République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université 20 Août 1955- Skikda

Faculté des Sciences Département d'Informatique

Mémoire de fin d'études

En vue de l'obtention du diplôme Master (LMD)

Spécialité : Informatique

Filière : Systèmes d'Information

Thème

Détection d'intrusion utilisant intelligence artificiel fédéré pour les systèmes de santé IoT basés sur la blockchain

-Encadré par :
- DR. Aliguechi

Réalisé par :
- CHENNOUF Imene
- KAOUANE Folla

2024

Remerciements

Nous tenons tout d'abord à exprimer notre profonde gratitude envers toutes les personnes qui ont rendu possible la réalisation de ce mémoire de fin d'études. Nos remerciements vont à Nous tenons à exprimer notre sincère reconnaissance envers notre directeur de mémoire DR.Aliguechi, pour son soutien précieux et son expertise tout au long de notre projet de recherche. Ses conseils avisés, sa disponibilité et son encouragement constant ont été essentiels à notre réussite académique.

Nous sommes également reconnaissants envers notre famille et nos amis pour leur soutien indéfectible et leur patience tout au long de cette période exigeante. Leur encouragement nous a permis de surmonter les défis rencontrés et d'atteindre nos objectifs.

Enfin, nous remercions toutes les personnes et institutions qui ont contribué de près ou de loin à la réalisation de ce mémoire.

Ce travail représente non seulement un accomplissement personnel. Nous sommes honorés d'avoir pu mener à bien ce projet et nous vous sommes reconnaissants pour votre précieuse contribution.

Merci à tous.

Résumé

Récemment, le système de santé basé sur l'Internet des objets (IoT) s'est considérablement développé, mais il est limité par l'absence d'un mécanisme de détection d'intrusion (IDS). Les technologies modernes comme la blockchain (BC), l'informatique en périphérie (EC) et l'apprentissage automatique offrent une solution de sécurité robuste adaptée à la protection des informations médicales des patients. Dans ce mémoire, on va réaliser une approche de détection d'intrusion pour un système de santé IoT proposée récemment. Cette approche représente une intégration de ces technologies.

Mots clé : Blockchain, IA, IA Fédéré, IOT, cloud, Santé

Abstract

Recently, the Internet of Things (IoT)-based healthcare system has significantly developed but is limited by the absence of an Intrusion Detection System (IDS). Modern technologies such as blockchain (BC), edge computing (EC), and machine learning offer a robust security solution suitable for protecting patients' medical information. In this thesis, we will implement an intrusion detection approach for a recently proposed IoT healthcare system. This approach integrates these technologies.

Keywords: Blockchain, IA, IA Federated, IOT, Cloud, Health care

الملخص

مؤخرًا، نمت أنظمة الرعاية الصحية المعتمدة على الإنترنت من خلال الأشياء المتصلة بشكل كبير، ولكنها ما زالت محدودة بسبب عدم وجود نظام كشف التسللات .تقدم التقنيات الحديثة مثل التقنية الحجرية والحوسبة على الحافة، والتعلم الآلي حلاً أمنيًا قويًا مناسبًا لحماية معلومات المرضى الطبية. في هذا البحث، سنقوم بتنفيذ نهج لكشف التسللات لنظام رعاية صحية معتمد على الأشياء المتصلة تم اقتراحه مؤخرًا. يدمج هذا النهج هذه التقنيات.

الكلمات الرئيسية: سلسلة الكتل، الذكاء الاصطناعي، الذكاء الاصطناعي الفيدرالي، إنترنت الأشياء، cloud، الصحة

Table de matière

Tables de figure

Introduction générale

1. Contexte du projet :

Les systèmes de santé IoT (Internet des Objets) représentent une avancée majeure dans la prestation des soins de santé, permettant une surveillance continue des patients et une gestion efficace des données médicales. Cependant, l'adoption croissante de ces technologies expose également les infrastructures de santé à des risques élevés de cyberattaques. La sécurité et la protection des données sensibles des patients deviennent ainsi des préoccupations critiques dans ce contexte technologiquement avancé.

2. Problématique

Les dispositifs IoT collectent et transmettent en temps réel une quantité immense de données médicales personnelles. Ces informations, souvent sensibles et confidentielles, sont particulièrement vulnérables aux cybermenaces telles que le vol de données, les intrusions malveillantes ou les interruptions de service. La centralisation des données dans les systèmes traditionnels expose également ces informations à un risque accru en cas de faille de sécurité.

3. Solution choisie

Pour répondre à ces défis, l'intégration de l'intelligence artificielle (IA) fédérée et de la technologie blockchain émerge comme une solution innovante et prometteuse. L'IA fédérée permet de maintenir la confidentialité des données en effectuant le traitement et l'analyse directement sur les dispositifs IoT eux-mêmes, sans nécessiter le transfert des données brutes vers un serveur centralisé. Cette approche garantit que les informations personnelles des patients restent localisées et protégées, réduisant ainsi les risques de compromission des données.

Parallèlement, la blockchain offre une infrastructure décentralisée et sécurisée pour enregistrer de manière immuable les transactions et les événements de sécurité critiques. En utilisant la blockchain, les systèmes de santé peuvent assurer l'intégrité des données médicales en empêchant la modification non autorisée des enregistrements et en permettant une traçabilité complète des accès aux données.

En combinant l'IA fédérée pour l'analyse sécurisée des données et la blockchain pour la sécurisation et la traçabilité, les systèmes de santé IoT peuvent non seulement renforcer leur résilience face aux menaces cybernétiques, mais aussi améliorer la confidentialité et la sécurité des informations médicales sensibles. Cette approche représente ainsi une avancée

significative dans la protection des infrastructures de santé modernes et dans la préservation de la confiance des patients dans l'utilisation des technologies IoT pour leurs soins de santé.

4. L'organisation de mémoire:

✓ Ce document est divisé en quatre chapitres organisés comme suit :

(Introduction générale)

Nous avons parlé de notre projet, ainsi que des problèmes actuels et proposer des solutions.

Chapitre 1(Internet des objets (IOT)

Dans ce chapitre, nous avons défini L'IOT et expliqué les concepts qui composent l'internet des objets L'avenir de plusieurs domaines.

Chapitre 2 (Sécurité des données dans IOT)

Dans ce chapitre nous avons présenté la sécurité des données et les déférents types des données dans IOT, nous avons parlé aussi sur les principaux concepts de base en sécurité dans l'Internet des objets, les menaces de sécurité pour l'IoT et les défenses possibles, En fin nous avons parlé sur l'Intrusion Détection System (IDS) et les méthodes de détection d'intrusion et ses classifications.

Chapitre 3 (Approche de détection intrusion basé sur les blockchain et IA)

Dans ce chapitre, nous avons parlé de la blockchain et ses grands principes, ses domaines et ses types et les avantages et les inconvénients de cette technologie. Nous avons défini l'intelligence artificielle, y compris leurs avantages et inconvénients, et aussi nous citez les types. Nous avons présenté l'approche de détection intrusion avec block Chain et IA

Chapitre 4 (Implémentation)

Dans ce chapitre Nous avons présenté l'implémentation de cette approche.

Conclusion générale

Finalement, nous terminons notre mémoire par une conclusion générale

Chapitre 01 : Internet des objets (IOT)

1. Introduction

Dans ce chapitre, nous aborderons la définition de L'Internet des objets, son histoire depuis qu'elle était inventée jusqu'à nos jours, et les avantage de l'IdO. Qui a pu marquer son utilisation dans divers domaines et lorsqu`on parle particulièrement de cette technologie dans le domaine des soins de santé.

2. Définitions d'Internet des objets

Il n'existe pas une définition standard et unifiée de l'Internet des objets, et certaines définitions concernent les aspects techniques de l'IoT, tandis que d'autres définitions évoquent l'utilisation et caractéristique

Définition 1

L'IoT définit différentes solutions techniques avec un ensemble de caractéristiques identification des objets, capter, stocker, traiter, et transférer des données dans les environnements physiques [01].

Définition 2

L'Internet des objets (IoT) est défini comme un réseau mondial de services intercone.Divers appareils et objets intelligents utilisés pour soutenir les activités humaies. Grâce à leurs capacités de détection, de calcul et de communication, ils jouent un rôle important dans la vie quotidienne.leur capacité à observer le monde physique et à foirdes informations la prise de décision deviendra partie intégrante de la future architecture Internet [02].

Définition 3

La technologie de l'Internet des objets est considérée comme l'émergence du futur Internet, et certains le définissent comme « des objets dotés d'identités et de personnalités virtuelles, fonctionnant dans des espaces intelligents et utilisant des interfaces intelligentes pour se connecter et communiquer dans divers environnements d'utilisation ». [03]

D'autres insistent sur l'aspect omniprésent de l'IoT, permettant aux individus de se connecter les uns aux autres n'importe où, n'importe quand et avec n'importe quoi. Ce nouveau paradigme informatique ne repose plus sur des ordinateurs personnels et des périphériques

informatiques, mais sur des objets du quotidien, en leur fournissant une intelligence de capteur intégrée et la capacité de communiquer sur Internet [04].

En façon générale, l'Internet des Objets concerne tous les objets pouvant être connectés à un réseau Internet. Mais aujourd'hui, l'IoT concerne plus particulièrement les objets connectés équipés de capteurs, de logiciels et d'autres technologies leur permettant de transmettre et de recevoir des données entre eux, à des fins d'information ou d'automatisation. Jusqu'à présent, la connectivité venait principalement du Wi-Fi, alors qu'aujourd'hui la 5G et les autres types de plateformes en réseau offrent de traiter presque partout d'immenses ensembles de données de manière rapide et fiable.

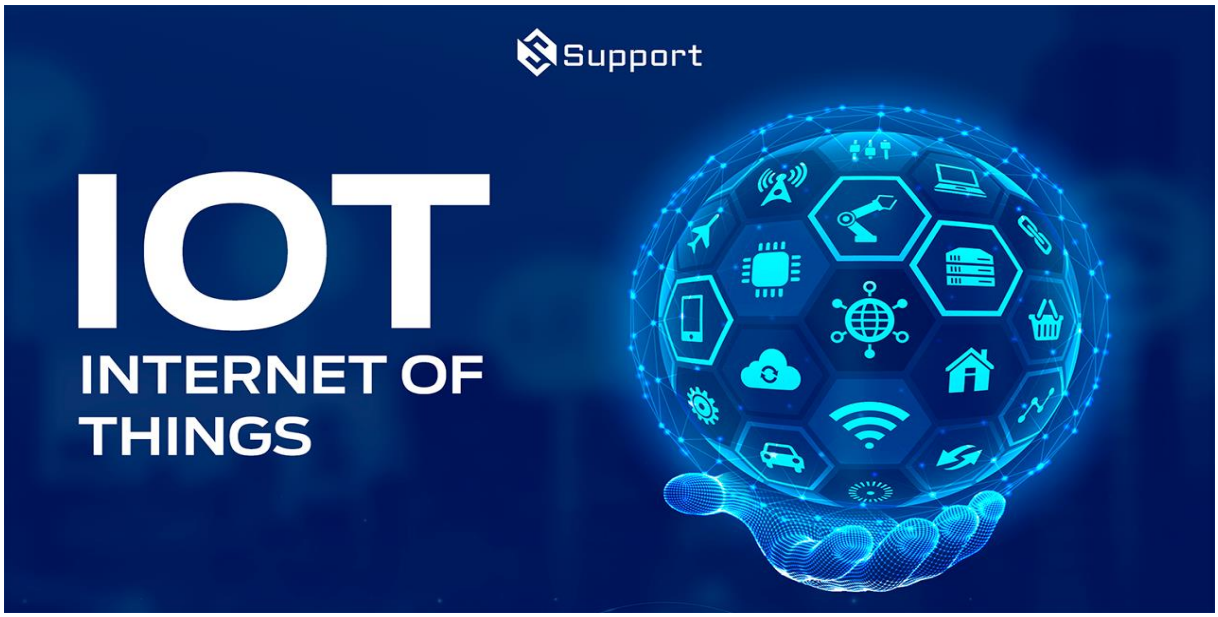

Figure 1 : Internet des objets

3. Historique de l'IoT

Historiquement le terme IoT a été utilisé pour la première fois en 1999 par Kevin Ashton, un ingénieur britannique, pour décrire un système où les objets physiques sont connectés à internet. Tous les objets utilisent la technologie d'identification par radiofréquence (RFID). Avec l'émergence du nouveau protocole IPv6, des secteurs tels que l'aérospatiale ont rapidement adopté le concept de l'Internet des objets et ont activement participé à la recherche. Le concept a gagné en popularité en 2007. Par la suite, l'idée de construire un Internet mondial des objets a été envisagée [05].

4. L'évolution d'internet des objets

En 1990, le premier objet de connexion est reformulé. Il s'agit de grille-pain, de machines à café ou d'autres objets du quotidien. En 2000, le fabricant coréen LG a lancé une entreprise sérieusement engagée dans les appareils électroménagers connectés à Internet, et la même année, les premières expériences avec des appareils connectés à Internet pour la recherche automatique d'informations sont réalisées.
En 2003, la population mondiale atteignait environ 6,3 milliards de personnes avec 500 millions d'appareils connectés à Internet [04]. Le résultat de la division du nombre d'appareils par la population mondiale (0,08) indique un faible nombre d'appareils connectés par habitant.Selon la définition de Cisco IBSG, l'Internet des objets n'existait pas en 2003 en raison du faible nombre d'objets connectés. En raison de l'explosion des smartphones et des tablettes, le nombre d'appareils et de personnes connectées à Internet a atteint 12,5 milliards en 2010, sur une population mondiale de 6,8 milliards.
Ainsi, pour la première fois dans l'histoire, il y a plus d'un appareil connecté par personne (1,84). Cisco explique l'évolution du nombre d'objets dans son livre blanc IoT [06]. Aujourd'hui, il dépasse de loin le nombre d'habitants de la planète et Comme mentionné, on s'attend à ce qu'elle continue de croître jusqu'à atteindre 50 milliards. [6]

Figure 2 : L'IOT Aujourd'hui

5. Les avantages de l'Internet des objets

Aujourd'hui, l'Internet des objets (IoT) a révolutionné la façon dont nous interagissons avec le monde qui nous entoure. Connecter des appareils et des objets du quotidien à Internet nous a permis de bénéficier d'une série d'avantages auparavant impensables. Dans cet article, nous explorerons les principaux avantages de l'Internet des objets et comment ce concept transforme notre quotidien [07].

5.1. Automatisation et efficacité

L'un des principaux avantages de l'IoT est l'automatisation des tâches. En connectant des appareils, nous pouvons les programmer pour qu'ils effectuent automatiquement des actions, ce qui nous fait gagner du temps et des efforts. Par exemple, nous pouvons programmer notre système de climatisation pour qu'il s'allume et s'éteigne selon nos préférences ou encore le contrôler à distance grâce à une application mobile. De plus, l'IoT nous permet également de collecter et d'analyser des données en temps réel, nous fournissant ainsi des informations précieuses sur l'utilisation de nos appareils. Cela nous aide à optimiser son fonctionnement et à prendre des décisions plus intelligentes, ce qui se traduit par une plus grande efficacité dans notre vie quotidienne [07].

5.2. Sécurité améliorée

L'IoT a également amélioré la sécurité dans divers aspects de nos vies. Par exemple, les systèmes de sécurité connectés à Internet nous permettent de contrôler et de surveiller notre maison ou notre entreprise à tout moment, même lorsque nous ne sommes pas physiquement présents. Cela nous donne une plus grande tranquillité d'esprit et nous aide à prévenir d'éventuels vols ou incidents. Un autre exemple de sécurité renforcée est l'utilisation de dispositifs de suivi GPS. Ces dispositifs permettent de localiser des objets ou des personnes en temps réel, ce qui est particulièrement utile dans les situations d'urgence ou pour éviter la perte d'objets de valeur [07].

5.3. Plus de commodité et de confort

L'IoT nous offre la possibilité de bénéficier d'un plus grand confort dans notre vie quotidienne. L'interconnexion des appareils nous permet de contrôler à distance différents aspects de notre environnement domestique ou de travail. On peut par exemple allumer les

lumières, monter ou baisser les stores, ou encore préparer du café depuis le confort de son canapé grâce à une application mobile ou un appareil vocal [07].

5.4. Qualité de vie améliorée

L'IoT a amélioré la qualité de vie des gens à bien des égards. Par exemple, dans la maison, les appareils intelligents permettent de contrôler à distance l'éclairage, la température et la sécurité, offrant ainsi commodité et sécurité. De plus, dans le domaine de la santé, les appareils médicaux connectés peuvent surveiller en permanence l'état de santé des patients et envoyer des alertes en cas d'anomalies [07].

5.5. Optimisation des ressources

L'IoT a facilité l'optimisation des ressources dans différents secteurs. Par exemple, dans l'industrie, les appareils connectés peuvent collecter des données en temps réel sur les performances des machines, identifiant ainsi les problèmes potentiels et évitant des interruptions de production coûteuses. Dans le domaine de l'énergie, les compteurs intelligents permettent une utilisation plus efficace de l'énergie, réduisant ainsi les coûts et l'impact environnemental [07].

5.6. Accès à l'information en temps réel

Avec l'IoT, il est possible d'accéder aux informations en temps réel, de n'importe où et à tout moment. Ceci est particulièrement utile dans des secteurs tels que la logistique, où la localisation des produits peut être suivie avec précision en temps réel. Toujours dans le domaine des transports, les capteurs connectés aux véhicules permettent de collecter des données sur la circulation et l'état des routes, ce qui facilite la prise de décision et l'optimisation des itinéraires [07].

5.7. Innovation et développement technologique

L'IoT a stimulé l'innovation et le développement technologique dans de nombreux domaines. L'interconnexion des appareils a ouvert de nouvelles possibilités dans des domaines tels que la domotique, la santé, l'agriculture, les transports et l'industrie, entre autres [07].

6. Domaines d'applications

L'Internet des Objets est d'ores et déjà utilisé dans divers domaines, soit de manière productive, soit de manière expérimentale dans le cadre des projets de recherche et de développement.

