الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العالي

Ministère de l'enseignement supérieur et de la recherche scientifique

Université 20 Août 1955-Skikda
Faculté des sciences
Département d'Informatique

جامعة 20 اوت1955 سكيكدة
كلية العلوم
قسم الاعلام الالي

Mémoire de fin d'études en vue de l'obtention du diplôme de

Master en Informatique

Option : Réseaux et Systèmes Distribués (RSD)

Thème

Un Système de Détection du Spam Email en utilisant le Deep Learning

Réalisé par :

Bougarouche Rania

Encadré par :

Dr. Ramdane Chikh

Promo 2021 / 2022

Remerciements

Avant tout, nous nous devons remercier ALLAH a tout-puissant pour toute la volonté et le courage qu'il nous a donnés pour l'achèvement de ce travail.

Je tiens à remercier toutes les personnes qui ont contribué au succès de mon travail et qui m'ont aidée lors de la rédaction de ce mémoire.

Je voudrais dans un premier temps remercier, mon Encadrant de mémoire.

Dr. Ramdane Chikh, Enseignant au niveau de l'Université 20 Aout 1955 - Skikda

Faculté des Sciences Département d'Informatique

Pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion.

Je remercie également toute l'équipe pédagogique de l'Université 20 Aout 1955 Skikda, Faculté des Sciences, Département d'Informatique.

Je tiens à témoigner toute ma reconnaissance aux personnes suivantes, pour leur aide dans la réalisation de ce mémoire.

Mon père et ma maman qui m'ont beaucoup appris sur les défis du monde à relever dans notre vie.

Ils ont partagé ses connaissances et expériences dans la vie, tout en m'accordant sa confiance et une large indépendance dans l'exécution de missions valorisantes.

Mes Frères, mes amies et toute ma famille, pour leur soutien constant et leur Encouragements.

Et Exceptionnellement Les Étudiants Master Informatique Promo 2021/2022.

Dédicace

Je dédiais ce travail.

À mon père et ma maman qui m'ont soutenu et encouragé durant

Ces années d'études.

Qu'ils trouvent ici le témoignage de mon profonde

Reconnaissance.

À mes Frères, ceux qui partageaient avec moi tous les

Moments d'émotion lors de la réalisation de ce travail.

Ils m'ont chaleureusement supporté et encouragé tout au long de mon parcours.

À ma famille, mes proches et à ceux qui me donnent

De l'amour et de la vivacité.

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

À tous ceux que j'aime.

Résumé

Le spam par e-mail est devenu un problème majeur de nos jours, avec la croissance rapide des internautes, les spams par e-mail augmentent également. Les gens les utilisent pour des comportements illégaux et contraires à l'éthique, le phishing et la fraude. Envoi de liens malveillants via des spams qui peuvent endommager notre système et peuvent également pénétrer dans votre système. Créer un faux profil et un compte de messagerie est très facile pour les spammeurs, ils se font passer pour une personne authentique dans leurs spams, ces spammeurs ciblent les personnes qui ne sont pas au courant de ces fraudes. Donc, il est nécessaire d'identifier les spams qui sont des fraudes, ce projet identifiera ces spams en utilisant la technique d'apprentissage en profondeur, cet article discutera des algorithmes d'apprentissage en profondeur et appliquera ces algorithmes sur nos ensembles de données pour la détection des spams par e-mail.

Mots clés : Spam, Email, courrier indésirables, ham, détection du Spam Email, Deep Learning, apprentissage en profondeur, Intelligence Artificielle

Table des Matières :

Liste de Figures :

Liste de Tables :

Introduction Générale :

Les modèles d'apprentissage en profondeur ont été utilisés à de multiples fins dans le, domaine de l'informatique, de la résolution d'un problème de trafic réseau à la détection d'un logiciel malveillant. Les e-mails sont utilisés régulièrement par de nombreuses personnes pour communiquer et socialiser. Les failles de sécurité qui compromettent les données des clients permettent aux « spammeurs » d'usurper une adresse e-mail compromise pour envoyer des e-mails illégitimes (spam). Ceci est également exploité pour obtenir un accès non autorisé à leur appareil en incitant l'utilisateur à cliquer sur le lien de spam dans l'e-mail de spam, ce qui constitue une attaque de phishing.

❖ Problématique :

En considérant la détection de manière traditionnelle, où des règles de détection de spam sont mises en place et ont constamment besoin d'être mises à jour manuellement, ce qui consomme du temps et des ressources, l'apprentissage en profondeur facilite les choses, car il apprend à reconnaître automatiquement les emails non sollicités (spam) et les emails légitimes (non spam). Puis il applique ces instructions apprises aux emails entrants inconnus.

❖ Contributions :

Afin de résoudre les problématiques précitées, nous proposons une approche de détection basée sur les réseaux de neurones.

Dans le cadre de notre travail, nous avons fixé les contributions suivantes :

- Le processus de détection, consiste à différencier un email sain d'un fichier Spam (détection des malwares).
- Utilisation la technique d'apprentissage en profondeur qui ont le potentiel de nous permettre d'effectuer une classification des fichiers malveillants avec une précision élevée.
- Si le résultat est un spam, on le détruire, sinon on le sauvegarde.

❖ **Organisation :**

Notre manuscrit est divisé en deux parties :

- Première partie : contient les chapitres 1 et 2 est une recherche sur les Spam Email et le Deep Learning.

- Deuxième partie : Contenant les chapitres 3 et 4, qui présentent respectivement la conception et l'implémentation du système proposé pour la détection des Spam Email, ainsi que les résultats expérimentaux obtenus.

Chapitre1 :

Spam Email

1. Introduction :

Qui d'entre nous n'a pas reçu des e-mails contenants des offres commerciales ? Ou des promesses apparemment miraculeuses de faire une différence dans la vie ? Ou des messages incompréhensibles ? Ces exemples que nous avons mentionnés ici sont précisément ce que nous appelons les " **Spam Email** ".

Spam Email est un grand problème pour les internautes. Les augmentations récentes du taux de spam ont causé une grande inquiétude parmi la communauté internet. De nombreuses solutions avaient été suggérées pour résoudre le problème. Dans ce chapitre, nous allons présentons tout d'abord : l'origine du mot « Spam », premier envoi massif, la définition, l'évolution, les catégories, les impacts, les solutions et les techniques pour identifier et éviter les **Email Spam.**

2. Origine du mot « Spam » :

Le terme a été inventé à l'origine en 1937 par le gagnant d'un concours organisé par la société américaine Hormel Foods[1] pour gagner 100 $ en trouvant un nom pour leur nouveau produit, par conséquent, "SPAM" est la marque de choix et le mot est formé de "Spiced Ham".

Figure 01 : Le jambon épicé « SPAM »

Cette préparation, souvent synonyme de nourriture de mauvaise qualité (utilisée par l'armée américaine pendant la Seconde Guerre mondiale), a été mise en scène dans un épisode de la série télévisée des années 70 "Monty Python Flying Circus". Dans cet épisode, les personnages bloquent toute discussion en criant "spam spam spam spam...". Tout semble dire d'où vient la connotation de l'ordinateur. Mécontente de voir son nom

[1] Hormel Foods : fabricant de viande en conserve

de marque réutilisé par les éditeurs de la solution en réponse à des informations préjudiciables, la maison mère a tenté plusieurs actions en justice sans succès. [1]

3. Premier envoi massif :

Premier envoi en masse par la société Digital Equipment Corporation d'un message à caractère publicitaire aux différents utilisateurs d'ARPANET[2] le spam original, plus de neuf pages, les lignes sont comme suit. :

```
DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE
DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T.  THE
DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM
AND THE DECSYSTEM-10 <PDP-10> COMPUTER ARCHITECTURE.  BOTH THE DECSYSTEM-2060T
AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM.
THE DECSYSTEM-2060 IS AN UPWARD EXTENSION OF THE CURRENT DECSYSTEM 2040
AND 2050 FAMILY. THE DECSYSTEM-2020 IS A NEW LOW END MEMBER OF THE
DECSYSTEM-20 FAMILY AND FULLY SOFTWARE COMPATIBLE WITH ALL OF THE OTHER
DECSYSTEM-20 MODELS.

WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY
AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS
MONTH.  THE LOCATIONS WILL BE:

               TUESDAY, MAY 9, 1978 - 2 PM
                   HYATT HOUSE (NEAR THE L.A. AIRPORT)
                   LOS ANGELES, CA

               THURSDAY, MAY 11, 1978 - 2 PM
                   DUNFEY'S ROYAL COACH
                   SAN MATEO, CA
                   (4 MILES SOUTH OF S.F. AIRPORT AT BAYSHORE, RT 101 AND RT 92)

A 2020 WILL BE THERE FOR YOU TO VIEW. ALSO TERMINALS ON-LINE TO OTHER
DECSYSTEM-20 SYSTEMS THROUGH THE ARPANET. IF YOU ARE UNABLE TO ATTEND,
PLEASE FEEL FREE TO CONTACT THE NEAREST DEC OFFICE
FOR MORE INFORMATION ABOUT THE EXCITING DECSYSTEM-20 FAMILY.
```

Figure 02 : premier Spam sur le réseau ARPANET, Gary Thuerk

L'expéditeur de ce message était un individu par le nom de Gary Thuerk, qui a travaillé en Digital Equipment Corporation le département marketing. Les réactions au premier spam ont été tout à fait mélangées. Étonnamment, il y avait un peu d'un débat de la justesse du message Utilisations abusives à fins non commerciaux. Quelques cas isolés d'utilisations inadéquates de systèmes de messagerie ont été constatés dans les années 80 et jusqu'au début des années 90. Ainsi, une annonce pour la vente d'un service de table est postée en 1985 sur un groupe de discussion Usenet. Plus tard en 1993, Richard Depew travaille sur le projet ARMM (Automated Retroactive Minimal Moderation), un système censé protéger les groupes de discussion Usenet d'utilisations abusives. Malheureusement, dans le cadre d'un essai d'une version buggée d'ARMM,

[2] **ARPANET :** est le premier réseau à transfert de paquets développé aux États-Unis.

R. Depew envoie 200 messages sur le groupe news.admin.policy. Face aux récriminations, il s'excuse et utilise le mot « spam » pour désigner ses messages. [2]

4. Définition de Spam Email :

SPAM (Sending and Posting Advertisement in Mass) est un e-mail envoyé à un grand nombre de personnes sans la demande du destinataire de l'e-mail. Cela envoie beaucoup de publicité. En général, la publicité est la forme de spam la plus connue et le courrier électronique est la méthode d'envoi la plus courante. Mais cette pratique ne se produit pas seulement dans les environnements professionnels. Les messages chaînés, les messages incitant un utilisateur à le transmettre à un certain nombre de personnes, ainsi que les messages invitant cette personne à fournir ses données personnelles ou financières, sont également considérés comme des spams.

5. Evolution du Email Spam :

Dans les années 1980, un grand nombre de cottes de mailles ont commencé à apparaître et ont été rapidement détruites. Le premier e-mail a été enregistré en février 1982. Au début des années 1990, le marketing Internet a finalement décollé, et avec lui est venu un flot de spam. Vers 1994, des spams plus médiatisés ont commencé à se matérialiser. Ce type de spam est particulièrement préoccupant, car il a été le premier à abuser de manière flagrante des systèmes de messagerie et d'actualités, en utilisant un logiciel automatisé pour envoyer des messages (e-mails) aux listes. Le premier spam répandu équivalent au spam d'aujourd'hui s'appelait le spam "Jésus". Jésus Spam a été envoyé à tous les groupes sur Usenet[3] en janvier 1994. Le spam le plus médiatisé de l'histoire, ou du moins le spam dont on parle le plus, est probablement le spam de Canter & Siegel.

Une équipe d'avocats mari et femme, Lawrence Kanter et Siegel, a décidé d'embaucher un programmeur capable d'écrire un logiciel pour faire de la publicité dans tous les groupes de discussion existants. Cela a donné naissance au premier logiciel de diffusion par lots connu. Plusieurs permutations différentes de spam ont été envoyées en peu de temps. Jogger et Siegel n'étaient pas les seuls à spammer pendant cette période. Michael Wolff and Company Inc a décidé de commencer à spammer certains des livres de Wolff, en commençant par un site Web appelé Chat Net. Wolfe a publié

[3] **Usenet :** est un système en réseau de forums, inventé en 1979.

environ 150 publicités différentes pour le livre en décembre 1994. Des publicités pour d'autres livres de la série ont suivi. En 1994, le spam a commencé à croître de façon exponentielle. Venez avril 1995, Jeff Slaton, qui s'est appelé le Roi de Spam, a commencé à reprendre l'industrie en inondant des listes de diffusion avec des annonces pour tout de petites entreprises aux annonces politiques.

En août 1995, la toute première liste connue d'adresses électroniques publiques à vendre : 2 millions d'adresses totales.

Pendant les trois ans suivants, on a battu avec le spam dans la force pleine et a été gardé à la baie, au moins en termes de volume.

Entre 1998 et 1999, on battrait le spam cède d'un facteur de 10 à un facteur d'environ 3 ou 4, mais vers la fin de 2000, il commencerait à ramper la sauvegarde de nouveau. Ceci mènerait finalement à une pointe massive dans le volume qui a seulement grandi depuis 2001.

