REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE IBN KHALDOUN - TIARET

MEMOIRE

Présenté à :

FACULTÉ DES MATHEMATIQUES ET D'INFORMATIQUE
DÉPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

MASTER

Spécialité : Réseaux et Télécommunications

Par :

KEDDI MANEL
MAARADJI BOCHRA

Sur le thème

Apprentissage profond pour la détection d'intrusions dans l'IoMT

Soutenu publiquement à Tiaret devant le jury composé de :

Mr Bekkar khaled	Grade Université M.A.A	Président
Mr Alem Abdelkader	Grade Université M.A.A	Encadrant
Mr Bouguessa Abdelkader	Grade Université M.A.A	Examinateur

2024-2025

Dédicace

À ceux qui ont semé en moi la confiance, à ceux dont les invocations ont été la source de ma persévérance et de ma réussite…

À mes parents, le battement de mon cœur,Ma gratitude éternelle pour leur amour, leurs sacrifices et leur patience.

À mes frères et sœurs, Le soutien de l'âme et les compagnons du chemin.

À mes véritables amis, Ceux qui ont adouci les difficultés du parcours Et ont été une lumière dans les moments d'épuisement.

À mon amie chère Manel,Pour sa présence sincère et son soutien constant.

À tous ceux qui m'ont soutenue par un mot, un sourire, ou un silence réconfortant…

Je dédie ce travail modeste comme un gage de fidélité et de profonde reconnaissance.

- Bochra

Dédicace

À mes chers parents, qui ont fait tous les sacrifices et m'ont comblée d'amour et de tendresse, leurs prières sincères m'accompagnant tout au long de mon parcours académique.

À mes chers frères : Amine, Zakaria et Khaled,et ma sœur djouher qui ont toujours été mon soutien et mes piliers à chaque étape

Àtoute ma famille, source de joie et de force.

À mon amie fidèle Maaradji Bouchra, avec qui j'ai partagé tous les moments d'études, des cours aux balades dans les couloirs de l'université, une amie qui m'a toujours soutenue et encouragée à chaque pas.

À tous mes amis et camarades, dont la compagnie a enrichi ce voyage.

À tous ceux qui ont eu un impact positif dans ma vie, qu'il soit petit ou grand.

À mon encadrant Bouazza Abdelhamide , ainsi qu'à mes collègues, pour leur compréhension et leur soutien qui ont été d'une grande importance dans l'accomplissement de ce travail.

- Manel

Remerciements

Avant toute chose, nous remercions Allah, le Tout-Puissant, qui nous a accordé la force, la patience et la persévérance nécessaires pour mener à bien ce travail.

Nous exprimons notre profonde gratitude à toutes les personnes qui nous ont soutenus, conseillés ou encouragés tout au long de ce parcours académique.

Nous adressons nos sincères remerciements à notre encadrant, le Dr. ***Alem Abdelkader****, pour avoir accepté d'encadrer ce travail, pour sa confiance, ses orientations générales, ainsi que pour son suivi tout au long du projet.*

Nous tenons à exprimer une reconnaissance particulière à Mr. ***Bouazaa Abdelhamid****, dont le soutien concret, les remarques pertinentes et la disponibilité constante ont été des facteurs déterminants dans l'avancement et la réalisation de ce mémoire. Nous saluons également sa grande courtoisie et son attitude respectueuse tout au long de cette collaboration.*

Nous remercions également l'ensemble des enseignants qui nous ont transmis leur savoir et contribué à notre formation académique durant toutes ces années.

Nous saluons aussi la qualité de l'enseignement reçu tout au long de notre parcours, qui a enrichi notre réflexion et renforcé notre approche scientifique. C'est pourquoi nous leur adressons notre gratitude la plus sincère.

Nous tenons également à exprimer notre reconnaissance aux membres du jury pour le temps qu'ils ont consacré à l'évaluation de ce mémoire, ainsi que pour leurs remarques constructives et enrichissantes.

Nos remerciements vont aussi à toute personne ayant eu la bonté et la patience de satisfaire notre curiosité et de nous aider dans notre travail par leurs conseils ou leur présence.

Enfin, nous exprimons notre reconnaissance profonde à nos familles et à toutes les personnes qui nous ont soutenus moralement au cours de cette aventure.

Résumé

L'Internet des Objets Médicaux (IoMT) constitue un réseau sophistiqué d'appareils médicaux interconnectés, dédiés à la collecte et à l'échange en temps réel de données médicales critiques. Cette technologie promet d'améliorer substantiellement la qualité des soins aux patients tout en réduisant notablement les coûts associés. Cependant, l'adoption rapide et massive de l'IoMT soulève des défis majeurs en matière de sécurité, pouvant compromettre l'intégrité des données médicales ainsi que la sécurité des patients en raison des vulnérabilités dans les flux d'informations. Pour répondre efficacement à ces enjeux, ce travail propose une approche combinant des réseaux neuronaux récurrents à mémoire longue et court terme (LSTM) avec une stratégie d'apprentissage fédéré basée sur la protection de la confidentialité des données. Ce modèle tire parti des caractéristiques temporelles intrinsèques du trafic réseau afin d'identifier précisément les comportements anormaux révélateurs d'intrusions, tout en assurant une confidentialité accrue grâce à une collaboration décentralisée entre divers dispositifs médicaux connectés. Les résultats expérimentaux démontrent que l'intégration du modèle LSTM avec l'apprentissage fédéré permet d'atteindre une précision élevée dans la détection des intrusions, tout en réduisant considérablement les fausses alertes comparativement aux méthodes conventionnelles. Ces performances soulignent le potentiel remarquable de cette approche pour renforcer efficacement la cybersécurité des réseaux IoMT, garantissant ainsi une protection optimale et rigoureuse des données médicales sensibles.

Mots clés : Internet des Objets Médicaux, cybersécurité, apprentissage profond, réseaux LSTM, apprentissage fédéré, confidentialité.

Abstract

The Internet of Medical Things (IoMT) represents a sophisticated network of interconnected medical devices dedicated to collecting and exchanging critical medical data in real-time. This technology promises significant improvements in patient care quality while substantially reducing associated costs. However, the rapid and widespread adoption of IoMT raises major security challenges, potentially compromising medical data integrity and patient safety due to vulnerabilities in information flows. To effectively address these issues, this work proposes an approach combining Long Short-Term Memory (LSTM) recurrent neural networks with a federated learning strategy focused on data privacy protection. The model leverages the intrinsic temporal characteristics of network traffic to accurately identify abnormal behaviors indicative of intrusions, while ensuring enhanced confidentiality through decentralized collaboration among various connected medical devices. Experimental results demonstrate that integrating the LSTM model with federated learning achieves high accuracy in intrusion detection, significantly reducing false alarms compared to traditional methods. These outcomes highlight the remarkable potential of this approach to effectively strengthen IoMT network cybersecurity, thus ensuring rigorous and optimal protection of sensitive medical data.

Keywords : Internet of Medical Things, cybersecurity, deep learning, LSTM networks, federated learning, privacy.

ملخص

تمثل إنترنت الأشياء الطبية (IoMT) شبكة متطورة من الأجهزة الطبية المتصلة التي تعمل على جمع وتبادل البيانات الطبية الحيوية بشكل فوري ومستمر. تقدم هذه التكنولوجيا فرصة كبيرة لتحسين جودة الخدمات الصحية المقدمة للمرضى، بالإضافة إلى تخفيض ملحوظ في التكاليف المرتبطة بالرعاية الصحية. ومع ذلك، فإن التوسع السريع في استخدام هذه التقنية يطرح تحديات أمنية كبيرة، قد تؤدي إلى تهديد سلامة وأمن بيانات المرضى نتيجة وجود تهديدات أمنية. لمواجهة هذه التحديات، يقدم هذا البحث منهجية تجمع بين الشبكات العصبية المتكررة ذات الذاكرة الطويلة والقصيرة المدى (LSTM)، واستراتيجية التعلم الاتحادي التي تركز على حماية خصوصية البيانات. يستفيد النموذج المقترح من النمط الزمني المميز لحركة البيانات في الشبكة لتحديد السلوكيات الشاذة التي قد تشير إلى محاولات اختراق بدقة عالية، مع ضمان حماية أفضل للخصوصية من خلال الاعتماد على التعاون اللامركزي بين الأجهزة الطبية المتصلة. أكدت النتائج التجريبية أن دمج نموذج LSTM مع استراتيجية التعلم الاتحادي يحقق نتائج دقيقة وموثوقة في اكتشاف محاولات الاختراق، كما يسهم بشكل فعال في الحد من الإنذارات الكاذبة مقارنة بالأساليب التقليدية. تعكس هذه النتائج الإمكانات الكبيرة للمنهج المقترح في تعزيز الأمن السيبراني لشبكات IoMT، مما يضمن توفير حماية قوية ومثلى للبيانات الطبية الحساسة.

كلمات مفتاحية :
إنترنت الأشياء الطبية، الأمن السيبراني، التعلم العميق، التعلم الاتحادي، الخصوصية

Table des matières

Table des figures

Liste des tableaux

Liste des sigles et acronymes

IOT	*internet of things.*
IOMT	*internet of medical things.*
RFID	*Radio Frequency Identification.*
WSN	*wireless sensor network.*
NFC	*Near Field Communication*
BLE	*Bluetooth Low Energy*
UWB	*Ultra Wideband*
Wi-Fi	*Wireless Fidelity*
Zigbee	*Zigbee Protocol*
6LoWPAN	*IPv6 over Low power Wireless Personal Area Networks*
LoRaWAN	*Long Range Wide Area Network*
HL7	*Health Level Seven*
CoAP	*Constrained Application Protocol*
MQTT	*Message Queuing Telemetry Transport*
HTTP	*HyperText Transfer Protocol*
DoS	*Denial of Service*
DDoS	*Distributed Denial of Service*
MITM	*Man In The Middle*
RSA	*Rivest-Shamir-Adleman*
ECC	*Elliptic Curve Cryptography*
IDES	*Intrusions Detection Expert System.*

IDS *Intrusions Detection System.*

HIDS *Host Intrusion Detection System.*

NIDS *Network Intrusion Detection System.*

DMZ *Zone Démilitarisée.*

IA *Intelligence artificielle.*

ML *Machine learning.*

DL *Deep learning.*

LSTM *Long Short-Term Memory.*

GRU *Gated Recurrent Unit.*

FL *Federated Learning.*

Introduction générale

Les dernières décennies ont été marquées par une transformation majeure dans le domaine technologique, caractérisée par une accélération significative de l'innovation et l'adoption généralisée de solutions intelligentes, notamment dans les technologies de communication et les systèmes interconnectés. Cette évolution a favorisé l'émergence du concept d'Internet des Objets (IoT), transformant profondément les modes d'interaction avec l'environnement grâce à l'intégration des technologies numériques dans le quotidien. Parmi les applications les plus remarquables de l'IoT se distingue particulièrement l'Internet des Objets Médicaux (IoMT).

L'IoMT a radicalement transformé le secteur de la santé par l'introduction de dispositifs médicaux connectés et de capteurs intelligents permettant un suivi continu et à distance des patients. Cette technologie facilite une surveillance efficace au sein des hôpitaux intelligents, à travers l'utilisation de dispositifs portables, d'applications mobiles dédiées à la santé, ainsi que de solutions de télémédecine. Elle contribue ainsi significativement à l'amélioration de l'éducation sanitaire, à la gestion proactive des maladies, et à l'optimisation globale de la qualité des soins médicaux.

Toutefois, cette adoption rapide et massive de l'IoMT engendre des défis critiques en matière de cybersécurité. Le secteur médical, en particulier, constitue l'une des principales cibles des cyberattaques, menaçant directement l'intégrité et la confidentialité des données sensibles des patients. La connectivité permanente de ces dispositifs médicaux expose ces systèmes à divers risques tels que l'interception, la manipulation et la divulgation non autorisée des données.

Face à ces menaces croissantes, les systèmes de détection d'intrusion (IDS) s'imposent comme des solutions essentielles permettant d'identifier et de neutraliser efficacement les activités malveillantes. L'émergence des techniques d'intelligence artificielle, notamment celles basées sur l'apprentissage profond, offre de nouvelles perspectives pour améliorer considérablement l'efficacité et la précision de ces systèmes. Cependant, la mise en œuvre de modèles performants nécessite généralement une grande quantité de données centralisées, ce qui soulève d'importantes préoccupations relatives à la confidentialité et à la conformité avec des réglementations telles que le RGPD et la HIPAA.

Dans ce cadre, l'apprentissage fédéré constitue une alternative pertinente, permettant d'entraîner les modèles de manière collaborative et décentralisée sans nécessité de partager les données brutes, renforçant ainsi la confidentialité des informations sensibles. Ce mémoire propose de concevoir et d'évaluer un système IDS utilisant les réseaux neuronaux récur-

rents à mémoire longue et court terme (LSTM) combinés à une approche d'apprentissage fédéré via l'algorithme FedAVG, afin de renforcer simultanément la sécurité et la confidentialité dans les environnements IoMT.

Le mémoire est structuré en quatre chapitres principaux :

- **Chapitre 1 :** Présentation approfondie de l'IoMT, ses définitions, composants matériels, applications, défis sécuritaires et exigences telles que l'informatique en périphérie (Edge Computing).
- **Chapitre 2 :** Analyse détaillée des systèmes IDS, leurs caractéristiques, classifications, mécanismes opérationnels et critères d'évaluation des performances.
- **Chapitre 3 :** Exploration des méthodes avancées d'intelligence artificielle et d'apprentissage profond adaptées à la détection d'intrusions, avec une attention particulière portée sur l'apprentissage fédéré.
- **Chapitre 4 :** Présentation concrète de la méthodologie expérimentale incluant la préparation des données, la mise en œuvre des modèles sélectionnés, et une évaluation exhaustive de leurs performances.

Chapitre 1

internet des objets médicaux

1.1 Introduction

La technologie IoMT est un domaine en évolution rapide, largement exploité dans une vaste gamme d'applications liées à la santé. Il s'agit d'une combinaison de dispositifs médicaux et de l'Internet des objets (IoT) (fig. 1.1). Chaque dispositif médical est connecté et surveillé en ligne par des professionnels de la santé. L'un de ses principaux avantages est sa capacité à fournir une surveillance à distance, en temps réel et continue, de l'état de santé du patient, permettant ainsi des soins plus rapides et moins coûteux, tout en améliorant le diagnostic et en fournissant des solutions de santé efficaces.

Bien que l'IoMT offre des services de soins de santé efficaces et fiables, elle présente également des risques, notamment une faible protection en matière de sécurité et des fuites potentielles de données médicales, portant atteinte à la vie privée des patients. De plus, les ressources informatiques sont limitées en raison de la capacité et de la mémoire restreintes des capteurs médicaux.

Ce chapitre présente les concepts fondamentaux de l'IoMT, en clarifiant l'infrastructure de cette technologie, ses principales applications dans le domaine médical, les défis auxquels elle est confrontée, ainsi que les évolutions des protocoles de sécurité, des technologies utilisées et des solutions innovantes visant à renforcer le niveau de protection.

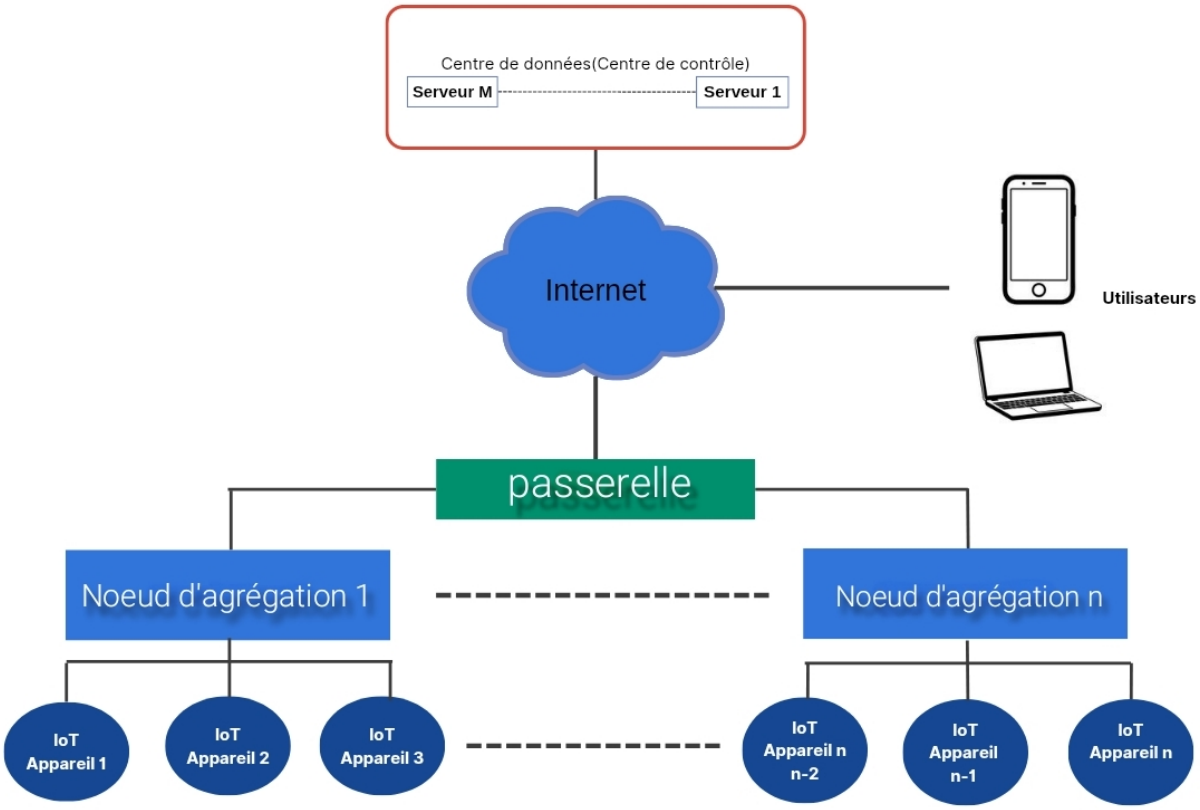


Fig. 1.1 : Modèl du système IOMT multimédia [1]

1.2 Internet des Objets (IoT)

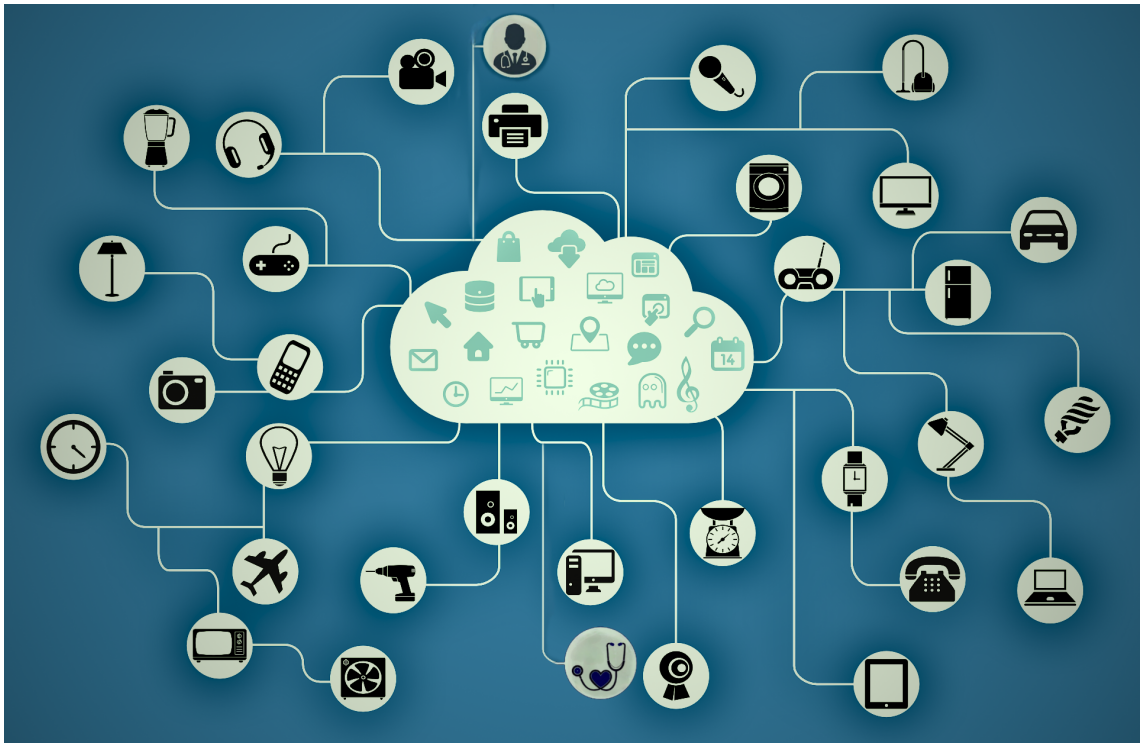


Fig. 1.2 : Internet des Objets (IoT)

L'Internet des Objets (IoT) représente un nouveau paradigme technologique visant à connecter des objets physiques tels que :les capteurs, les actionneurs et les appareils intelligents à Internet. Cette connectivité leur permet de collecter, analyser et partager des données, voire d'agir de manière autonome ou semi-autonome sans intervention humaine directe.

Le terme « Internet of Things » a été utilisé pour la première fois en 1999 par Kevin Ashton, dans un contexte lié à la gestion des chaînes d'approvisionnement. Grâce à l'évolution rapide de technologies telles que la RFID, les réseaux de capteurs sans fil et l'informatique en nuage (cloud computing), cette idée est rapidement passée du concept théorique à une réalité technologique concrète.

L'architecture de l'IoT repose généralement sur trois couches fondamentales : la couche physique (composée des capteurs et actionneurs), la couche intergicielle (middleware), qui assure le traitement et le stockage des données, et enfin la couche de présentation, dédiée à la visualisation et à l'analyse des informations.

En 2011, le nombre de dispositifs connectés a dépassé celui des êtres humains sur Terre. Selon une étude publiée en 2013, il était prévu que ce nombre atteigne 24 milliards d'ici 2020 ,un seuil qui a effectivement été dépassé, confirmant ainsi la croissance exponentielle des technologies liées à l'IoT dans des domaines variés tels que la santé, les transports, les villes intelligentes et l'industrie.

En raison de la diversité croissante des applications de l'IoT, plusieurs sous-domaines spécialisés ont émergé. Parmi les plus importants figure l'Internet des Objets Médicaux (IoMT), qui désigne l'application des technologies IoT dans le domaine de la santé [2].

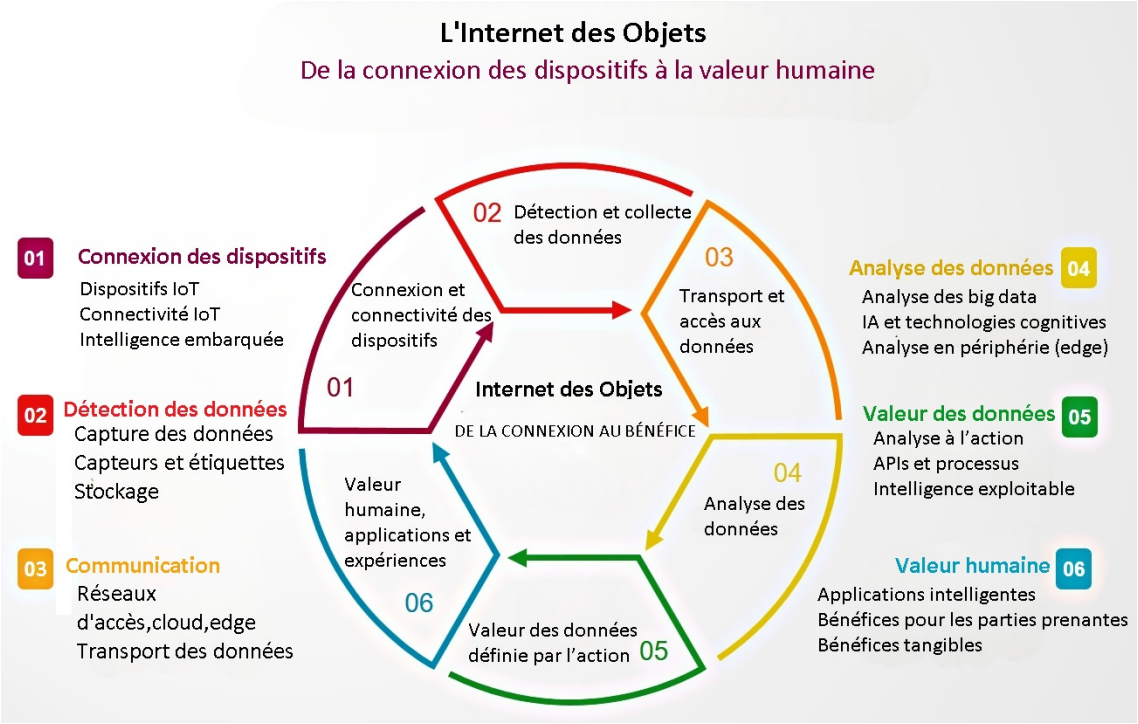


FIG. 1.3 : Les étapes du cycle de vie de L'internet des Objets (IoT)

1.3 Définition de l'Internet des objets médicaux (IoMT)

L'Internet des Objets Médicaux (IoMT) désigne un réseau de dispositifs médicaux connectés sans fil, d'applications logicielles et de technologies numériques utilisées dans le domaine des soins de santé. Il permet la collecte de données cliniques en temps réel auprès des patients, leur transmission aux professionnels de santé et leur intégration dans les systèmes hospitaliers pour un suivi continu et intelligent.

Ces dispositifs reposent sur des technologies avancées telles que le cloud computing, permettant de stocker, traiter et analyser de vastes volumes de données médicales en temps réel. L'IoMT contribue ainsi à améliorer la qualité des soins en facilitant la prise de décision fondée sur les données, en optimisant la surveillance des patients, en renforçant l'efficacité des traitements et en réduisant les coûts globaux.