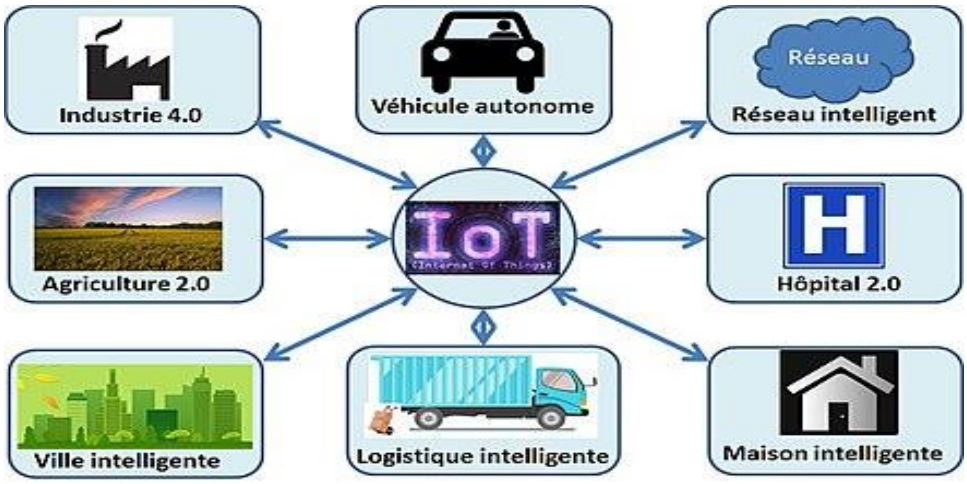

Figure 3 : Domaine d'application de l'IOT

6.1 Santé (health care)

S'il y a un domaine qui devrait faire massivement à appel l'IdO, c'est celui de la santé. On parle plus généralement et dans le contexte actuel des choses de la e-Santé pour faire référence à une santé intelligente reposant sur des objets médicaux connectés, un concept apparu avec le « boom » des Smartphones et la popularisation d'Internet. L'IoT surveillera les signes fournir des cliniques aux patients en créant des réseaux personnels et des capteurs médicaux surveiller les constantes biologiques telles que la température corporelle, Tension artérielle et activité respiratoire [06]. Afin de faciliter la surveillance et d'apporter des solutions, notamment aux personnes à mobilité réduite, dans le domaine de la santé, leurs activités dans leur milieu de vie sont surveillées grâce à des capteurs portables (accéléromètres, gyroscopes, etc.) ou fixes. Que ce soit pour assurer le suivi précis et à temps réel d'un patient, en mesurant à tout moment une caractéristique du corps sans l'intervention d'un médecin, ou pour vérifier la bonne prise d'un traitement, l'arrivée de l'Internet des Objets va permettre de traiter avec rapidité et précision les flux d'informations collectées et ,ça peut même aller à prévoir les interventions nécessaires au cas d'urgence dans la mesure du possible. En mettant de côté les objets permettant un coaching, comme par exemple les pèse-personnes connectés, ce domaine s'adresse plus particulièrement aux personnes âgées. Il existe plusieurs technologies qui intègrent déjà les principes de l'IDO comme les "Wearable

Technologies" capables d'être portées par l'utilisateur, à la manière de lunettes, bracelets, lentilles, puces ou encore sous forme de patchs intégrés dans le corps [02].

Figure 4 l'IOT in domaine santé:

6.2 Environnement

Dans ce domaine, un rôle clé est joué par capacité à détecter et autogérer les phénomènes naturels, vent, Hauteurs des rivières, etc. De plus, une intégration transparente de ces données hétérogènes [08].

6.3 Villes intelligentes (Smart City)

Le terme villes intelligentes est utilisé pour désigner l'écosystème cyber [09]. Grâce à des services avancés, il est en effet pu optimiser l'utilisation de l'infrastructure physique de la ville (réseau routes, réseaux électriques, etc.), améliorant ainsi la qualité de vie des personnes citoyen.

6.4 La publicité

L'internet des objets se reflète dans les activités de marketing car il offre des moyens de diffuser des messages publicitaires au grand public.

L'exemple le plus courant est celui des codes QR, qui peuvent être scannés par des applications spécifiques sur les smartphones pour accéder rapidement et facilement à des informations supplémentaires sur l'annonceur et ses produits [02].

6.5 Le transport

L'Internet des Objets constitue un facteur d'importance pour l'avenir des transports, autant dans le domaine de l'automobile et du transport privé que dans tout ce qui concerne le transport public [02].

6.6 Domotique (domotique)

Il s'agit d'un ensemble de technologies qui permettent à une maison d'être intelligente, de penser par elle-même et de contrôler divers appareils à partir de la même interface (téléphone, panneau) grâce à l'internet des objets. Cela a facilité et créé une communication entre les appareils ménagers et a permis de les contrôler à distance. Par conséquent, l'internet des objets s'est étendu aux villes [08].

7. Composantes de l'IoT

Les composant l'IoT est cinq. L'objet connecté est d'abord un objet qui a une fonction mécanique et/ou électrique propre, il peut soit être conçu directement connectable, soit il est déjà existant et la connectivité est rajoutée à posteriori. L'objet connecté a pour fonction de collecter des données de capteurs, de traiter ces données et de les communiquer à l'aide de d'une fonction de connectivité et de recevoir des instructions pour exécuter une action. Généralement ces fonctions de l'objet connecté nécessitent une source d'énergie, surtout quand les données sont prétraitées directement dans l'objet [09].

- **Capteur**

Les capteurs sont des dispositifs permettant de transformer une grandeur physique observée (température, luminosité, mouvement etc…) en une grandeur digitale utilisable par des logiciels. Il existe une très grande variété de capteurs de tous types, les objets connectés ont souvent la fonction de captation de ces grandeurs physiques sur leurs lieux d'utilisation. Exemple de capteurs : lumière, présence, proximité, position, déplacement, accélération, rotation, température, humidité, son, vibration, électrique, magnétique… [02]

- **Réseaux de capteurs**

Pour répondre aux besoins de communication entre eux, les capteurs sont équipés de dispositifs sans fil pour l'envoi et la réception de données. Cependant, cela ne suffit pas à rendre accessible ou du moins interopérable, transparent et simplifié une gamme de capteurs. Pour cela il faut aussi organiser les capteurs. Un réseau de capteurs se caractérise par le fait

que ses éléments sont de très petits appareils,Équipé de fonctions de transmission sans fil [10].

- **Énergie**

La plus importante contrainte à laquelle sont soumis les restes aux capteurs concernant l'énergie. L'autonomie temporelle des nœuds s'évalue en termes d'années [11].

- **Actionneurs :**

Les actionneurs sont des dispositifs qui convertissent des données numériques en phénomènes physiques pour produire une action. Ils sont en quelque sorte à l'opposé du capteur. Exemple pour les actionneurs : afficheurs, alarmes, caméras, haut-parleurs, interrupteurs, lampes, moteurs, pompes, serrures, vannes, ventilateurs, cylindres [10].

- **Connectivité :**

La connectivité de l'objet est assurée par une petite antenne **r**adiofréquence qui permet à l'objet de communiquer avec un ou plusieurs réseaux (détaillés dans la section « Réseaux IoT »). Les objets pourront transmettre des informations telles que leur identité, leur statut, une alarme ou les données d'un capteur d'une part, et recevoir des informations telles que des commandes d'action et des données d'autre part. Le module de connectivité permet également la gestion du « cycle de vie de l'objet », c'est-à-dire l'authentification et l'enregistrement sur le réseau, la mise en service, la mise à jour et la suppression de l'objet du réseau [10].

8. Conclusion

L'IoT comme le permet l'évolution de internet actuel notre mode de vie et les objets intelligents se sont considérablement améliorés Le milieu environnement interagit les uns avec les autres. Dans ce chapitre, nous avons défini L'IOT et expliqué les concepts qui composent l'internet des objets L'avenir de plusieurs domaines.

Chapitre 02 :Sécurité des données dans IOT

1. Introduction

La sécurité des informations essentielles sur IoT devrait s'intégrer dans différentes fonctionnalités telles que l'identification, la confidentialité et la confidentialité des données, etc. Ainsi, avec le développement rapide et un mélange d'appareils hétérogènes, il formule une infrastructure IoT à très grande échelle. Il est donc prévu que IoT soit menacé par sa technologie polyvalente et ses capacités futures. Les menaces de sécurité pour l'IoT telles que le déni de service, la force brute, les attaques de l'homme du milieu et de nombreuses autres attaques sont envisagées dans le réseau interconnecté. Ces attaques se produisent en raison d'un mot de passe faible, de l'absence de cryptage, de la fuite d'informations personnelles, etc., de sorte que le stockage de ces données confidentielles sur le cloud est assez alarmant. Si ces attaques de sécurité ne sont pas résolues à un certain niveau de sécurité, ces services de sécurité faibles peuvent être nocifs pour le marché de IoT. Cela implique non seulement de tels problèmes de sécurité, mais également des problèmes de contrôle d'accès, d'authentification de divers réseaux et des problèmes de stockage d'informations. Ce problème nécessite une infrastructure de sécurité bien définie qui puisse résoudre ces problèmes et réduire les défis de sécurité. [12]

2. Qu'est-ce que la sécurité des données ?

La sécurité des données est l'ensemble des moyens mis en œuvre pour empêcher la corruption des données. Elle comprend l'utilisation de systèmes, processus et procédures qui rendent les données inaccessibles aux individus susceptibles de les utiliser de manière nuisible ou non intentionnelle. Les failles de sécurité relatives aux données peuvent être mineures et faciles à réparer, ou majeures et causer des dommages importants. La sécurité des données concerne les particuliers comme les entreprises. En ce qui concerne les particuliers, les failles peuvent entraîner des violations telles que l'usurpation d'identité ou le vol d'informations personnelles au sujet, par exemple, d'une carte de crédit. Au niveau des entreprises, les types de violations potentielles sont nombreux. Parmi les exemples, on trouve des cas de ransomwares, où les hackers exigent une contrepartie financière, et de malwares ordinaires, où les hackers ont pour but de perturber les activités.

Figure 5 : Sécurité des données

Le défi que rencontre aujourd'hui la plupart des entreprises est la fragmentation des données à travers plusieurs systèmes et plateformes. La migration massive vers le cloud et l'utilisation d'applications SaaS (Le Software as a Service) présentent d'énormes avantages en

termes d'efficacité et de coûts, mais elles impliquent également de confier le contrôle de la sécurité à un fournisseur tiers. L'hacker dispose donc de multiples points d'entrée et une gestion superficielle des données confidentielles, même dans un scénario apparemment anodin, peut mettre en danger les données de l'entreprise et de ses clients. [13]

3. Types des données dans IOT

Avec les premières années d'analyse et de développement des projets et des technologies liées à l'Internet des Objets, il est possible de résumer les données associées aux objets connectés en 4 types de données. La démarche est importante, car elle est un guide pour le déploiement des solutions de Big Data associées à l'IoT. [14]

3.1. Les données d'état

Ce sont les données logiquement les plus répandues, car elles sont naturellement associées à l'objet connecté. Elles permettent de mettre en place une base de référence et serviront de plus en plus comme matière première pour alimenter les moteurs d'algorithmes des solutions de Big Data, et réaliser du prévisionnel sur le long terme. [14]

3.2. Les données de localisation

Extension logique du GPS, ces données se complètent : le GPS fonctionne bien en déplacement, à l'extérieur, mal sur le statique, sur des déplacements courts et surtout en intérieur. Le potentiel est énorme, certes dans la chaine logistique qui devrait être la première à l'industrialiser, mais également avec un énorme marché grand public, celui de la localisation d'un objet ou d'une personne. Des fonctionnalités qui demandent à bénéficier d'un traitement en temps réel. [14]

3.3. Les données personnalisées

Les acteurs du marché sont très prudents dans ce domaine : ils distinguent les données anonymes sur les usages et les préférences individuelles aux données personnelles associées à la vie privée. En fait, se profile derrière ces données une notion essentielle, source de scepticisme de la part des utilisateurs, l'automatisation. Toute la difficulté est de pouvoir associer des règles à des usages en passant de la moyenne aux pratiques de l'individu, sans heurter le respect de la vie privée [14]

4. Principaux concepts de base en sécurité dans l'Internet des Objets

4.1. Confidentialité

La protection contre la divulgation des flux de données et l'analyse du trafic par des entités non autorisées sont fournies par le service de confidentialité. Le mécanisme de sécurité le plus adapté afin d'assurer ce service de sécurité est le chiffrement des données. Ce dernier peut être réalisé avec un système soit asymétrique (à clé publique), soit symétrique (à clé secrète). La connaissance de la clé secrète permettant le chiffrement et le déchiffrement est impliquée dans le système de chiffrement symétrique. Cependant, concernant le système de chiffrement asymétrique, la connaissance par toutes les entités de la clé publique de chiffrement n'implique pas la connaissance de la clé privée correspondante. L'existence d'un mécanisme de gestion de clés est, en plus des mécanismes de chiffrement, nécessaire à l'échange desdites clés entre les entités communicantes [15].

4.2. Intégrité

Deux grandes parties sont englobées dans l'intégrité, qui est un service de sécurité, dans le contexte de l'Internet des Objets : l'intégrité des données et l'intégrité des objets. Le fait que les données échangées dans un environnement IoT n'aient pas été détruites ou modifiées lors de leur acheminement d'une manière non autorisée, est assuré par l'intégrité des données. Celle-ci est nécessaire pour s'assurer que les commandes reçues par les objets et les informations collectées soient légitimes, afin de fournir ainsi un service fiable. Deux processus sont impliqués par la vérification de l'intégrité des données : l'un dans l'émetteur et l'autre dans le récepteur. Des informations de contrôle (valeur de contrôle cryptographique comme le hachage ou code de contrôle par bloc tel que le BCC) sont ajoutées par l'entité émettrice en fonction des données envoyées. Les mêmes informations de contrôle sont générées par l'entité réceptrice, et ce, en se basant sur les données reçues et en les comparant à celles-ci afin de déterminer si elles ont été modifiées durant l'acheminement dans l'environnement IoT [15]. Le type d'intégrité qui concerne les objets est le deuxième dans le contexte de l'IoT. Les objets dans l'IoT peuvent être attaqués physiquement en étant déployés dans des environnements non fiables, le but étant de, par exemple, modifier le code d'exécution en cours sur ces objets, d'où la nécessité de l'intégrité des objets. La détection et l'empêchement des modifications apportées à la configuration des objets et au système d'exploitation sont permises par ce deuxième service d'intégrité, qui est à assurer dans l'Internet des Objets. L'élimination et le verrouillage du périphérique non conforme sont également permis par l'intégrité des Objets. Une empreinte numérique (digital fingerprit) dudit objet est utilisée afin de mettre en place ce type d'intégrité, et ce, pour comparer les données devant exister sur l'objet et les données qui y existent. [16]

4.3. Disponibilité

La disponibilité concerne la possibilité pour une entité autorisée, sur demande, d'accéder à des ressources et de les utiliser après une authentification et un contrôle d'accès. Un service qui est, suite à une attaque de type DoS (Denial of Service) à titre d'exemple, non disponible, est un service pouvant être compromis à tout moment, donc non sécurisé. De ce fait, la disponibilité est un service de sécurité [17]. Afin de fournir un environnement pleinement opérationnel en plus d'être connecté à Internet, la disponibilité dans l'Internet des Objets est essentielle. D'une part, ce service assure la disponibilité du service IoT offert aux utilisateurs, et d'autre part, il permet de collecter des données sans interruption en intégrant la

disponibilité des dispositifs (i.e., objets, passerelles). La configuration de l'environnement IoT détermine la disponibilité du service IoT. Il est donc nécessaire de se protéger contre les attaques de type déni de service (DoS; DDOS : Distributed DoS), et de choisir de manière appropriée les protocoles d'administration et de gestion. La disponibilité, de façon continue, des services offerts dans l'IoT est impérative, la criticité de quelques-uns de ces services devant être prise en compte. La disponibilité permanente des services critiques dans l'IoT, tels que certaines applications dans le domaine de l'e-santé, 24 heures sur 24 durant les 365 jours de l'année, est requise [16]

4.4. Identification et Authentification

L'identification, dont le principe repose sur l'utilisation d'un identifiant attribué de manière individuelle à un utilisateur, s'agit de l'établissement de l'identité de l'utilisateur d'un service IoT. A l'identification succède l'authentification qui permet à l'utilisateur d'apporter la preuve de son identité. Un code secret ou un authentifiant est utilisé par l'utilisateur que lui seul connait. Or, c'est le contrôle d'accès qui donne un droit d'accès si l'authentification a été réussie, ce n'est donc pas cette dernière qui assure ce privilège [15]. Des avantages peuvent être fournis à l'environnement IoT grâce aux mécanismes d'identification et d'authentification. De ce fait, à travers ces deux derniers, cet environnement intègre des dispositifs robustes et capables d'éviter les violations et de réduire les risques d'intrusion [18].

4.5. Non-répudiation

Le fait que la participation aux échanges ne soit pas niée par une extrémité de communication est permis par le service de sécurité de type non répudiation, qui peut être présenté sous diverses formes. La non répudiation avec preuve de l'origine en est la première forme, dans laquelle la preuve de l'origine des données est reçue par le destinataire. Un signataire numérique peut constituer cette preuve, et ce, par l'utilisation du chiffrement asymétrique appliqué au résultat de hachage des données échangées. La non répudiation avec preuve de la remise des données est la deuxième forme, qui s'agit de la réception de cette preuve par l'émetteur sous forme d'un accusé de réception, à titre d'exemple [15]. Dans l'Internet des Objets, le service de sécurité de type non répudiation est nécessaire pour fournir une preuve d'envoi par les utilisateurs des services IoT d'ordre d'exécution, mais aussi une preuve d'envoi des données par les objets. Ceci permet de sauvegarder et de suivre, dans des fichiers de traces, tous les évènements ayant eu lieu dans un environnement IoT[16].

4.6. Contrôle d'accès

L'utilisation non autorisée d'une ressource IoT est permise par le contrôle d'accès. Conformément à une politique de sécurité, une liste des entités dont l'accès à une ressource est autorisé ainsi que leur niveau d'accès sont définis afin de réaliser ce contrôle. L'offre de ce service vise à la mise en place de différents types d'accès aux ressources (écriture, lecture, modification, exécution d'une tâche ou suppression d'une information). Le contrôle d'accès, à travers des bases d'informations conservées par la ressource ou par des centres d'autorisation, est basé sur un ou plusieurs éléments (une matrice de structure répartie ou hiérarchique, une liste de contrôle d'accès, etc). Des informations d'authentification (étiquettes de sécurité, mots de passe, etc) sont comprises dans ces bases d'informations [15]. Deux types d'entités, devant être authentifiés mutuellement, sont importants dans le cadre du contrôle d'accès dans l'IoT : les collecteurs de données (les objets IoT) qui reçoivent les commandes ou envoient les données ; et les détenteurs de données (les utilisateurs des services IoT) [16].

5. Pourquoi la sécurité des données est-elle importante ?

La sécurité des données consiste à protéger les informations numériques contre tout accès non autorisé, toute corruption ou tout vol tout au long de leur cycle de vie. Le concept couvre tous les aspects de la sécurité de l'information, depuis la sécurité physique du matériel et des appareils de stockage jusqu'aux contrôles des administrateurs et des accès, en passant par la sécurité logicielle des applications. Les politiques et les procédures organisationnelles en font également partie.

