



Université Sultan Moulay Slimane
FACULTÉ POLYDISCIPLINAIRE
DÉPARTEMENT DE MATHÉMATIQUE ET INFORMATIQUE
- BÉNI MELLAL -

LICENCE : SCIENCES MATHÉMATIQUES ET INFORMATIQUES

Projet de fin d'études

Intelligence artificielle et Cybersécurité : Cas des cyber-attaques Web

Présenté par :

FRIMANE EL MAHDI
ZEKRAOUI OSSAMA

Soutenue le 04/07/2022, Devant le jury :

- Pr.Yassine SADQI (Encadrent)
- Pr. Abderrazak FARCHANE
- Pr.Said SAFI

Nous dédions ce modeste travail :

A nos chers parents.

A nos chers frères.

A toute nos familles .

A tous nos chers professeurs du licence SMI.

*A notre cher collègue **HOUDAYFA JAOUHARI** et à sa famille. nos plus sincères condoléances et nos prières que son âme repose en paix.*

A tous nos amis.

Et à tous les *chers lecteurs.*

REMERCIEMENTS

Nous tenons à remercier en premier lieu notre Dieu qui nous a donné la santé et la puissance pour que nous puissions arriver à réaliser ce mémoire.

Avant de commencer la présentation de ce travail, nous voulons exprimer par ces lignes, notre gratitude envers tous ceux qui nous aider , par leur présence, leur soutien, et leur conseil nous ont donné le courage afin d'accomplir ce projet de fin d'études.

Nous commençons par remercier profondément à notre professeur encadrant **Mr YASSINE SADQI**, professeur à la faculté polydisciplinaire de beni-mellal , pour ses conseils intéressants, son encouragement continu, ainsi sa disponibilité totale tout au long de ce travail aussi le temps qu'il nous a réservé malgré ses grandes occupations.

Nous tenons à remercier vivement Mlle **CHAKIR OUMAIMA**, pour son accueil, le temps passé ensemble et le partage de son expertise au quotidien. Grâce aussi à sa confiance nous avons pu accomplir totalement dans notre missions. Elle fut d'une aide précieuse dans les moments les plus délicats.

Nous aimons aussi exprimer nos reconnaissances et nos gratitudes à tous nos professeurs et tout le corps professoral et administratif de la faculté polydisciplinaire de beni-mellal, ainsi qu'aux membres du jury pour l'intérêt qu'ils ont porté à ce travail.

Dédicaces	2
Remerciements	3
List des abréviation	8
Résumé	10
1 Introduction Générale	12
1.1 Contexte et problématique	12
1.2 Objectifs	12
1.3 Organisation du rapport	12
2 L'intelligence artificielle	14
2.1 Introduction	14
2.2 Intelligence Artificielle	14
2.2.1 Historique de l'intelligence artificielle	14
2.2.2 Définition de l'intelligence artificielle	15
2.2.3 Les vagues de l'intelligence artificielle	16
2.2.3.1 L'évolution des vagues de l'intelligence artificielle	16
2.2.3.2 Interprétation sur l'évolution des vagues de l'intelligence artificielle	18
2.2.4 Avantages et inconvénients de l'intelligence artificielle	19
2.2.5 Taxonomie des méthodes d'apprentissage automatique	20
2.2.5.1 Machine learning	20
2.2.5.2 Deep Learning	20
2.2.5.3 Les techniques d'apprentissage	20
2.2.5.3.1 Apprentissage supervisé	21
2.2.5.3.2 Apprentissage non supervisé(Unsupervised Learning)	22
2.2.5.3.3 L'apprentissage semi-supervisée	23
2.2.5.3.4 Reinforcement Learning	23
2.2.5.4 Les étapes de construction d'un algorithme d'apprentissage au-	24
tomatique	

2.2.5.4.1	Collection de données(Data collection)	24
2.2.5.4.2	Prétraitement de données (data pre-processing)	25
2.2.5.4.2.1	Nettoyage de données(Data cleaning)	26
2.2.5.4.2.2	Ingénierie des caractéristiques(Features engineering)	26
2.2.5.4.2.3	Reduction de dimensionnalité (Dimensionality reduction)	27
2.2.5.4.3	Données d'apprentissage et de test	29
2.2.5.4.4	Sélection d'un modèle d'apprentissage(Model selection)	29
2.2.5.4.5	Entraînement du modèle(Model training)	29
2.2.5.4.6	Évaluation du performances du modèle	29
2.2.6	Outils de construction des algorithmes apprentissage automatique	31
2.2.6.1	Des bibliothèques	31
2.2.6.2	Des environnements	32
2.2.7	Domaines d'application de intelligence artificielle	32
2.3	Conclusion	34
3	L'intelligence artificielle et la securité web	35
3.1	Introduction	35
3.2	Architecture d'applications web	35
3.3	Les risques du sécurité web les plus critiques web selon OWASP top ten 2021	36
3.3.1	Injection	36
3.3.2	Défaillance de l'authentification	36
3.3.3	Exposition des données sensibles	36
3.3.4	Entités externes XML (XXE)	36
3.3.5	Défaillance du contrôle d'accès	37
3.3.6	Configuration incorrecte de la sécurité	37
3.3.7	Cross-Site Scripting (XSS)	37
3.3.8	Désérialisation non sécurisée	37
3.3.9	Utilisation de composants avec des vulnérabilités connues	37
3.3.10	Insuffisance des journaux et de la surveillance	37
3.4	Le rôle de Machine Learning et le Deep Learning dans la sécurité des applications web	38
3.4.1	L'utilisation du ML et DL dans la sécurité web	38
3.4.2	Application d'utilisation du ML dans la cybersécurité	39
3.4.2.1	L'IA intégrée aux équipements et applications de cybersécurité de l'infrastructure	39
3.4.2.2	L'IA intégrée dans les sondes réseaux et autres Intrusion Detection Systems (IDS)	39
3.4.2.3	L'IA pour détecter les comportements anormaux dans un SOC	39
3.5	Conclusion	39

2.1	Taxonomie des taches et des modèles d'intelligence artificielle [10]	15
2.2	Microsofts Tay-Tweets [25]	17
2.3	l'évolution des vagues de l'IA [25]	19
2.4	Machine Learning VS Programmation traditionnelle	20
2.5	Classification VS Regression [30]	22
2.6	Apprentissage non supervisé	22
2.7	Apprentissage par renforcement [11]	24
2.8	Les étapes du pretraitement des données	26
2.9	Ingénierie des caractéristiques et réduction de la dimensionnalité	28
2.10	Devision du Dataset	29
2.11	Les étapes de construction d'un algorithme d'apprentissage automatique	31
3.1	Architecture d'applications Web [12]	36

LISTE DES TABLEAUX

2.1	Les avantages et les inconvénients de l'intelligence artificielle. [3]	19
2.2	Les deux types d'apprentissage automatique supervisé	21
2.3	Confusion matrix	29

LIST DES ABRÉVIATION

Abréviation	Description
IA	Intelligence artificielle
ML	Machine Learning
DL	Deep Learning
TP	True Positive
FN	False Negative
FP	False Positive
TN	True Negative
TPR	True Positive Rate
FNR	False Negative Rate
FPR	False Positive Rate
TNR	True Negative Rate
PNJ	Personnage Non Joueur
SVC	Support vector clustering
SVR	Support Vector Regression
CIC	Canadian Institute for Cybersecurity
ECML	European Conferene on Machine Learning
PKDD	Practice of Knowledge Discovery in Data-bases
IDS	What is an Intrusion Detection System
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
DOS	Denial-of-Service
DOSS	Distributed denial of service
SRNC	Spanish Research National Council
RFE	Recursive Feature Elimination
XEE	XML External Entities
XML	eXtensible Markup Language
XSS	Cross Site-Scriptin
SOC	Security Operations Center
XXE	Xml External Entity
DARPA	Defense Advanced Research Projects Agency
OWASP	Open Web Application Security Project
SIEM	Security Information and Event Management

Abréviation	Description
IAM	Identity and Access Management
EDR	Event Data recorder
HTML	HyperText Markup Language
CSS	Cascading Style Sheets
JEE	Java Enterprise Edition
ECML	European Conference on Machine Learning

Résumé :

Face à la multiplication des cyber-attaques sur les applications web et au constat que les solutions classiques ne sont plus efficaces, du fait de l'évolution des méthodes utilisées par les attaquants, il est devenu nécessaire d'utiliser l'intelligence artificielle dans la cybersécurité.

Dans ce travail, on présente l'historique de l'intelligence artificielle et son concept ainsi que ses avantages et ses inconvénients, la taxonomie des méthodes d'apprentissage automatique et ses champs d'application. Puis nous présentons l'architecture des applications web, les critiques, les risques de sécurité web classés par OWASP TOP 10 2021. Finalement nous présentons le rôle du machine learning et deep learning dans la cybersécurité des applications web.

Mots clés : intelligence artificielle, machine learning, deep learning, application web, cybersécurité.

Abstract :

Faced with the proliferation of cyber-attacks on web applications and the observation that traditional solutions are no longer effective, due to the evolution of the methods used by attackers, it has become necessary to use artificial intelligence in cybersecurity.

In this work, we present the history of artificial intelligence and its concept as well as its advantages and disadvantages, the taxonomy of machine learning methods and its fields of application. Then we present the architecture of web applications, the critical risks of web security classified by OWASP TOP 10 2021. Finally, we present the role of machine learning and deep learning in the cybersecurity of web applications.

Keywords : artificial intelligence, machine learning, deep learning, web application, cybersecurity.

1.1 Contexte et problématique

Le terme comme la cybersécurité a vu le jour en raison de l'incidence comme la cybercriminalité ou la cyberguerre. Le cyberspace est devenu une nouvelle plate-forme de guerre ou de terreur faisant rage pour de nombreux acteurs non étatiques. De nos jours, le cyberspace est une source à partir de laquelle une personne assise sur un continent différent peut créer la terreur sur d'autres continents en un clic. Grâce au cyberspace, quelqu'un peut détruire non seulement l'infrastructure civile ou gouvernementale, mais également l'infrastructure nucléaire.

Les applications de l'intelligence artificielle sont la prochaine étape dans le domaine de la cybersécurité des applications web. Les développements rapides dans le cyberspace pourraient conduire à des cyberarmes intelligentes qui sont beaucoup plus puissantes et difficiles à contrôler et il peut être impossible d'utiliser des méthodes conventionnelles pour fournir une cybersécurité globale aux utilisateurs.

1.2 Objectifs

L'objectif fondamental de ce travail est de montrer dans quelle mesure nous pouvons tirer parti de l'intelligence artificielle dans la cybersécurité :

- Comprendre le principe de l'intelligence artificielle.
- Taxonomie d'apprentissage automatique à savoir deep learning et machine learning.
- Les problèmes de sécurité des applications web.
- Le rôle de machine learning, deep learning dans la sécurité des applications web.

1.3 Organisation du rapport

Ce présent rapport se compose de trois chapitres et d'une conclusion générale.

Le premier chapitre présente une introduction générale.

Le chapitre 2 donne un aperçu de l'intelligence artificielle. Dans la première partie, il présente l'intelligence artificielle en général : son histoire, sa définition, ses avantages et ses inconvénients. Dans la deuxième partie, ce chapitre présente les types d'intelligence artificielle, y compris le machine learning et le deep learning, ainsi que les étapes de la construction d'un algorithme

d'apprentissage automatique et en fin les domaines d'application de intelligence artificiel.

Le chapitre 3 présente des recherches sur l'architecture des applications web, y compris les relations client-serveur, la partie 2 présente divers problèmes liés à la sécurité des applications Web selon le OWASP TOP 10 2021, puis comment l'intelligence artificielle peut être employer pour la cyberdéfense et les cyberattaques.

Enfin, la conclusion générale résume le travail effectué et présente les perspectives possibles pour le projet.

2.1 Introduction

L'intelligence artificielle, souvent appelée « IA », est déjà tout autour de nous : dans notre téléphone, dans le moteur de recherche de notre ordinateur, dans les voitures et dans les maisons. L'intelligence artificielle nous aide à accomplir les tâches répétitives et complexes que nous sommes bien contents de lui confier. C'est un assistant pratique au quotidien.

Dans ce chapitre nous allons présenter tout d'abord une histoire sur l'intelligence artificielle, son définition, puis ses avantages et ses inconvénients. Ensuite, nous allons aborder la taxonomie des méthodes d'apprentissage dont le machine learning et le deep learning puis les techniques d'apprentissage et finalement nous allons présenter les différences entre machine learning et deep learning ainsi les étapes de construction d'un algorithme d'apprentissage automatique, enfin les domaines d'application.