Ces dernières années, l'IoMT a connu une expansion remarquable, devenant une composante essentielle de l'infrastructure de santé dans de nombreux établissements à travers le monde. Comme illustré dans la figure 1.4, ce système met en évidence l'interaction intelligente entre les patients et les dispositifs médicaux, créant un environnement numérique intégré qui soutient activement l'amélioration des services médicaux [3].

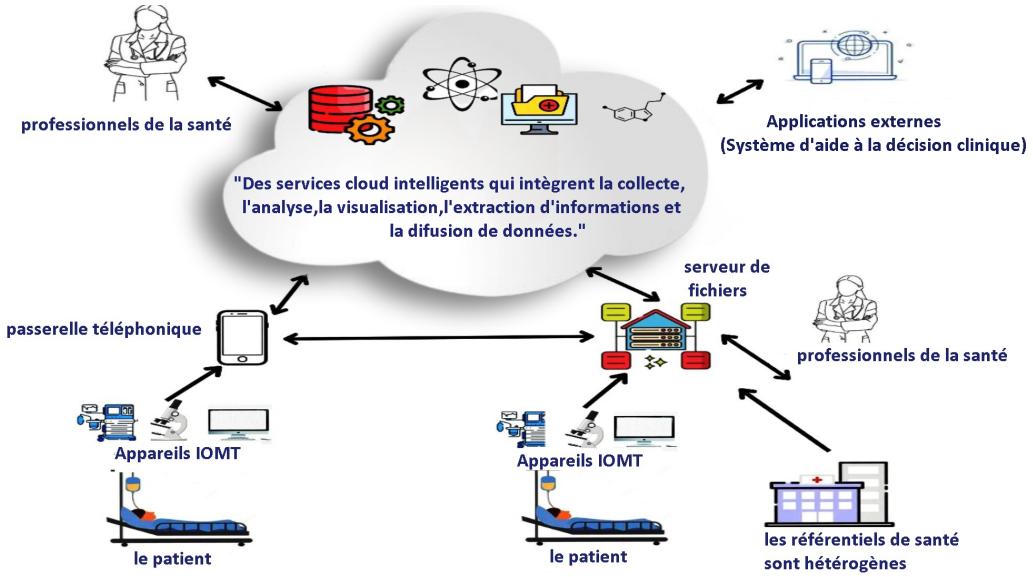


FIG. 1.4 : Internet des objets médicaux
[3]

1.4 Types de dispositifs IOMT

Les dispositifs médicaux jouent un rôle fondamental au sein des systèmes de santé intelligents, car ils répondent à des besoins spécifiques. Nombre d'entre eux sont disponibles sur le marché médical ou utilisés dans les hôpitaux pour une surveillance intelligente à distance et en temps réel[4].

1.4.1 Les dispositifs portables et les dispositifs personnalisés

Ces appareils intelligents collectent et surveillent les données physiologiques vitales. Ils incluent notamment : citer[4] :

→ **Appareils de fitness intelligents :** utilisés pour surveiller l'activité physique et aider à adopter un mode de vie sain, en s'adaptant aux capacités physiques du patient.

→ **Tensiomètres intelligents :** comme *Omron EVOLV* ou *Philips Upper Arm BPM*, permettent une surveillance précise et immédiate de la pression artérielle, facilitant une détection rapide des anomalies.

→ **Les dispositifs de mesure de la glycémie :** utilisés notamment par les patients diabétiques pour surveiller le taux de sucre dans le sang. Des exemples incluent *GlucoWise* et *iBGStar*, souvent connectés à des smartphones. En cas de baisse d'insuline, ces dispositifs déclenchent automatiquement une injection via pompe à insuline.

→ **Les appareils de suivi alimentaire :**destinés aux patients atteints de troubles alimentaires, ils fournissent des recommandations nutritionnelles personnalisées et des notifications automatiques.

→ **moniteurs de fréquence cardiaque intelligents :** surveillent le rythme cardiaque pour détecter les anomalies ou prédire une crise cardiaque. Ils intègrent souvent des réseaux de capteurs corporels sans fil.

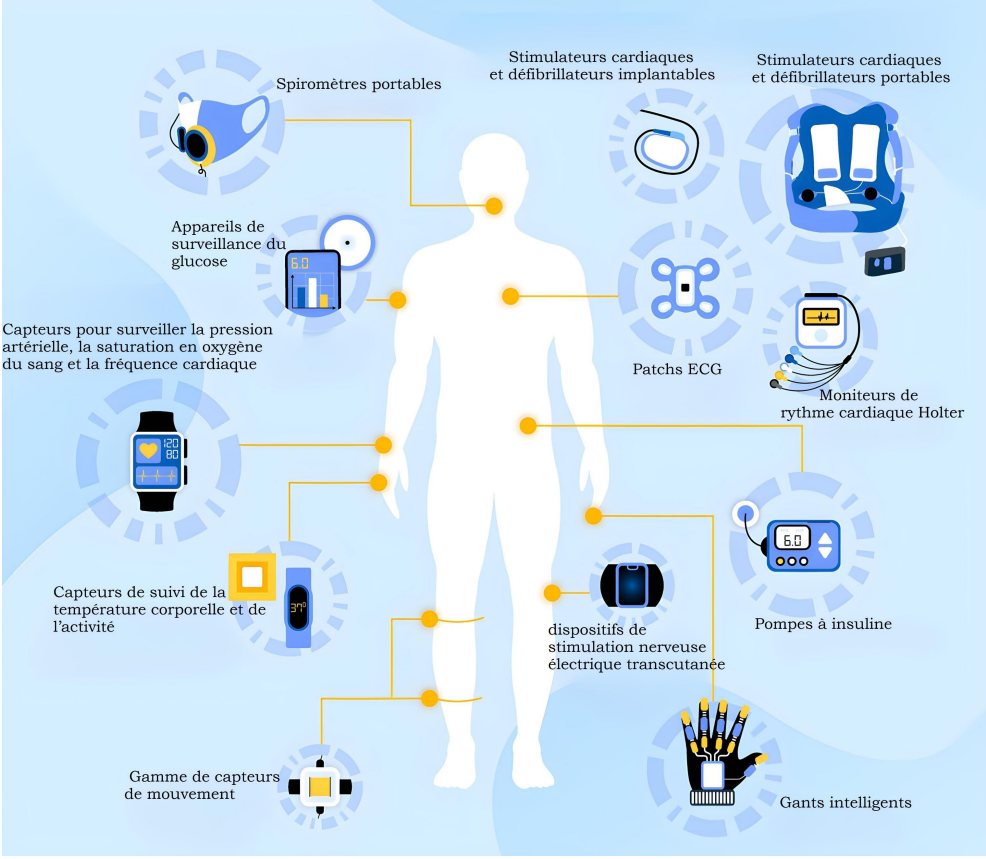


FIG. 1.5 : Exemple de dispositifs portables pour la surveillance de la santé IOMT [5]

1.4.2 Les dispositifs médicaux à domicile

Ces dispositifs sont utilisés en dehors des hôpitaux et permettent une surveillance médicale à distance. Ils exploitent des technologies simples (Internet, e-mail, objets connectés) pour communiquer avec les établissements de santé. On peut citer [4] :

→ Appareils respiratoires.

→ Pompes à injection.

→ Appareils de dialyse.

→ Équipement de premiers secours.

→ Équipements de nutrition, équipements d'urination.

→ Équipements de soins pédiatrique.

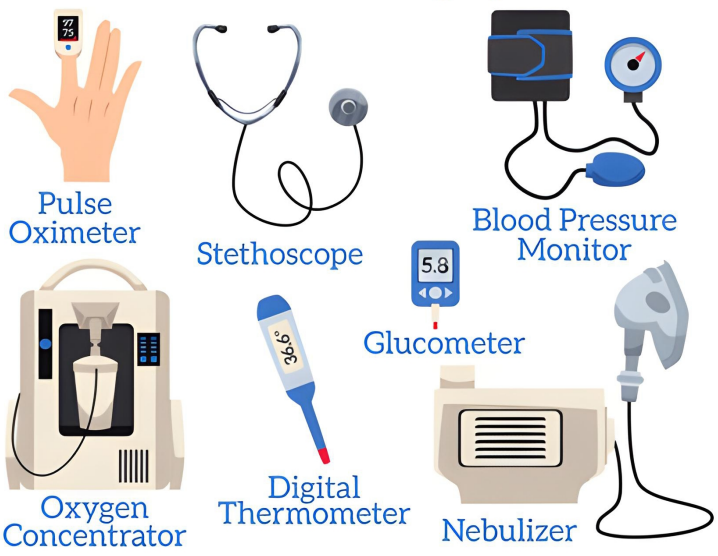


FIG. 1.6 : Exemple de dispositifs médicaux à domicile

1.4.3 Dispositifs médicaux dans les hôpitaux

Utilisés dans les hôpitaux et cliniques, ces dispositifs doivent répondre à des exigences strictes pour gérer des situations critiques. Parmi les plus courants, on trouve [4] :

→ Défibrillateurs.

→ Matériel d'anesthésie.

→ Appareils de surveillance des patients.

→ Appareil d'électrocardiographes (ECG).

→ Tables d'opération et systèmes de chauffages.

→ électrochirurgicales et dispositifs d'éclairage

Application médicales	taux de donnés	les bandes passantes	précision
ECG(12 dérivatin)	288 kbps	100-1000 HZ	12bits
ECG(6 dérivatin)	71 kbps	100-500 HZ	12bits
EMG	320 kbps	0-10000 HZ	16bits
EEG (12 dérivatin)	43,2 kbps	0-150 HZ	12bits
saturation sanguine	16 kbps	0-1 HZ	8bits
surveillance du glucose	1600 kbps	0-50 HZ	16bits
température	120 kbps	0-1 HZ	8bits
capture de mouvement	35 kbps	0-500 HZ	12bits

TAB. 1.1 : exemples concret illustrant spécification des dispositif médicaux [6]

1.5 Domaines d'application de l'IoMT

- **Médecin intelligent :** L'un des projets d'avenir vise à développer des robots capables de remplir les fonctions d'un véritable médecin, notamment en matière de diagnostic, de surveillance et d'interaction avec les patients.
- **infirmiers intelligents :** L'utilisation de robots pour exécuter des tâches infirmières devient de plus en plus fréquente. Dans certains cas, des assistants infirmiers intelligents peuvent effectuer plusieurs fonctions de soins, bien que leur usage reste limité.
- **Réceptionniste intelligent :** Des robots capables d'accueillir les patients, comprendre leurs besoins médicaux, répondre aux appels téléphoniques et gérer les rendez-vous sont en cours de développement.
- **Technologies médicales intelligentes :** Des équipements médicaux intelligents sont utilisés pour apporter une assistance immédiate, notamment à travers des drones médicaux capables d'intervenir rapidement en cas d'urgence (ex. arrêt cardiaque), ou pour effectuer certaines opérations chirurgicales. La réalité virtuelle et augmentée ainsi que l'IA sont aussi employées pour l'entraînement médical ou l'analyse biochimique.
- **Surveillance des patients en temps réel :** La surveillance à distance permet un suivi continu, rentable et réactif des patients. Elle comprend la mesure de plusieurs biomarqueurs tels que le niveau de forme physique, la glycémie, la fréquence respiratoire et la fréquence cardiaque. Parmi les exemples récents figurent les inhalateurs intelligents ou encore les montres connectées (comme l'Apple Watch) utilisées pour surveiller les symptômes de dépression [7] . Ce type d'application est déjà en usage dans de nombreux hôpitaux et foyers[4].
- **Caméras en capsules à avaler :** Ces capsules médicales de pointe, équipées de caméras miniatures, permettent une visualisation en temps réel des organes internes pour la détection précoce de maladies chroniques. Elles reposent sur des technologies avancées comme les capsules à rayons X ou les dispositifs endoscopiques à avaler basés sur des hydrogels [4].
- **Systèmes personnels d'intervention d'urgence :** Il s'agit de solutions innovantes permettant l'envoi d'alertes instantanées en cas d'urgence médicale (AVC, crise cardiaque, etc.), grâce à la transmission des signes vitaux vers un centre hospitalier. Un exemple : la ceinture intelligente ActiveProtective, portée à la taille, utilise le Bluetooth et l'intelligence artificielle pour transmettre les données en temps réel[4].

1.6 Communications de l'Internet des objets médicaux

Les données sont transférées en temps réel entre les dispositifs médicaux via quatre types principaux de réseaux de communication[4] :

Type de réseau	Description
Réseau de captures corporels (BAN)	Les signaux vitaux des patients sont collectés à l'aide d'un dispositif portable ou d'un capteur mobile, vers l'unité de contrôle soit via un smartphone vers le centre de données médical, soit en utilisant un appareil médical sans fil via des protocoles tels que Zigbee, Bluetooth ou WI-FI (fig 1.6).
Réseau de zone domestique (HAN)	utilisé pour collecter des données à l'intérieur de la maison du patient et les envoyer à un point d'accès disponible (AP), les transmissions peuvent dépendre d'un réseau Wi-Fi ou LTE.
Réseau de zone de voisinage (NAN)	permet aux utilisateurs de se connecter rapidement à Internet. Il est utilisé pour créer des connexions sans fil entre les zones proches comme les maisons et leurs quartiers, dans une seule portée.
Réseau étendus	le réseau étendu est un moyen de transmettre des données en temps réel aux équipes d'intervention d'urgence. Une fois reçu, le point d'accès peut également envoyer des données aux services en nuage à des fins de stockage.

Tab. 1.2 : les Types de réseaux de comunication (IoMT)

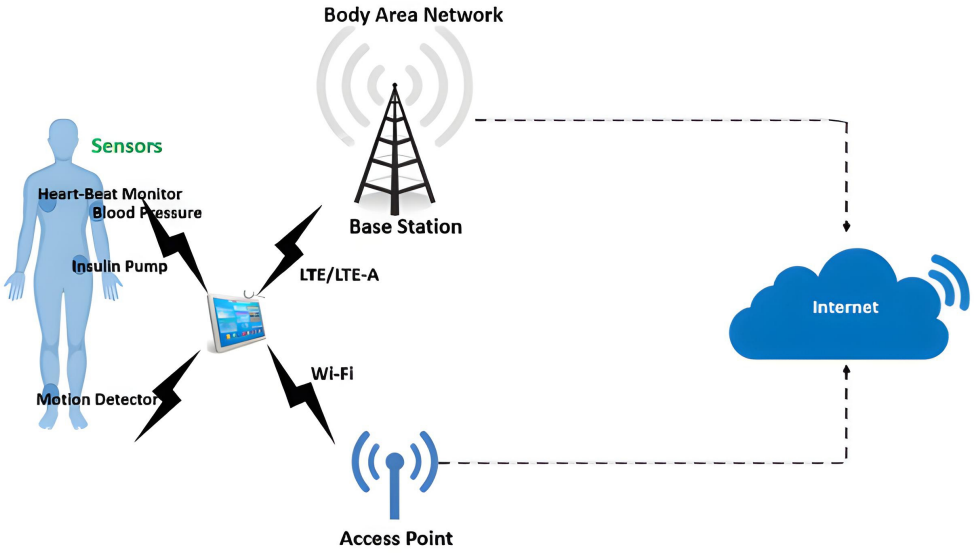


Fig. 1.7 : Réseau de captures corporels (BAN)
[4]

1.7 Architecture de L'IoMT

1.7.1 Architecture à trois couches

De nombreux chercheurs ont proposé des architectures qui peuvent être appliquées à l'internet des objets. Parmi les architectures les plus importantes, citons l'architecture IoT, l'architecture EPCglobal, l'architecture basée sur les réseaux de capteurs, l'architecture autonome et l'architecture machine à machine .

L'architecture M2M couvre certains contenus connexes de l'EPCglobal et du réseau de capteurs sans fil (WSN) et est l'architecture la plus largement utilisée dans le domaine de l'IoT.

Dans le domaine médical, l'IoT adopte une architecture centralisée à trois niveaux : la couche de perception, la couche réseau, et la couche d'application . Cette structure constitue la base fonctionnelle de l'Internet des Objets Médicaux (IoMT)[8].

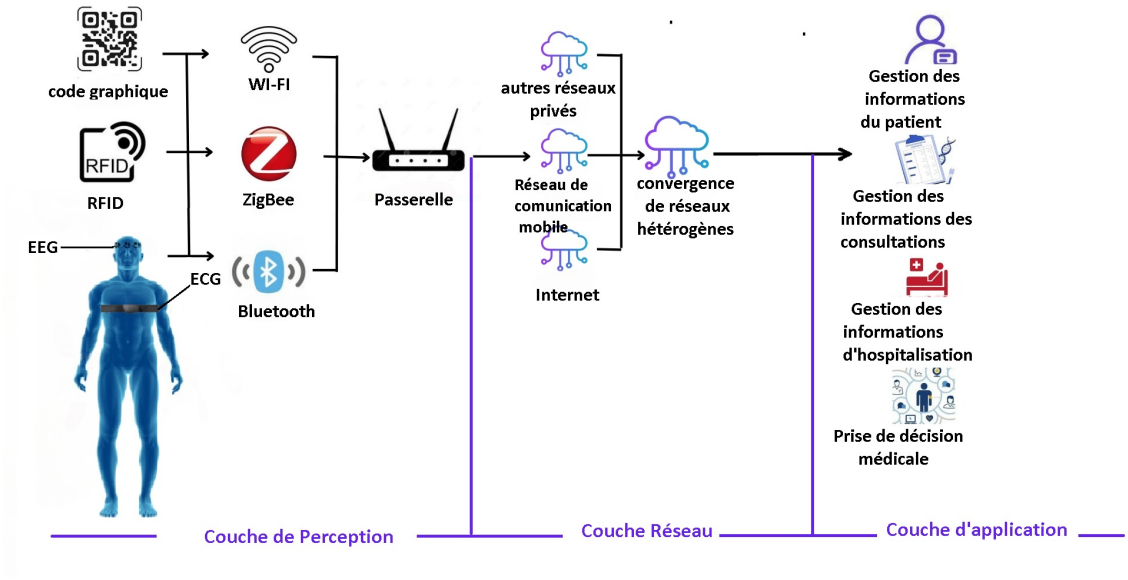


Fig. 1.8 : Architecture IOMT (3 couches)
[9]

1.7.2 Couche perceptuelle

Il s'agit de la couche fondamentale de l'IoMT. Elle est responsable de la collecte des données médicales à partir de diverses sources et de leur transmission vers les couches supérieures pour traitement. Elle se compose de deux sous-couches :

1. **la couche de collecte des données :**
   est basée sur un réseau de dispositifs intelligents et de capteurs spécialisés tels que des capteurs physiologiques et chimiques, ainsi que sur les technologies RFID la reconnaissance d'images Toutes les données et tous les appareils identifiés dans le

réseau sont transformés en systèmes cyber-physique (CPS) intelligents et faciles à interagir. Il existe trois principaux types de CPS dans l'IdO : CPS Passif , CPS actif , CPS Internet .

2. **Sous-couche d'accès aux données :**
   Collecte les données des capteurs et les transmet à la couche réseau à l'aide de technologies de transport telles que :
   Bluetooth , Wi-Fi , ZigBee.Cette technologie doit être choisie en fonction des caractéristiques environnementales réelles des dispositifs médicaux de l'IdO et besoins.

1.7.3 Couche réseau

La couche réseau est divisée en deux sous-couches :

1. **Couche de transfert de données :** Il remplit une fonction similaire à celle du système nerveux humain . Il s'appuie sur les réseaux de communication mobiles, Internet, ainsi que sur des réseaux spécialisés pour transmettre les données collectées à partir de la première couche de perception en temps réel, de manière précise et fiable. Il vise à assurer une communication fluide entre les différents organes et systèmes.

2. **Couche de service :** Cette couche est considérée comme l'intégrative intelligente du système, elle est destinée à intégrer des réseaux hétérogènes et à normaliser les formats de données et leurs descriptions. Son objectif principal est de permettre une intégration efficace des systèmes existants et des technologies modernes, à adapter aux environnements hospitaliers.

1.7.4 Couche d'application

La couche d'application se compose de deux niveaux fonctionnels :

1. **Applications de gestion de l'information médicale :** Ce niveau comprend la gestion des informations sur les équipements et fournitures médicales, la gestion des données des patients, ainsi que les informations liées aux consultations des cliniques externes et aux soins hospitaliers.

2. **Applications de soutien à la décision médicale :**
   Ce niveau est consacré à l'analyse des informations sur les patients, à l'évaluation des données sur les maladies, à l'analyse des traitements médicamenteux, ainsi qu'à l'interprétation des données diagnostiques et thérapeutiques, dans le but de soutenir une prise de décision clinique efficace basée sur les données.

1.7.5 Technologies de L'IOMT

Les systèmes de santé intelligents basés sur l'IoMT reposent sur un ensemble de technologies avancées permettant la collecte, la transmission et l'analyse des données médicales. Parmi les plus essentielles, on retrouve : [8] :

Identification par radiofréquence (RFID) : est une technologie utilisées pour l'identification sans contact des patients, du personnel médical et des équipements. Elle repose sur l'usage d'ondes radio pour transférer des données entre une étiquette électronique, un lecteur RFID et un système de gestion centralisé. Dans le contexte médical, elle est utilisée pour :

- Le suivi des équipements médicaux,
- L'identification automatique des patients,
- La surveillance des paramètres vitaux comme l'ECG ou la pression artérielle.

Sa capacité à fonctionner sans ligne de visée directe et sa résistance aux interférences la rendent particulièrement adaptée aux environnements hospitaliers complexes.

Réseau de capteurs sans fil (WSN) : Les WSN permettent la surveillance en temps réel de l'état physiologique des patients grâce à des capteurs distribués dans l'environnement. Chaque nœud de capteur intègre :

- Un microcontrôleur,
- Des interfaces de collecte (température, pression, mouvement),
- Un module de communication sans fil,
- Et une alimentation autonome.

Ces réseaux permettent une collecte continue et à faible coût des données de santé, favorisant la réactivité dans la prise de décision clinique.

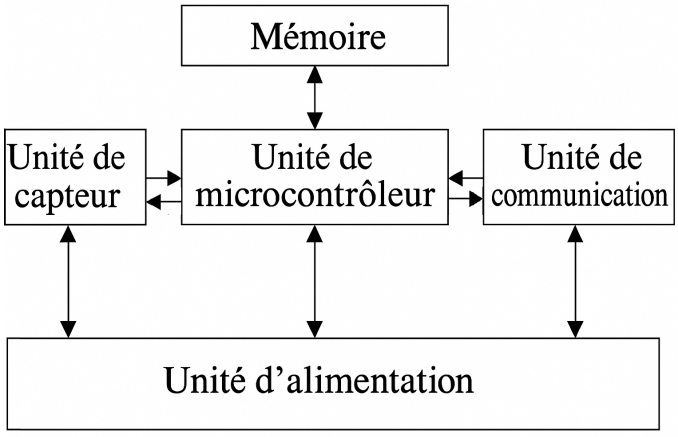


Fig. 1.9 : Architecture (WSN)
[10]

Le middleware : Le middleware joue un rôle clé dans l'Internet des objets (IoT) et, plus particulièrement, dans l'Internet des objets médicaux (IoMT). Il constitue l'interface entre les dispositifs intelligents (capteurs, lecteurs RFID, etc.) et les systèmes dorsaux (comme les bases de données ou les applications hospitalières).

Il remplit plusieurs fonctions essentielles :

- Faciliter l'intégration entre les différents composants du système,
- Assurer le traitement en temps réel des données issues des capteurs : filtrage, agrégation et transmission.
- Garantir une communication efficace entre les dispositifs médicaux et les systèmes d'information.

Les intergiciels (middleware) reposent sur des protocoles et interfaces standardisés, ce qui permet leur adaptation à diverses applications médicales, telles que :

- le transfert d'informations du dossier médical électronique (DME),
- la gestion des ressources humaines médicales,et la gestion des équipements.

Compte tenu de la diversité des sources de données et de la complexité de l'environnement IoMT, il devient nécessaire d'adopter des intergiciels sémantiques. Ces derniers allient le traitement classique à une compréhension sémantique des données, afin d'améliorer la compatibilité et l'harmonisation entre les composants du système.

1.7.6 Architecture à quatre couches

L'architecture de l'IoMT est généralement divisée en quatre couches principales, englobant tout le processus allant de la collecte des données biométriques à leur stockage et visualisation. Elle comprend :[11] :

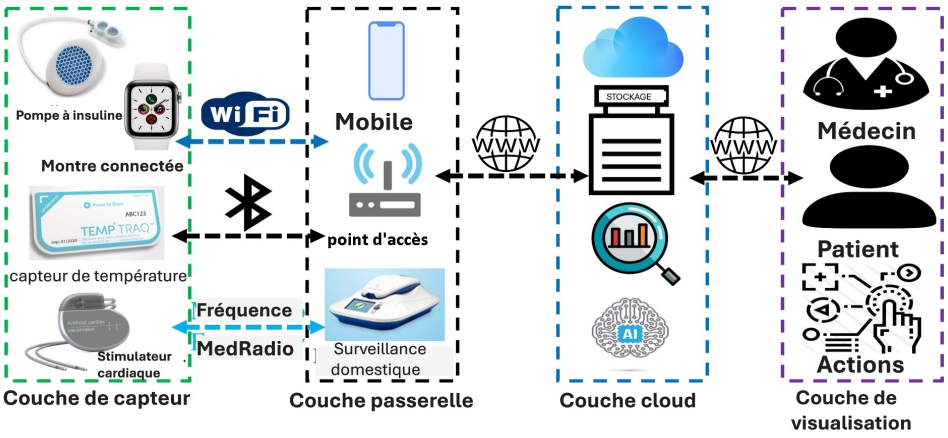


FIG. 1.10 : Architecture (4 couches)
[11]

1.7.6.1 Couche des capteurs (Sensor Layer)

Cette couche intègre une variété de capteurs miniaturisés, implantés ou portables, chargés de surveiller en continu les signes vitaux du patient. Les données collectées sont transmises à la couche supérieure via des technologies de communication sans fil telles que le Wi-Fi, le Bluetooth ou la bande MedRadio, dédiée aux dispositifs médicaux implantables (IMDs), permettant ainsi une surveillance en temps réel.