Depuis 2001, le spam a grandi exponentiellement. Vers la fin de 2002, le spam était devenu dans le volume par un facteur de presque 60 comparés à son volume juste six ans antérieurs. Le spam est maintenant tout à fait et complètement hors du contrôle. Au cours des dernières années, des filtres de spam plus complexes ont été conçus et mis en œuvre, utilisant tout de jeux de règle heuristiques de base aux filtres statistiques Les utilisateurs trouvent de plus en plus de spam dans leurs boîtes de réception chaque jour. Beaucoup de chercheurs croient maintenant que le spam est responsable de n'importe où de 35% à 65% de tout le trafic de courrier électronique sur Internet aujourd'hui, avec un taux de croissance annuel énorme de 15% à 20%. [3]

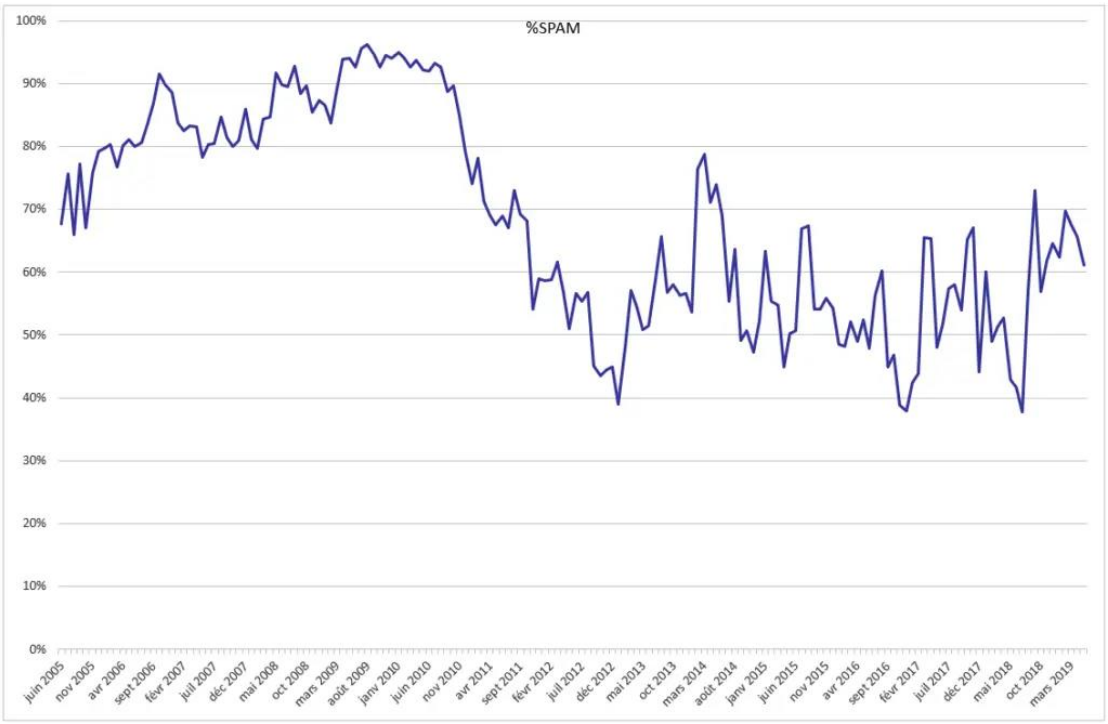


Figure 3 : Évolution du taux de spam Email depuis 2005

Le graphique ci-dessus montre le taux de Spam par rapport au nombre total d'e-mails reçus par les destinataires de 2005 en mai 2019. En 2005, le taux moyen de spam était d'environ 70 % de tous les e-mails reçus. En 2009, le spam a atteint un pic significatif en juillet et août à près de 96 %. Le volume de spam a fortement chuté entre 2010 et 2012 en raison du démantèlement des botnets. La quantité de spam a diminué, mais elle est devenue plus sophistiquée. Depuis 2013, nous avons vu des taux de spam fluctuer entre 50 % et 60 % en moyenne, approchant parfois 70 % à 80 % du trafic de messagerie. La moyenne au premier semestre 2019 était de 65,26 %.

6. **Catégories de l'Email Spam :**

Les spams peuvent être classés en fonction de leur objectif, De nombreux spammeurs envoient leurs e-mails en masse au public, par exemple ils envoient des publicités commerciales pour participer à des campagnes politiques, tandis que d'autres ont des intentions criminelles ou de développement. Cette section présente les types les plus courants :

6.1.La publicité commerciale :

Spam qui suit toute intention commerciale est notée UCE[4], l'UCE est une sorte de marketing direct et est considérée par les entreprises comme un outil important pour aborder clients (potentiels), car e-mail fournir un moyen pas cher et facile de communiquer avec un grand groupe de clients. Cependant, la plupart des UCE ne sont pas envoyés par les agences de publicité elles-mêmes, mais par les spammeurs, qui reçoivent des commissions de ces sociétés. Selon, une étude estime que le coût de l'envoi d'un seul e-mail est compris entre 0,01 US $ et 0.05US, une autre étude suggère que cela coûte 0,00032 cents pour obtenir une adresse email. « Une étude menée par le Wall Street Journal en 2002 a montré que le taux de retour aussi bas que 0,001% peut être rentable lorsque vous utilisez l'e-mail. L'étude a estimé qu'au moment où la société de commercialisation a atteint tous les 100 millions d'adresses qu'elle avait dans le dossier, il aurait probablement empoché plus de 25.000 USD pour le projet.[4]

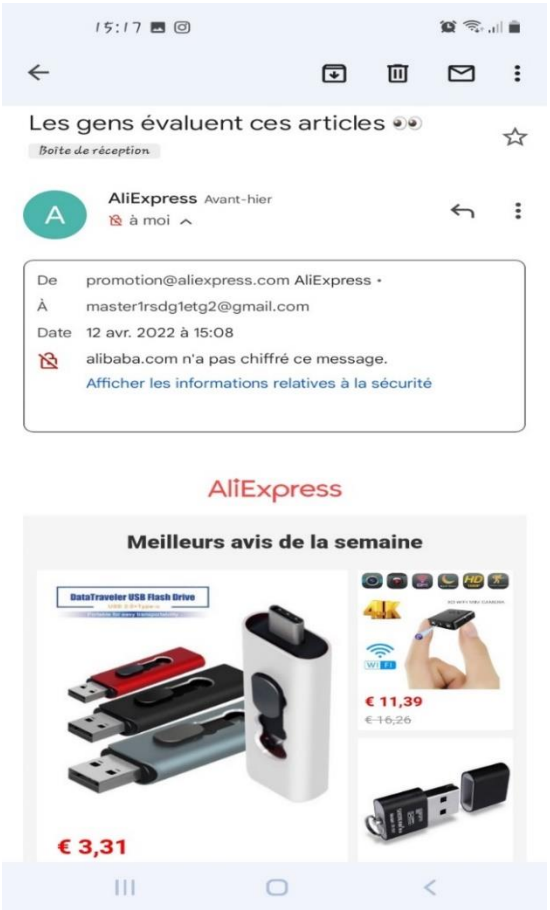
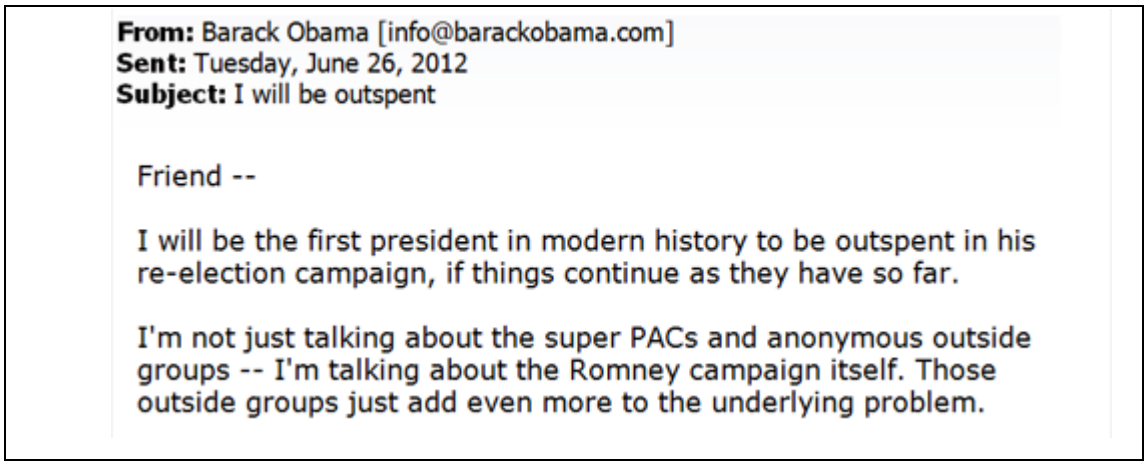


Figure 4 : exemple de UCE itech

[4] **UCE** : Unsolicited commercial e-mail (Spam Email Commercial).

6.2. Publicité non commerciale :

Les e-mails publicitaires ne sont pas seulement de nature commercial. Ils peuvent également soutenir des idées politiques, culturelles, religieuses, ou organisations. Par exemple, en 2003, les membres du Congrès américain ont envoyé des centaines de milliers de messages non sollicités à des constituants.[4]


From: Barack Obama [info@barackobama.com]
Sent: Tuesday, June 26, 2012
Subject: I will be outspent

Friend --

I will be the first president in modern history to be outspent in his re-election campaign, if things continue as they have so far.

I'm not just talking about the super PACs and anonymous outside groups -- I'm talking about the Romney campaign itself. Those outside groups just add even more to the underlying problem.

Figure 5 : exemple de Spam email non commerciale.

6.3. Fraude et le phishing :

Certains spammeurs envoient des e-mails qui sont frauduleuse, intentionnellement trompeur, ou connus pour entraîner dans des activités frauduleuses de la part de l'expéditeur. Les e-mails qui sont de nature frauduleuse sont également représentés comme « arnaque ». Les exemples de messages frauduleux sont ceux qui prétendent recueillir des fonds pour les victimes souffrant d'un accident vasculaire cérébral personnel du destin ou aux victimes d'une catastrophe naturelle. Un autre exemple est le transfert du Nigeria fraude de l'argent, escroquerie nigériane ou 419 escroqueries après l'article pertinent du Code pénal nigérian qu'elle viole : Les gens partout dans le monde ont reçu des lettres du Nigeria, officiellement d'un « haut fonctionnaire » ou « dirigeant » d'une entreprise d'État nigérian qui prétend avoir volé des millions de dollars d'un paiement de l'aide étrangère ou des subventions de l'ONU[5].

L'auteur de la lettre déclare qu'il ne peut pas mettre de l'argent dans son propre compte bancaire nigérian mais nécessite un compte bancaire étranger à travers lequel pour blanchir l'argent. Les coupables promettent que si vous autorisez les millions d'être

[5] **ONU :** Organisation des Nations Unies

déposé dans votre compte bancaire, vous pouvez garder n'importe où entre 10% et 30% du dépôt, qui est illustré dans cette Figure.

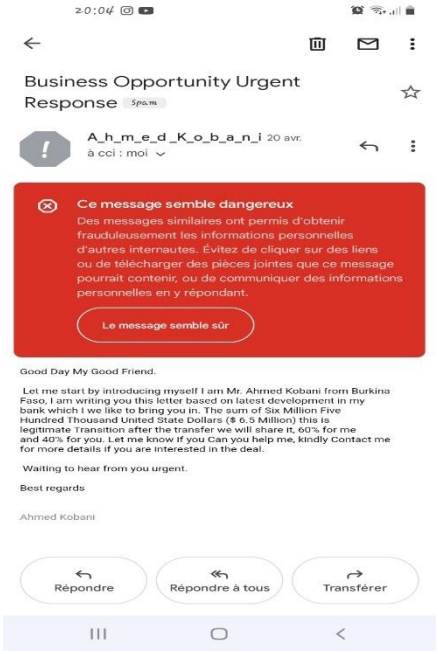


Figure 6 : exemple de Spam email “Fraude et le phishing“.

Un type particulier de fraude phishing e-mails qui semblent provenir d'une entreprise bien connue, mais le sont pas. Aussi appelé « usurpation de marque », ces messages sont souvent utilisés pour inciter les utilisateurs à révéler des informations personnelles, telles que l'e-mail, des informations financières et des mots de passe. [4]

6.4. Canulars et la chaîne des Emails :

Un canular est une tentative de tromper le public en lui faisant croire que quelque chose de faux, c'est vrai, la plupart du temps associée à une recommandation de transmettre le canular à autant de gens que possible. Beaucoup e-mail en garde les utilisateurs contre les virus, vers ou chevaux de Troie, certains désinformer sur les événements politiques ou sociaux, tandis que d'autres sont des canulars charité, canulars, plaisanterie, ou à vocation commerciale, par exemple en offrant des chèques cadeaux gratuitement. Une liste des canulars est fournie sur la page web, la page Web fournit des types encore plus de canulars. Un canular peut également être utilisé pour distribuer des logiciels malveillants en incitant un utilisateur à visiter une page Web qui installe les logiciels malveillants.

Chaîne e-mail est un terme utilisé pour décrire les e-mails qui vous encouragent à les transmettre à quelqu'un d'autre, les versions Internet des chaînes de lettres. [4]

6.5. Joe jobs :

Joe jobs est le terme Internet pour le courrier électronique forgé qui semble avoir été envoyé par l'une des parties, mais a en fait été forgé par quelqu'un d'autre dans le but de générer des plaintes au sujet, et nuire à la réputation d'une victime innocente. Par exemple, un " Joe jobs" pourrait spammer un message contenant des mauvaises choses à des milliers de personnes qui utilisent une adresse de retour forgé de afin de l'indignation des bénéficiaires et provoquer leur boîte aux lettres inondations John Smith des plaintes ou de ternir la réputation de l'entreprise. [4]

6.7. Malware :

Un logiciel malveillant est un logiciel conçu pour infiltrer et endommager les systèmes informatiques. Il est généralement considéré comme contenant des virus informatiques, des chevaux de Troie, des logiciels espions et des logiciels publicitaires. Ce type de logiciel est souvent envoyé en tant que non suspect d'une pièce jointe. Lorsque l'utilisateur ouvre le fichier, le logiciel malveillant s'installe. Les logiciels malveillants sont utilisés pour infecter un serveur afin que le serveur puisse être contrôlé à distance et utilisé pour envoyer des spams. Ces serveurs infectés sont appelés ordinateurs zombies. De nombreuses personnes pensent que la plupart des spams sont envoyés par un botnet, qui est un réseau de PC zombies, mais il est difficile de prouver cette hypothèse. [4]

Figure 7 : exemple de Spam email “Malware“.

