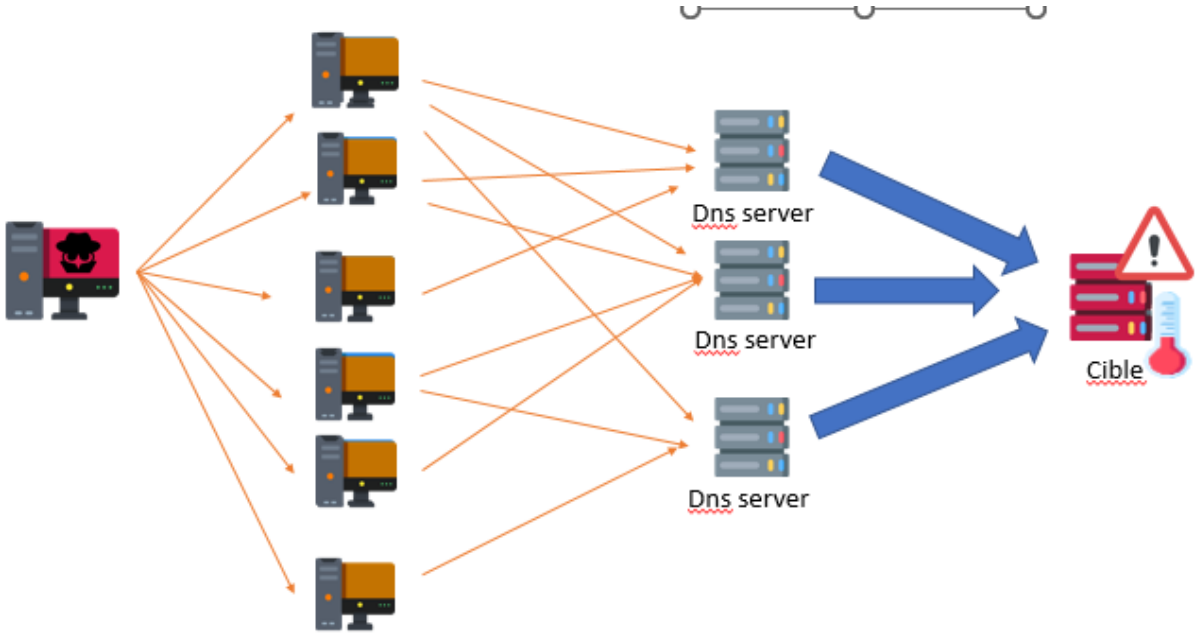


Figure 1-3 : L'attaque par distribué réflexion déni de service (DrDoS)

1.2.4. Synthèse et comparaison

Toute attaque conçue pour dénier le service aux utilisateurs visés peut être qualifiée d'attaque DoS. Cependant, si une attaque est lancée par plusieurs hôtes simultanément, elle s'appelle DDoS. Cependant, si une attaque est effectuée par un seul hôte, elle est différenciée en une attaque DoS (normale) (par opposition à une attaque DoS distribuée). Et si une attaque est lancée par plusieurs hôtes simultanément à l'aide d'une amplification de flux, cela s'appelle un DrDoS. (Distributed Reflection Denial of Service).

L'avantage de DDoS est la capacité à générer plus de trafic d'attaque. De plus, il est très difficile de bloquer les attaques car il y a tellement d'endroits d'où arrivent les demandes. De plus, il est très difficile de trouver le véritable attaquant qui a effectué l'attaque (puisqu'un attaquant DDoS et DrDoS peut lancer une attaque et rester à l'écart, toutes les autres machines infectées envoient des requêtes à un hôte sans se rendre compte qu'"elles feront désormais partie d'une attaque DDoS et DrDoS)

La méthode d'attaque DrDoS. Dans une attaque DrDoS, le site cible semble être attaqué par les serveurs victimes, et non par l'attaquant réel. Cette approche est appelée usurpation d'identité. Cela implique de simuler la source de la demande. L'amplification est un autre avantage de la méthode d'attaque DrDoS. En impliquant plusieurs serveurs victimes, la requête initiale d'un attaquant produit une réponse

plus importante que celle qui a été envoyée, augmentant ainsi la bande passante de l'attaque, ce qui la rend plus susceptible de provoquer une panne par déni de service.

1.3. Différents types d'attaques DoS

Il existe plusieurs types d'attaques, Mais nous allons expliquer les types les plus courants :

1.3.1. Attaque par SMURF

L'attaque SMURF est un moyen de générer un trafic réseau informatique important sur un réseau victime. Il s'agit d'un type d'attaque par déni de service qui inonde un système cible via des messages ping de diffusion usurpés. Une attaque par déni de service (Attaque DoS) ou attaque par déni de service distribué (Attaque DDoS) est une tentative de compromettre la disponibilité d'une ressource réseau pour ses utilisateurs prévus.

Dans une telle attaque, un auteur diffuse un grand nombre de requêtes d'écho ICMP (ping) à toutes les adresses du réseau. Toutes les requêtes diffusées ont une adresse IP source usurpée de la victime visée dans leur champ d'adresse IP source. Une fois que le périphérique de routage a transmis la demande d'écho à l'hôte ciblé (par exemple via une diffusion de couche 2), la plupart des hôtes de ce réseau IP répondront à la demande d'écho ICMP en y répondant par une réponse d'écho. La réponse du groupe à la requête d'écho entraînera un important trafic envoyé à l'hôte victime. Sur un réseau de diffusion multi-accès, des centaines de machines peuvent répondre à chaque paquet de requête d'écho [8]

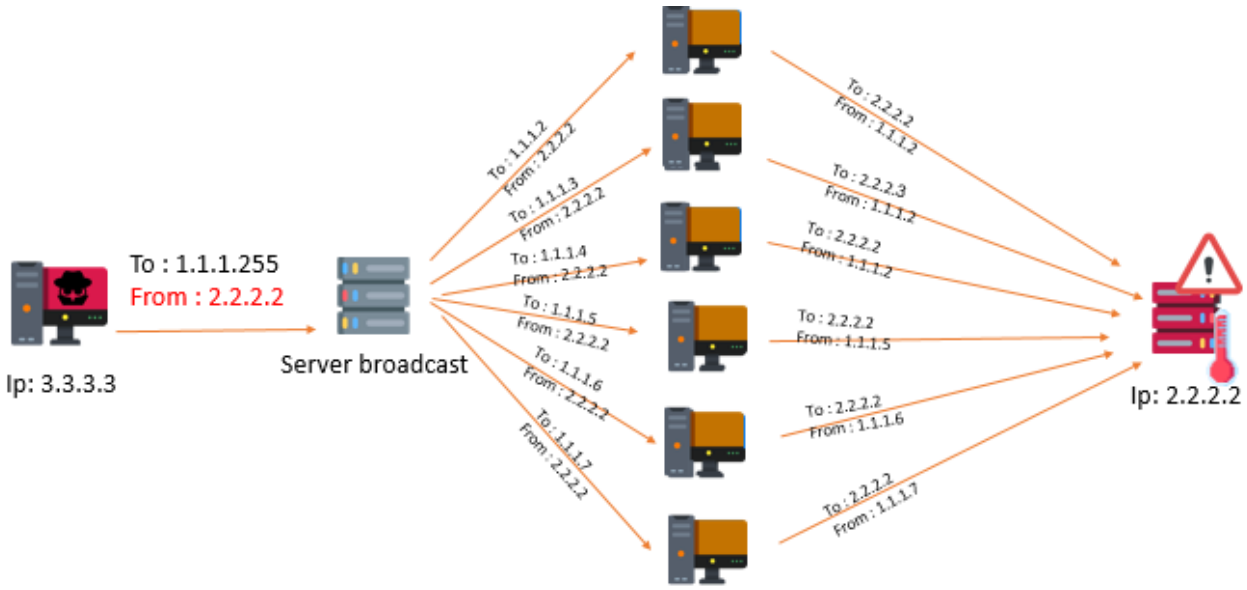


Figure 1-4 : Attaque par SMURF

1.3.2. Attaque par SYN FLOOD

Dans la connexion TCP, la connexion client et serveur doit être établie avant la transmission des données. C'est ce qu'on appelle l'établissement de liaison à trois voies TCP. Le client doit envoyer un message SYN au serveur, puis le serveur le reconnaîtra en envoyant un message SYN-ACK au client et le client doit envoyer un message ACK au serveur et la connexion est établie. Cependant, la poignée de main TCP à trois voies normales se transformera en une inondation TCP SYN lorsque l'attaquant envoie des paquets SYN répétés à un port aléatoire sur le serveur ciblé en utilisant une fausse adresse IP comme illustré [9]

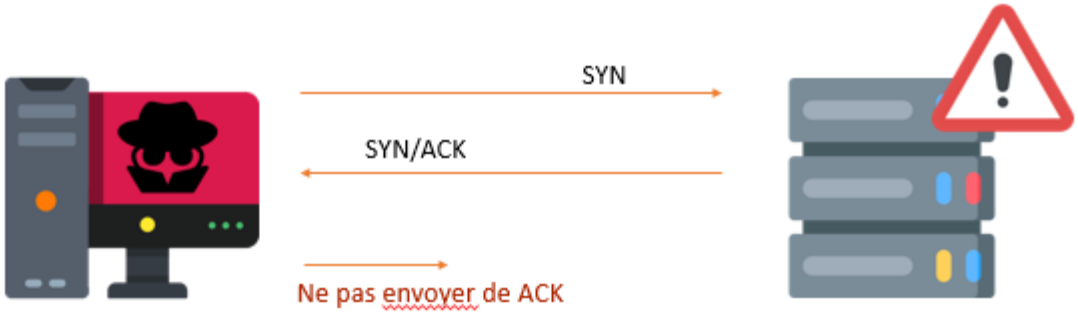


Figure 1-5 : Attaque par SYN FLOOD

1.3.3. Attaque par UDP FLOOD

UDP est un protocole sans connexion dans lequel aucune connexion n'est établie avant la transmission de données entre l'expéditeur et le destinataire. De plus, UDP ne peut pas détecter la perte de paquets pendant la transmission des données et il ne peut envoyer aucun message d'erreur. Le plus grand avantage d'UDP par rapport à TCP est sa vitesse de transmission élevée. Cependant, les paquets UDP peuvent être exploités par des attaquants pour lancer des attaques par inondation UDP telles que des attaques à bande passante élevée. L'inondation UDP est lancée en envoyant un grand nombre de paquets UDP vers des ports de destination aléatoires vers l'ordinateur de la victime.[10]

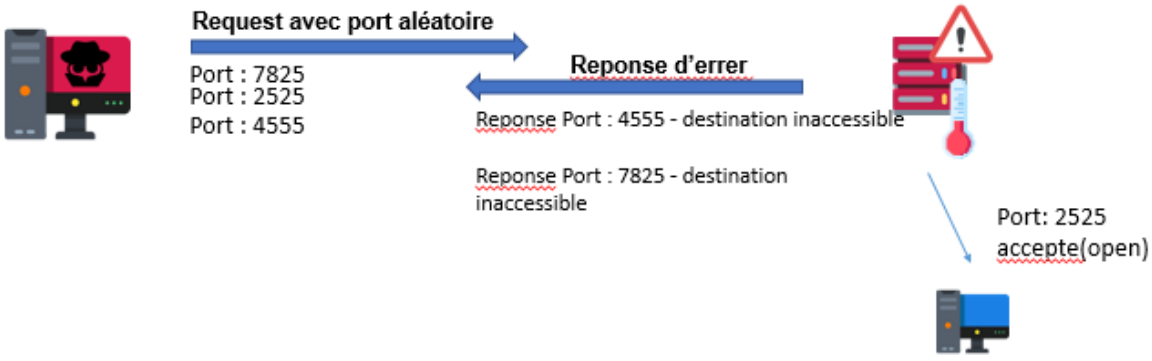


Figure 1-6 : Attaque par UDP FLOOD

1.3.4. Attaque par HTTP FLOOD

Attaque http flood sont un type d'attaque de déni de service distribué (DDoS) conçu pour exécuter des cibles d'inondation avec des requêtes HTTP. Lorsque la cible est saturée de demande et ne peut pas répondre au trafic existant, un rejet de service se produira pour les demandes supplémentaires des utilisateurs existants [11]. Il existe deux variétés d'attaques HTTP flood :

HTTP GET : Dans cette forme d'attaque, plusieurs ordinateurs ou autres appareils sont coordonnés pour envoyer plusieurs demandes d'images, de fichiers ou d'autres éléments à partir du serveur cible. Un déni de service se produit pour des demandes supplémentaires provenant de sources de trafic légitimes lorsque la cible est submergée de demandes et de réponses entrantes.

HTTP POST : Lorsqu'un formulaire est soumis sur un site Web, le serveur doit traiter la demande entrante et transmettre les données à une couche de persistance, généralement une base de données. Le traitement des données de formulaire et l'exécution des commandes de base de données nécessaires sont relativement intensifs par rapport à la puissance de traitement et à la bande passante requises pour envoyer une requête POST. Cette attaque exploite la différence de consommation relative des ressources en envoyant un grand nombre de requêtes POST directement au serveur cible jusqu'à ce que sa capacité soit saturée et qu'un déni de service se produise[11].

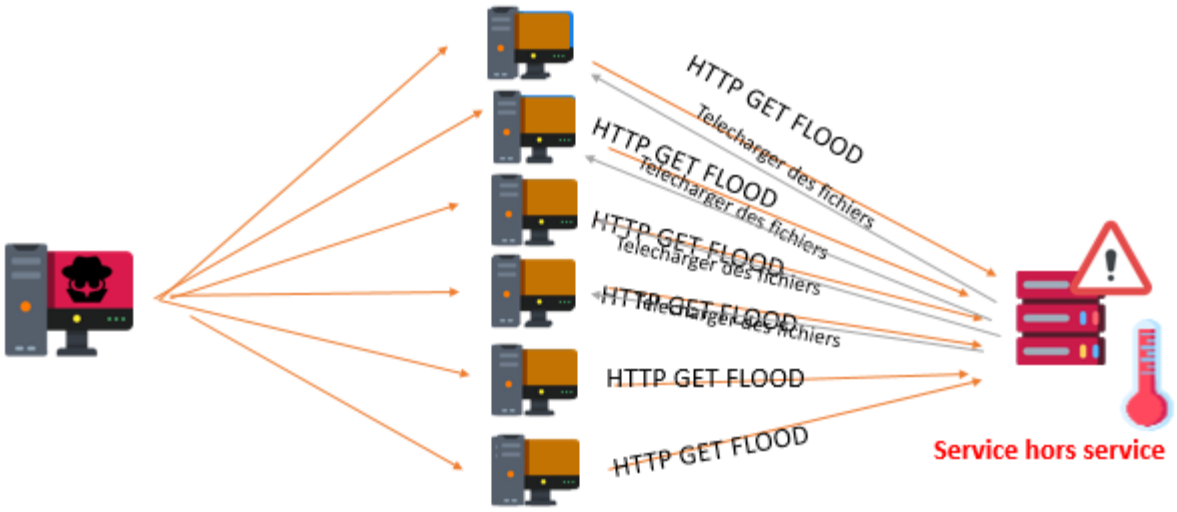


Figure 1-7 : Attaque par HTTP FLOOD

1.4. Les systèmes de détection des intrusions (IDS)

Les méthodes et technologies traditionnelles de prévention des intrusions, telles que les pares-feux, le chiffrement et le contrôle d'accès, sont pour la plupart inefficaces face à l'émergence rapide de nouvelles menaces sophistiquées, grâce à la croissance rapide des technologies de réseau, en particulier des réseaux sans fil Les données sont un problème critique qui ne peut être ignoré.

Un IDS est une combinaison de logiciel et de matériel qui tente de détecter une intrusion. Un système de détection d'intrusion peut être défini comme un système automatisé chargé de détecter les intrus entrant dans un système informatique tout en vérifiant les contrôles de sécurité fournis par les systèmes d'exploitation ou les outils de contrôle du réseau. Son objectif principal est de détecter l'utilisation non autorisée, la mauvaise utilisation et l'abus des systèmes informatiques par les utilisateurs internes et externes. [12].

1.4.1. Les types des systèmes de détection d'intrusion

Il existe deux grands types d'IDS :

1.4.1.1. IDSs à base de signature :

Une technique de détection qui ne se concentre pas sur la recherche d'intrusions. Il se concentre sur l'analyse du comportement en le comparant à un modèle considéré comme normal, et il est basé sur un ensemble de signatures, dont chacune représente un profil de l'attaque.

Les approches basées sur les signatures recherchent dans les flux réseau les empreintes digitales d'attaques connues, telles que les logiciels antivirus, avec des signatures définies comme une série d'événements et de conditions liés à une tentative d'intrusion. Ensuite, en utilisant le pattern matching, identifiez les idées. Si l'IDS est en mode actif, une alarme peut être émise si une attaque est détectée ; sinon, IDS enregistrera simplement l'attaque [13].

1.4.1.2. IDSs à base d'anomalie :

Des IDS basés sur des anomalies, dont le déploiement nécessite une phase d'apprentissage dans laquelle l'outil apprend le comportement « normal » des flux applicatifs présents sur son réseau. Par conséquent, chaque flux et son comportement par défaut doivent être déclarés. L'IDS émet une alerte lorsqu'un flux anormal est détecté, mais ne peut pas indiquer la criticité de l'éventuelle attaque. Les identifiants comportementaux sont apparus bien plus tard que les identifiants de signature et n'ont pas encore bénéficié de leur maturité. Par conséquent, l'utilisation d'un tel IDS peut être délicate dans la mesure où les alarmes déclenchées peuvent contenir un grand nombre de fausses alarmes.[13]

1.4.2. Architecture des IDS et principe de fonctionnement :

Le système de détection d'intrusion se compose de plusieurs outils, chaque outil ayant sa propre tâche, dont le but général est de détecter les intrus dans la première phase, puis d'informer l'opérateur ou le personnel informatique de la possibilité d'intrusion dans le réseau informer.

Un modèle général de structure d'un système de détection d'intrusion a été proposé par l'IDWG [5], qui englobe et normalise la structure d'un système de détection d'intrusion. La Figure 1-8 détaille les différents composants de ce système. Les IDS peuvent ne pas avoir complètement séparé tous ces composants, comme le montre la figure (Figure 1-8). Certains IDS combinent ces composants en un seul module, d'autres ont plusieurs instances de ces modules [14]

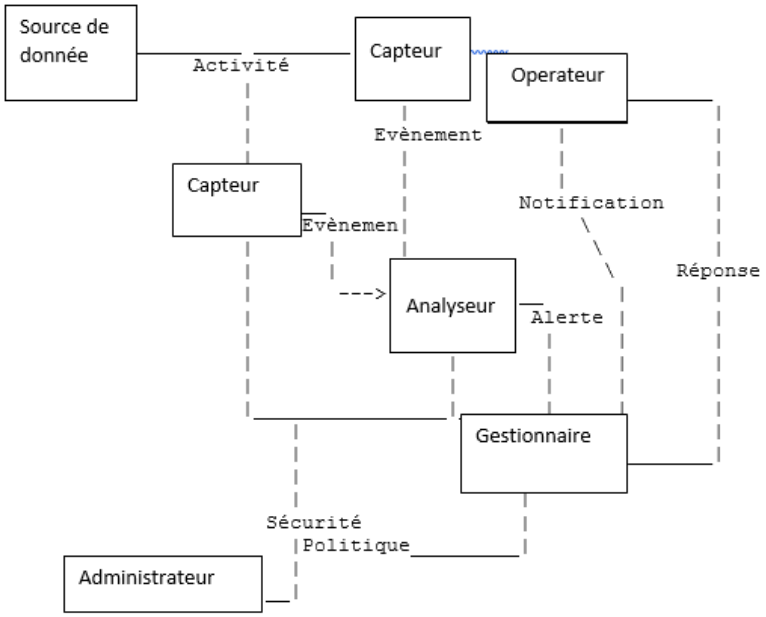


Figure 1-8 : Un modèle fonctionnel du Système de détection d'intrusion proposé par l'IDWG [14]

L'Administrateur : la personne responsable de la création de la politique de sécurité de l'organisation qui déploie et configure les différents composants d'IDS. il prend en charge la déclaration prédéfinie des activités autorisées sur le réseau ou sur des hôtes spécifiques pour répondre aux besoins d'un système d'information.