1.7.6.2 Couche de passerelle (Gateway Layer)

En raison des capacités limitées de calcul et de mémoire des capteurs, les données sont directement transmises à cette couche sans traitement préalable. Elle comprend des dispositifs plus puissants, comme les smartphones des patients ou des points d'accès dédiés, qui assurent des fonctions telles que la validation, le stockage temporaire et une première analyse basée sur l'intelligence artificielle. Les données sont ensuite redirigées vers le cloud via Internet.

1.7.6.3 Couche nuageuse (Cloud Layer)

Le cloud reçoit, stocke et traite les données issues de la couche précédente. L'analyse permet d'identifier les changements dans l'état de santé du patient afin d'en informer les professionnels de santé. Cette couche comprend également les serveurs de génération de clés (KGS), assurant la création des identifiants sécurisés et la gestion des communications avec les nœuds distants.

1.7.6.4 Couche de visualisation/action

Cette couche représente l'interface interactive, où les données de santé sont affichées aux médecins et aux patients pour suivre l'état de santé. Cette couche comprend les procédures, les recommandations et les traitements que le médecin propose en fonction de l'état de santé du patient. Parmi ces procédures, on trouve la prescription de nouveaux médicaments ou l'ajustement des doses des différents médicaments.

1.8 Avantages de l'IoMT

L'Internet des Objets Médicaux (IoMT) s'impose progressivement comme une composante essentielle dans le domaine de la santé connectée. En raison de son intégration croissante dans les systèmes de soins modernes, il est important d'examiner les bénéfices concrets qu'il apporte à différents niveaux. La section suivante présente un aperçu des principaux avantages liés à l'utilisation de l'IoMT[12] :

Avantages	Description
Amélioration des Résultats pour les Patients	L'IoMT contribue à la détection précoce des changements de santé en assurant une surveillance continue et en envoyant des alertes instantanées, permettant une réponse rapide et sauvant des vies.
Réduction des Coûts	Les coûts dans le secteur de la santé peuvent être réduits grâce à l'utilisation des technologies IoMT. ceci est fait en améliorant la gestion des ressources ce système réduit le besoin de visites fréquentes dans les hôpitaux, ce qui contribue à réduire les coûts financiers sur Patients et installations médicales.
Accessibilité et ergonomie	Facile à utiliser et ne nécessite pas de compétences techniques complexes. Ces appareils permettent aux individus de surveiller et de surveiller facilement leur état de santé.
Alertes Automatiques	En cas de détérioration de la santé du patient, les appareils envoient une alarme immédiate au personnelmédical et aux patients qui permet de Sauver des vies .
Gestion facile des dossiers des patients	Gérez les dossiers des patients plus rapidement et avec plus de précision, ce qui leur fait gagner du temps supplémentaire pour interagir avec les patients et prendre des décisions Thérapeutique médicale .

Tab. 1.3 : les avantages de l'Internet des objets médicaux (IoMT)

Fig. 1.11 : Avantages majeurs de l'IOMT
[13]

1.9 Les Protocoles de communication de l'internet Des Objets médiceaux

Basée sur l'architecture de l'IoMT, qui comprend trois couches principales, avec deux sous-couches intermédiaires – la couche d'adaptation et la couche de transport – utilisées pour assurer la liaison entre la couche réseau et la couche application, la sélection des protocoles de communication dans l'IoMT se fait avec soin en fonction des caractéristiques spécifiques du milieu médical. Il est essentiel de prendre en compte des critères tels que l'étendue de la communication requise au sein de l'établissement de santé, le volume et la fréquence des données cliniques transmises (par exemple, les signes vitaux), ainsi que la mobilité des dispositifs, notamment les appareils portables [14][15].

Un protocole de communication est un système qui permet l'échange sécurisé d'informations entre différents objets connectés. Il permet à l'utilisateur de transmettre des données de manière fiable et sécurisée [16]. Il existe différents types de protocoles, chacun présentant des caractéristiques spécifiques.

1.9.1 Couche perceptuelle

assure la collecte initiale des données cliniques à travers des dispositifs médicaux intelligents souvent portables et à faible consommation énergétique. elle s'appuie sur des protocoles de communication sans fil adaptés, généralement basés sur la norme IEEE 802.15.4, qui permet une transmission efficace dans des bandes de fréquences telles que 868 MHz, 915 MHz et 2,4 GHz. Cette norme constitue une base commune à plusieurs protocoles largement utilisés dans les systèmes IoMT, tels que ZigBee, 6LoWPAN et ISA100.11a, permettant ainsi une interopérabilité fiable entre capteurs et systèmes médicaux.

1.9.1.1 RFID (Identification par Radiofréquence)

La technologie RFID, déjà détaillée dans la section relative à l'architecture de l'IoMT, joue un rôle essentiel au sein de la couche de perception. Elle permet l'identification automatique des patients et des dispositifs médicaux, ainsi que la collecte de données physiologiques via des capteurs intégrés.

Grâce à l'utilisation d'étiquettes actives ou passives, RFID assure une communication sans fil à courte portée entre les objets médicaux et les systèmes d'information, facilitant ainsi la traçabilité, la surveillance environnementale et la sécurité des accès dans les environnements hospitaliers.

Protocole infrarouge (IrDA)

Le protocole IrDA (Infrared Data Association) est utilisé pour la transmission de données à courte portée à l'aide de faisceaux infrarouges dirigés. Il est largement appliqué dans le domaine médical, notamment dans les capteurs de température et les caméras

thermiques, servant à mesurer la température corporelle locale à partir d'images infrarouges.

L'architecture du protocole IrDA repose sur trois couches principales :

- **La couche physique** : elle assure la transmission du signal infrarouge entre les dispositifs.
- **La couche IrLAP (Infrared Link Access Protocol)** : elle est responsable de l'établissement et du maintien de la connexion entre deux dispositifs, selon le standard *HDLC (High-level Data Link Control)*, et permet un transfert fiable des données.
- **La couche IrLMP (Infrared Link Management Protocol)** : elle gère l'utilisation simultanée du même lien IrLAP par plusieurs services, et prend en charge la découverte des appareils et des services disponibles à proximité.

Ce protocole est adapté aux environnements nécessitant une communication directe, rapide et sécurisée sans interférences radio, ce qui le rend particulièrement pertinent pour certaines applications médicales.

1.9.1.2 Protocole NFC

Le protocole NFC permet la communication entre appareils sur de courtes distances (quelques centimètres) à des vitesses allant jusqu'à 424 kbit/s. Il fonctionne à une fréquence de 13,56 MHz et peut opérer en mode actif ou passif.

L'utilisation de la technologie NFC a été étudiée avec des dispositifs ingérables ou implantables à l'intérieur du corps humain. Ces dispositifs peuvent fonctionner sans batterie ni connexions électriques externes, ce qui les rend adaptés à des applications telles que les dispositifs ECG implantables.

1.9.1.3 Bluetooth(BLE)

Le Bluetooth est une technologie de communication sans fil basée sur la norme IEEE 802.15.1, fonctionnant à une fréquence de 2,4 GHz. Il est adapté aux dispositifs à faible puissance et à faible coût.

Cette technologie convient au transfert de données à courte portée entre appareils mobiles, avec une portée allant jusqu'à 100 mètres dans les anciennes versions, et jusqu'à 400 mètres dans la version BLE 5.0. Le taux de transfert de données peut atteindre 2 Mbit/s.

BLE est utilisé dans les dispositifs alimentés par batterie nécessitant une faible consommation d'énergie, ce qui le rend idéal pour les applications IoMT qui demandent une connectivité à courte distance et une faible latence, telles que les dispositifs de sport et de fitness, les interfaces humaines (HID) et les appareils médicaux portables.

1.9.1.4 Z-Wave

est un protocole sans fil à faible consommation d'énergie développé par Zensys, largement utilisé dans les réseaux IoT, notamment dans les domaines de la domotique et de la santé.

Il prend en charge deux types de périphériques : les contrôleurs et les périphériques esclaves. Un réseau Z-Wave peut contenir jusqu'à 232 nœuds, avec une couverture allant jusqu'à 32 mètres grâce à des connexions point à point. Il fonctionne à une fréquence de 900 MHz et prend en charge un débit de transmission de 40 Kbit/s.

1.9.1.5 UWB

Basé sur la norme IEEE 802.15.3, le protocole UWB est conçu pour assurer des communications sans fil à haut débit et à courte portée, en particulier dans les environnements intérieurs. Sa vitesse varie de 110 à 480 Mbps, ce qui le rend adapté aux applications nécessitant une grande capacité, telles que la transmission audio et vidéo.

UWB transmet les données en générant de l'énergie radio à des intervalles spécifiques et en occupant une bande passante très large. Grâce à sa faible puissance et sa haute précision, il est considéré comme approprié pour une utilisation dans des environnements sensibles aux ondes radio, comme les hôpitaux.

Par exemple, il peut être utilisé dans les dispositifs de surveillance cardiaque (ECG) pour transmettre les données des capteurs vers l'unité de traitement, notamment dans les situations nécessitant une communication précise à courte portée.

1.9.2 Couche réseau

La couche réseau joue un rôle central dans la transmission sécurisée des données médicales collectées par les capteurs. Elle s'appuie sur divers dispositifs comme les routeurs, les passerelles ou les points d'accès, et repose sur des mécanismes tels que l'adressage IP et le routage. cette couche fait face à des défis critiques liés à la gestion de la confiance, la confidentialité, l'intégrité, et la protection contre les attaques par déni de service.

Plusieurs protocoles utilisés à ce niveau sont basés sur la norme IEEE 802.15, notamment WiFi, ZigBee, LoRaWAN, 6LoWPAN, ainsi que certaines technologies cellulaires comme le 3G/4G/5G, qui permettent la communication à distance dans les environnements hospitaliers.

1.9.2.1 Wi-Fi

Le WiFi est un protocole sans fil de portée moyenne (jusqu'à 100 mètres), basé sur les normes IEEE 802.11. Il est largement utilisé pour connecter des appareils médicaux dans les réseaux locaux. Toutefois, sa consommation énergétique relativement élevée limite son efficacité dans certaines applications de l'IoT.

Pour pallier ces limitations, le standard WiFi HaLow (IEEE 802.11ah) a été développé afin d'offrir une connectivité à faible consommation et une portée plus étendue. Ce

standard est particulièrement adapté aux capteurs et dispositifs médicaux nécessitant une communication efficace à basse consommation.

Des études ont démontré la faisabilité d'utiliser le WiFi en toute sécurité dans les environnements hospitaliers, notamment pour la connexion d'équipements critiques comme les pompes à perfusion, les défibrillateurs et les respirateurs artificiels.

1.9.2.2 Zigbee

ZigBee est un protocole de communication sans fil à faible coût, faible vitesse et faible consommation énergétique, conforme à la norme IEEE 802.15.4. Il est conçu pour les réseaux personnels (PAN) et offre une portée allant jusqu'à 100 mètres, avec un débit compris entre 40 et 250 kbps.

Dans le domaine médical, ZigBee est largement utilisé pour connecter des capteurs biomédicaux au coordinateur, voire pour permettre la communication entre plusieurs coordinateurs. En 2009, la ZigBee Alliance a introduit un profil d'application spécifique, appelé ZigBee Health Care, conçu pour les dispositifs d'assistance opérant dans des environnements de santé non invasifs.

Ce profil, basé sur ZigBee Pro, prend en charge l'échange de données entre divers dispositifs médicaux et non médicaux. Il prend également en charge le standard IEEE 11073 pour la transmission sécurisée et normalisée des données de santé, notamment via une technique dite de "tunneling".

1.9.2.3 WIA-PA

Le WIA-PA est une norme chinoise de communication sans fil développée pour l'automatisation des processus industriels. Il vise à remplacer des standards comme IEEE 802.15.1, IEEE 802.15.4 et IEEE 802.11. Ce protocole est conçu pour assurer la mesure, la surveillance et le contrôle en boucle ouverte des processus de production. Faisant partie des protocoles capables de répondre aux exigences de temps réel et de fiabilité dans les environnements industriels, il a également été proposé pour des usages médicaux, notamment dans les systèmes de télésurveillance à travers des réseaux de capteurs sans fil.

1.9.2.4 ISA100.11a

ISA100.11a est une norme issue du comité ISA100, qui vise à normaliser les communications sans fil dans l'industrie. Elle couvre l'ensemble du cycle de production, y compris le contrôle des processus, la traçabilité des équipements et les applications longue distance. Ce protocole repose sur une topologie en réseau maillé pour garantir des communications sécurisées. Les couches physique et liaison de données sont basées sur le standard IEEE 802.15.4. Tout comme le WIA-PA, ISA100.11a a été proposé pour des applications médicales, notamment pour la transmission des données dans des systèmes de surveillance à distance.

1.9.2.5 6LoWPAN

Le protocole 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) a été développé par le groupe de travail de l'IETF (Internet Engineering Task Force) pour permettre l'intégration des dispositifs à faible consommation dans les réseaux IP. Il s'appuie sur la norme IEEE 802.15.4 et permet la transmission de paquets IPv6 dans des environnements contraints, caractérisés par une faible bande passante, des paquets de petite taille et des adresses variables.

6LoWPAN introduit des mécanismes d'encapsulation et de compression d'en-têtes afin d'optimiser le transport des paquets IPv6 sur des réseaux à ressources limitées. Dans le domaine de la santé, ce protocole est utilisé pour connecter les capteurs médicaux et les dispositifs IoMT aux réseaux IP, facilitant ainsi l'interconnexion entre les capteurs eux-mêmes, mais aussi leur liaison avec des équipements intermédiaires ou des routeurs connectés à Internet.

1.9.2.6 LoRaWAN

La technologie LoRa (Long Range) a été développée par l'entreprise Semtech en tant que protocole de couche physique destiné aux réseaux étendus à faible consommation (LPWAN). Elle fonctionne sur des bandes de fréquences libres qui diffèrent selon les régions : 868 MHz en Europe, 915 MHz en Amérique du Nord et en Australie, et 923 MHz en Asie. LoRa permet la transmission de données sur de longues distances, pouvant dépasser 10 kilomètres dans les zones à faible densité de population, tout en maintenant une consommation énergétique minimale.

Comme LoRa ne définit que la couche physique, un protocole de couche supérieure appelé LoRaWAN (LoRa Wide Area Network) a été conçu pour assurer la gestion des communications à la couche MAC. LoRaWAN agit également comme protocole de couche réseau, en orchestrant l'échange de données entre les dispositifs terminaux et les passerelles.

Optimisé pour une consommation énergétique réduite, LoRaWAN prend en charge des réseaux étendus comptant des millions d'appareils, avec des débits allant de 0,3 kbps à 50 kbps. Il prend en charge la communication bidirectionnelle, assure la sécurité des échanges, et convient à des applications variées comme les villes intelligentes, l'industrie et les systèmes de santé connectée. Par exemple, des recherches ont démontré son efficacité dans des systèmes de surveillance médicale à distance pour les zones rurales, ainsi que dans des dispositifs portables pour l'analyse de fluides biologiques utilisant LoRa pour la transmission longue distance.

1.9.3 Couche d'application

La couche application constitue l'interface finale entre les données médicales collectées et les applications logicielles cliniques. Elle assure la transformation des informations reçues en un format exploitable par les dispositifs médicaux et les serveurs spécialisés. Plusieurs protocoles y sont utilisés, certains à usage général comme MQTT, CoAP ou HTTP/HTTPS, qui offrent des communications légères et sécurisées adaptées aux dispositifs médicaux contraints. D'autres sont spécifiquement conçus pour le domaine médical, comme

les protocoles d'encodage HL7 et XML Encode, qui garantissent une structuration normalisée des données de santé.

1.9.3.1 HL7

Health Level Seven (HL7) est un ensemble de standards conçu pour permettre l'échange, l'intégration, le partage et la récupération des informations électroniques de santé entre différents systèmes médicaux. Il garantit une communication fluide et transparente en définissant un langage commun, des structures de données uniformes et des types bien spécifiques, facilitant ainsi l'interopérabilité entre des systèmes hétérogènes.

HL7 soutient non seulement la pratique clinique, mais également la gestion, la prestation et l'évaluation des services de santé. Il permet aussi la collecte structurée des données mesurées à partir de dispositifs médicaux standards ou non standards.

Ce standard comprend plusieurs versions et spécifications, telles que HL7 v2.x, HL7 v3, ainsi que des standards complémentaires pour l'échange de documents comme DICOM et NCPDP, assurant une intégration complète et efficace dans les environnements médicaux numériques.

1.9.3.2 CoAP(Constrained Application Protocol)

Il s'agit d'un protocole de transfert Web conçu pour les dispositifs à ressources limitées. Il adopte le protocole UDP et suit le modèle architectural REST tout en assurant une faible consommation d'énergie. CoAP est structuré en deux sous-couches principales : la couche de messagerie et la couche requête/réponse, ce qui permet une gestion efficace de la fiabilité des communications. Il prend en charge les communications unicast et multicast, contrairement aux protocoles basés sur TCP. Ce protocole est largement utilisé dans les environnements médicaux, notamment dans l'IoMT, en raison de sa légèreté, de sa fiabilité dans les réseaux contraints et de son adéquation aux systèmes de surveillance à distance.

1.9.3.3 MQTT(Message Queuing Telemetry Transport)

Développé par IBM, le protocole MQTT repose sur le modèle publication/abonnement (publish/subscribe) et fonctionne sur la couche application, au-dessus de TCP. Il a été conçu pour optimiser l'efficacité énergétique et la bande passante, répondant ainsi aux exigences des dispositifs IoMT à ressources limitées. Il prend en charge des charges utiles de données très petites, à partir de 2 octets, tout en pouvant atteindre jusqu'à 256 Mo. Grâce à sa légèreté et à sa capacité à fonctionner sur des réseaux peu fiables ou à faible débit, MQTT est largement utilisé pour assurer la communication entre dispositifs médicaux et plateformes IoMT. Il permet une transmission asynchrone efficace des données, tout en intégrant des identifiants uniques des dispositifs dans la charge utile, ce qui facilite leur gestion et leur traçabilité.

1.9.3.4 HTTP(HyperText Transfer Protocol)

Le protocole HTTP est utilisé conformément aux exigences spécifiques du système, telles que le volume des données à transmettre, le type de dispositifs impliqués, et la stabilité du réseau. Il a été adopté par plusieurs chercheurs dans la conception de systèmes IoMT, notamment pour assurer le transfert des données entre les dispositifs médicaux, le cloud et les utilisateurs finaux. La flexibilité et l'universalité de ce protocole en font une solution adaptable aux environnements de soins de santé, en dépit de sa consommation relativement élevée de ressources dans les dispositifs contraints.

1.10 Les défis en la mise en œuvre de L'IOMT

L'application de l'Internet des objets médicaux (IoMT) dans les systèmes de santé soulève plusieurs défis majeurs. L'un des plus importants est l'absence de standardisation, qui complique l'interopérabilité entre les dispositifs médicaux de différents fabricants et entrave l'adoption de mesures de sécurité rigoureuses[4].

Par ailleurs, la sécurité des données des patients, transmises entre les objets connectés et les infrastructures cloud, demeure une préoccupation centrale. De plus, certains établissements de santé rencontrent des obstacles liés à l'intégration de technologies complexes, souvent en raison de la résistance institutionnelle ou de la difficulté à se conformer à des normes réglementaires en constante évolution.Si ces défis ne sont pas relevés, ils risquent de limiter considérablement les bénéfices potentiels de l'IoMT[17].

Principaux défis techniques et organisationnels

- **Sécurité des données et gestion efficace** : Les données sensibles des patients étant transférées entre les dispositifs et les systèmes cloud, il est crucial d'assurer leur protection à l'aide de mécanismes robustes. Des solutions comme la blockchain peuvent y contribuer efficacement.
- **Interopérabilité des systèmes** : Pour assurer un échange fluide de données entre dispositifs hétérogènes, des protocoles standards et des architectures ouvertes mais sécurisées doivent être développés.
- **Modernisation des infrastructures** : L'intégration de l'IoMT requiert un renouvellement des technologies existantes dans les établissements de santé, ainsi que la formation continue du personnel.
- **Conformité réglementaire** : Le respect des réglementations en vigueur est indispensable. Cela implique une veille réglementaire continue et l'adoption d'équipements certifiés.

1.10.1 Préoccupations liées aux dispositifs médicaux connectés

Les préoccupations relatives à IoMT sont principalement classées en quatre grandes catégories : la sécurité,la confiance , la Vie privée et exactitude[4].

- **Problèmes de sécurité :**En raison de leur dépendance à des communications sans fil ouvertes, les dispositifs IoMT sont particulièrement vulnérables aux attaques. Ces failles permettent aux attaquants d'intercepter les données sensibles, d'accéder aux systèmes sans autorisation, d'injecter des logiciels malveillants, voire de compromettre la sécurité des patients.
- **Problèmes de confiance :** La compromission de la vie privée et de la sécurité engendre une perte de confiance des patients envers les dispositifs médicaux intelligents. Cette méfiance croissante remet en question l'acceptation de la technologie dans le domaine médical.
- **Problèmes de vie privée :** Les attaques passives, comme l'analyse de trafic, exposent l'identité et les données médicales des patients. Ces atteintes à la vie privée peuvent entraîner un vol d'identité ou une divulgation non autorisée d'informations confidentielles.
- **Crainte de l'exactitude :** Des erreurs médicales attribuées à un manque de précision dans les dispositifs IoMT ont entraîné des décès et des blessures graves. Cela soulève des inquiétudes concernant la fiabilité des diagnostics et des traitements automatisés.

1.11 Types d'attaques sur les appareils médicaux de l'Internet des objets médicaux

Les attaquants exploitent diverses vulnérabilités présentes dans les systèmes IoMT. Ces menaces sont classées en fonction des couches de l'architecture. Il est pertinent de les organiser selon la couche concernée : perception, réseau et application. Cette classification permet de mettre en évidence les vulnérabilités spécifiques à chaque niveau [10][18] :

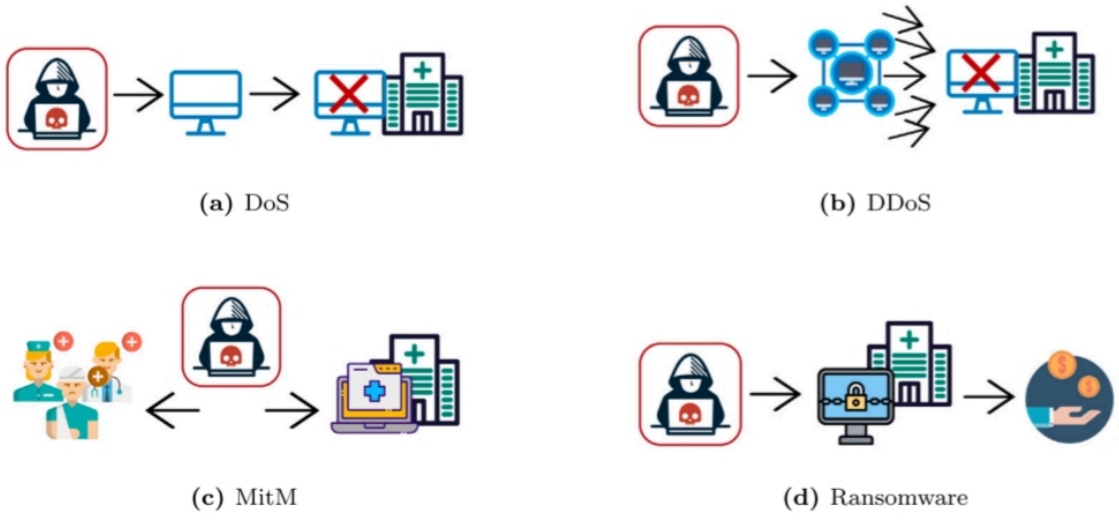


Fig. 1.12 : exemples d'attaques
[19]

Couche	Attaque	Description	Effet
Couche Perceptuelle	Attaque par canal auxiliaire (Side-channel attack)	Ce type d'attaque exploite les canaux d'émission secondaires des dispositifs médicaux connectés, comme les variations électromagnétiques, la consommation d'énergie ou le temps d'exécution, pour extraire des informations sensibles. Sans interagir directement avec le système, l'attaquant peut ainsi contourner les mécanismes classiques de sécurité et compromettre la confidentialité des données traitées.	Confidentialité, Intégrité
	Altération des dispositifs (Tampering devices)	Cette attaque implique l'accès physique aux dispositifs IoMT dans le but de modifier leur fonctionnement ou les données qu'ils traitent. Cela peut se produire, par exemple, par l'altération des capteurs via une interface RFID ou un lien de communication vulnérable. L'attaquant peut exploiter des failles matérielles ou logicielles pour compromettre l'intégrité du dispositif, voire l'endommager totalement.	Confidentialité, Intégrité
	Clonage d'étiquette	L'attaquant duplique les données collectées via une attaque par canal auxiliaire. Les étiquettes RFID sont facilement clonables, ce qui permet un accès non autorisé à des données médicales sensibles.	Confidentialité, Intégrité, Autorisation
	Suivi par capteurs	Des capteurs non sécurisés, tels que le GPS ou ceux utilisés dans la détection de chute et la surveillance à distance, peuvent être exploités pour suivre la localisation des patients ou falsifier les données de position, compromettant ainsi leur vie privée.	Confidentialité, Intégrité, Autorisation, Vie privée

Tab. 1.4 : Attaques au niveau de la couche perception

Couche	Attaque	Description	Effet
couche Réseau	Écoute clandestine	Interception non autorisée des communications afin de capter et exploiter des données sensibles,	Confidentialité, non-répudiation et la vie privée
	Attaque par rejeu (Replay attack)	L'attaquant intercepte un message d'authentification légitime entre deux entités, puis le renvoie ultérieurement pour tromper le système.	Autorisation
	Attaque de l'homme du milieu (Man-in-the-middle)	L'attaquant intercepte la communication entre deux dispositifs IoMT, accède à leurs données confidentielles, et peut les modifier avant qu'elles n'atteignent leur destination.	Confidentialité, Autorisation
	Attaque par Déni de service (DoS/DDoS)	Les attaques DoS sont lancées depuis un seul nœud, tandis que les attaques DDoS impliquent plusieurs sources afin de saturer une cible avec des requêtes, rendant le service indisponible pour les utilisateurs légitimes.	Disponibilité
	Attaque Sinkhole	Un nœud malveillant attire le trafic en prétendant offrir une meilleure connexion, permettant ensuite d'autres attaques comme l'écoute ou la suppression sélective de paquets.	Confidentialité, Intégrité, Disponibilité
	Point d'accès rogue (Rogue Access)	Un faux point d'accès est installé dans le réseau pour intercepter le trafic des utilisateurs légitimes.	
	Attaque par sniffing	Cette attaque consiste à intercepter passivement les données échangées entre deux nœuds. L'attaquant peut observer les communications entre les différentes couches du système sans être détecté.	Confidentialité
	Attaque par redirection sélective (Selective Forwarding)	Un nœud malveillant modifie, supprime ou redirige certains paquets, ce qui provoque une perte ou altération des données transmises.	Confidentialité, Intégrité, Disponibilité, Autorisation

Tab. 1.5 : Attaques au niveau de la couche réseau

Couche	Attaque	Description	Effet
Couche D'application	Attaque par force brute	Des outils automatisés sont utilisés pour tester de nombreuses combinaisons de mots de passe jusqu'à réussir à accéder au système.	Confidentialité, Intégrité
	Injection SQL	Des requêtes SQL malveillantes sont introduites dans la base de données pour accéder, modifier ou supprimer des données sensibles.	Confidentialité, Intégrité, Disponibilité, Autorisation
	Détournement de compte	L'attaquant intercepte des paquets lors du processus d'authentification pour prendre le contrôle du compte de l'utilisateur légitime.	Confidentialité, Intégrité
	Logiciel de rançon (Ransomware)	Ce type d'attaque chiffre des données sensibles, comme les informations médicales, et exige une rançon pour fournir la clé de déchiffrement.	Intégrité, Disponibilité

Tab. 1.6 : Attaques au niveau de la couche application

1.12 Sécurité IoMT

1.12.1 Sécurité informatique

La sécurité informatique est devenue indispensable et vitale pour toutes les organisations. Elle englobe l'ensemble des stratégies, méthodes, solutions et outils mis en œuvre pour protéger les réseaux et les données sensibles du système d'information contre les risques, les menaces, les tentatives d'accès non autorisé, ainsi que contre le vol, la modification ou la destruction des données. Elle vise également à réduire les risques d'accidents ou de défaillances, et à garantir la continuité et la fiabilité des services informatiques.