6.8. Messages Bounce :

Les messages Bounce sont des e-mails non distribuables qui sont retournés à leur expéditeur. Quand une réception d'e-mail serveur reçoit un message avec une adresse non livrable, il va générer un nouveau "rebond" message à l'expéditeur présumé avertir l'utilisateur que l'e-mail est non distribuable ". Selon une étude réalisée par Ironport, le rebond des e-mails qui sont dues au spam non livrable e-mails avec l'adresse de retour forgé et donc "mal dirigé" ou renvoyé à une partie innocente, environ 9% de tout le trafic de messagerie ou 1,67 milliards de rebond des e-mails tous les jours, Bounce messages ne sont pas eux-mêmes le spam e-mails, mais elles représentent une part importante du trafic e-mail qui est due au spam. [4]

7. Les impacts causés par l’Email Spam :

En plus d’être inconvénient pour l’utilisateur de recevoir plusieurs messages indésirables, d’autres problèmes causés par le SPAM doivent aussi être considérés :

- **Perte de temps :** Chaque fois qu'un utilisateur reçoit des messages indésirables, il perd du temps en les supprimant.
- **Diminution de productivité :** Les personnes qui utilisent le courrier électronique comme outil de travail passent plus de temps à rechercher des messages importants en raison du volume de courrier indésirable.

  Il existe toujours un risque de cliquer sur des liens et d'endommager des données informatiques importantes.
- **Ne pas recevoir des emails importants :** Si votre boîte de réception est pleine de SPAM, vous ne pourrez peut-être pas recevoir certains e-mails, en particulier ceux qui sont plus lourds et nécessitent de l'espace.
- **Fraudes financières :** Certains des messages contiennent des liens vers l'installation de programmes frauduleux sur des ordinateurs ou l'incitation de personnes à remplir des données sur des sites Web d'institutions financières clonées**.**
- **Perte de messages :** À cause du grand nombre de Spam, il est possible de supprimer des messages qui étaient importants, d'oublier la lecture d'un certain email ou bien de prendre plus de temps pour répondre.
- **Recevoir du contenu indésirable :** Il y a plein de messages impropres ou offensifs envoyés vers des listes aléatoires d'emails.

  Donc vous pouvez peut-être recevoir de contenus qui ne correspondent pas à vos croyances et valeurs.

8. Les techniques pour identifier l'Email Spam :

Certaines personnes ne peuvent pas identifier facilement le SPAM. Mais de nombreux fournisseurs et sociétés de logiciels et d'informatique proposent des services pour intercepter et se protéger contre ce type de message.

Ces protections sont parfois des filtres anti-spam. Bien qu'elles soient efficaces, ces mesures peuvent classifier quelques messages légitimes comme indésirables.

Par conséquent, il est nécessaire de vérifier périodiquement la case SPAM pour s'assurer qu'aucune information importante n'a été envoyée par erreur.

Mais méfiez-vous des caractéristiques qui peuvent faire que votre message soit identifié comme SPAM :

- Message d'un expéditeur que vous ne connaissez pas auquel vous fournissez vos coordonnées personnelles.
- Des e-mails auxquels vous ne vous attendez pas, en particulier sur des sujets sans rapport avec vos intérêts quotidiens.
- Des offres de produits miraculeux, comme des médicaments pour l'amaigrissement instantané.
- Publicité avec des avantages excessifs.
- De nouvelles scandaleuses ou de théories de conspiration.
- Une newsletter d'un site web que vous n'avez jamais visité.
- Les e-mails avec un titre qui semble établir une conversation avec vous. Par exemple : "Bonjour, vous vous rappelez de moi ?"
- Des messages avec des liens vers un site web qui vous offre un cadeau.
- Des textes avec des avertissements en disant que le message ne s'agit pas de SPAM. Après tout, des emails légitimes n'ont pas besoin d'avertissement ?

9. Les techniques pour éviter d'avoir l'Email Spam :

Si vous naviguez sur internet seulement en tant qu'utilisateur, vous avez quelques astuces pour vous protéger du SPAM.

- **Maintenez votre antivirus toujours mis à jour**

Ayez un antivirus sur votre ordinateur pour bloquer tout type d'attaque à vos données personnelles. Mais cela ne garantit pas que vos informations seront toujours en sécurité.

Utilisez l'antivirus périodiquement sur votre ordinateur personnel et celui où vous travaillez.

Installez un antivirus aussi sur votre portable. Aujourd'hui nous utilisons souvent les portables pour accéder à l'internet.

- **N'informez pas vos données personnelles.**

Les données comme l'email ou vos coordonnées bancaires sont très confidentielles. Vous ne devez donc pas les informer aux pages suspectes.

Les mauvais codes envoyés à votre email peuvent transformer votre système en serveur pour l'envoi de SPAM. Et en général, il est difficile de détecter si votre ordinateur est infecté. La plupart des personnes ne découvrent un virus que quand l'ordinateur est déjà très lent ou avec des problèmes de connexion.

- **Ne partagez pas de chaines de messages**

Ne partagez pas de messages douteux. En général, ils sont utilisés pour capturer des adresses email et les utiliser pour envoyer des SPAMs sans l'approbation de l'utilisateur.

Sachez que la plupart des histoires racontées dans les messages chaînes sont fausses. Donc certifiez-vous qu'il s'agit d'un vrai message pour ne pas partager des contenus incorrects.

- **Utilisez des outils antispam**

L'Antispam est essentiel, car il dirige les messages suspects vers un dossier SPAM hors votre boîte de réception. Alors, même si vous n'avez pas cette fonctionnalité installée sur votre ordinateur, utilisez les ressources offertes par les services de messagerie.

- **Séparez les emails par catégorie**

Si possible, essayez d'avoir plus d'un email et séparez-les par catégorie. Vous pouvez, par exemple, avoir un compte que pour les abonnements de listes et de promotions. Vous arrivez donc à éviter que certains SPAMs arrivent à votre messagerie personnelle ou commerciale.

- **Ne croyez pas en toutes les promotions**

Évitez de cliquer sur les pop-ups qui vous dirigent vers des cadeaux extraordinaires. Vérifiez toujours si les cadeaux sont vraiment réels et si le site que les offres sont fiables.

Plusieurs institutions ont déjà sur ses pages des informations qui confirment ou non l'envoi de cadeaux, promotions et réductions. Donc, rappelez-vous d'analyser tous les messages que vous recevez avant le clic.

10. Types de solutions contre les Spam email :

Cette partie aborde les solutions anti-spam selon deux approches. Il existe différents types de solutions prenant place à des niveaux variés (dans l'architecture réseau). L'objectif est d'expliciter leurs différences, leurs avantages et inconvénients respectifs afin d'aider chaque personne à choisir le type de solution le plus adapté à son cas.

10.1. Au niveau d'application d'une solution anti-spam :

Selon le type de solution anti-spam, le traitement est réalisé à différents niveaux du cheminement emprunté par les messages. Il peut intervenir en 3 endroits :

10.1.1. Au niveau du poste client :

Le filtrage des messages au niveau du poste client est couramment utilisé par les particuliers, car il est adapté à leur infrastructure technique (pas de serveur de messagerie mais utilisation des services d'un FSI[6]), parce qu'il est bon marché, voire gratuit, mais aussi parce qu'il est facile à installer et à gérer. Pour ces mêmes raisons, ce type de solution anti-spam conviendra aussi à de très petites structures formées de quelques postes.

Pour les entreprises, l'anti-spam au niveau du poste client n'est pas adapté à plusieurs titres :

- Le déploiement et la maintenance sont réalisés individuellement (une mauvaise efficience en résulte).
- La solution (dans le cas où elle est payante) multipliée par le nombre de postes peut constituer un lourd investissement.
- L'utilisateur devra être formé à maîtriser cet outil. Il devra ensuite gérer et mettre à jour lui-même ses règles de filtrage, avec plus ou moins de succès (mais il est libre de le personnaliser).
- Les spams sont acheminés jusqu'à leur destination. Ils encombrent donc tous les niveaux de l'infrastructure de messagerie : liaison internet et réseau interne (bande passante), serveur de messagerie et poste client (ressources système).

10.1.2. Au niveau du serveur de messagerie :

A l'inverse du traitement des spams au niveau du client, le traitement depuis le serveur de messagerie est couramment utilisé en milieu professionnel (pour les sociétés disposant d'un tel serveur en interne). Ses avantages contrastent clairement avec les inconvénients du filtrage au niveau du client :

[6] FSI : Fournisseur de Service Internet

- Le déploiement et la maintenance sont centralisés.
- La prise en charge d'une grande quantité d'adresses email est généralement moins coûteuse (que celle du filtrage au niveau client).
- Le traitement ne requiert pas de paramétrisation de la part de l'utilisateur.
- Le spam n'est pas transmis jusqu'au poste client (moins de trafic réseau et économie des ressources en bout de chaîne).
- L'entreprise garde le contrôle total sur la solution anti-spam. Ceci est valable aussi bien pour les tâches de configuration que pour le déploiement contrôlé d'éventuelles mises à jour et correctifs (limiter le risque et évaluer l'impact par des tests).

Comme les autres solutions, le filtrage au niveau du serveur présente aussi des

Inconvénients :

- Le traitement consomme des ressources sur le serveur. Ce dernier doit alors être suffisamment puissant pour assurer le bon fonctionnement du service SMTP[7] et des fonctions anti-spam.
- La bande passante internet reste encombrée par les spams.
- L'anti-spam est adapté au serveur de messagerie et au système d'exploitation utilisé. Une modification de cet environnement peut le rendre incompatible.
- Des ressources humaines formées à l'outil sont nécessaires en interne pour l'installation, l'administration et la maintenance de l'anti-spam.

10.1.3. Au niveau d'une passerelle :

Le filtrage des messages au moyen d'une passerelle anti-spam (située à l'entrée du réseau, généralement dans une DMZ[8]) offre de nombreux avantages similaires au filtrage depuis le serveur (maintenance centralisée, coût, pas de paramétrisation par l'utilisateur).

Cette solution présente aussi d'autres avantages spécifiques :

- Le filtrage est réalisé en entrée, ce qui épargne la bande passante en interne.

[7] SMTP : Simple Mail Transfer Protocol.
[8] DMZ : demilitarized zone.

- Les ressources du serveur de messagerie situé en aval sont économisées (il ne réalise plus de filtrage et ne traite que les messages légitimes).
- Le traitement est directement réalisé sur le flux SMTP, ce qui le rend tout à fait indépendant du type de serveur de messagerie et du système d'exploitation utilisé. Une modification de l'infrastructure est donc sans effet sur le traitement des spams.

Les inconvénients d'une telle méthode sont aussi semblables aux solutions installées sur le serveur de messagerie (bande passante internet encombrée, ressources humaines nécessaires à son administration).

Concrètement, le traitement des spams au niveau d'une passerelle est réalisable de deux façons :

- En utilisant un serveur dédié : la solution logicielle prend place sur un serveur consacré à cette tâche de filtrage. Le déploiement est moins facile que pour une Appliance, mais le dépannage en cas de panne est rapide (pièces de remplacement à disposition ou serveur de secours prêt à prendre la relève).
- En utilisant un boîtier de filtrage autonome (« Appliance ») : l'installation est facilitée mais une panne matérielle est problématique puisqu'elle ne peut être résolue rapidement par l'entreprise (à l'inverse d'un serveur facilement réparable, une Appliance est composée de matériel propriétaire). La redondance est aussi très mauvaise, à moins d'investir dans deux boîtiers.

10.2. Techniques anti-spam Email :

Cette partie présente les principaux types de filtres permettant le tri de la messagerie.

10.2.1. Listes noires et RBL :

Une liste noire rassemble des adresses de machines ou domaines bannis (car permettant l'envoi ou la transmission de spams).

Un RBL (Realtime Blackhole List) : est une liste maintenue en temps réel (son utilisation étant généralement accessible au public).

Il arrive malheureusement que des serveurs soient blacklistés à tort. En fonction de la

RBL utilisée, le risque de générer des faux positifs est plus ou moins élevé. Plusieurs différences peuvent expliquer ces disparités :

- Différents critères peuvent définir qui est considéré comme spammeur.
- Collectes différentes des nouvelles entrées de la liste.
- Procédures de retrait des machines ou domaines listés différentes.
- Autre type de liste (de relais ouverts, proxy ouverts, spammeurs, etc.).

De façon plus générale, les listes noires sont administrées selon 3 catégories d'organisations :

- Les associations à but non lucratif dédiées à la lutte anti-spam.
- Les administrateurs regroupés pour combattre le spam.
- Les administrateurs indépendants exploitant une liste pour leur utilisation personnelle mais qui en autorisent l'accès au public.

Prendre en compte ces paramètres permet d'évaluer en partie un RBL. A priori, il est conseillé pour les entreprises sensibles au problème des faux positifs de privilégier les

RBL maintenues par les associations, moins sujettes à blacklister par erreur des adresses ou domaines légitimes.

Une étude réalisée entre mi-mars et fin octobre 2004 représente bien l'ampleur des erreurs commise : l'organisation « Halte Au Spam » a suivi à cette période 72 grandes organisations françaises (dont une part cotée au CAC 40) afin de contrôler leur présence éventuelle parmi une vingtaine de listes noires. Voici les résultats :

- 38 organisations sur 72 ont été listées à au moins un moment de la période concernée.
- L'entité la plus blacklistée est un FAI (présent sur 15 listes).
- La liste noire la plus agressive était australienne, bloquant 14 organisations sur 72.
- La réputée liste britannique Spamhaus SBL n'a listé aucune des 72 organisations suivies.

Manifestement, un choix scrupuleux des listes utilisées est primordial.

Un autre problème grève lourdement l'efficacité des listes noires : l'envoi de spams à partir d'ordinateurs « zombies ». Blacklister ces machines émettrices de spam n'est pas possible puisque les connexions internet grand public utilisent habituellement des adresses IP allouées de façon dynamique. Par ailleurs, le domaine du FAI ne doit pas être banni sous peine de pénaliser la totalité des abonnés. Ceci explique d'ailleurs pourquoi l'étude ci-dessus avait relevé qu'un FAI avait été banni auprès de 15 listes.

Efficace auparavant, les listes noires sont de moins en moins performantes face aux méthodes d'envoi récentes. Bruno Rasle (co-auteur d'« Halte Au Spam » annonçait à ce sujet début 2007 que cette technique était désormais dépassée [JDN06].

10.2.2. Listes blanches :

Par opposition aux listes noires, les listes blanches contiennent tous les expéditeurs de confiance.

Utilisée dans la plupart des cas en complément d'autres techniques, la liste blanche est très appréciée car elle dispense l'anti-spam d'analyser le message. De plus, le risque de faux positif est totalement écarté (pour les expéditeurs spécifiés dans la liste).

En principe, une liste blanche est initialement vide : elle se remplit au fur et à mesure des messages légitimes reçus (ce processus d'apprentissage étant automatisé dans la quasi-totalité des outils).