[5] IDWG (Intrusion Detection Working Group)

La source de données : Il existe différents types de données provenant de plusieurs sources (réseau, système, application et alertes). Le système IDS n'a aucune restriction sur les sources de données utilisées, il utilise donc des capteurs appropriés pour analyser les informations provenant de ces sources afin de détecter les activités non autorisées ou indésirables.

Le capteur et l'analyseur : est le composant clé du système, d'abord le capteur accède aux données brutes et collecte toutes les informations sur l'activité en cours et les transmet à l'analyseur sous forme d'événements (séquence d'activités). L'administrateur de sécurité analyse ensuite ces événements pour signaler des activités ou des événements non autorisés ou indésirables susceptibles d'intéresser l'administrateur de sécurité. Dans la plupart des IDS existants, le capteur et l'analyseur font partie du même ensemble

Le gestionnaire : C'est également un composant clé, permettant aux opérateurs de gérer divers composants du système à partir de là. Les fonctions du gestionnaire incluent généralement (mais sans s'y limiter) la configuration du capteur, la configuration de l'analyseur, la gestion des notifications d'événements, l'intégration des données et la gestion des rapports.

Réponse : Ce sont des mesures prises en réponse à un incident. Cela peut être fait automatiquement par les entités du schéma IDS car il peut être initié par un humain. L'envoi d'une notification à l'opérateur est une réponse très courante. D'autres réponses incluent (mais sans s'y limiter) l'activité de journalisation, la journalisation des données brutes (à partir de sources de données) caractérisant les événements, les temps d'arrêt du réseau ou de l'utilisateur ou les sessions d'application, la modification des contrôles d'accès au réseau ou au système.

.[14]

1.4.3. Emplacement de l'IDS

1.4.3.1. Les NIDS (Systèmes de détection d'intrusion basés sur le réseau) :

Un NIDS est divisé en trois parties principales : la collecte, les signatures et les alertes. Il écoute donc tout le trafic réseau, puis analyse les flux de transit dans le réseau et génère des alertes lorsque des paquets apparaissent dangereux (voir Figure 1-9)

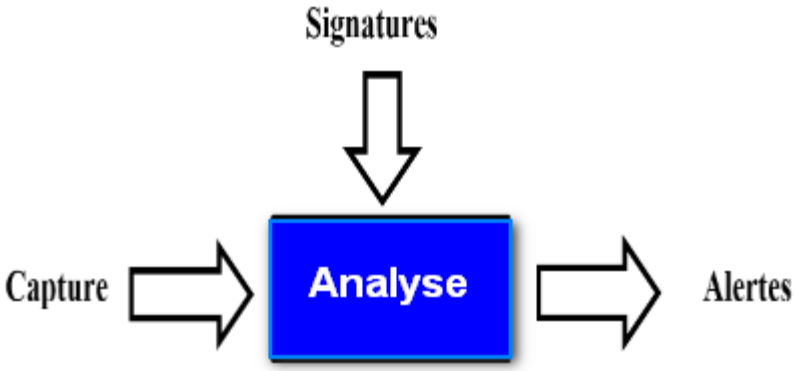


Figure 1-9 : les composants d'un NIDS [15]

La tâche principale de NIDS est d'analyser et d'interpréter les paquets circulant dans ce réseau. Les réseaux NIDS sont mis en œuvre par des capteurs stratégiquement placés sur le réseau et générant des alertes lorsqu'une attaque est détectée. Ces alertes sont envoyées à une console de sécurité pour analyse et traitement éventuel, et les capteurs du réseau sont en mode furtif, les rendant invisibles aux autres machines. Pour ce faire, votre carte réseau est configurée en mode "promiscuous", un mode dans lequel la carte réseau lit tout le trafic de données et n'est pas configurée avec une adresse IP.[15].

1.4.3.2. Les HIDS (Host-Base Intrusion Détection System):

Les HIDS réside sur un hôte spécifique et analyse uniquement les informations sur cet hôte. HIDS se comporte comme un démon ou un service standard sur l'hôte serveur/système. De plus, l'impact sur le dispositif correspondant peut être immédiatement observé, par exemple en cas d'attaque réussie par l'utilisateur. Système de détection d'intrusion utilisent deux types de sources pour fournir des informations sur l'activité de la machine : les journaux du système d'exploitation et les pistes d'audit : les pistes d'audit sont plus précises et détaillées et fournissent de meilleures informations, tandis que les journaux ne fournissant que des informations de base sont plus petits (voir Figure 3.2) [15].

1.4.3.3. Les IDSs hybrides

Les IDS hybrides rassemblent En pratique, on la combinaison de NIDS et HIDS. Ils permettent, en un seul outil, de surveiller les réseaux et les terminaux. Les sondes sont placées en des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes ces sondes remontent alors les alertes à une machine qui va centraliser, et agréger/lier les informations d'origines multiple, ils sont donc basés sur une architecture distribuée, où chaque composant unifie son format d'envoi d'alerte.[16]

Dans ce tableau récapitulatif, mettant en avant les avantages, désavantages de chacun de ces IDS. Ils discutent également dans ce tableau de la responsabilité du déploiement et de mise à jour de ces systèmes.

Table 1-1 : Résume des diffèrent placements des IDS

Type d'IDS	Avantage	Désavantages	Placement	Déploiement & Possibilité
HIDS	- Détecte les intrusions sur appariteur les fichiers appels régime soit évènements enchevêtrement entre l'hôte-pas indigence d'équipement de davantage	-besoin de l'installer sur chaque machine -détection d'attaques locales uniquement	Machine virtuelle ou physique	Utilisateur & Administrateur
NIDS	Détecte les intrusions en surveillant le trafic réseau. -besoin d'être place sur le réseau (physiquement) -peut surveiller plusieurs systèmes en même temps.	-Difficile de détecter des intrusions provenant de contenu chiffre. -Ne peut pas détecter les attaques ne transitant pas par le NIDS.	Réseau physique ou virtuel	Administrateur
Hyperviseur-IDS	-Détecte les intrusions entre les VM en analysant le trafic réseau	-Récent en difficile de s'interfacer avec les hyperviseurs. - composant critique	Hyperviseur	Administrateur
DIDS	-Caractéristiques des HIDS /NIDS. -Détecte les intrusions en associant plusieurs systèmes de détections d'intrusions (HIDS /NIDS).	Cout de déploiement et de configuration. - Surcout en communication -Coopération dans lequel les systèmes complexe.	Partout	Utilisateur & Administrateur

1.4.4. Méthodes de détection :

Le cœur du système de détection d'intrusion est le module de détection d'activités malveillantes. La première génération de systèmes s'appuie sur les connaissances des professionnels de la sécurité pour identifier les attaques, après avoir développé diverses méthodes de détection pour construire un système de détection de haute précision et plus efficace. Les approches de détection d'intrusion se divisent en deux groupes principaux : la détection d'anomalies et la détection de signature

. Cependant, il n'y a pas de différence significative entre ces deux classes dans leurs propriétés, pour toutes les propriétés des méthodes de détection, selon Liao et al. Suggested (2013 [17])) avec un regard approfondi sur son personnage Statistique : Basis in Statistique, Model, Rules, Cases and Inférence.

Les approches basées sur les statistiques consistent surtout en des statistiques sur les caractéristiques des particularité analogues que l'affiliation prédéterminé, la moyenne, l'variété utopie et les probabilités d'distinguer les interventions. Le marquage basé sur des modèles se concentre sur la modélisation des techniques de classification échec des traquenards connues. Les techniques basées sur des menstruel sont surtout appliquées à l'habitude Ifthensiafter comme modéliser et découper les

Interventions connues inspirées de concepts biologiques exacts que le défilé immunitaire, les algorithmes génétiques et l'raison en essaim. Des travaux récents consistent à réunir ces autres méthodes de marquage comme une nomination sophistiquée comme bénéficier davantage de brièveté et une meilleure efficacité. [17].

1.4.5. Les mesures de notation IDS :

Procédures qui nous permettent d'évaluer l'efficacité globale des systèmes de détection d'intrusion comme suit :

Précision : IDS est précis dans la détection des attaques sans faux positifs. L'inexactitude survient lorsqu'une action légitime dans l'environnement est déclarée anormale ou indicative.

Puissance de traitement : mesurée par la vitesse à laquelle les événements sont traités. Si le système IDS est plus efficace, la détection en temps réel sera possible. Complétude : c'est la capacité d'IDS à détecter toutes les attaques.

Tolérance aux pannes : la plupart des systèmes de détection d'attaques fonctionnent sur des systèmes d'exploitation ou des appareils connus pour être vulnérables aux attaques. Par conséquent, IDS doit résister à ces attaques, en particulier les attaques par déni de service.

Vitesse : IDS doit être plus rapide lors de l'analyse et de l'exécution afin de réduire le temps de réponse et d'empêcher un attaquant de modifier la source de l'analyse ou de perturber le fonctionnement du système [18]

En général, un taux de détection élevé pour un système IDS basé sur l'apprentissage automatique et une précision de détection élevée avec un faible taux de fausses alarmes sont essentiels pour l'efficacité des systèmes [19].

Les principaux aspects à prendre en compte lors de la mesure de la précision de la détection et de la classification des attaques sont :

- True Positive (TP) : nombre d'intrusions correctement détectées
- True Negative (TN) : nombre de non-intrusions correctement détectées
- False Positive (FP) : nombre de non-intrusions mal détectées
- False negative (FN) : nombre d'intrusions mal détectée

Il existe différents types d'erreurs qui proviennent du détecteur et affectent ses performances d'une manière ou d'une autre. Le véritable avantage est lorsque l'alarme se déclenche lorsque les politiques de sécurité sont violées. Du côté négatif, aucune alarme ne se déclenche et rien n'est à sa place. arrive normalement. Un faux positif, c'est quand une alarme retentit alors que rien d'inhabituel ne s'est produit. Un faux négatif, c'est quand l'alarme ne sonne pas Si quelque chose d'inhabituel s'est produit À première vue, vous pouvez penser qu'un faux résultat positif est moins dangereux qu'un faux négatif.

CHAPITRE 1 : Les systèmes IDS et les attaques DoS

La sécurité du réseau est devenue un problème sérieux car plusieurs attaquants tentent d'attaquer les réseaux pour atteindre un objectif, comme l'économie. De nombreuses méthodes de protection du réseau ont été proposées, telles que les systèmes de détection d'intrusion, la cryptographie, les pares-feux, etc. Parmi ces outils de sécurité, la détection d'intrusion est généralement considérée comme l'une des méthodes les plus encourageantes pour nous protéger contre les cyberattaques nouvelles, dynamiques et complexes, dans ce chapitre, nous introduisons une attaque par déni de service et ses types génériques, ainsi que certains des types bien connus de systèmes de déni de service et de détection d'intrusion et leur modèle général. Nous avons ensuite discuté des trois types de systèmes de détection d'intrusion : les systèmes de détection d'intrusion basés sur l'hôte (HIDS), les systèmes de détection d'intrusion basés sur le réseau (NIDS) et les systèmes de détection d'intrusion hybrides. Nous avons discuté des techniques de système de détection d'intrusion avant d'introduire les techniques de détection de bot, dans le chapitre suivant, nous présenterons l'apprentissage automatique, l'apprentissage en profondeur et les activités connexes.

CHAPITRE 2 : Etat de l’art sur l’apprentissage profond pour la cybersécurité

L'intelligence artificielle (IA) s'articule autour du travail, de la conception et de la mise en œuvre de systèmes de machines difficiles à faire fonctionner normalement pour l'homme. Elle est devenue un sujet essentiel de la recherche scientifique de ce siècle, elle est devenue une grande influence dans de nombreux domaines, dans ce chapitre nous présenterons l'apprentissage automatique et ses types après cela nous expliquerons l'apprentissage profond et ses types.

De plus, dans ce chapitre, de nombreux travaux liés à notre travail seront présentés, qui ont été développés pour détecter une attaque par déni de service dans les détecteurs d’infiltration.

2.1. Généralités sur l’apprentissage automatique

2.1.1. Définition

L'apprentissage automatique est un sous-domaine de l'intelligence artificielle. Ce qui est lié à l'étude des algorithmes des appareils électroniques avec un processeur qui permettent à ces systèmes d'apprendre et d'améliorer leur capacité automatiquement à partir de chaque expérience sans ou avec intervention humaine. Selon l'approche d'apprentissage, le type de données entrées et sorties, et le type de problème résolu, les algorithmes d'apprentissage automatique ont été divisés en plusieurs types : apprentissage supervisé, non supervisé, semi-supervisé et apprentissage renforcé.

2.1.2. Approches de l'apprentissage automatique

2.1.2.1. L'apprentissage supervisé

Nous utilisons ce type d'apprentissage lorsque les données sont sous l'une des deux formes, variables d'entrée et valeurs cibles de sortie. L'algorithme commence à apprendre la fonction de mappage des variables d'entrée aux valeurs cibles de sortie. Il existe deux types de ce modèle : la classification (où la variable de sortie est discrète), la régression (où la variable de sortie est continue).

2.1.2.2. Apprentissage non supervisé

L'apprentissage non supervisé est utilisé lorsque les données ne sont utilisées qu'en entrée et qu'il n'y a pas de variable de sortie correspondant à ces données. Pour en savoir

plus sur les caractéristiques des données, un tel algorithme modélise les modèles sous-jacents de ces données.

2.1.2.3. Apprentissage semi-supervisé

Ce type d'algorithme est un intermédiaire entre les techniques d'apprentissage non supervisé et supervisé. Cet algorithme s'entraîne en utilisant une combinaison de données non étiquetées (petite quantité) et étiquetées (petite quantité). L’algorithme d'apprentissage non supervisé regroupe les premières données similaires, puis il étiquette les données non étiquetées au repos en utilisant les données étiquetées existantes

2.2. L’apprentissage profond pour la cybersécurité

Avec d'énormes quantités de données disponibles à partir de l'infrastructure réseau, des réseaux, des systèmes d'exploitation ou des systèmes d'information, des méthodes et des technologies pour relever les défis de la cybersécurité, tels que l'apprentissage automatique, l'exploration de données, les statistiques et d'autres capacités interdisciplinaires [20]. L'apprentissage en profondeur peut être utilisé dans l'apprentissage automatique pour les identifiants de détection de défauts basés sur les signatures ou la détection d'anomalies. Ces méthodes de classification et de prédiction peuvent être utilisées pour détecter des modèles et des comportements anormaux de diverses attaques de réseau, permettant au réseau de réagir en temps réel. Ils ont la capacité de détecter les attaques au fur et à mesure qu'elles se produisent, ainsi que d'anticiper les futures attaques potentielles [21]. D'autre part, la collecte de données et le trafic réseau ont conduit au problème du Big Data, et les experts en sécurité veulent toujours de meilleures performances des systèmes IDS qui ont le taux de détection le plus élevé et le taux de faux positifs le plus élevé. D'où des approches d'apprentissage en profondeur qui s'adaptent bien à de très grandes quantités de données. Ce dernier a été introduit dans la détection d'anomalies du réseau pour faire la distinction entre un comportement normal et anormal afin de détecter une activité malveillante ou suspectée [17].

2.3. Quelques méthodes d’apprentissage profond

Les réseaux neuronaux profonds sont un ensemble de neurones organisés en une séquence de couches interconnectés. Ce qui les différencie, c‘est l‘architecture du réseau

(la manière dont les neurones sont organisés dans le réseau et la manière dont ils se fonctionnent. Parmi de nombreuses implémentions de modèles d'apprentissage profond :

2.3.1. Les réseaux de neurones artificiels (ANN)[6]

ANN est un type de réseau de neurones (NN) causé par des réseaux de neurones biologiques. ANN est un groupe de neurones ou de nœuds connectés les uns aux autres. Où les connexions sont pondérées. Chaque neurone utilise une fonction d'activation non linéaire pour la somme de ses entrées pondérées afin de la convertir en entrée/sortie [20].

Dans le réseau direct, les données d'entrée sont distribuées dans le réseau direct, chaque couche cachée reçoit une entrée de la sortie de la couche précédente, générant la sortie finale en fonction des paramètres de poids, de la sélection de la fonction d'activation et des données d'entrée. Les paramètres de pondération du réseau sont ajustés à l'aide de l'optimisation de descente de gradient (GDO) pour réduire la fonction de perte. [22]

La fonction d'activation est la fonction qui transforme la combinaison linéaire des signaux d'entrée en une valeur de sortie. Les fonctions d'activation les plus populaires sont (tableau 3.1) : sigmoid, ReLU, Tanh, and LeakyReLU [23]

[6] ANN: Artificial neural networks (Ang)

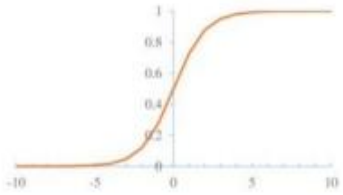
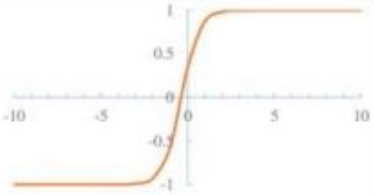
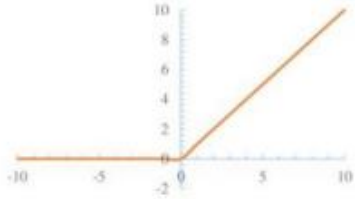
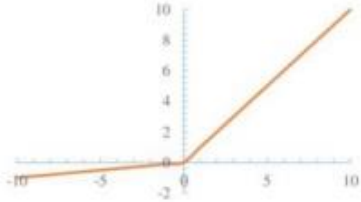
Name	Graph	Function
Sigmoïde		$f(x) = \frac{1}{1+e^{-x}}$
Tanh		$f(x) = \frac{2}{1+e^{-2x}} - 1$
ReLU		$f(x) = \begin{cases} 0 & pour\ x < 0 \\ x & pour\ x \geq 0 \end{cases}$
LeakyReLU		$f(x) = \begin{cases} 0.01x & pour\ x < 0 \\ x & pour\ x \geq 0 \end{cases}$

Table 2-1 : Les fonctions d'activation les plus courantes [24]

2.3.2. Réseaux de neurones convolutifs (CNN[7])

Le réseau de neurones convolutifs (CNN) est un type de réseau de neurones à anticipation, il comprend des couches de convolution et des opérations de mise en commun. Il est capable d'extraire des fonctionnalités locales et globales 56

[7] CNN: Convolutional neural networks (Ang)

Comme le montre la figure 3.5, un réseau neuronal convolutif comporte trois couches : la couche convolutive, la couche de regroupement (couche de sous-échantillonnage) et la couche entièrement connectée.