Dans le domaine des dispositifs médicaux connectés (IoMT), ces impératifs en matière de sécurité revêtent une importance d'autant plus cruciale en raison de la sensibilité des données médicales et de l'impact potentiel sur la santé des patients.

1.12.2 Objectifs de sécurité dans l'IoMT

La sécurité des systèmes IoMT est essentielle en raison de la sensibilité des données des patients, et de nombreux chercheurs s'appuient sur le modèle **CIANA** Qui comprend cinq objectifs principaux : confidentialité, intégrité, disponibilité, non-répudiation, authentification[11].

- **confidentialité :** S'assurer que les données (ne peuvent être lues que par des personnes autorisées à y accéder , qu'elles soient collectées, transmises ou stockées. Le chiffrement et le les listes de contrôle d'accès sont nécessaires pour maintenir la confidentialité.
- **l'intégrité des données :** les données médicales arrivent en bon etat pendant leur traitement ou de leur transmission, ne subisent aucune altération non-autorisée et sont exactes. cela permet de maintenir la fiabilité des diagnostics et des traitements.
- **Disponibilité :** Garantir le bon fonctionnement des systèmes IoMT pour tous les utilisateurs autorisés en permanence et à tout moment, grâce à des mises à jour régulières, une surveillance et la mise en place de voies de secours en cas d'attaques.
- **Disponibilité :** Garantir le bon fonctionnement des systèmes IoMT pour tous les utilisateurs autorisés en permanence et à tout moment, grâce à des mises à jour régulières, une surveillance et la mise en place de voies de secours en cas d'attaques.
- **Non-répudiation :** Cette condition garantit l'impossibilité de nier toute interaction dans le système et oblige les utilisateurs à assumer la responsabilité de leurs actions. Cela se fait en utilisant des techniques de signature numérique.

1.12.3 Autres exigences de sécurité dans L'IoMT

- **Authentification et autorisation :**Il s'agit de vérifier l'identité d'un utilisateur avant de lui accorder l'accès au réseau IoMT, en utilisant une authentification mutuelle entre les dispositifs et le serveur pour renforcer la sécurité. L'autorisation, quant à elle, définit les droits d'accès pour chaque entité authentifiée, veillant à ce qu'elle n'interagisse qu'avec les ressources auxquelles elle est autorisée.
- **Anonymat :** Il est essentiel pour empêcher la reconnaissance directe des individus. Les identités des patients et du personnel médical doivent rester cachées aux entités non autorisées lorsqu'elles interagissent avec le système.
- **La confidentialité persistante(progressive et régressive) :** La confidentialité progressive vise à protéger les données transférées ou les clés futures, même si des clés antérieures ont été compromises. Inversement, la confidentialité régressive garantit que les anciennes clés restent sécurisées même si les données actuelles sont attaquées. Ces deux formes sont assurées par l'utilisation de clés temporelles, générées et utilisées uniquement lorsque les horloges des dispositifs de communication sont synchronisées.
- **Échange sécurisé de clés :** Il consiste à partager des clés entre les nœuds du système de manière sécurisée, afin d'assurer la confidentialité des communications entre les dispositifs médicaux. Des techniques comme l'algorithme de Diffie-Hellman permettent aux deux parties de générer une clé partagée en toute sécurité.
- **Résilience contre l'abus d'entiercement des clés :** Cette exigence vise à empêcher toute entité interne d'abuser de ses privilèges pour usurper l'identité d'un utilisateur légitime, offrant ainsi une protection contre les menaces internes. Cela

peut être réalisé à l'aide de clés asymétriques combinées à des fonctions de hachage cryptographique robustes.

- **Établissement de clés de session :**Après le processus d'authentification, les nœuds du système doivent établir des clés de session pour sécuriser les échanges. Cela se fait généralement à l'aide de clés symétriques ou asymétriques associées à une fonction de hachage cryptographique.

1.12.4 Mécanismes de sécurité dans l'Internet des objets médical (IoMT)

Assurer la protection des dispositifs médicaux connectés face à l'augmentation des menaces et des risques, grâce à différentes technologies de sécurité, allant des méthodes traditionnelles aux technologies émergentes[11].

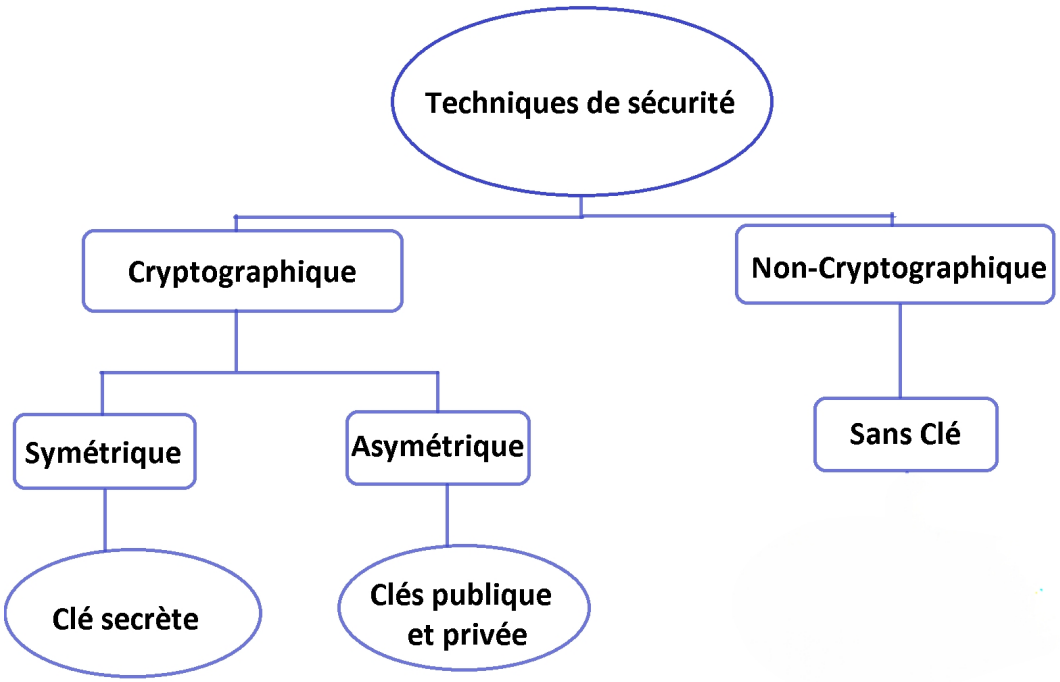


Fig. 1.13 : Mécanismes de sécurité [20]

1.12.5 La cryptographie symétrique

La cryptographie symétrique est principalement utilisée pour protéger les flux de données internes entre dispositifs IoMT. Elle est fréquemment employée en raison de sa rapidité et de sa faible consommation de ressources, ce qui est crucial pour les dispositifs médicaux aux capacités limitées. Cette méthode garantit la confidentialité des communications sans nécessiter d'opérations de calcul complexes, en se basant sur l'utilisation d'une seule clé secrète partagée pour le chiffrement et le déchiffrement des données.

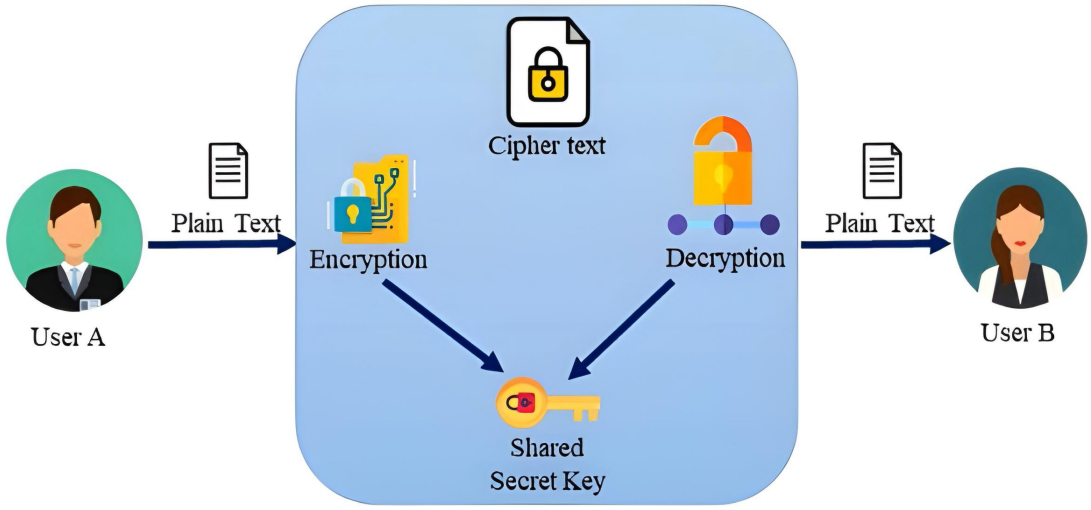


FIG. 1.14 : La cryptographie symétrique
[21]

1.12.6 La cryptographie asymétrique (RSA, ECC)

Contrairement à la cryptographie symétrique, la cryptographie asymétrique utilise deux clés distinctes : l'une publique et l'autre privée. La clé publique est accessible à tous, tandis que la clé privée est strictement confidentielle et propre à chaque utilisateur. Elle est particulièrement adaptée à la vérification de l'identité des dispositifs médicaux et à la garantie que seuls des acteurs autorisés puissent initier une communication. Les algorithmes couramment utilisés incluent RSA (Rivest–Shamir–Adleman) et ECC (Elliptic Curve Cryptography). Ces méthodes sont souvent combinées avec des fonctions de hachage cryptographique (FHC) et des signatures numériques, afin d'assurer à la fois l'authentification, l'intégrité des données et la fiabilité des échanges.

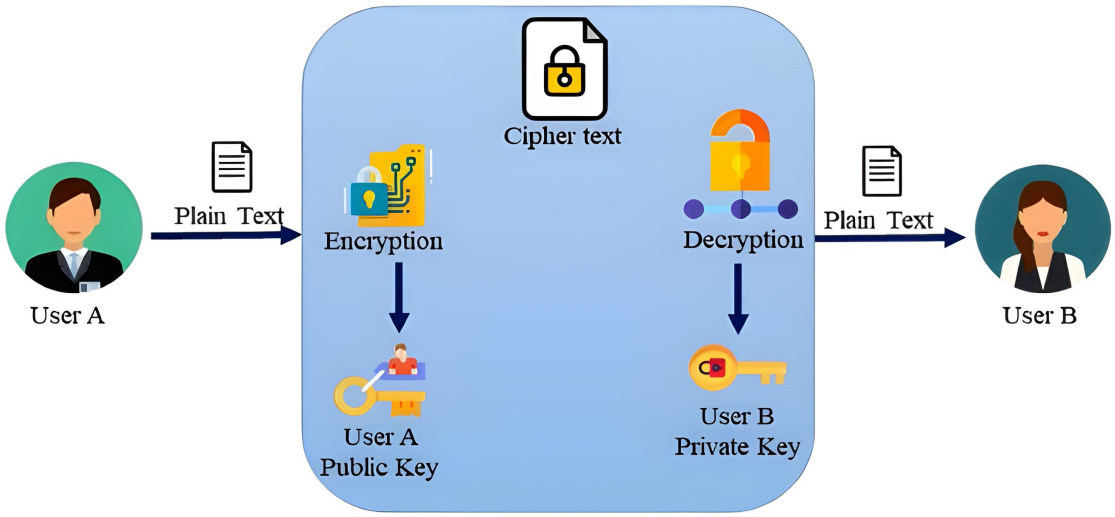


FIG. 1.15 : La cryptographie asymétrique
[21]

1.12.7 Le chiffrement homomorphe

Le chiffrement homomorphe permet d'effectuer des calculs directement sur des données chiffrées, sans avoir à les déchiffrer au préalable. Cette approche est particulièrement avantageuse dans les systèmes IoMT, car elle protège la confidentialité des données médicales tout en permettant leur traitement à distance dans des environnements cloud. Les données des patients sont ainsi stockées sous forme chiffrée, réduisant les risques de fuites tout en maintenant la fonctionnalité des services.

1.12.8 Les techniques de sécurité sans clé (Keyless Security) :

Ces techniques visent à éliminer la dépendance aux clés prépartagées pour l'authentification et à proposer des solutions alternatives adaptées aux dispositifs médicaux connectés. Elles comprennent :

- **l'authentification biométrique :** Basée sur des caractéristiques physiologiques uniques comme les empreintes digitales ou les signaux ECG (électrocardiogramme), elle permet une identification fiable sans stockage de clés cryptographiques, ce qui la rend adaptée aux dispositifs à faibles ressources.
- **L'authentification basée sur des jetons :**Chaque utilisateur ou dispositif reçoit un jeton sécurisé (par exemple, RFID, X-Auth-Token), utilisé pour accéder aux ressources du système de manière contrôlée.
- **Les systèmes proxy :**Utilisés pour sécuriser les communications entre les capteurs médicaux et les dispositifs de commande. Ils peuvent être intégrés dans des équipements portables tels que des ceintures ou des vestes intelligentes.
- **les technologies de communication par la lumière :** Le Li-Fi (Light Fidelity) utilise la lumière visible pour transmettre les données, offrant une alternative sécurisée aux ondes radio. Grâce à une portée de transmission limitée, il améliore la confidentialité et minimise les interférences avec les réseaux hospitaliers.
- **Technologie blockchain et IA :** La blockchain garantit l'intégrité et la traçabilité des transactions dans l'écosystème IoMT, en permettant un partage sécurisé des données entre les patients, les médecins et les autres parties prenantes. Elle limite le risque de fraude et renforce la confiance.

  L'intelligence artificielle, quant à elle, contribue à la sécurité en analysant en temps réel le comportement des dispositifs et en détectant automatiquement les anomalies ou les cyberattaques émergentes.

1.13 Informatique en périphérie (Edge Computing)

L'Edge Computing, qui émerge comme une solution efficace pour renforcer la sécurité dans l'IoMT, est une technologie moderne permettant de traiter les données localement, c'est-à-dire au niveau des dispositifs médicaux ou à proximité de leur source de génération,

sans avoir à les transférer vers des serveurs cloud distants. Cette approche contribue à minimiser la latence, ce qui la rend idéale pour la gestion de données sensibles en temps réel, tout en améliorant la confidentialité et la sécurité. De plus, elle permet de réduire les coûts liés au transfert et au stockage des données. Grâce à l'informatique en périphérie, les établissements de santé peuvent offrir des soins plus rapides et personnalisés aux patients, tout en limitant leur dépendance à une connexion réseau continue[22].

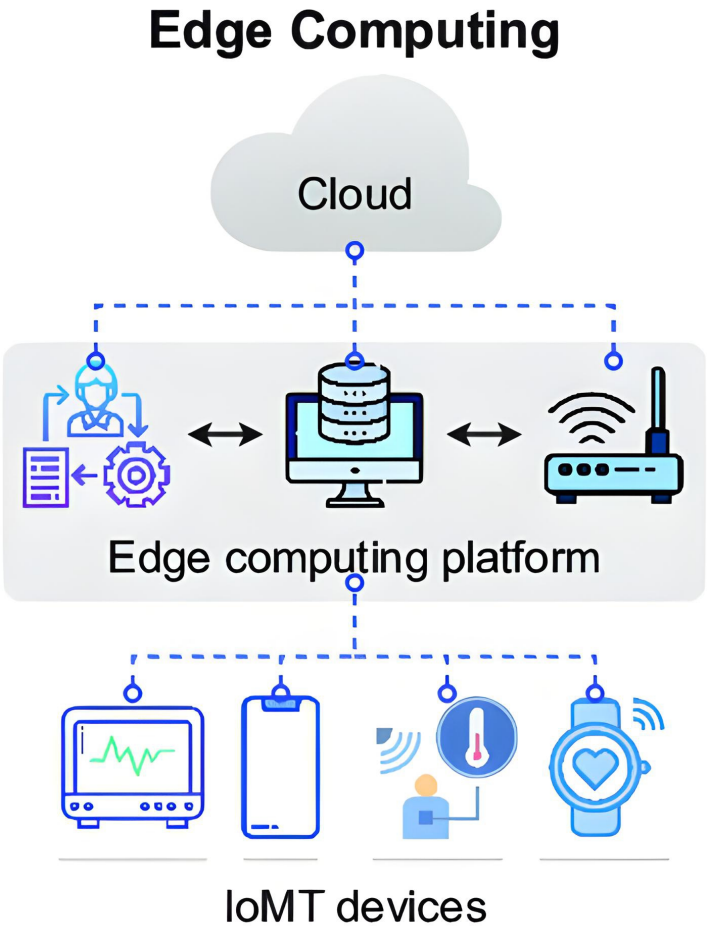


Fig. 1.16 : Architecture de l'edge computing dans les systèmes de santé basés sur l'IoMT [23]

1.13.1 Avantages

- **Proximité aux sources de données :** Le traitement local des données sensibles améliore la sécurité et la protection de la vie privée, car il élimine la nécessité de les transmettre sur Internet, réduisant ainsi les risques de piratage ou de fuite.
- **Réduction de la latence :** En traitant les données à proximité de leur point de création, l'Edge Computing permet une réponse quasi-instantanée, essentielle pour les applications critiques dans le domaine médical.
- **Réduction de la bande passante :** L'analyse locale diminue le volume de données à transférer vers le cloud, réduisant ainsi la congestion du réseau.

- **Renforcement de la sécurité et de la confidentialité :** En évitant le transfert de données vers des serveurs distants, l'Edge Computing limite l'exposition aux attaques externes.
- **Support à la mobilité :** Cette technologie s'adapte aux changements fréquents de position des dispositifs médicaux, assurant un service stable même en cas de mobilité élevée.
- **Connaissance géographique :** Grâce à la connaissance de la localisation des dispositifs, il est possible d'offrir des services localisés, comme la distribution de contenu spécifique à une région ou le traitement décentralisé.
- **Hétérogénéité :** L'Edge Computing est capable de gérer une grande diversité de dispositifs, d'applications et de protocoles, grâce à sa compatibilité avec différents standards et modèles de données.

1.14 Conclusion

Dans ce chapitre, nous avons exploré le monde de l'IdO médical, de sa définition générale à ses diverses applications dans le domaine de la santé. Nous avons présenté les types d'appareils utilisés et leurs types de communication, ainsi que l'architecture et les protocoles de ce système. Nous avons également mis en évidence les avantages que l'IdO médical procure, tout en soulignant les défis en matière de sécurité et les types d'attaques qui le menacent. Pour contrer ces risques, divers objectifs de sécurité et mécanismes de protection ont été introduits, y compris l'informatique périphérique. Cependant, les dispositifs IoMT restent vulnérables aux menaces, d'où la nécessité de consacrer le chapitre suivant à l'analyse des systèmes de détection d'intrusion (IDS) spécifiquement adaptés à ce cadre.

Chapitre 2

Les systèmes de détection d'intrusion (IDS)

2.1 Introduction

À l'ère actuelle, les cyberattaques se caractérisent par une rapidité et une complexité accrues, exposant ainsi les organisations et les individus à des risques significatifs de perte de données critiques. Malheureusement, les solutions traditionnelles telles que les antivirus et les pare-feux montrent souvent leurs limites face à ces menaces émergentes.

C'est dans ce contexte que sont apparus récemment des dispositifs de sécurité innovants, appelés systèmes de détection d'intrusion (IDS), visant à renforcer la défense des infrastructures informatiques.

Le présent chapitre a pour vocation d'éclaircir les concepts fondamentaux relatifs aux IDS. Par la suite, une classification détaillée de ces systèmes sera développée afin de mieux comprendre leurs spécificités et leurs domaines d'application.

2.2 Système de détection d'intrusions

Le premier modèle de détection d'intrusions a été développé en 1984 par Dorothy Denning et Peter Neuman. Ce modèle, basé sur des règles d'approche comportementale, est appelé IDES (Intrusion Detection Expert System). En 1988, il a été développé pour devenir un IDS (Intrusion Detection System). [24]

Ce dernier est un mécanisme conçu pour identifier des activités anormales ou suspectes sur une cible donnée (un réseau ou une machine) en utilisant une base de connaissances. Il consiste à détecter les activités intrusives d'un attaquant vers ou depuis un système informatique en se basant sur l'observation des activités générées par les utilisateurs.

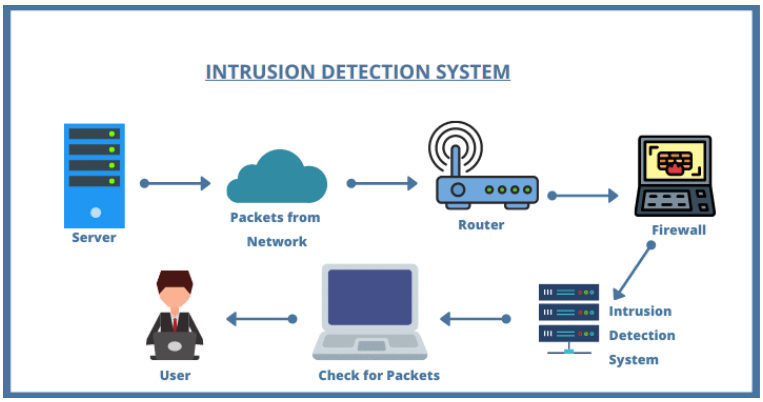


Fig. 2.1 : Architecture système détection d'intrusions.
[25]

2.3 Différents types d'IDS

Il existe plusieurs manières de classer les systèmes de détection d'intrusion, en fonction des méthodes d'analyse et de surveillance utilisées. Ces systèmes se répartissent généralement en trois grandes familles distinctes d'IDS :

2.3.1 La détection d'intrusions basée sur l'hôte

L'HIDS (Host Based IDS) est un système de détection d'intrusions conçu pour surveiller uniquement le trafic sur une machine spécifique. Il analyse les journaux du système, les appels système et vérifie l'intégrité des fichiers à l'aide de techniques comme les signatures numériques ou les valeurs de hachage. Afin d'assurer son efficacité, le HIDS nécessite un système sain et non compromis. Cependant, en cas de compromission par un attaquant, l'efficacité du HIDS diminue fortement, le rendant incapable de détecter des menaces supplémentaires.

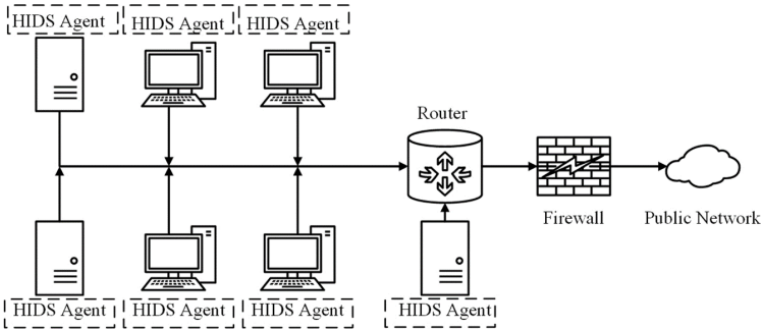


Fig. 2.2 : Exemple d'une architecture HIDS.
[26]

2.3.1.1 Avantages

- Découvrir plus facilement un Cheval de Troie puisque les informations et les possibilités sont très étendues.
- Détecter des attaques impossibles à détecter avec des IDS réseau puisque le trafic est souvent crypté.
- Observer les activités sur l'hôte avec précision.