10.2.3. Listes grises :

Une liste grise permet de se prémunir du spam par un système de rejet temporaire du message.

Lorsqu'un message est reçu, le serveur crée un triplet formé de :

- L'adresse IP du serveur émetteur.
- L'adresse email de l'expéditeur.
- L'adresse email du destinataire.

Si ce triplet est déjà connu, le message est acheminé. Sinon, le message est temporairement rejeté (un code de refus temporaire est envoyé au serveur émetteur).

Si le serveur émetteur est légitime, il réexpédiera le message plus tard (un serveur envoyant des spams ne le faisant habituellement pas). Le message est alors accepté

(le triplet étant placé en liste blanche). Toutefois, un temps d'attente trop court entre les deux messages cause aussi le refus du deuxième message (ce temps étant paramétrable).

Selon Bruno Rasle, le greylisting est globalement satisfaisant mais ne doit pas être utilisé seul :

« C'est une technique efficace. Elle est facile à implémenter et permet en premier niveau, d'écrémer rapidement. Mais elle ne suffit pas. Il faut la compléter par d'autres approches. Le greylisting pose en effet comme postulats que les serveurs de messagerie sont bien configurés et que les PC zombies ne retransmettent pas. C'est une vision un peu optimiste. »

Ajoutons également certains points sensibles relevés par Fabrice Prigent de l'Université de Toulouse 1 dans son retour d'expérience :

- Les services disposant de nombreux serveurs traitant l'envoi de messages (p.ex. Hotmail) risquent d'être régulièrement refoulés puisque le deuxième envoi ne se fait pas forcément avec la même adresse IP d'émetteur (le triplet n'étant par conséquent plus le même). Former le triplet avec une part de l'adresse (les 3 premiers bytes par exemple) résout le problème.
- Lorsque plusieurs MX sont utilisés, les triplets doivent être stockés dans une base unique.
- Certains serveurs ne réémettent pas les messages à cause d'une mauvaise interprétation du code d'erreur 450 (échec temporaire) considéré comme code 550 (échec définitif). La seule solution est de les placer en liste blanche.

10.2.4. Analyse des URL :

L'analyse des URL spécifiées dans le corps du message est un bon moyen pour détecter un spam (leur contrôle se fait la plupart du temps au moyen d'une liste noire d'URL).

10.2.5. Analyse des pièces jointes :

L’analyse des pièces jointes est une technique supplémentaire permettant de détecter les spams, en principe lorsqu’ils véhiculent un malware ou du contenu reconnu comme étant du spam (dans un fichier PDF, GIF, etc.).

11. Conclusion :

Enfin, les Email Spam augment de jour en jour, et devient plus en plus dangers. Les informations des internautes peuvent être attaques par ce type de menace informatique, donc, il faut détecter et filtre les Email Spam pour se protège.

Dans le prochain chapitre, on va parler de nouveau type de détection plus élevée qu’est “ le Deep Learning “.

Chapitre2 :

Deep Learning

1. Introduction :

L'apprentissage automatique et l'IA ont changé le monde qui nous entoure ces dernières années grâce à leur innovation de rupture. De plus, ce sont les différentes techniques d'apprentissage en profondeur qui amènent l'apprentissage automatique à un tout autre niveau où les machines peuvent apprendre à discerner les tâches, inspirées par le réseau neuronal du cerveau humain. C'est la raison pour laquelle nous avons le contrôle vocal sur nos smartphones et télécommandes TV. Dans ce chapitre, nous allons présenter tout d'abord l'Intelligence Artificielle, la Machine Learning, enfin, on va parler de Deep Learning.

2. Définition d'Intelligence Artificielle :

Une intelligence artificielle est une technologie capable de produire des résultats similaires à ceux issus du cerveau humain. Pour entraîner une intelligence artificielle à reconnaître des formes circulaires dans des images contenant aléatoirement des formes carrées ou des formes circulaires, on lui montre un grand nombre d'exemples d'images d'un cercle et un grand nombre d'exemples d'images d'un carré. Plus le nombre d'exemples est grand, plus la machine devient capable de reconnaître seule les formes circulaires, car elle a en mémoire beaucoup de cas de figure possibles avec lesquels elle peut comparer l'image qu'elle traite. C'est cette technique qu'on appelle « apprentissage automatique » (machine Learning).

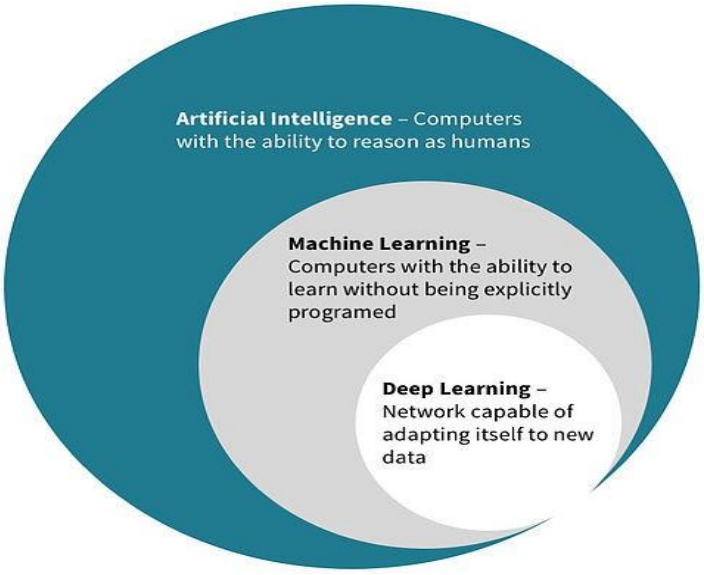


Figure 8 : La relation entre IA, ML, DL

3. Définition de Machine Learning :

Le ML est une sous-section de l'intelligence artificielle qui équipe les ordinateurs pour apprendre à partir de données sans avoir à programmer explicitement l'algorithme d'apprentissage. Le modèle de ML capable de prendre des décisions précises comprend de nombreuses étapes commençant par la phase de collecte de données. Les données collectées sont généralement divisées en deux parties, à savoir un ensemble de formation qui entraîne le modèle ML et un ensemble de tests utilisé pour déterminer les performances du modèle entièrement formé. Les données collectées sont ensuite prétraitées lors de la phase de préparation des données. Ensuite, un algorithme approprié pour résoudre le problème en question est déterminé. Une fois le modèle formé, il peut être évalué sur un nouvel ensemble de données. Les algorithmes de ML les plus utilisés sous chacune de ces classes sont abordés dans les sections suivantes.

3.1. Les types de la Machine Learning :

3.1.1. Apprentissage supervisé :

Les modèles d'apprentissage automatique qui utilisent des ensembles de données étiquetés pour la formation effectuent un apprentissage supervisé. L'algorithme s'appuie sur les étiquettes de sortie pour former une relation entre la variable d'entrée ou la variable indépendante et la variable de sortie ou la variable dépendante. L'apprentissage supervisé peut être classé en problèmes de régression et de classification en fonction de la tâche effectuée par l'algorithme. À l'aide de ces données, un modèle d'apprentissage supervisé qui prédit une valeur de prix numérique peut être développé pour résoudre ce problème de régression. Les algorithmes tels que la régression linéaire et la régression logistique sont des algorithmes de ML populaires basés sur la régression qui sont utilisés dans l'apprentissage supervisé. La deuxième classe de problèmes d'apprentissage supervisé est connue sous le nom de problèmes de classification. Les tâches de classification impliquent de mapper les données de test à deux catégories ou plus.

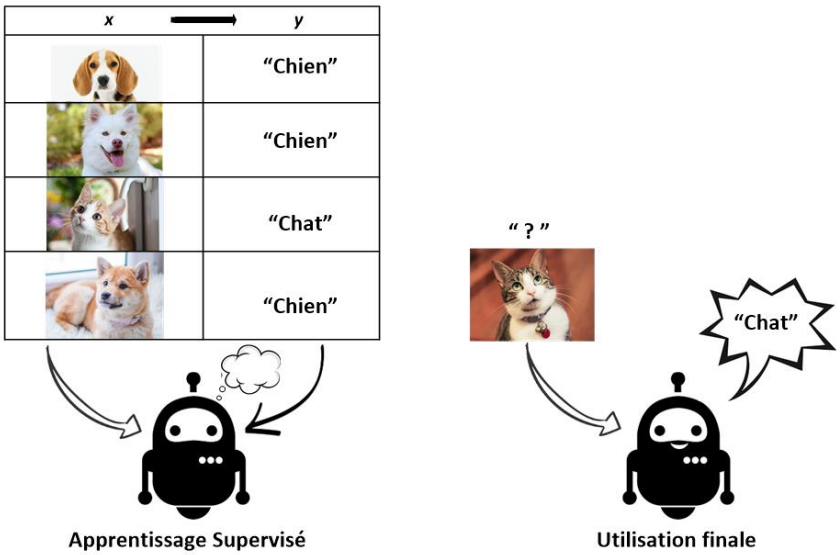


Figure 9 : exemple d'apprentissage supervisé

3.1.2. L'apprentissage non supervisé :

L'apprentissage non supervisé implique la découverte de modèles auparavant inconnus à partir de données non étiquetées. Contrairement aux algorithmes supervisés, les algorithmes non supervisés peuvent aider à résoudre un plus large éventail de problèmes, car il est plus facile d'obtenir des données non étiquetées. Des points de données similaires sont regroupés. Cela aide à identifier les modèles insoupçonnés dans les données. La réduction de dimensionnalité est une technique qui fusionne les entités corrélées en une seule entité et, par conséquent, simplifie les données disponibles sans perdre trop d'informations. En utilisant cette technique, le modèle s'entraînera plus rapidement et moins d'espace mémoire est nécessaire pour contenir les données. L'objectif des algorithmes d'apprentissage des règles d'association est d'explorer des fichiers de données volumineux et de découvrir des modèles intéressants et de nouvelles relations entre les différentes caractéristiques des données.

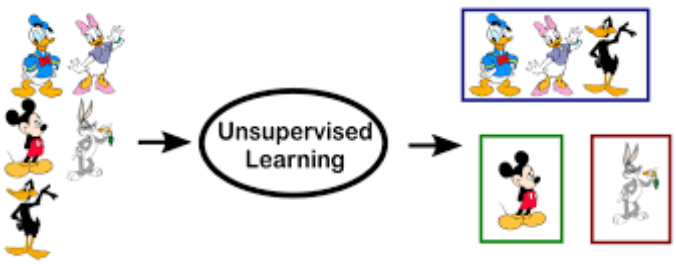


Figure 10 : Exemple d'apprentissage non supervisé

3.1.3. Apprentissage semi-supervisé :

Dans l'apprentissage semi-supervisé, les algorithmes peuvent gérer une combinaison principalement composée de données non étiquetées et d'une quantité beaucoup plus faible de données étiquetées. Ceci est particulièrement utile dans le domaine médical car il faut généralement beaucoup de temps et l'expertise des professionnels de la santé pour étiqueter les images de numérisation médicale. Les algorithmes d'apprentissage semi-supervisés ne nécessiteraient que quelques images étiquetées, ce qui permettrait d'économiser beaucoup de temps et d'efforts.

4. Machine Learning vers Deep Learning :

L'apprentissage automatique signifie que les ordinateurs apprennent à partir de données à l'aide d'algorithmes pour effectuer une tâche sans être explicitement programmés. L'apprentissage en profondeur utilise une structure complexe d'algorithmes modélisés sur le cerveau humain. Cela permet le traitement de données non structurées telles que des documents, des images et du texte. L'apprentissage automatique est un type d'intelligence artificielle. Le Deep Learning est une partie particulièrement complexe du Machine Learning. Pour le décomposer en une seule phrase :

L'apprentissage en profondeur est un sous-ensemble spécialisé de l'apprentissage automatique qui, à son tour, est un sous-ensemble de l'intelligence artificielle. En d'autres termes, l'apprentissage en profondeur est l'apprentissage automatique, Mais creusons un peu plus.

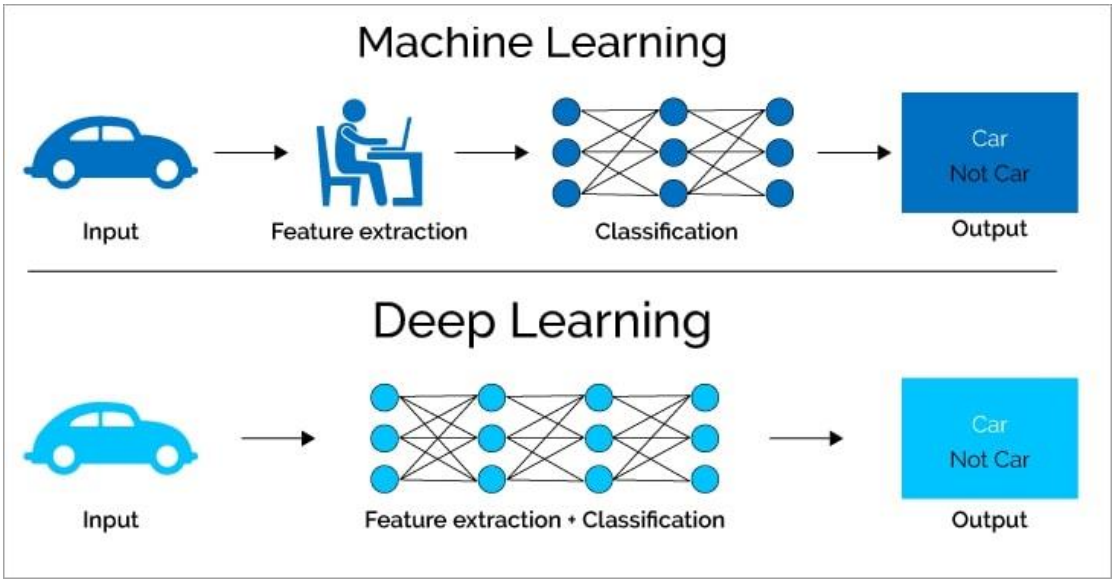


Figure 11 : Machine Learning vs Deep Learning

5. Définition Deep Learning :

L'apprentissage aux profondeurs est une autre branche de l'IA. Contrairement à ML, DL ne traite pas toutes les fonctionnalités de la même manière. DL apprend d'abord quelles fonctionnalités ont un impact significatif sur le résultat et sur cette base, le DL crée une combinaison de toutes les fonctionnalités pour le processus d'apprentissage. Cette propriété de DL demande beaucoup de données. Un modèle DL a au moins une ou plusieurs couches cachées. Les couches masquées se situent entre les couches d'entrée et de sortie. Couches masquées sont des couches intermédiaires à travers lesquelles l'algorithme DL apprend quelle combinaison de fonctionnalités peut être utilisée pour obtenir les meilleurs résultats cohérents. DL est largement utilisé dans divers problèmes de classification et de régression supervisés. La formation des algorithmes d'apprentissage en profondeur se fait par rétropropagation, l'algorithme apprenant les paramètres de chaque couche à partir de la couche suivante immédiate et ainsi de suite. Certains des algorithmes DL bien connus sont les réseaux de neurones récurrents (RNN), les réseaux de neurones à convolution (CNN) et les réseaux de neurones contradictoires généraux (GAN). Généralement, ces modèles comportent de nombreux blocs de traitement de données différents avant les couches cachées. Certains des blocs couramment utilisés sont la convolution, la mise en commun et la normalisation. Le bloc de convolution utilise des noyaux (ou des filtres) pour convoluer plusieurs entités à la fois en fonction de la taille du noyau pour obtenir les informations spatiales sur les données. Le bloc de regroupement est utilisé pour réduire la taille de

l'ensemble de fonctionnalités en prenant la moyenne ou le maximum de plusieurs fonctionnalités. Cela permet d'augmenter la vitesse de calcul de l'algorithme et, en même temps, de préserver les informations. La normalisation est utilisée pour normaliser les données dans une entité. En effet, en raison de plusieurs étapes de traitement, les données peuvent changer de manière significative, et si une entité a des nombres relativement plus élevés qu'une autre entité, alors l'entité avec un nombre plus élevé domine les résultats. Pour éviter cela, nous normalisons les données entre les entités afin que toutes les entités soient pondérées de manière égale avant d'entrer dans les couches masquées.