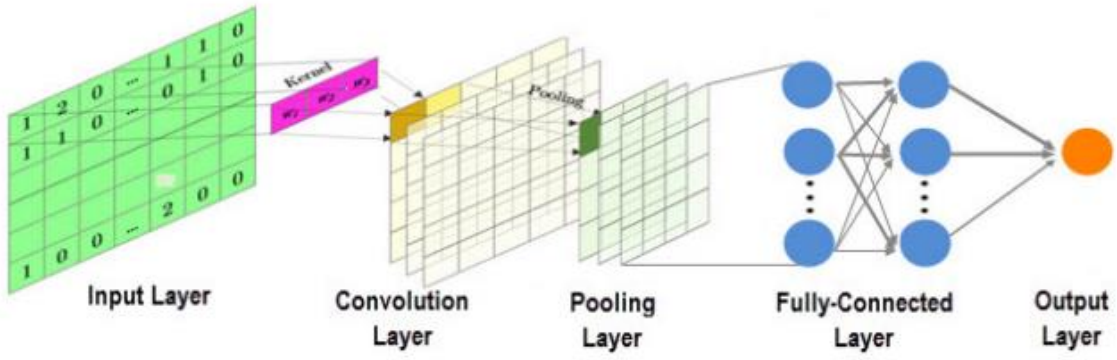


Figure 2-1 : L'architecture d'un réseau neuronal convolutive [25]

2.3.3. Réseaux de neurones récurrents (RNN[8])

Le réseau neuronal récurrent (RNN) est un modèle d'apprentissage séquentiel courant. RNN apprend les caractéristiques des données de série à l'aide d'une mémoire des entrées précédentes stockées dans l'état interne du réseau neuronal. Comme le montre la figure 4, un cycle dirigé est utilisé pour établir les connexions entre les neurones [25]

[8] RNN: Recurrent neural networks (Ang)

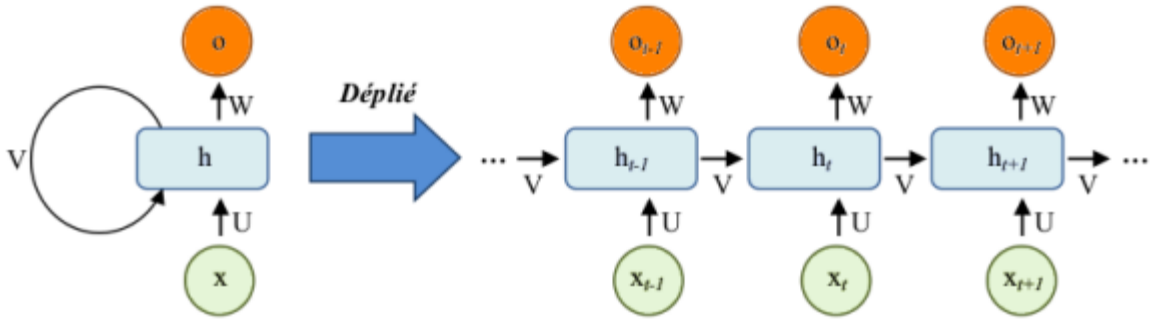


Figure 2-2 : L'architecture d'un modèle RNN [25]

2.4. Travaux connexes sur la détection des attaques DoS basés Deep et Machine learning

Dans les travaux précédents d'apprentissage en profondeur, les résultats ont montré qu'il surpasse complètement l'apprentissage automatique tel que la machine à vecteur de support 'SVM' et réseaux de neurones artificiels 'ANN' dans la détection des intrus.

Hamouda et al [26]ont utilisé le dataset CICDDoS2019 pour développer trois modèles d'apprentissage en profondeur discriminants pour la détection Des agressions DDoS, Ils ont utilisé le sous-échantillonnage aléatoire pour répliquer trois sous-ensembles de données pour trois classifications distinctes. Pour la classification, il a utilisé trois modèles d'apprentissage en profondeur (apprentissage supervisé) : un réseau de neurones profond (DNN), un réseau de neurones convolutif (CNN) et un réseau de neurones récurrent (RNN). La classification multi-classes (normal/attaque) et la classification binaire (normal/attaque) couvrent toutes deux des types d'attaques distincts, avec précision (7 classe : 80 % , 2 classe : 99 % , 13 classe : 60 %), Il a produit l'évaluation des performances d'apprentissage automatique (précision, rappel, score F1), L'inconvénient de cela est que les données de test ont été renommées manuellement à l'aide de l'éditeur" Notepad ++"

Sharafaldin et al [4]**,** Travailler avec l'ensemble de données CICDDoS2019 est la contribution majeure de l'article. Plusieurs types et familles d'attaques DDoS sont

examinées dans cet article afin de proposer une nouvelle taxonomie DDoS pour la couche applicative. Ils ont également examiné les ensembles de données DDoS les plus populaires et noté les failles et les limitations les plus courantes. En réponse à ces failles, ils ont créé un nouvel ensemble de données, CICDDoS2019, qui comprend 11 attaques DDoS pour l'évaluation des algorithmes et des systèmes IDS/IPS. Nous avons également inclus les éléments les plus critiques pour détecter diverses attaques DDoS. De plus, il fournit une analyse complète pour chacun d'eux basée sur les 12 diagrammes RadViz des facteurs les plus pertinents pour chaque type de trafic réseau. Il applique différents algorithmes d'apprentissage automatique : forêt aléatoire, Naive Bayes, régression logistique, avec précision(f1=69%). Table 2-2

Algorithme	Précision	Recall	F1-score
ID3	0.78	0.65	0.69
Random Forest	0.77	0.56	0.62
Naive Bayes	0.41	0.11	0.05
Logistic Regression	0.25	0.02	0.04

Table 2-2 : Les résultats de Sharafaldin et al[4]

Farage et al [27] . Les auteurs il propose Un modèle IDS basé sur un réseau neuronal convolutif, un modèle IDS basé sur un réseau neuronal profond et un modèle IDS basé sur un réseau neuronal récurrent font partie des trois modèles IDS basés sur l'apprentissage profond présentés. À l'aide de deux nouveaux ensembles de données sur le trafic réel, l'ensemble de données CIC-DDoS2019 et l'ensemble de données TON_IoT, les performances de chaque modèle sont étudiées dans deux types de classification (binaire et multi classe). En termes de mesures de performance cruciales, les résultats révèlent que les approches d'apprentissage en profondeur surpassent les tactiques d'apprentissage automatique conventionnelles De plus, le modèle IDS basé sur CNN bat les approches IDS d'apprentissage en profondeur de pointe, qui ont été évaluées à l'aide de l'ensemble de données CIC-DDoS2019 et de l'ensemble de données TON_IoT, avec une précision de détection du trafic binaire de 99,95 % et une précision de détection du trafic multi classe. de 95 %.

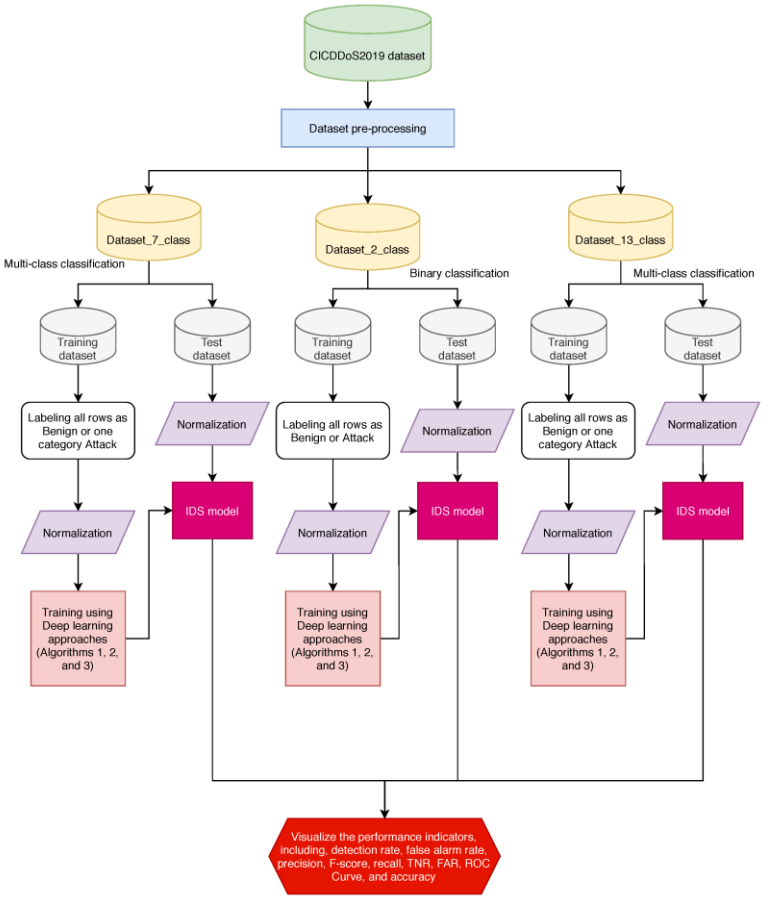


Figure 2-3 : Organigramme de la méthodologie utilise dans article [27]

Hosseini S et al [5],Dans cet article, il propose un cadre hybride basé sur une approche de flux de données pour détecter Attaque DDoS avec apprentissage incrémental. Nous utilisons une technique qui divise la charge de calcul entre côté client et proxy en fonction de leurs ressources pour organiser la tâche à grande vitesse. Le côté client contient trois étapes, la première est la collecte de données du système client, la seconde est la fonctionnalité extraction basée sur la sélection de caractéristiques vers l'avant pour chaque algorithme, et le test de divergence. En conséquence, si la divergence est supérieure à un seuil, l'attaque est détectée sinon les données sont traitées du côté proxy. Ils sont utilisés le Bayes naïf, la forêt aléatoire, l'arbre de décision, le perceptron multicouche (MLP) et les k plus proches voisins (K-NN) du côté proxy pour obtenir de meilleurs résultats. Différentes attaques ont leur comportement spécifique, et parce que des différentes fonctionnalités sélectionnées pour chaque algorithme, les performances appropriées pour détecter les attaques et une plus grande capacité à distinguer de nouveaux types d'attaques est obtenue.

Les résultats montrent que la forêt aléatoire produit meilleurs résultats parmi les autres algorithmes mentionnés.

Table 2-3 : Travaux antérieurs connexes pour la détection d'intrusion basé sur le deep learning

Travaille	Année	Domaine	Techniques	Dataset	Mesures de performances	Cité
Sharafaldin et al.[4]	2019	IDS	Id3 ,RF ,Naive Bayes ,Logistic regression	CICDDoS2019	F1 score: 0.69 Figure 2-2	286
Hamouda Djallal et al.[26]	2020	IDS	CNN, DNN, RNN	CICDDoS2019	7 class : 80 % 2 class : 99 % 13 class : 60 %	18
Farage et al [27]	2021	IDS	CNN, DNN, RNN	TON_IoT CICDDoS2019	CNN 95 % RNN 94 % DNN 94%	18
LI, JUNHONG [28]	2020	IDS	Machine learning	CICDDoS2019	F1 score :77.393 %	6
Mittal M et al.[29]	2022	IDS	DNN et LSTM	CICIDS2017	Classification binaire : acc=98.72%	54
Abdullah emir et al. [30]	2021	SDN	DNN	CICDDoS2019	Classification binaire : acc = Jour 1 : 99.99% Jour 2 : 94.57%	22
Tavallaee et al. [31]	2009	IDS	RandomForest NaiveBayes	NSL-KDD	2 classes : Acc =82.02%	3649
Al-Yaseen et al. [32]	2017	IDS	SVM ELM	KDD 99	2 classes : Acc =95.75%	331
Maseer et al. [33]	2021	IDS	KNN SVM	CICIDS2017	2 classes : Acc =98.86%	50
Gohil et al. [34]	2000	IDS	SVM KNN	CICDDoS2019	2 classes : Acc =97.72%	516
Almaini et al. [35]	2021	IDS	Kalman Backpropagation Neural Network	CICDDoS2019	2 classes : Acc =94%	6

Le domaine de l'apprentissage automatique est très vaste, en particulier l'apprentissage profond. L'apprentissage profond a renouvelé les algorithmes chaque semaine. Par conséquent, l'application d'outils d'apprentissage profond est très importante à notre époque. C'est la base de l'apprentissage automatique. C'est un bon et important focus dans le domaine de la cybersécurité, notamment pour les chercheurs.

Dans notre domaine, les méthodes d'apprentissage automatique sont utilisées pour analyser le système et découvrir un trafic inhabituel en apprenant au système à découvrir des événements, au moyen de modèles mathématiques extraits d'algorithmes d'apprentissage automatique, et dans cette section, nous avons expliqué l'apprentissage automatique dans la cybersécurité en de nombreuses études (de 2000 à 2022) en utilisant différentes bases de données, réelles ou factices, à des fins d'apprentissage automatique, afin de déterminer la démarche scolaire nécessaire et la meilleure à suivre dans la seconde partie.

CHAPITRE 3 : Contribution, résultat et discussion

Les systèmes de détection d'intrusion pour les cyberattaques ont fait l'objet de nombreux travaux de recherche en matière d'apprentissage en profondeur, qui a été appliqué dans les systèmes de détection d'intrusion utilisant de nombreux ensembles de données différents pour la cybersécurité, plus les données sont réalistes, plus l'efficacité de la système de détection d'intrusion Un ensemble de données du monde réel de l'Institut canadien de la cybersécurité (CIC) nommé CICDDoS2019, composé d'attaques par déni de service distribué (DDoS) , nous avons proposé un modèle CNN d'apprentissage en profondeur, afin d'identifier ces différents attaques de dispositifs de détection d'intrusion pour résoudre le problème de détection des attaques par déni de service et améliorer son taux de détection, la vitesse de détection des attaques doit être élevée et le taux de fausses alarmes faible, compte tenu des différentes métriques d'évaluation des algorithmes d'apprentissage profond .

3.1. Environnement de développement

3.1.1. Matériel utilisé

La machine sur laquelle a été développé notre système a la configuration suivante :

Table 3-1 : Caractéristiques de matériel

Materials	Caractéristiques
PC	Processeur: Intel (R) Co (TM) i3- 3217U CPU @ 1.80 GHz. Mémoire Vive (Ram) : 6,00 Go. Disque Dur : 512 Go. Système d'exploitation : Windows10 Professionnel N.

3.1.2. Environnement logiciel

Spyder : Est Créé et il est développé par «Pierre Raybaut» en 2008, c'est est un environnement scientifique puissant écrit en Python, et il est conçu par et pour les scientifiques, les ingénieurs, et les analystes de données (Spyder Website Contributors, 2018).

Google Colab : Colaboratory ou "Colab" en abrégé, est une initiative de recherche de Google qui a été développée pour aider à la diffusion de l'enseignement et de la recherche sur l'apprentissage automatique. Il s'agit d'un environnement de bloc-notes Jupyter qui s'exécute entièrement dans le cloud et ne nécessite aucune configuration. Google fournit une utilisation gratuite du GPU et c'est une fonctionnalité qui attire les développeurs. Offre également des bibliothèques python courantes telles que NumPy, Matplotlib, TensorFlow et Keras pour aider les développeurs à écrire, modifier et exécuter du code python. Les développeurs peuvent utiliser ces bibliothèques pour analyser et visualiser des données [36].

3.1.3. Langages de programmation et bibliothèque

Nous avons utilisé le langage python v 3.7 , et la bibliothèque pandas NumPy pour le traitement de donnes et keras pour appliquer le model

Python : langage de programmation open source le plus utilisé par le développeur. Ce langage a pris les devants dans la gestion des infrastructures, l'analyse des données ou le développement de logiciels.

Scikit-mutliflow : (également connu sous le nom de skmultiflow) bibliothèque dans python pour l'apprentissage automatique gratuite et open source pour les données multi-sorties/multi-étiquettes et de flux écrites en Python.

Pandas : bibliothèque dans Python permettant la manipulation de donnée et l'analyse des données. En particulier, il propose des structures de données et des opérations pour manipuler des tableaux de chiffres et des séries temporelles.

Matplotlib : bibliothèque destinée à tracer et visualiser des données sous formes des graphiques programmer en python.

3.2. Données utilisées pour l'expérimentation

3.2.1. Les Datasets d'évaluation des attaques DoS basé sur Deep learning

L'ensemble de données utilisé dans les travaux publiés de l'étude approfondie de la cybersécurité joue un rôle important dans la validation de toutes les approches DL proposées. Certains de ces ensembles de données ne sont pas facilement accessibles en raison de problèmes de confidentialité. Un ensemble de données conçu pour détecter une cyberattaque peut être [37]:

Table 3-2 : Collecte de données publies sur la cybersécurité

Dataset	Type	Etiqueté	Année
KDD99 [38]	Trafic du réseau	Oui	1999
NSL-KDD [39]	Trafic du réseau	Oui	2009
MAWI [40]	**Trafic internet**	Oui	2011
ISCX dataset [39]	Trafic du réseau	Oui	2012
CIC DoS dataset [39]	Trafic du réseau	Oui	2017
CIC DDoS[39]	Trafic du réseau	Oui	2019

3.2.2. Le dataset CICDDoS2019

L'ensemble de données utilisé dans cet travaille dans cette thèse dataset CICDDoS2019[41]. Cet ensemble de données ne contient que des attaques DDoS et un trafic bénin. Ils représentent de véritables données de flux réseau avec de nombreux types d'attaques DDOS parmi les plus récents et les plus connus. Ces données sont des formats plus condensés qui contiennent essentiellement des informations descriptives de connexion réseau où chaque donnée (chaque flux réseau) regroupe tous les paquets qui ont certaines caractéristiques dans la fenêtre temporelle et qui ne contiennent pas de charge utile. L'ensemble de données contient deux copies des données, des données PCAP [9] brutes et

[9] PCAP : packet capture

des données CSV. Les auteurs ont utilisé l'analyseur de trafic CICFlowMeter-V3 pour extraire fichiers PCAP, Les résultats ont été enregistrés dans des fichiers CSV classés structurés (type d'attaque) par l'Université du Nouveau-Brunswick[41].