2.3.1.2 Inconvénients

- Ils ont moins de facilité à détecter les scans.
- Ils sont sensibles aux attaques de type DoS.
- Consomme beaucoup de ressources CPU.

2.3.2 La détection d'intrusion réseau NIDS (Network Intrusion Detection System)

Les NIDS (Network-based Intrusion Detection Systems) sont des systèmes utilisés pour protéger les réseaux en écoutant et surveillant, en temps réel, tout le trafic réseau. Ils analysent ensuite les données collectées et génèrent des alertes en cas de détection d'intrusions ou de paquets potentiellement malveillants.

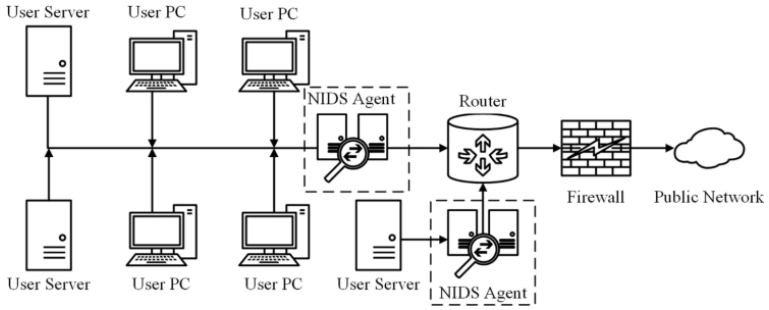


FIG. 2.3 : Exemple d'une architecture NIDS.
[26]

2.3.2.1 Avantages

- Les capteurs peuvent être bien sécurisés puisqu'ils se contentent d'observer le trafic.
- Détecter plus facilement les scans grâce aux signatures.
- Filtrage de trafic.
- Assurer la sécurité contre les attaques puisqu'il est invisible.
- Facile à appliquer, car il n'a aucun impact sur les systèmes ou l'infrastructure standard.
- Le NIDS permet d'analyser le trafic réseau.

2.3.2.2 Inconvénients

- NIDS peut ne pas reconnaitre l'attaque lorsque la taille du réseau devient trop grand.
- NIDS ne peut pas analyser les paquets chifrés, ce qui rend une partie du trafic invisible pour le processus, ce qui réduit l'efficacité de NIDS.
- Les attaques impliquant des paquets corrompu ou fragmentés ne sont pas facilement détectées.

2.3.3 Système détection d'intrusion Hybride

Les IDS hybrides combinent les caractéristiques des NIDS et des HIDS pour surveiller à la fois le réseau et les terminaux. Les sondes sont placées à des points stratégiques et fonctionnent comme des NIDS et/ou des HIDS en fonction de leurs emplacements. Les alertes sont ensuite remontées vers une machine centrale qui les centralise et relie les informations provenant de multiples sources. Ces systèmes utilisent une architecture distribuée où chaque composant unifie son format d'envoi, permettant ainsi une communication efficace et une extraction d'alertes plus précises.

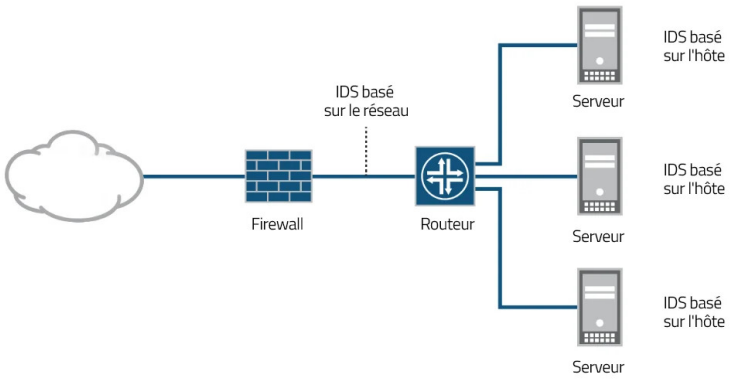


FIG. 2.4 : Exemple d'une architecture hybride.
[27]

2.3.3.1 Avantages

- Moin de faux positifs.
- Une meilleure corrélation (la corrélation permet la géneration d'avertissements existants).
- Possibilité de réaction sur les analyseurs.

2.3.3.2 Inconvénients

- Taux élevé de faux positifs.

2.4 Caractéristiques d'un système de détection d'intrusion

Un système de détection d'intrusions idéal devrait présenter les caractéristiques suivantes :

- Il doit être capable de résister à toute tentative de corruption, c'est-à-dire qu'il doit être en mesure de repérer si lui-même a subi une modification non désirée.
- Utiliser de ressources de surveillance minimale. La période s'adaptera au cours du temps aux modifications du comportement du système et des utilisateurs surveillés.
- L'utilisation minimale des ressources sur le système (calcule, stockage, etc…) est installée.
- Capacité à accepter les mise à jour et les modification de configuration pour recevoir de nouvelle disposition des directives de sécurité et des modifications.
- Facile et simple à utilisée : facilté d'installation et de configuration.
- Facile pour configurer des directives de sécurité spécifiques d'un réseau.

2.5 Architecture d'un IDS

L'architecture fondamentale d'un système de détection d'intrusion se compose de trois modules principaux :

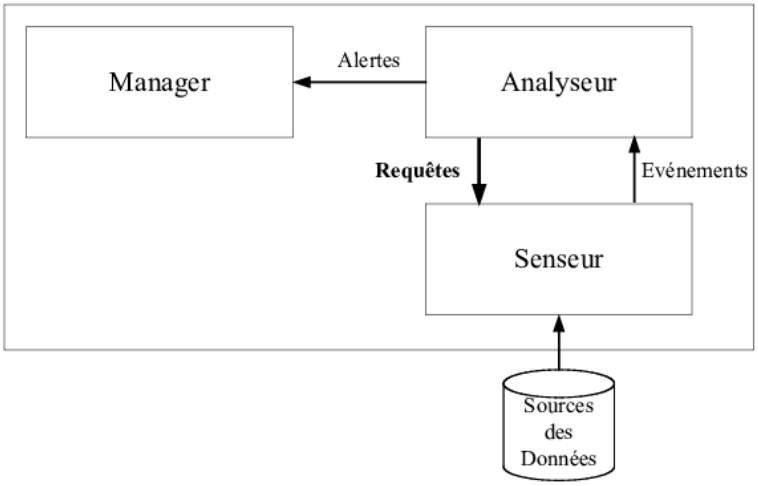


Fig. 2.5 : L'architecture la plus simple d'un IDS.
[28]

2.5.1 Capteurs(Sensor)

c'est le gestionnaire qui filtre et formate les informations brutes envoyées à partir de la source de données. Le résultat de ce processus est un message formaté, également appelé événement. Représente les unités de base d'un scénario d'attaque.

2.5.2 Analyseur(Analyzer)

permet d'analyser les événements générés par le capteur. Si une activité intrusive est déterminée, un avertissement est émis dans le cadre du format standard. Dans cette architecture, le capteur et l'analyseur forment ensemble la sonde.

2.5.3 Gestionnaire(Reponse/Manager)

le gestionnaire recueille les bénéficiaires de l'alarme du capture et fournit aux administrateurs des activités supplémentaires.

2.6 Les Fonctions principales d'un IDS

Les IDS proposent les fonctions suivantes : [29]

- Détection d'attaques (actives ou passives).
- Génération des rapports.

- Outils de corrélation avec d'autres éléments de l'architecture de sécurité.
- Réaction aux attaques par le blocage de route ou la fermeture de connexion.

2.7 Mise en place d'un IDS

L'implémentation d'un système de détection d'intrusion (IDS) est cruciale pour renforcer la sécurité d'un réseau ou d'une infrastructure informatique. Cette procédure comprend une série d'étapes pour mettre en place et paramétrer efficacement un IDS dans le but de se prémunir contre les intrusions et les actions malveillantes.

2.7.1 Le positionnement d'IDS

Le choix judicieux des lieux stratégiques pour la mise en place d'un IDS est crucial. L'image suivante illustre un réseau local ainsi que les trois emplacements possibles pour un IDS.

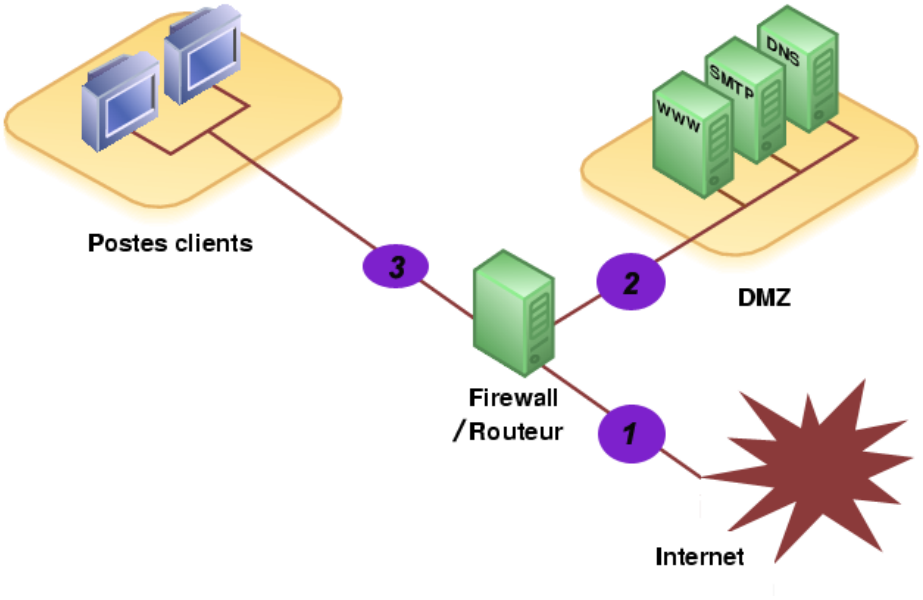


Fig. 2.6 : Les positions des IDS.
[30]

- Position (1) : à ce niveau, l'IDS sera en mesure de repérer toutes les attaques frontales provenant de l'extérieur avant qu'elles n'atteignent le pare-feu. Cela provoquera un nombre élevé d'alertes, ce qui compliquera la consultation des journaux.
- Position (2) : Si l'IDS est placé dans la DMZ, il pourra identifier les attaques qui ont réussi à passer le pare-feu et qui requièrent une certaine expertise pour être repérées. Les journaux seront plus faciles à lire, car les attaques ne seront pas consignées.
- Position (3) : Positionner l'IDS à cet endroit détectera les attaques internes émanant du réseau local de la société. Il pourrait être sage de choisir cette position, compte

tenu du fait que (80) des attaques proviennent de l'intérieur. En outre, si le système informatique a été contaminé par des chevaux de Troie (suite à une navigation imprudente sur Internet), leur détection et leur suppression s'effectue sans grande difficulté.

En théorie, il est recommandé de positionner des systèmes de détection d'intrusion (IDS) à trois endroits stratégiques pour maximiser leur efficacité. Les journaux générés par ces IDS peuvent ensuite être examinés à l'aide de l'application « ACID » (http ://acid-lab.sourceforge.net/), qui permet une analyse approfondie des alertes et une présentation claire des résultats via une interface web conviviale et complète.

Cependant, si une seule machine IDS peut être installée, il est préférable de la placer en position 2, qui est cruciale pour assurer le bon fonctionnement des services.

2.8 Classifications des systèmes détection d'intrusion

On peut classer les divers systèmes de détection d'intrusion existants selon plusieurs critères qui sont :

- La méthode de détection.
- Le comportement du système après la détection.
- La source des données.
- La fréquence d'utilisation.

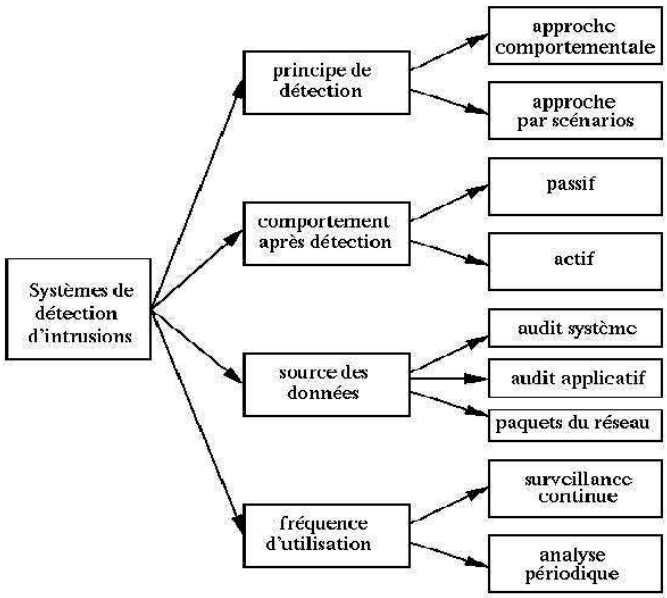


FIG. 2.7 : Classification d'un système de détection d'intrusion. [31]

2.9 Méthode de détection des IDS

On distingue deux catégories de techniques pour la détection des intrusions : Détection d'anomalies (méthode comportementale), détection par signature, également connue sous le nom de détection de mauvaise utilisation, détection basée sur l'apparence ou encore méthode scénaristique.

2.9.1 Approche par scénario ou par signature

Cette méthode repose sur la connaissance des techniques utilisées par les attaquants, stockées dans une base de données. Elle compare ensuite l'activité de l'utilisateur à cette base de données pour détecter les événements qui sortent du cadre normal. Lorsqu'une activité suspecte est identifiée, elle déclenche une alerte pour signaler un potentiel risque. [29]

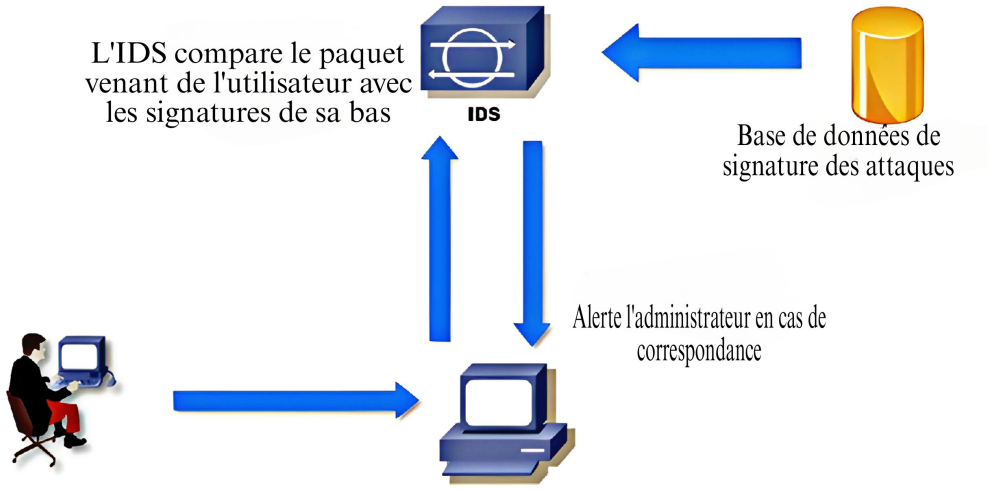


Fig. 2.8 : Procédure de détection d'attaques d'un IDS à base de signature. [32]

2.9.2 Approche comportementale (détection d'anomalies)

Cette méthode repose sur la connaissance des techniques utilisées, la détection implique d'observer le comportement de l'utilisateur ou d'une application dans le but d'identifier une éventuelle intrusion. Elle se fonde sur l'établissement d'un modèle basé sur le comportement normal du système, et toute déviation de ce modèle est surveillée. Par conséquent, toute activité suspecte peut être identifiée et reportée, comme une intrusion éventuelle.

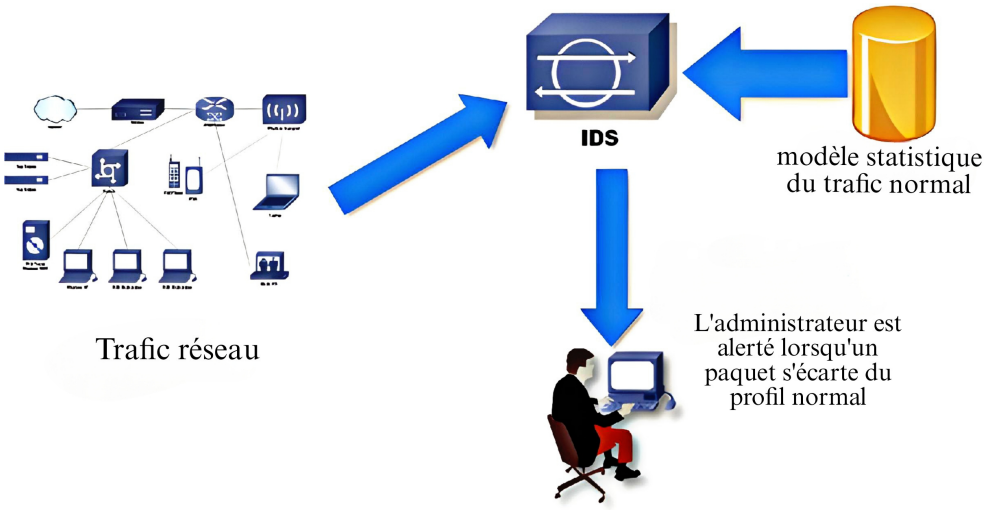


FIG. 2.9 : Procédure de détection d'attaques d'un IDS à base base d'anomalies. [32]

2.10 Comparaison entre les deux approches

Le tableau suivant établit une comparaison entre les caractéristiques des deux précédentes approches :

Signature	**Anomalie**
Pas de faux positifs (FP).	Faux positifs nombreux.
Pas de détection d'attaques non connues.	Prise en compte de nouvelles attaques.
Mise à jour rapide	Mise à jour délicate (phase d'entraînement)

TAB. 2.1 : Comparaison entre les deux approches.

2.11 Les Mesures D'évaluation de l'IDS

Il y a plusieurs critères de classification pour les IDS, dont certains sont connus sous différentes appellations. La matrice de confusion suivante illustre un classificateur binaire, outil qui peut servir à mesurer l'efficacité d'un IDS. Dans la matrice, chaque colonne illustre les instances d'une classe prédite alors que chaque ligne illustre les instances d'une classe réelle. Les IDS sont habituellement jugés en fonction des critères de performance standards suivants [33] :

Actual Class	Predicted Class	
	Normal	Attack
Normal	True negative (TN)	False Positive (FP)
Attack	False Negative (FN)	True Positive (TP)

FIG. 2.10 : Matrice de confusion pour le système IDS.

2.11.1 Taux de vrai positifs (TPR)

Le taux de vrais positifs (TPR, True Positive Rate) est calculé comme le rapport entre le nombre d'attaques correctement détectées et le nombre total d'attaques. Si toutes les intrusions sont détectées, le TPR atteint une valeur de 1, un scénario idéal mais extrêmement rare pour un IDS. Le TPR est également connu sous le nom de taux de détection (DR, Detection Rate) ou sensibilité. Il peut être exprimé mathématiquement comme suit :

TPR = TP / (TP + FN).

2.11.2 Taux de faux positifs (FPR)

Le taux de faux positifs (FPR, False Positive Rate) est défini comme le rapport entre le nombre d'instances normales qui ont été incorrectement classées comme des attaques et le nombre total d'instances normales. Il peut être exprimé mathématiquement comme suit :

FPR = FP / (FP + TN).

2.11.3 Taux de faux négatifs (FNR)

On parle de faux négatifs (False Negatives) lorsqu'un système de détection échoue à identifier une anomalie et la classe à tort comme une activité normale. Ce phénomène reflète une lacune dans la capacité de détection du système. Il peut être exprimé mathématiquement par la formule suivante :

FNR = FN / (FN + TP).

2.11.4 Taux de classification (CR) ou précision

Le taux de classification (CR, Classification Rate) mesure la précision avec laquelle un IDS identifie correctement le comportement du trafic, qu'il soit normal ou anormal. Il est défini comme le pourcentage des instances correctement prédites par rapport au nombre total d'instances. Il peut être exprimé mathématiquement comme suit :

CR = (TP + TN) / (TP + TN + FN + FP).

2.12 Comportement d'un IDS en cas d'attaque

On distingue deux catégories d'IDS : les actifs et les passifs.

2.12.1 Réponse active

L'objectif de la réponse active est, quant à lui, de stopper une attaque dès sa détection, sans nécessiter d'intervention humaine. Deux méthodes principales sont alors mises à disposition : la reconfiguration du pare-feu et l'interruption de la session TCP en cours.

La reconfiguration du pare-feu permet de bloquer directement le trafic malveillant au niveau du pare-feu, soit en fermant le port exploité, soit en interdisant l'adresse IP de l'attaquant. Cette fonctionnalité dépend toutefois du type de pare-feu utilisé, car tous ne supportent pas la reconfiguration automatique via un système de détection d'intrusion (IDS). De plus, cette reconfiguration est limitée par les capacités techniques du pare-feu.

Par ailleurs, l'IDS peut également interrompre une connexion déjà établie entre l'agresseur et sa cible, afin d'empêcher toute transmission de données ou modification du système visé.

2.12.2 Réponse passive

Un IDS en mode passif réagit à une intrusion détectée en enregistrant celle-ci dans un fichier de log, qui sera ensuite examiné par le responsable de la sécurité. Il peut également déclencher des alertes, telles que l'envoi de courriers électroniques à un ou plusieurs utilisateurs, entre autres mesures. Cette approche vise principalement à documenter les attaques afin de prévenir leur récurrence, mais elle ne permet pas d'empêcher concrètement la survenue d'une intrusion.

2.13 Limites des IDS

Parmi les faiblesses des IDS, on trouve : [34]

- Nombreux faux positifs.
- Configuration complexe et longue.
  - Nombreux faux positifs après configuration.
- Pas de connaissance de la plate-forme.
  - De ses vulnérabilités.
  - Du contexte métier.
- Les attaques applicatives sont difficilement détectables.

  - Injection SQL.
  - Exploitation de CGI mal conçus.

- Attaque contre IDS lui-même.
- Ils ne peuvent pas compenser les trous de sécurité dans les protocoles réseaux.
- Ils ne peuvent pas compenser des manques significatifs dans votre stratégie de sécurité, votre politique de sécurité ou votre architecture de sécurité.

2.14 Conclusion

En conclusion, ce chapitre a mis en lumière l'importance croissante des Systèmes de Détection d'Intrusion (IDS) dans le paysage de la cybersécurité moderne. Leur fiabilité et leur capacité à détecter les menaces en temps réel en font des outils incontournables dans les stratégies de protection des systèmes informatiques. De plus, leur adoption généralisée s'explique par les nombreux avantages qu'ils offrent par rapport aux autres solutions de sécurité. Ces systèmes ne se limitent pas à protéger les entreprises contre les attaques, mais jouent également un rôle clé dans la préservation de l'intégrité des données et la continuité des opérations. Ainsi, ils s'imposent comme des piliers essentiels pour répondre aux défis croissants de la sécurité informatique.

Chapitre 3

Apprentissage profonde

3.1 Introduction

L'intelligence artificielle (IA) est l'un des domaines modernes qui a provoqué une transformation significative dans de nombreux secteurs. Grâce à sa capacité à apprendre à partir des données et à les traiter, elle est devenue un outil puissant pour résoudre des problèmes complexes. Parmi les techniques les plus importantes de l'intelligence artificielle, on trouve l'apprentissage automatique (Machine Learning) et l'apprentissage profond (Deep Learning), qui sont de plus en plus utilisés dans les applications modernes, notamment pour l'analyse des données et la détection des motifs.

Avec l'émergence de nouveaux défis liés à la confidentialité et à la sécurité des données, le concept d'apprentissage fédéré (Federated Learning) s'est imposé comme une solution innovante. Cette approche permet d'entraîner des modèles d'IA directement sur des dispositifs distribués, sans centraliser les données, préservant ainsi la vie privée tout en maintenant des performances élevées.

Ce chapitre se concentre sur l'explication des bases théoriques et pratiques de l'apprentissage profond. Dans un premier temps, nous présenterons une définition de l'intelligence artificielle et de l'apprentissage automatique, en mettant en avant les différents types d'apprentissage. Ensuite, nous approfondirons les concepts de l'apprentissage profond en expliquant la différence avec l'apprentissage automatique traditionnel et en détaillant les principes fondamentaux qui le sous-tendent, tels que la propagation et la propagation à l'avant (Forward Propagation) ainsi que la rétropropagation (Back Propagation).

3.2 Définition d'intelligence artificielle (AI)

L'intelligence artificielle (IA) désigne un domaine de l'informatique qui se concentre sur la création de systèmes capables de simuler des fonctions cognitives humaines, telles que l'apprentissage, la prise de décision.La capacité à résoudre des problèmes et à comprendre le langage naturel.Elle repose sur des algorithmes et des modèles mathématiques qui permettent aux machines d'analyser des données, d'apprendre à partir de celles-ci, et de prendre des décisions autonomes ou semi-autonomes. AI encompasses various subfields, including : Machine Learning (ML),Deep Learning (DL).