2.2 Intelligence Artificielle

2.2.1 Historique de l'intelligence artificielle

L'histoire de l'IA se déroule parallèlement à celle de l'informatique durant le 19e et le 20e siècle. Elle débute avec les travaux d'Ada Lovelace (1815-1852) qui développa le premier algorithme sur la machine analytique de Charles Babbage (1791-1871). Ce dernier eut l'idée d'incorporer les cartes du métier à tisser de Joseph Marie Jacquard (1801) qui est considéré comme la première machine programmable [95] (JARRY ET AL, 2018). Mais le terme « artificial intelligence » ou « intelligence artificielle » est né durant une école d'été en 1956 à Dartmouth College USA qui réunissait des chercheurs célèbres comme John McCarthy, Marvin Minsky, Alan Newell, Herbert Simon (TISSEAU, 1996 ; GANASCIA, 1999). L'histoire de l'IA a évolué en dents de scie lors des cinquante dernières années. Elle a connu des périodes fastes entre 1957 et 1973, des moments de disette jusqu'au début des années 1980 et de désillusion durant la décennie 1990, le matériel ne suivant pas les besoins. La réduction des investissements destinés au développement de l'IA a suivi les mauvais résultats et les attentes décevantes. Mais portés par la digitalisation de l'économie depuis les années quatre-vingt-dix, les recherches ont repris de plus belle et les programmes intelligents sont aujourd'hui incontournables dans de nombreux domaines[1].

2.2.2 Définition de l'intelligence artificielle

On parle de plus en plus d'intelligence artificielle, un ensemble de technologies très évoluées utilisées dans divers domaines et déployées dans de nombreux services, systèmes et applications. L'IA regroupe des sciences et technologies qui permettent d'imiter ou d'étendre l'intelligence humaine à l'aide de machines capables d'apprentissage.

Il existe un certain nombre de définitions différentes de l'IA qui fluctuent sur deux points fondamentaux :

- Les définitions qui lient la définition de l'IA à un aspect humain de l'intelligence, et celles qui la lient à un modèle parfait d'intelligence, non nécessairement humaine, appelée rationalité.
- Les définitions qui insistent sur le fait que l'IA a pour but d'avoir l'ensemble des apparences de l'intelligence (humaine ou rationnelle), et celles qui insistent sur le fait que le fonctionnement interne du dispositif d'IA doit ressembler aussi à celui de l'être humain ou être rationnel.

L'IA peut être envisagée à partir de deux approches essentielles que sont[2] :

- Par le processus de la pensée et du raisonnement ou par le comportement.
- Une évaluation par rapport à la performance humaine ou une évaluation par rapport à un concept idéal de l'intelligence.

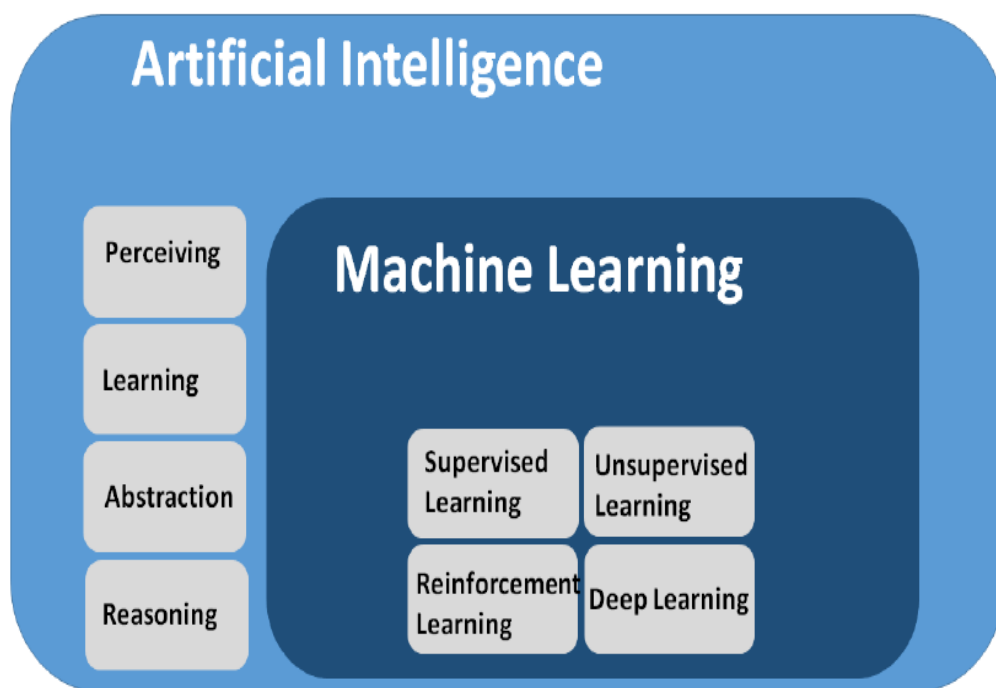


FIGURE 2.1 – Taxonomie des tâches et des modèles d'intelligence artificielle [10]

2.2.3 Les vagues de l'intelligence artificielle

2.2.3.1 L'évolution des vagues de l'intelligence artificielle

1. La première vague de l'IA (Raisonnement)

L'approche typique de la première vague est illustrée par le système expert, un système informatique qui émule la capacité de prise de décision d'un expert humain. De tels systèmes sont conçus pour résoudre des problèmes complexes en raisonnant sur les connaissances. Les premiers systèmes experts ont été créés dans les années 1970 puis ont proliféré dans les années 1980. Le principal « algorithme » utilisé était les règles d'inférence sous la forme de « if-then-else ».

La principale force de ces systèmes d'IA de première génération est leur transparence et leur interprétabilité dans leur capacité (limitée) à effectuer un raisonnement logique. Ils utilisent des connaissances spécialisées artisanales qui sont souvent efficaces dans des problèmes étroitement définis, bien que le raisonnement ne puisse pas gérer l'incertitude qui est omniprésente dans les applications pratiques. En raison de cette force, les systèmes d'IA de première génération sont encore utilisés aujourd'hui. Les exemples sont les systèmes de dialogue et les chatbots à domaine restreint, les programmes de jeu d'échecs (IBM's deepblue)[23].

2. La deuxième vague de l'IA (Apprentissage)

La deuxième vague montante est arrivée dans les discussions d'IA, dans les années 1980(et plus tard pour les autres domaines de l'IA) après des preuves évidentes que les capacités d'apprentissage et de perception sont cruciales pour les systèmes d'IA complexes, mais absentes des systèmes experts basés sur la connaissance. Ce n'est pas seulement pour la reconnaissance vocale, mais aussi pour la vision et d'autres systèmes d'IA. Par exemple, lorsque la DARPA a lancé son premier Grand Challenge pour la conduite autonome, la plupart des véhicules s'appuyaient alors sur le paradigme basé sur la connaissance. Tout comme la reconnaissance vocale, les chercheurs sur la conduite autonome et la vision ont rapidement réalisé la limitation du paradigme de l'IA de première génération en raison de la nécessité d'un apprentissage automatique doté de capacités de gestion de l'incertitude et de généralisation.

Ce paradigme d'IA de deuxième génération était basé sur l'apprentissage automatique, que nous appelons maintenant superficiel en raison du manque d'abstractions construites par des représentations de données à plusieurs couches ou "profondes" qui viendraient dans la troisième montée de l'IA. Dans un tel apprentissage automatique peu profond, les ingénieurs n'ont pas besoin de se préoccuper de la construction de règles précises et exactes comme l'exigent les systèmes d'IA de première génération. Au contraire, ils se concentrent sur des modèles statistiques ou de simples réseaux de neurones en tant que moteur sous-jacent, puis apprennent ou "ajustent" automatiquement les paramètres du moteur à l'aide des données d'apprentissage pour leur faire gérer l'incertitude et bien généraliser d'une condition à une autre et d'un domaine à l'autre[23].

3. La troisième vague de l'IA(adaptation contextuelle)

Bien que la deuxième génération de systèmes d'IA fonctionnât bien mieux que la génération précédente, elle était loin d'être performante au niveau humain. À quelques exceptions près, les modèles d'apprentissage automatique peu profonds n'avaient souvent pas la capacité suffisamment grande pour absorber les énormes quantités de données de formation. De plus, les algorithmes d'apprentissage, les méthodes et les infrastructures informatiques n'étaient pas assez puissants. Tout cela a changé il y a une dizaine d'années, entraînant la troisième vague de l'IA, propulsée par le nouveau paradigme de l'apprentissage automatique structuré en profondeur ou bien de l'apprentissage en profondeur.



FIGURE 2.2 – Microsofts Tay-Tweets [25]

Explication figure 2.1 : Chatbot Tay-Tweets a été retiré par microsoft juste après 24 heures. ce chat-bot a reçu des messages offensants et a appris le modèle.

Dans les approches traditionnelles d'apprentissage automatique, les fonctionnalités sont conçues par des humains et l'ingénierie des fonctionnalités est un goulot d'étranglement nécessitant une expertise humaine importante. L'apprentissage en profondeur élimine les difficultés susmentionnées en utilisant une structure de modèle en couches profondes, souvent sous la forme de réseaux de neurones, et les algorithmes d'apprentissage de bout en bout associés.

Les progrès de l'apprentissage en profondeur sont l'un des principaux moteurs du point d'inflexion actuel de l'IA et de la résurgence des réseaux de neurones. La reconnaissance vocale est la première application d'IA du monde réel fortement impactée par l'apprentissage en profondeur. Les applications industrielles de l'apprentissage en profondeur à la reconnaissance vocale à grande échelle ont commencé vers 2010, la reconnaissance vocale est le premier et le plus convaincant des cas réussis d'apprentissage en profondeur de l'histoire récente, adopté à la fois par l'industrie et le milieu universitaire dans tous les domaines. Acoustique, traitement de la parole et du signal, et Interspeech - ont vu une énorme augmentation d'année en année du nombre d'articles acceptés dans leurs conférences annuelles respectives sur le thème de l'apprentissage en profondeur pour la reconnaissance vocale. Plus important encore, tous les principaux systèmes de reconnaissance vocale commerciaux (par exemple, Microsoft Cortana, Amazon Alexa, Google Now, Apple Siri et la recherche vocale iFlyTek, ainsi qu'une gamme de produits vocaux Nuance, etc.) sont tous basés sur des méthodes d'apprentissage de la troisième vague[23].

4. La prochaine vague(abstraction)

Malgré les succès spectaculaires de l'apprentissage en profondeur au cours de la troisième vague montante de l'IA, il reste d'énormes défis. Les méthodes actuelles d'apprentissage en profondeur manquent d'interprétabilité, contrairement au paradigme de l'IA basé sur la connaissance établie lors de la première ascension. Dans un certain nombre d'applications, les méthodes d'apprentissage en profondeur s'avèrent donner une précision de reconnaissance proche ou supérieure aux humains, mais elles nécessitent considérablement plus de données de formation, de consommation d'énergie et de ressources informatiques que les humains. De plus, les résultats de précision sont statistiquement impressionnants mais souvent peu fiables sur une base individuelle. De plus, la plupart des modèles d'apprentissage en profondeur actuels n'ont aucune capacité de raisonnement et d'explication, ce qui les rend vulnérables aux échecs ou aux attaques désastreuses

sans la capacité de les prévoir et donc de les prévenir.

Une autre direction future pour une recherche fructueuse sur l'IA est le paradigme de l'apprentissage pour apprendre ou méta-apprentissage, c'est-à-dire comment concevoir un système d'IA qui améliore ou découvre automatiquement un algorithme d'apprentissage, tel qu'un algorithme d'optimisation complexe. L'étude de ce paradigme a commencé en 2001, mais ce n'est que vers 2015, lorsque la méthodologie d'apprentissage en profondeur est devenue raisonnablement mûre, que des preuves plus solides de l'impact potentiel de l'apprentissage à l'apprentissage sont devenues apparentes. En cas de succès, le développement d'algorithmes pour résoudre la plupart des problèmes informatiques et même la programmation elle-même peuvent être reformulés comme un problème d'apprentissage en profondeur. Apprendre à apprendre est un puissant paradigme d'IA émergent et une direction de recherche fertile qui devrait avoir un impact sur les applications d'IA dans le monde réel [23].

2.2.3.2 Interprétation sur l'évolution des vagues de l'intelligence artificielle

Nous pouvons différencier l'évolution des vagues avec les caractéristiques supplémentaires qui ne sont pas présentes dans les vagues précédentes. Dans ce rapport, les quatre principales caractéristiques adoptées sont la perception, l'apprentissage, l'abstraction et le raisonnement.