Lorsqu'elles sont correctement exécutées, de solides stratégies de sécurité des données protègent les actifs informationnels des organisations contre les cybercriminels, mais aussi contre les menaces internes et les erreurs humaines, qui sont les principales causes de violation des données à l'heure actuelle. La sécurité des données implique le déploiement d'outils et de technologies qui donnent à l'organisation une meilleure visibilité sur l'endroit où sont stockées ses données critiques et sur la manière dont elles sont utilisées. Ces outils doivent idéalement offrir des protections comme le chiffrement, le masquage des données et la rédaction de fichiers sensibles. En outre, ils doivent proposer l'automatisation des rapports afin de simplifier les audits et de respecter les exigences réglementaires. [19]

6. Quelles menaces de sécurité pour l'IoT ?

L'IoT est un secteur en pleine croissance. De plus en plus de cas d'usages se créent, et des données de tous types sont collectées, analysées, corrélées et diffusées. Suivant les cas d'usages, les données et la valeur qu'elles procurent peuvent attirer des attaques.

Il convient donc de mener une réflexion adaptée quant aux menaces et risques de sécurité inhérents au développement des dispositifs IoT. Sans oublier que la prolifération des IoT augmente aussi la surface d'attaque possible…. [20]

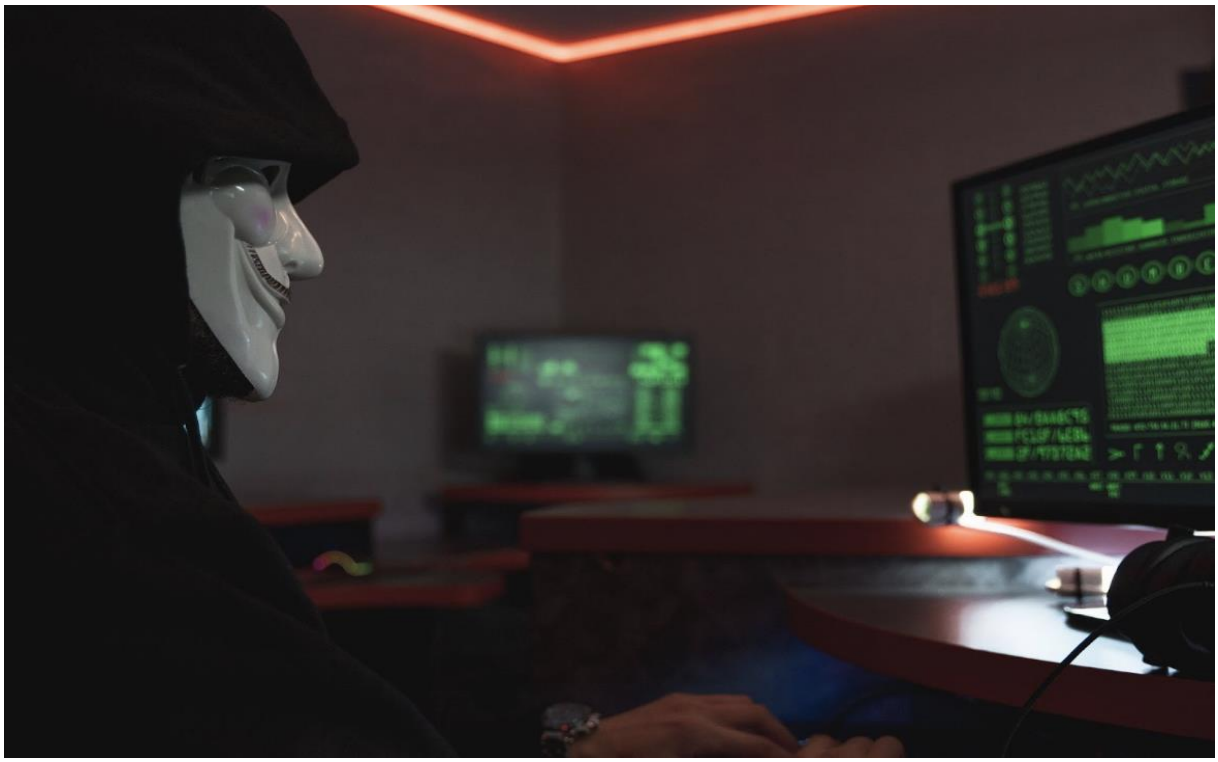

Figure 6 :Menaces

La croissance du nombre d'objets connectés fait de l'IoT une cible potentielle de différentes attaques, d'où l'importance de s'y préparer au plus tôt.

Les plateformes de données sont un des composants de la chaîne de valeur qui présente un risque. Elles consolident et centralisent toutes les données et sont de ce fait au cœur même des analyses qui seront menées. Elles sont susceptibles d'être attaquées par différentes méthodes :

6.1. Les attaques par dénis de service

En 2020, plus de 10 millions d'attaques de ce type ont été enregistrées en entreprise dans le monde, selon une enquête de Netscout. La communication avec des dispositifs comme des ordinateurs et des objets connectés est bloquée et la récolte des données ou l'envoi des

paramètres est retardée voire impossible. Cette attaque menace la disponibilité permanente des interfaces et des données récoltées, pourtant essentielles dans tout projet IoT [19].

6.2. La création de porte dérobée à cause des API non sécurisées

Les API permettent entre autre de connecter des services entre eux et ainsi de faire transiter les données. Elles peuvent néanmoins laisser place à des portes dérobées ou backdoor si elles sont défaillantes. A travers ce backdoor, des données peuvent être détournées, dans certains cas sans même que l'utilisateur ne le sache. La fuite de données non sensibles à cause des API non sécurisées peut paraître anodine, mais cette fuite est synonyme de prise en main de l'API par l'attaquant. Cette API, qui vous informe de la température de votre salle de réunion, peut être utilisée pour vous localiser par exemple. [20]

6.3. Intrusion

Une intrusion peut être considérée comme l'ensemble d'actions qui ont pour but de compromettre l'intégrité la confidentialité ou la disponibilité d'une ressource. Ces actions de franchissement d'un accès non-autoris ou de manipulation interdite d'une ressource, peuvent être menées par un individu externe n'ayant aucun privilège sur les ressources d'un système ou par un individu interne qui outrepasse ses privilèges [21].

Accès non autorisé :

- Utilisation de mots de passe par défaut ou faibles, permettant aux attaquants d'accéder facilement aux dispositifs.
- Mauvaise gestion des autorisations, permettant à des utilisateurs non autorisés d'accéder à des fonctions critiques.

7. Quelles sont les mécanismes de sécurité ?

De manière générale, les mécanismes de sécurité visent à protéger l'accès aux biens (c'est-à-dire aux données et ressources) d'un système contre les menaces de sécurité. Ainsi, l'utilisation des mécanismes de sécurité permet de mettre en œuvre les services de sécurité afin d'empêcher la divulgation et/ou la modification non-autorisée des données et/ou l'accès non-autorisé aux ressources [22].

7.1 Détection d'intrusion

La détection d'intrusion est un ensemble de techniques et de méthodes employées dans l'analyse des informations collectées par les mécanismes d'audit de sécurité pour détecter

toute activité suspecte au niveau du réseau et ses hôtes[20].D'autre facon La détection d'intrusion est le processus de surveillance de votre trafic réseau et d'analyse de celui-ci pour détecter des signes d'éventuelles intrusions, telles que des tentatives d'exploitation et des incidents pouvant constituer des menaces imminentes pour votre réseau. Pour sa part, la prévention des intrusions consiste à effectuer une détection des intrusions puis à arrêter les incidents détectés, généralement en supprimant des paquets ou en mettant fin à des sessions. Ces mesures de sécurité sont disponibles sous forme de systèmes de détection d'intrusion (IDS) et de systèmes de prévention d'intrusion (IPS), qui font partie des mesures de sécurité du réseau prises pour détecter et arrêter les incidents potentiels et sont des fonctionnalités incluses dans les pare-feu nouvelle génération (NGFW) [23].

7.2 Les fonctions de hachage

Les fonctions de hachage sont des fonctions qui prennent une entrée de longueur arbitraire et la compressent en un résultat d'une longueur fixe, que l'on nomme « haché » ou « condensé ». Suivant la fonction de hachage utilisée, la taille de la sortie produite diffère. Toutefois cette taille est fixe pour une fonction de hachage donnée (quel que soit l'entrée donnée). De la même façon, selon la fonction de hachage utilisée, pour une valeur d'entrée donnée, la valeur de sortie produite changera, mais pour une fonction de hachage donnée et pour une valeur d'entrée donnée, c'est toujours le même haché qui sera produit. Les fonctions de hachage sont largement utilisées dans la conception des protocoles cryptographiques, aussi bien que ceux utilisant de la cryptographie symétrique qu'asymétrique. Ainsi, en cryptographie, les fonctions de hachage sont souvent utilisées pour l'authentification, les signatures numériques et les codes d'authentification de messages [22].

7.3 Les mécanismes de chiffrement

7.3.1 Chiffrement symétrique

Afin d'échanger des données de façon sécurisée, avec un algorithme de chiffrement symétrique, l'émetteur et le récepteur (ou les récepteurs) doivent utiliser un secret partagé (c'est-à-dire une clé). La notion de symétrie provient du fait que c'est la même clé, qualifiée de secrète, que les entités communicantes utilisent à la fois pour chiffrer (opération de transformation du message clair en message chiffré) et pour déchiffrer (opération de transformation du message chiffré en message clair). La clé doit rester secrète pour les entités du système n'ayant pas les droits (par contre, elle peut être partagée au sein d'un groupe si

cela est nécessaire et elle devient une clé de groupe toutefois, une fois la clé de groupe partagée, il est difficile d'exclure un membre du groupe car il faut repartager la clé) [24, 25].

7.3.2 Le chiffrement asymétrique

Pour réaliser le chiffrement asymétrique, chaque entité communicante doit posséder deux clés cryptographiques : une clé privée (connue seulement par l'entité qui la possède) et une clé publique (accessible par tous). Dans un tel schéma, une tierce partie de confiance peut agir comme une autorité de certification CA (« Certificate Authority ») soit pour signer les clés publiques afin de prouver leur authenticité, soit pour générer les paires de clés (privée/publique) pour chaque entité et pour fournir les clés publiques à tous. Si l'on se place dans ce dernier cas, lorsqu'une entité désire envoyer un message sécurisé à une autre, elle chiffre son message avec la clé publique du destinataire, clé récupérée auprès de la CA. L'entité qui reçoit le message le déchiffre en utilisant sa propre clé privée [26, 27].

7.4 Les crypto systèmes à clé publique

Les crypto systèmes à clé publique sont complémentaires de ceux à clés symétriques qui permettent essentiellement d'assurer le chiffrement efficace. Par exemple, ils permettent d'assurer le processus d'authentification afin d'initier la mise en place de clés de session (c'est-à-dire des clés symétriques) pour protéger le canal de communication. Ainsi, nous allons présenter brièvement le fonctionnement de RSA, premier crypto système de ce type, pour ensuite nous attarder sur la cryptographie basée sur les courbes elliptiques que nous avons largement utilisée car elle est particulièrement adaptée aux environnements contraints comme ceux qui sont étudiés dans cette thèse. [22]

8. Système de détection d'intrusion

8.1. Définition

IDS signifie "Intrusion Détection System". Ce système est mis en place afin de surveiller l'activité sur un réseau ou une machine donnée. Le but est de repérer toute tentative d'intrusion est de réagir selon les besoins de l'entreprise. Ce sont des composants matériels ou logiciels utilisés afin de détecter une activité suspectes sur l'environnement cible (réseau, ordinateur, serveur, etc.). Cette détection se base soit sur le comportement de la machine soit sur des signatures fournies par l'éditeur de la solution et qui doivent être mises à jour régulièrement, on parle d'une base de connaissance. [28]

8.2. Les méthodes de détection d'intrusion

L'idée de base de la détection d'intrusion part de l'hypothèse que les comportements d'une activité intrusive sont plus ou moins différents de ceux des activités normales et sont donc détectables [29]. Plusieurs approches de détection d'intrusion ont été proposées dans la littérature. Généralement ces approches sont classées en quatre catégories : la détection d'anomalie, la détection basée sur les signatures et la détection basée sur des spécifications et l'analyse des protocoles avec Etat. Des solutions combinant plusieurs méthodes de détection sont appelées détections hybrides.

8.2.1 La détection d'anomalie (anomaly detection)

Le principe de base de la détection d'anomalie est de modéliser durant une première période, dite phase d'apprentissage, le comportement « normal » du système en définissant une ligne de conduite (dite Baseline ou profil). Ensuite, en une seconde phase, période de détection, il est considéré comme suspect tout comportement inhabituel c'est-à-dire les déviations significatives par rapport au modèle de comportement « normal ». [30] propose un modèle typique de détection d'anomalie illustré par la figure 2.

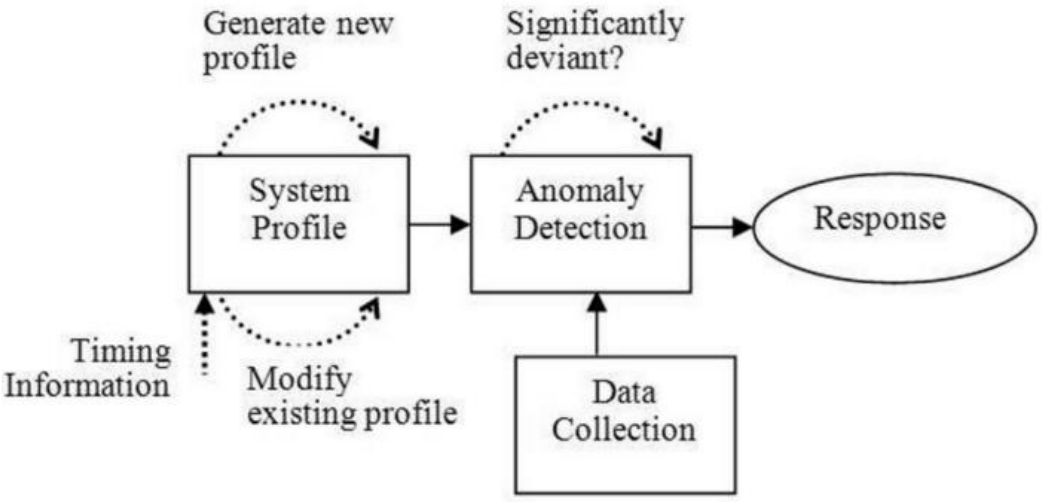

Figure 7 : Système typique de détection d'anomalie proposé dans [30]

Le système illustré ici est constitué de quatre composantes à savoir la collecte de données (Data Collection), le profil normal du système (System Profile), la détection d'anomalie (Anomaly Detection) et la réaction (response). Les activités normales du système ou les données relatives au trafic sont enregistrées par la composante de collection de données. Des techniques de modélisation spécifiques sont utilisées pour créer les profils normaux du

système. La composante de détection d'anomalie détermine combien les activités en cours s'écartent des profils normaux du système et à quel seuil d'écart ces activités devraient être signalées comme anormales. Enfin, la composante de réaction signale l'intrusion et éventuellement les informations de timing correspondantes. L'avantage principal de la détection d'anomalie est sa capacité à trouver de nouvelles attaques. Ce qui constituera la plus grande limitation de la détection d'abus. Cependant, en raison des hypothèses sous-jacentes aux mécanismes de détection des anomalies, leurs taux de fausses alarmes sont en général très élevés. De nombreuses techniques de détection anomalie ont été proposées dans la littérature. Ces modèles vont des modèles statistiques avancés à des modèles d'intelligence artificielle et des modèles biologiques basés sur les systèmes immunitaires humains. Bien qu'il soit difficile de classer ces techniques, nous pouvons les diviser en quatre catégories sur la base des enquêtes précédentes sur les systèmes de détection d'anomalie [30, 31, 32, 33, 34, 35, 36, 37]. Il s'agit notamment de modèles statistiques avancés, de modèles fondés sur des règles, de modèles d'apprentissage, de modèles biologiques et de modèles fondés sur des techniques de traitement du signal. [38]

8.2.2 La détection basée (signature-based detection)

La détection basée sur les signatures est aussi connue sous le nom de détection d'abus (misuse detection). Cette approche vise à coder les connaissances sur les modèles de flux de données qui correspondent à des procédures intrusives sous la forme de signatures spécifiques. Ainsi, une signature est un modèle qui correspond à une menace spécifique étudiée. Les intrusions sont détectées en faisant un matching entre les évènements du système et les signatures. Les correspondances trouvées sont considérées comme des intrusions. Pour illustrer la détection basée sur les signatures nous avons conçu la figure 3. Elle est inspirée de l'illustration de la figure 2 dans [30].

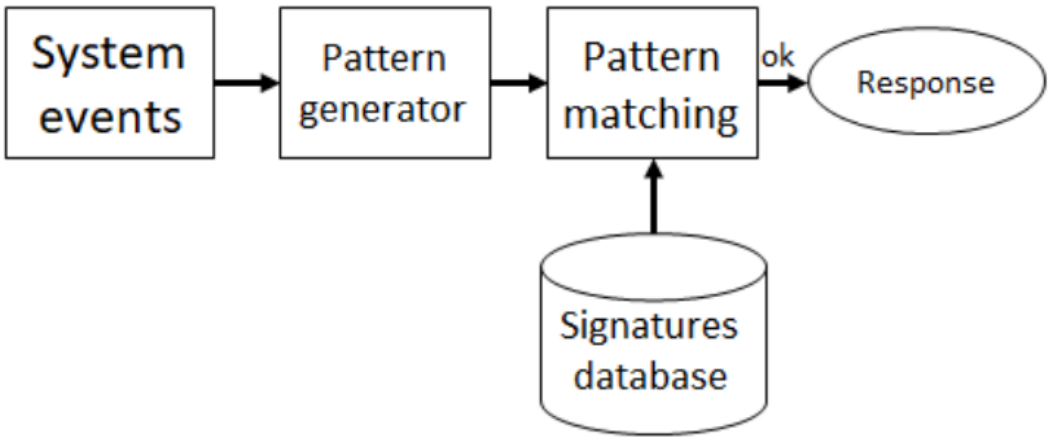

Figure 8 : – Système typique de détection basée sur les signatures[38]

Ce modèle comprend cinq composantes : System events qui collecte les évènements courants du système, Pattern generator qui génère les signatures des évènements du système à partir des évènements collectés, Pattern matching qui compare les signatures générées à partir des évènements courants avec celles des attaques connues, Signatures database qui est la base de données des signatures connues. La dernière composante, response, est la réaction effectuée quand un matching est positif. Plusieurs catégories de techniques sont couramment utilisées pour mettre en œuvre la détection basée sur les signatures, à savoir le pattern matching, les techniques basées sur des règles, les techniques basées sur des états et le data mining. Nous discutons de ces techniques dans la section des approches innovatrices et prospectives. [38]

8.2.3 La Détection de spécification (specification-based detection)

Dans les approches de détection basées sur des spécifications, les experts en sécurité prédéfinissent les comportements autorisés du système et les événements qui ne correspondent pas aux spécifications sont étiquetés comme des attaques. Au lieu d'apprendre les profils normaux du système, ici la détection est basée sur la connaissance des experts. Cette approche, en théorie, permet de détecter des attaques invisibles qui pourraient être menées. Cependant, spécifier le comportement d'un grand nombre de programmes s'exécutant dans des environnements d'exploitation réels est une tâche excessivement difficile [38].