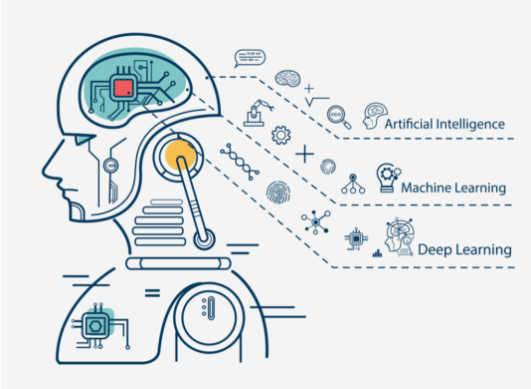


Fig. 3.1 : Exemple de l'intelligence artificielle.
[35]

3.3 L'apprentissage automatique(Machine Learning)

3.3.1 Définition

L'apprentissage automatique, une discipline clé de l'intelligence artificielle, offre aux machines la capacité d'apprendre à partir de données historiques afin de réaliser des tâches de manière autonome. Les performances de ces systèmes dépendent fortement de la qualité, de la diversité et de la préparation des données utilisées (notamment en termes d'absence de biais et d'annotations précises). En s'appuyant sur des algorithmes sophistiqués et des techniques statistiques avancées, l'apprentissage automatique permet d'améliorer les prédictions et les performances des systèmes sans qu'une programmation explicite soit nécessaire. Parmi ses applications courantes, on trouve le filtrage des courriels indésirables, les systèmes de recommandation de produits et la détection des fraudes. [36]

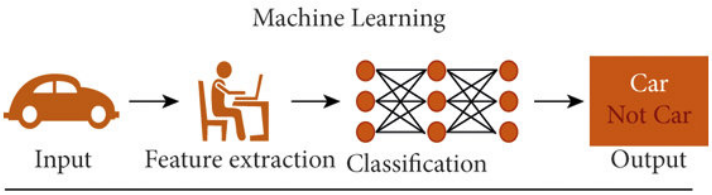


Fig. 3.2 : Exemple de machine learning.
[36]

3.3.2 Type d'apprentissage automatique

Le domaine de l'apprentissage automatique se divise en trois catégories principales : l'apprentissage supervisé, l'apprentissage non supervisé et l'apprentissage par renforcement.

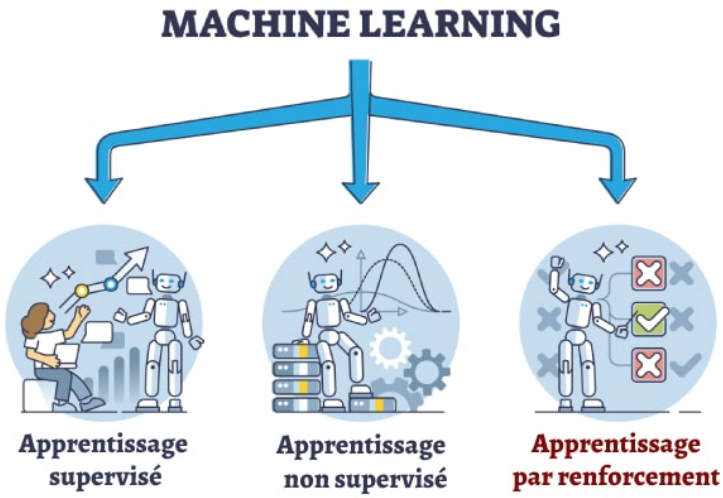


Fig. 3.3 : Exemple type d'apprentissage automatique .
[37]

3.3.2.1 L'apprentissage supervisé

L'apprentissage supervisé est une technique d'apprentissage automatique où le modèle est formé à partir d'un ensemble de données contenant des entrées et des sorties prédéfinies. L'objectif est de permettre au modèle de comprendre les schémas et les relations dans les données, afin de prédire correctement les sorties pour de nouvelles entrées.

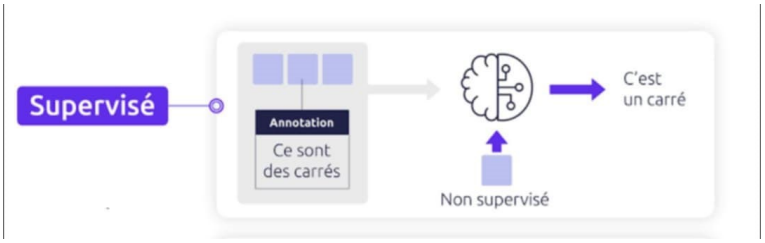


Fig. 3.4 : Exemple l'apprentissage supervisé.
[38]

3.3.2.2 L'apprentissage non supervisé

L'apprentissage non supervisé est une méthode d'apprentissage automatique où le modèle est formé à partir de données non étiquetées, c'est-à-dire sans sorties prédéfinies. L'objectif est d'identifier des structures ou des relations cachées dans les données, telles que le regroupement en clusters ou la réduction de dimensions.

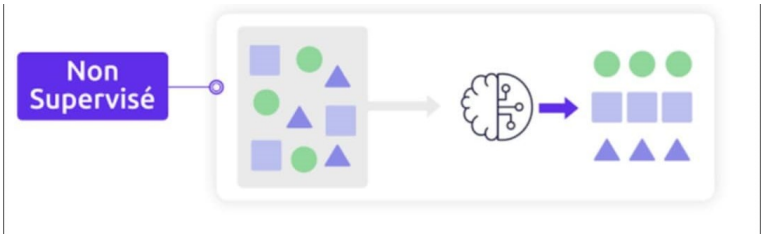


Fig. 3.5 : Exemple l'apprentissage non supervisé.
[38]

3.3.2.3 L'apprentissage par renforcement

L'apprentissage par renforcement est une méthode d'apprentissage automatique où le modèle apprend à interagir avec son environnement en prenant des décisions basées sur un processus d'essais et d'erreurs. Le modèle est récompensé pour les actions correctes ou pour l'atteinte d'objectifs définis, ce qui lui permet de développer des stratégies optimales pour maximiser son efficacité.

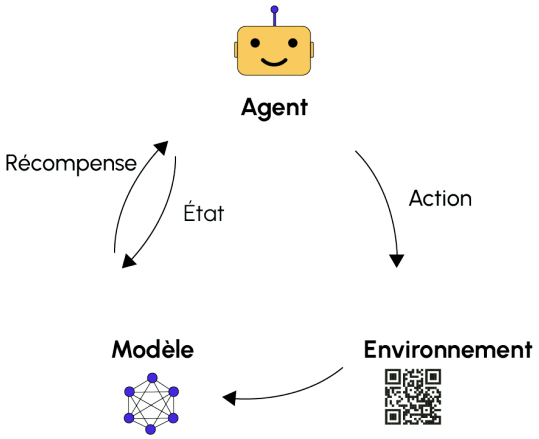


FIG. 3.6 : Exemple l'apprentissage par renforcement.
[39]

3.4 L'apprentissage profond(Deep Learning)

3.4.1 Définition

L'apprentissage profond est une branche spécialisée de l'apprentissage automatique. En termes techniques, il opère de la même façon que l'apprentissage automatique, mais avec des capacités et des méthodes distinctes. Dans le cadre de l'apprentissage profond, les modèles exploitent diverses couches pour assimiler et déceler des concepts à partir des données. [36]

Le Deep Learning, ou apprentissage profond, s'inspire du fonctionnement des neurones présents dans le cerveau humain, ce qui constitue la base de l'idée des réseaux neuronaux artificiels. On fait aussi référence à l'apprentissage profond ou aux réseaux de neurones profonds.

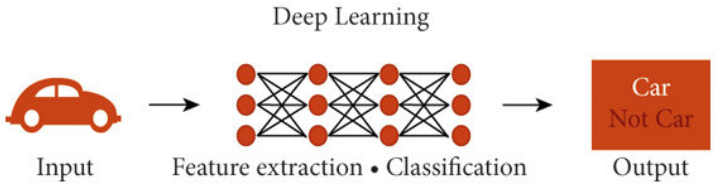


FIG. 3.7 : Exemple deep learning.
[36]

3.4.2 Compariason entre l'apprentissage automatique et l'apprentissage profond.

On an résumer la comparaison entre les deux types d'apprentissage dans le tableau suivant :

	Apprentissage profond	**Apprentissage automatique**
Exigences en matiére de donneés	Nécessite de grandes qualités de données.	.Peut s'entrainer sur moins de données
Précision	Fournit une grande precision .	Donne moins de precision.
Temps de d'éxecution	Prend plus de temps pour s'entrainer.	Prend moins de temps pour s'entrainer
Dépendancematérielle	Nécessite un GPU pour s'entrainer correctement.	Trains sur CPU.
Réglage paramétres Peut etre réglé de différentes maniéres.	Capacités de réglage limitées.	Capacités de réglage limitées

TAB. 3.1 : comparaison entre l'apprentissage profond et l'apprentissage automatique.

3.4.3 Fonctionnements

Le fonctionnement de l'apprentissage profond se base sur un réseau de neurones artificiels organisés en couches hiérarchiques. reliés Tout d'abord un réseau de neurones artificiels est composé de nombreux neurones artificiels entre eux selon une architecture de réseau spécifique.

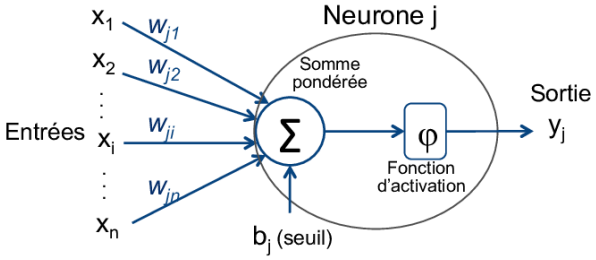


FIG. 3.8 : La structure d'un neurone artificiel.
[40]

L'objectif d'un réseau de neurones est de transformer les entrées en sorties significatives. Le neurone calcule la valeur de sortie en appliquant une fonction d'activation à une somme pondérée des valeurs d'entrée. Et fondamentalement, chaque neurone d'un réseau peut être implémenté comme indiqué ci-dessus et il est possible de constater que le neurone artificiel est composé de six éléments de base, à savoir :

- Entrées : cela représente les caractéristiques et essentiellement l'ensemble de données entrant dans les réseaux.
- Poids : cela représente la dimension ou la force de la connexion entre les unités. Si le poids du nœud 1 au nœud 2 a une quantité plus élevée, alors le neurone 1 a une influence plus considérable sur le neurone 2.

- Biais : c'est la même chose que l'interception ajoutée dans une équation linéaire. C'est un neurone spécial ajouté à chaque couche dans le réseau neuronal, qui stocke simplement la valeur de 1 dont la tâche est de modifier la sortie ainsi que la somme pondérée de l'entrée vers l'autre neurone.

- Somme nette : elle calcule la somme totale.

- Fonction d'activation : un neurone peut être activé ou non, ce qui est déterminé par une fonction d'activation. La fonction d'activation calcule une somme pondérée et ajoute en plus le biais pour donner le résultat [41].

- Sortie : elle consiste en la valeur finale produite par le neurone pour un ensemble particulier de signaux d'entrée [42].

3.4.4 Les couches d'un Réseau de neurone

Typiquement, un réseau neuronal artificiel se divise en trois segments identifiés comme couches, que l'on nomme généralement : [41]

- Couche Entrée : (InputLayer) c'est l'ensemble de neurones qui porte le signal d'entré du réseau, et par la suite tous les neurones de cette couche sont reliés à la couche suivante.

- Couche cachée : (Hiddenlayers) elles peuvent être une ou plusieurs, c'est ici où les relations entre les variables vont être mises en exergue. Le choix du nombre de couches et de neurones est intuitif et nécessite de l'expérience venant de l'expert.

- Couche sortie : (OutputLayer) elle représente le résultat du réseau de neurones c'est ce qu'on appelle la prédiction.

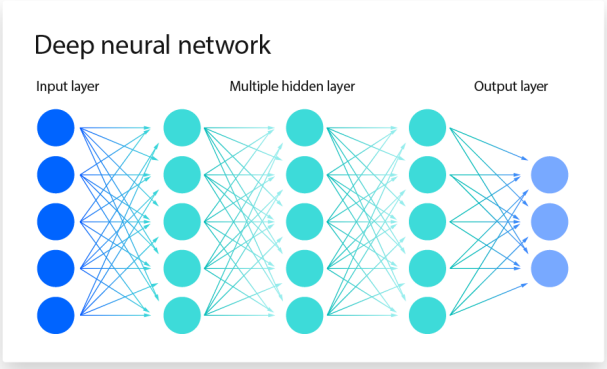


Fig. 3.9 : Les couches d'un Réseau de neurone.
[43]

3.4.5 Les fonctions d'activations

Les fonctions d'activation sont des formules mathématiques qui décident de la sortie d'un réseau de neurones. Chaque neurone du réseau est associé à une fonction qui détermine si ce dernier doit être activé (« déclenché ») ou non, en se basant sur la pertinence de l'information fournie par chaque neurone pour la prédiction du modèle. Les fonctions d'activation contribuent aussi à normaliser la sortie de chaque neurone dans une intervalle de 1 à 0 ou entre -1 et 1 :

3.4.5.1 Fonction d'activation binaire

Une fonction d'activation binaire est une fonction d'activation qui se fonde sur un critère de seuil. Si la valeur d'entrée dépasse ou est inférieure à un certain seuil, le neurone s'active et transmet un signal identique au niveau suivant. L'inconvénient d'une fonction de seuil est qu'elle

n'autorise pas les résultats à plusieurs valeurs - par exemple, elle n'est pas capable de gérer la classification des entrées en diverses catégories. [41]

3.4.5.2 Fonction d'activation linéaire

La fonction d'activation linéaire A=cx pose deux problèmes principaux :

- Problème d'apprentissage : La dérivée demeure constante, rendant la rétropropagation inefficace puisque les gradients sont indépendants des entrées, ce qui empêche la mise au point idéale des poids.
- Réduction du réseau : Avec des fonctions d'activation linéaires appliquées à chaque couche, le réseau se transforme en une simple couche, incapable de reproduire des relations non linéaires.

Donc comme des solutions :

L'emploi de fonctions d'activation non linéaires (telles que ReLU, Sigmoïde, Tanh, Softmax) apporte la complexité requise, ce qui permet au réseau de se former efficacement et de gérer des enjeux complexes.

3.4.5.3 Fonctions d'activation non linéaires

Les modèles de réseaux de neurones modernes utilisent des fonctions d'activation non linéaires. Elles permettent au modèle de créer des mappages complexes entre les entrées et les sorties du réseau, qui sont essentiels pour apprendre et modéliser des données complexes telles que des images, des vidéos, de l'audio et des ensembles de données non linéaires ou à haute dimensionnalité. Presque tous les processus imaginables peuvent être représentés sous forme de calcul fonctionnel dans un réseau de neurones, à condition que la fonction d'activation soit non linéaire. Les fonctions non linéaires résolvent les problèmes d'une fonction d'activation linéaire.

- Elles permettent la rétropropagation du gradient car elles ont une fonction dérivée qui est liée aux entrées.

- Elles permettent l'empilement de plusieurs couches de neurones pour créer un réseau neuronal profond. De multiples couches cachées de neurones sont nécessaires pour apprendre des ensembles de données complexes avec des niveaux élevés de précision. [41]

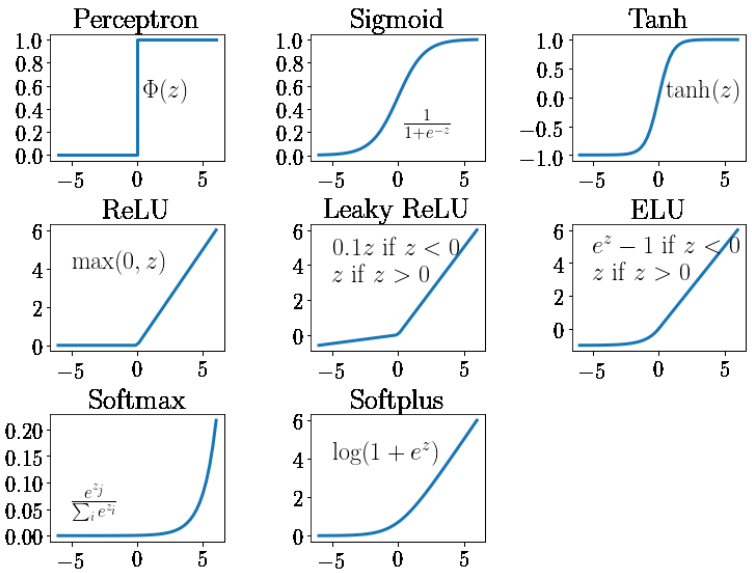


FIG. 3.10 : Les fonctions d'activation.
[44]

3.5 Topologies des réseaux de neurones

Il existe deux topologies des réseaux de neurones comme suite :

3.5.1 Propagation avant (forward propagation)

Ceci est réalisé en se basant sur les valeurs des résultats via les entrées. Cette procédure se réalise en utilisant l'une des formules d'activation comme la Sigmoid, Relu, Tanh, Softmax, entre autres. Avant le commencement, certaines valeurs de theta sont fixées.

3.5.2 Back propagation

Les poids sont déterminés de façon inverse. Cela consiste à identifier l'écart entre la valeur prévisionnelle et la valeur concrète, puis à appliquer une différenciation partielle. On s'en sert pour ajuster les valeurs de poids présumées.

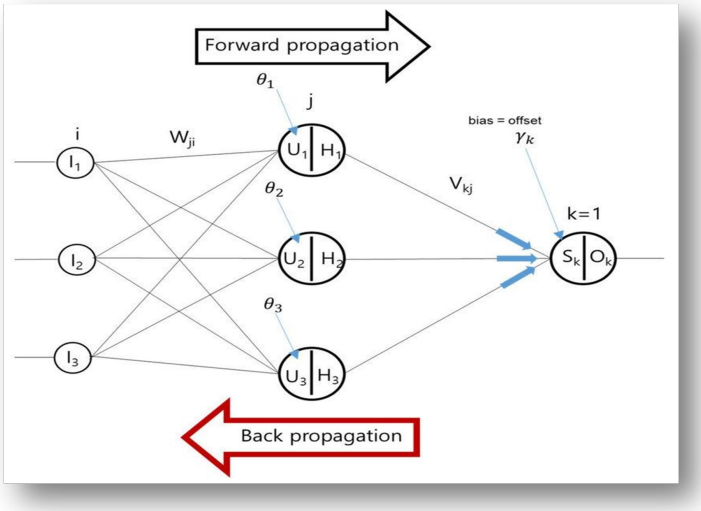


FIG. 3.11 : Topologies des réseaux de neurones.
[45]

3.6 Les modules du deep learning

3.6.1 Le réseau neuronal profond(deep neural network(DNN))

Les réseaux neuronaux profonds (DNN), également appelés réseaux de neurones profonds, sont composés d'un ensemble de neurones organisés en plusieurs couches, appelées perceptrons multicouches (MLP). Ils se distinguent des réseaux neuronaux traditionnels (Artificial Neural Network) par leur profondeur et le nombre de couches et de neurones qui les composent. Lorsqu'un ANN possède deux couches cachées ou plus, il est connu sous le nom de réseau neuronal profond. Leur objectif est de modéliser des données avec des architectures complexes en combinant différentes transformations non linéaires. [46]

Le concept de base du perceptron a été introduit par Rosenblatt en 1958 [41]. Le perceptron calcule une sortie unique à partir de multiples entrées réelles (xi) en effectuant. une combinaison linéaire en fonction de ses poids d'entrée (w), puis en appliquant une fonction d'activation non linéaire. Mathématiquement, cela peut être exprimé comme suit : y = $\sigma(\Sigma n{=}1$ Wixi + b) = (WT X + b) Où :

- W : vecteur des poids
- X : vecteur des entrées
- b : biais
- σ : fonction d'activation

Un MLP typique comprend une couche d'entrée constituée de nœuds sources, une ou plusieurs couches cachées contenant des nœuds de calcul, et une couche de sortie composée de nœuds. Le signal d'entrée se propage de couche en couche dans le réseau. Les réseaux

DNN sont généralement utilisés dans des problèmes d'apprentissage supervisé. La formation du modèle (apprentissage) consiste à ajuster tous les poids et les biais à leurs valeurs optimales. couches de réduction d'échantillonnage. [42]

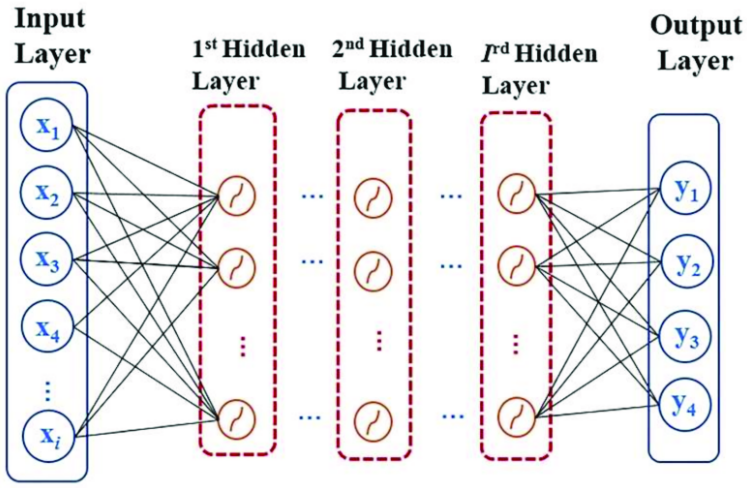


FIG. 3.12 : La topologie DNN.
[47]

3.6.2 Le réseau neuronal convolutif (CNN)

Le terme "réseau neuronal convolutif "fait référence à l'utilisation par le réseau d'une procédure mathématique connue sous le nom de convolution. Les réseaux convolutifs sont un type de réseau neuronal qui remplace la multiplication générale de matrices dans au moins une couche par une convolution. Le CNN est l'un des meilleurs algorithmes d'apprentissage pour effectuer l'opération de convolution, ce qui facilite l'extraction de caractéristiques pertinentes à partir de points de données localement connectés. La sortie des noyaux convolutifs est ensuite transmise à la fonction d'activation (une unité de traitement non linéaire) qui prend en charge à la fois l'apprentissage des abstractions et l'introduction de non-linéarité dans l'espace des caractéristiques. Cette non-linéarité génère divers motifs d'activation, ce qui facilite l'apprentissage des différences de signification dans les images. La topologie CNN est divisée en plusieurs étapes d'entraînement qui comprennent des couches convolutives, des unités de traitement non linéaires et des couches de réduction d'échantillonnage. [42]

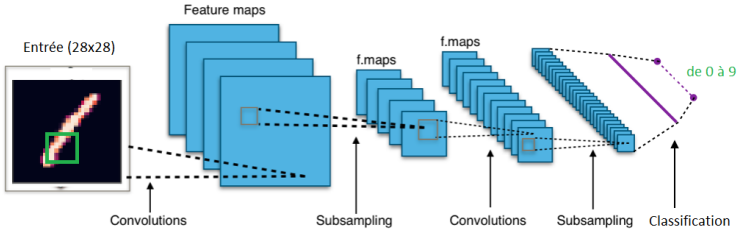


FIG. 3.13 : La topologie CNN.
[48]

3.6.3 Réseaux de Neurones Récurrents (RNN)

Les réseaux récurrents sont fréquemment utilisés lorsqu'il y a une entrée séquentielle. Ces entrées sont couramment rencontrées lors du traitement de texte ou de la voix. Au lieu de traiter complètement un seul exemple, avec des problèmes séquentiels, seule une partie du problème peut être traitée à la fois. Par exemple, pour construire un réseau qui écrit des pièces de théâtre shakespeariennes, l'entrée serait naturellement les pièces existantes de Shakespeare. Ce que le réseau doit apprendre à faire, c'est de prédire le mot suivant de la pièce. Pour ce faire, il doit se souvenir du texte qu'il a vu jusqu'à présent. Les réseaux récurrents proposent un mécanisme pour cela. Ils permettent également de construire des modèles qui fonctionnent naturellement avec des entrées de longueurs variables (comme des phrases ou des morceaux de discours, par exemple). [46]

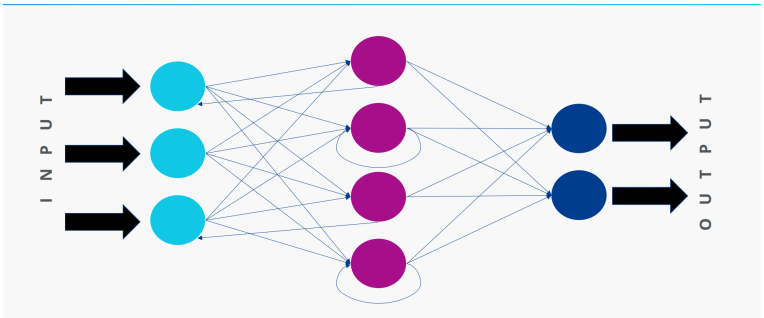


FIG. 3.14 : La topologie de RNN.
[47]

3.6.4 Réseaux Long Short-Term Memory (LSTM)

Les réseaux de mémoire à long terme généealement simplement appelés (LSTM) sont un type spécial de RNN, capable d'apprendre les dépendances à long terme. Ils ont été introduits par (Hochreiter et Schmidhuber, 1997), et ont été affinés et popularisés par de nombreuses personnes dans les travaux suivants. Ils fonctionnent extrêmement bien sur une grande variété de problèmes et sont maintenant largement utilisés (Hochreiter et Schmidhuber, 1997) Les LSTM sont explicitement conçus pour éviter le problème de dépendance à long terme. Se souvenir des informations pendant de longues périodes est pratiquement leur comportement par défaut, pas quelque chose qu'ils ont du mal à apprendre ! Tous les réseaux de neurones récurrents ont la forme d'une chaîne de modules répétitifs de réseau de neurones. Dans les RNN standard, ce module répétitif aura une structure très simple, telle qu'une seule couche de tanh.

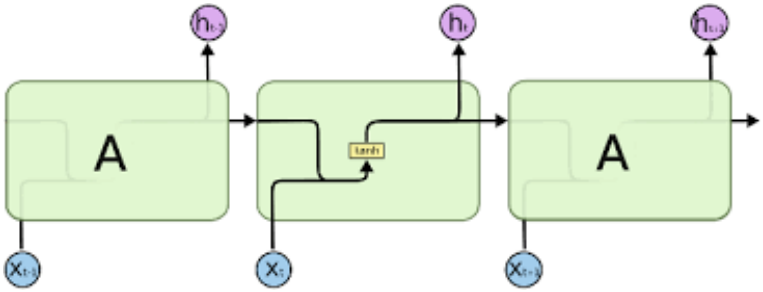


FIG. 3.15 : Le module répétitif dans un RNN standard contient une seule couche.
[49]

Les LSTM ont également une structure en chaîne, mais le module répétitif à une structure différente. Au lieu d'avoir une seule couche de réseau neuronal, il y en a quatre, interagissant d'une manière très spéciale.