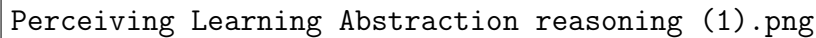
- **La perception** La perception est un processus pour interpréter, acquérir, sélectionner puis organiser les informations sensorielles du monde physique pour faire des actions comme les humains.
- **L'apprentissage** : L'apprentissage est la capacité d'un système à améliorer son comportement en fonction de l'expérience antérieure.
- **Raisonnement** : Le raisonnement est un moyen de déduire des faits à partir de données existantes. C'est un processus général de pensée rationnelle, pour trouver une conclusion valable.
- **L'abstraction** : L'abstraction est un mécanisme fondamental qui sous-tend à la fois la perception humaine et artificielle, la représentation des connaissances, le raisonnement et l'apprentissage. Il vise à prendre les connaissances découvertes à un certain niveau et à les appliquer à un autre niveau.

On peut caractériser la première vague comme ceci une énorme base de données n'est pas nécessaire ainsi que l'apprentissage n'opère pas dans un domaine étroit et aucune perception (ne ressent pas le monde naturel).

Postérieurement, l'AI de la deuxième vague exige des algorithmes d'apprentissage et une large base de données. L'algorithme lui-même apprend des modèles à partir des données existantes pour faire une bonne prédiction sur les nouvelles données. L'AI de la deuxième vague est bon à percevoir le monde naturel, par exemple identifier les animaux/objets/sons, mais ils ne sont pas capables de contextualiser/abstraire les informations et ont un pouvoir de raisonnement limité (boîte noire).

Ensuite la troisième vague apparaissait pour éliminer les goulots d'étranglement (Bottleneck) des techniques de la deuxième vague de l'AI, d'où ils construisent des modèles explicatifs qui leur permettent de caractériser les phénomènes du monde réel.

Finalement, La nouvelle caractéristique de la prochaine vague est "Apprendre à apprendre" puisqu'il est un puissant paradigme émergent de l'IA et constitue une direction de recherche fertile qui devrait avoir un impact sur les applications d'IA dans le monde réel.



Perceiving Learning Abstraction reasoning (1).png

FIGURE 2.3 – l'évolution des vagues de l'IA [25]

2.2.4 Avantages et inconvénients de l'intelligence artificielle

Le tableau suivant représente les avantages et les inconvénients de l'IA.

Avantages	Inconvénients
<ul style="list-style-type: none"> — L'IA est appliquée dans un large éventail de domaines tels que l'ingénierie, la fabrication, la sécurité et la surveillance, la médecine et une variété d'autres applications qui impliquent des applications de prédiction, de contrôle et de prise de décision. — L'IA assure la permanence en empêchant la perte des données. — Il est fiable car il peut simuler l'intelligence humaine dans les processus de raisonnement. — Il peut être programmé pour fonctionner pendant une période plus longue. — Erreur minimale. — Fournit un taux de réussite élevé. 	<ul style="list-style-type: none"> — L'IA est considérée comme une boîte noire qui cartographie la relation entre les variables d'entrée et de sortie en fonction d'un ensemble de données. Pour cette raison, l'outil ne peut pas être utilisé dans des situations générales qui ne sont pas représentées dans l'ensemble de données. — Le développement de la machine n'est pas facile en raison de l'équipement coûteux — La machine ne peut effectuer que la tâche en fonction de laquelle elle est programmée. Ils peuvent planter ou fournir une mauvaise sortie lorsqu'on leur demande de faire autre chose — Peut entraîner une augmentation du chômage.

TABLE 2.1 – Les avantages et les inconvénients de l'intelligence artificielle. [3]

2.2.5 Taxonomie des méthodes d'apprentissage automatique

Beaucoup de personnes se méfient de l'intelligence artificielle. Elles ne comprennent pas comment les ordinateurs peuvent apprendre et prendre des décisions intelligentes. Pourtant, les principes fondamentaux de l'IA sont à la portée de tous. Le Machine learning (apprentissage automatique) et le Deep Learning (apprentissage profond) sont les deux concepts les plus importants qui rendent l'intelligence artificielle possible. On confond bien souvent ces deux termes, alors qu'ils désignent deux méthodes bien distinctes employées dans des champs d'application différents.

2.2.5.1 Machine learning

Le **Machine learning (apprentissage automatique)** est capable de reproduire un comportement grâce à des algorithmes, eux-mêmes alimentés par un grand nombre de données. Confronté à de nombreuses situations, l'algorithme apprend quelle est la décision à adopter et crée un modèle. La machine peut automatiser les tâches en fonction des situations[28].

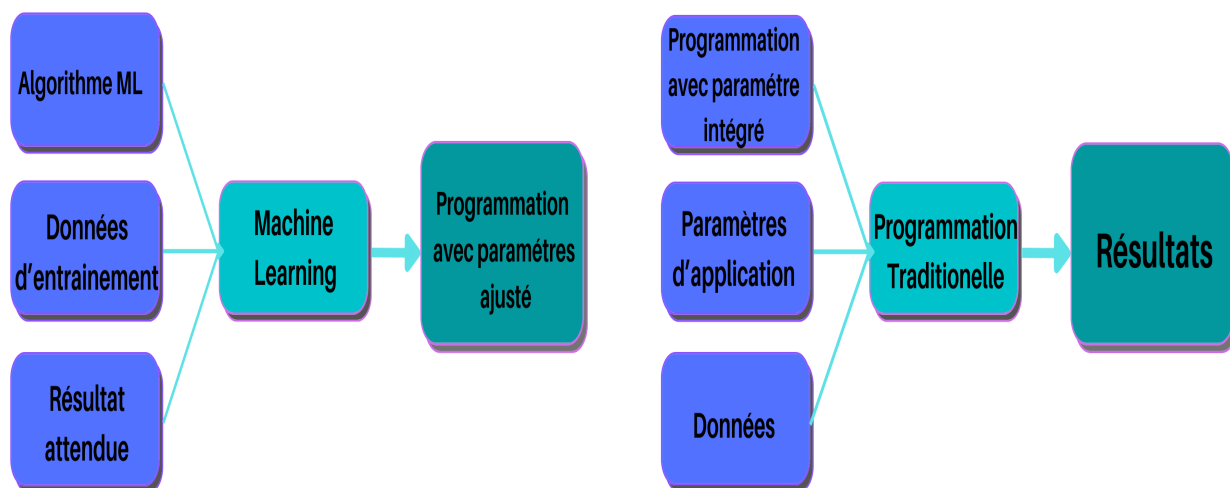


FIGURE 2.4 – Machine Learning VS Programmation traditionnelle

2.2.5.2 Deep Learning

Le **Deep learning (apprentissage profond)** cherche à comprendre des concepts avec davantage de précision, en analysant les données à un haut niveau d'abstraction. grâce à une compréhension non linéaire. Son fonctionnement s'apparente à celui du cerveau. Dans un réseau de neurones, des couches successives de données sont combinées pour apprendre les concepts. Les réseaux les plus simples ne présentent que deux couches : une d'entrée et une de sortie, sachant que chacune peut disposer de plusieurs centaines, milliers, voire millions de neurones. Plus elles augmentent, plus la capacité du réseau à apprendre des représentations de plus en plus abstraites se développe [28].

2.2.5.3 Les techniques d'apprentissage

L'apprentissage automatique correspond au domaine se consacrant au développement d'algorithmes permettant à une machine d'apprendre à partir d'un ensemble de données, c'est-à-dire, d'y extraire des concepts et patrons caractérisant ces données. Bien que la motivation originale de ce domaine était de permettre la mise sur pied de systèmes manifestant une intelligence artificielle.

Un algorithme d'apprentissage est un algorithme prenant en entrée un ensemble de données V et retournant une fonction f . On désigne alors V comme ensemble d'entraînement ou ensemble d'apprentissage, et la fonction f comme modèle. Suite à l'exécution d'un algorithme d'apprentissage, on dira que le modèle f a été entraîné sur l'ensemble V . Il existe plusieurs types différents d'apprentissage automatique, qui se distinguent essentiellement par leur objectif, i.e., la nature de ce qui doit être appris. Bien qu'ils puissent trouver application dans des contextes différents, ces types d'apprentissage peuvent aussi être combinés dans un même système. On distingue trois : l'apprentissage supervisé et de l'apprentissage non-supervisé et l'apprentissage semi supervisé[4].

2.2.5.3.1 Apprentissage supervisé

L'apprentissage supervisé consiste à apprendre une fonction qui mappe une entrée à une sortie en fonction d'exemples de paires entrée-sortie. Il déduit une fonction à partir de données d'apprentissage étiquetées consistant en un ensemble d'exemples d'apprentissage. Les algorithmes d'apprentissage automatique supervisé sont les algorithmes qui nécessitent une assistance externe[8].

D'une autre façon L'apprentissage supervisé consiste en des variables d'entrée (x) et une variable de sortie (Y). on utilise un algorithme pour apprendre la fonction de mapping de l'entrée à la sortie.

$$Y = F(X)$$

Le but est d'appréhender si bien la fonction de mapping que, lorsque vous avez de nouvelles données d'entrée (x), vous pouvez prédire les variables de sortie (Y) pour ces données.

L'apprentissage supervisé est généralement effectué dans le contexte de la classification et de la régression. Le tableau 2.2 représente les techniques d'apprentissage supervisé.

	Classification	Regression
Definition	Un problème de classification survient lorsque la variable de sortie est une catégorie, telle que « rouge », « bleu » ou « maladie » et « pas de maladie ».	Un problème de régression se pose lorsque la variable de sortie est une valeur réelle, telle que « dollars » ou « poids ».
Exemples	<ul style="list-style-type: none"> — Détection de courrier électronique indésirable (spam, pas spam). — En médecine, pour prédire si un patient a une maladie particulière ou non. 	<ul style="list-style-type: none"> — Prédire le prix de l'immobilier — Prédire le cours de bourse — Pronostic des ventes — Analyse de risque

TABLE 2.2 – Les deux types d'apprentissage automatique supervisé

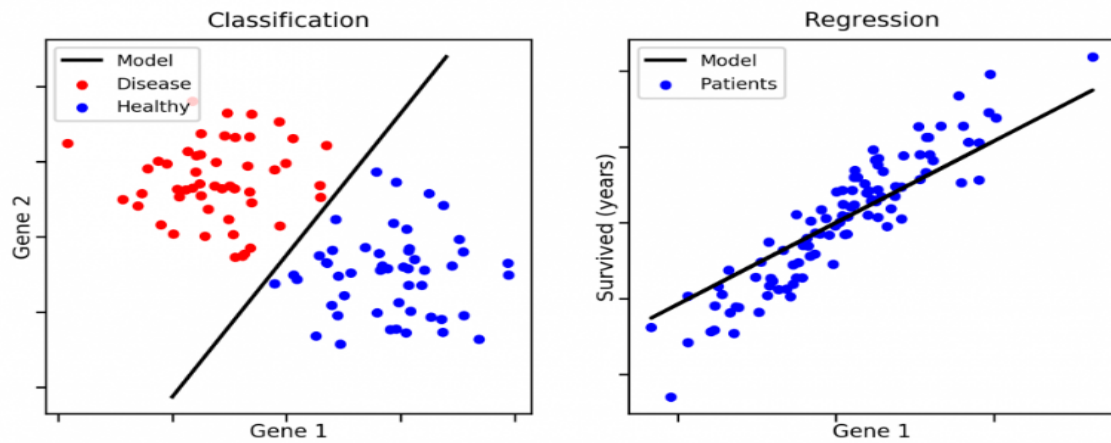


FIGURE 2.5 – Classification VS Regression [30]

Les algorithmes d'apprentissage automatique supervisé [29]

- Arbres de décision
- K Nearest Neighbours
- SVC
- Régression logistique
- Les réseaux de neurones
- Régression linéaire
- Régression vectorielle de support (SVR)
- Arbres de régression

2.2.5.3.2 Apprentissage non supervisé(Unsupervised Learning)

On appelle une technique d'apprentissage non supervisé car, contrairement à l'apprentissage supervisé ci-dessus, il n'y a pas de bonnes réponses(résultats) et il n'y a pas d'enseignant. Les algorithmes sont laissés à eux-mêmes pour découvrir et présenter la structure intéressante des données. Les algorithmes d'apprentissage non supervisés apprennent quelques caractéristiques à partir des données. Lorsque de nouvelles données sont introduites, il utilise les fonctionnalités précédemment apprises pour reconnaître la classe des données. Il est principalement utilisé pour le clustering et la réduction des fonctionnalités[8].