8.2.4 L'analyse de protocoles avec Etat (Stateful protocol analysis)

L'analyse de protocole avec état consiste à comparer des profils prédéfinis de définitions généralement acceptées de l'activité de protocole bénigne pour chaque état de protocole par rapport aux événements observés afin d'identifier les déviations. Contrairement à la détection

fondée sur les anomalies, qui utilise des profils propres à l'hôte ou au réseau, la détection par état s'appuie sur des profils universels développés par les fournisseurs qui précisent comment des protocoles particuliers devraient et ne devraient pas être utilisés. L'état "stateful" dans Stateful protocol analysis signifie que l'IDS est capable de de comprendre et de suivre l'état du réseau, des protocoles de transport et d'application qui ont une notion de l'État [38].

8.3 Classification de IDS

8.3.1 Classification basée sur les méthodes de détection

Du point de vue des méthodes de détection, les techniques de détection d'intrusion sont généralement divisées en techniques de détection d'abus et en techniques de détection d'anomalies

- **Basé sur la technologie de détection des abus**

La technologie de détection des abus [39] est basée sur le principe de la correspondance de motifs, collecte les caractéristiques du comportement d'attaque et établit une base de données de signatures pour cela. Lorsque le comportement de l'utilisateur surveillé correspond aux enregistrements de la base de données de signatures, le système juge le comportement comme une intrusion. La technologie de détection des abus peut réduire le taux de faux positifs. Cependant, le taux de faux négatifs augmentera également. Une fois que les caractéristiques de l'attaque changent, la technologie de détection des abus deviendra incompétente. Les techniques de détection des abus existantes sont généralement divisées en méthodes de détection des abus basées sur des systèmes experts [40], des méthodes de détection des abus basées sur l'analyse de transition d'état [41], des méthodes de détection des abus basées sur la surveillance du clavier [42] et des méthodes basées sur la probabilité conditionnelle.

- **Basé sur la technologie de détection des anomalies**

Les techniques de détection des anomalies [39] sont basées sur des principes d'analyse statistique. Tout d'abord, nous déterminons les caractéristiques du comportement normal et les décrivons avec des méthodes quantitatives. Lorsque le comportement de l'utilisateur s'écarte de l'opération normale, il est défini comme un comportement agressif. L'efficacité des techniques de détection des anomalies dépend en grande partie de l'exhaustivité des caractéristiques typiques de l'utilisateur et de la fréquence de détection. Les attaques inconnues peuvent être détectées efficacement car chaque épisode n'a pas besoin d'être défini. En même temps, le système peut également s'adapter aux changements de comportement de

l'utilisateur grâce à l'auto-optimisation et à l'ajustement. Cependant, avec l'amélioration continue du modèle, la technologie de détection des anomalies consommera plus de ressources système, et le comportement d'attaque à ce stade devient de plus en plus intelligent, ce qui affaiblit progressivement la capacité de détecter les attaques inconnues. Les techniques de détection des anomalies existantes sont généralement divisées en techniques de détection des anomalies basées sur un réseau neuronal [43], techniques de détection des anomalies basées sur la prédiction de motifs [44] et techniques de détection des anomalies basées sur l'exploration de données [45].

8.3.2 Classification basée sur la source de données

Du point de vue des sources de données, les systèmes de détection d'intrusion peuvent généralement être divisés en systèmes de détection d'intrusion basés sur l'hôte (Host Intrusion Détection System, HIDS) et en systèmes de détection d'intrusion basés sur le réseau (Network Intrusion Détection System, NIDS).

- **Détection d'intrusion basée sur l'hôte**

Les attaques contre les systèmes hôtes ou serveurs sont la principale préoccupation de la HIDS (Host Intrusion Detection System) [46, 47]. Les personnes travaillant avec les HIDS utilisent deux techniques principales, à savoir les techniques de détection des anomalies et les techniques de détection des abus. En utilisant la technologie de détection des abus et la technologie de détection des anomalies, l'auteur [47] a proposé une méthode pour surveiller les données collectées par l'hôte. Ce système utilisait l'analyse des fichiers journaux et la technologie des réseaux neuronaux BP pour surveiller les données collectées par l'hôte. Par conséquent, il peut aider à améliorer le taux de détection et la précision de la recherche. [48]

- **Détection d'intrusion basée sur le réseau**

Lorsque la carte réseau est en mode promiscuité, le NIDS (Network Intrusion Detection System) [48, 49] peut surveiller en temps réel le service de communication sur tout le segment du réseau. Peu importe si vous utilisez la détection d'intrusion basée sur l'hôte ou la détection d'intrusion basée sur le réseau. Ils ont tous quelques problèmes, donc ils continuent de s'améliorer. Ils ont trouvé une meilleure façon de détecter les intrusions réseau. Tout d'abord, ils placent un nœud serveur dans une partie spécifique du réseau, puis ils placent le système de détection d'intrusion sur le serveur avant que chaque paquet de données n'atteigne

l'hôte de destination. L'hôte de destination ne peut pas recevoir de paquets de données provenant de l'extérieur du réseau. Même si certains paquets de données lui sont envoyés directement, ils doivent être envoyés au serveur pour être vérifiés avant de pouvoir continuer. Si le serveur trouve que le paquet de données est une intrusion, il le jette immédiatement. [48]

8.3.3 Classification basée sur l'architecture

Du point de vue architectural, les systèmes de détection d'intrusion peuvent être divisés en systèmes centralisés et distribués. Les systèmes de détection d'intrusion centralisés ont leur moteur d'analyse et leur centre de contrôle dans un seul système et ne peuvent pas fonctionner à distance. Cette architecture est simple, ne compromet pas la confidentialité en raison de la communication, et n'affecte pas la bande passante du réseau. Cependant, cette méthode présente une scalabilité et une confirmabilité médiocre. En revanche, le moteur d'analyse et le système de détection d'intrusion distribué sont deux systèmes qui peuvent être exploités à distance via le réseau. À l'heure actuelle, la plupart des systèmes de détection d'intrusion sont distribués. Cette architecture est hautement évolutive et sécurisée, mais elle est également coûteuse à entretenir. [48]

8.3.4 Classification basée sur le mode de travail

Le système de détection d'intrusion peut être divisé en détection en ligne et détection hors ligne en fonction du mode de fonctionnement. La détection en ligne peut surveiller la génération de données et l'analyser en temps réel. Bien que cette méthode puisse protéger le système en temps réel, il n'est pas facile de garantir des performances en temps réel lorsque le système est de grande envergure. En revanche, la détection hors ligne analyse le comportement d'intrusion après qu'il se produit. Cette méthode peut gérer de nombreux événements mais ne peut pas fournir rapidement des mesures de protection pour le système. [48]

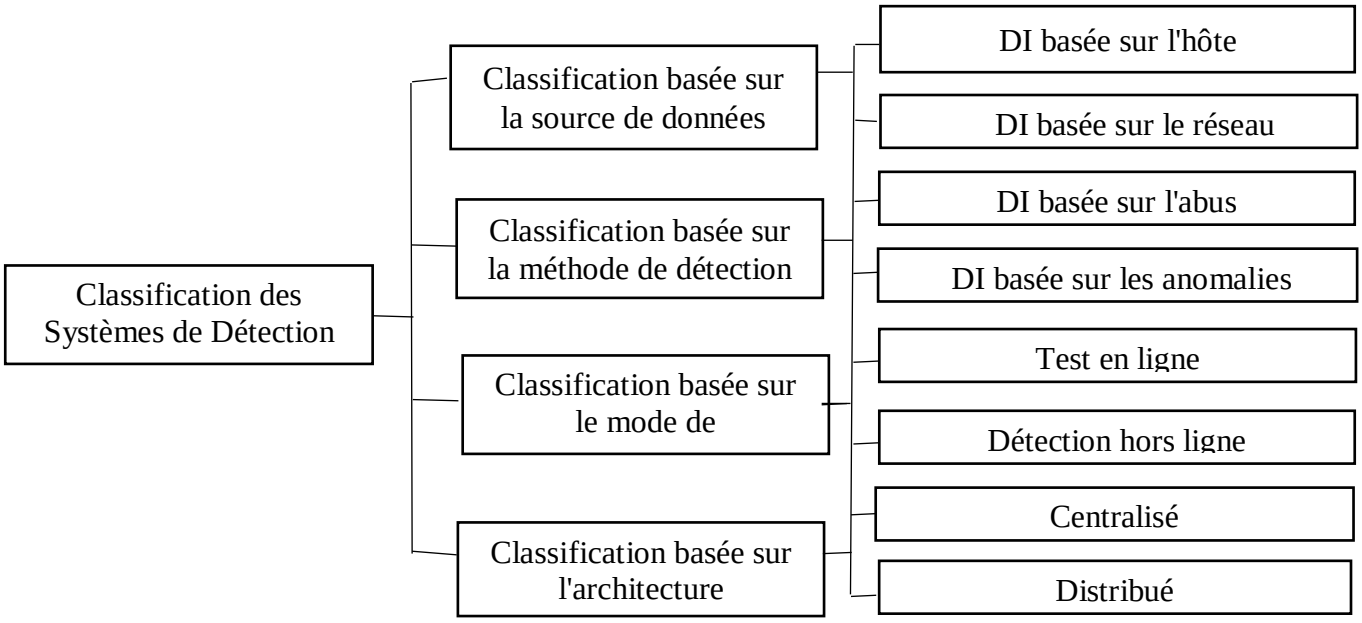

Figure 9 : classification des systèmes de détection d'intrusion

9. Conclusion

Dans ce chapitre nous avons présenté la sécurité des données et les déférents types des données dans IOT, nous avons parlé aussi sur les principaux concepts de base en sécurité dans l'Internet des objets, les menaces de sécurité pour l'IoT et les défenses possibles, En fin nous avons parlé sur l'Intrusion Détection System (IDS) et les méthodes de détection d'intrusion et ses classifications.

Chapitre 03 : Approche de détection d'intrusion basé sur le blockchain et IA

1. Introduction

Dans ce chapitre, nous aborderons la définition de la blockchain, et les avantage de de cette nouvelle technologie, et aussi parle sur les domaines d'application de blockchain. Dans ce chapitre aussi, nous examinerons également certaines informations liées à l'intelligence artificielle, y compris ses avantages et ses types. Après nous citons la méthode de détection intrusion avec Blockchain et IA

2. Blockchain

2.1 Définition

Nous présentons ci-dessous quelques définitions qui permettent de mieux comprendre ce qu'est la blockchain selon plusieurs points de vue :

- **Basique** : la blockchain s'agit d'un logiciel qui stocke et transfère des données via internet, de façon transparente et sécurisée, et sans organe central de contrôle.
- **Littéral :** une blockchain désigne une chaine de blocs dans lesquels sont stockés les informations de toute nature.
- **Généraliste** : une blockchain est une technologie qui permet d'effectuer des transactions, grâce à un mécanisme de consensus collectif couplé avec l'utilisation d'un grand livre de compte public, décentralise et partagé, établit la confiance, la responsabilité et la transparence tout en rationalisant les processus d'affaires.
- **Technique** : une blockchain est une nouvelle technologie de base de données. Cette base de données transactionnelle distribuée est comparable à un registre dans lequel chaque nouvelle transaction est écrite à la suite des autres, sans avoir la possibilité de la modification ou la suppression. Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie entre les membres ou participants (nœuds).

Pour résumer la blockchain est une base de données transactionnelle distribuée, elle permet de stockager et transmettre les informations via Internet, de façon transparente, sécurisée et autonome, tout cela sans organe central de contrôle [50].

Figure 10 : Block chain

2.2 Grands principes de la blockchain

Les principes sur lesquels est fondée la blockchain sont les suivants [50]:

- La blockchain est une base de données, qui est répartie entre tous les nœuds.
- La d´décentralisation et la désintermédiation : il n'existe aucune autorité centrale pour contrôler la blockchain donc il n'y a pas de tiers de confiance.
- Le consensus : le fruit d'un consensus distribué c'est d'effectuer une transaction.
- L'immutabilité : Une fois qu'une transaction est enregistrée sur la blockchain et que la blockchain a été mise à jour, cette transaction ne peut pas être modifiée.
- La confiance partagée et la transparence : la blockchain assure la sécurité et la transparence des données.

Les blockchains les plus connues et utilisées dans le monde sont : Bitcoin et Ethereum, mais la blockchain ne se limite pas à celles-ci car il existe d'autres types [50].
La technologie blockchain change les règles du jeu : moins de centralisation, moins d'autorité et plus de partage [50].

2.3 Domaines d'application de blockchain

Voici quelques domaines d'application de la technologie blockchain [51, 52, 53, 54, 55,56] :

- **Vote** : la blockchain promet un vote s´sécurisé et inviolable dont le résultat, transparent et fiable, est auditable par tous, même si les résultats de votes sont publiquement affichés sur la blockchain l'identité des personnes votant ne peut pas être connue grâce au système de clé publique/clé privée. L'identité est ainsi protégée,

et les questions liées à une élection frauduleuse sont écartées. On peut trouver par exemple dans ce secteur la plate-forme start-up Follow My Vote.

- **Santé** : les données médicales sont souvent stockées numériquement. Les rassembler et les rendre disponibles à tout moment est peut-ˆêtre le plus grand potentiel de la blockchain. Dans certaines circonstances, la technologie peut sauver des vies. Cela peut être expliqué manière éclatante par trois exemples : un registre de dons d'organes, le rappel de m´médicaments contrefaits et des projets de recherche m´médicale.

  Par le passé, les listes d'attente pour les dons d'organes ont été falsifiées à plusieurs reprises. En conséquence, la volonté de la population de donner un organe diminue. La blockchain pourrait empêcher la manipulation à l'avenir.

  Avec l'aide de la technologie blockchain, la qualité des produits pharmaceutiques pourrait également être mieux contrôlée, puisque toute la chaîne de production, de la fabrication aux fluctuations de température et tout le parcours de transport jusqu''a la livraison aux pharmacies, pourrait être surveillée et stockée dans la blockchain. Le résultat : si la chaîne du froid n'est pas respectée, le médicament ne sera pas livré. Quoi qu'il en soit, les sociétés pharmaceutiques pourraient attribuer un code QR à chaque m´médicament que les patients peuvent scanner pour vérifier qu'il est authentique. Falsifier cela ne serait pas impossible, mais cela coûterait beaucoup plus cher qu'auparavant.

  Les projets de recherche pourraient également bénéficier grandement de la technologie de la blockchain : d'une part, ils pourraient partager la puissance de calcul et travailler plus étroitement ensemble, et d'autre part, les patients pourraient rendre leurs données de la blockchain disponibles pour des études au moyen d'une déclaration de consentement.

  Cela prendra du temps parce que la technologie blockchain en est encore au tout début. Les concepts fondamentaux ne peuvent être testés dans la pratique que lorsque les hôpitaux, les cabinets médicaux et autres organisations médicales ont mis en place l'infrastructure nécessaire. Mais c'est aussi son plus grand avantage : aujourd'hui, la nouvelle technologie peut être entièrement conçue pour le bénéfice du patient.

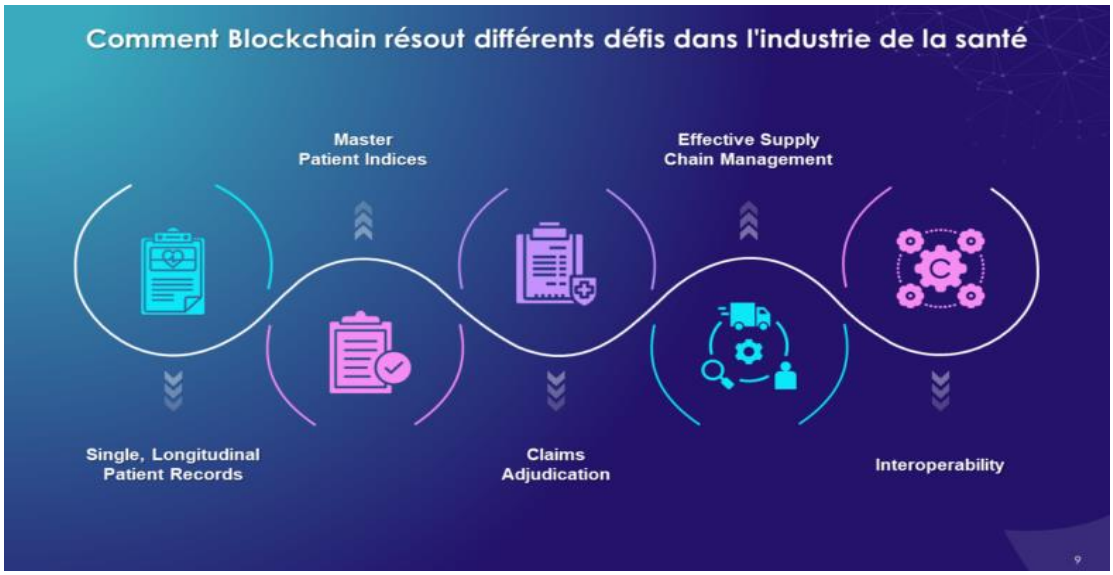

Figure 11 : Applications de la block Chain dans la santé

- **Les assurances** : Les blockchains ont le potentiel de révolutionner le monde de l'assurance.

  Leurs potentiels technologiques permettent de cartographier de nouveaux business models totalement numériques, transparents et sécurisés pour des interactions rapides entre de nombreux acteurs. Avec les blockchains, les assureurs peuvent simplifier et accélérer la tarification et la fourniture de services, déterminer l'authenticité des biens et des documents, et suivre l'historique des activités frauduleuses d'une personne.
- **Commerce** : La blockchain peut améliorer les processus de nombreuses façons. Par exemple, le suivi des marchandises d`es le début de la chaîne d'approvisionnement jusqu'aux points de vente et de service, via cette technologie, nous pouvons prendre les mesures nécessaires en cas de problèmes dans la chaîne.
- **Banque** : Les banques agissent souvent en tant qu'intermédiaires au sein de l'économie mondiale, gérant et coordonnant le système financier grâce à leur comptabilité interne. Comme cela n'est pas visible publiquement, cela force la confiance dans les banques et leur infrastructure souvent obsolète.

  La technologie blockchain a le potentiel de perturber non seulement le marché mondial des changes, mais le secteur bancaire dans son ensemble en désactivant ces intermédiaires et en les remplaçant par un système fiable, illimité et transparent, facilement accessible à tous.

  La blockchain a permis d'effectuer des transactions plus rapides et moins chères, d'améliorer l'accès au capital, de créer plus de sécurité des données, d'appliquer des accords de confiance grâce à des contrats intelligents et de rendre la conformité plus

fluide.

2.4 Avantages et inconvénients de la blockchain

La blockchain comme toutes autres technologies a des avantages ainsi des inconvénients et c'est ce que nous allons voir dans cette section.