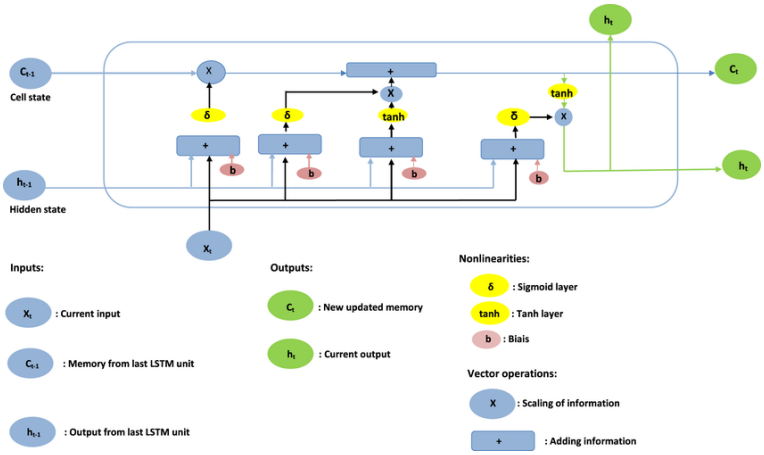


FIG. 3.16 : : Le module répétitif dans un LSTM.
[49]

Un réseau LSTM typique est composé de blocs de mémoire appelés cellules. Deux états sont en cours transféré à la cellule suivante, l'état de la cellule et l'état caché. L'état cellulaire est la chaîne principale de flux de données, qui permet aux données de circuler en avant essentiellement inchangées. Cependant, certaines transformations linéaires peuvent se produire. Les données peuvent être ajoutées ou supprimées de l'état de la cellule via des portes sigmoïdes. Une porte est similaire à une couche ou à une série d'opérations matricielles, qui contiennent différents poids individuels. Les LSTM sont conçus pour éviter le problème de dépendance à long terme car ils utilisent des portes pour contrôler le processus de mémorisation.

3.6.5 Réseaux Gated Recurrent Unit (GRU)

Sont un système de porte dans les réseaux de neurones récurrents, introduit en 2014 par Kyunghyun Cho et al.

Le GRU est comme une longue mémoire à court terme (LSTM) avec une porte d'oubli, mais a moins de paramètres que LSTM, car il n'a pas de porte de sortie.

Les performances de GRU sur certaines tâches de modélisation de musique polyphonique, de modélisation de signaux vocaux et de traitement du langage naturel se sont avérées similaires à celles de LSTM.

Les GRU ont montré que le déclenchement est en effet utile en général et l'équipe de Bengio a conclu qu'aucune conclusion concrète sur laquelle des deux unités de déclenchement était la meilleure.

3.6.5.1 Les Composants Principaux de GRU

- La Porte de Mise à Jour (Update Gate) :

  -Contrôle la quantité d'informations de l'état précédent (hidden state) qui sera transmise à l'état actuel. -Aide à décider ce qu'il faut conserver du passé.

- La Porte de Réinitialisation (Reset Gate) :

  -Utile pour "oublier partiellement" les informations anciennes. -Contrôle la quantité d'informations de l'état précédent qui doit être oubliée.

- Le Nouveau Contenu de Mémoire (New Memory Content) :

  -Calculé en fonction de l'entrée actuelle et de l'état précédent, tout en étant modulé par la porte de réinitialisation.

- L'État Actuel (Current State) :

  -Combine l'état précédent et le nouveau contenu de mémoire à l'aide de la porte de mise à jour.

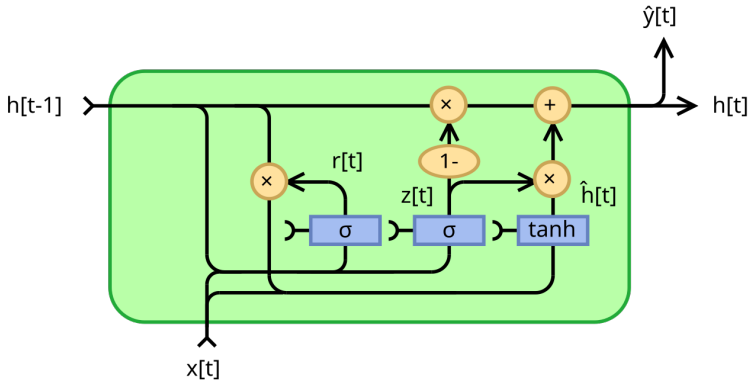


Fig. 3.17 : Unité de base GRU.
[49]

Après avoir exploré les principaux modules et concepts de l'apprentissage profond, nous introduisons désormais l'apprentissage fédéré (Federated Learning) comme une extension innovante répondant aux défis de confidentialité et de traitement décentralisé des données.

3.7 Apprentissage Fédéré

Apprentissage fédéré (FL : Federated Learning), est une méthode d'apprentissage automatique décentralisée qui permet à plusieurs appareils ou organisations de collaborer pour entraîner un modèle global sans partager leurs données brutes. Au lieu de centraliser les données sur un serveur, chaque participant conserve ses données localement et ne partage que les mises à jour du modèle (poids ou gradients).

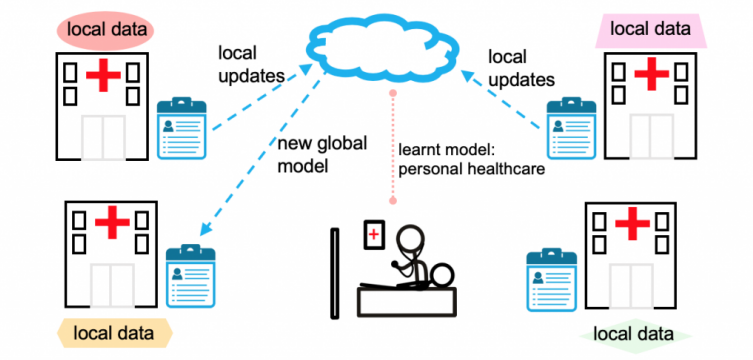


Fig. 3.18 : Apprentissage Fédéré
[50]

3.8 Les aspects fondamentaux de l'apprentissage fédéré (Federated Learning)

3.8.1 Apprentissage centralisé (centralized Learning)

L'apprentissage fédéré centralisé est un paradigme dans lequel un serveur central joue un rôle clé dans la coordination du processus d'apprentissage. Les appareils locaux entraînent leurs modèles sur leurs propres données, puis envoient uniquement les mises à jour des modèles (telles que les poids ou gradients) au serveur central. Ce serveur agrège ces mises à jour, généralement à l'aide d'algorithmes comme Federated Averaging, afin de constituer un modèle global amélioré. Ce modèle global est ensuite redistribué aux appareils pour une nouvelle itération d'entraînement local. Ce mécanisme permet de préserver la confidentialité des données, puisque les données brutes ne quittent jamais les dispositifs locaux, tout en bénéficiant d'une amélioration continue du modèle grâce à la coordination centrale. Contrairement aux approches complètement décentralisées, l'apprentissage fédéré centralisé repose sur ce serveur central, facilitant ainsi la gestion et la supervision du processus d'apprentissage.[51]

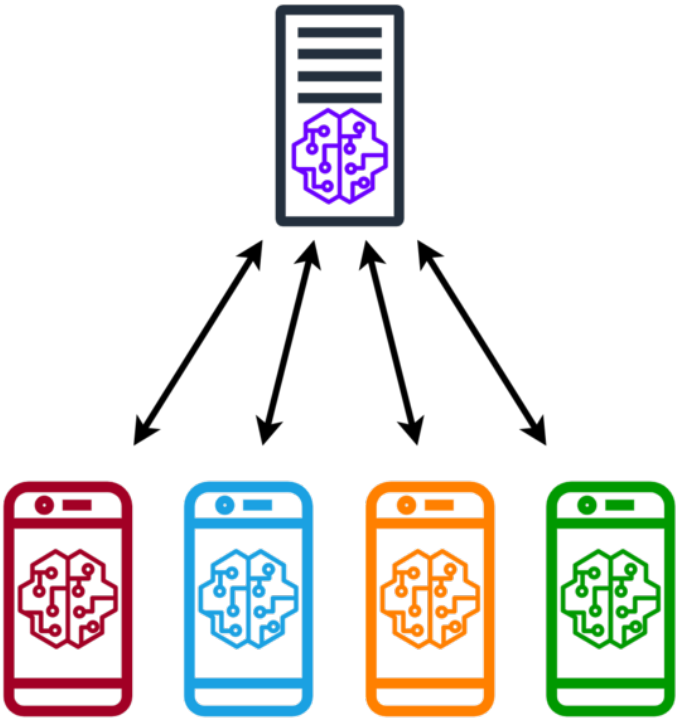


FIG. 3.19 : L'apprentissage centralisé.
[51]

3.8.2 Apprentissage décentralisé (Decentralized Learning)

L'apprentissage décentralisé est une approche d'apprentissage automatique où les données restent localisées sur des dispositifs ou des systèmes distribués, plutôt que d'être centralisées sur un serveur unique. Dans ce contexte, chaque dispositif effectue un entraînement local sur ses propres données et partage uniquement des informations nécessaires, comme les mises à jour du modèle (poids ou gradients), avec un serveur central ou d'autres dispositifs.

Cette méthode offre plusieurs avantages :

- Confidentialité des données : Les données sensibles ne quittent jamais leur emplacement d'origine, réduisant ainsi les risques de violations de la vie privée.
- Réduction des coûts de communication : Seules les mises à jour sont transmises, ce qui limite l'utilisation de la bande passante.
- Robustesse : L'absence de dépendance à un serveur central diminue les risques de panne ou de points de défaillance uniques.

L'apprentissage décentralisé est utilisé dans des contextes où la confidentialité, la latence et l'efficacité des ressources sont des préoccupations majeures, comme dans l'Internet des objets (IoT), les systèmes médicaux ou les applications mobiles.

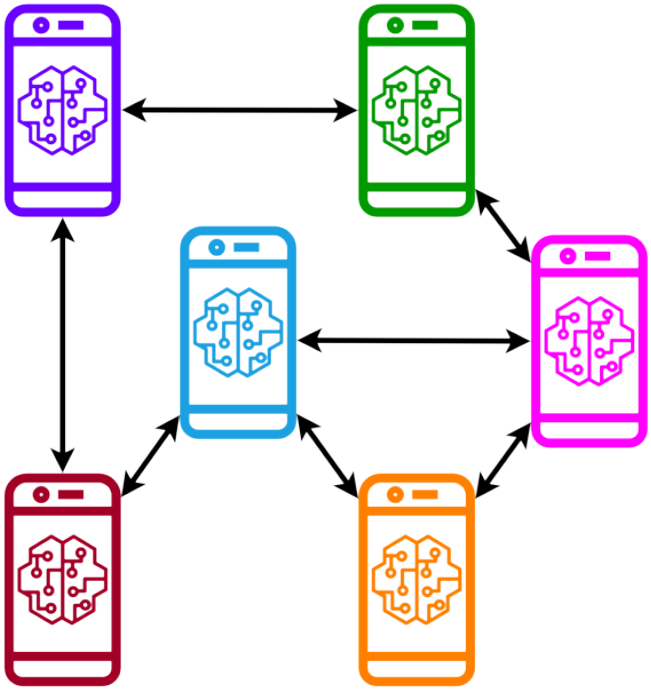


FIG. 3.20 : L'apprentissage décentralisé.
[51]

3.8.3 Processus de l'apprentissage fédéré (Federated Learning Process)

Le Processus de l'apprentissage fédéré est une série d'étapes organisées permettant à plusieurs dispositifs ou organisations de collaborer pour entraîner un modèle d'apprentissage automatique commun, sans partager leurs données locales. L'objectif principal de ce processus est de garantir la confidentialité des données tout en optimisant leur utilisation via une méthode d'apprentissage décentralisée. [52]

3.8.3.1 Étapes principales du processus :

- Initialisation du modèle global (Model Initialization) : Un modèle de base est créé par un serveur central et distribué aux dispositifs participants.

- Entraînement local (Local Training) : Chaque dispositif entraîne le modèle sur ses données locales.

  -Les données restent sur le dispositif.

  -Seules les mises à jour nécessaires (poids ou gradients) sont générées.

- Envoi des mises à jour (Update Collection) : Les dispositifs envoient leurs mises à jour locales au serveur central via une connexion sécurisée, sans transmettre les données brutes.

- Agrégation des mises à jour (Model Aggregation) : Le serveur central regroupe les mises à jour provenant des dispositifs pour améliorer le modèle global.

  -Des algorithmes comme FedAvg sont souvent utilisés pour l'agrégation.

- Redistribution du modèle (Model Redistribution) : Le modèle global mis à jour est renvoyé aux dispositifs participants pour de nouvelles itérations d'entraînement.

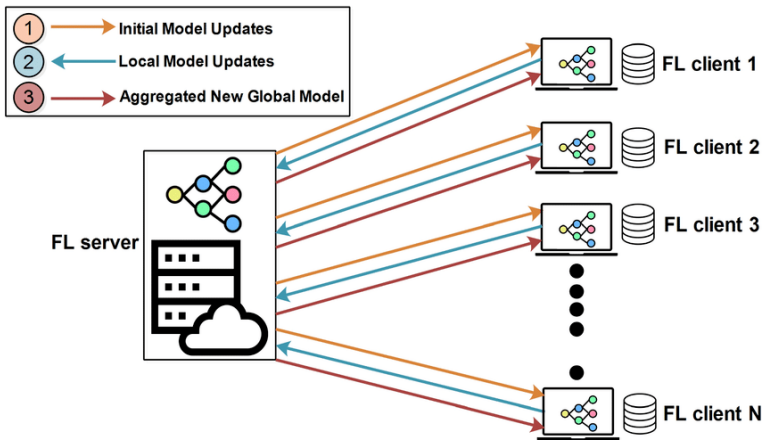


Fig. 3.21 : Processus de l'apprentissage fédéré.
[52]

3.9 Algorithmes de l'Agrégation des Modèles dans l'Apprentissage Fédéré

Les algorithmes d'agrégation des modèles jouent un rôle essentiel dans l'apprentissage fédéré. Ils permettent de combiner les mises à jour des modèles locaux (réalisées sur différents appareils) en un modèle global tout en respectant la confidentialité des données. Voici les principales méthodes :

3.9.1 Federated Averaging

L'algorithme Federated Averaging est une méthode populaire utilisée dans l'apprentissage fédéré pour agréger les mises à jour des modèles provenant des appareils locaux. Chaque appareil effectue un entraînement local sur ses données pendant plusieurs itérations, puis envoie ses mises à jour (poids ou gradients) au serveur central. Le serveur central calcule une moyenne pondérée de ces mises à jour, en fonction de la quantité de données sur chaque appareil, afin de créer un modèle global amélioré. Ce modèle global est ensuite redistribué aux appareils pour une nouvelle phase d'entraînement local.

Cette approche permet de préserver la confidentialité des données en évitant leur transfert vers un serveur central, tout en réduisant la quantité de communication nécessaire entre les appareils et le serveur.

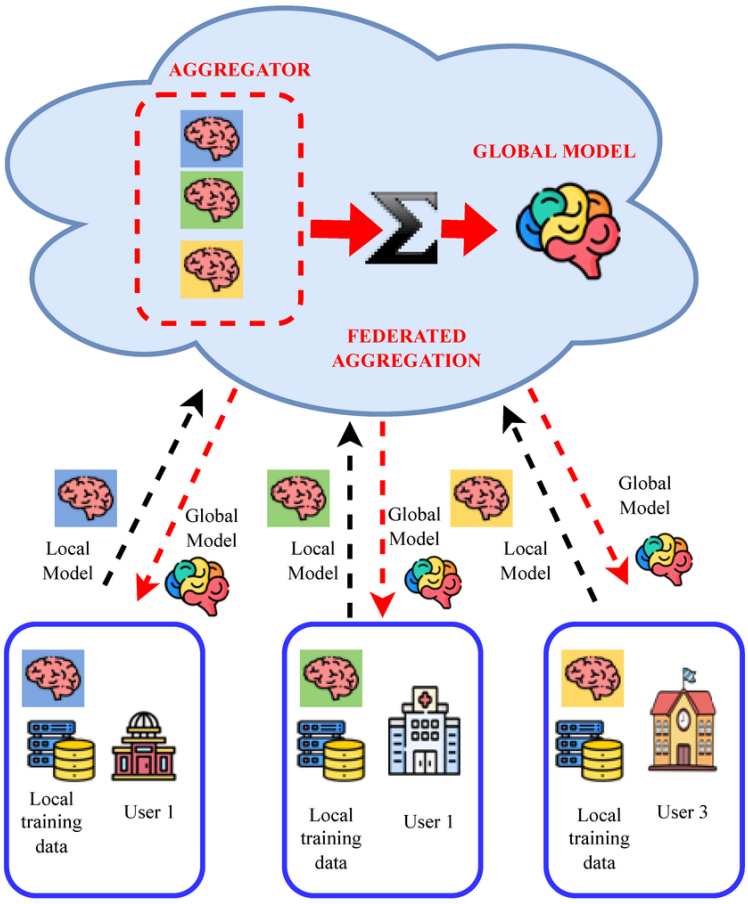


FIG. 3.22 : Federated Averaging.
[53]

3.9.2 Agrégation Pondérée

L'agrégation pondérée est une technique utilisée dans l'apprentissage fédéré pour combiner les mises à jour des modèles envoyées par les différents appareils. Contrairement à une simple moyenne, chaque mise à jour est pondérée en fonction de critères spécifiques, généralement la taille des données locales sur chaque appareil.

Cette approche permet de donner plus d'importance aux appareils disposant de plus de données, ce qui améliore la qualité du modèle global. L'agrégation pondérée aide ainsi à refléter fidèlement la contribution réelle de chaque participant dans le processus d'apprentissage, ce qui est particulièrement important lorsque les données sont inégalement réparties entre les appareils.

3.9.3 Agrégation des Gradients

L'agrégation des gradients est une technique clé dans l'apprentissage fédéré utilisée pour mettre à jour le modèle global en combinant les gradients calculés localement par les appareils participants. Chaque appareil effectue un entraînement local sur ses données, calcule les gradients résultants, puis les envoie au serveur central.

Le serveur central agrège ces gradients en effectuant une moyenne, souvent pondérée

en fonction de la taille des données locales sur chaque appareil. Une fois les gradients agrégés, ils sont utilisés pour ajuster les paramètres du modèle global.

Cette méthode permet d'intégrer efficacement les contributions des appareils participants tout en préservant la confidentialité des données, car seules les informations sur les gradients sont partagées, et non les données brutes.

3.9.4 Agrégation avec Préservation de la Confidentialité

Utilise des techniques comme la confidentialité différentielle ou le chiffrement homomorphe pour protéger les données lors de l'agrégation. Ces méthodes assurent une sécurité accrue, mais augmentent la complexité.

Ces algorithmes permettent de construire un modèle global tout en minimisant le risque de divulgation des données sensibles.

3.10 Conclusions

En conclusion, les avancées rapides dans les techniques de Deep Learning ont profondément transformé les méthodes de détection des intrusions. À travers une exploration approfondie des concepts de l'apprentissage automatique, de l'apprentissage profond, et des différents types de réseaux neuronaux, nous avons démontré le potentiel de ces outils pour analyser efficacement les données et détecter les attaques informatiques avec précision.

De plus, l'intégration des techniques d'apprentissage fédéré dans ce contexte ouvre de nouvelles perspectives pour la sécurité informatique. En permettant une collaboration décentralisée tout en préservant la confidentialité des données, l'apprentissage fédéré répond aux défis uniques posés par la protection des données sensibles, notamment dans des environnements critiques tels que l'Internet des Objets Médicaux (IoMT).

Dans le prochain chapitre, nous présenterons notre contribution spécifique à la détection des intrusions dans l'environnement IoMT, en montrant comment exploiter la puissance combinée du Deep Learning et de l'apprentissage fédéré pour relever ces défis de manière innovante et efficace.

Chapitre 4

Implémentation du système IDS pour L'IOMT

4.1 Introduction

Ce chapitre présente la méthodologie suivie pour concevoir un système IDS basé sur l'apprentissage profond destiné à sécuriser les environnements IoMT. Il détaille les étapes de préparation des données, ainsi que l'entraînement et l'évaluation des modèles neuronaux MLP, LSTM et GRU. L'intégration de l'apprentissage fédéré à travers l'algorithme FedAVG est également abordée afin d'assurer confidentialité et collaboration. Enfin, les principales étapes d'implémentation du système proposé sont explicitées.

4.2 Environement de développement

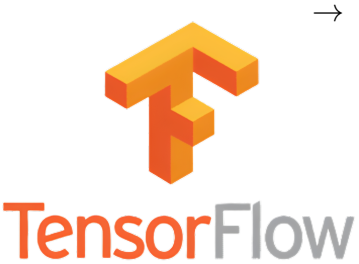
4.2.1 Langage et bibliothèques utilisées

- **Définition python :** Python est un langage de programmation puissant et facile à apprendre, il est orientée objet et de haut niveau avec sémantique dynamique. ses structures de données intégrées, combinées à un typage dynamique . Python est idéal pour l'écriture de scripts et le développement rapide d'applications dans de nombreux domaines [54].

- **Définition jupyter :**est un outil interactif open source ,qui permet aux utilisatures de créer et de partager des documents comprenant du code en direct,du texte, des visualisations et des équations...[55]

Bibliothèques utilisées :

→ **Pandas** est une bibliothèque Python puissante dédiée à l'analyse et la manipulation des données. Basée sur NumPy, elle fournit des structures comme les dataframes qui permettent de traiter, filtrer et restructurer efficacement de grands ensembles de données, facilitant ainsi l'exploration et la préparation des données pour le machine learning[56].



→ **TensorFlow** est une bibliothèque open-source développée par Google pour le calcul numérique et le machine learning, en particulier les réseaux de neurones. Elle offre un écosystème riche d'outils permettant de concevoir, entraîner et déployer des modèles d'apprentissage automatique sur diverses plateformes, du cloud aux appareils mobiles[56].

→ **Keras** est une bibliothèque open source de haut niveau dédiée au développement et à l'expérimentation rapide de modèles d'apprentissage profond. Conçue pour offrir une interface conviviale et modulaire, elle permet de construire des réseaux neuronaux complexes avec une syntaxe claire et intuitive. Keras repose sur des bibliothèques de calcul comme TensorFlow, Theano ou CNTK, et facilite le prototypage rapide, tout en assurant une compatibilité avec des architectures variées comme les MLP, CNN et RNN. Elle est largement utilisée dans le domaine de la recherche et de l'industrie pour des tâches d'analyse d'image, de texte, ou de séries temporelles[57].

→ **NumPy** est une bibliothèque Python essentielle pour le calcul scientifique. Elle fournit un objet tableau multidimensionnel performant (ndarray), ainsi qu'un ensemble complet de fonctions permettant d'effectuer des opérations mathématiques avancées, de l'algèbre linéaire, des statistiques, et des transformations numériques. Grâce à sa structure optimisée, NumPy sert de fondation à de nombreuses autres bibliothèques scientifiques comme Pandas ou Scikit-learn[58].

→ **Scikit-learn** est une bibliothèque Python open-source largement utilisée pour l'apprentissage automatique. Elle prend en charge des algorithmes supervisés et non supervisés tels que la régression linéaire, la classification et le clustering. Elle fonctionne en synergie avec NumPy et SciPy, ce qui la rend adaptée à la manipulation de données complexes[59].

Plateforme d'Exécution :

→ **Google Colab :**

Google Colaboratory (souvent abrégé en Colab) est un environnement de développement interactif basé sur le cloud, proposé par Google. Il permet d'écrire et d'exécuter du code Python dans des notebooks Jupyter hébergés à distance. Conçu pour la recherche et l'apprentissage automatique, il prend en charge les bibliothèques populaires comme TensorFlow, Keras et PyTorch, et offre gratuitement l'accès à des GPU et TPU pour l'accélération des calculs. Il est idéal pour l'enseignement, la collaboration, et les expérimentations en science des données[59].

4.3 Description du jeu de données CICIoMT2024s

Le jeu de données CICIoMT2024, élaboré par l'Institut Canadien de Cybersécurité (CIC), constitue une référence essentielle dans le domaine de la cybersécurité appliquée aux réseaux de l'Internet des objets médicaux (IoMT). Il reproduit fidèlement un trafic réseau typique des environnements IoMT, intégrant à la fois des comportements légitimes et malveillants, et couvrant divers protocoles de communication tels que le Wi-Fi, le MQTT et le Bluetooth[60]. Ce jeu de données comporte environ 9 millions d'instances, regroupant 18 scénarios distincts d'attaques ciblant spécifiquement 40 dispositifs médicaux connectés. Ces attaques sont classées en cinq catégories principales (voir Figure 4.1) : déni de service distribué (DDoS), déni de service (DoS), reconnaissance (Recon), attaques spécifiques au protocole MQTT, et usurpation d'identité (Spoofing). Cette volumétrie importante permet de développer et d'évaluer efficacement des modèles robustes d'apprentissage automatique et profond (ML/DL), capables de faire face à la complexité et à l'hétérogénéité propres aux environnements IoMT [61].