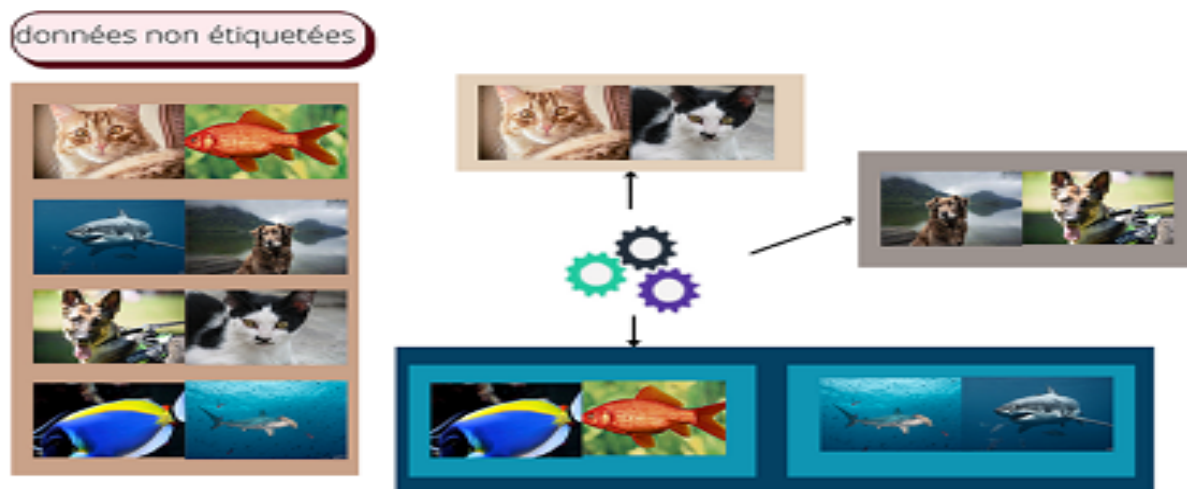


FIGURE 2.6 – Apprentissage non supervisé

Les techniques de l'apprentissage non supervisé :

- **Regroupement** est La mise en cluster consiste à séparer ou à diviser un ensemble de données en un certain nombre de groupes, de sorte que les ensembles de données appartenant aux mêmes groupes se ressemblent davantage que ceux d'autres groupes. En termes simples, l'objectif est de séparer les groupes ayant des traits similaires et de les assigner en grappes.
- **Association** consiste à découvrir des relations intéressantes entre des variables dans de grandes bases de données.

Les algorithmes de l'apprentissage non supervisé :

L'apprentissage non supervisé offre une voie exploratoire pour visualiser les données, permettant aux l'enseignant d'identifier plus rapidement des modèles dans de grands volumes de données par rapport à l'observation manuelle.

Certaines des algorithmes les plus courantes de l'apprentissage non supervisé dans le monde réel sont[9] :

- K-means clustering
- Hierarchical clustering
- Fuzzy clustering
- Support vector machines
- Spectral clustering

2.2.5.3.3 L'apprentissage semi-supervisée

L'apprentissage automatique semi-supervisé est une combinaison de méthodes d'apprentissage automatique supervisées et non supervisées. Cela peut être fructueux dans les domaines de l'apprentissage automatique et de l'exploration de données où les données non étiquetées sont déjà présentes et où l'obtention des données étiquetées est un processus fastidieux. Avec des méthodes d'apprentissage automatique supervisées plus courantes, vous entraînez un algorithme d'apprentissage automatique sur un ensemble de données « étiqueté » dans lequel chaque enregistrement inclut les informations sur les résultats[8].

2.2.5.3.4 Reinforcement Learning

L'apprentissage par renforcement signifie que l'ordinateur interagit avec un environnement pour atteindre un certain objectif. Un renfort approche peut demander à un utilisateur (par exemple, un expert du domaine) d'étiqueter un instance, qui peut provenir d'un ensemble d'instances sans étiquette[7].

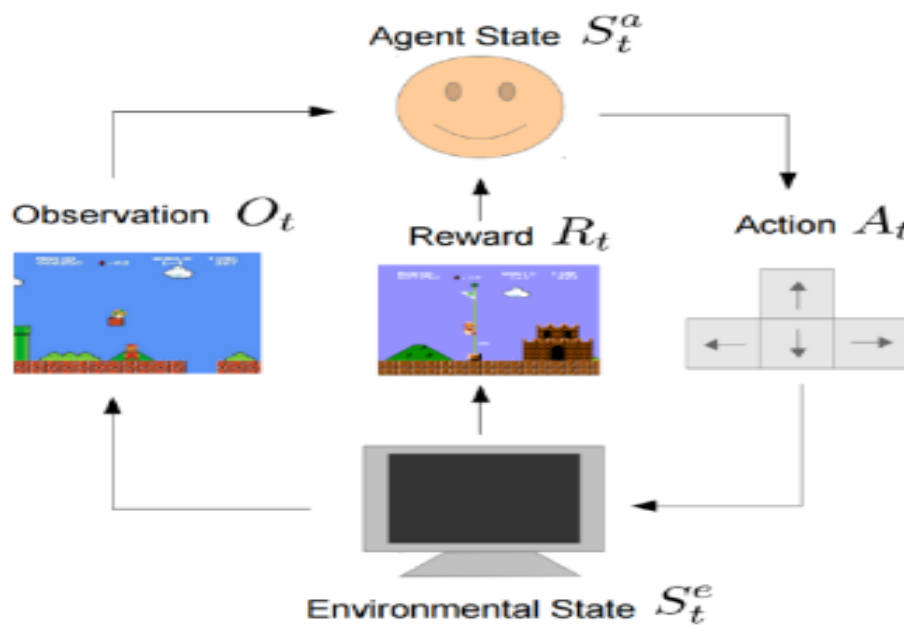


FIGURE 2.7 – Apprentissage par renforcement [11]

2.2.5.4 Les étapes de construction d'un algorithme d'apprentissage automatique

Pour la construction d'un algorithme d'apprentissage il y'en a des étapes à suivre dont les détails seront expliqués dans les prochains paragraphes.

2.2.5.4.1 Collection de données(Data collection)

La collecte de données initie le début du processus de ML et DL Les données peuvent être recherchées sur le web « lac de données » et être partagées.

L'ensemble de données constituent la base de la recherche sur la sécurité des réseaux informatiques. Le choix correct et l'utilisation raisonnable de l'ensemble de données sont les conditions préalables à la réalisation de recherches pertinentes en matière de sécurité. La taille de l'ensemble de données affecte également les effets d'entraînement des modèles d'un algorithme d'apprentissage automatique.

Les données de sécurité des réseaux informatiques peuvent généralement être obtenues de deux manières : 1) directement et 2) à l'aide d'un ensemble de données public existant[22].

1. **L'accès direct** : consiste à utiliser divers moyens de collecte directe des cyberdonnées requises, par exemple via les outils logiciels Win Dump ou Wireshark pour capturer les paquets réseau. Cette approche est très ciblée et adaptée à la collecte de données à court terme ou de petites quantités[22].
2. **A l'aide d'une base de données public existant** : les données à long terme ou de grandes quantités de données, le temps d'acquisition et les coûts de stockage augmenteront. L'utilisation d'une base de données de sécurité réseau existants peut économiser du temps de collecte de données et augmenter l'efficacité de la recherche en obtenant rapidement les diverses données nécessaires à la recherche[22].

Cette section présentera certains des ensembles de données de sécurité accessibles sur Internet.

- **CIC IDS2017** : L'ensemble de données CIC IDS 2017 est une donnée développée par la Faculté d'informatique de l'Université du Nouveau-Brunswick en 2017. Basé sur des recherches antérieures de Shiravi Ali CIC 2017 est une version améliorée de l'ensemble

de données ISCX 2012 . Le jeu de données CIC IDS 2017 est généré à partir de la généralisation réelle du trafic.

CIC IDS 2017 se compose de 5 jours de collecte de données avec 225 745 packages avec plus de 80 caractéristique et a rassemblé plus de sept jours d'activité réseau (c'est-à-dire normale et intrusion). Dans l'ensemble de données CIC 2017, la simulation d'attaque est divisée en sept catégories, à savoir Brute Force Attack, Heart Bleed Attack, Botnet, DoS Attack, DDoS Attack, Web Attack et Infiltration Attack[25].

- **CSIC HTTP 2010** : L'ensemble de données CSIC HTTP-2010 gère un grand nombre de requêtes web. L'ensemble de données HTTP CSIC-2010 est connu comme l'ensemble de données le plus ancien et le plus efficace pour la détection d'attaques dans les requêtes Web[18].

l'ensemble de données CSIC HTTP-2010 contient un trafic généré destiné à une application Web de commerce électronique. Il s'agit d'un ensemble de données généré automatiquement qui contient 36 000 requêtes normales et plus de 25 000 requêtes anormales (c'est-à-dire des attaques Web)[19].

- **ECML/PKDD 2007** Le challenge d'analyser le trafic web de l'ECML-PKDD 2007 consiste à déterminer si une requête HTTP donnée contient une ou plusieurs attaque(s) et si ces attaques réussiraient en fonction du contexte du serveur (OS, . . .). Dans un second temps, l'intervalle d'attaque doit être déterminé avec précision ($\pm n$ caractères, $n=3$)[20].

- **CSE-CIC-IDS2018** : Il s'agit de l'ensemble de données cybernétiques le plus récent et réaliste de l'Établissement canadien pour la cybersécurité (CIC) en 2018. Pour la détection des intrusions et l'anticipation des logiciels malveillants, les ensembles de données du CIC et de l'ISCX ont été utilisés dans le monde entier. L'objectif principal de cet ensemble de données est de créer une manière ordonnée de traiter la production d'un ensemble de données de référence différent et de grande envergure pour la détection d'intrusion sur la formation de profils de clients qui contiennent des représentations théoriques des occasions et des pratiques observées sur le système.

Cet ensemble de données se compose de sept situations d'attaque distinctes : Botnet, Heartbleed, Brute-force, Denial of Service et Distributed Denial of Service, infiltration à l'intérieur du réseau et attaques Web. Le cadre d'agression comprend 50 machines et l'association des victimes a 5 divisions et trente serveurs et 420 machines sont incorporées[21].

2.2.5.4.2 Prétraitement de données (data pre-processing)

Prétraitement des données est un processus de transformation des données de manière à ce qu'elles conviennent à un algorithme d'apprentissage. Cela peut avoir un impact important sur les performances du modèle.

Steve Lohr du New York Times a déclaré : « Les scientifiques des données, selon des interviews et des estimations d'experts, passent 50% à 80% de leur temps embourbés dans le travail de collecte et de préparation de données numériques indisciplinées, avant qu'elles ne puissent être explorées pour trouver des pépites utiles. »

Des enquêtes montrent que les scientifiques des données consacrent près de 80% de leur temps à la préparation des données

La figure suivante résume les étapes important du prétraitement de données.

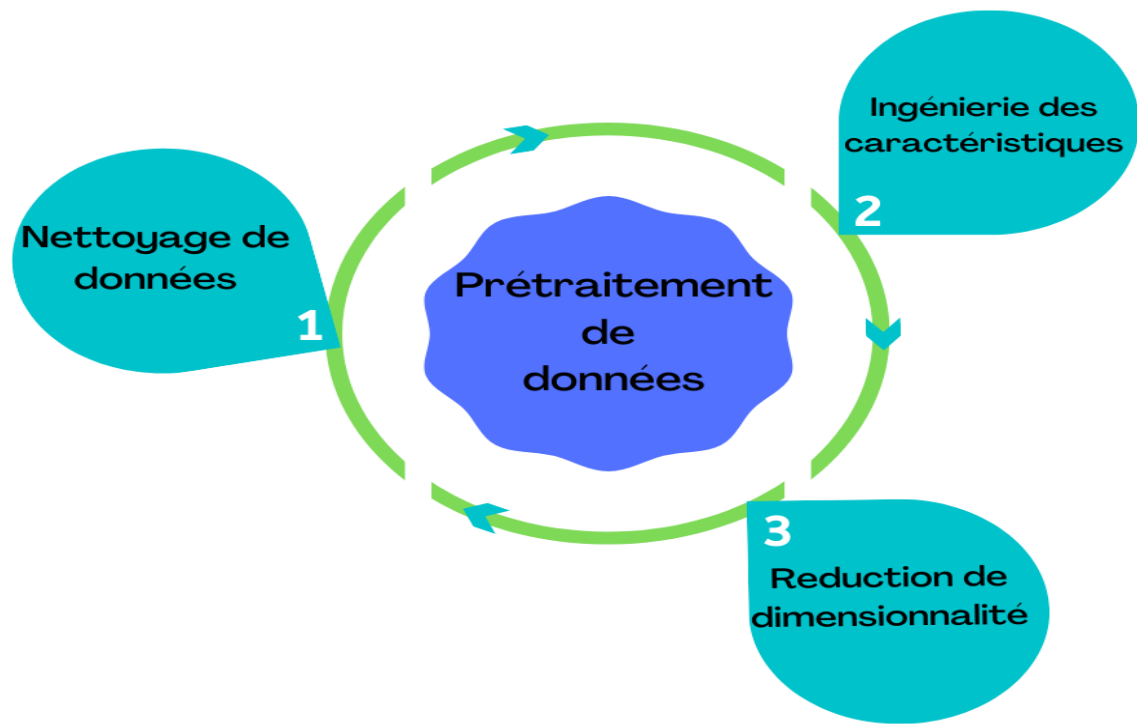


FIGURE 2.8 – Les étapes du pretraitement des données

2.2.5.4.2.1 Nettoyage de données(Data cleaning)

Les données du monde réel peuvent être incomplètes, bruyantes et incohérentes, ce qui peut masquer des schémas utiles. Cela est dû à[16] :

- Données incomplètes : valeurs d'attributs manquantes, certains attributs d'intérêt manquants ou contenant uniquement des données agrégées.
- Données bruitées : contenant des erreurs ou des valeurs aberrantes.
- Données incohérentes : contenant des divergences dans les codes ou les noms.