2.4.1 Avantages

Parmi les avantages de blockchain on site [57,58] :

- **Des transactions sans intermédiaire** : La blockchain permet des transactions directes entre les participants sans l'intervention d'un tiers. Ces intermédiaires tels que les banques ou les notaires ne sont plus nécessaires.
- **Stabilité** : Les blocs confirmés sont très difficiles à annuler, donc une fois les données enregistrées sur la blockchain, il est extrêmement difficile de les supprimer ou de les modifier. Cela fait de la blockchain une excellente technologie pour stocker des enregistrements financiers ou d'autres données nécessitant une piste d'audit, car chaque changement est suivi et enregistré en permanence dans un grand livre distribué et public.
- **La sécurité** : Comme cette technologie dispose de divers mécanismes de vérification des données, l'altération des informations contenues dans les blockchains devient pratiquement impossible. Pour commencer, chaque fois que vous souhaitez modifier des données dans un bloc, vous devez modifier tous les blocs de cette chaîne.
- **Décentralisation** : Contrairement aux systèmes traditionnels qui reposent sur une autorité centrale, la blockchain fonctionne sur un réseau distribué, éliminant ainsi le besoin d'une tierce partie de confiance.
- **Réduction des frais et des délais** : Les transactions sur la blockchain peuvent être effectuées directement entre les parties concernées, éliminant ainsi les frais et les délais associés aux intermédiaires.
- **Traçabilité accrue** : Chaque transaction sur une blockchain est enregistrée de manière permanente et immuable, ce qui permet de retracer facilement l'historique complet des actifs.
- **Automatisation des processus** : Les contrats intelligents (smart contracts) sur la blockchain permettent d'automatiser l'exécution des accords, ce qui réduit les risques d'erreur et de fraude.

- **Accessibilité mondiale** : La blockchain est accessible à quiconque dispose d'une connexion Internet, ce qui ouvre de nouvelles opportunités commerciales et financières à l'échelle mondiale.
- **Innovation technologique** : La blockchain est une technologie émergente qui stimule l'innovation dans de nombreux secteurs, notamment la finance, la santé, l'immobilier et la logistique.

2.4.2 Inconvénients

Parmi les inconvénients du blockchain on trouve [58,59] :

- **Difficulté de mise en œuvre** : La blockchain étant quelque chose de révolutionnaire, l'un de ses inconvénients est sa difficulté à mettre en œuvre. Comme il s'agit d'une technologie disruptive, il faut du temps pour établir tous les protocoles essentiels à son bon fonctionnement. Les entreprises peuvent donc mettre des années à adopter et à fonctionner uniquement avec ce système.
- **Chômage :** Comme cette technologie vise à éliminer l'intermédiaire dans les transactions, l'une des conséquences possibles sera la perte définitive de celui-ci. Autrement dit, si cette technologie se développe et si elle doit être de plus en plus mise en œuvre, il n'y aura pas besoin d'intermédiaire. Et cela peut signifier son éradication totale (ou presque).

2.5 Type de blockchain

La technologie de la blockchain permet de sécuriser les transactions et échanges d'informations via un réseau sécurisé, utilisée notamment avec les cryptomonnaies. Elle est appliquée dans des réseaux privés avec accès restreint, gérés par des administrateurs. Il existe des blockchains privées et publiques, ainsi que des blockchains de consortium et hybrides. Toutes fonctionnent sur un réseau P2P, chaque nœud ayant une copie du registre partagé, régulièrement mise à jour et vérifiée [60].

2.5.1 Blockchain publique

La blockchain publique est en outre un système de registre distribué et non restrictif qui ne nécessite aucune permission, et toute personne ayant accès peut être autorisée à obtenir les données ou une partie de la blockchain. Ce type de blockchain permet également l'autorisation de vérifier les enregistrements actuels et passés [61][62]. De plus, il est utilisé pour le minage et l'échange de cryptomonnaies. Dans ce segment, les blockchains les plus courantes sont

Bitcoin et Litecoin. Ce système est généralement sécurisé en suivant des règles et des méthodes de sécurité strictes. Cependant, le non-respect des protocoles de sécurité peut le rendre risqué.

2.5.2 Blockchain privée

Ce type de blockchain fonctionne uniquement sur des systèmes et réseaux fermés et est généralement utile aux organisations et entreprises, dont seuls certains membres peuvent être intégrés. Ce type de blockchain dispose de la sécurité, des autorisations, des permissions et de l'accessibilité appropriées. Selon les experts, les blockchains privées sont déployées pour le vote, la gestion de la chaîne d'approvisionnement, la découverte et la gestion de l'identité numérique, la propriété des actifs, etc. Il existe certaines blockchains privées populaires comme Multichain, les projets Hyperledger, Corda, etc [63].

2.5.3 Blockchain hybride

Dans les blockchains hybrides, la personnalisation maximale est considérée comme le principal avantage avec un système privé basé sur des permissions ainsi qu'un système public sans permission. Dans ce type de systèmes blockchain, les utilisateurs peuvent accéder à certaines sections sélectionnées tandis que le reste peut être enregistré ou conservé en toute sécurité grâce aux avantages des enregistrements du registre. Les blockchains hybrides sont suffisamment flexibles pour que les utilisateurs puissent rejoindre facilement comme une blockchain privée. Ce type de blockchain est capable d'améliorer la sécurité et la transparence du réseau blockchain [64] [60].

2.5.4 Blockchains de consortium

Un autre type de blockchain semi-décentralisée, et ce type de blockchain est capable dans l'organisation de la gestion du réseau blockchain. Ce type de blockchain est capable de réaliser des activités même au sein d'une seule organisation. Ici, la blockchain est capable d'échanger des informations ou de faire du minage et est utilisée dans des domaines tels que les banques, les organisations gouvernementales, etc. Quelques exemples de ce type de consortium sont Energy Web Foundation, R3, etc [63].

2.6 Contrat intelligent dans la blockchain

Les contrats intelligents présentent plusieurs avantages. Par exemple, un garant intermédiaire n'est plus nécessaire pour les transactions, et les deux parties à la transaction n'ont plus à se soucier des problèmes de confiance, ce qui accélérera la vérification et l'exécution du contrat. Un contrat intelligent correspond à un morceau de code de programme, mais une fois déployé dans la blockchain, il ne peut pas être modifié. Comme la blockchain peut être considérée comme une base de données distribuée et que les contrats intelligents sont déployés dans le système blockchain, elle bénéficie également des avantages d'un système distribué, ce qui peut garantir la sécurité et la fiabilité des données. Cependant, la technologie des contrats intelligents est encore loin d'une application pratique et fait face à de nombreux défis [65].

3. L'intelligence artificielle :

3.1 Définition

L'intelligence artificielle (IA) est un domaine de l'informatique qui vise à créer des systèmes capables d'accomplir des tâches qui nécessitent habituellement l'intelligence humaine. Ces tâches peuvent inclure l'apprentissage, le raisonnement, la résolution de problèmes, la reconnaissance de formes et le traitement du langage naturel.

Les systèmes d'IA utilisent des algorithmes, des modèles et des données pour effectuer ces tâches. Ils peuvent être programmés pour apprendre à partir de données passées, s'adapter à de nouvelles situations, et améliorer leur performance au fil du temps. Les applications de l'IA sont vastes et incluent des domaines tels que la santé, la finance, l'automatisation industrielle, la reconnaissance vocale et d'images, les véhicules autonomes, et bien d'autres [66].

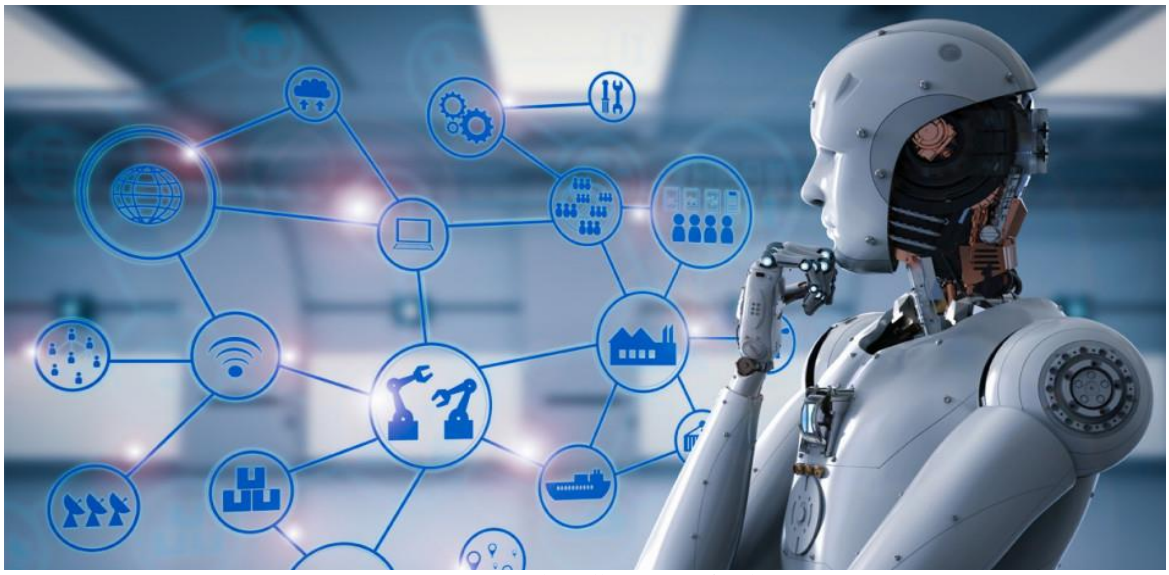

Figure 12 :l'intelligence artificiel

3.2 Les avantages de l'intelligence artificielle en entreprise

Pour une entreprise, l'utilisation de l'intelligence artificielle présente plusieurs avantages [67].

3.2.1 Améliorer la productivité et les processus

Quelle que soit la taille de votre structure, la productivité est l'une de vos préoccupations. Avec l'IA il est possible d'améliorer considérablement vos processus et d'automatiser certaines tâches courantes et répétitives.

Les collaborateurs peuvent ainsi être plus performants et être plus productifs dans leur travail. Vous éliminez les étapes inutiles, réduisez les erreurs et offrez plus de souplesse à vos salariés. [67]

3.2.2 Gagner du temps

L'un des avantages de l'intelligence artificielle est qu'elle permet de gagner du temps dans la réalisation des tâches. Grâce à l'automatisation, il est plus simple d'accélérer certains processus et de ne plus perdre de temps face à certaines actions chronophages.

D'ailleurs, elle est une alliée de poids pour traiter plus rapidement de grands volumes de données. Les salariés ont ainsi la possibilité de se focaliser sur des missions plus importantes avec plus d'efficacité. [67]

3.2.3 Réduire les coûts

Si au premier abord, investir dans l'IA semble cher, il faut savoir qu'à la longue, elle permet

de mieux gérer les ressources et donc de réduire les coûts. Comme elle est capable d'automatiser plusieurs tâches, elle peut vous éviter d'engager des dépenses dans d'autres outils.

Aussi, sa capacité à effectuer le travail de plusieurs individus, plus rapidement et sans erreur, vous aide à réaliser des économies et à ne pas perdre d'argent. [67]

3.2.4 Proposer de nouveaux outils

Grâce aux avancées technologiques, l'intelligence artificielle prend donc une place toute nouvelle au sein de notre société. Sans cesse en quête de nouvelles innovations, elle permet de proposer de nouveaux outils et logiciels facilitant aussi la vie en entreprise. Mettre en place de nouveaux services, faciliter les processus, créer des applications métier ou des business app, construire des logiciels intelligents, participer aux développement des smart cities… l'IA améliore les conditions de travail des collaborateurs comme des individus en général. [67]

3.2.5 Analyser et exploiter les données

Peu importe la taille et le secteur d'activité d'une entreprise, les données qui transitent sont une source d'information précieuse. Avec le développement du Big data, l'affluence de données est conséquente et intarissable. Avec l'intelligence artificielle, les structures peuvent optimiser le ciblage de leurs clients en analysant de grands volumes de données. Cela leur permet de mieux connaître leurs clients et d'augmenter la rentabilité.[67]

3.2.6 Améliorer le service clients :

Les clients sont justement l'une des préoccupations principales des entreprises. Une bonne utilisation de l'IA peut considérablement améliorer le service clients afin de mieux satisfaire les utilisateurs et répondre à leurs besoins. Chatbots, assistant virtuel ou encore automatisation, l'intelligence artificielle propose de nombreux outils afin de favoriser la résolution de problèmes en autonomie et d'alléger la charge de travail des employés.

[67]

3.3 Quels sont les types d'intelligence artificielle ?

Grâce au développement de l'intelligence artificielle et aux technologies découvertes comme le Depp Learning ou le machine Learning, les chercheurs s'accordent pour discerner 3 types d'intelligence artificielle [67] :

3.3.1 L'intelligence artificielle générale

L'intelligence artificielle générale ou profonde est une intelligence artificielle qui peut accomplir toutes sortes de tâches cognitives, tout comme le ferait un être humain ou un animal. Toujours perçus comme des hypothèses, certains chercheurs se posent des questions sur GPT-4 et la possibilité qu'il s'agisse d'une première forme d'intelligence artificielle générale. Dans cette optique, la plupart des chercheurs en IA estiment que l'humanité possède les compétences technologiques nécessaires pour développer une IA globale, en particulier grâce aux réseaux de neurones.

3.3.2 L'intelligence artificielle forte

Lorsqu'un modèle fait référence à des connaissances philosophiques et présente des signes d'une conscience propre, on parle d'IA forte ou de superintelligence. Tout à fait proche d'un scénario de science-fiction, les experts en IA estiment cependant que la création d'une IA performante est aujourd'hui impossible. Selon leur point de vue, il est impossible de concevoir la conscience et les sentiments dans des systèmes mathématiques qui manipulent et répondent à travers des symboles et des calculs.

3.3.3 L'intelligence artificielle faible

L'IA faible ou étroite est la dernière différence entre l'intelligence artificielle et l'IA. L'intelligence artificielle est un système qui peut effectuer une seule tâche de manière presque parfaite, sans nécessiter de supervision humaine. Il s'agit du modèle le plus couramment employé et conçu pour accélérer différents processus dans divers domaines d'activité.

4. Une approche de détection intrusion basé sur blockchain et intelligence artificiel

4 .1. Définitions

4.1.1. Intelligence Artificielle Fédérée

L'IA fédérée, ou Federated Learning (FL), est une approche décentralisée où les données ne sont pas centralisées. Au lieu de transférer les données vers un serveur central pour l'entraînement, les algorithmes de machine learning sont envoyés aux dispositifs locaux. Ces dispositifs entraînent le modèle en utilisant leurs données locales et envoient uniquement les mises à jour (c'est-à-dire les poids du modèle) au serveur central. Ce serveur central agrège les mises à jour pour améliorer le modèle global [69].

4.1.2. Définition du cloud

Le terme "cloud" désigne un ensemble de serveurs distants interconnectés qui fournissent des ressources et des services via Internet. Ces services comprennent le stockage de données, l'hébergement de sites web, l'exécution d'applications, la gestion de bases de données, et bien plus encore. L'utilisation du cloud permet aux entreprises et aux particuliers d'accéder à des ressources informatiques puissantes sans avoir besoin de gérer physiquement ces ressources [70].

4.2. Méthode Détection intrusion avec Blockchain et IA

Dans ce travail [70], un mécanisme intelligent de détection d'intrusion, nommé FIDANN,pour sécuriser les services de données médicales en utilisant DMO-ANN via l'apprentissage fédéré (FL). Le framework d'apprentissage automatique distribué est FL. Chacune des nombreuses organisations en Floride a accès aux données et aux ressources informatiques. Ce mécanisme est spécifiquement conçu pour compiler des modèles d'apprentissage automatique locaux qui ont été formés sur des appareils informatiques locaux contenant des données, sans partager les informations en dehors des institutions. Les modèles globaux de ML sont ensuite agrégés. « Les données ne bougent pas, le modèle bouge » est le principe central de FL. La Figure 4 décrit la structure de la méthodologie proposée [71].

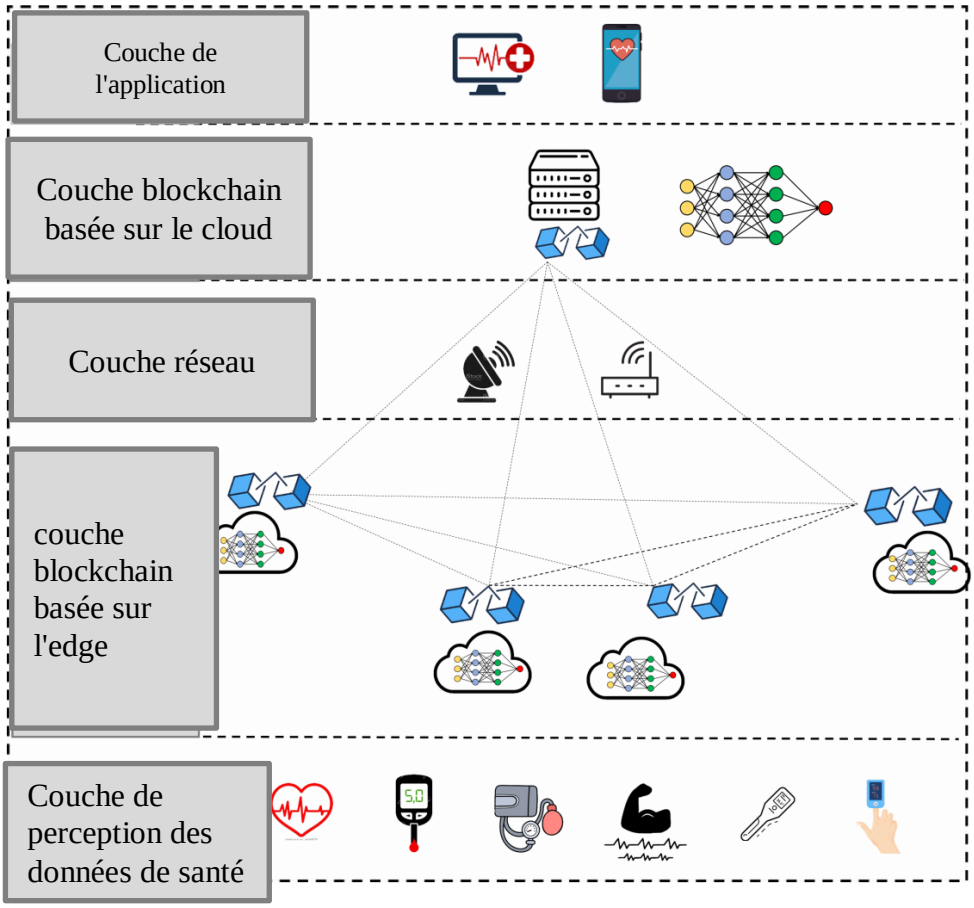

Figure 13 : Aperçu de la méthodologie proposée[70]

4.2.1. La collecte des données

L'utilisation généralisée des dossiers de santé électroniques (EHR) offre aux chercheurs un accès facile et peu coûteux à des données cliniques longitudinales étendues. La plupart des recherches en apprentissage fédéré (FL) utilisent des données EHR provenant de divers centres médicaux. Le jeu de données MIMIC59, qui contient des informations sur envirn 40 000 patients gravement malades du Beth Israel Deaconess Medical Center, est devenu la référence pour la recherche en apprentissage automatique (ML). Cependant, MIMIC présente des limitations pour la recherche en FL car il provient d'un seul institut de recherche [71].