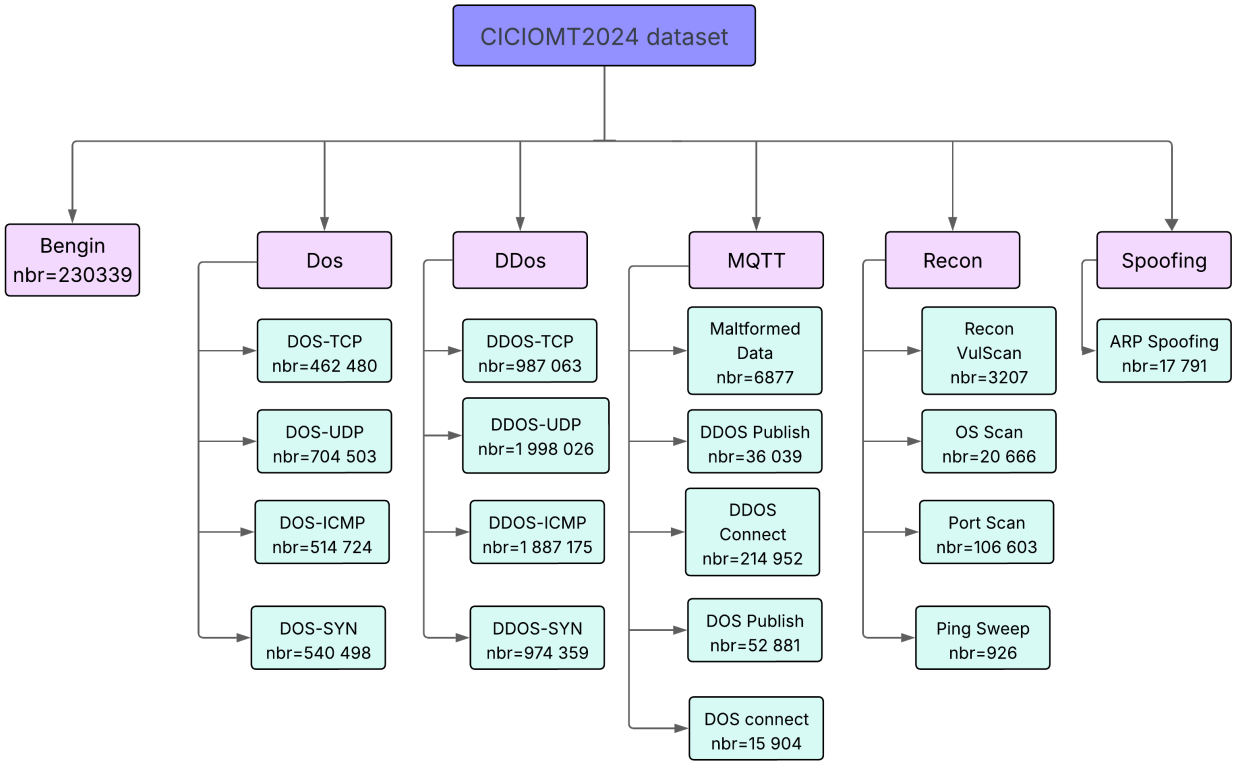


Fig. 4.1 : Ensemble de données CICIOMT2024
[61]

#	Feature	#	Feature	#	Feature
1	Header Length	16	Rst count	31	LLC
2	Duration	17	IGMP	32	Tot sum
3	Rate	18	HTTPS	33	Min
4	Srate	19	HTTP	34	Max
5	Drate	20	Telnet	35	AVG
6	Fin flag number	21	DNS	36	Std
7	Syn flag number	22	SMTP	37	Tot size
8	Rst flag number	23	SSH	38	IAT
9	Psh flag number	24	IRC	39	Number
10	Ack flag number	25	TCP	40	Radius
11	Ece flag number	26	UDP	41	Magnitude
12	Cwr flag number	27	DHCP	42	Variance
13	Syn count	28	ARP	43	Covariance
14	Ack count	29	ICMP	44	Weight
15	Fin count	30	IPv	45	Protocol Type

TAB. 4.1 : Liste des caractéristiques (features) du dataset CIC-IoMT2024

4.4 Nettoyage et Prétraitement des Données

4.4.1 Nettoyage de données

Un nettoyage de base a été appliqué au jeu de données CICIoMT2024. Il aurait consisté à supprimer certaines colonnes peu informatives, à vérifier l'homogénéité des fichiers CSV, et à traiter les valeurs manquantes ou anormales telles que NaN ou INF. Ce prétraitement vise à améliorer la qualité des données en entrée pour les modèles d'apprentissage.

4.4.2 Encodage

Pour permettre aux modèles de Deep Learning de traiter les classes du jeu de données, la colonne des étiquettes appelée « Type » aurait été encodée à l'aide de la méthode Label Encoding. Cette transformation permet de représenter les catégories sous forme numérique, ce qui est nécessaire pour l'entraînement des modèles.

4.4.3 Normalisation

Une normalisation aurait été appliquée aux caractéristiques numériques afin de garantir une échelle cohérente entre les différentes variables. Cette étape permettrait d'accélérer l'apprentissage des modèles et d'améliorer leur performance, en évitant que certaines variables n'aient un poids disproportionné par rapport à d'autres.

4.4.4 Équilibrage des classes

application de l'algorithme SMOTE (Synthetic Minority Oversampling Technique) uniquement sur l'ensemble d'entraînement afin de compenser efficacement le déséquilibre des classes.

4.5 Méthodologie proposée

Ce travail vise à concevoir un système robuste de détection d'IDS destiné aux environnements IoMT, dans l'objectif de garantir la sécurité et la confidentialité des données médicales sensibles. Dans un premier temps, nous avons implémenté et évalué trois modèles basés sur des architectures d'apprentissage profond : le MLP, GRU et LSTM. L'évaluation de ces modèles a été réalisée sur le jeu de données CICIoMT2024 en adoptant deux approches distinctes : une classification binaire suivie d'une classification multiclasses. À l'issue de cette étape, le modèle offrant les meilleures performances a été sélectionné pour intégrer une approche d'apprentissage fédéré fondée sur l'algorithme FedAVG, permettant ainsi d'améliorer simultanément la confidentialité des données et l'efficacité collaborative des dispositifs connectés dans les réseaux IoMT.

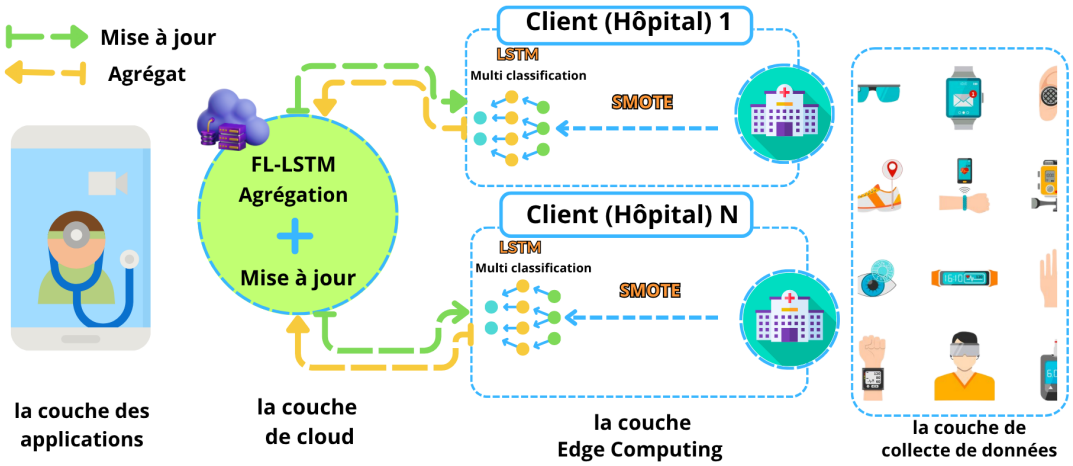


FIG. 4.2 : Architecture de méthodologie proposée.

4.6 Validation des performances

L'évaluation des modèles repose sur des critères rigoureux : exactitude, précision, rappel et score F1, assurant ainsi une validation robuste, complète et reproductible des résultats.

4.7 Description détaillée des architectures retenues

Cette section présente en détail les architectures de réseaux de neurones sélectionnées pour notre étude comparative. Chaque modèle a été configuré avec des paramètres

spécifiques optimisés pour la tâche de classification considérée.

Modèle	Structure des couches	Optimiseur	Techniques complémentaires
MLP	• 3 couches denses (256, 128, 64 unités) • Couche dense finale (nombre de classes, Softmax)	Adam (lr = 0,001)	Dropout, Batch Normalization
GRU	• 3 couches GRU (256, 128, 64 unités) • Couche dense finale (nombre de classes, Softmax)	Adam (lr = 0,001)	Dropout, Batch Normalization
LSTM	• 3 couches LSTM (256, 128, 64 unités) • Couche dense finale (nombre de classes, Softmax)	Adam (lr = 0,001)	Dropout, Batch Normalization
FedAVG	• 3 couches LSTM (256, 128, 64 unités) • Couche dense finale (nombre de classes, Softmax)	Adam (lr = 0,001)	10 rounds, num_client = 4

TAB. 4.2 : Architectures et paramètres des modèles évalués

4.7.1 Paramètres complémentaires

Les paramètres suivants ont été appliqués de manière cohérente à travers tous les modèles pour assurer une comparaison équitable :

- **Dropout** : appliqué après chaque couche LSTM avec des valeurs typiques comprises entre 0,2 et 0,5 pour réduire le surapprentissage.
- **BatchNormalization** : utilisé pour stabiliser et accélérer l'apprentissage en normalisant les entrées de chaque couche.
- **Batch size / Epochs** :
  - Taille de lot (batch size) = 64

– Nombre d'époques = 100

- **EarlyStopping / ReduceLROnPlateau** : techniques recommandées pour éviter le surapprentissage et améliorer la convergence du modèle pendant l'entraînement.

4.8 Résultats et discussion

Cette section présente une analyse comparative des performances des modèles proposés, ainsi que l'impact de l'intégration de l'apprentissage fédéré dans un contexte IoMT.

4.8.1 Analyse comparative des performances des modèles MLP, GRU et LSTM en classification multi-classe

Les modèles MLP, GRU et LSTM ont été évalués dans un scénario de classification multi-classe afin de comparer leur efficacité dans la détection des attaques au sein d'environnements IoMT. Les résultats obtenus sont résumés dans le tableau suivant :

Modèle	Exactitude (%)	Précision (%)	Rappel (%)	F1-Score (%)
MLP	88.48	88.63	88.48	88.5
GRU	74.34	79.35	74.34	64.34
LSTM	91.62	91.64	91.62	91.63

TAB. 4.3 : Performances comparatives des modèles en classification multi-classe

Le modèle LSTM présente les meilleures performances globales avec une précision de 91,62 %. Le modèle MLP obtient également des résultats satisfaisants, avec une précision de 88,48 %. En revanche, le modèle GRU affiche des performances inférieures, notamment en termes de rappel et de score F1, ce qui indique une capacité limitée à capturer efficacement la dynamique temporelle complexe des données IoMT.

4.8.2 Évaluation approfondie du modèle LSTM selon différents scénarios

Après avoir sélectionné le modèle LSTM, nous avons évalué ses performances selon trois scénarios distincts : classification binaire, classification multi-classe et apprentissage fédéré via l'algorithme FedAVG. Les résultats obtenus sont résumés clairement dans le tableau suivant :

Scénario	Exactitude (%)	Précision (%)	Rappel (%)	F1-Score (%)
Classification binaire	**99.74**	**99.54**	**99.94**	**99.74**
Classification (multi-classe)	91.62	91.64	91.62	91.63
Apprentissage fédéré (FedAVG)	91.45	91.47	91.45	91.45

TAB. 4.4 : Performances du modèle LSTM dans différents scénarios

Ces résultats mettent clairement en évidence la performance remarquable du modèle LSTM, particulièrement dans le scénario de classification binaire avec une précision exceptionnelle de 99,74 %. Même dans un cadre multi-classe plus complexe, le modèle conserve un niveau élevé de précision de 91,62 %. Par ailleurs, l'intégration de l'apprentissage fédéré (FedAVG) a permis d'obtenir un modèle collaboratif performant, atteignant une précision très satisfaisante de 91,45 %, tout en apportant des avantages significatifs en termes de confidentialité des données sensibles dans les environnements IoMT.

4.9 Conclusion

En conclusion, les expérimentations réalisées avec les modèles MLP, GRU et LSTM ont mis en évidence des résultats globalement satisfaisants, soulignant toutefois la supériorité notable du modèle LSTM dans les scénarios évalués, tant en classification binaire qu'en classification multi-classe. Par ailleurs, l'intégration de l'approche d'apprentissage fédéré via l'algorithme FedAVG a permis de maintenir des niveaux élevés de performance tout en garantissant efficacement la confidentialité des données médicales sensibles.

Conclusion

Conclusion générale

Ce mémoire s'inscrit dans une démarche scientifique visant à améliorer significativement la sécurité des infrastructures de l'IoMT, un secteur stratégique en forte croissance et confronté à des défis critiques en matière de cybersécurité. Dans cette perspective, nous avons conçu et évalué un système innovant de détection d'intrusions basé sur des techniques avancées d'apprentissage profond afin de détecter efficacement les comportements malveillants au sein des réseaux médicaux connectés.

À partir d'une analyse approfondie des architectures IoMT et de leurs principales vulnérabilités, nous avons procédé à l'évaluation comparative de trois modèles neuronaux : le MLP, GRU, et LSTM, en utilisant le jeu de données spécialisé CICIoMT2024.

Les résultats expérimentaux obtenus démontrent clairement la supériorité du modèle LSTM, atteignant une précision remarquable de 91,62 % en classification binaire. Cette performance exceptionnelle du LSTM s'explique par sa capacité avancée à modéliser les dépendances temporelles complexes du trafic réseau, permettant ainsi une détection fine et précise des attaques sophistiquées.

Par ailleurs, nous avons intégré une approche d'apprentissage fédéré basée sur l'algorithme FedAVG afin de préserver rigoureusement la confidentialité des données sensibles des patients. Cette stratégie collaborative, fondée sur le principe de décentralisation, permet de construire un modèle global robuste tout en assurant que les informations critiques restent localisées sur les dispositifs individuels. Cette contribution constitue une avancée majeure dans le renforcement de la protection de la vie privée dans le contexte médical.

Les expérimentations réalisées confirment pleinement la pertinence et l'efficacité de notre approche dans la sécurisation proactive des environnements IoMT. Toutefois, des défis subsistent, notamment concernant la détection d'attaques rares ou nouvelles, ainsi que la gestion efficace des contraintes computationnelles liées aux dispositifs médicaux disposant de ressources limitées.

En termes de perspectives, les futures recherches pourraient se concentrer sur l'amélioration des performances globales du système IDS par le traitement du déséquilibre des données, l'élargissement et l'enrichissement des jeux de données disponibles, et l'exploration de modèles plus légers adaptés aux dispositifs à faibles ressources. Enfin, renforcer la capacité adaptative du système face à des scénarios d'attaque nouveaux et complexes demeure un axe prioritaire.

Ainsi, ce travail offre une contribution substantielle et prometteuse à la sécurisation des systèmes IoMT, répondant efficacement aux exigences cruciales de confidentialité, d'évolutivité et de fiabilité dans le secteur de la santé connectée.

Bibliographie

[1] H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier, and M. M. Mansour, "One round cipher algorithm for multimedia iot devices," *Multimedia tools and applications*, vol. 77, pp. 18383–18413, 2018.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot) : A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] J. N. S. Rubí and P. R. L. Gondim, "Iomt platform for pervasive healthcare data aggregation, processing, and sharing based on onem2m and openehr," *Sensors*, vol. 19, no. 19, p. 4283, 2019.

[4] J.-P. A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier, and A. Chehab, "Securing internet of medical things systems : Limitations, issues and recommendations," *Future Generation Computer Systems*, vol. 105, pp. 581–606, 2020.

[5] ScienceSoft, "Développement d'applications pour les pneumatiques médicaux." https://www.scnsoft.com/ar/healthcare/wearable-medical-devices. consulté le 27 mai 2025.

[6] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, "A comprehensive survey of wireless body area networks : On phy, mac, and network layers solutions," *Journal of medical systems*, vol. 36, pp. 1065–1094, 2012.

[7] N. James, "Top 7 trends in internet of things (iot) in healthcare." https://www.verifiedmarketreports.com/blog/top-7-trends-in-internet-of-things-iot-in-healthcare/, janvier 2025. Consulté le 10 avril 2025.

[8] L. Sun, X. Jiang, H. Ren, and Y. Guo, "Edge-cloud computing and artificial intelligence in internet of medical things : architecture, technology and application," *IEEE access*, vol. 8, pp. 101079–101092, 2020.

[9] F. Muheidat and L. A. Tawalbeh, "Aiomt artificial intelligence (ai) and internet of medical things (iomt) : applications, challenges, and future trends," in *Computational*

Intelligence for Medical Internet of Things (MIoT) Applications, pp. 33–54, Elsevier, 2023.

[10] R. Hireche, H. Mansouri, and A.-S. K. Pathan, "Security and privacy management in internet of medical things (iomt) : A synthesis," *Journal of cybersecurity and privacy*, vol. 2, no. 3, pp. 640–661, 2022.

[11] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the internet-of-medical-things (iomt) systems security," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707–8718, 2021.

[12] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of medical things (iomt) : Applications, benefits and future challenges in healthcare domain.," *J. Commun.*, vol. 12, no. 4, pp. 240–247, 2017.

[13] K. H. Almotairi, "Application of internet of things in healthcare domain," *Journal of Umm Al-Qura University for Engineering and Architecture*, vol. 14, no. 1, pp. 1–12, 2023.

[14] Lexhan Group, "Protocoles iot pour objets connectés : lesquels utiliser ?." https://www.lexhan-group.fr/blog/connectivite/protocoles-iot-pour-objets-connectes/, 2024. Consulté le 7 avril 2025.

[15] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in iomt communications : A survey," *Sensors*, vol. 20, no. 17, p. 4828, 2020.

[16] DatiPlus, "Protocole iot : Définition et utilisation." https://dati-plus.com/protocole-iot/, 2024. Consulté le 8 avril 2025.

[17] Allisone, "Après l'iot, l'internet des objets médicaux (iomt)." https://www.allisone.ai/blog/iomt-internet-of-medical-things, Mar. 2025. Consulté le 15 avril 2025.

[18] D. J. Hemanth, J. Anitha, and G. A. Tsihrintzis, *Internet of medical things*. Springer, 2021.

[19] M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. A. Ramírez-Gutiérrez, and C. Feregrino-Uribe, "Artificial intelligence for iomt security : A review of intrusion detection systems, attacks, datasets and cloud–fog–edge architectures," *Internet of Things*, vol. 23, p. 100887, 2023.

[20] R. Hireche, H. Mansouri, and A.-S. K. Pathan, "Fault tolerance and security management in iomt," in *Towards a Wireless Connected World : Achievements and New Technologies*, pp. 65–104, Springer, 2022.

[21] S. Rani, A. Kataria, S. Kumar, and P. Tiwari, "Federated learning for secure iomt-applications in smart healthcare systems : A comprehensive review," *Knowledge-based systems*, vol. 274, p. 110658, 2023.

[22] ObjectBox, "Iot edge computing and digitalization in healthcare." https://objectbox.io/iot-edge-computing-and-digitalization-in-healthcare/. [En ligne ; consulté le 27 avril 2025].

[23] R. Chengoden, N. Victor, T. Huynh-The, G. Yenduri, R. H. Jhaveri, M. Alazab, S. Bhattacharya, P. Hegde, P. K. R. Maddikunta, and T. R. Gadekallu, "Metaverse for healthcare : a survey on potential applications, challenges and future directions," *Ieee Access*, vol. 11, pp. 12765–12795, 2023.

[24] H. Mezili, *Vers une amélioration de la détection d'intrusion par les méthodes de sélection des fonctionnalités à l'aide des arbres de décision.* PhD thesis, Université Ibn Khaldoun-Tiaret-, 2021.

[25] Network Simulation Tools, "Intrusion detection system projects." https://networksimulationtools.com/intrusion-detection-system-projects/. Consulté le 13 mai 2025.

[26] M. F. Elrawy, A. I. Awad, and H. Hamed, "Intrusion detection systems for iot-based smart environments : a survey," *Journal of Cloud Computing Advances Systems and Applications*, vol. 7, 12 2018.

[27] I. Industriel, "Système de détection d'intrusion (ids)," 2025. Accédé : 10 avril 2025.

[28] J.-M. Percher, R. Puttini, L. Mé, O. Camp, B. Jouga, and P. Albers, "Un système de détection d'intrusions distribué pour réseaux ad hoc," *Technique et Science Informatiques*, vol. 23, pp. 391–420, 03 2004.

[29] C. Bidan, G. Hiet, L. Mé, B. Morin, and J. Zimmermann, "Vers une détection d'intrusions à fiabilité et pertinence prouvables," 10 2006.

[30] A. inconnu, "Les ids par la pratique : Snort," 2004. Consulté le 10 avril 2025.

[31] F. Jemili, *Système de Détection et de Prévision d'Intrusions : À base de réseaux d'inférence incertaine et imprécise dans une architecture multi-agent.* 12 2013.

[32] A. inconnu, "Évasion aux ids, pare-feu et pots de miel," 2020. Consulté le 10 avril 2025.

[33] N. Saxena, S. Roy, A. Ghosh, and S. Ghosh, "Survey of intrusion detection systems : techniques, datasets and challenges," *Cybersecurity*, vol. 5, no. 1, pp. 1–22, 2019. Consulté le 10 avril 2025.

[34] B. Yann and J.-B. Marchand, "Détection d'intrusions et analyse forensique," *Journal of Cybersecurity and Digital Forensics*, vol. 12, no. 2, pp. 45–58, 2021. Consulté le 10 avril 2025.

[35] C. Magazine, "Définition deep learning," 2022. Consulté le 10 avril 2025.

[36] Pangeanic, "Quelle est la différence entre l'apprentissage automatique et l'apprentissage profond ?," 2021. Consulté le 10 avril 2025.

[37] Linedata, "Qu'est-ce que l'apprentissage supervisé ?," 2021. Consulté le 10 avril 2025.

[38] Diabolocom, "Traitement du langage naturel (nlp) : guide complet," 2023. Consulté le 10 avril 2025.

[39] J. Robert, "Reinforcement learning : Définition et application," 2020. Consulté le 10 avril 2025.

[40] S. Laqrichi, *Approach to build realistic models for estimating project effort/cost in an uncertain environment : application to the software development field.* PhD thesis, 12 2015.

[41] A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow.* O'Reilly Media, 3 ed., 2022.

[42] O. Chapelle, B. Schölkopf, and A. Zien, eds., *Semi-Supervised Learning.* MIT Press, 2006.

[43] IBM, "What is a neural network ?." https://www.ibm.com/think/topics/neural-networks, 2025. Consulté le 10 avril 2025.

[44] E. Franck, "Introduction aux réseaux de neurones." https://irma.math.unistra.fr/~franck/cours/SciML/output/html/chapAP_sec1.html, 2025. Consulté le 10 avril 2025.

[45] B. Kouakou, *Développement d'instrumentation optique fondée sur le principe de la spectroscopie par télédétection pour la caractérisation des espèces volantes de la faune.* PhD thesis, 09 2020.

[46] A. Alzahrani and M. Alenazi, "Designing a network intrusion detection system based on machine learning for software defined networks," *Future Internet*, vol. 13, no. 111, pp. 1–19, 2021.

[47] Équipe éditoriale IONOS, "Qu'est-ce qu'un recurrent neural network (rnn) ?," mars 2025. Consulté le 10 avril 2025.

[48] S. DC, "Tutorial cnn partie 1: Mnist digits classification." https://www.kaggle.com/code/stephanedc/tutorial-cnn-partie-1-mnist-digits-classification, 2024. Consulté le 10 avril 2025.

[49] B. Braunschweig, "Intelligence artificielle - livre blanc," 2016. Consulté le 10 avril 2025.

[50] T. Li, "Federated learning : Challenges, methods, and future directions." https://blog.ml.cmu.edu/2019/11/12/federated-learning-challenges-methods-and-future-directions/, novembre 2019. Consulté le 10 avril 2025.

[51] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge intelligence : Paving the last mile of artificial intelligence with edge computing," 05 2019.

[52] A. Qammar, J. Ding, and H. Ning, "Federated learning attack surface : taxonomy, cyber defences, challenges, and future directions," *Artificial Intelligence Review*, vol. 55, 06 2022.

[53] Y. Supriya and T. Gadekallu, "Particle swarm-based federated learning approach for early detection of forest fires," *Sustainability*, vol. 15, p. 964, 01 2023.

[54] P. S. Foundation, "Python software foundation : Python blurb." https://www.python.org/doc/essays/blurb/. [En ligne ; consulté le 27 mai 2025].

[55] P. Jupyter, "Project jupyter." https://jupyter.org/. [En ligne ; consulté le 27 mai 2025].

[56] Mobiskill, "Les bibliothèques python à utiliser pour le machine learning." https://www.mobiskill.fr/blog-posts/les-bibliotheque-python-a-utiliser-pour-le-machine-learning. [En ligne ; consulté le 3 juin 2025].

[57] IONOS, "Qu'est-ce que keras ?." https://www.ionos.fr/digitalguide/web-marketing/search-engine-marketing/quest-ce-que-keras/. [En ligne ; consulté le 3 juin 2025].

[58] N. Developers, "What is numpy ?." https://numpy.org/devdocs/user/whatisnumpy.html. [En ligne ; consulté le 3 juin 2025].

[59] GeeksforGeeks, "Libraries in python." https://www.geeksforgeeks.org/libraries-in-python/. [En ligne ; consulté le 3 juin 2025].

[60] C. I. for Cybersecurity, "Cic iomt dataset 2024: Attack vectors in healthcare devices - a multi-protocol dataset for assessing iomt device security." https://www.unb.ca/cic/datasets/iomt-dataset-2024.html. [En ligne ; consulté le 27 mai 2025].

[61] S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi, and A. A. Ghorbani, "Ciciomt2024: A benchmark dataset for multi-protocol security assessment in iomt," *Internet of Things*, vol. 28, p. 101351, 2024.