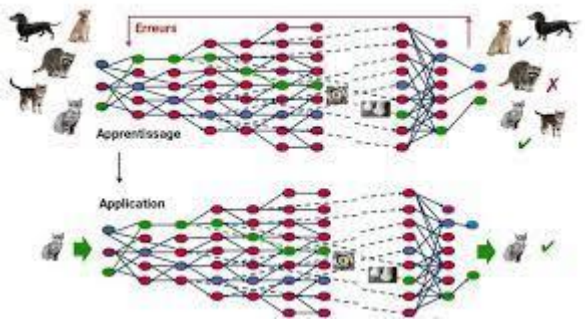


Figure 12 : Apprentissage en profondeur

5.1. Techniques Deep Learning :

5.1.1. Réseaux de neurones convolutionnels :

CNN Convolutional Neural Networks est un type avancé et à haut potentiel du modèle classique de réseau de neurones artificiels. Il est conçu pour s'attaquer à une plus grande complexité, au prétraitement et à la compilation de données. Il se réfère à l'ordre d'arrangement des neurones présents dans le cortex visuel d'un cerveau animal.

Les CNN peuvent être considérés comme l'un des modèles flexibles les plus efficaces pour se spécialiser dans les données d'image et non d'image. Ceux-ci ont quatre organisations différentes :

• Il est constitué d'une seule couche d'entrée, qui est généralement un agencement bidimensionnel de neurones pour l'analyse des données d'image primaires, qui est similaire à celui des pixels photo.

• Certains CNN consistent également en une couche de sortie unidimensionnelle de neurones qui traite les images sur leurs entrées, via les couches convolutives connectées dispersées.

• Les CNN ont également la présence d'une troisième couche dite couche d'échantillonnage pour limiter le nombre de neurones impliqués dans les couches réseau correspondantes.

• Dans l'ensemble, les CNN ont une ou plusieurs couches connectées qui connectent l'échantillonnage aux couches de sortie.

Ce modèle de réseau peut aider à dériver des données d'image pertinentes sous la forme d'unités ou de blocs plus petits. Les neurones présents dans les couches de convolution sont responsables du groupe de neurones de la couche précédente.

Une fois les données d'entrée importées dans le modèle convolutif, la construction du CNN comporte quatre étapes :

• Convolution : le processus dérive des cartes d'entités à partir des données d'entrée, suivies d'une fonction appliquée à ces cartes.

• Max-Pooling : Cela aide CNN à détecter une image en fonction de modifications données.

• Aplatissement : à cette étape, les données générées sont ensuite aplaties pour qu'un CNN les analyse.

• Connexion complète : elle est souvent décrite comme une couche cachée qui compile la fonction de perte pour un modèle.

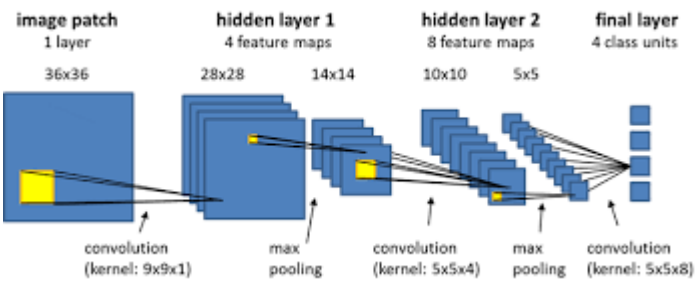


Figure 13 : Réseaux de neurones convolutionnels

Les CNN sont adéquats pour les tâches, y compris la reconnaissance d'images, l'analyse d'images, la segmentation d'images, l'analyse vidéo et le traitement du langage naturel. Cependant, il peut y avoir d'autres scénarios où les réseaux CNN peuvent s'avérer utiles comme :

• Ensembles de données d'images contenant l'analyse de documents OCR

• Toutes les données d'entrée bidimensionnelles qui peuvent être ensuite transformées en données unidimensionnelles pour une analyse plus rapide

• Le modèle doit être impliqué dans son architecture pour produire une sortie.

5.1.2. Réseau neuronal artificiel :

ANN signifie Artificial Neural Networks. C'est un système informatique déduit des méthodes de traitement et de la capacité d'apprentissage d'un cerveau humain. Il s'agit essentiellement d'une représentation d'un cerveau humain et de son fonctionnement. L'objectif principal du réseau de neurones artificiels est, comme son nom l'indique, le réseau de neurones qui traite tout ce que vous interprétez et essaie de l'apprendre par la suite. Un cerveau humain est constitué de milliards de neurones.

Le neurone est fondamentalement une unité de base du cerveau humain. Une unité de base désigne la plus petite unité indivisible et dans le cas du cerveau humain,

C'est un neurone. Les organes sensoriels présents dans notre corps comme la bouche, la langue, les oreilles, les yeux, la peau détectent l'environnement et envoient un signal au cerveau. Ces signaux sont reçus par les neurones. Les neurones interprètent et traitent les signaux et génèrent une sortie appropriée pour prendre les mesures appropriées à un moment donné. Ainsi, lorsque nous essayons d'obtenir cette fonctionnalité artificiellement, elle relève d'un réseau de neurones artificiels. Vous trouverez ci-dessous un schéma d'un nœud qui est essentiellement une réplique du neurone et décrit la fonctionnalité. Un nœud est divisé en deux parties principales. Le premier étant la partie sommation et le second étant la partie fonction. Comme votre cerveau est composé de millions de neurones, le réseau sera également composé de plusieurs nœuds pour générer la sortie. À chaque nœud, il y aura un signal et chaque

signal se verra attribuer son poids respectifs (comme pour x1- > w1 et x2- > w2 et ainsi de suite comme indiqué dans la figure ci-dessous).

Ensuite tout cela passera par la partie sommation qui calculera la somme pondérée. Par la suite, cette somme pondérée est entrée dans la partie fonction qui est essentiellement la fonction de transfert. Le travail principal de la fonction de transfert est que si nous fournissons une entrée à la fonction, une sortie appropriée ou l'action désignée sera générée. Donc, D'une certaine manière, cette fonction d'activation génère ou définit une sortie particulière pour un nœud donné en fonction de l'entrée donnée qui est fournie. La sortie générée est définie par la fonction (Figure 13).

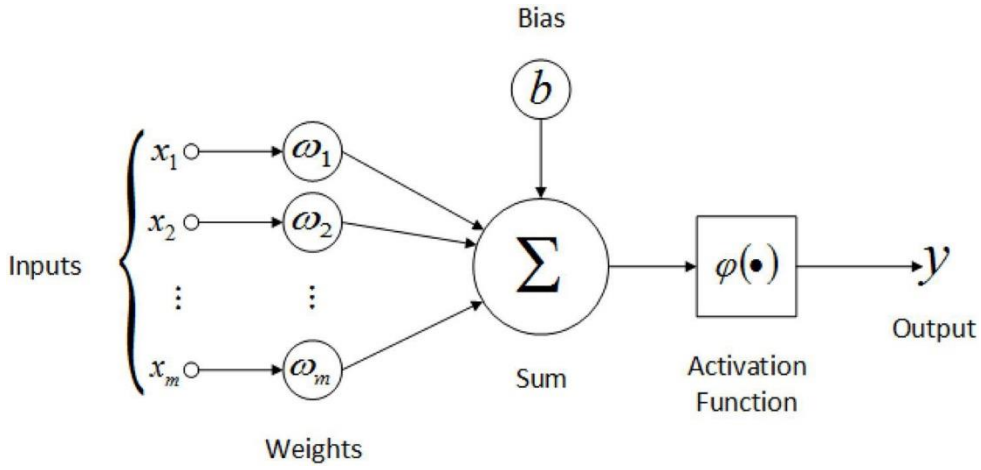


Figure 14 : Structure d'ANN

5.1.3. Réseaux antagonistes génératifs :

Il s'agit d'une combinaison de deux techniques d'apprentissage en profondeur des réseaux de neurones - un générateur et un discriminateur. Alors que le réseau générateur produit des données artificielles, le discriminateur aide à discerner entre une vraie et une fausse donnée.

Les deux réseaux sont compétitifs, car le générateur continue de produire des données artificielles identiques aux données réelles et le discriminateur détecte en permanence les données réelles et irréelles. Dans un scénario où il est nécessaire de créer une bibliothèque d'images, le réseau Generator produirait des données simulées pour les images authentiques. Il générerait alors un réseau de neurones de déconvolution.

Il serait ensuite suivi d'un réseau de détecteurs d'images pour différencier les images réelles des fausses. A partir d'une chance de précision de 50%, le détecteur doit développer sa qualité de classification puisque le générateur se développerait mieux dans sa génération d'images artificielles. Une telle concurrence contribuerait globalement à l'efficacité et à la rapidité du réseau.

Fonctionne mieux dans :

• Génération d'images et de textes

• Amélioration d'images

• Processus de découverte de nouveaux médicaments

5.1.4. Cartes auto-organisées :

Les SOM ou cartes auto-organisatrices fonctionnent à l'aide de données non supervisées qui réduisent le nombre de variables aléatoires dans un modèle. Dans ce type de technique d'apprentissage en profondeur, la dimension de sortie est fixée comme un modèle bidimensionnel, chaque synapse se connectant à ses nœuds d'entrée et de sortie.

Au fur et à mesure que chaque point de données est en compétition pour sa représentation de modèle, le SOM met à jour le poids des nœuds les plus proches ou des unités de meilleure correspondance

(BMU). En fonction de la proximité d'un BMU, la valeur des poids change. Comme les poids sont considérés comme une caractéristique de nœud en soi, la valeur représente l'emplacement du nœud dans le réseau.

Fonctionne mieux dans :

• Lorsque les jeux de données ne sont pas accompagnés de valeurs d'axe Y

• Explorations de projets pour analyser le cadre de l'ensemble de données

• Projets créatifs en musique, vidéos et texte avec l'aide de l'IA

5.1.5. Machines Boltzmann :

Ce modèle de réseau n'a pas de direction prédéfinie et a donc ses nœuds connectés dans un arrangement circulaire. En raison de cette unicité, cette technique d'apprentissage en profondeur est utilisée pour produire des paramètres de modèle.

Différent de tous les modèles de réseau déterministes précédents, le modèle des machines de Boltzmann est appelé stochastique.

Fonctionne mieux dans :

• Surveillance du système

• Mise en place d'une plateforme de recommandation binaire

• Analyser des ensembles de données spécifiques

5.1.6. Apprentissage par renforcement en profondeur :

Avant de comprendre la technique du Deep Renforcement Learning, l'apprentissage par renforcement fait référence au processus par lequel un agent interagit avec un environnement pour modifier son état. L'agent peut observer et agir en conséquence, l'agent aide un réseau à atteindre son objectif en interagissant avec la situation.

Ici, dans ce modèle de réseau, il y a une couche d'entrée, une couche de sortie et plusieurs couches multiples cachées - où l'état de l'environnement est la couche d'entrée elle-même. Le modèle fonctionne sur les tentatives continues de prédire la récompense future de chaque action entreprise dans l'état donné de la situation.

Fonctionne mieux dans :

• Jeux de société comme les échecs, le poker

• Voitures sans chauffeur

• Robotique

• Gestion de l'inventaire

• Tâches financières telles que la tarification des actifs

5.1.7. Auto-encodeurs :

L'un des types de techniques d'apprentissage en profondeur les plus couramment utilisés, ce modèle fonctionne automatiquement en fonction de ses entrées, avant de prendre une fonction d'activation et un décodage de sortie final. Une telle formation de goulot d'étranglement conduit à produire des catégories de données moindres et à tirer parti de la plupart des structures de données inhérentes.

Les types d'auto-encodeurs sont :

• Clairsemé : Où les couches cachées sont plus nombreuses que la couche d'entrée pour que l'approche de généralisation ait lieu afin de réduire le surajustement. Il limite la fonction de perte et empêche l'auto-encodeur de surutiliser tous ses nœuds.

• Débruitage : Ici, une version modifiée des entrées est transformée en 0 au hasard.

• Contractive : Ajout d'un facteur de pénalité à la fonction de perte pour limiter le surajustement et la copie de données, en cas de couche cachée plus nombreuse que la couche d'entrée.