L'ensemble de données comprend deux jours, le premier jour (03- 11-2019) où l'ensemble de données contenait 7 attaques DDOS différentes et à jour, l'ensemble de données complet contenait 19,750,116 instances, Parmi eux **55,678** trafic légitimes, tous les détails dans la

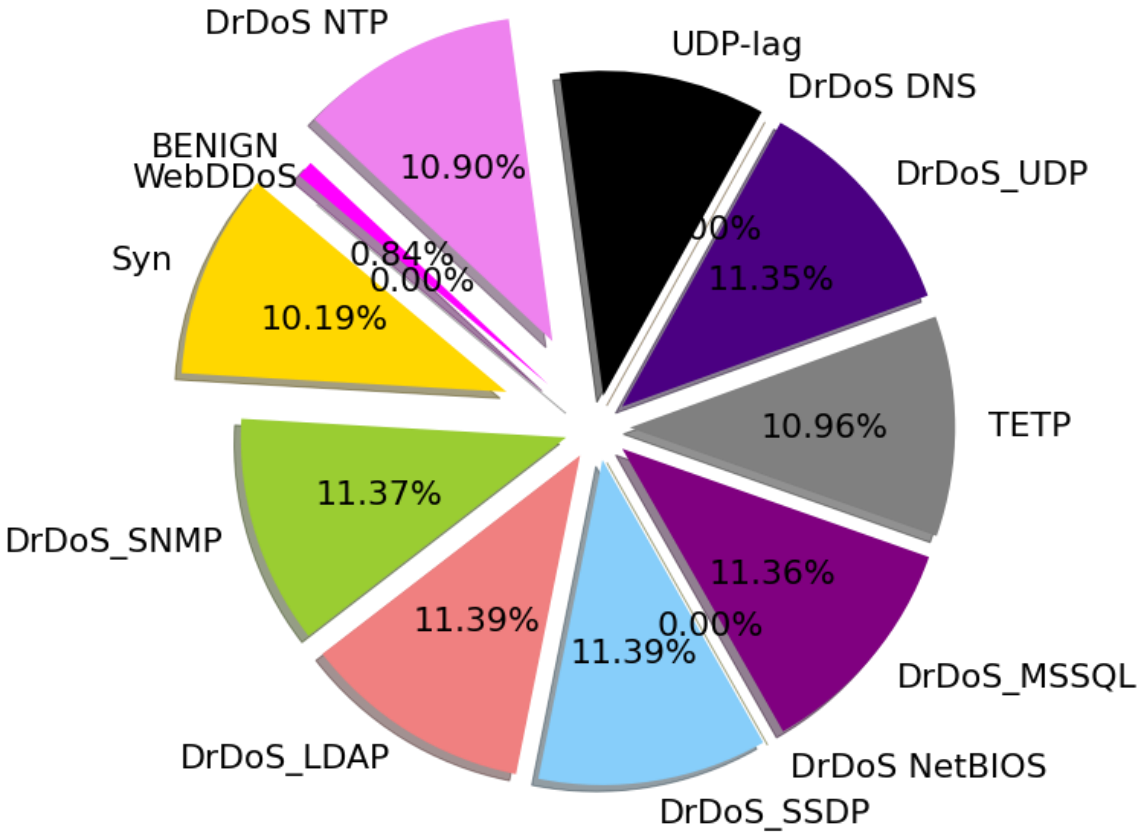


Figure 3-1: l'ensemble de donnée par pourcentage (jour 01-12-2019)

-
- Pourcentage de dataset CICDDoS2019 dans la (Figure 3-2 , Table 3-4)On note que l'attaque WebDDos est complètement nulle, donc dans notre travail, on prendra toutes les attaques qui ont un pourcentage inférieur à 0.001

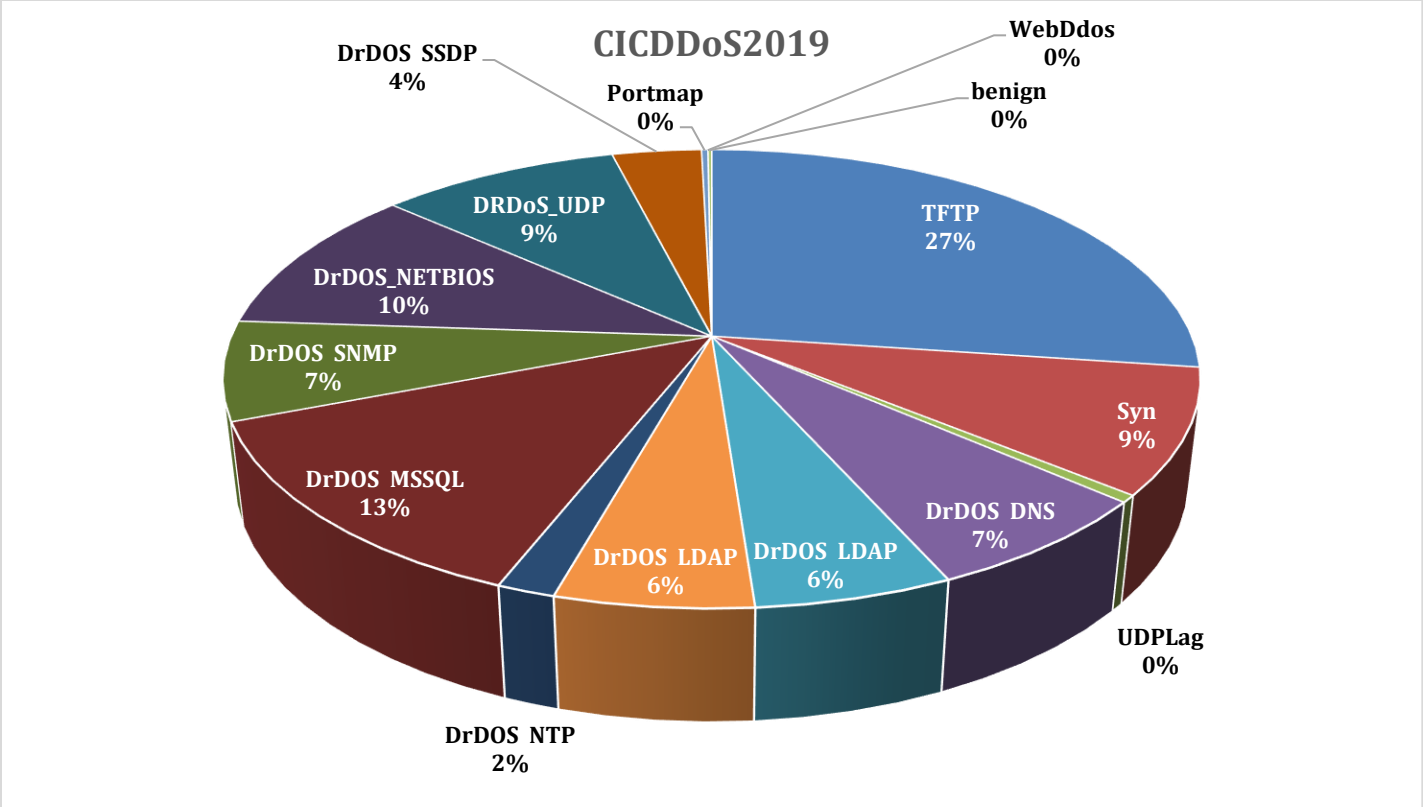


Figure 3-2 : pourcentage des attaques dans le dataset CICDDoS2019

Table 3-4 : Pourcentage de chaque type d'attaque dans le dataset

Type d'attaque	Nombre d'attaque	Pourcentage
TFTP	20,082,580	32.3587%
Syn	6,473,789	10.4311%
UDPLag	368,334	0.5935%
DrDOS DNS	5,071,011	8.1708%
DrDOS LDAP	4,085,121	6.5823%
DrDOS LDAP	4,085,121	6.5823%
DrDOS NTP	1,202,642	1.9378%
DrDOS MSSQL	9,706,754	15.6403%
DrDOS SNMP	5,159,870	8.3140%

DrDOS_NETBIOS	7,750,776	12.4887%
DRDoS_UDP	7,001,800	11.2819%
DrDOS SSDP	2,610,611	4.2064%
Portmap	186,960	0.3012%
WebDdos	439	0.0007%
Benign	112,541	0.1813%
Total :	62,062,452	100.0000%

Table 3-5 , Il contient 7 fichiers CSV , et aussi la deuxième jour (01- 12-2019) où l'ensemble de données contenait 12 attaques DDOS différentes et à jour, l'ensemble de données complet contenait 50062112 instances, Parmi eux 56863 trafic légitimes, tous les détail dans la Table 3-3 , et contient 11 fichiers CSV ,l'ensemble de données contient également 86 caractéristiques (Features) que nous avons montré dans Figure 3-4 qui montre la relation de chaque colonne à l'autre, et avec cela, donc âpre traitement nous avons quatre sous-ensembles.

Table 3-3 : l'ensemble de donnée (jour 01-12-2019)

Fichier(csv)	Nombre de lignes	Type d'attaque	Nombre d'occurrences
Syn	1582681	Syn	1582289
		BENIGN	392
TFTP	20107827	TFTP	20082580
		BENIGN	25247
UDPLag	370605	UDP-lag	366461
		BENIGN	3705
		WebDDos	439
DrDoS _DNS	5074413	DrDoS DNS:	5071011
		BENIGN	3402
DrDoS _LDAP	2181542	DrDoS LDAP	2179930

		BENIGN	1612
DrDoS_MSSQL	4524498	DrDoS_MSSQL	4522492
		BENIGN	2006
DrDoS_NTP	1217007	DrDoS_NTP	1202642
		BENIGN	14365
DrDoS_NETBIOS	4093986	DrDoS_NETBIOS	4093279
		BENIGN	1707
DrDoS_SNMP	5161377	DrDoS_SNMP	5159870
		BENIGN	1507
DrDoS_SSDP	2611374	DrDoS_SSDP	2610611
		BENIGN	763
DrDoS_UDP	3136802	DrDoS_UDP	3134645
		BENIGN	2157
Total :	50,062,112	BENIGN	56,863
		12 - Attaque	50,005,249

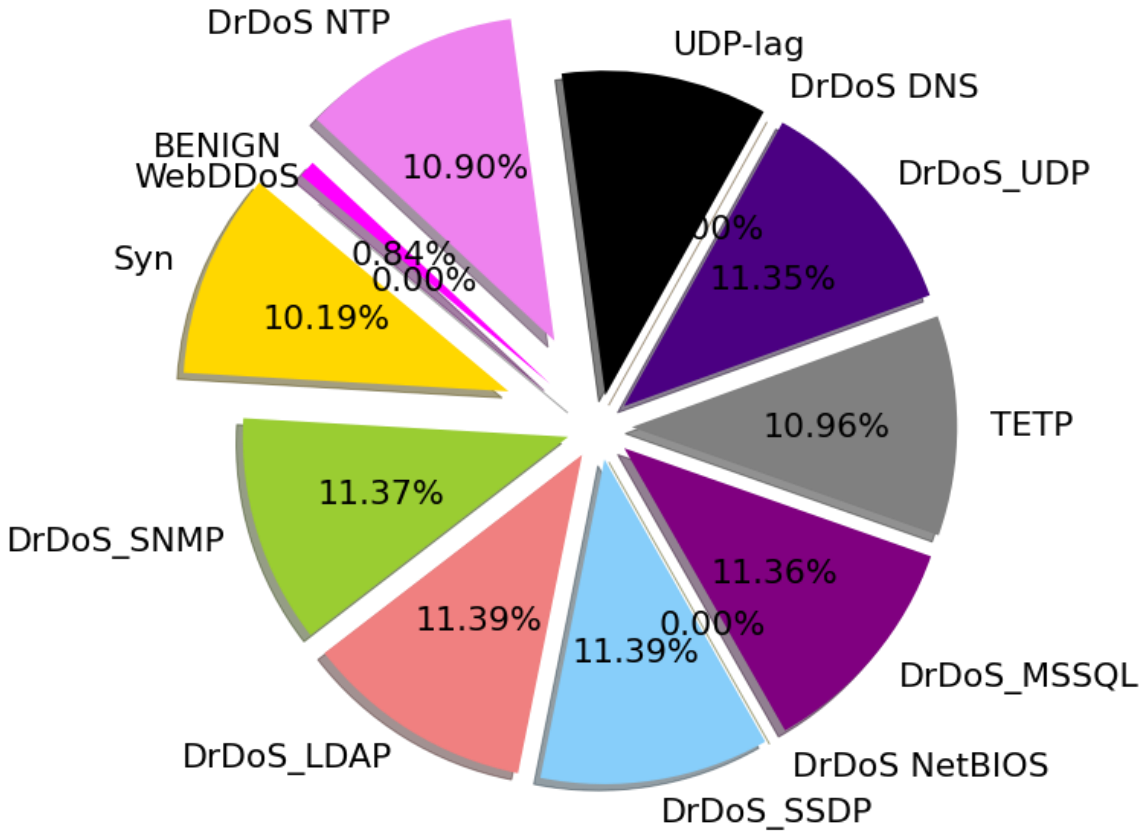


Figure 3-1: l'ensemble de donnée par pourcentage (jour 01-12-2019)

- Pourcentage de dataset CICDDoS2019 dans la (Figure 3-2 , Table 3-4)On note que l'attaque WebDDos est complètement nulle, donc dans notre travail, on prendra toutes les attaques qui ont un pourcentage inférieur à 0.001

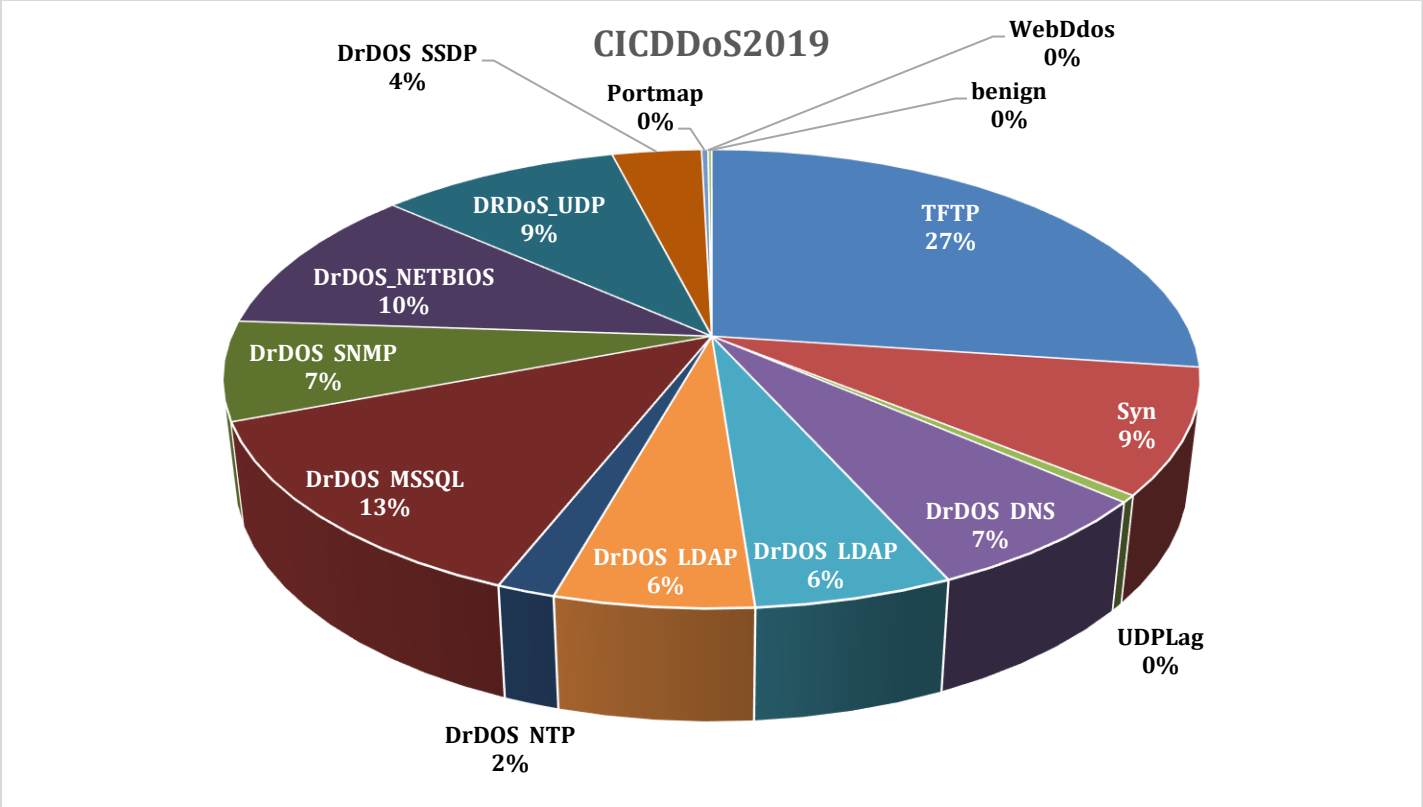


Figure 3-2 : pourcentage des attaques dans le dataset CICDDoS2019

Table 3-4 : Pourcentage de chaque type d'attaque dans le dataset

Type d'attaque	Nombre d'attaque	Pourcentage
TFTP	20,082,580	32.3587%
Syn	6,473,789	10.4311%
UDPLag	368,334	0.5935%
DrDOS DNS	5,071,011	8.1708%
DrDOS LDAP	4,085,121	6.5823%
DrDOS LDAP	4,085,121	6.5823%
DrDOS NTP	1,202,642	1.9378%
DrDOS MSSQL	9,706,754	15.6403%
DrDOS SNMP	5,159,870	8.3140%
DrDOS_NETBIOS	7,750,776	12.4887%

DRDoS_UDP	7,001,800	11.2819%
DrDOS SSDP	2,610,611	4.2064%
Portmap	186,960	0.3012%
WebDdos	439	0.0007%
Benign	112,541	0.1813%
Total :	62,062,452	100.0000%

Table 3-5 : l'ensemble de donnée (Jour 03-11 -2019)

Fichier(csv)	Nombre de lignes	Type d'attaque	Nombre d'occurrences
Syn	4320541	Syn	4284751
		BENIGN	35790
UDPLag	725165	UDPlag	1873
		BENIGN	4068
		UDP	112475
		Syn	606749
LDAP	2113234	LDAP	1905191
		BENIGN	5124
		NetBios	202919
MSSQL	5161377	MSSQL	5159870
		BENIGN	1507
NETBIOS	3455899	NETBIOS	3454578
		BENIGN	1321
Portmap	191694	Portmap	186960
		BENIGN	4734
UDP	3782206	UDP	3754680
		MSSQL	24392
		BENIGN	3134
Total :	19,750,116	BENIGN :	55,678
		7- Attaque	19,694,438

Deux classes principales figurent dans ce dataset, les accès de type **Bénin** (Traffic légitime) et les **Attaques**, deux types d'attaques **DDoS** sont capturés dans cet ensemble de données.

Le premier est DDoS basé sur la réflexion, y compris MSSQL, SSDP, NTP, TFTP, DNS, LDAP, NetBIOS et SNMP. Dans ce type d'attaque, les véritables attaquants peuvent se cacher derrière les clients légitimes et les utiliser dans une attaque. Cela rend les victimes plus difficiles à différencier les utilisateurs et les attaquants uniquement par la source. Ces attaques sont basées sur les protocoles TCP (MSSQL et SSDP), UDP (NTP et TFTP) ou les deux protocoles (DNS, LDAP, NETBIOS et SNMP).