Nettoyage de données consiste à détecter et à supprimer les enregistrements inexacts, faux, incomplets, corrompus ou non pertinents de l'ensemble de données. L'une des approches les plus courantes pour le nettoyage des données est le nettoyage variable par variable. Dans cette approche, les valeurs des caractéristiques illégales ou mal orthographiées sont supprimées de l'ensemble de données en fonction de certains facteurs tels que la valeur minimale et maximale ne doivent pas être en dehors de la plage autorisée, la variance et l'écart type ne doivent pas être supérieurs à la valeur seuil et il ne doit pas y avoir être toute valeur mal orthographiée dans l'ensemble de données.

2.2.5.4.2.2 Ingénierie des caractéristiques(Features engineering)

L'ingénierie des caractéristiques est une tâche centrale dans la préparation des données pour l'apprentissage automatique. C'est la pratique consistant à construire des caractéristiques appropriées à partir de caractéristiques données qui conduisent à des performances prédictives améliorées. L'ingénierie des caractéristique implique l'application de fonctions de transformation telles que des opérateurs arithmétiques et d'agrégation sur des caractéristiques données pour en générer de nouvelles. Les transformations permettent de mettre à l'échelle une entité ou de convertir une relation non linéaire entre une entité et une classe cible en une relation linéaire, plus facile à apprendre [15]. C'est l'une des parties les plus difficiles et les plus chronophages de la préparation des données.

Les nouvelles caractéristiques sont créées sur la base de différents calculs entre les caractéristique existantes. Les nouvelles caractéristiques peuvent être un ratio, une transformation mathématique ou toute formule statistique ou scientifique pour générer une caractéristique plus significative. L'ingénierie des caractéristiques peut être effectuée à la fois manuellement par des statisticiens et en utilisant des techniques d'encodage des caractéristiques dans le cas de variables catégorielles. Il existe une idée fausse générale selon laquelle l'ingénierie des caractéristiques ne peut être bénéfique que pour les problèmes de régression linéaire ou de classification de texte. L'ingénierie des caractéristiques s'est avérée très bénéfique pour les machines à vecteurs de support, les forêts aléatoires, les réseaux de neurones et les machines à amplification de gradient. L'encodage est important car l'apprentissage automatique lui-même est basé sur des modèles mathématiques et des algorithmes, de sorte que la plupart des algorithmes ne peuvent pas classer entre les valeurs catégorielles et continues. L'encodage suit deux méthodologies : nominale et ordinale. Le codage nominal est effectué là où l'ordre des données n'est pas très important et vice-versa.

Outre l'encodage, il existe d'autres techniques d'ingénierie des caractéristiques telles que la normalisation. La normalisation est utilisée pour mettre à l'échelle toutes les valeurs d'un ensemble de données dans une plage fixe comprise entre 0 et 1. La formule utilisée pour la normalisation est la suivante[15] :

$$X_n = \frac{X - X_{min}}{X_{max} - X_{min}}$$

Bien qu'elle améliore l'évolutivité numérique du modèle, elle ne doit pas toujours être utilisée car elle peut nuire aux performances d'un modèle.

2.2.5.4.2.3 Réduction de dimensionnalité (Dimensionality reduction)

La réduction de la dimensionnalité réduit simplement la dimensionnalité de vos caractéristiques. Il existe deux approches du processus : la sélection de caractéristiques et l'extraction de caractéristiques.

1. **L'extraction de caractéristiques** : est plus adaptée aux données utilisées pour la reconnaissance de formes ou le traitement d'images où des inférences significatives ne peuvent pas être obtenues simplement en regardant les données[15].
2. **Sélection des caractéristiques** : Consiste à avoir toutes les caractéristiques prises en compte pour la modélisation peut réduire la prévisibilité du modèle. Il est toujours préférable de sélectionner les caractéristiques qui contribuent davantage à la variable cible. Ça peut être fait en utilisant des méthodes manuelles comme la sélection univariée où chaque caractéristique est évaluée pour déchiffrer son importance. Méthodes statistiques comme la variance et la corrélation de Pearson sont utilisées pour l'analyse univariée. Mais univarié l'analyse est plus fiable lorsque les données sont linéaires, aussi il est extrêmement difficile d'effectuer une analyse univariée sur un grand ensemble de données. Dans ce cas, l'analyse multivariée peut être effectuée. Il existe trois méthodes pour effectuer une analyse multivariée : filtre, wrapper et intégré.

Voici les méthodes de sélection des caractéristiques utilisées dans l'analyse multivariée [15] :

■ **Test du Chi-Square :**

Il s'agit d'un type de méthode de filtrage statistique utilisée pour évaluer la corrélation entre différentes caractéristiques à l'aide de leur distribution de fréquence. Dans cette méthode, la sélection des caractéristiques est basée sur les propriétés intrinsèques des caractéristiques et est indépendante de tout algorithme ML

■ **Élimination de caractéristiques récursives (RFE) :**

Il s'agit d'un type de méthode wrapper utilisée pour la sélection des caractéristiques. Le terme "wrapper" est utilisé car cette méthode encapsule un classificateur dans un algorithme de sélection de caractéristiques. Dans RFE, les caractéristiques sont supprimées de manière récursive de l'ensemble de données en fonction d'un estimateur externe utilisé qui est le classifieur. Le classificateur attribue des pondérations à une caractéristiques en fonction de ses performances. C'est un algorithme gourmand qui cherche à générer le sous-ensemble le plus performant.

■ **Sélection de caractéristiques basée sur l'arborescence :**

Il s'agit d'un type de méthode intégrée dans laquelle il existe une méthode intégrée pour l'importance des caractéristiques qui génère un ensemble de caractéristiques avec leur importance. Les méthodes intégrées peuvent être utilisées à l'aide d'algorithmes qui ont des méthodes de sélection de caractéristiques intégrées[15].

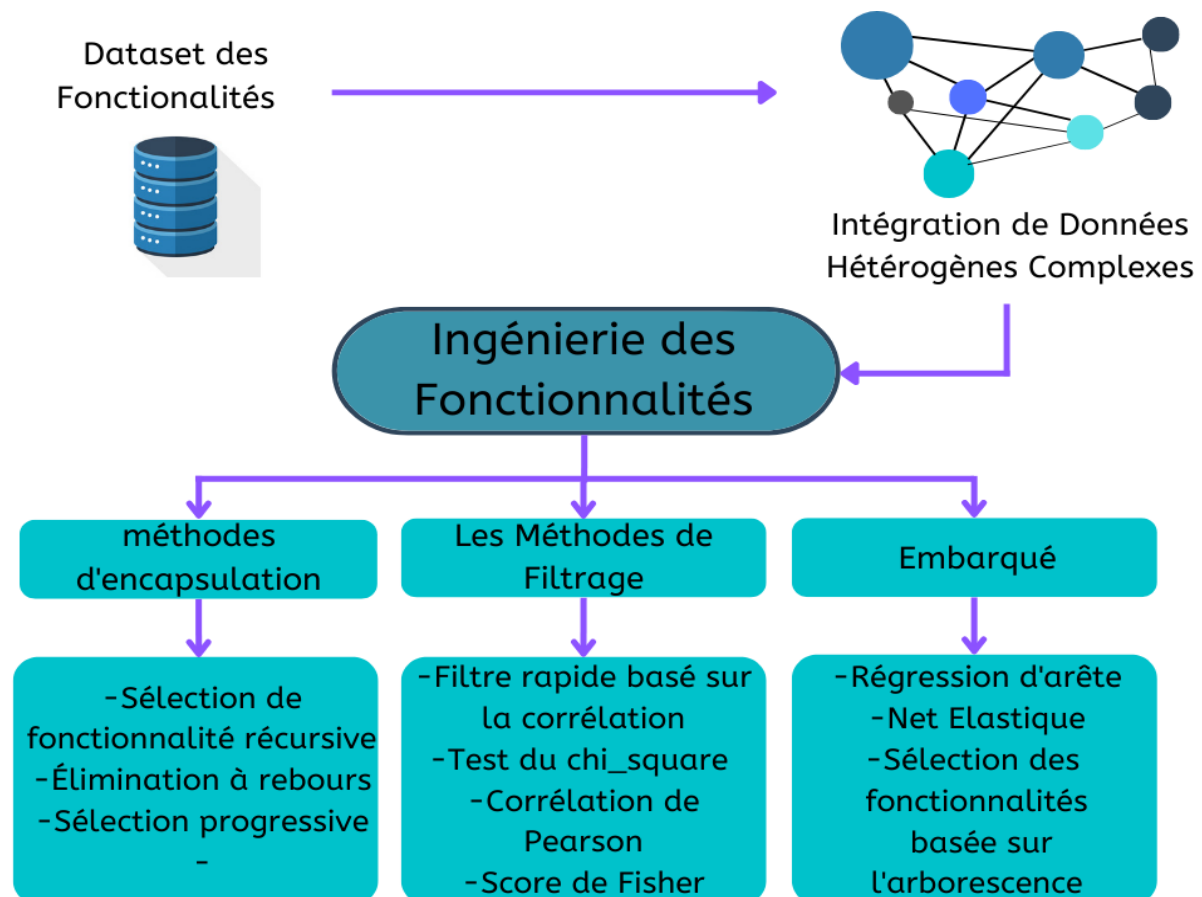


FIGURE 2.9 – Ingénierie des caractéristiques et réduction de la dimensionnalité

2.2.5.4.3 Données d'apprentissage et de test

Après le prétraitement des données d'apprentissage automatique, nous divisons notre ensemble de données en un ensemble d'entraînement et un ensemble de test. Il s'agit de l'une des étapes cruciales après le prétraitement des données, car ce faisant, nous pouvons améliorer les performances de notre modèle d'apprentissage automatique.



FIGURE 2.10 – Devision du Dataset

2.2.5.4.4 Sélection d'un modèle d'apprentissage (Model selection)

Après la préparation des données et division les données en ensemble d'entraînement et de test, des modèles appropriés doivent être sélectionnés pour la détection des attaques web. Puisqu'il s'agit d'un problème de classification, des classificateurs appropriés doivent être sélectionnés pour effectuer la classification des données (légitimes ou malveillantes)[15].

2.2.5.4.5 Entraînement du modèle (Model training)

Après la collection du données et la préparation des données ainsi que le choix du modèles l'étape suivante est d'entraîner le modèle.

2.2.5.4.6 Évaluation du performances du modèle

Le modèle des performances du modèle est une partie très importante dans la construction d'un algorithme d'apprentissage automatique. Parmi les métriques d'évaluation des performances des modèles d'apprentissage les plus utilisées dans le domaine de cybersécurité on trouve Exactitude (Accuracy), Rappel (recall), Précision (Precision), f1-score, FPR, FNR ou sont calculer à l'aide de la matrice de confusion.

La matrice de confusion est un tableau qui décrit en détail les résultats de la classification, qu'ils soient correctement ou incorrectement classés et que différentes classes soient distinguées, pour une classification binaire, une matrice 2*2 [22].

	prédit comme positif	prédit comme negative
Étiqueté comme positif	Vrai positif (VP)	Faux négatif (FN)
Étiqueté comme négatif	Faux positif (FP)	Vrai négatif (VN)

TABLE 2.3 – Confusion matrix

- Vrai positif(True positive) (**TP**) : échantillons positifs correctement classés par le modèle.
- Faux négatif(False negative) (**FN**) : échantillon positif mal classé par le modèle.
- Faux positif(False positive) (**FP**) : échantillon négatif mal classé par le modèle.
- Vrai négatif(True Negative) (**TN**) : échantillons négatifs correctement classés par le modèle.

De plus, les métriques suivantes peuvent être calculées à partir de la matrice de confusion :

- **Exactitude (Accuracy)** : Rapport du nombre d'échantillons correctement classés au nombre total d'échantillons pour un ensemble de données de test donné. Lorsque les cours sont équilibrés. c'est une bonne mesure ; sinon, cette métrique n'est pas très utile.

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

- **Précision (Precision)** : Il calcule le rapport de tous les "éléments correctement détectés" à tous les "éléments réellement détectés".

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

- **Rappel ou Taux de vrais positifs (Recall ou True Positive Rate)** : Il calcule le rapport de tous les "éléments correctement détectés" à tous les "éléments qui doivent être détectés".