• Empilé : Pour un encodeur automatique, une fois qu'une autre couche cachée est ajoutée, cela conduit à deux étapes d'encodage à celle d'une phase de décodage.

Fonctionne mieux dans :

• Détection de fonctionnalités

• Mettre en place un modèle de recommandation convaincant

• Ajouter des fonctionnalités à de grands ensembles de données

5.1.8. Backpropagation :

La rétro-propagation est utilisée dans le réseau à rétroaction. Cet algorithme utilise une technique appelée descente de gradient ou règle delta pour rechercher une valeur minimale de la fonction d'erreur dans l'espace des poids. Dans cet algorithme,

nous calculons d'abord l'erreur, c'est-à-dire à quelle distance se trouve la sortie de notre modèle de celle réelle, puis nous vérifions si cette erreur est minimale ou non. Si l'erreur est énorme, les paramètres qui incluent les pondérations et le biais sont mis à jour. Après la mise à jour, nous vérifions à nouveau l'erreur. Nous devons répéter ce processus

Jusqu'à ce que notre erreur devienne minimale. Une fois que notre erreur est minimisée, nous pouvons alimenter les entrées de notre modèle et produire la sortie.

Considérez le graphique ci-dessous.

Figure 15 : Backpropagation ' Global Loss Minimum '

5.1.9. <u>Descente en dégradé :</u>

Dans le contexte mathématique, le gradient fait référence à une pente qui a un angle mesurable et peut être représentée dans une relation entre des variables. Dans cette technique d'apprentissage en profondeur, la relation entre l'erreur produite dans le réseau de neurones et celle des paramètres de données peut être représentée par "x" et "y". Étant donné que les variables sont dynamiques dans un réseau de neurones, l'erreur peut donc être augmentée ou diminuée avec de petits changements.

De nombreux professionnels visualisent la technique comme celle d'un sentier fluvial descendant les pentes de la montagne. L'objectif d'une telle méthode est — de trouver la solution optimale. Puisqu'il y a la présence de plusieurs solutions minimales locales dans un réseau de neurones, dans lesquelles les données peuvent être piégées et

conduire à des compilations plus lentes et incorrectes, il existe des moyens de s'abstenir de tels événements.

En tant que terrain de la montagne, il existe des fonctions particulières dans le réseau de neurones appelées fonctions convexes, qui permettent aux données de circuler aux débits attendus et d'atteindre leur minimum le plus élevé. Il peut y avoir des différences dans les méthodes prises par les données entrant dans la destination finale en raison de la variation des valeurs initiales de la fonction.

Fonctionne mieux dans :

• Mise à jour des paramètres dans un modèle donnée

6. Conclusion :

Le Deep Learning est un domaine important qui a nous facilite beaucoup de choses, dans ce chapitre, on a parlé de l'intelligence Artificiel, Machine Learning, Deep Learning et ses techniques. Dans le prochain chapitre, on va faire la conception et la description de notre système

Chapitre3 : Conception et Description de notre Projet

1. Introduction :

En tant que le Spam Email est un gros problème qui menace les internautes, il faut le réduire et détruire. Dans ce chapitre on va créer un système qui détecter et filtrer les Spam Email en utilisant le Deep Learning et ses techniques, mais, tout d'abord on va voir et parler de : l'architecture du système proposée, les travaux connexes, la base de données utilisée et enfin, les techniques d'application pour détecter le Spam Email.

2. L'architecture du système proposé :

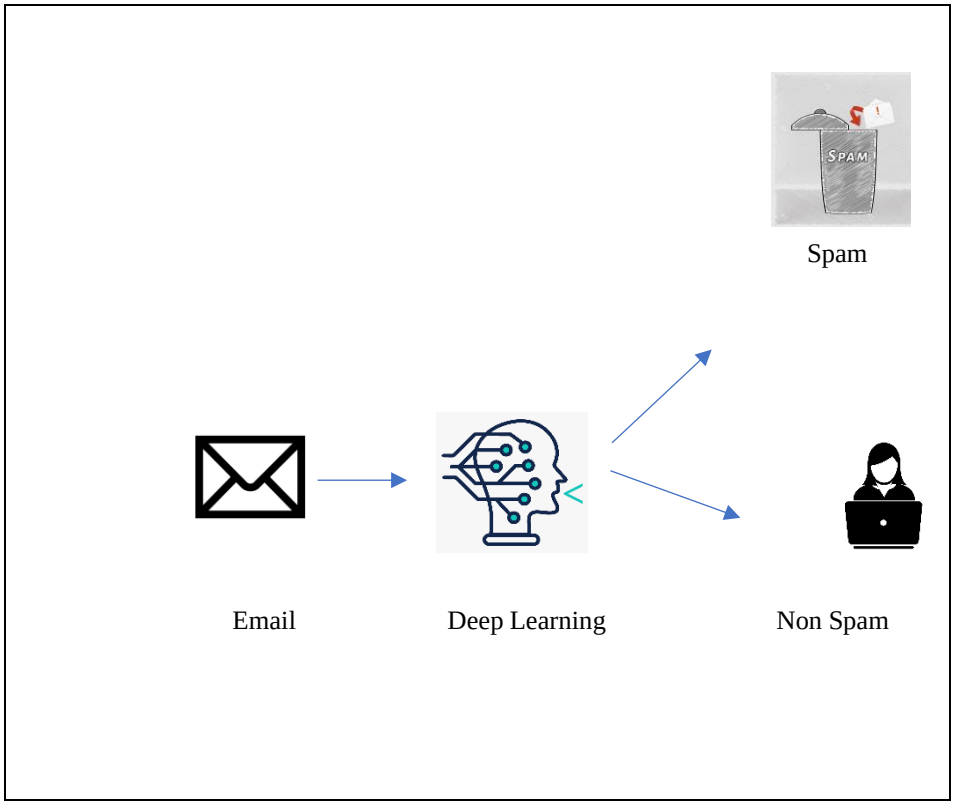


Figure 16 : L'architecture du système proposée

3. Les travaux connexes :

Le spam email est un problème sérieux qui menace la sécurité de ses destinataires. Par conséquent, de nombreux chercheurs ont proposé des algorithmes de Deep Learning pour le filtrer et le détruire.

Safaa Magdy et autres [5] ont construit un classificateur en temps réelle utilisent la puissance de l'application de réseaux de neurones avec des hyperparamètres réglés

dans le but d'une classification précise des e-mails, tels que le spam/spam ou le phishing, avec un taux de réussite de 99,33 %

Esraa Abdelnabi et Qusai Yassin [6] ont proposé un modèle d'apprentissage en profondeur appelé BiLSTM qui utilise un réseau de neurones optimisé, qui utilise par défaut l'incorporation de mots Keras ; Chaque mot est représenté par un entier unique, avec un taux estimé à 96 %.

Shreyasi Sinha, Isha Ghosh et Suresh Chandra Satapathy et autre [7], ont proposé un modèle basé sur la rétropropagation et la rétropropagation avec Momentum pour effectuer la détection de spam. Les auteurs ont optimisé le modèle en utilisant SGO (Social Group Optimisation) pour améliorer les performances de classification. Le réseau de neurones est utilisé pour travailler avec tous les types de données (texte, audio, image, etc.) à des fins de classification et de regroupement. L'utilisation de la rétropropagation a un inconvénient qui est qu'elle nécessite plus d'itérations et augmente donc le temps de calcul.

Des approches plus sophistiquées ont été utilisées par M. ALAUTHMAN et d'autres dans [8], car ils ont proposé un détecteur de spam NN récurrent profond avec une précision de 98,7 %.

Soni et autre [9] ont proposé un modèle d'apprentissage en profondeur nommé THEMIS qui utilise un RCNN amélioré pour reconnaître les e-mails de spam montrant l'en-tête et le corps de l'e-mail à la fois au niveau des caractères et au niveau des mots. Les résultats des tests ont donné une précision de 99,84 % pour THEMES, ce qui est supérieur à la fois à LSTM et à CNN en ce qui concerne leur expérience.

Hassanpur et al. [10] représentent les e-mails aux vecteurs en utilisant la bibliothèque word2vec au lieu d'utiliser des méthodes basées sur des règles. Les représentations vectorielles sont introduites dans un NN qui est le modèle d'apprentissage. Leur approche atteint une précision de plus de 96 % par rapport aux algorithmes d'apprentissage automatique standard.

Seth et autre [11] ont proposent un modèle CNN hybride analysant à la fois le contenu textuel et visuel de l'e-mail pour le classer en spam ou ham. Leur modèle atteint une précision élevée de 98,87 %.

Ezpeleta et al. [12] améliorent la précision de la classification des spams à l'aide de classificateurs de filtrage bayésiens jusqu'à 99,21 % en ajoutant une fonction de score de polarité qui reflète la sémantique du contenu des e-mails, ce qui conclut que l'analyse des sentiments des e-mails peut aider à détecter les spams.

Reference	Année	Technique Utilisé	Base Donnée	Précision
[5]	2022	ANN	SPAM Assian Phishing Corpus	99,35%
[6]	2021	BiLSTM	2113 Spam 3113 Non Spam	96%
[7]	2021	Rétropropagation + Momentum	UCI	93,35%
[8]	2020	ANN récurant	1813 Spam 2788 Non Spam	98,7%
[9]	2019	Themis	7782 Spam 997 Non Spam	99,84%
[10]	2018	NN	Un ensemble de donnée ouvert	96%
[11]	2017	CNN	_	98,87%
[12]	2016	Bayesian	_	99,21%

Table 1 : Résumé de travaux connexes

4. La Base de Donnée :

On a utilisé une base de données de UCL qu'est un ensemble de données qui contient 4600 courriers électroniques (1813 Spam et 2787 non Spam), on a 3220 (70%) email pour l'entrainement et 1380 (30%) email pour le teste, on a obtenu une matrice de 4600 lignes et 58 colons. L'ensemble de données comprend un ensemble de caractéristiques extraites de chaque email (on a obtenu 57 caractéristiques). Ces derniers représentent les fréquences de certains mots discriminants dans le corps du message.

Base de Données	Spam Email	Non Spam Email	Total
UCL	1813	2787	4600

Table 2 : Base de Données information

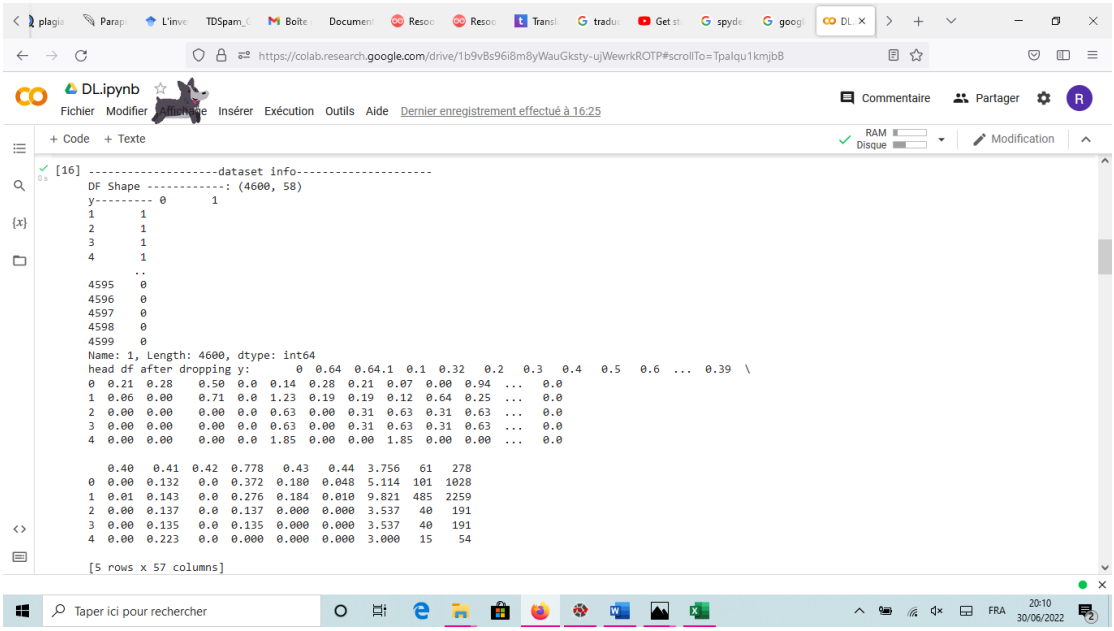


Figure 17 : L'affichage d'information de base de données

5. Technique d'application pour détecter les Spam Email :

Récemment, il a été démontré que les réseaux de neurones réussissaient à détecter les logiciels malveillants et à classer les spams Email. La force des NN réside dans l'utilisation d'une ou de quelques couches cachées qui produisent un modèle non linéaire qui capture les interactions difficiles entre les caractéristiques d'entrée et la classe de sortie cible. L'apprentissage en profondeur augmente la flexibilité de la conception du modèle et sa précision par rapport aux algorithmes d'apprentissage classiques. Il surpasse les autres solutions à bien des égards, en particulier en termes de capacité d'extrapolation pour de nouveaux exemples à partir d'un ensemble de données de formation limité. Notre travail étudie la puissance de l'application de réseaux de neurones avec des hyperparamètres réglés dans le but d'une classification précise des e-mails comme non spam/spam ou phishing. Le temps de formation et le temps de test sont surveillés car notre objectif est de construire un classificateur en temps réel. De plus, nous gardons un œil sur la précision de la validation pour assurer la capacité d'extrapolation de notre classificateur développé.

6. Conclusion :

Après d'voir vu l'architecture de notre système, ensuite on parler de quelques travaux connexes, on a fait une partite description sur notre base de données et on a donné les résultats obtenus, enfin on a parlé de technique qui on a utilisé pour détecter le Spam Email. Dans le prochain et le dernier chapitre on va faire l'implémentation de notre projet.

Chapitre 4 : L'implémentation du Système

1. Introduction :

Dans le président chapitre, nous avons présenté notre système qui consiste à la proposition d'une approche pour la détection des Spam Email en utilisent le Deep Learning. Dans ce chapitre, on va faire une description du matériel, logiciel, langage et l'environnement de programmation utilisé et enfin, des captures d'écran sur le code source de notre projet.