Le second sont les attaques basées sur l'exploitation, y compris SYN flood, UDP flood et l'UDP-Lag. Ce type d'attaque usurpera l'adresse IP source et enverra un grand nombre de paquets au serveur victime. Cela entraînera l'épuisement des ressources de la victime. Dans la Figure 3-3 explique les deux types attaque base sur l'exploitation et attaque base sur réflexion.

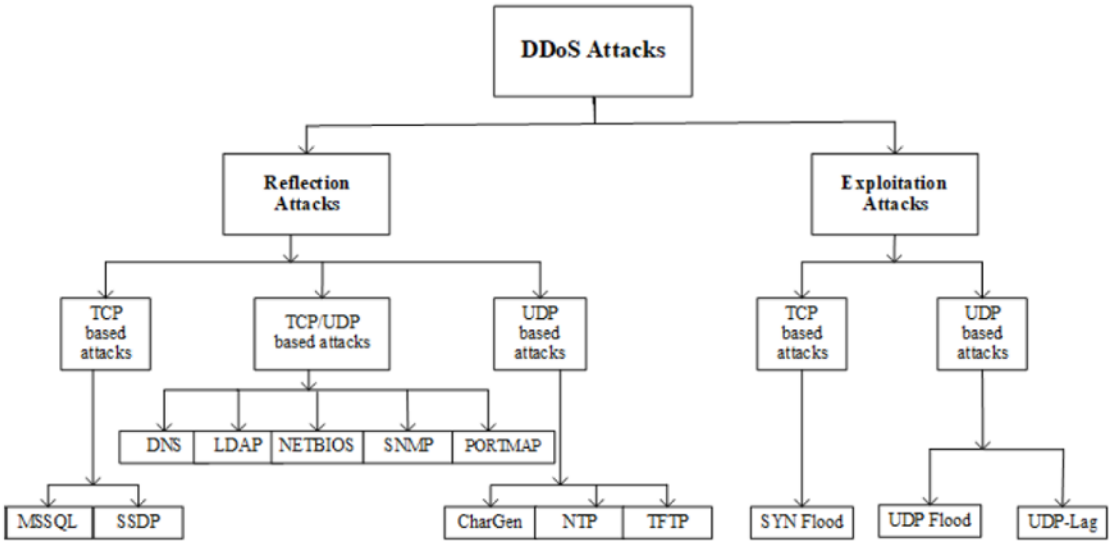


Figure 3-3 : les attaques par réflexion et les attaques par l'exploitation[41]

SYN : SYN flood, Il vise à consommer toutes les ressources du serveur et à rendre le serveur indisponible. L'attaquant envoie constamment une demande de connexion (SYN) au serveur de la victime mais ne répond pas à un ACK du serveur de la victime. Cette

utilisation de TCP restera une connexion semi-ouverte pendant un certain temps, et tous les ports deviendront indisponibles [42].

SSDP: Simple Service Discovery Protocol (SSDP). Il s'agit d'un type d'attaques DDoS par réflexion. L'attaque SSDP DDoS envoie un flux de trafic amplifié au serveur de la victime. Il exploite les protocoles réseau Universal Plug and Play (UPnP). Cette attaque peut submerger l'infrastructure de la cible et mettre ses ressources Web hors ligne[43], [44].

NTP : Network Time Protocol (NTP) , est un type de protocole utilisé pour synchroniser les horloges via Internet. L'amplification NTP utilise des serveurs NTP pour submerger la cible avec le trafic UDP. L'attaquant envoie généralement des requêtes aux serveurs NTP en usurpant l'adresse IP, qui appartient aux victimes[45].

DNS : L'attaque DNS est un type d'attaque DDoS par amplification qui exploite les serveurs de noms de domaine et épuise la bande passante des victimes. Cette attaque peut submerger les victimes et les rendre inaccessibles. Les attaques DNS peuvent être facilement lancées par des bots[46].

NetBIOS: Network Basic Input/Output System. Cette attaque est basée sur UDP. Permet aux attaquants de voir les informations de mémoire de l'ordinateur de la victime sur le réseau[47] .

MSSQL : MSSQL signifie Microsoft SQL. Les attaquants se font passer pour Microsoft SQL Server et envoient des réponses aux victimes. Il abuse du protocole de résolution Microsoft SQL Server et usurpe l'adresse IP du serveur MS SQL [48].

TFTP : L'attaque TFTP est un type d'attaque DDoS par amplification basée sur le protocole Trivial File Transfer Protocol (TFTP). Le facteur d'amplification peut atteindre jusqu'à 60. Un serveur TFTP est normalement utilisé pour stocker les images des appareils et les fichiers de configuration. TFTP est un protocole sans état et n'a pas de méthodes d'authentification, ce qui le rend plus facile à lancer et plus difficile à détecter [49].

SNMP : Simple Network Management Protocol est un protocole de gestion de réseau utilisé pour configurer et collecter des informations à partir de périphériques réseau. Lors d'une attaque par réflexion SNMP, les attaquants envoient un grand nombre de requêtes

SNMP à l'aide d'une adresse IP usurpée appartenant à la victime. Après cela, les serveurs SNMP répondront à l'adresse IP de la victime [50] .

UDP : UDP flood, User Datagram Protocol (UDP), pour lancer des attaques. L'attaquant envoie une grande quantité de paquets UDP au port du serveur victime avec une adresse IP usurpée. Si aucun programme n'est en cours d'exécution sur ce port, le serveur victime enverra un paquet ICMP pour le rappeler à l'expéditeur. Cependant, l'adresse IP source est inaccessible et le serveur victime ne recevra jamais de réponse. En faisant cela, les ports du serveur victime seront épuisés[51] .

UDP-Lag: L'attaque UDP-Lag est une sorte d'attaque qui perturbe la connexion entre le client et le serveur. Cette attaque est principalement utilisée dans les jeux en ligne. Cette attaque peut rendre la connexion UDP plus lente que la normale. Cela pourrait être un problème sérieux lorsque le serveur nécessite un court délai [4].

LDAP: Lightweight Directory Access Protocol. Il s'agit d'un type d'attaque DDOS par amplification, dans laquelle le facteur d'amplification peut aller jusqu'à 55[61]. LDAP est principalement utilisé dans les réseaux d'entreprise, c'est la raison pour laquelle il est largement utilisé pour attaquer les réseaux d'entreprise[52]

- **Les types des colonnes dans le dataset CICDDoS2019** :

  Nous leur expliquerons des mots spéciaux

  FWD (Forword) : direction vers l'avant

  BWD (backword) : direction sens inverse

  STD (standard deviation) : déviation normative

  IAT (Time between tow package) : Temps entre le paquet de remorquage

  Bulk avg : Moyenne d’information collectée

  Idle : temps de flux inactive

Les flags (psh, urg ….) : cette un protocole(pour activer cette protocole ou non)

Toutes les colonnes d'une type Object il va changer la type âpre le traitement

Objet : Flow ID--Source ip--Destination ip--Timestamp--SimillarHTTP—Label

Float64:

total Length of Fwd Packet -- total Length of Bwd Packet -- Fwd Packet Length Min -- Fwd Packet Length Max -- Fwd Packet Length Mean -- Fwd Packet Length Std -- Bwd Packet Length Min -- Bwd Packet Length Max -- Bwd Packet Length Mean -- Bwd Packet Length Std -- Flow Bytes/s -- Flow Packets/s -- Flow IAT Mean -- Flow IAT Max -- Flow IAT Min -- Fwd IAT Max -- Fwd IAT Mean -- Fwd IAT Total -- Fwd IAT Std -- Bwd IAT Min -- Bwd IAT Max -- Bwd IAT Mean -- FWD Packets/s -- Bwd Packets/s -- Packet Length Mean -- Packet Length Std -- Packet Length Max -- Packet Length Variance -- Idle Mean -- Idle Max -- Fwd IAT Min -- Average Packet Size -- down/Up Ratio -- Active Mean -- Active Min -- Idle Std -- Active Max -- Active Std -- Idle Min

Int64:

Source Port--Destination port--Bwd Segment Size Avg--Fwd Bytes/Bulk Avg--Fwd Packet/Bulk Avg--Fwd Bulk Rate Avg--Bwd Bytes/Bulk Avg--Bwd Packet/Bulk Avg--Bwd Bulk Rate Avg--Subflow Fwd Bytes--Subflow Bwd Packets--Subflow Bwd Bytes--Fwd Init Win bytes--Bwd Init Win bytes--Fwd Act Data Pkts--Fwd Seg Size Min--PSH Flag Count--ACK Flag Count--Inbound--ECE Flag Count--Fwd Segment Size Avg--RST Flag Count--Protocol--Flow duration--Fwd URG Flags--Bwd URG Flags--Fwd Header Length--Bwd Header Length--FIN Flag Count--SYN Flag Count--Bwd PSH Flags--Fwd PSH flags--Bwd IAT Total--Bwd IAT Std--CWR Flag Count--total Fwd Packet--Flow IAT Std--total Bwd packets--URG Flag Count

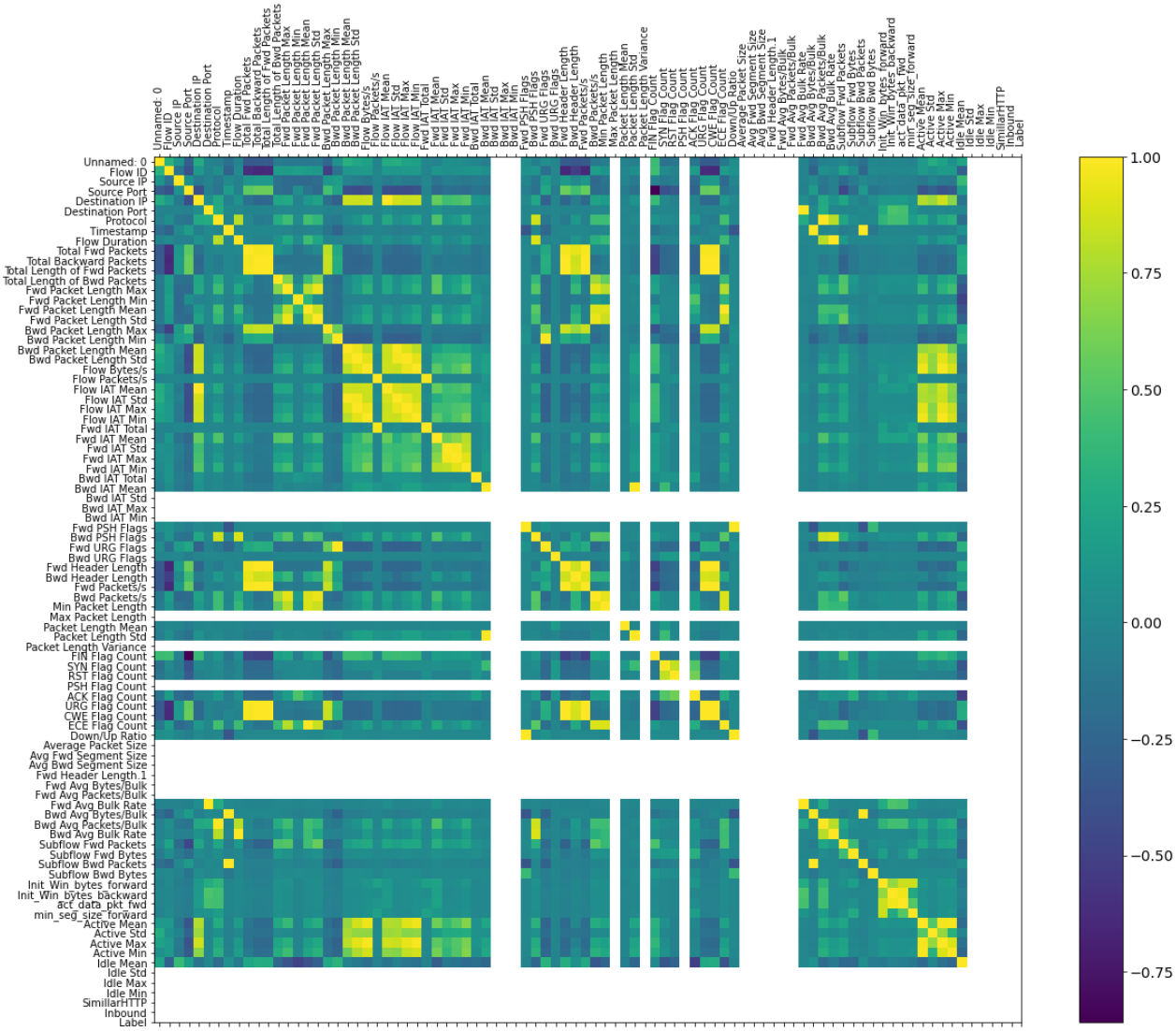


Figure 3-4 : Matrice de confusion par les colonnes

3.2.3. Prétraitements et normalisation des données

3.2.3.1. Uniformisation des étiquettes

Comme indiqué dans les tableaux , Les données sont extraites de manière aléatoire de l'ensemble de données CICDDoS2019 [41] réelles, Pour la transparence de l'expérience et pour ne pas altérer l'ensemble de données , Et c'est en le choisissant en fonction du jour dans la première expérience et en le mélangeant dans la deuxième expérience en augmentant au maximum le nombre d'attaques DDoS , et pour le rendre plus réaliste, nous avons pris le pourcentage de présence de chaque attaque et lui a appliqué le même travail.

Ainsi, par criblage, nous avons extrait trois groupes de données, la première sous-ensembles 1 dans la Table 3-6 Nous avons remplacé tous les types d'attaques existants par attaque et Benign (trafic légitime) et la deuxième sous-ensembles 2 dans la Table 3-7 le ensembles 2 nous l'avons pris le fichier dans le jour (03-11-2019), retrouver toutes les informations sur Table 3-5 et la troisième sous-ensembles 3 dans la Table 3-8 le ensemble 3 nous l'avons pris le fichier dans le jour (01-12-2019), retrouver toutes les informations sur Table 3-3 et le quatrième nous avons collecté toutes les informations des deux jours et extrait un ensemble de données qui comprend toutes les attaques disponibles dans cicddos2019, puis le pourcentage de chaque type de cyberattaque a été calculé. Nous avons extrait 2 % du total, nous allons extraire les données suivantes Positionner

Table 3-6 : Sous ensembles 1 (2 classes)

	Les Classes	**Nb d'instances pour L'apprentissage**	**Nbr d'instances pour le Test**
Dataset_1 (2-Classes)	BENIGN	2,301,741	575,362
	Attaque	11,599	2,973

Table 3-7 : Sous ensembles 2 (8 classes)

	Les Classes	**Nb d'instances pour L'apprentissage**	**Nbr d'instances pour le Test**
Dataset_2 (8-Classes)	**BENIGN**	11,453	2,783
	LDAP	263,332	70,641
	Portmap	149,404	37,556
	Syn	544,632	137,041
	MSSQL	331,248	82,497
	UDP	389,303	97,038
	NetBIOS	482,474	120,401

	UDP-lag	301,48	79,487

Table 3-8 : Sous ensembles 3 (13 classes)

	Les Classes	Nb d'instances pour L'apprentissage	Nbr d'instances pour le Test
Dataset_3 (13-Classes)	BENIGN	56795	Stratifié avec 25 % des données d'apprentissage a été utilisé pour éviter l'erreur d'échantillonnage du pourcentage de données déséquilibrées et également pour garantir que les données d'apprentissage et de test avaient le même pourcentage fractionné pour chaque classe.
	DrDoS_LDAP	100,000	
	DrDoS_SSDP	100,000	
	DrDoS_UDP	100,000	
	DrDoS_DNS	100,000	
	DrDoS_MSSQL	100,000	
	DrDoS_NetBIOS	100,000	
	DrDoS_SNMP	100,000	
	Syn	100,000	
	DrDoS_NTP	100,000	
	UDP-lag	100,000	
	TFTP	100,000	
	WebDDoS	439	

- **Pour cette expérience qui s'appelait l'expérimentation 4**, nous avons combiné les deux jours ensemble pour détecter autant d'attaques que possible dans cet ensemble de données CICDDoS2019, et avons également modifié les étiquettes de classe de données comme suit :

Table 3-9 : Modifier des étiquettes par classe

Les classes	Modifier des étiquettes des classes
LDAP	DrDoS_LDAP
MSSQL	DrDoS_MSSQL
NetBIOS	DrDoS_NetBIOS
UDP	DrDoS_UDP

Table 3-10 : Sous ensembles 4 (14 classes)

	Les Classes	**Nb d'instances pour L'apprentissage**	**Nbr d'instances pour le Test**
Dataset_4 (14-Classes)	BENIGN	1813	Stratifié avec 25 % des données d'apprentissage a été utilisé pour éviter l'erreur d'échantillonnage du pourcentage de données déséquilibrées et également pour garantir que les données d'apprentissage et de test avaient le même pourcentage fractionné pour chaque classe.
	DrDoS_LDAP	65823	
	DrDoS_SSDP	42064	
	DrDoS_UDP	112819	
	DrDoS_DNS	81708	
	DrDoS_MSSQL	156403	
	DrDoS_NetBIOS	124887	
	DrDoS_SNMP	83140	
	Syn	1043011	
	DrDoS_NTP	19378	
	UDP-lag	5935	
	TFTP	323587	
	WebDDoS	439	
	Portmap	3012	

3.2.3.2. Prétraitement de données

Afin de construire un modèle précis et d'obtenir les meilleurs résultats, il est très important d'effectuer des analyses exploratoires sur l'ensemble de données et ses caractéristiques. L'ensemble de données est traité avant d'être appliqué au réseau neuronal profond. Nous avons terminé les étapes de traitement suivantes :

- Nous avons effectué une enquête sur les données pour supprimer toutes les lignes en double et indésirables, qu'il ne s'agisse pas d'un nombre "**NAN**" (pas un nombre) ou d'un nombre infini "**INF**" (valeur infinie) , nous l'avons supprimé car il manque des données et ne nous aidera pas dans le processus d'apprentissage automatique, et il a été supprimé car l'ensemble de données dont nous disposons est trop volumineux et nous ne l'utilisons pas pleinement pour l'apprentissage.
- Dans deuxième, après avoir fait les statistiques pour chaque colonne résumant la dispersion et la distribution de l'ensemble de données à la présence d'une colonne vide (dont la valeur est toujours 0 ou 1) dans toutes les attaques, ces caractéristiques ne contiennent aucune information discriminatoire permettant l'attaque classes à distinguer les unes des autres

Les colonnes sont,**' Fwd URG Flags',' Bwd URG Flags','FIN Flag Count',' PSH Flag Count',' ECE Flag Count', ' Bwd PSH Flags','Fwd Avg Bytes/Bulk',' Fwd Avg Packets/Bulk',' Fwd Avg Bulk Rate',' Bwd Avg Bytes/Bulk', ' Bwd Avg Packets/Bulk','Bwd Avg Bulk Rate',** Qui ont été supprimés car ils se sont installés à 0 ou 1 (Figure 3-5)dans toutes les attaques

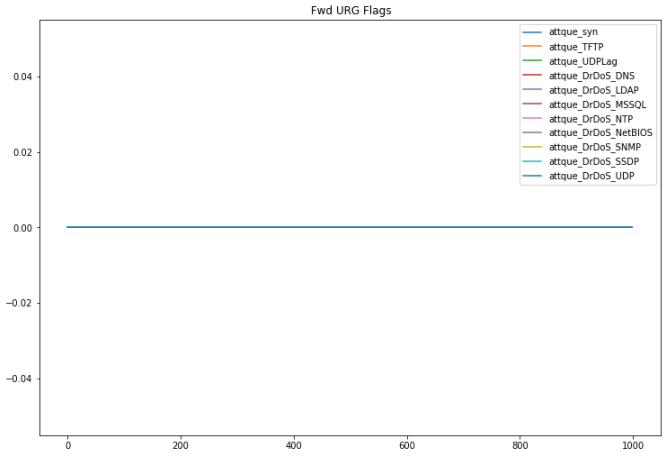


Figure 3-5 : exemple pour colonne supprimer (stabilise a 0)

Dans le troisième étape, d'autres colonnes catégorielles ont été supprimées de " **'Flow ID** ", " **Source IP** ", " **Destination IP** ", " **Timestamp** ", "**Inbound**" et ces propriétés sont liées aux informations de contact et ne représentent pas des caractéristiques importantes des attaques,

Lors de la dernière étape, nous avons traité toutes les lignes dans tous les fichiers il a été conclu qu'il y a des lignes impaires au taux de 1/100000 dans lignes nous l'avons supprimé et avec cela, nous avons terminé notre travail en termes de prétraitement de donnes et nous passerons à la normalisation des données

3.2.3.3. Normalisation des données

La normalisation des données est généralement requise lorsque les chercheurs appliquent des techniques d'apprentissage en profondeur à des données qui ont des échelles différentes sur les attributs, Nous avons recherché une comparaison des performances du modèle avec ou sans la normalisation des traits effectuée par Wang et al [53], Les modèles discriminatoires gagnent en efficacité

Dans cette travaille, les imitateurs sont StandardScaler et MinMaxScaler .