4.2.2. Couche blockchain basée sur la périphérie

Les passerelles IoT, intégrant des équipements de détection médicale, forment la couche périphérique de la blockchain et supportent divers protocoles réseau. Un système de détection d'intrusion (IDS) a été mis en place pour standardiser les données et identifier les attaques par réseaux neuronaux. Le module proposé, intégré dans le modèle FL et entraîné à la périphérie, vise à réduire le temps de détection des infiltrations à mesure que les ressources d'attaque se rapprochent.

Comme le modèle d'apprentissage fédéré (FL) peut être appliqué à des ensembles de données plus petits, il nécessitera moins de temps de traitement et de calcul. Une fois que les modules ont été appris, leurs poids respectifs seront envoyés à un registre distribué basé sur la blockchain et enregistrés dans un bloc lié qui relie les nœuds GW au nœud serveur dans la couche cloud suivante. Ces cubes interconnectés seront également utilisés pour la synthèse et la moyenne. Enfin, la chaîne est cryptée en utilisant une fonction de hachage qui lie les blocs entre eux, la rendant immuable grâce à l'utilisation de méthodes de consensus (contrats intelligents - SC).

Les SC basés sur la blockchain sont des protocoles automatisés pour l'exécution de transactions financières. Grâce aux SC, les participants aux transactions peuvent prédéterminer les conditions sous lesquelles elles seront effectuées mécaniquement. Il existe une large gamme d'environnements adaptés au déploiement des SC. En d'autres termes, les SC permettent aux utilisateurs d'exécuter un script sur un réseau blockchain de manière vérifiée, résolvant ainsi de nombreux problèmes avec un minimum de confiance. Les protocoles déterministes et les garanties fournies par un SC permettent aux utilisateurs d'éliminer le besoin d'un tiers de confiance. Un SC peut être identifié de manière unique par son adresse et son compte sur le registre distribué. Ainsi, il peut fonctionner comme un séquestre puisqu'il peut surveiller son état et acquérir des actifs basés sur la blockchain. Avec l'aide du réseau, le SC met à disposition un ensemble d'opérations qui peuvent être initiées en envoyant une transaction au contrat. Chaque nœud du réseau a accès à chaque SC stocké sur la blockchain, ce qui signifie qu'ils peuvent tous voir les instructions du contrat et les suivre. On peut considérer le dispositif portable du patient et les professionnels de santé comme deux parties qui doivent se fier à l'intégrité de la blockchain. De plus, comme indiqué précédemment, les patients peuvent donner et refuser l'accès à leurs données en utilisant d'autres SC.

Un des problèmes les plus importants du FL, les attaques par empoisonnement, sont abordées par le modèle proposé. Chaque serveur périphérique (ES) obtient les valeurs de poids mises à jour, chiffre les informations recueillies et crée la signature associée en utilisant sa propre clé secrète. Ensuite, l'ES combine le texte chiffré et le transmet, avec la signature, à la couche blockchain active gérée par un SC, garantissant la confidentialité et la validité de la transaction. Lorsqu'un SC reçoit des données de plusieurs ES, il utilise les clés publiques associées à ces ES et les données enregistrées sur la blockchain pour déterminer si les données sont valides ou non. En réponse, la blockchain active peut être récupérée par le CPCC, qui

peut alors extraire le texte clair agrégé en utilisant sa clé secrète. Les connexions entre le CPCC et les ES, ainsi qu'entre les ES et le modèle local approprié, sont bidirectionnelles dans la plupart des applications de calcul en périphérie IoT. Semblable au stockage d'informations en périphérie basé sur des terminaux, le modèle local peut envoyer et recevoir des données avec le CPCC en utilisant le réseau blockchain et les ES [71].

4.2.3. Couche réseau

Dans la couche réseau, il s'agit du composant responsable de garantir la sécurité des transactions de données se déplaçant des couches inférieures aux couches supérieures. Il est appelé la couche de connexion et son objectif principal est d'offrir la gestion des routes [71].

5.2.4. Couche blockchain basée sur le cloud

Pour maintenir à jour les poids globaux de l'algorithme ANN, la couche BC basée sur le cloud est chargée de moyenner les poids rapportés par les serveurs périphériques (ES) et de les enregistrer dans le registre de la blockchain. Pour une sécurité réseau optimale, le cloud distribue périodiquement les poids modifiés mentionnés ci-dessus à toutes les passerelles, où ils sont utilisés pour mettre à jour les poids des modèles locaux. La figure 5 montre le réseau blockchain FIDANN. Enfin, La couche application est responsable du suivi des signes vitaux d'un patient [71].

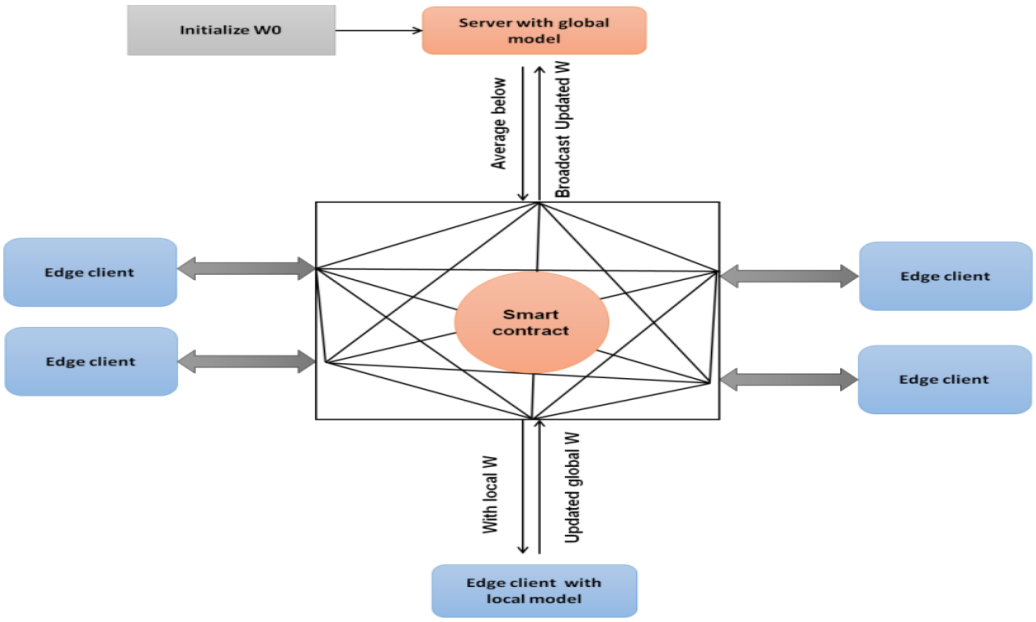

Figure 14: Représentation du réseau block Chain FIDANN[70]

4 .2.5. Description du formulaire de divulgation

La tâche de détection d'intrusion est réalisée par DMO-ANN. Le DMO fonctionne sur le même concept que l'algorithme métaheuristique basé sur une population aléatoire. Cette méthode a été conçue pour simuler la dynamique de groupe et les techniques de recherche de nourriture de la mangouste naine. Les mangoustes naines sont des créatures sociales qui cherchent leur nourriture en groupe, mais quand il s'agit de manger, chaque animal agit indépendamment. En raison de leur nature semi-nomade, elles construisent un terrier pour dormir près d'une source abondante de nourriture puis passent à la suivante. Comme indiqué dans l'Équation (1), le DMO commence ses mises à jour en établissant les valeurs initiales pour la population candidate des mangoustes. Les populations sont créées de manière aléatoire entre la limite inférieure (LB) et la limite supérieure (UB) d'un problème donné (UB).

N = [

$$\begin{matrix} n_{1,1} & n_{2,1} & \dots & n_{1,i-1} & n_{i,1} \\ n_{1,1} & n_{2,2} & \dots & n_{2,\,i-1} & n_{2,\,i} \\ \vdots & \vdots & n_{d,s} & \vdots & \vdots \\ n_{x,1} & n_{x,2} & \dots & n_{x,i-1} & n_{x,i} \end{matrix}$$

] (1)

Où N est la collection de candidats actuellement disponibles, produite aléatoirement à l'aide de l'équation (2), nd, est la coordonnée de la jth dimension de la ith population, x est la taille de la population et i est la dimension du problème.

$$n_{ds} = unifrnd\,(VarMin, VarMax, VarSize) \quad (2)$$

Où $unifrnd$ est un entier aléatoire uniformément distribué, $VarMin$ et $VarMax$ sont les valeurs minimales et maximales autorisées, et $VarSize$ est la taille du problème. À cette itération, la meilleure solution est la même que la meilleure solution de l'itération précédente. Le DMO, comme d'autres algorithmes méta euristiques, se compose de deux phases : l'exploitation (où chaque mangouste effectue une recherche approfondie dans une zone spécifique) et l'exploration (où les mangoustes explorent aléatoirement pour trouver une nouvelle source abondante de nourriture ou de nouveaux monticules de sommeil (SM)). Les trois principales structures sociales du DMO – le groupe des éclaireurs, les nourrices et le groupe alpha –

réalisent les activités au cours des deux phases. La femelle alpha (α) dans une unité familiale est choisie selon l'équation (3).

$$\alpha = \frac{\text{fitd}}{\sum_{d=1}^{x} \text{fitd}} \quad (3)$$

Le symbole x-bn représente le nombre de mangoustes dans le groupe Bn désigne le nombre de nourrices, et peep est le cri de la femelle alpha, qui maintient la famille sur le bon chemin. La position du monticule de sommeil (SM) est déterminée par la source de nourriture abondante, comme décrit dans l'Équation (4) ci-dessous.

$$N_{d+1} = N_d + phi * peep \quad (4)$$

Où phi est un nombre distribué aléatoirement entre [-1,1]. Le monticule de sommeil (SM) est évalué à la fin de chaque cycle ; l'Équation (5) est une représentation du monticule de sommeil.

$$jc\_\frac{fit_{d+1} - fit_d}{\text{Max}\{|fit_{d+1} - fit_d|\}} \quad (5)$$

Lorsqu'un monticule de sommeil (SM) est découvert, l'Équation (6) fournit une valeur représentative de la moyenne.

$$\varphi = \frac{\sum_{d=1}^{x} \text{dcd}}{x} \quad (6)$$

Dès que les critères pour changer de nourrices sont remplis, le processus passe au groupe des éclaireurs (SG), où le prochain monticule de sommeil (SM) est évalué en fonction de la proximité d'une source de nourriture appropriée. Puisque les mangoustes ne retournent souvent pas aux monticules de sommeil déjà utilisés, le SG doit toujours être à la recherche de nouveaux monticules pour garantir le succès de l'exploration. Dans le DMOA, la recherche de nourriture et l'activité du SG se produisent simultanément, en supposant que plus la famille cherche de la nourriture loin, plus la probabilité d'identifier le prochain SM est élevée, comme simulé par l'Équation.

$$Nd + 1 = \begin{cases} Nd - ME * phi * rand * [Nd - \vec{C}] \; if \; \varphi d + 1 > \varphi d \\ Nd - ME * phi * rand * [Nd - \vec{C}] \; else \end{cases}$$

Le paramètre $Me = \left(1 - \frac{iter}{Max\ iter}\right)^{\left(2 - \frac{iter}{Max\ iter}\right)}$ qui contrôle le mouvement collectif volatil du groupe de mangoustes est réduit de manière linéaire avec le temps, et le rand est une valeur

aléatoire entre [0,1]. Le désir de la mangouste d'aller vers un nouveau monticule de feuilles mortes est représenté par le vecteur $\vec{C} = \sum_{d=1}^{x} \frac{nd \times jcd}{Nd}$

Pendant que le groupe des éclaireurs (SG) et le groupe de recherche de nourriture cherchent un monticule de sommeil (SM) et une source de nourriture, le groupe des nourrices reste avec les jeunes. Puisqu'ils ne cherchent pas de nourriture et ne font pas de reconnaissance, les membres de ce groupe sont soustraits de la population candidate. Comme le montre l'Équation 7, les nourrices rejoignent le groupe de recherche de nourriture ou d'éclaireurs pour trouver de la nourriture lorsqu'un critère spécifique est atteint.

L'approche ANN avec rétropropagation est utilisée pour le mécanisme de détection. La propagation avant dans un réseau neuronal est utilisée pendant la phase d'entraînement. Les nœuds de la couche de sortie produisent une valeur après la passe avant. Pendant la passe avant, l'entrée totale du nœud est d'abord déterminée, puis la sortie du nœud est déterminée en utilisant la fonction d'activation. Cette formule est utilisée pour calculer l'entrée totale reçue par chaque neurone dans un réseau neuronal à propagation avant.

$$Total\ Input = f_1 * a_1 + f_2 * a_2 + \cdots + f_w * a_w + 1 * m_n$$
$$Where: f_1, f2, \ldots\ldots, ff - Input\ neurons \quad (8)$$

$a1, a2, , an$ - Poids associés aux neurones d'entrée

a_n - Poids associé au biais

La sortie du neurone est calculée en utilisant la fonction d'activation. Pour déterminer la sortie du neurone, la fonction d'activation est utilisée.

$$function\ Activation = 1/(1 + {}^{(-TotalInput)}) \quad (9)$$

Où:

Total Input -L'entrée totale du neurone.

L'entraînement des réseaux neuronaux artificiels en utilisant une technique connue sous le nom de rétro propagation, combinée à une approche d'optimisation telle que la descente de gradient, est répandue. La propagation et les mises à jour des poids sont les deux phases du la passe avant est comparée à la sortie prédite lors de la phase de rétro propagation [71].

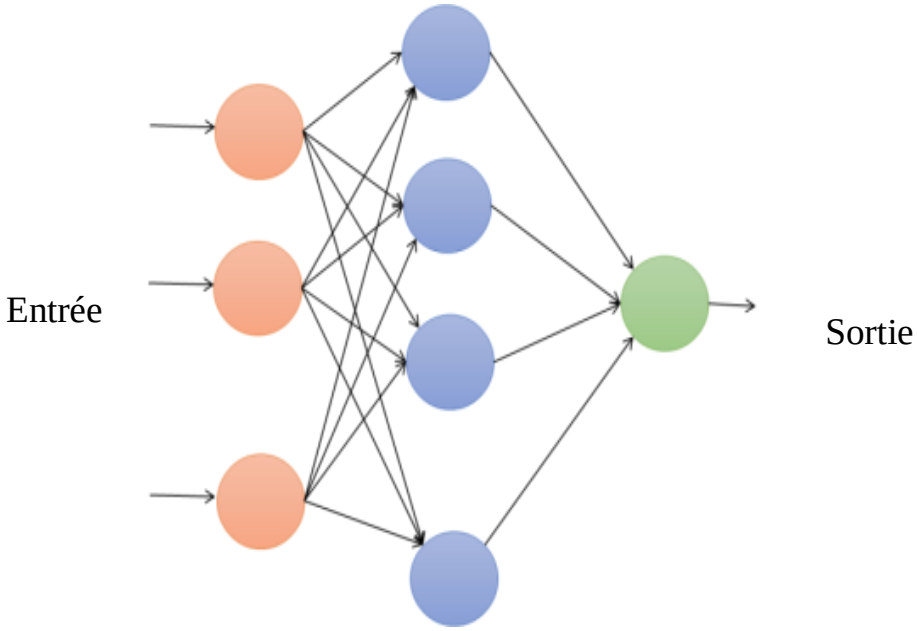

Figure 15 Représentation de l'ANN[71]

5.Conclusion

Dans ce chapitre, nous avons parlé de la blockchain et ses grands principes, ses domaines et les avantages et les inconvénients de cette technologie. Nous avons défini l'intelligence artificielle, y compris leurs avantages et inconvénients, et aussi nous citez les types. Nous avons présenté la methode de detection intrusion avec block Chain.

Chapitre 04 : Implémentation

1. Introduction

Après avoir terminé la phase de spécification et conception, dans une première partie, nous entamerons la conception technique en décrivant l'architecture générale de notre système. Ensuite, nous allons citer les ressources matérielles et logicielles qu'on réunit pour l'implémentation et la réalisation de notre système.

2. Implémentation

2.1 Environnement de développement :

Cette partie est réservée aux détails de l'environnement de développement et le langage de programmation utilisés pour la réalisation de notre système.

- **Environnement matérielle :**

Pour réaliser l'application, et pour le tester, on a utilisé les machines suivantes :

Figure 16 :TOSHIBA DESKTOP-LLER47G

- **Processors**: 11th Gen Intel(R) Core(TM) i7-7600U CPU @ 2.80GHz 2.90 GHz
- **Mémoire installée** : (RAM) : 8.00 Go
- **Type de système** : système d'exploitation 64 bits.
- **Système d'exploitation** : Windows 10

2.2 Environnement logicielle :

- **Langage de programmation :**

Anaconda : Anaconda Navigator est l'interface de navigation d'Anaconda, elle permet de lancer les différentes API disponibles et de gérer les différents packages et environnements du logiciel. Cette interface permet de naviguer simplement dans le logiciel, sans devoir connaître toutes les lignes de code de

Notebook Jupyter : est une application Web open source qui permet aux data scientists de créer et de partager des documents comprenant du code en direct, des équations et d'autres ressources multimédias [73].

Python : Le langage de programmation Python a été créé en 1989 par Guido van Rossum, aux Pays-Bas. Le nom Python vient d'un hommage à la série télévisée Monty Python's Flying Circus dont G. van Rossum est fan. La première version publique de ce langage a été publiée en 1991. La dernière version de Python est la version 3. Plus précisément, la version 3.11 a été publiée en octobre 2022. La version 2 de Python est obsolète et n'est plus maintenue, évitez de l'utiliser [74].

MetaMask : est une extension de navigateur Web et une application mobile qui vous permet de gérer vos clés privées Ethereum. Ce faisant, il sert de portefeuille pour Ether et d'autres jetons, et vous permet d'interagir avec des applications décentralisées ou dapp [75].

Solidity : est un langage de programmation orienté objet dédié à l'écriture de contrats intelligents [76]. Il est utilisé pour implémenter des smartcontrat sur diverses blockchains, notamment Ethereum. Il a été développé par Christian Reitwiessner, Alex Beregszaszi, Yoichi Hirai et plusieurs anciens contributeurs principaux d'Ethereum pour permettre l'écriture de contrats intelligents sur des plateformes de blockchain telles qu'Ethereum [77]

Remix IDE : est une application Web et de bureau open source. Il favorise un cycle de développement rapide et dispose d'un riche ensemble de plugins avec des interfaces graphiques intuitives [78].

Microsoft : Word est un logiciel de traitement de texte publié par Microsoft. La version la plus récente est Word 2021. Si ce bandeau n'est plus pertinent [79].