2. Langage de programmation :

2.1.Python :

Python est un langage de programmation interprété, multiparadigme et multiplateformes. Il favorise la programmation impérative structurée, fonctionnelle et orientée objet. Il est doté d'un typage dynamique fort, d'une gestion automatique de la mémoire par ramasse-miettes et d'un système de gestion d'exceptions ; il est ainsi similaire à Perl, Ruby, Scheme, Smalltalk et Tcl.

Le langage Python est placé sous une licence libre proche de la licence BSD4 et fonctionne sur la plupart des plates-formes informatiques, des smartphones aux ordinateurs centraux5, de Windows à Unix avec notamment GNU/Linux en passant par macOS, ou encore Android, iOS, et peut aussi être traduit en Java ou .NET. Il est conçu pour optimiser la productivité des programmeurs en offrant des outils de haut niveau et une syntaxe simple à utiliser.

Il est également apprécié par certains pédagogues qui y trouvent un langage où la syntaxe, clairement séparée des mécanismes de bas niveau, permet une initiation aisée aux concepts de base de la programmation6.

Python est un langage qui peut s'utiliser dans de nombreux contextes et s'adapter à tout type d'utilisation grâce à des bibliothèques spécialisées. On l'utilise également comme langage de développement de prototype lorsqu'on a besoin d'une application fonctionnelle avant de l'optimiser avec un langage de plus bas niveau. Il est particulièrement répandu dans le monde scientifique, et possède de nombreuses bibliothèques optimisées destinées au calcul numérique.

3. Environnement du travail :

3.1. Google Colab :

Colab (ou "Colaboratory") vous permet d'écrire et d'exécuter du code Python dans votre navigateur avec

- Aucune configuration requise
- Accès gratuit aux GPU
- Partage facile

Que vous soyez étudiant, data scientist ou chercheur en IA, Colab peut vous simplifier la tâche. Regardez la présentation de Colab pour en savoir plus ou commencez tout de suite.

Colab vous permet d'importer un ensemble de données d'images, d'entraîner un classificateur d'images sur cet ensemble et d'évaluer le modèle, tout cela avec quelques lignes de code. Les notebooks Colab exécutent ce code sur les serveurs cloud de Google. Vous avez donc à votre disposition toute la puissance du matériel Google, y compris les GPU et TPU, quelle que soit la puissance de votre ordinateur. Vous n'avez besoin que d'un navigateur.

Colab est très largement utilisé par la communauté du machine Learning, par exemple dans les applications suivantes :

- Premiers pas avec TensorFlow
- Développement et entraînement de réseaux de neurones
- Expérimentation avec les TPU
- Dissémination de la recherche en IA
- Création de tutoriels

3.2. Spyder :

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

3. Un puissant environnement de développement interactif pour le langage Python avec des fonctionnalités avancées d'édition, de test interactif, de débogage et d'introspection.
4. Un environnement de calcul numérique grâce au support d'IPython (interpréteur Python interactif amélioré) et des bibliothèques Python populaires telles que NumPy (algèbre linéaire), SciPy (traitement du signal et des images) ou matplotlib (traçage 2D/3D interactif).
    - Spyder peut également être utilisé comme une bibliothèque fournissant de puissants widgets liés à la console pour vos applications basées sur PyQt par exemple, il peut être utilisé pour intégrer une console de débogage directement dans la disposition de votre interface utilisateur graphique.

4. Outils de Deep Learning :

4.1. Pandas : est une bibliothèque open source sous licence BSD fournissant des structures de données et des outils d'analyse de données hautes performances et faciles à utiliser pour le langage de programmation Python.

4.2. Keras : est l'API de haut niveau de TensorFlow 2 : une interface accessible et hautement productive pour résoudre les problèmes d'apprentissage automatique, en mettant l'accent sur l'apprentissage en profondeur moderne. Il fournit des abstractions et des blocs de construction essentiels pour le développement et la livraison de solutions d'apprentissage automatique avec une vitesse d'itération élevée. Keras permet aux ingénieurs et aux chercheurs de tirer pleinement parti de

l'évolutivité et des capacités multiplateformes de TensorFlow 2 : vous pouvez exécuter Keras sur TPU ou sur de grands clusters de GPU, et vous pouvez exporter vos modèles Keras pour qu'ils s'exécutent dans le navigateur ou sur un mobile dispositif.

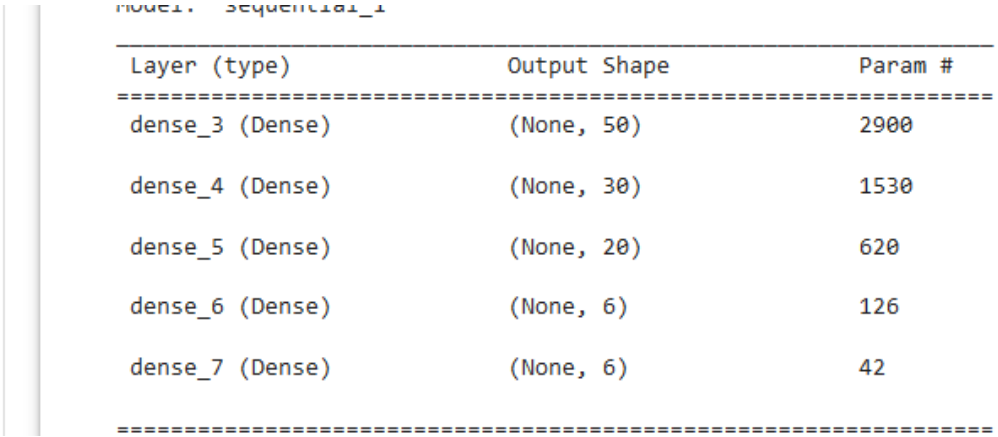
4.3. Sk-Learn : est une bibliothèque libre Python destinée à l'apprentissage automatique. Elle est développée par de nombreux contributeurs notamment dans le monde académique par des instituts français d'enseignement supérieur et de recherche comme Inria. Elle propose dans son framework de nombreuses bibliothèques d'algorithmes à implémenter, clé en main. Ces bibliothèques sont à disposition notamment des data scientists. Elle comprend notamment des fonctions pour estimer des forêts aléatoires, des régressions logistiques, des algorithmes de classification, et les machines à vecteurs de support. Elle est conçue pour s'harmoniser avec d'autres bibliothèques libres Python, notamment NumPy et SciPy.

5. Résultat :

La simulation de notre classificateur de Spam emails est implémentée à l'aide du langage open source Python et de l'outil Pandas pour l'analyse des données. Le framework open source Pandas est utilisé pour analyser les données et la sélection des fonctionnalités, est largement utilisé dans l'exploration de données, le prétraitement des données, la visualisation et la modélisation de l'apprentissage en profondeur. Le temps d'exécution de notre classifieur est calculé à l'aide d'un ordinateur personnel exécutant Windows 10 avec un processeur Intel(R) Core (TM) i3-3217U CPU @1.80 GHz et avec 4 Go de RAM. Pour former notre modèle de réseau neuronal, le Google Colab est utilisé à la place de la machine locale qui a 1,17/ 12,68GB de RAM et 38,36/107,72 GB disque dure. Nous avons utilisé KERAS dans la construction de réseaux d'apprentissage en profondeur. On a obtenu une précision de 90,94% et F1-score 90,85% qui signifie que notre système est fort.

```
Epoch 1/200
4/4 - 1s - loss: 1.8145 - accuracy: 0.3630 - val_loss: 1.7606 -
val_accuracy: 0.4087 - 657ms/epoch - 164ms/step
Epoch 2/200
4/4 - 0s - loss: 1.7555 - accuracy: 0.3829 - val_loss: 1.7107 -
val_accuracy: 0.4087 - 40ms/epoch - 10ms/step
Epoch 3/200
4/4 - 0s - loss: 1.7131 - accuracy: 0.3876 - val_loss: 1.6811 -
val_accuracy: 0.4087 - 42ms/epoch - 11ms/step
Epoch 4/200
4/4 - 0s - loss: 1.6858 - accuracy: 0.3870 - val_loss: 1.6583 -
val_accuracy: 0.4072 - 45ms/epoch - 11ms/step
Epoch 5/200
4/4 - 0s - loss: 1.6611 - accuracy: 0.3860 - val_loss: 1.6335 -
val_accuracy: 0.4087 - 53ms/epoch - 13ms/step
Epoch 6/200
4/4 - 0s - loss: 1.6398 - accuracy: 0.3876 - val_loss: 1.6211 -
val_accuracy: 0.3942 - 47ms/epoch - 12ms/step
Epoch 7/200
4/4 - 0s - loss: 1.6228 - accuracy: 0.3693 - val_loss: 1.5910 -
val_accuracy: 0.4087 - 50ms/epoch - 12ms/step
Epoch 8/200
4/4 - 0s - loss: 1.5985 - accuracy: 0.3870 - val_loss: 1.5723 -
val_accuracy: 0.4065 - 51ms/epoch - 13ms/step
Epoch 9/200
4/4 - 0s - loss: 1.5801 - accuracy: 0.3801 - val_loss: 1.5521 -
val_accuracy: 0.4065 - 60ms/epoch - 15ms/step
Epoch 10/200
```

Figure 18 : Quelque mesure de performance d'application de nos classificateurs NN aux bases de données pendant 200 époques



Model: "sequential_1"

Layer (type)	Output Shape	Param #
dense_3 (Dense)	(None, 50)	2900
dense_4 (Dense)	(None, 30)	1530
dense_5 (Dense)	(None, 20)	620
dense_6 (Dense)	(None, 6)	126
dense_7 (Dense)	(None, 6)	42