La fonction de mappage StandardScaler est illustrée dans.Equation 3-1

$$f'_{:,i} = \frac{f_{:,i} - \text{mean}\left(f_{:,i}\right)}{\text{std}\left(f_{:,i}\right)}$$

Equation 3-1 : StandardScaler

La fonction de mappage MinMaxScaler est illustrée dans.Equation 3-2

$$f'_{:,i} = \frac{f_{:,i} - min\left(f_{:,i}\right)}{max\left(f_{:,i}\right) - min\left(f_{:,i}\right)}$$

Equation 3-2 : MinMaxScaler

Puisque nous avons des nombres négatifs dans l'ensemble de donnée alore l'équation de StandardScaler ressaie toujours de mettre à l'échelle toutes les données dans une distribution normale avec une moyenne de zéro et un écart type d'un. Cela ferait tomber 50% des données dans la plage négative. Dans ce cas, MinMaxScaler fait un meilleur.[53]

3.2.4. L'Architecture de modèle et Model proposé

Nous avons mis en œuvre la méthode de réseau profond CNN, après quoi les méthodes ont été modifiées et améliorées en essayant plusieurs combinaisons de plusieurs paramètres, nous expliquerons certaines de ses caractéristiques adoptées dans ce travail :

Les couches d'entrée ont des dimensions (le nombre de neurones) comme le nombre d'entités (Features) dans le vecteur d'entrée

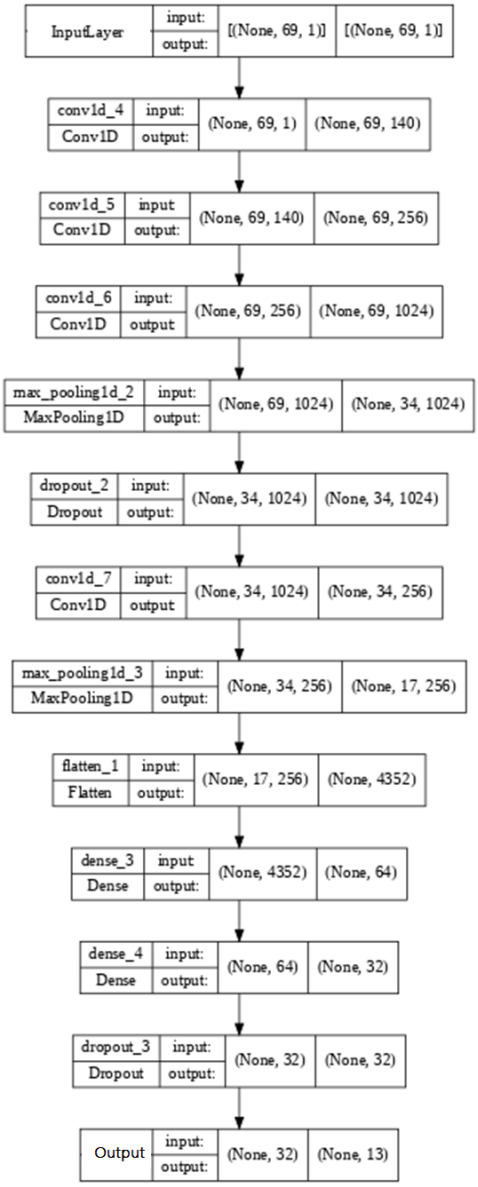
• La fonction d'activation utilisée était ReLU, différentes autres fonctions comme tanh et sigmoid ont été expérimentées, mais le ReLU a toujours les meilleurs résultats.

• Les couches de sortie ont les mêmes dimensions que le nombre de classes, et la fonction d'activation "Softmax" est choisie pour la classification multicouche. Il donne une probabilité (dont la somme est égale à 1) pour la sortie, nous l'avons donc utilisé dans la dernière étape pour la plus grande probabilité et pour faire de la catégorie associée l'affinité attendue

• De plus, la technologie dropout a été utilisée, lorsqu'on tombe au problème de sur-apprentissage (Overfitting), Afin de produire un modèle généralisable, cette approche considère une fraction de neurones en pourcentage.

- La fonction de perte (Loss function) était par deux techniques :
  " **categorical-cross-entropy** " pour la classification multi-classes
  " **binary-cross-entropy** " pour la classification binaire (normale/Attaque).

- Pour L'optimiseur utilise " Adam" avec un taux d'apprentissage (Learning Rate) de 0.001, Cette technique vous montrera comment mettre à jour les pondérations du réseau neuronal pour réduire les pertes, permettant au modèle de converger rapidement et de faire de meilleures prédictions avec moins d'erreurs.
- Ensuite, La technique d'optimisation "Adam" vous indiquera comment mettre à jour les poids d'un réseau de neurones pour réduire les pertes, permettant au modèle de converger rapidement et de faire de meilleures prédictions avec le moins d'erreurs.



Model: "sequential"

Layer (type)	Output Shape	Param #
conv1d (Conv1D)	(None, 69, 140)	840
conv1d_1 (Conv1D)	(None, 69, 256)	107776
conv1d_2 (Conv1D)	(None, 69, 1024)	525312
max_pooling1d (MaxPooling1D)	(None, 34, 1024)	0
dropout (Dropout)	(None, 34, 1024)	0
conv1d_3 (Conv1D)	(None, 34, 256)	786688
max_pooling1d_1 (MaxPooling1D)	(None, 17, 256)	0
flatten (Flatten)	(None, 4352)	0
dense (Dense)	(None, 64)	278592
dense_1 (Dense)	(None, 32)	2080
dropout_1 (Dropout)	(None, 32)	0
dense_2 (Dense)	(None, 13)	495

Total params: 1,701,783
Trainable params: 1,701,783
Non-trainable params: 0

Figure 3-6 : le modèle Cnn utilisé pour 13-Class classification

Les CNN 1D ont d'abord été étudiés en utilisant des couches de convolution 1D pour le traitement du langage naturel[54] . Les événements de trafic réseau sont représentés sous forme de données de séries chronologiques 1D dans notre recherche. Les caractéristiques de flux sont recueillies sur des périodes similaires, mais des millions de connexions bénignes et d'attaques DDoS malveillantes se comportent différemment. En conséquence, nous avons utilisé CNN 1d pour extraire les caractéristiques de discrimination spatiale..

Pour découvrir les paramètres appropriés et une meilleure topologie de réseau, nous avons commencé avec un CNN de taille moyenne avec différents nombres de couches convolutives et un nombre varié de filtres (16, 32,64, ,256 et 1024) avec des longueurs de 5, 3 et 2 pour les couches de convolution.

la Figure 3-6 La figure 1 montre l'évaluation de la précision des modèles CNN en utilisant de nombreuses couches convolutives choisies par expérience. En général, plus nous utilisons de couches convolutives, plus la précision est élevée, mais après deux ou trois couches, l'amélioration de la précision est plutôt stable et il faut un beaucoup de temps pour apprendre. Ce qui se passera dans nos prochains travaux est d'améliorer l'environnement d'exécution.

L’architecture du CNN utilisée dans cette étude est illustrée dans la Figure 3-6 a. elle est composée de 3 couches de convolution 1D pour la debut pour démarrer le modèle car la profondeur (Input = 69) de cette étude est très faible par rapport à d'autres projets d'apprentissage en profondeur, une couche Maxpooling 1D apre cochee convolution 1D et Maxpooling 1D et 4 couches entièrement connectées. Le CNN commence avec une convolution 1D, le modèle nécessite une entrée tridimensionnelle. [batch_shape, steps, features], l’input-shape dans notre modèle c’est (None, 1, 69), ce modèle va accepter n’importe quel batch_shape avec des séquences de longueur 1 et une vecteur d’entrée de 69 colones.

Les 3 couches de convolution ont des nombres de filtres variés de différentes tailles, ils ont le **Padding same** pour conserver la même taille des cartes de caractéristiques d’entrées, l’opération de convolution 1D utilisant plusieurs filtres nous donne une carte de caractéristiques applées (Features map), ensuite, chaque couche convolution 1D et Maxpooling 1D appliquée la fonction d’activation **ReLU** .

une couche de **Dropout** est utilisée afin pour éviter le sur-apprentissage (Overfitting) . La dernière couche contient la fonction **Soft-max** qui donne la distribution de probabilité sur chaque classe. pour optimiser la reseau utlisée ”**Adam** “ .

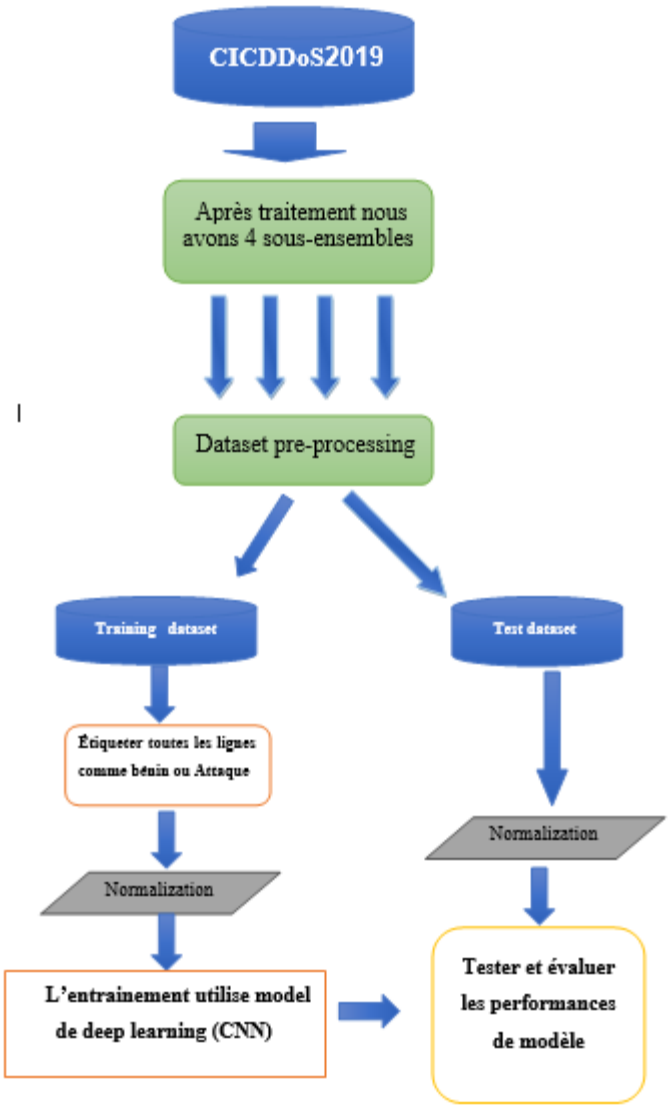


Figure 3-7 : Schéma conceptuel de notre méthode d'implémentation DL

3.3. Résultats et Discussion

Nous avons implémenté un modèle d'apprentissage en profondeur CNN utilisant. Ces modèles ont été formés et testés sur 4 sous-ensembles de données différentes du CICDDoS2019 Dataset.

Plusieurs tests ont été faits afin d'obtenir les bonnes Hyperparamètres pour chaque modèle. Ces paramètres ne peuvent pas ajuster durant la phase de l'apprentissage, pourtant qu'ils ont un grand impact sur les performances des modèles durant l'apprentissage. Ils comprennent les variables qui

déterminent la structure du réseau (Nbr de neurones, Nbr de couches, fonction d'activation, . . .), le lot d'échantillons (Batch Size) et le nombre d'itérations . . .etc.

Lorsqu' on arrive à un bon modèle avec le minimum de taux d'erreur et le maximum d'exactitude, nous avons ensuite testé ce modèle sur le sous-ensemble de test. Les résultats sont présentés dans les figures ci-dessus 4.5.

3.3.1. Les mesures d'évaluation du modèle

Pour évaluer notre modèle, nous avons utilisé la matrice de confusion :

3.3.1.1. La matrice de confusion

Une matrice de confusion est un tableau qui est utilisé pour définir la performance d'un algorithme de classification. Elle permet de visualiser et de résumer les performances d'un algorithme de classification. Chaque colonne de la matrice représente les instances d'une classe réelle, tandis que chaque ligne représente les instances d'une classe prédite [55] comme le montre la Figure 3-8

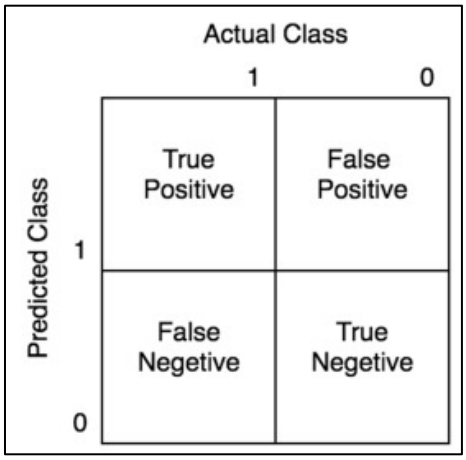


Figure 3-8 : Matrice de confusion

- True positive (TP) : Un résultat de test qui indique correctement la présence d'une condition ou d'une caractéristique.
- False positive (FP) : Un résultat de test qui indique à faux qu'une condition ou un attribut particulier est présent.

- True negative (TN) : Un résultat de test qui indique correctement l'absence d'une condition ou d'une caractéristique.
- False negative (FN) : Un résultat de test qui indique à faux qu'une condition ou un attribut particulier est absent.

3.3.1.2. Mesures de performance de la classification

Les mesures de performance d'un algorithme de classification sont accuracy, precision, recall et F1 score, qui sont calculés sur la base des valeurs TP, TN, FP et FN mentionnées précédemment [55]:

- Accuracy (ACC) : donne la proportion du nombre total de prédictions qui étaient correctes :

$$ACC = \frac{TP+TN}{TP+TN+FP+FN} \quad \text{..... (1)}$$

- Precision : ou the positive prédictive value (PPV), est la proportion de valeurs positives par rapport au total des instances positives prédites. En d'autres termes, la précision est la proportion de valeurs positives qui ont été correctement identifiées :

$$PPV = \frac{TP}{TP+FP} \quad \text{..... (2)}$$

- Recall : appelée aussi Sensitivité ou true positive rate (TPR) est la proportion de valeurs positives par rapport au total des cas positifs réels :

$$TPR = \frac{TP}{TP+FN} \text{..... (3)}$$

- F1 score : est la moyenne harmonique de la precision et le recall :

$$F1\ score = 2 \times \frac{PPV \times TPR}{PPV+TPR} = \frac{2TP}{2TP+FP+FN} \text{..... (4)}$$

Les modèles de base utilisés pour la comparaison Les auteurs [55] ont testé 4 algorithmes de machine learning communs à partir des données d'entraînement (Training Data) et de test (Test Data) des CICDDoS_2019 Dataset afin de servir comme référence de base pour une étude comparative. Ils ont commencé par la sélection des caractéristiques les plus importantes à l'aide

de la bibliothèque SKLearn, après ils ont choisi 4 algorithmes ML les plus communs : ID3 (Decision Tree), Random forest, Naive Bayes, et Logistic Regression. Les mesures d'évaluation ainsi que les résultats obtenus sont illustrées dans le tableau Table 3-16

3.3.2. Les modèles de base utilisés pour la comparaison

Les auteurs ont testé, l'apprentissage automatique en utilisant 4 **(**ID3 (Decision Tree), Random forest, Naive Bayes, et Logistic Regression**)** algorithmes communs et l'autre en utilisant l'apprentissage en profondeur (**CNN**, **RNN**, **DNN**) sur l'ensemble de données cicddos2019, composé de trafic réel pour servir de référence pour la comparaison, les échelles de notation extraites par eux sont présentées dans le **Table 3-11:**

Table 3-11 : Comparaison des résultats du machine learning et du deep learning

Méthode	Precision	Recall	f1-score
DNN	0.85	0.83	0.82
CNN	0.91	0.90	0.89
RNN	0.78	0.89	0.88
ID3	0.78	0.65	0.69
Random Forest	0.77	0.56	0.62
Naive Beyes	0,41	0,11	0,05
Logistic Regresion	0,25	0,02	0,04

Les précisions de la détection des attaques DDoS model propose de CNN pour les 4 expérimentations ont été illustrées dans le Table 3-16.