Ganache : Environnement de développement personnel utilisé pour tester et déployer des contrats intelligents Ethereum en mode local [80].

- **Bibliothèques utilisées :**

Pandas : est une bibliothèque écrite pour le langage de programmation Python permettant la manipulation et l'analyse de données. Elle propose en particulier des structures de données et des opérations de manipulation de tableaux numériques et de séries temporelles [81].

Firebase :est un ensemble d'outils pour l'hébergement et le développement d'applications mobiles et web, qui permet l'envoi de notifications et de publicités, la remontée des erreurs et des clics effectués dans l'application.[82]

- **Sklearn.model_selection :** La classe `model_selection` de scikit-learn (sklearn) fournit des outils pour diviser les ensembles de données, valider les modèles, et optimiser les hyperparamètres, facilitant ainsi l'évaluation et la sélection de modèles d'apprentissage automatique.
- **Sklearn.preprocessing :** est un module de la bibliothèque scikit-learn qui fournit des outils pour normaliser, standardiser et transformer des données afin de les préparer pour des modèles d'apprentissage automatique.
- **Numpy :** est une bibliothèque pour le langage de programmation Python, utilisée pour le calcul scientifique et technique, qui permet de travailler efficacement avec des tableaux et des matrices multidimensionnels, tout en offrant une vaste collection de fonctions mathématiques pour les manipuler.
- support (SVM), utilisés pour la classification, la régression et la détection des valeurs aberrantes.
- **TensorFlow :** est une bibliothèque open source développée par Google pour le machine learning et l'intelligence artificielle, permettant de créer, d'entraîner et de déployer des modèles de réseaux de neurones complexes à grande échelle sur diverses plateformes

- **Web 3 :** Web 3.0 représente la prochaine phase d'évolution d'Internet, caractérisée par une infrastructure décentralisée basée sur la blockchain

3. Application de l'approche

Etape 01 : Transformation des données textuelles en données numériques et division en ensembles d'entraînement et de test

Les données sont chargées depuis l'internet. Column_names spécifie les noms des colonnes pour le DataFrame data. LabelEncoder transforme les colonnes de type texte en valeurs numériques. Tandis que la division en ensembles d'entraînement et de test permet d'évaluer les performances du modèle sur des données non vues, assurant ainsi une meilleure généralisation et prévention du sur apprentissage.

```
Shape des données d'entraînement : (455, 30)
Shape des données de test : (114, 30)
Epoch 1/10
15/15 ━━━━━━━━━━━━━━━━━━━━ 1s 4ms/step - accu
```

Figure 17 :Résultat de télécharger et nettoyer les données

Etape 02 : Définition du modèle de réseau de neurones(ANN)

Un modèle de réseau de neurones simple est défini avec trois couches denses. fc1 et fc2 utilisent l'activation ReLU, tandis que fc3 utilise une activation linéaire (adaptée pour la classification multi-classes)

```
class SimpleANN(nn.Module):
    def __init__(self):
        super(SimpleANN, self).__init__()
        self.fc1 = nn.Linear(41, 64)
        self.fc2 = nn.Linear(64, 32)
        self.fc3 = nn.Linear(32, 2)

    def forward(self, x):
        x = torch.relu(self.fc1(x))
        x = torch.relu(self.fc2(x))
        x = self.fc3(x)
        return x
```

Figure 18 : Définition du modèle

Etape 03 : Optimisation des poids initiaux en utilisant l'algorithme DMO

Nous avons défini l'algorithme DMO (Dwarf Mongooses) pour optimiser les poids initiaux du modèle. Une population initiale de poids aléatoires est générée et optimisée au fil de plusieurs itérations, où les poids sont ajustés en fonction d'une fonction de fitness simple ici.

```
Iteration 1/100, Best Cost: 1323.1504127928479
Iteration 2/100, Best Cost: 1279.5205337373054
Iteration 3/100, Best Cost: 1116.8049272902044
Iteration 4/100, Best Cost: 958.2339256250079
Iteration 5/100, Best Cost: 837.5035115722891
Iteration 6/100, Best Cost: 723.8125582165565
Iteration 7/100, Best Cost: 610.3741264305979
Iteration 8/100, Best Cost: 538.028928455403
Iteration 9/100, Best Cost: 479.2911099626107
Iteration 10/100, Best Cost: 415.7838414538561
Iteration 11/100, Best Cost: 363.6006268545353
Iteration 12/100, Best Cost: 308.7366369030973
Iteration 13/100, Best Cost: 288.7003459012228
Iteration 14/100, Best Cost: 254.10839282333563
Iteration 15/100, Best Cost: 227.0899993068615
Iteration 16/100, Best Cost: 187.8323385635149
Iteration 17/100, Best Cost: 176.2473391981061
Iteration 18/100, Best Cost: 156.9205276356784
Iteration 19/100, Best Cost: 133.5270262213204
```

Figure 19 : des poids initiaux en utilisant l'algorithme DMO

Étape 4 : Entraînement du réseau de neurones avec les poids optimisés

Nous avons utilisé les poids optimisés obtenus grâce à l'algorithme DMO pour initialiser les poids du modèle de réseau de neurones. Ensuite, nous avons entraîné le modèle, Les données d'entraînement et testé sur les données de test à travers plusieurs époques.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

```
Epoch 1/10
15/15 ━━━━━━━━━━━━━━━━━━━━ 1s 4ms/step - accuracy: 0.3348 - loss: 0.8301
Epoch 2/10
15/15 ━━━━━━━━━━━━━━━━━━━━ 0s 2ms/step - accuracy: 0.8306 - loss: 0.5485
Epoch 3/10
15/15 ━━━━━━━━━━━━━━━━━━━━ 0s 2ms/step - accuracy: 0.9201 - loss: 0.4337
Epoch 4/10
15/15 ━━━━━━━━━━━━━━━━━━━━ 0s 3ms/step - accuracy: 0.9376 - loss: 0.3442
Epoch 5/10
15/15 ━━━━━━━━━━━━━━━━━━━━ 0s 2ms/step - accuracy: 0.9184 - loss: 0.3002
Epoch 6/10
15/15 ━━━━━━━━━━━━━━━━━━━━ 0s 2ms/step - accuracy: 0.9256 - loss: 0.2582
Epoch 7/10
15/15 ━━━━━━━━━━━━━━━━━━━━ 0s 2ms/step - accuracy: 0.9276 - loss: 0.2377
Epoch 8/10
15/15 ━━━━━━━━━━━━━━━━━━━━ 0s 2ms/step - accuracy: 0.9486 - loss: 0.2132
Epoch 9/10
15/15 ━━━━━━━━━━━━━━━━━━━━ 0s 2ms/step - accuracy: 0.9468 - loss: 0.1843
Epoch 10/10
```

Figure 20 :Résultat de accuracy de chaque epoch

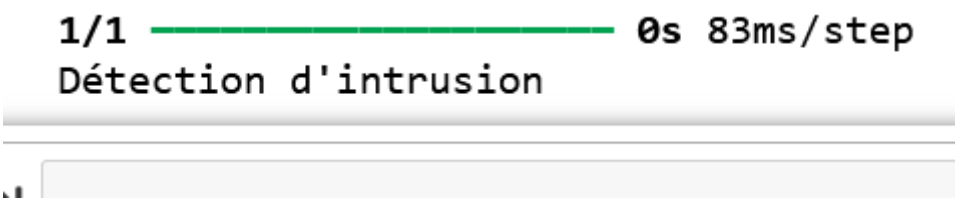

Figure 21 :Détection d'intrusion

Etape 5 : Crée contrat intelligent

Nous avons créé une contrat intelligent en Solidity, nommé WeightsStorage, permet de stocker et de gérer des poids associés à des indices spécifiques :

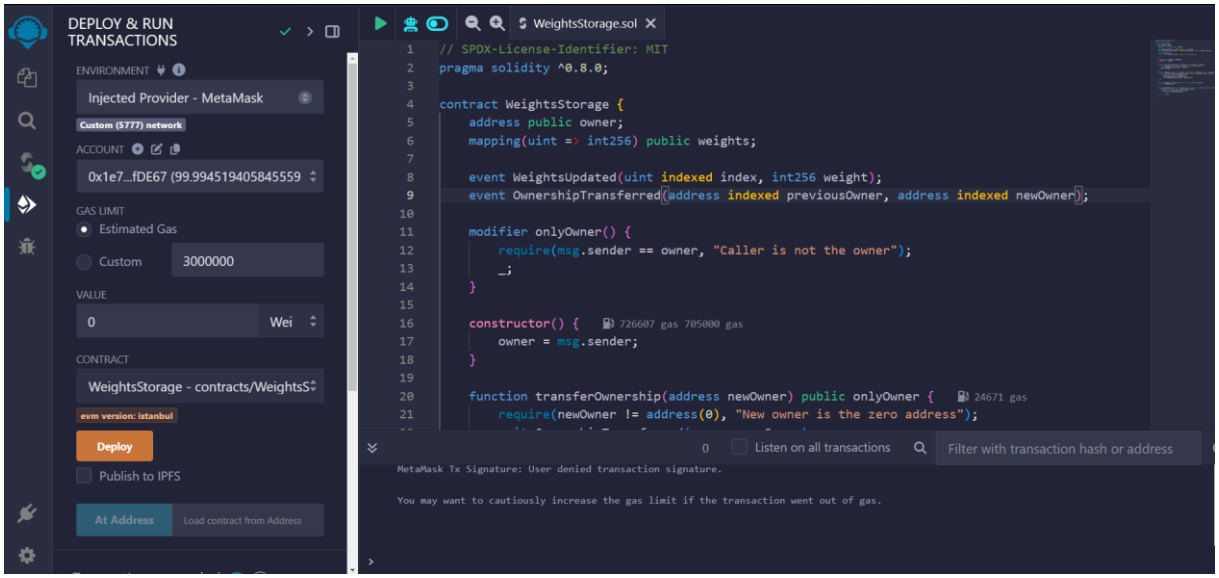

Figure 22 :Contrat intelligent

Etape 6 : faire transaction

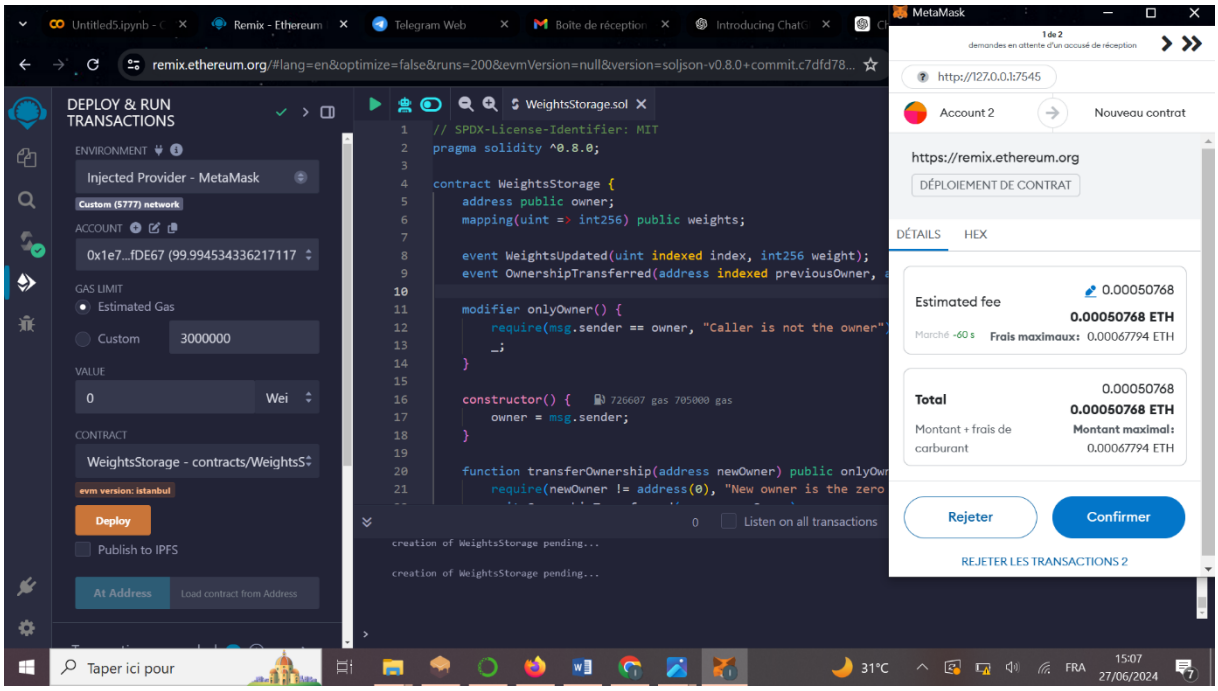

Figure 23 :Faire une transaction avec Metamask

Etape 7 : confirmé la transaction

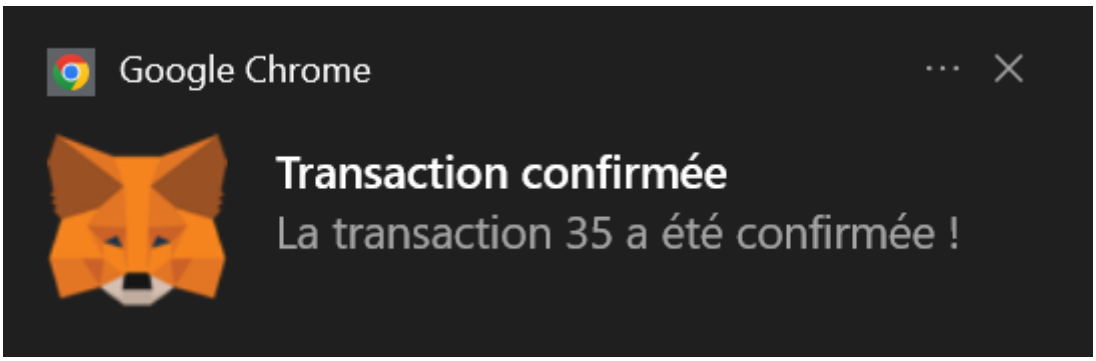

Figure 24 :cofirmé la transaction

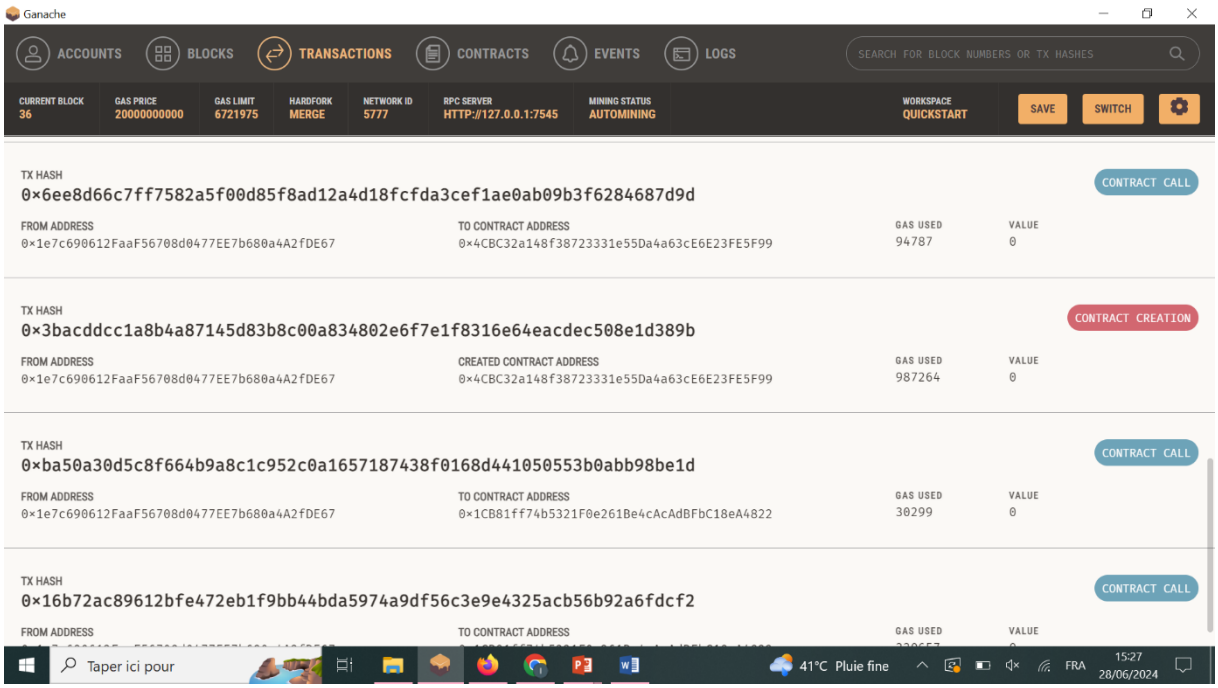

Figure 25 :Les transactions dans Ganache

Etape 8 : Envoi des poids du modèle au contrat intelligent (smart contract)

✓ Configuration du compte et du contrat

Pour interagir avec un contrat intelligent sur la blockchain en utilisant Web3.py, vous devez configurer plusieurs éléments, y compris l'URL de votre fournisseur Web3 (par exemple, Ganache), l'adresse de votre compte, la clé privée, et les détails de votre contrat intelligent (adresse et ABI).