Figure 19 : Les couche Dense de notre système

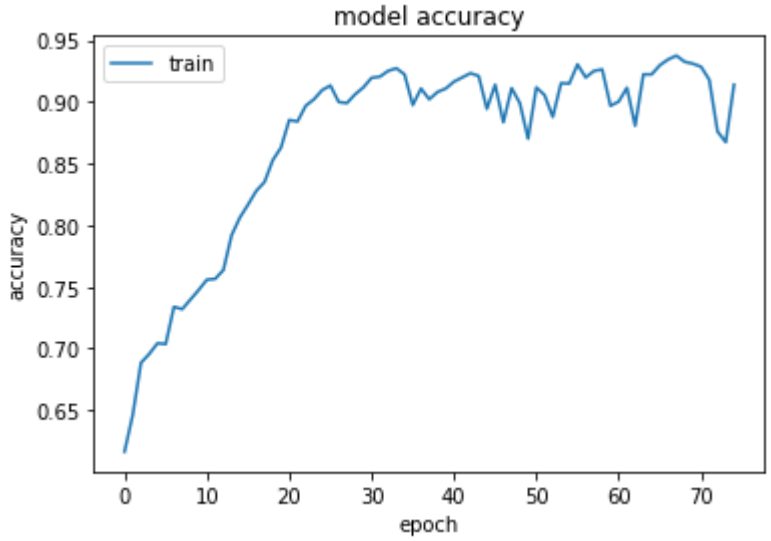


Figure 20 : Graphe de performance model Accuracy de notre Deep Learning

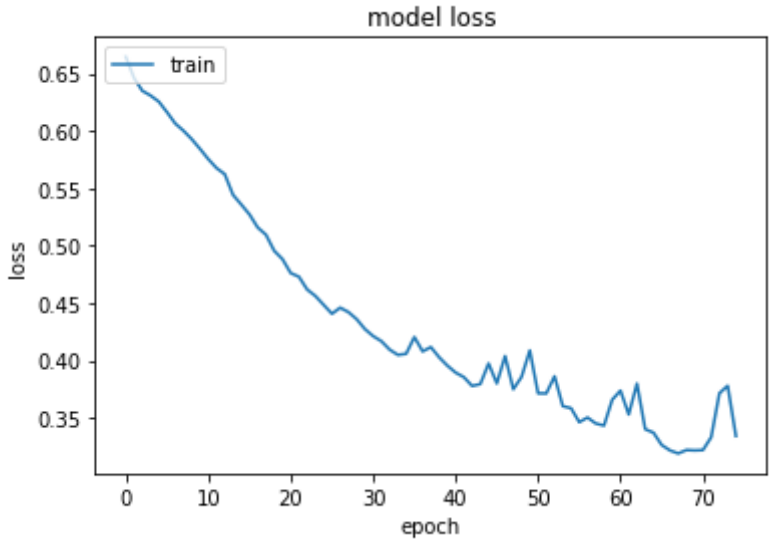


Figure 21 : Graphe de performance model Loss de notre Deep Learning

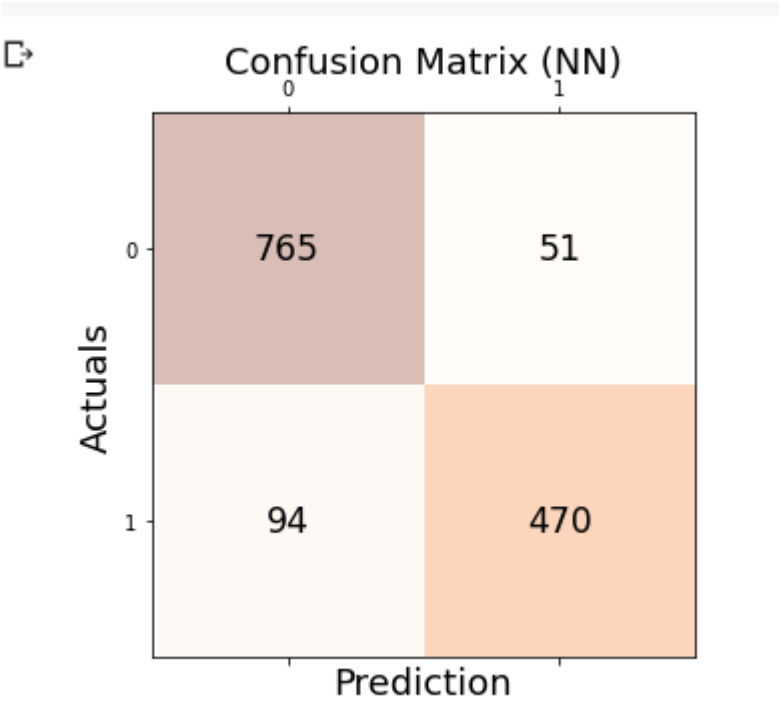


Figure 22 : Matrice de confusion

6. Des captures d'écran de code source :

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

Figure 23 : Connection de drive avec Google Colab

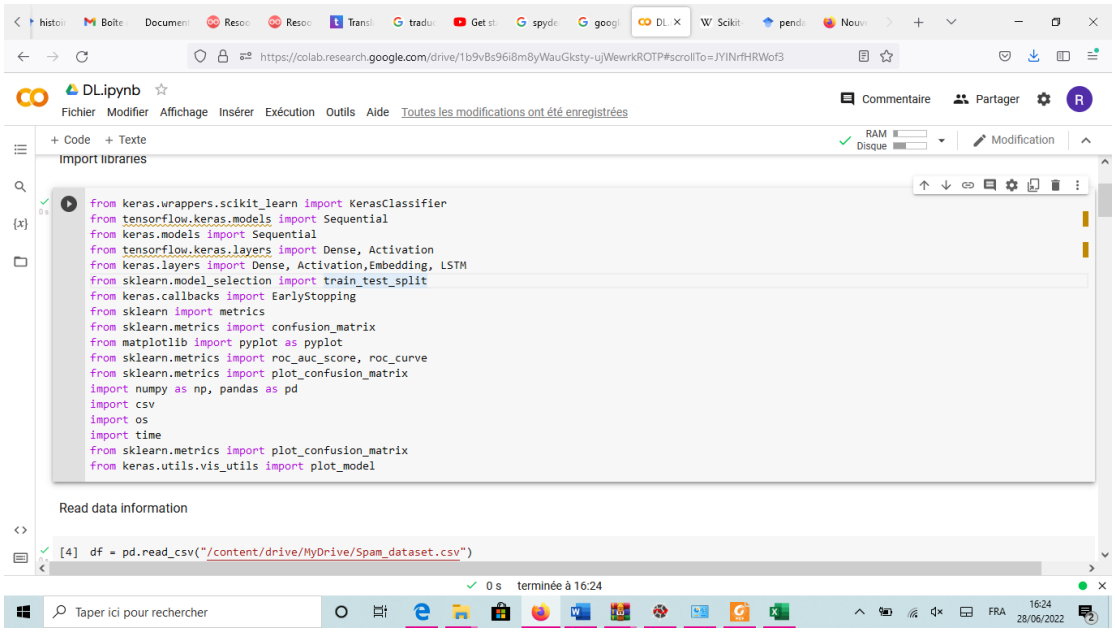


Figure 24 : Les bibliothèques utilisées

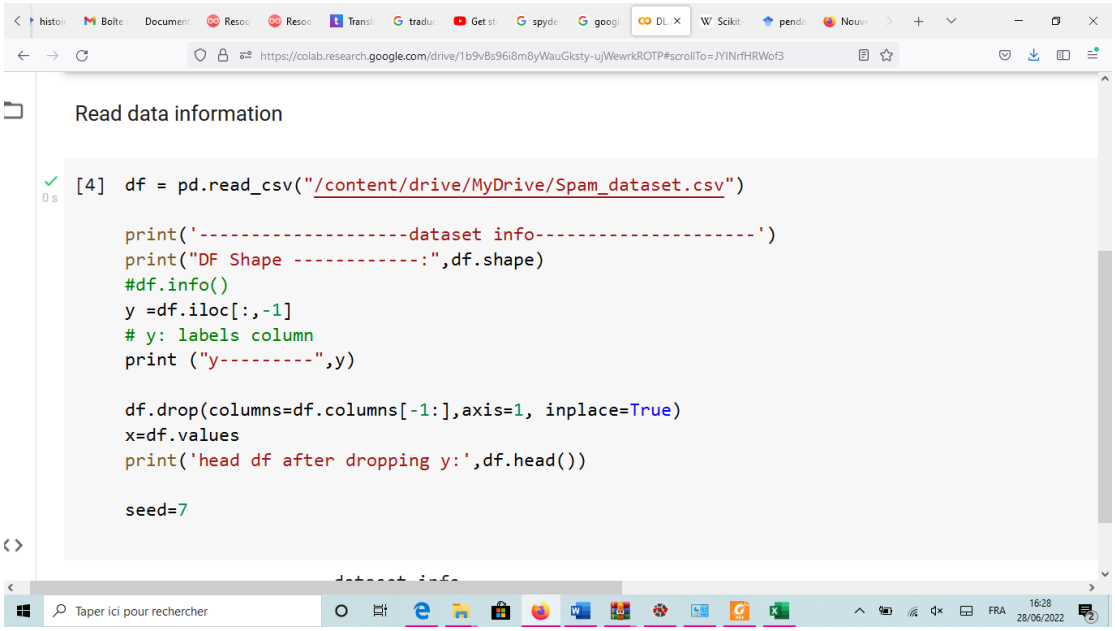


Figure 25 : La récupération et la lecture de Base de Données

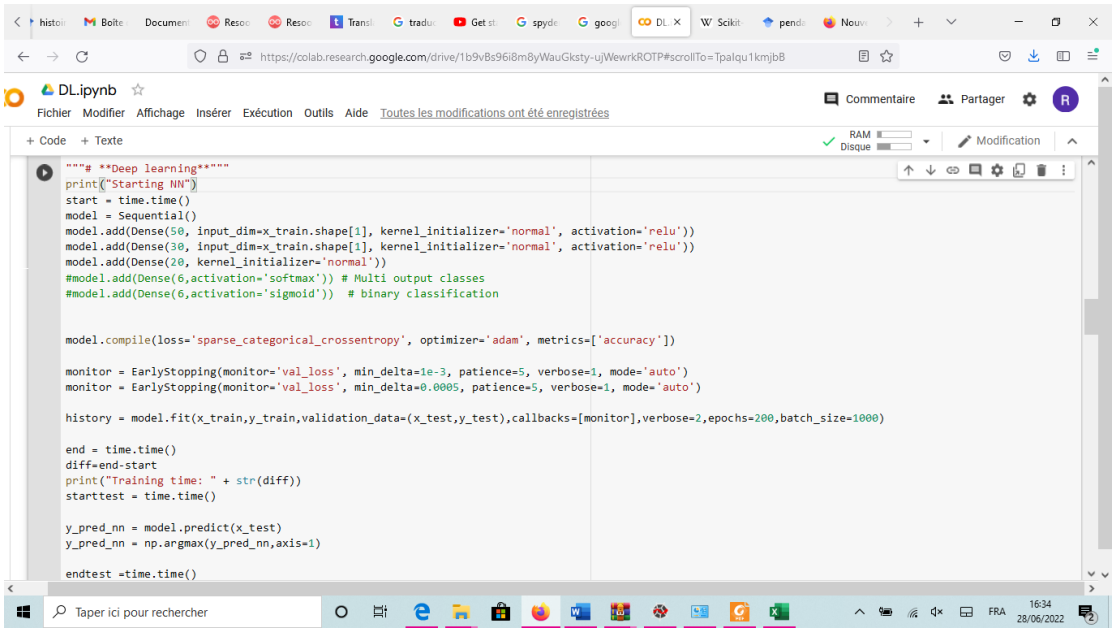


Figure 26 : L'entrainement de Deep Learning

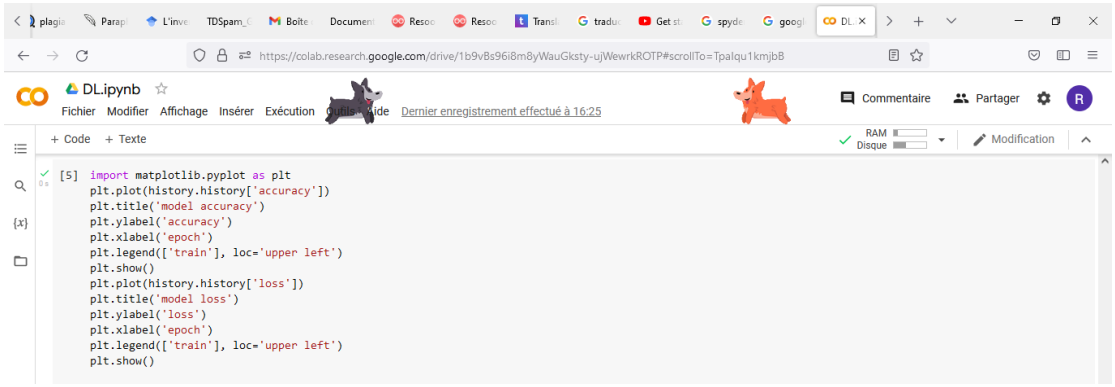


Figure 27 : Code source pour le graphe de précision

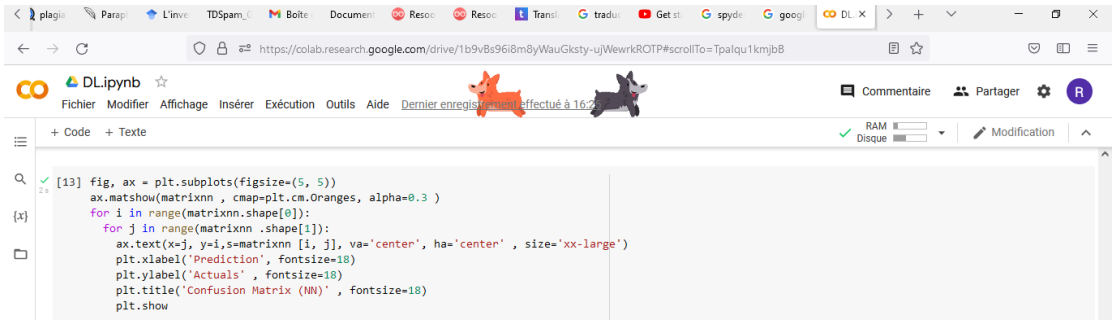


Figure 28 : Code source pour la matrice de confusion

7. Conclusion :

Dans ce dernier chapitre, on a parlé premièrement de, matériels et logiciels utilisés, deuxièmement, les différents environnements de développement, le langage et les bibliothèques utilisées, enfin, on a mis des capteurs d'écran de notre projet.

Conclusion Général :

Les Spam Email sont devenus une menace mondiale importante, car vous pouvez exposer à un risque d'usurpation d'identité ou permettre à un attaquant de télécharger des virus et des logiciels malveillants sur votre ordinateur. Dans le pire des cas, vous pourriez être accusé de crimes que vous ne saviez pas que vous aidiez le spammeur à commettre ; Comme être impliqué dans le blanchiment d'argent ou acheter et vendre des biens volés

❖ Résumé des contributions

Pour conclure, nous proposons un petit récapitulatif de tout ce qui a été réalisé dans ce mémoire et qui a pour but la mise en œuvre d'un système de détection des Spam Email basé sur les techniques d'apprentissage au profond (DL). En premier lieu, nous avons présenté les Spam Email en faisant le tour des différents types et les techniques pour les identifier et les éviter. Ensuite, nous avons parlé des d'apprentissage au profond, et nous avons parlé des différentes techniques et méthodes pour la détection. Ensuite, nous avons détaillé l'architecture de notre système en présentant l'environnement utilisé avec ces différents composants qui ont permis l'avènement de notre système, et expliquer le mode de fonctionnement de ce dernier, à la fin, nous avons présenté les résultats obtenus.

❖ Travaux futurs et perspectives

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

o Utiliser un Dataset contenant un plus grand nombre de fichiers.

o Dans ce travail, nous avons utilisé que technique de réseaux neurones alors qu'il existe d'autre méthodes peuvent être utilisé pour faire l'entraînement pour une meilleure précision.

o Développer un système pour d'autres malwares tel que Ddos.

Bibliographie :

[1] Guillon, P. (2008). Etat de l'art du spam, solutions et recommandations (Doctoral dissertation, Haute école de gestion de Genève).

[2] Brunton, F., & Libbrecht-Carey, N. (2016). Une histoire du spam. *Reseaux*, (3), 33-67.

[3] Schryen, G. (2007). Anti-spam measures. Springer Berlin Heidelberg.

[5] Magdy, S., Abouelseoud, Y., & Mikhail, M. (2022). Filtrage efficace des spams et des e-mails de phishing basé sur l'apprentissage en profondeur. *Réseaux informatiques*, *206*, 108826.

[6] Yaseen, Q. (2021). Détection des courriers indésirables à l'aide de techniques d'apprentissage en profondeur. *Procedia Computer Science*, *184*, 853-858.

[7] Sinha, S., Ghosh, I. et Satapathy, SC (2021). Une étude pour le modèle ANN pour la classification des spams. Dans *Intelligent Data Engineering and Analytics* (pp. 331-343). Springer, Singapour.

[8] Alauthman, M. O. H. A. M. M. A. D. (2020). Botnet spam e-mail detection using deep recurrent neural network. *Int. J*, *8*(5), 1979-1986.

[9] Soni, AN (2019). Détection de courrier indésirable à l'aide d'algorithmes avancés de réseau neuronal à convolution profonde. *Journal pour le développement innovant en sciences pharmaceutiques et techniques*, *2* (5), 74-80.

[10] Hassanpour, R., Dogdu, E., Choupani, R., Goker, O., & Nazli, N. (2018, mars). Détection des e-mails de phishing à l'aide d'algorithmes d'apprentissage en profondeur. Dans *Actes de la conférence ACMSE 2018* (pp. 1-1).

[11] Seth, S., & Biswas, S. (2017, décembre). Classification multimodale des spams à l'aide de techniques d'apprentissage en profondeur. En *2017, 13e Conférence internationale sur la technologie signal-image et les systèmes basés sur Internet (SITIS)* (pp. 346-349). IEEE.

[12] Ezpeleta, E., Zurutuza, U., & Gómez Hidalgo, JM (2016, avril). L'analyse des sentiments aide-t-elle au filtrage bayésien du spam ? Dans *Conférence internationale sur les systèmes hybrides d'intelligence artificielle* (pp. 79-90). Springer, Cham.

[13] Guillon, P. (2008). Etat de l'art du spam, solutions et recommandations (Doctoral dissertation, Haute école de gestion de Genève).

[14] Zdziarski, J. A. (2005). Ending spam : Bayesian content filtering and the art of statistical language classification. No starch press.

[15] Islam, M. R., & Zhou, W. (2007, June). Architecture of adaptive spam filtering based on machine learning algorithms. In *International Conference on Algorithms and Architectures for Parallel Processing* (pp. 458-469). Springer, Berlin, Heidelberg.