3.3.3. Résultat

- **Dans la première expérimentation (classification binaire) :** a été réalisée sur le sous-ensemble de données de l'ensemble de données CICDDoS2019 présenté dans le tableau Table 3-6. Les modèles sont évalués directement sur l'ensemble de test. Le modèle Cnn est formé sur 50 itérations, nous voyons les précisions de formation et de validation augmenter du début à la fin, atteignant une valeur maximale, tendant vers 1. Nous remarquons également que la valeur de la perte chute fortement au cours de l'entraînement et de l'évaluation et atteint une

valeur où le minimum tend vers 0. Cela signifie que ces modèles apprennent mieux et font de meilleures prédictions après chaque période d'amélioration (Figure **3-9**)

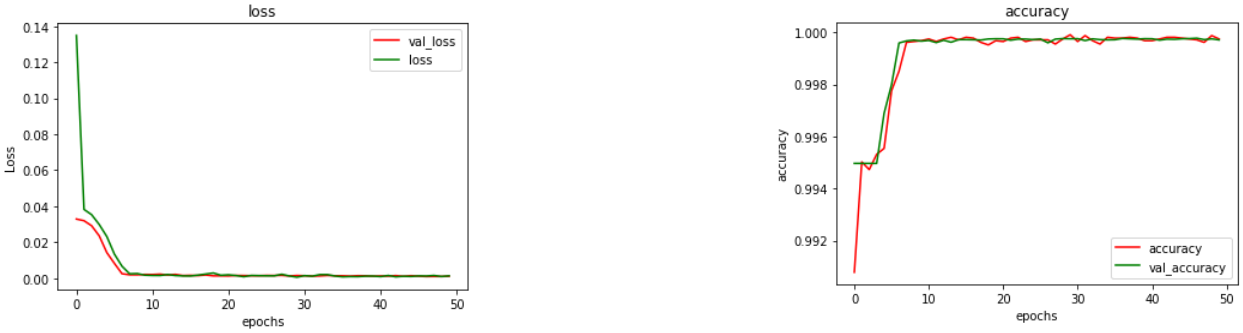


Figure 3-9 : L'exactitude et la perte de la classification binaire

l est clair que nos méthodes DL surpassent largement toutes les autres méthodes d'apprentissage automatique, avec une grande précision et un bon taux de rappel. Parmi nos méthodes, CNN a obtenu les meilleurs résultats avec une précision de 99.97%, grâce à sa capacité à reconnaître les schémas discriminatoires pour chaque catégorie, le Table 3-12 montre le rapport de classification des attaques La matrice de confusion a également été extraite pour montrer les résultats plus Figure 3-10.

Table 3-12 : Le rapport de classification binaire

	Precision	recall	F1-score	Support
0 - Attaque	1.00	1.00	1.00	575423
1 -beingin	0.95	0.99	0.97	2912
Accuracy			**1.00**	578335
Mcro avg	0.98	0.99	0.99	578335
Weighted avg	1.00	1.00	1.00	578335

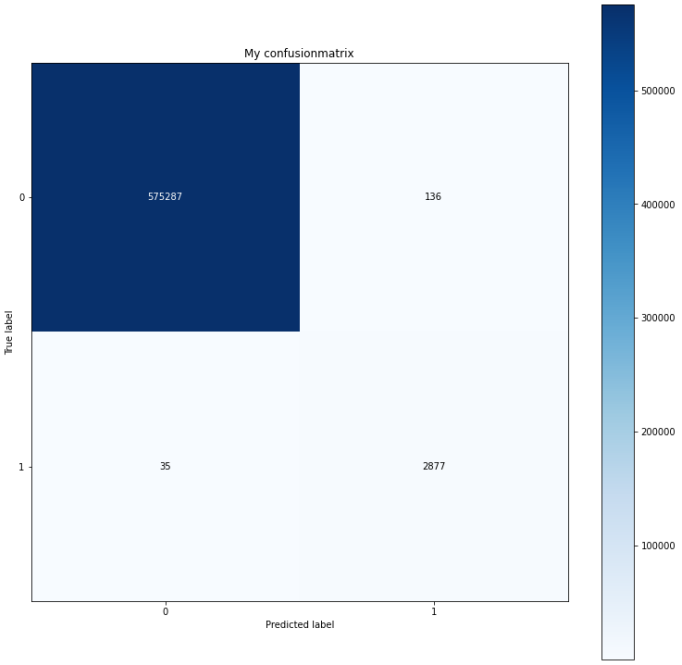


Figure 3-10 : Matrice de confusion (2 - classes)

- **La deuxième expérimentation (8-classes** classifications**) :** a été réalisée sur le sous-ensemble de données dans le tableau Table 3-6. Les modèles sont évalués directement sur l'ensemble de test. Le modèle est formé sur 50 itérations. Cela signifie que ces modèles apprennent mieux et font de meilleures prédictions après chaque période d'amélioration (Figure 3-11). Les meilleurs résultats avec une précision 92%, le tableau 4.9 montre le rapport de classification des attaques

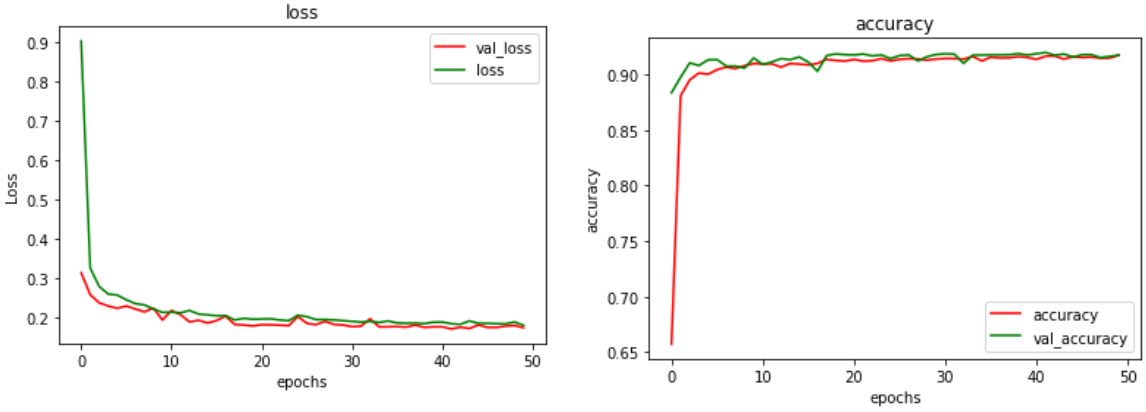


Figure 3-11 : L'exactitude et la perte (8 classes classifications)

Table 3-13 : Le rapport de classification (7 classes classifications)

	Precision	**Recall**	**F1-score**	**Support**
SYN	1.00	1.00	1.00	136583
NetBIOS	0.97	0.99	0.98	2872
UDP	0.50	0.00	0.00	36960
MSSQL	0.97	0.97	0.97	97331
LDAP	1.00	0.40	0.57	362
PORTMAP	0.77	1.00	0.87	120732
BENIGN	1.00	1.00	1.00	40832
UDPLag	0.96	0.97	0.97	0.96
Accuracy			**0.92**	518336
Mcro avg	0.90	0.79	0.79	518336
Weighted avg	0.90	0.92	0.89	518336

- **La troisième expérimentation (13-classes** classifications**) :** : a été réalisée sur le sous-ensemble de données dans le tableau Table 3-8 . Les modèles sont évalués directement sur l'ensemble de test. Le modèle est formé sur 40 itérations. Cela signifie que ces modèles apprennent mieux et font de meilleures prédictions après chaque période d'amélioration (Figure 3-12), les meilleurs résultats avec une précision 78 %, grâce à sa capacité à reconnaître les schémas discriminatoires pour chaque catégorie, le Figure 3-13 montre le rapport de classification des attaques,

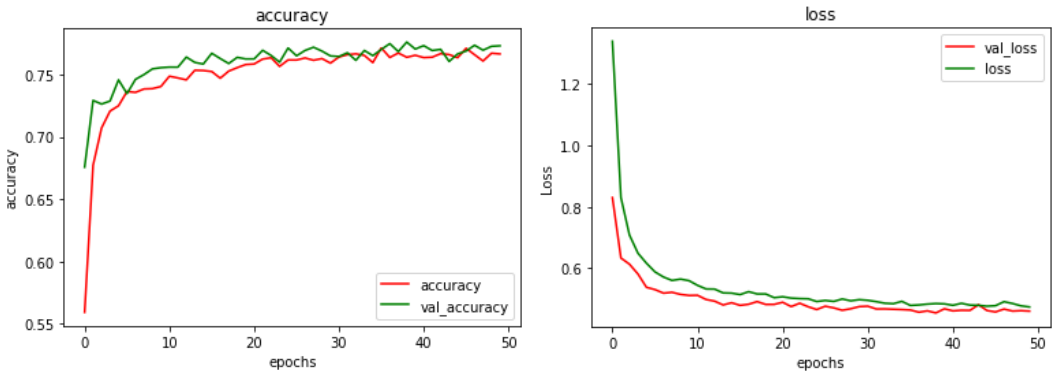


Figure 3-12: L'exactitude et la perte (13 classes classifications)

Table 3-14 : Le rapport de classification (13 classes classifications)

		Precision	Recall	F1-score	Support
1	**TFTP**	0.98	0.94	0.96	24925
2	**DrDoS_MSSQL**	0.95	0.97	0.96	24894
3	**DrDoS_UDP**	0.48	0.91	0.63	25110
4	**SYN**	0.84	0.97	0.90	25023
5	**DrDoS_DNS**	0.89	0.98	0.93	25064
6	**DrDoS_NetBIOS**	0.67	0.82	0.74	24867
7	**DrDoS_SNMP**	0.57	0.85	0.68	24917
8	**DrDoS_LDAP**	0.79	0.16	0.27	25046
9	**DrDoS_SSDP**	0.53	0.09	0.16	24870
10	**DrDoS_NTP**	0.99	0.99	0.99	25112
11	**UDP_lag**	0.93	0.72	0.81	25155
12	**WebDDoS**	0.50	0.88	0.64	96
13	**BENIGN**	1.00	0.98	1.00	19730
	Accuracy			**0.78**	294809
	Mcro avg	0.78	0.79	0.74	294809
	Weighted avg	0.80	0.78	0.75	294809

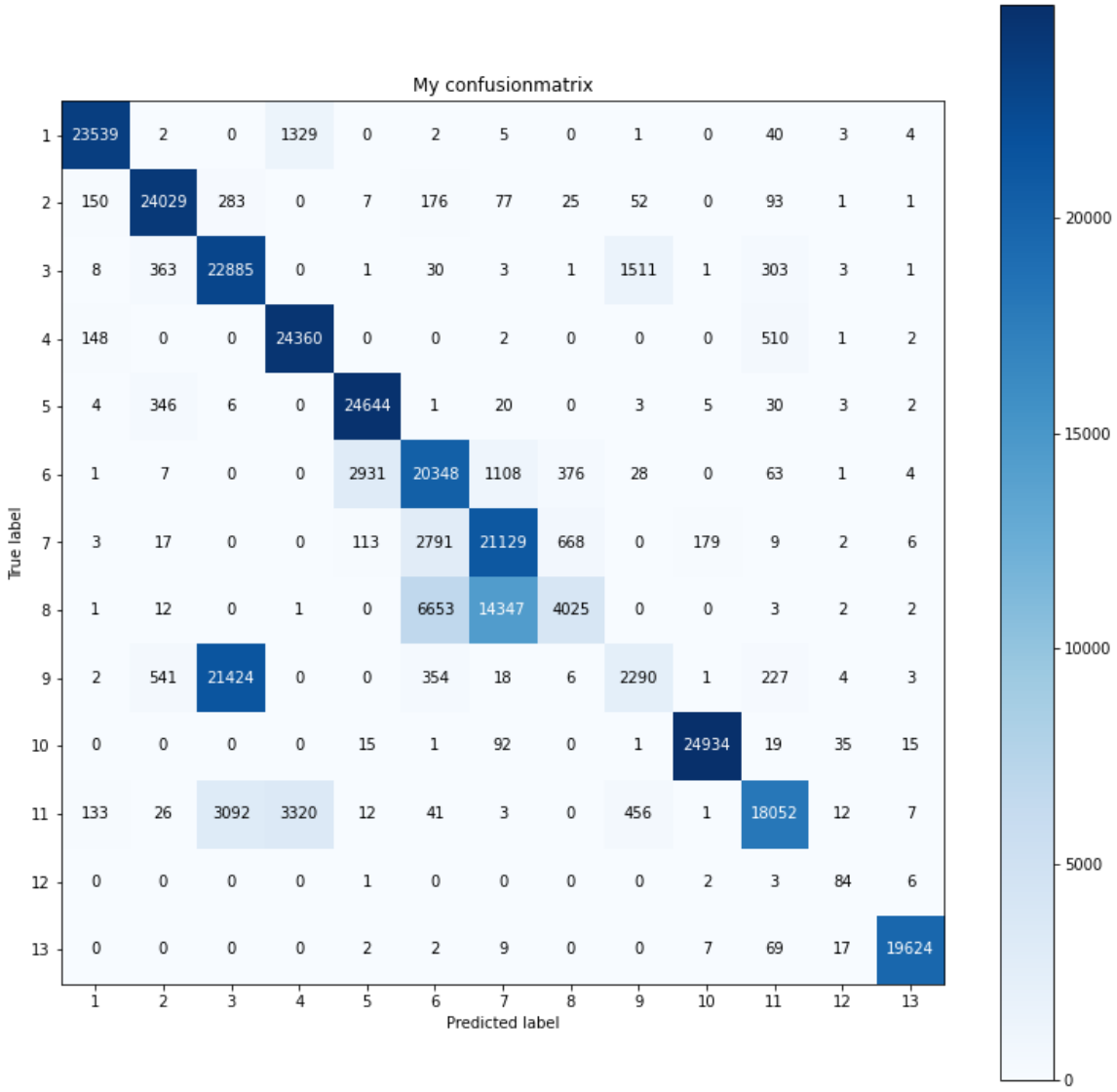


Figure 3-13 : Matrice de confusion (13 classifications)

Dans le matrice de confusion Figure 3-15 : Nous concluons que les attaques DrDoS_LDAP et UDP_lag ont causé le double du résultat obtenu , Parce que les caractéristiques de cette attaque ,étant donné que les caractéristiques de cette attaque sont similaires, même les administrateurs réseau ont du mal à les différencier.

- **La quatrième expérimentation (14-classes** classifications **hybride)** : a été réalisée sur le sous-ensemble de données dans le tableau Table 3-10 . Les modèles sont évalués directement sur l'ensemble de test. Le modèle est formé sur 50 itérations. Cela signifie que ces modèles apprennent mieux et font de meilleures prédictions après chaque période d'amélioration (Figure 3-14), les meilleurs résultats avec une précision 87 %, grâce à sa capacité à reconnaître les

schémas discriminatoires pour chaque catégorie, le Table 3-15 montre le rapport de classification des attaques La matrice de confusion a également été extraite pour montrer les résultats plus

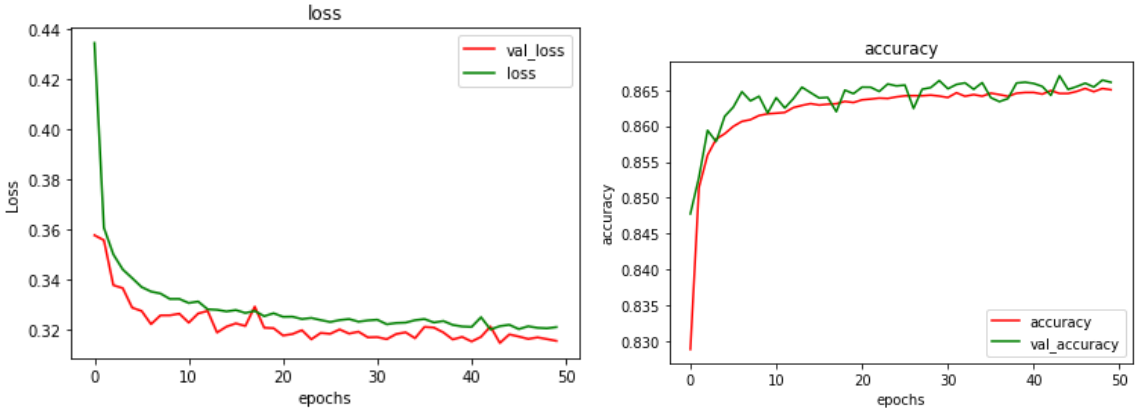


Figure 3-14 : : L'exactitude et la perte (14 classes classifications)

Table 3-15 : Le rapport de classification (14 classes classifications)

		Precision	Recall	F1-score	Support
1	**TFTP**	0.98	0.97	0.97	81071
2	**DrDoS_MSSQL**	0.97	0.98	0.97	38859
3	**DrDoS_UDP**	0.72	0.98	0.83	28061
4	**SYN**	0.91	0.95	0.93	26051
5	**DrDoS_DNS**	0.90	0.98	0.94	31444
6	**DrDoS_NetBIOS**	0.70	0.81	0.75	20823
7	**DrDoS_SNMP**	0.61	0.86	0.72	20455
8	**DrDoS_LDAP**	0.82	0.14	0.24	16463
9	**DrDoS_SSDP**	0.74	0.00	0.00	10502
10	**DrDoS_NTP**	0.98	0.98	0.98	4797
11	**UDP_lag**	0.99	0.64	0.78	1501
12	**PORTMAP**	0.00	0.00	0.00	762
13	**BENIGN**	0.90	0.98	0.94	453
14	**WebDDoS**	0.67	0.88	0.76	88

Accuracy			**0.86**	281330
Mcro avg	0.78	0.73	0.70	281330
Weighted avg	0.87	0.86	0.83	281330

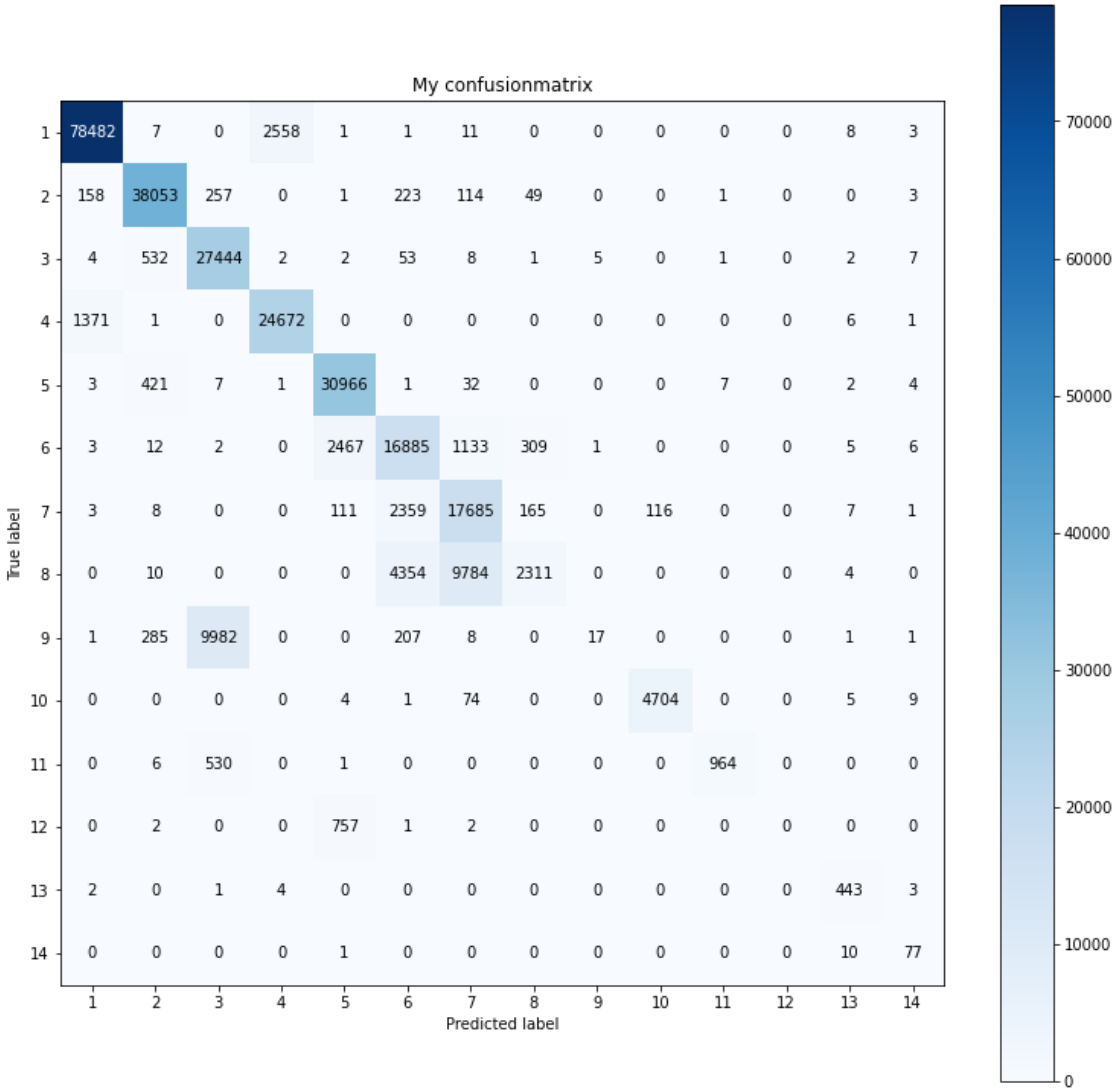


Figure 3-15 : Matrice de confusion (14 classifications)

Tous ces résultats sont bons, et nous en avons surpassé beaucoup, mais pas les meilleurs résultats, il y a les travaux dont nous avons parlé plus tôt, ils ont obtenu d'excellents résultats, mais avec un bon équipement par conséquent, nous comparons notre travail avec le travail qui a travaillé sur le même environnement de travail, qui est google colab gratuit avec (12 GB RAM).

la raison de la baisse des résultats obtenus ,il existe trois types d'attaques avec les mêmes caractéristiques, même les administrateurs réseau ont du mal à les distinguer en raison de leur similitude par exemple : L'attaque DRDoS SSDP et L'attaque DRDOS SNMP il est également difficile de faire la distinction entre Portmap et DRDOP UDP et on ne peut pas manipuler les caractéristiques des attaques, ce qui fait régresser les bons résultats t on ne peut pas manipuler les caractéristiques des attaques, les résultats peuvent être plutôt bons

Conclusion

Nous avons implémenté un modèle d'apprentissage en profondeur CNN utilisant l'ensemble de données CICDDoS2019 pour détecter une attaque DDoS.