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

- **Taux de faux négatifs (False Negative Rate)** : Rapport entre le nombre d'échantillons positifs mal classés et le nombre d'échantillons positifs.

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

- **Taux de faux positifs (False Positive Rate)** : Rapport entre le nombre d'échantillons négatifs mal classés et le nombre total d'échantillons négatifs.

$$FPR = \frac{FP}{FP + TN}$$

- **Taux vrai négatif (True Negative Rate)** : Rapport entre le nombre d'échantillons négatifs correctement classés et le nombre d'échantillons négatifs.

$$TNR = \frac{TN}{TN + FN}$$

- **F1-Score** : Il calcule la moyenne harmonique de la précision et du rappel.

$$F1 = \frac{2 * TP}{2 * TP + FN + FP}$$

- **[NOTE]** Les étapes de construction d'un algorithme d'apprentissage automatique sont les mêmes pour l'apprentissage automatique et l'apprentissage approfondi, excepte que dans l'apprentissage approfondi on passe l'étape de sélection des caractéristiques.

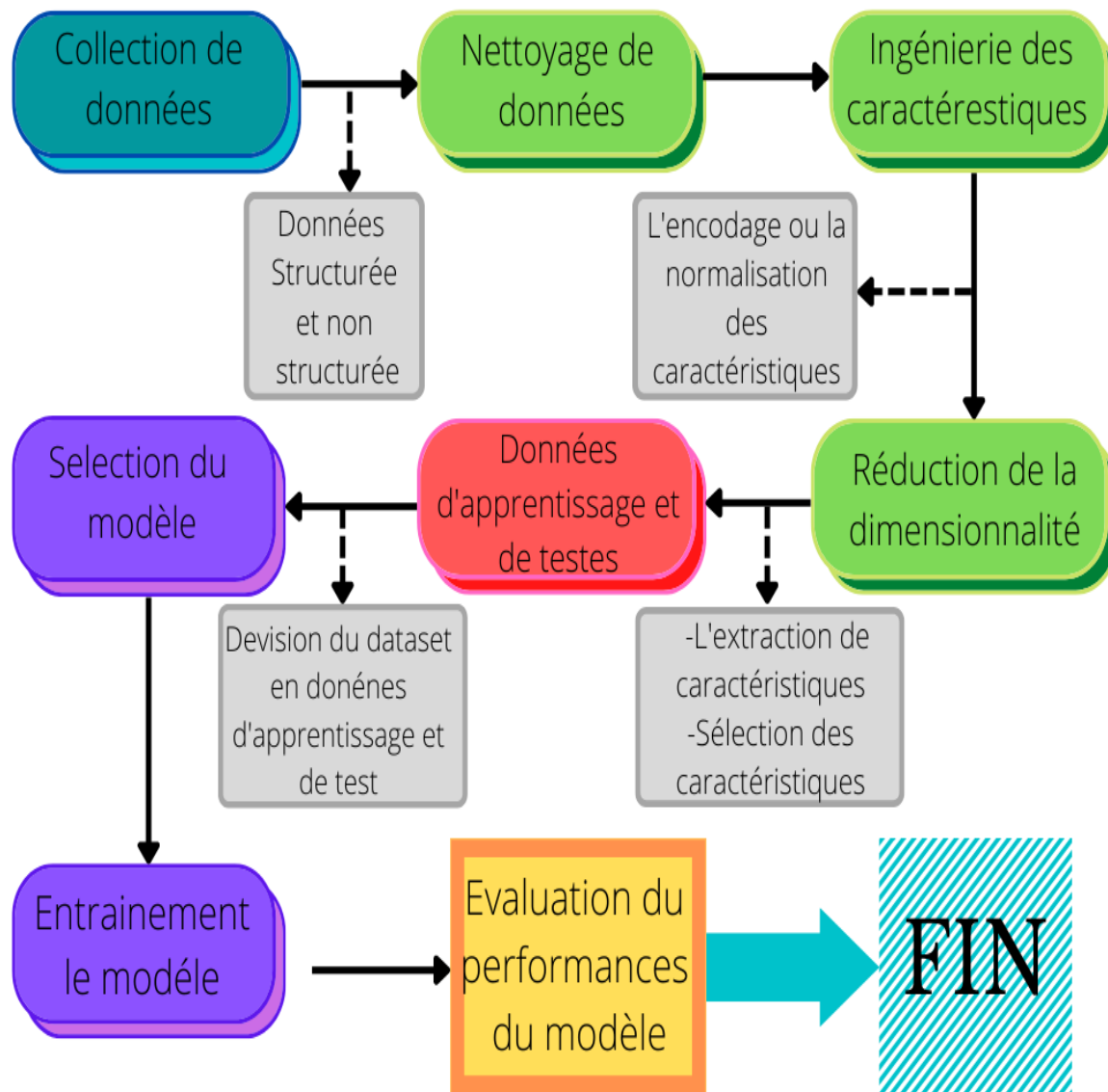


FIGURE 2.11 – Les étapes de construction d'un algorithme d'apprentissage automatique

2.2.6 Outils de construction des algorithmes apprentissage automatique

2.2.6.1 Des bibliothèques

Parmi les bibliothèques de construction des algorithmes d'apprentissage les plus utilisées on peut citer Scikit-learn et Keras.

Scikit-learn

Scikit-learn est une puissante bibliothèque d'apprentissage automatique open source écrite en Python qui s'est développée rapidement au cours des dernières années. Il permet l'intégration facile et rapide des méthodes d'apprentissage automatique dans le code Python. La bibliothèque scikit-learn comprend une large gamme de méthodes de classification, de régression, d'estimation de matrice de covariance, de réduction de dimensionnalité, de prétraitement des données et de génération de problèmes de référence. Il est accessible via l'URL <http://scikit-learn.org> [26].

Keras

Keras est une interface de programmation d'application (API) de réseau neuronal de haut niveau, ainsi elle est conçue pour réduire la charge cognitive des utilisateurs finaux, en détournant l'attention des détails de mise en œuvre standard et en permettant à la place de se concentrer sur la création de modèles. En tant que tel, Keras est extrêmement convivial pour les débutants et, pour beaucoup, un point d'entrée vers l'apprentissage automatique lui-même. Dans le même temps, Keras s'intègre en douceur avec son backend TensorFlow et permet aux utilisateurs de créer n'importe quel modèle qu'ils auraient pu implémenter dans TensorFlow pur. Cette flexibilité fait de Keras un excellent outil même pour les praticiens experts en apprentissage en profondeur et a récemment conduit à l'adoption de Keras par TensorFlow comme interface officielle du framework[27].

2.2.6.2 Des environnements

Parmi les environnements de construction des algorithmes d'apprentissage les plus utilisées on peut citer deux solutions cloud Kaggle Notebooks et GoogleColab.

Kaggle Notebooks

Kaggle Notebooks est un environnement informatique dans le cloud qui permet une analyse reproductible et collaborative. Le dernier type est les blocs-notes Jupyter (généralement simplement des « blocs-notes »). Les cahiers Jupyter consistent en une séquence de cellules, où chaque cellule est formatée en Markdown (pour écrire du texte) ou dans un langage de programmation de votre choix (pour écrire du code)[35].

GoogleColab

GoogleColab est un environnement Jupyter Notebooks en ligne de Google. Il fait tout ce qu'un ordinateur portable local ferait, mais il est dans le cloud, donc aucune installation de logiciel n'est nécessaire et il est disponible depuis n'importe quel ordinateur connecté à Internet. Les blocs-notes Colab vous permettent de combiner du code exécutable et du texte enrichi dans un seul document, ainsi que des images, HTML, LaTeX et plus encore. Lorsque vous créez vos propres blocs-notes Colab, ils sont stockés dans votre compte Google Drive. Vous pouvez facilement partager vos blocs-notes Colab avec des collègues ou des amis, leur permettant de commenter vos blocs-notes ou même de les modifier[36].

2.2.7 Domaines d'application de intelligence artificielle

- **Banque et finance** : L'industrie bancaire et financière est l'un des premiers à adopter l'intelligence artificielle.

Des chatbots proposés par les banques, par exemple, SIA par l'institution financière dépositaire de l'Inde, aux robo-traders intelligents d'Aidya et Nomura Securities pour le trading autonome à haute fréquence, les utilisations sont innombrables.

Des fonctionnalités telles que les robots IA, les conseillers en paiement numérique et les mécanismes de détection de fraude biométrique permettent d'offrir des services de meilleure qualité à une clientèle plus large.

L'adoption de l'IA dans le secteur bancaire est constante pour retravailler les entreprises du secteur, offrir des expériences plus utiles et plus personnalisées à leurs clients, réduire les risques et augmenter les opportunités impliquant les moteurs financiers de notre économie moderne.

- **Surveillance** : L'IA a permis de développer des outils de reconnaissance faciale pouvant être utilisés à des fins de surveillance et de sécurité.

En conséquence, cela permet aux systèmes de surveiller les images en temps réel et peut constituer un développement révolutionnaire en matière de sécurité publique.

La surveillance manuelle d'une caméra de vidéosurveillance nécessite une intervention humaine constante, elle est donc sujette aux erreurs et à la fatigue. La surveillance basée sur l'IA est automatisée et fonctionne 24h/24 et 7j/7, fournissant des informations en temps réel.

Selon un rapport du Carnegie Endowment for International Peace, au moins 75 des 176 pays utilisent des outils d'IA à des fins de surveillance.

Dans tout le pays, 400 millions de caméras de vidéosurveillance sont déjà in situ, alimentées par des technologies d'intelligence artificielle, principalement la reconnaissance faciale.

- **Jeux :** Dans l'industrie du jeu également, les systèmes de jeux informatiques alimentés par l'IA nous font entrer dans une ère de remplacement de l'expérience immersive dans le jeu.

L'IA est utilisée pour obtenir des comportements réactifs, adaptatifs ou intelligents principalement chez les personnages non joueurs (PNJ), presque comme l'intelligence humaine dans les jeux vidéo. Il sert à améliorer l'expérience du joueur au lieu d'apprendre par machine ou de décider.

L'IA a également joué un rôle énorme dans la création de jeux vidéo et en les adaptant davantage aux préférences des joueurs.

Matthew Guzdial de l'Université de l'Alberta et son équipe travaillent à tirer parti de la puissance de l'IA pour aider les joueurs vidéo à créer le jeu précis dont ils ont besoin pour jouer.

- **Les médias sociaux :** Les médias sociaux ne sont pas seulement une plate-forme pour réseauter et s'exprimer. Elle façonne inconsciemment nos choix, nos idéologies et notre tempérament.

Tout cela grâce aux outils d'Intelligence synthétique qui fonctionnent silencieusement en arrière-plan, nous montrant les messages que nous "pourrons" aimer et annonçant des produits qui "pourraient" être utiles en fonction de notre historique de recherche et de navigation.

Par exemple, Instagram a récemment révélé comment il utilisait l'IA pour personnaliser le contenu de l'onglet Explorer.

Cela facilite la publicité sur les réseaux sociaux en raison de sa capacité sans précédent à diffuser des annonces payantes auprès des utilisateurs de la plate-forme en fonction d'un ciblage démographique et comportemental très précis.

Saviez-vous que nous avons également des outils d'intelligence artificielle qui écriront pour nous des publicités Facebook et Instagram. Un autre énorme avantage de l'IA dans les médias sociaux est qu'elle permet aux spécialistes du marketing d'analyser et de suivre chaque étape qu'ils franchissent[31].

- **Santé :** L'IA est largement utilisée dans le domaine de la santé de nos jours. De nombreux pays sont encore se développant dans ce domaine. Plus de 100 entreprises qui sont des startups, utilisent différentes applications de L'IA dans la santé. Une application d'IA appelée infirmière virtuelle effectue presque toutes les tâches effectuées par infirmières humaines. Certaines entreprises ont développé des systèmes de consultation. C'est utile lorsque les médecins ne sont pas disponibles. Il traite les patients en fonction des symptômes signalés. Il offre des conseils médicaux à partir d'une grande base de données. En cas d'urgence, il conseille également de consulter un médecin.

- **Education :** AI a de nombreuses applications dans le domaine de l'éducation. Cela inclut répondre ou demander questions, donner des commentaires, etc. Les systèmes de tutorat intelligents ont également une énorme influence sur le terrain de l'éducation.

- **Droit :** Récemment, plusieurs cabinets d'avocats ont également commencé à utiliser des applications liées à l'IA. Il aide à la recherche sur la recherche de cas différents pour le cas

actuelBanks utilise des chatbots pour diverses applications telles que la vérification du solde, l'activation du compte etc. Les gens peuvent interagir dans leur langue maternelle. Ce système aide les clients qui ne connaissent pas avec la technologie.