✓ Connexion à Ganache

```
Connected to Ganache. Latest block number: 35
```

Figure 26 :connecte a Ganache

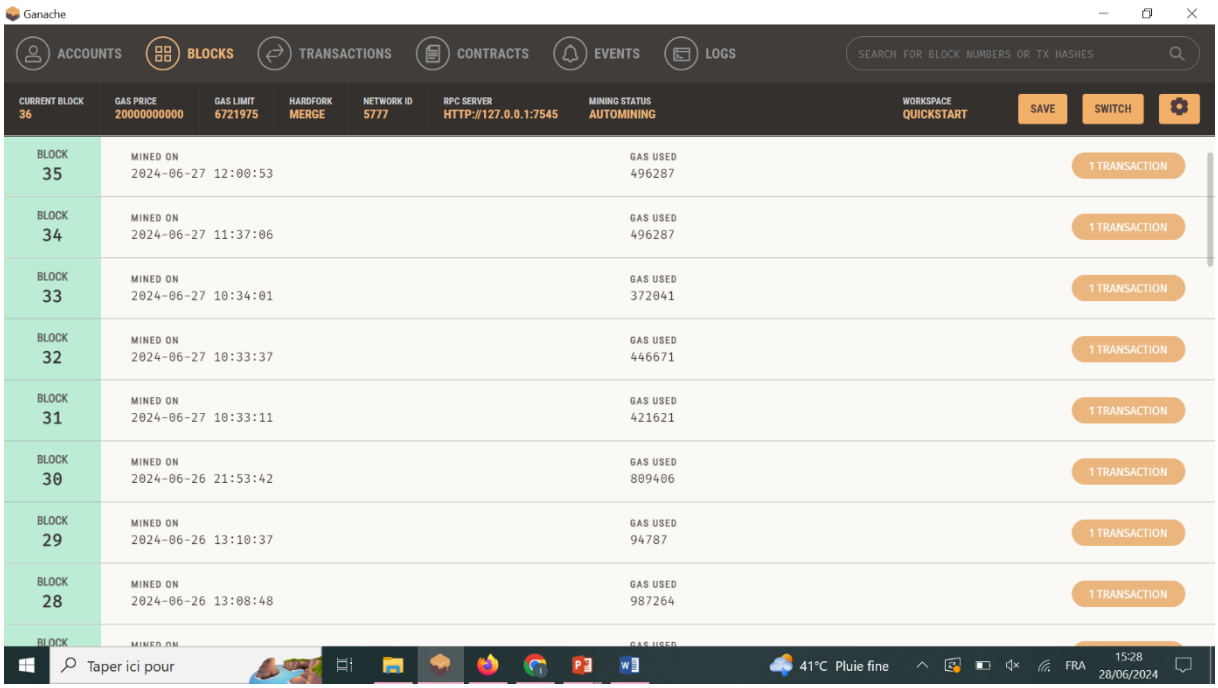

Figure 27 :les blocks dans Ganache

- ✓ **Fonction pour envoyer les poids au contrat intelligent**

```
def send_weights_to_contract(indices, int_weights):
    nonce = web3.eth.get_transaction_count(account_address)
    transaction = contract.functions.setWeights(indices, int_weights).build_transaction({
        'gas': 3000000,
        'gasPrice': web3.toWei('20', 'gwei'),
        'nonce': nonce,
        'chainId': 1337  # ID pour Ganache (peut varier selon la configuration de Ganache)
    })
    signed_txn = web3.eth.account.sign_transaction(transaction, private_key=private_key)
    tx_hash = web3.eth.send_raw_transaction(signed_txn.rawTransaction)
    print(f"Transaction hash: {web3.toHex(tx_hash)}")
```

Figure 28 :code source de envoyer les poids au contrat intelligent

Etape 9 : Firebase cloud

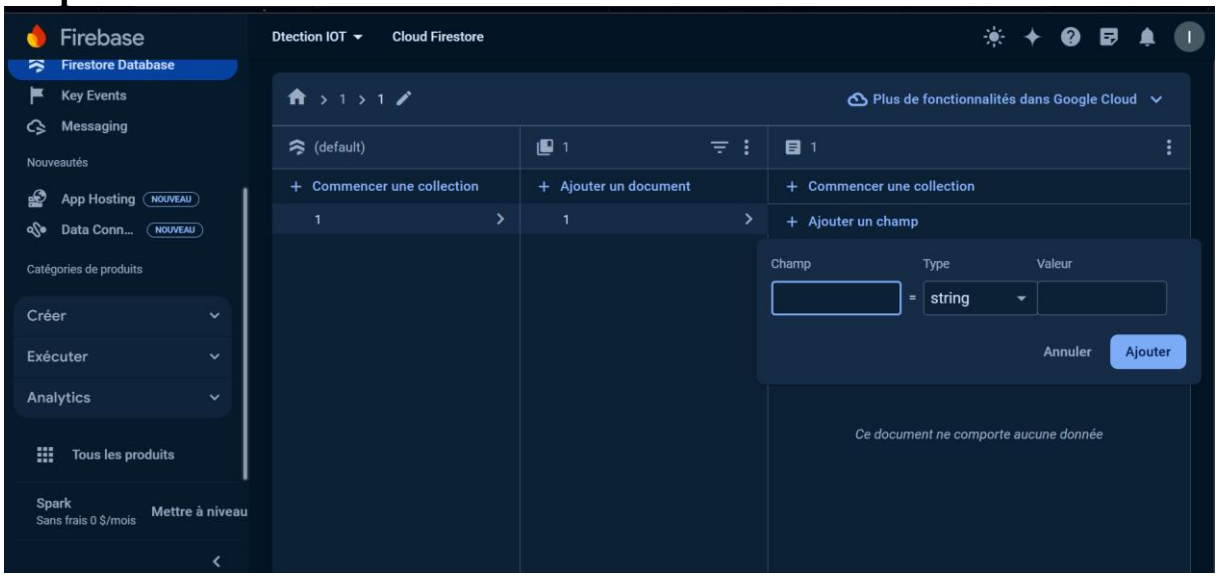

Figure 29 :Firebase consol

4. Conclusion

Au cours de ce chapitre, nous avons présenté les différentes phases de la réalisation. Nous avons commencé par les différentes technologies utilisées ainsi que l'environnement matériel et logiciel de notre travail. Et enfin, nous avons exposé certains imprimes écrans témoignant des différentes facettes de notre system.

Conclusion générale

Conclusion Générale

La combinaison de la détection d'intrusion basée sur l'intelligence artificielle fédérée et de la technologie blockchain pour les systèmes de santé IoT représente une avancée cruciale dans la sécurisation des données médicales sensibles et dans la protection des infrastructures critiques.

En intégrant l'apprentissage fédéré, qui permet l'analyse des données directement sur les dispositifs IoT sans compromettre la confidentialité, avec la blockchain, qui assure la traçabilité et l'intégrité des informations, ces systèmes deviennent plus résilients face aux cybermenaces. Les dispositifs IoT peuvent collaborer pour détecter les comportements anormaux et les intrusions potentielles tout en maintenant les données des patients sécurisées et privées.

L'utilisation de la blockchain comme registre immuable garantit également que toutes les transactions et interactions entre les dispositifs sont enregistrées de manière transparente et vérifiable. Cela renforce la confiance des patients et des professionnels de la santé dans l'utilisation des technologies IoT pour améliorer les soins tout en maintenant un niveau élevé de sécurité.

En résumé, la détection d'intrusion IA fédéré pour les systèmes de santé IoT basés sur la blockchain offre une solution robuste pour relever les défis de sécurité croissants tout en exploitant le potentiel des technologies émergentes pour améliorer les services de santé de manière sûre et efficace. Ce développement prometteur ouvre la voie à de nouvelles avancées dans la protection des données médicales et dans la transformation numérique des soins de santé.

References

[01] P-J. Benghozi, S. Bureau, F. Massit-Folléa, C. Waroquiers, and S. Davidson. L'internet des objets : quels enjeux pour l'Europe. Éd. de la Maison des sciences de l'homme, 2009.

[02] thttps://www.researchgate.net/publication/345951182

[03] Tafazolli, R., 2006. Technologies for the wireless future. Chichester: Wiley.

[04] Taleb Omar, Mankouri Abdelkrim. « Programmation de la sécurité Internet des Objet, Etude de cas module WIFI Electric imp », Mémoire de master, Université de Tlemcen, Algérie, 2016.

[05]https://www.synox.io/actualites-sectorielle/internet-des-objets-iot-qu-est-ce-que-cest/#:~:text=Historiquement%20le%20terme%20IoT%20a,l'%C3%A9cosyst%C3%A8me%20des%20objets%20connect%C3%A9s.

[06] Evans, D., 2011. The Internet of Things How the Next Evolution of the Internet Is Changing Everything. [Ebook] Etats-Unis : Cisco internet business solutions group (IBSG), pp.2-5. Disponible à : [Consulté le 4 février 2022].

[07]https://polaridad.es › ventajas-del-internet-de-las-cosas

[08] Atoumi .M Y, Bensadi. S, « Approche évolutionnaire pour la composition de services sensible à la QoS dans l'Internet des Objets à large échelle », Mémoire de master, Université de Bejaia, Algérie, 2018.

[09] Yick, J., Mukherjee, B. and Ghosal, D., 2008. Wireless sensor network survey. Computer Networks, 52(12), pp.2292-2330.

[10]Connectwave. 2022. Comment se compose un système IoT ? [En ligne] Disponible à : <https://www.connectwave.fr/techno-appli-iot/iot/reseaux-et-infrastructures-iot> [Consulté le 4 février 2022].

[11] Puccinelli, D. and Haenggi, M., 2005. Wireless sensor networks: applications and challenges of ubiquitous sensing. IEEE Circuits and Systems Magazine, 5(3), pp.19-31.

[12] http://dspace.univ-tiaret.dz/bitstream/123456789/2580/1/TH.M.GE.FR.2022.16.pdf

[13] https://www.talend.com/fr/resources/what-is-data-security/

[14]https://itsocial.fr/articles-decideurs/4-types-de-donnees-internet-des-objets-pour-3-modeles-big-data/

[15] TU-T X.800. Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du ccitt. Standard, ITU-T RECOMMENDATIONS, Switzerland, March 1991.

[16] Mécanisme de Sécurité pour L'internet des Objets Par Yasmine Labiod ,Annaba, Année

2022

[17] Arsalan Mosenia and Niraj K Jha. A comprehensive study of security of internet-of things. IEEE Transactions on emerging topics in computing, 5(4) :586–602, 2016. doi : 10.1109/tetc.2016.2606384.

[18] SShancang Li. Chapter 4 - iot node authentication. In Shancang Li and Li Da Xu,editors, Securing the Internet of Things, pages 69–95. Syngress, Boston, 2017. ISBN 978-0-12-804458-2. doi: https ://doi.org/10.1016/B978-0-12-804458-2.00004-4. URL https ://www.sciencedirect.com/science/article/pii/B9780128044582000044.

[19]https://navigacom.com/fr/blog/scurit-des-projets-iot-quelles-menaces-pour-vos-plateformes-de-donnes-

[20] Bah didi El Mokhtar Salem, Système de détection d'intrusion avec une approche D'apprentissage automatique, Université Saad Dahlab de Blida Faculté des sciences

[21] Fatma Merabet. Solutions de sécurité pour l'internet des objets dans le cadre de l'assistance à l'autonomie à domicile. Cryptographie et sécurité [cs.CR]. Université de Limoges; Université Mouloud Mammeri (Tizi-Ouzou, Algérie), 2021. Français.

[22] https://www.juniper.net/fr/fr/research-topics/what-is-ids-ips.html

[23] Gustavus J Simmons. Symmetric and asymmetric encryption. ACM Computing Surveys .

[24] Alexandra Boldyreva, Nathan Chenette, Younho Lee, and Adam O'neill. Order-preserving symmetric encryption. In Annual International Conference on the Theory and Applications of C

[25] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Annual International Cryptology Conference, pages 537–554. Springer, 1999.

[26] Monika Agrawal and Pradeep Mishra. A comparative survey on symmetric key encryption techniques. International Journal on Computer Science and Engineering, 4(5) :877, 2012. Cryptographic Techniques, pages 224–241. Springer, 2009 (CSUR), 11(4) :305–330, 1979

[27] https://www.ibm.com/fr-fr/topics/data-security

[28] Cours : Cyber Sécurité 1 Master 1 ISIDS Année 2021/2022 Université Batna 2 ChaPItre 5 : LeS SyStèmeS De DéteCtIon/PréventIon D'IntruSIon (IDS/IPS).

[29]DE Denning, « An intrusion-detection model», IEEE Transactions on software engineering (1987), 222–232.

[30] Ali A. Ghorbani, Wei Lu, Mahbod Tavallaee, « Network Intrusion Detection and Prevention: Concepts and Techniques », Page 34-35, 28 octobre 2009.

[31] S. Axelsson, « Intrusion detection systems: A survey and taxonomy », Tech. Report 99-15, Chalmers University of Technology, Department of Computer Engineering, 2000.

[32] J. Lee, S. Moskovics, and L. Silacci, « A Survey of Intrusion Detection Analysis Methods », 1999.

[33] A. Jones and R. Sielken, « Computer system intrusion detection: A survey », Tech. report, Department of Computer Science, University of Virginia, Thornton Hall, Charlottesville, VA, September 2000.

[34] J. McHugh, « Intrusion and intrusion detection », International Journal of Information Security 1 (2001), no. 1, 14–35.

[35] M. Dacier H. Debar and A. Wespi, « A revised taxonomy for intrusion-detection systems », Tech. report, IBM Research Report, 1999

[36] Teresa F. Lunt, « Detecting intruders in computer systems », Proceedings of the 1993 Conference on Auditing and Computer Technology, 1993.

[37] A. Sundaram, « An introduction to intrusion detection », Crossroads 2 (1996), no. 4, 3–7.

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

[39] X. Zhan, H. Yuan, and X. Wang, "Research on block chain network intrusion detection system," in Proceedings of the 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA), pp. 191–196, Xi'an, China, September 2019.

[40] C. M. Ou, "Host-based intrusion detection systems inspired by machine learning of agent-based artifcial immune systems," in Proceedings of the 2019 IEEE International Symposium on INnovations in Intelligent SysTems and Applications (INISTA), pp. 1–5, Sofa, Bulgaria, July 2019.

[41] L. Hong, "Immune mechanism based intrusion detectionsystems," in Proceedings of the 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 568–571, Wuhan, China, April 2009.

[42] D. S. Bauer and M. E. Koblentz, "NIDX-an expert system for real-time network intrusion detection," in Proceedings of the 1988 Proceedings. Computer Networking Symposium, pp. 98–106, Washington, DC, USA, August 1988.

[43] H. Lu and J. Yang, "Danger theory of immune systems and intrusion detection systems," in Proceedings of the 2009 International Conference on Industrial Mechatronics and

Automation, pp. 208–211, Chengdu, China, May 2009.
[44] M. E. Pamukov and V. K. Poulkov, “Multiple negative selection algorithm: improving detection error rates in IoT intrusion detection systems,” in Proceedings of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), pp. 543–547, Bucharest, Romania, September 2017.
[45] E. D. Alalade, “Intrusion detection system in smart home network using artifcial immune system and extreme learning machine hybrid approach,” in Proceedings of the 2020 IEEE 6th World Forum on Internet of Tings (WF-IoT), pp. 1-2, New Orleans, LA, USA, June 2020.
[46] Y. Shen, Y. Fei, L. F. Zhang, A. Ji-yao, and M. L. Zhu, “An intrusion detection system based on system call,” in Proceedings of the 2005 1st IEEE and IFIP International Conference in Central Asia on Internet, p. 4, Bishkek, September 2005.
[47] A. Garg and P. Maheshwari, “A hybrid intrusion detection system: a review,” in Proceedings of the 2016 10th InternationalConference on Intelligent Systems and Control (ISCO), pp. 1–5, Coimbatore, India, January 2016.
[48] Hindawi Security and Communication Networks Volume 2023, Article ID 3171334, 10 pages https://doi.org/10.1155/2023/3171334.
[49] E. M. Campos, P. F. Saura, A. Gonzalez-Vidal et al., “Eval- ́uating federated learning for intrusion detection in internet of things: review and challenges,” Computer Networks, vol. 203, Article ID 108661, 2022.
[50] : blockchain la revolution de la confiance , laurent leloup, paris, eyrolles, 2017
[51] : die blockchain – technologie-feld und wirtschaftliche anwendungsbereiche johannes scherk b.sc., mag. gerlinde p¨ochha cker-tr¨oscher, mai 2017
[52] : principes cles d’une application blockchain godebarge ferreol,rossat romain, em lyon business school , decembre 2016.
[53] : music on the blockchain marcus o’dair,2016
[54] :la blockchain, une revolution pour la finance ? leonard beth et annika cayrol 2017
[55] :der blockchain-nebel lichtet sich auch f¨ur die assekuranz christian richter , andre schlieker 2017
[56] : https ://www.industrie-techno.com/article/ces-5-secteurs-que-va-revolutionnerla-blockchain.53233, consulté le 26/10/2020
[57] :blockchain blueprint for a new economy melanie swan, fevrier 2015.
[58] :beginning blockchain bikramaditya singhal, gautam dhameja, priyansu sekhar panda

,2018.

[59] :learning bitcoin richard caetano, november 2015.

[60] Yang, X.M., Li, X., Wu, H.Q. and Zhao, K.Y. 2017. The application model and challenges of blockchain technology in education. Modern Distance Education Research, 2, 34-45

[61] Kumar, N.M. and Mallick, P.K. 2018. Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132(1): 1815-1823

[62] Williams, P. 2019. Does competency-based education with blockchain signal a new mission for universities?. Journal of Higher Education Policy and Management, 41(1): 104-117.

[63] Blockchain Technology and its Types—A Short Review P.K. Paul1*, P.S. Aithal2 , Ricardo Saavedra3 and Surajit Ghosh4

[64] Omar, I.A., Jayaraman, R., Salah, K., Yaqoob, I. and Ellahham, S. 2021. Applications of blockchain technology in clinical trials: Review and open challenges. Arabian Journal for Science and Engineering, 46(4): 3001-3015.

[65] Digital Object Identifier 10.1109/ACCESS.2022.3174052 A Review on Recent Progress of Smart Contract in Blockchain

[66]https://Intelligence_artificielle_Resolution_de.pdf

[67] : https://datascientest.com › intelligence-artificielle-definit..

[68] :Josh Digital https://www.josh-digital.com › 6-avantages-de-intellige..

[69] "Federated Learning: Collaborative Machine Learning without Centralized Training Data" par Google AI. Disponible à : Google AI Blog

[70] NIST Definition of Cloud Computing

[71] Using Federated Artificial Intelligence System of Intrusion Detection for IoT Healthcare System Based on Blockchain Priyanka Tyagi 1 , S.K. Manju bargavi 2 1Computer Science and Engineering, School of Engineering and Technology, Sharda University, Noida, ndia 2Department of CS &IT, Jain (Deemed to be University), Bangalore, India

[72]https://datascientest.com/installer-anaconda-tout-savoir#:~:text=Anaconda%20Navigator%20est%20l'interface,lignes%20de%20code%20de%20Conda.

[73]https://www.databricks.com/fr/glossary/jupyter-notebook#:~:text=Un%20notebook%20Jupyter%20est%20une,et%20d'autres%20ressources%20multim%C3%A9dias.

[74] https://python.sdv.univ-paris-diderot.fr/
[75]https://support.metamask.io/fr/getting-started/getting-started-with-metamask/#:~:text=MetaMask%20est%20une%20extension%20de,des%20applications%20d%C3%A9centralis%C3%A9es%20ou%20dapps.

[76] (en) Afshar, Evangelist et Salesforce, « Ethereum Is The Second Most Valuable Digital Currency, Behind Bitcoin [archive] », *HuffPost*, 17 juillet 2017 (consulté le 10 avril 2019)

[77] « List of contributors [archive] »
[78] https://medium.com/@toure5013/deploier-votre-premier-smart-contract-avec-solidity-remix-ide-ganache-metamak-77eed853feea#:~:text=Remix%20IDE%20est%20une%20application,avec%20des%20interfaces%20graphiques%20intuitives.
[79]https://fr.wikipedia.org/wiki/Microsoft_Word#Les_critiques_du_logiciel
[80]https://www.cointribune.com/lexique/ganache/#:~:text=D%C3%A9finition%20Ganache&text=Environnement%20de%20d%C3%A9veloppement%20personnel%20utilis%C3%A9,intelligents%20Ethereum%20en%20mode%20local.
[81] https://fr.wikipedia.org/wiki/Pandas
[82]https://fr.wikipedia.org/wiki/Firebase