Table 3-16 : Les résultats des méthodes proposées

	Précision	**Recall**	**F1-measure**	**Accuracy**
1- Expérimentation Data-set_1 (2-Classes)	1.00	1.00	1.00	1.00
2- Expérimentation Data-set_2 (7-Classes)	0.90	0.92	0.89	0.92
3- Expérimentation Data-set_3 (13-Classes)	0.80	0.78	0.75	0.77
4- Expérimentation Data-set_4 (14-Classes)	0.87	0.86	0.83	0.87

Le développement et la modification des données étaient un problème auquel nous étions confrontés et qui nous prenait beaucoup de temps à résoudre, et l'un des problèmes auxquels nous étions confrontés était que les appareils disponibles pour travailler étaient faibles (RAM ,GPU ,Processeur) et ne remplissaient pas leur objectif , nous avons fait quatre ensembles différents ,

En prélevant des échantillons à partir d'un ensemble de données différent et aléatoire afin que le résultat soit plus réaliste et non manipulé La première classification (classification binaire) , et les trois autres étaient l'expression d'une classification multi-classe , Et nous avons fait une nouvelle suggestion en prenant tous les types d'attaques sur la base de données et en prenant chaque type d'attaque comme un pourcentage qui se trouve sur l'ensemble d'informations par exemple : (Le nombre typique d'attaques DDos_TFTP est de 20 millions dans l'ensemble de données, nous le prendrons à 5% le nombre d'attaques sera de 1 million) ,Ensuite, de nombreuses expériences sont menées pour obtenir le meilleur résultat et le meilleur entraînement grâce à une expérience ,Les résultats de l'apprentissage en profondeur étaient meilleurs que les résultats de l'apprentissage automatique classique et certains des travaux précédents avec l'apprentissage en profondeur utilisant le même ensemble d'informations, et nous avons également obtenu des résultats très satisfaisants avec une précision de détection très élevée pour différents types d'attaques et plusieurs expériences sur l'ensemble de données, et nous pouvons considérer ce modèle comme quelque chose de très bon pour les dispositifs de détection d'intrusion pour la cybersécurité dans le trafic réseau.

Conclusion générale

La cybersécurité est un groupe d'entreprises, en particulier dans la sécurisation des éléments vulnérables à travers (ICT). Les systèmes de détection d'intrusion font partie intégrante de la cybersécurité, la détection d'intrusion doit être disponible dans tous les segments du réseau pour réduire les attaques par déni de service. Les logiciels antivirus ou les pares-feux au sein du réseau sont insuffisants et inefficaces contre ces attaques. Nous avons mené cette étude pour intégrer l'apprentissage en profondeur et son développement pour aider l'intrusion le détecteur fonctionne mieux dans la détection d'intrusion à l'aide de l'apprentissage en profondeur,

Nous avons donc commencé par choisir le meilleur ensemble de données modernes avec des informations sur les flux réels nommé CICDDoS2019 pour détecter les cyberattaques et le type d'attaque, avec la variété de ces attaques (attaque par déni de service), il est difficile pour le système de détection d'intrusion de les distinguer des utilisateurs légitimes sur les grands réseaux Internet. Après cela, nous avons mené cette étude afin d'aider les administrateurs réseau à explorer ces attaques

Ensuite, nous avons choisi d'implémenter un modèle d'apprentissage en profondeur, un réseau de neurones convolutifs (CNN), et (CNN) a été choisi pour avoir les meilleurs résultats dans les travaux qui nous concernent.

Les résultats obtenus sont raisonnablement satisfaisants en le comparant avec des travaux connexes car il s'agit d'un trafic réel, et nous avons donc amélioré d'un bon pourcentage le temps d'exploration et le taux d'erreur dans la découverte, nous pouvons donc l'utiliser comme système de détection d'avertissement en temps réel

Perspective

Dans nos travaux futurs, nous travaillerons sur les fichiers pcap du jeu de données pour augmenter le nombre d'attaques afin de peser le nombre d'attaques par déni de service d'apprentissage profond, en utilisant des programmes de détection de trafic réseau.

[1] G. N. Nayak and S. G. Samaddar, "Different flavours of Man-In-The-Middle attack, consequences and feasible solutions," *Proceedings - 2010 3rd IEEE International Conference on Computer Science and Information Technology, ICCSIT 2010*, vol. 5, pp. 491–495, 2010, doi: 10.1109/ICCSIT.2010.5563900.

[2] V. D. Gligor and S. H. Shattuck, "On Deadlock Detection in Distributed Systems," *IEEE Transactions on Software Engineering*, vol. SE-6, no. 5, pp. 435–440, 1980, doi: 10.1109/TSE.1980.230491.

[3] B. Zhang, T. Zhang, and Z. Yu, "DDoS detection and prevention based on artificial intelligence techniques," *2017 3rd IEEE International Conference on Computer and Communications, ICCC 2017*, vol. 2018-January, pp. 1276–1280, Mar. 2018, doi: 10.1109/COMPCOMM.2017.8322748.

[4] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," *Proceedings - International Carnahan Conference on Security Technology*, vol. 2019-October, Oct. 2019, doi: 10.1109/CCST.2019.8888419.

[5] S. Hosseini and M. Azizi, "The hybrid technique for DDoS detection with supervised learning algorithms," *Computer Networks*, vol. 158, pp. 35–45, Jul. 2019, doi: 10.1016/J.COMNET.2019.04.027.

[6] R. R. Nuiaa, S. Manickam, and A. H. Alsaeedi, "Distributed reflection denial of service attack: A critical review," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 6, pp. 5327–5341, Dec. 2021, doi: 10.11591/IJECE.V11I6.PP5327-5341.

[7] D. Roy and P. Nourry, "Sécurité du réseau fixe d'un opérateur : focus sur les dénis de service".

[8] G. R. Zargar and P. Kabiri, "Identification of effective network features to detect smurf attacks," *SCOReD2009 - Proceedings of 2009 IEEE Student Conference on Research and Development*, pp. 49–52, 2009, doi: 10.1109/SCORED.2009.5443345.

[9] D. H. Kim, P. T. Dinh, S. Noh, J. Yi, and M. Park, "An Effective Defense Against SYN Flooding Attack in SDN," *ICTC 2019 - 10th International Conference on ICT Convergence: ICT Convergence Leading the Autonomous Future*, pp. 369–371, Oct. 2019, doi: 10.1109/ICTC46691.2019.8939937.

[10] Z. Y. Shen, M. W. Su, Y. Z. Cai, and M. H. Tasi, "Mitigating SYN Flooding and UDP Flooding in P4-based SDN," *2021 22nd Asia-Pacific Network Operations and Management Symposium, APNOMS 2021*, pp. 374–377, Sep. 2021, doi: 10.23919/APNOMS52696.2021.9562660.

[11] A. Praseed and P. S. Thilagam, "HTTP request pattern based signatures for early application layer DDoS detection: A firewall agnostic approach," *Journal of Information Security and Applications*, vol. 65, p. 103090, Mar. 2022, doi: 10.1016/J.JISA.2021.103090.

[12] J. W. Kim, "Integrating Artificial immune Algorithms for Intrusion Detection".

[13] "Mise en place d'une sonde snort Monitoring network Projets du M3 REALISATION : Slimane Tanji Snort".

[14] "RFC 4766 - Intrusion Detection Message Exchange Requirements." https://datatracker.ietf.org/doc/rfc4766/ (accessed May 31, 2022).

[15] Ghenima BOURKACHE, "Un IDS réparti basé sur une société d'agents intelligents." Accessed: May 31, 2022. [Online]. Available: http://dlibrary.univ-boumerdes.dz:8080/bitstream/123456789/912/1/Bourkache%2C%20Ghenima%20magister.pdf

[16] Lehmann Guillaum, " cours de sécurité informatique 2003-04-13." Accessed: May 31, 2022. [Online]. Available: https://di.univ-blida.dz/jspui/bitstream/123456789/7211/1/Benhassine%20Oualid%20et%20Boutebali%20Imadeddine.pdf

[17] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, pp. 16–24, 2012, doi: 10.1016/j.jnca.2012.09.004.

[18] H. Debar, M. Dacier, and A. Wespi, "Revised taxonomy for intrusion-detection systems," *Annales des Telecommunications/Annals of Telecommunications*, vol. 55, no. 7, pp. 361–378, Jul. 2000, doi: 10.1007/BF02994844.

[19] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, pp. 493–501, Mar. 2019, doi: 10.1007/S12083-017-0630-0.

[20] S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*. Accessed: Jun. 11, 2022. [Online]. Available: https://www.routledge.com/Data-Mining-and-Machine-Learning-in-Cybersecurity/Dua-Du/p/book/9781439839423

[21] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," *Proceedings - IEEE Symposium on Security and Privacy*, pp. 305–316, 2010, doi: 10.1109/SP.2010.25.

[22] J. M. Johnson and T. M. Khoshgoftaar, "Survey on deep learning with class imbalance," *Journal of Big Data*, vol. 6, no. 1, pp. 1–54, Dec. 2019, doi: 10.1186/S40537-019-0192-5/TABLES/18.

[23] Aboubakry Moussa SOW, "COMME EXIGENCE PARTIELLE DE LA MAÎTRISE EN MATHÉMATIQUES ET INFORMATIQUE APPLIQUÉE," 2020. Accessed: Jun. 07, 2022. [Online]. Available: https://depot-e.uqtr.ca/id/eprint/9600/1/eprint9600.pdf

[24] A. H. Lashkari, G. D. Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of tor traffic using time based features," *ICISSP 2017 - Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, vol. 2017-January, pp. 253–262, 2017, doi: 10.5220/0006105602530262.

[25] Q. Zhong, Y. Sun, and Z. Qiu, "Deep Recurrent Neural Network with Sharing Weights for Solving High-Dimensional PDEs," *Proceedings of 2021 IEEE International Conference on Data Science and Computer Application, ICDSCA 2021*, pp. 6–9, 2021, doi: 10.1109/ICDSCA53499.2021.9650325.

[26] "Université 8 mai 1945 - GUELMA: Un système de détection d'intrusion pour la cybersécurité." https://dspace.univ-guelma.dz/jspui/handle/123456789/10125 (accessed May 23, 2022).

[27] M. A. Ferrag, L. Shu, H. Djallel, and K. K. R. Choo, "Deep Learning-Based Intrusion Detection for Distributed Denial of Service Attack in Agriculture 4.0," *Electronics 2021, Vol. 10, Page 1257*, vol. 10, no. 11, p. 1257, May 2021, doi: 10.3390/ELECTRONICS10111257.

[28] "DETECTION OF DDOS ATTACKS BASED ON DENSE NEURAL NETWORKS, AUTOENCODERS AND PEARSON CORRELATION COEFFICIENT." https://dalspace.library.dal.ca/handle/10222/78536 (accessed May 23, 2022).

[29] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: a systematic review," *Soft Computing*, p. 1, 2022, doi: 10.1007/S00500-021-06608-1.

[30] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feed forward based deep neural network model," *Expert Systems With Applications*, vol. 169, p. 114520, 2021, doi: 10.1016/j.eswa.2020.114520.

[31] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," *IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2009*, Dec. 2009, doi: 10.1109/CISDA.2009.5356528.

[32] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021, doi: 10.1109/ACCESS.2021.3056614.

[33] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," *Expert Systems with Applications*, vol. 67, pp. 296–303, Jan. 2017, doi: 10.1016/J.ESWA.2016.09.041.

[34] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajković, "Distributed denial of service attacks," *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, vol. 3, pp. 2275–2280, 2000, doi: 10.1109/ICSMC.2000.886455.

[35] M. Almiani, A. AbuGhazleh, Y. Jararweh, and A. Razaque, "DDoS detection in 5G-enabled IoT networks using deep Kalman backpropagation neural network," *International Journal of Machine Learning and Cybernetics*, vol. 12, no. 11, pp. 3337–3349, Apr. 2021, doi: 10.1007/S13042-021-01323-7/TABLES/4.

[36] S. Ray, K. Alshouiliy, and D. P. Agrawal, "Dimensionality reduction for human activity recognition using google colab," *Information (Switzerland)*, vol. 12, no. 1, pp. 1–23, Jan. 2021, doi: 10.3390/INFO12010006.

[37] "Deep Learning for Cyber Security Applications: A Comprehensive Survey." https://www.researchgate.net/publication/355282522_Deep_Learning_for_Cyber_Security_Applications_A_Comprehensive_Survey (accessed Jun. 07, 2022).

[38] "KDD Cup 1999 Data." http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed Jun. 07, 2022).

[39] "Datasets | Research | Canadian Institute for Cybersecurity | UNB." https://www.unb.ca/cic/datasets/index.html (accessed Jun. 07, 2022).

[40] “MAWILab - Documentation.” http://www.fukuda-lab.org/mawilab/documentation.html (accessed Jun. 07, 2022).

[41] “DDoS 2019 | Datasets | Research | Canadian Institute for Cybersecurity | UNB.” https://www.unb.ca/cic/datasets/ddos-2019.html (accessed Jun. 07, 2022).

[42] “Resisting SYN flood DoS attacks with a SYN cache.” https://www.usenix.org/legacy/event/bsdcon02/full_papers/lemon/lemon_html/ (accessed Jun. 09, 2022).

[43] “What is an SSDP DDoS attack?” https://ddos-guard.net/en/terminology/attack_type/ssdp-ddos-attack (accessed Jun. 09, 2022).

[44] “Attackers Using New MS SQL Reflection Techniques.” https://myakamai.force.com/customers/s/article/Attackers-Using-New-MS-SQL-Reflection-Techniques?language=en_US (accessed Jun. 09, 2022).

[45] L. Rudman and B. Irwin, “Characterization and analysis of NTP amplification based DDoS attacks,” *2015 Information Security for South Africa - Proceedings of the ISSA 2015 Conference*, Nov. 2015, doi: 10.1109/ISSA.2015.7335069.

[46] M. Anagnostopoulos, G. Kambourakis, P. Kopanos, G. Louloudakis, and S. Gritzalis, “DNS amplification attack revisited,” *Computers & Security*, vol. 39, no. PART B, pp. 475–485, Nov. 2013, doi: 10.1016/J.COSE.2013.10.001.

[47] “UDP-Based Amplification Attacks | CISA.” https://www.cisa.gov/uscert/ncas/alerts/TA14-017A (accessed Jun. 09, 2022).

[48] “DETECTION OF DDOS ATTACKS BASED ON DENSE NEURAL NETWORKS, AUTOENCODERS AND PEARSON CORRELATION COEFFICIENT.” https://dalspace.library.dal.ca/handle/10222/78536 (accessed Jun. 09, 2022).

[49] B. Sieklik, R. MacFarlane, and W. J. Buchanan, “Evaluation of TFTP DDoS amplification attack,” *Computers & Security*, vol. 57, pp. 67–92, Mar. 2016, doi: 10.1016/J.COSE.2015.09.006.

[50] J. Yu, H. Lee, M.-S. Kim, and D. Park, “Traffic flooding attack detection with SNMP MIB using SVM,” *Computer Communications*, vol. 31, no. 17, pp. 4212–4219, Nov. 2008, doi: 10.1016/J.COMCOM.2008.09.018.

[51] A. Singh and D. Juneja, "Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks," *Aarti Singh et. al. / International Journal of Engineering Science and Technology*, vol. 2, no. 8, pp. 3405–3411, 2010, Accessed: Jun. 09, 2022. [Online]. Available: https://www.researchgate.net/publication/50315626

[52] "ANALISIS KEAMANAN JARINGAN SINGLE SIGN ON (SSO) DENGAN LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP) MENGGUNAKAN METODE MITMA | Amarudin | SEMNASTEKNOMEDIA ONLINE." https://ojs.amikom.ac.id/index.php/semnasteknomedia/article/view/469 (accessed Jun. 09, 2022).

[53] W. Wang, X. Zhang, S. Gombault, and S. J. Knapskog, "Attribute normalization in network intrusion detection," *I-SPAN 2009 - The 10th International Symposium on Pervasive Systems, Algorithms, and Networks*, pp. 448–453, 2009, doi: 10.1109/I-SPAN.2009.49.

[54] Y. Kim, "Convolutional Neural Networks for Sentence Classification," *EMNLP 2014 - 2014 Conference on Empirical Methods in Natural Language Processing, Proceedings of the Conference*, pp. 1746–1751, Aug. 2014, doi: 10.48550/arxiv.1408.5882.

[55] D. K. Sharma, M. Chatterjee, G. Kaur, and S. Vavilala, "Deep learning applications for disease diagnosis," *Deep Learning for Medical Applications with Unique Data*, pp. 31–51, Jan. 2022, doi: 10.1016/B978-0-12-824145-5.00005-8.