- **Transport** : De nombreuses entreprises comme Uber, Tesla, Google ont développé des voitures autonomes. Assistants virtuels-Récemment, de nombreux assistants virtuels sont développés par les sociétés Google, Apple, Amazon, Microsoft. Google a créé Google Assistant, Apple-Siri, Amazon-Alexa, MicrosoftCortana. L'utilisateur peut interagir avec son langage naturel. Les assistants virtuels nous aident à effectuer diverses tâches telles que la gestion des horaires, la lecture de musique, des clips audio, etc.
- **E-commerce** : Les sites de commerce électronique comme Amazon gardent une trace des articles achetés par personnes et identifie le modèle d'intérêt de l'utilisateur. Les robots Heavy Industries-AI sont utilisés dans les industries pour effectuer des travaux dangereux. Ils assure l'efficacité[5].
- **Cybersécurité** : Dans ce contexte, les organisations ont commencé à utiliser l'IA pour aider à gérer une gamme croissante de risques de cybersécurité, de défis techniques et de contraintes de ressources en améliorant leurs systèmes. robustesse, résilience et réponse. Les chiens policiers fournissent une analogie utile pour comprendre pourquoi les entreprises utilisent l'IA pour accroître la cybersécurité. Les policiers utilisent des chiens policiers spécifiques capacités à chasser les menaces; de même, les systèmes d'IA travaillent avec des analystes de sécurité pour modifier la vitesse à laquelle les opérations peuvent être effectuées. À cet égard, la relation entre les systèmes d'IA et les opérateurs de sécurité doit être comprise comme une intégration synergique, dans laquelle la valeur ajoutée unique des humains et des systèmes d'IA est préservée et renforcée, plutôt que comme une concurrence entre les deux[6].

2.3 Conclusion

Dans ce chapitre on a montré que l'intelligence artificielle (IA) est un aspect très important de nos vies; des ordinateurs, des jeux vidéo et même des appareils de cuisine et de la cybersécurité. En tant qu'humains, nous avons permis à l'IA de s'infiltrer dans notre vie quotidienne alors qu'elle accomplit la tâche la plus simple pour nous, mais elle n'est pas accomplie au mieux de ses capacités. En tant qu'êtres humains, nous pouvons accomplir une tâche au meilleur de nos capacités en combinant nos expériences, nos émotions et notre logique. D'autre part, l'intelligence artificielle qui subit une grande évolution d'une vague à l'autre, formule une conclusion à travers une série d'équations mathématiques, de nombreux nombres de codes et une série de zéros et d'uns afin d'imiter nos capacités humaines de prise de décision. les différentes vagues d'intelligence artificielle se développent de temps en temps afin de réduire l'intervalle de succès humain par rapport à l'une des techniques d'apprentissage automatique.

CHAPITRE 3

L'INTELLIGENCE ARTIFICIELLE ET LA SECURITÉ WEB

3.1 Introduction

Face à la complexité et au volume croissants des cyberattaques des applications web, l'intelligence artificielle (IA) aide les analystes des opérations de sécurité sous-équipés à garder une longueur d'avance sur les menaces. En extrayant des renseignements sur les menaces à partir de millions de documents de recherche, de blogs et d'articles d'actualité, les technologies d'IA, telles que le Machine Learning et le traitement automatique du langage naturel, fournissent des informations rapides qui permettent d'éliminer le bruit des alertes quotidiennes et de réduire considérablement les temps de réponse.

Dans ce chapitre nous allons présenter tout d'abord les problèmes liés à la sécurité des applications web, ensuite nous allons aborder le rôle de Machine Learning/Deep Learning dans la sécurité des applications web.

3.2 Architecture d'applications web

Les applications web sont la solution réseau essentielle pour offrir des services web standard. Le développement de ces applications est basé sur le développement côté client et côté serveur. Le côté serveur implique un serveur web, une application web et un serveur de base de données ; il utilise des langages de script principaux, notamment .NET, PHP et JEE (Jakarta Enterprise Edition). Le côté client fonctionne sur le navigateur web de l'utilisateur avec des langages de script frontaux, notamment CSS/HTML, Javascript, etc. Ces deux éléments sont généralement interconnectés via le protocole HTTP. La figure 3.1 présente l'architecture des applications web côté serveur et côté client. La toile les applications sont devenues partie intégrante de la vie quotidienne des individus en raison de leur accessibilité et de leur commodité. Cependant, cette popularité accrue est une arme à double tranchant. En effet, Les applications web sont la principale autoroute permettant aux attaquants de mettre en péril des services critiques dans des secteurs vitaux tels que la santé, l'éducation, la banque et le commerce électronique [12].

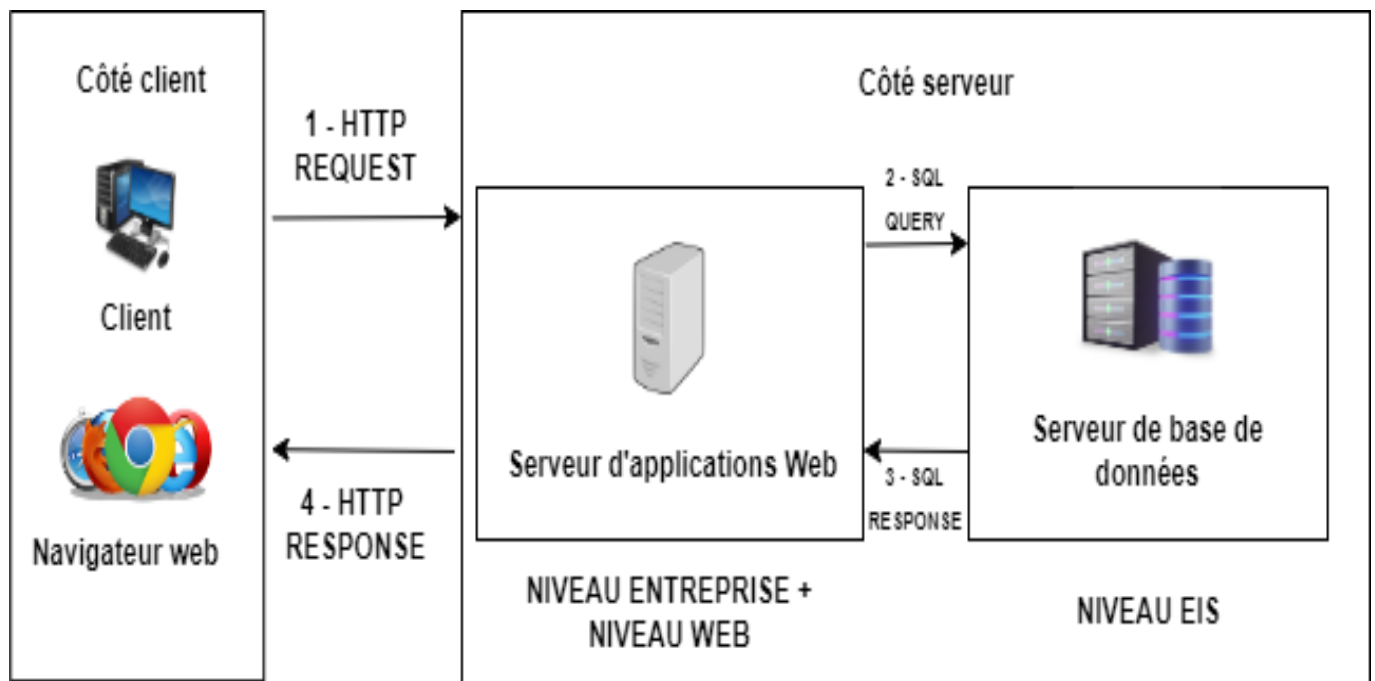


FIGURE 3.1 – Architecture d'applications Web [12]

3.3 Les risques de sécurité web les plus critiques selon OWASP top ten 2021

Selon le rapport OWASP TOP 10 2021 [32], les vulnérabilités web les plus critiques sont classées :

3.3.1 Injection

Une faille d'injection se produit quand une donnée non fiable est envoyée à un interpréteur en tant qu'élément d'une commande ou d'une requête. Les données hostiles de l'attaquant peuvent duper l'interpréteur afin de l'amener à exécuter des commandes inhabituelles ou à accéder à des données non autorisées.

3.3.2 Défaillance de l'authentification

Les failles de violation de gestion d'authentification et de session se produisent quand les fonctions correspondantes ne sont pas mises en œuvre correctement, permettant aux attaquants de compromettre les mots de passe, clés, jetons de session, ou d'exploiter d'autres failles d'implémentation pour s'approprier les identités d'autres utilisateurs.

3.3.3 Exposition des données sensibles

Correspond aux failles de sécurité exposant des données sensibles comme les mots de passe, les numéros de carte de paiement ou encore les données personnelles et la nécessité de chiffrer ces données.

3.3.4 Entités externes XML (XXE)

L'attaque d'entité externe XXE ou XML est une vulnérabilité d'application Web qui affecte un site Web qui analyse le XML non sécurisé piloté par l'utilisateur. L'attaque XXE, lorsqu'elle

est effectuée avec succès, peut divulguer des fichiers locaux dans le système de fichiers du site Web. XXE est ciblé pour accéder à ces fichiers locaux sensibles du site Web qui sont vulnérables à une analyse syntaxique dangereuse.

3.3.5 Défaillance du contrôle d'accès

Correspond aux failles de sécurité sur les droits des utilisateurs authentifiés. Les attaquants peuvent exploiter ces défauts pour accéder à d'autres utilisateurs.

3.3.6 Configuration incorrecte de la sécurité

Une faille due à une mauvaise configuration de sécurité se produit quand les serveurs d'application, serveurs Web, serveur de base de données, et la plate-forme n'ont pas de configuration sécurisée correctement établie et déployée.

3.3.7 Cross-Site Scripting (XSS)

Les failles de Cross-Site Scripting (XSS) se produisent chaque fois qu'une application prend des données non fiables et les envoie à un navigateur Web sans validation. XSS permet à des attaquants d'exécuter du script dans le navigateur de la victime afin de détourner des sessions utilisateur, défigurer des sites Web, ou rediriger l'utilisateur vers des sites malveillants.

3.3.8 Désérialisation non sécurisée

Alors que les objets peuvent être sérialisés pour les stocker ou les transférer, à un moment donné, ils peuvent avoir besoin d'être à nouveau désérialisés. Dans cette logique de désérialisation, des vulnérabilités peuvent résider. Le plus gros problème avec cet algorithme est que le processus de désérialisation ne discrimine pas car il désérialisera tout objet auquel l'application pourrait avoir accès. L'attaquant peut modifier les attributs de l'objet ou même en insérer un nouveau entièrement. Le processus de sérialisation peut laisser l'application vulnérable de plusieurs manières selon la logique de l'application et l'objet sérialisé. Nous allons examiner quelques exemples, mais sachez qu'il existe d'autres moyens d'exploiter cette vulnérabilité.

3.3.9 Utilisation de composants avec des vulnérabilités connues

De nouvelles cyber-vulnérabilités et menaces émergent chaque jour, mettant les utilisateurs en danger, mais toutes ne sont pas des zéro-jours. La plupart de ces menaces se produisent en raison de dépendances logicielles telles que l'utilisation de composants tels que des bibliothèques et des frameworks qui sont auparavant connus pour être vulnérables ou qui le deviennent plus tard en raison de correctifs logiciels non corrigés ou de mises à jour non implémentées à temps.

3.3.10 Insuffisance des journaux et de la surveillance

Une journalisation et une surveillance insuffisantes sont l'absence de journaux d'informations critiques pour la sécurité ou le manque de format de journal, de contexte, de stockage, de sécurité et de réponse rapide pour détecter un incident ou une violation[13].

3.4 Le rôle de Machine Learning et le Deep Learning dans la sécurité des applications web

3.4.1 L'utilisation du ML et DL dans la sécurité web

Les méthodes de sécurité traditionnelles ne sont plus adéquates face au nombre croissant de failles de sécurité et de vulnérabilités. Au lieu d'attendre qu'une vulnérabilité soit exploitée, les équipes de sécurité doivent être proactives dans la prévention et la préparation des cyber attaques.

L'intégration de l'IA dans les systèmes de sécurité est le moyen le plus efficace de lutter contre les cybers attaques. Les entreprises peuvent utiliser l'intelligence artificielle pour améliorer le processus de chasse aux menaces de sécurité en lui fournissant de grandes quantités de données d'application. Les logiciels d'IA peuvent évaluer les menaces et mettre en œuvre la contre-stratégie la plus efficace.

L'intelligence artificielle est un énorme pas en avant dans le monde de la technologie. Cela ouvre une pléthore de nouvelles opportunités qui faciliteront la vie de nombreuses personnes. Le revers de la médaille est que les cyber attaquants peuvent utiliser l'IA pour développer et déployer de nouvelles méthodes d'attaque contre les organisations. La seule façon de combattre les entités malveillantes avec l'IA est d'utiliser également l'IA contre elles.[14]

Avec l'augmentation massive de la quantité de menaces basées sur le Web et la complexité de leur détection, la sécurité web est devenue un sujet de recherche important. Les systèmes de détection d'attaques web basés sur des approches traditionnelles, telles que les approches basées sur les signatures et les anomalies, sont inefficaces pour sécuriser les applications web contre ces attaques. Parce que les systèmes basés sur les signatures ne peuvent pas détecter les attaques inconnues car ils s'appuient sur une liste de signatures d'attaques connues, et les systèmes basés sur les anomalies affectent la disponibilité des applications web en raison d'un FPR élevé. Tous ces défis ont souligné l'importance d'utiliser des techniques basées sur l'IA pour la sécurité web. Par rapport aux approches mentionnées, les systèmes de détection et de prévention des attaques web basés sur l'IA peut détecter les attaques connues et inconnues, telles que les attaques zero-day, avec un faible FPR et FNR . Diverses solutions basées sur l'IA ont été déployées pour détecter les attaques basées sur le web. Un système de détection d'attaques web basé sur l'IA est un système de classification déployé pour faire la distinction entre le trafic HTTP/s authentique et malveillant. En général, il s'agit d'un modèle qui apprend à partir d'une collection de données de formation pour identifier des modèles de comportements dangereux, de sorte que lorsque des actions similaires se produisent, elles peuvent être détectées automatiquement en temps réel.

En plus de la détection des attaques, les technologies basées sur l'IA peuvent être utilisées pour la détection des vulnérabilités. Il existe une distinction importante entre la détection des attaques et la détection des vulnérabilités. Le premier fait référence à la détection d'attaques d'utilisateurs malveillants. La seconde fait référence à la détection des faiblesses de l'application web qu'un attaquant peut utiliser pour mener des agressions compromettant des données sensibles ou détruisant l'application web. Selon le top 10 OWASP 2021, les vulnérabilités des applications web peuvent être classées en 10 catégories principales, à savoir le contrôle d'accès cassé, les échecs cryptographiques, l'injection, la conception non sécurisée, la mauvaise configuration de la sécurité, les composants vulnérables et obsolètes, les échecs d'identification et d'authentification, les échecs d'intégrité des logiciels et des données. , les échecs de journalisation et de surveillance de la sécurité et la falsification des demandes côté serveur. La détection de ces vulnérabilités avant le lancement de l'application web est une étape critique qui permet d'améliorer le niveau de sécurité d'une application web.

3.4.2 Application d'utilisation du ML dans la cybergdéfense

3.4.2.1 L'IA intégree aux équipements et applications de cybersécurité de l'infrastructure

Des technologies d'intelligence artificielle sont déjà intégrees dans des outils comme les anti-virus, les solutions EDR (Endpoint Detection and Response), les passerelles mail ou web, les firewalls, l'IAM, les CASB, les solutions DLP... , soit des équipements qui réagissent automatiquement aux attaques en filtrant le trafic malicieux. La plupart des éditeurs le font y compris en utilisant certaines technologies avancées telles que le deep learning (Google l'a intégree depuis 2015 pour filtrer les spams dans Gmail).

3.4.2.2 L'IA intégree dans les sondes réseaux et autres Intrusion Detection Systems (IDS)

De nombreuses sondes intégrent des technologies d'IA, en complément de leur moteur de détection. La plupart de ces systèmes apprennent le comportement « normal » de l'infrastructure et toute déviation est remontée comme un signe d'un risque cyber. Les alertes remontées sont exploitées par des analystes, typiquement au sein d'un SOC, avec un taux de faux positifs non négligeable. L'ajout de ces technologies dans une infrastructure augmenter la charge de travail, tout en permettant de détecter plus d'attaques, ou de les détecter plus tôt. Un des enjeux est donc de mieux intégrer ces outils. Concrètement, la pertinence de ces technologies d'IA est d'autant plus grande qu'elles sont déployées dans les environnements où le trafic est relativement déterministe, tels que dans les environnements industriels.

3.4.2.3 L'IA pour détecter les comportements anormaux dans un SOC

Dans ce cas d'usage, l'IA est utilisée en parallèle ou en complément de la détection temps réel effectuée par exemple dans un SIEM : le système apprend du comportement standard de l'infrastructure ou des utilisateurs et mesure des écarts par rapport à ce comportement.

À la différence des sondes qui sont placées à un endroit précis de l'infrastructure, l'information récoltée par l'outil peut-être extrêmement hétérogène et provenir de multiples sources, ce qui accroît très sensiblement le niveau de difficulté. De fait, ces technologies paraissent aujourd'hui plus pertinentes en complément des outils classiques pour des environnements stables et déterministes[33].

3.5 Conclusion

Les applications Web sont la meilleure solution basée sur Internet pour fournir des services Web en ligne, mais elles posent également de sérieux problèmes de sécurité. Ainsi, l'amélioration de la sécurité des applications Web contre les tentatives de piratage est d'une importance primordiale. Le pare-feu d'application Web traditionnels basés sur des règles manuelles et l'apprentissage automatique traditionnel nécessitent une grande expertise du domaine et une intervention humaine et ont des résultats de détection limités face au nombre croissant d'attaques Web inconnues.

En guise de conclusion, dernièrement le concept de l'intelligence artificielle débattu dans une large envergure au niveau mondiale . Cette discipline qui vise à remplacer les activités menées par l'humanité avec une techniques basées sur des machines de hautes technologies et capables de traiter automatiquement des équations et des situations très compliquées et dans un laps de temps. Cette technique peut être classifiée en machine learning qu'elle s'appuie sur un algorithme qui adapte lui-même le système à partir des retours faits par l'humain. Le système est ensuite alimenté par des données structurées et catégorisées lui permettant de comprendre comment classer de nouvelles données similaires. En fonction de ce classement, le système exécute ensuite les actions programmées et deep learning qui n'a pas besoin de données structurée et le système fonctionne à partir de plusieurs couches de réseaux neuronaux, qui combinent différents algorithmes en s'inspirant du cerveau humain et capable de travailler à partir de données non structurées.

Dans un contexte mondial connu actuellement par la concurrence aigüe à tout niveau, on trouve ce concept de l'IA en tant que levier majeur essentiel pour l'évolution de la majorité des domaines dont principalement la finance, la santé, l'éducation, la défense militaire, jeux, transport, commerce et la cybersécurité dans fait partie la cybersécurité des applications web. Etant donné que les applications web sont assujetties perpétuellement à des risques de sécurité dont les plus critiques sont qualifiées par OWASP TOP 10, les méthodes classiques de leur sécurisation demeurent dépassées et peu efficaces puisque la réaction de la détection des cyber attaques s'effectuent généralement en vain ; d'où l'intérêt de recourir à l'intelligence artificielle. Dans ce cas cette branche permet d'intervenir préalablement contre les intrusions et les anomalies. Néanmoins, les experts de la cybersécurité ne cessent de se développer dans la recherche scientifique ayant trait à ce domaine afin d'acquérir des compétences exceptionnelles puisqu'ils se trouvent toujours contraints de lutter contre des attaquants qui emploient eux aussi l'IA .

Bibliographie :

- [1] Yameogo, R.A., 2020. Risques et perspectives du big data et de l'intelligence artificielle : approche éthique et épistémologique (Doctoral dissertation, Normandie Université). page 68
- [2] Yameogo, R.A., 2020. Risques et perspectives du big data et de l'intelligence artificielle : approche éthique et épistémologique (Doctoral dissertation, Normandie Université).page 65,66
- [3] PK, F.A., 1984. What is Artificial Intelligence?. "Success is no accident. It is hard work, perseverance, learning, studying, sacrifice and most of all, love of what you are doing or learning to do"., p.65. ;Page :71
- [4] Larochelle, H., 2009. Étude de techniques d'apprentissage non-supervisé pour l'amélioration de l'entraînement supervisé de modèles connexionnistes. ; Chapitre 1 ; page 1
- [5] PK, F.A., 1984. What is Artificial Intelligence?. "Success is no accident. It is hard work, perseverance, learning, studying, sacrifice and most of all, love of what you are doing or learning to do"., p.65.
- [6] Artificial Intelligence and Cybersecurity ; Page :15
- [7] Haq, N.F., Onik, A.R., Hridoy, M.A.K., Rafni, M., Shah, F.M. and Farid, D.M., 2015. Application of machine learning approaches in intrusion detection system : a survey. IJARAI-International Journal of Advanced Research in Artificial Intelligence, 4(3), pp.9-18. ; page 10
- [8] Mahesh, B., 2020. Machine learning algorithms-a review. International Journal of Science and Research (IJSR).[Internet], 9, pp.381-386. ; page 381 383 384
- [9] Károly, A.I., Fullér, R. and Galambos, P., 2018. Unsupervised clustering for deep learning : A tutorial survey. Acta Polytechnica Hungarica, 15(8), pp.29-53. ;page 33

- [10] Dr. Rizwan A Khan , Introduction to Machine Learning ,page 5
- [11] Dr. Rizwan A Khan , Introduction to Machine Learning , page 35
- [12] Alaoui, R.L. and Nfaoui, E.H., 2022. Deep Learning for Vulnerability and Attack Detection on Web Applications : A Systematic Literature Review. Future Internet, 14(4), p.118.
- [13] EXISTANTES, I.L.C., Organisation des attaques web : classes et attributs.
- [14] Hoffman, W., 2021. Making AI Work for Cyber Defense.
- [15] Nargesian, F., Samulowitz, H., Khurana, U., Khalil, E.B. and Turaga, D.S., 2017, August. Learning Feature Engineering for Classification. In Ijcai (pp. 2529-2535).
- [16] Zhang, S., Zhang, C. and Yang, Q., 2003. Data preparation for data mining. Applied artificial intelligence, 17(5-6), pp.375-381.
- [17] Yulianto, A., Sukarno, P. and Suwastika, N.A., 2019, March. Improving adaboost-based intrusion detection system (IDS) performance on CIC IDS 2017 dataset. In Journal of Physics : Conference Series (Vol. 1192, No. 1, p. 012018). IOP Publishing.
- [18] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A., Chen, S., Liu, D. and Li, J., 2020. Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13(10), p.2509.
- [19] Alaoui, R.L. and Nfaoui, E.H., 2022. Deep Learning for Vulnerability and Attack Detection on Web Applications : A Systematic Literature Review. Future Internet, 14(4), p.118.
- [20] Raissi, C., Brissaud, J., Dray, G., Poncelet, P., Roche, M. and Teisseire, M., 2007, September. Web analyzing traffic challenge : description and results. In Proceedings of the ECML/PKDD (pp. 47-52).
- [21] Kanimozhi, V. and Jacob, T.P., 2019. Calibration of various optimized machine learning classifiers in network intrusion detection system on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. International Journal of Engineering Applied Sciences and Technology, 4(6), pp.2455-2143.
- [22] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H. and Wang, C., 2018. Machine learning and deep learning methods for cybersecurity. Ieee access, 6, pp.35365-35381.
- [23] Deng, L., 2018. Artificial intelligence in the rising wave of deep learning : The historical path and future outlook [perspectives]. IEEE Signal Processing Magazine, 35(1), pp.180-177.
- [24] Bonfanti, M.E. and Kohler, K., 2020. Intelligence artificielle et cybersécurité. Politique de sécurité : analyses du CSS, 265.
- [25] Dr. Rizwan A Khan , Introduction to Machine Learning

- [26] Kramer, O., 2016. Scikit-learn. In Machine learning for evolution strategies (pp. 45-53). Springer, Cham.
- [27] Grattarola, D. and Alippi, C., 2021. Graph neural networks in TensorFlow and keras with spektral [application notes]. IEEE Computational Intelligence Magazine, 16(1), pp.99-106.

Webographie :

- [28] <https://www.oracle.com/fr/artificial-intelligence/deep-learning-machine-learning-intelligence-artificielle.html> , accessed 25 June 2022
- [29] <https://www.ibm.com/cloud/learn/supervised-learning>, Accessed 25 June 2022
- [30] <https://analyticsinsights.io/apprentissage-supervise-vs-non-supervise/>, Accessed 25 June 2022
- [31] <https://techvidvan.com/tutorials/artificial-intelligence-applications/>, Accessed 25 June 2022
- [32] <https://owasp.org/www-project-top-ten/2017/>, Accessed 25 June 2022
- [33] <https://www.actuia.com/contribution/thomas-gayet/ia-et-cybersecurite-8-cas-dusage-principaux/>, Accessed 25 June 2022
- [34] <https://openai.com/dall-e-2/>, Accessed 25 June 2022
- [35] <https://www.kaggle.com/docs/notebooks>, Accessed 25 June 2022
- [36] <https://colab.research.google.com/notebooks/intro.ipynb>, Accessed 25 June 2022

