Titre: Title:	Architecture de communication sécurisée pour les systèmes de soins de santé dans les villes intelligentes
Auteur: Author:	Hadjer Goumidi
Date:	2025
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Goumidi, H. (2025). Architecture de communication sécurisée pour les systèmes de soins de santé dans les villes intelligentes [Thèse de doctorat, Polytechnique Montréal]. PolyPublie. https://publications.polymtl.ca/71957/

POLYTECHNIQUE MONTRÉAL

affiliée à l'Université de Montréal

Architecture de communication sécurisée pour les systèmes de soins de santé dans les villes intelligentes

HADJER GOUMIDI

Département de génie informatique et génie logiciel

Thèse présentée en vue de l'obtention du diplôme de *Philosophiæ Doctor*

Génie informatique

Décembre 2025

POLYTECHNIQUE MONTRÉAL

affiliée à l'Université de Montréal

Cette thèse intitulée :

Architecture de communication sécurisée pour les systèmes de soins de santé dans les villes intelligentes

présentée par **Hadjer GOUMIDI**

en vue de l'obtention du diplôme de *Philosophiæ Doctor*

a été dûment acceptée par le jury d'examen constitué de :

Martine BELLAÏCHE, présidente
Samuel PIERRE, membre et directeur de recherche
Alejandro QUINTERO, membre
Abdelhak Mourad GUEROUI , membre externe

DÉDICACE

À ma chère mère et à mon cher père,
vous qui avez toujours cru en moi, m'avez encouragée sans relâche et soutenue à chaque étape de ma vie. C'est grâce à votre amour et à vos prières que j'ai pu réaliser mes rêves et arriver jusqu'ici.

À mon mari, mon compagnon de route, qui m'a soutenu, poussé et encouragé à aller jusqu'au bout, même dans les moments les plus difficiles. Merci d'avoir toujours cru en ma force.

À mes deux trésors, mes filles adorées, qui illuminent mes journées et me donnent la plus belle raison de persévérer. Que mes efforts vous inspirent à poursuivre vos rêves.

À ma sœur et à mes frères, pour leur affection, leur soutien constant et leurs mots qui m'ont portée dans les moments de doute.

À vous tous, ma réussite est aussi la vôtre.

REMERCIEMENTS

Je tiens tout d'abord à exprimer ma profonde gratitude à mon directeur de recherche, Professeur Samuel Pierre, pour m'avoir donné l'opportunité de réaliser cette thèse au sein du Laboratoire de recherche en réseautique et informatique mobile (LARIM). Ses conseils avisés, sa disponibilité et son encadrement rigoureux ont été essentiels à l'aboutissement de ce travail doctoral.

J'adresse également mes sincères remerciements aux membres du jury, Professeur Alejandro Quintero, Professeure Martine Belaïche et Professeur Mourad Gueroui, pour l'honneur qu'ils me font d'évaluer cette thèse et pour leurs remarques constructives qui contribueront à enrichir mes travaux.

Je souhaite exprimer une reconnaissance particulière à la Docteure Franjieh El Khoury, coordonnatrice du LARIM et superviseure du projet APSEC. Sa bienveillance, son écoute constante et son soutien, tant sur le plan académique que personnel, m'ont accompagnée tout au long de ce parcours. Je tiens également à la remercier pour la relecture attentive de mes différents travaux, ainsi que pour ses conseils précieux et son dévouement.

Je remercie également la compagnie Flex Group, qui m'a permis d'allier recherche académique et immersion en milieu industriel durant mes études, et d'enrichir ainsi mon expérience.

Je remercie aussi chaleureusement mes collègues et amis du LARIM pour les moments d'échanges, de collaboration et d'amitié qui ont rendu ce chemin plus agréable. J'ai une pensée spéciale pour Gaëlle, Carria, Goulnoush, Fatima-Zohra et Olson, dont la présence et l'amitié m'ont beaucoup apporté au quotidien.

Enfin, j'adresse un grand merci à toutes les personnes qui, de près ou de loin, m'ont accompagnée dans ce cheminement doctoral et ont contribué à la réussite de ce travail.

RÉSUMÉ

Avec la croissance exponentielle de l'Internet des objets médicaux « Internet of Medical Things » (IoMT) et l'intégration massive de dispositifs connectés dans les hôpitaux et systèmes de santé intelligents, la protection des données médicales est devenue un enjeu majeur. Ces dispositifs, souvent contraints en termes de calcul, de mémoire et d'énergie, échangent des informations sensibles à travers des environnements dynamiques et exposés à de multiples menaces. Dans ce contexte, la sécurité des données médicales doit être assurée en tenant compte de quatre dimensions fondamentales : la confidentialité, l'intégrité, l'authentification et le contrôle d'accès.

L'objectif principal de cette thèse est de concevoir des modèles robustes pour renforcer la sécurité des systèmes de santé intelligents. Pour atteindre cet objectif, nous avons divisé nos travaux en trois volets complémentaires.

Dans le premier volet, nous proposons un schéma cryptographique post-quantique léger, basé sur l'algorithme « Binary Ring Learning With Errors » (BRLWE). Ce schéma combine la décomposition en trois parties « Three-way decomposition » avec la multiplication de Karatsuba pour l'optimisation du calcul polynomial, et la méthode de permutation aléatoire « Random Shuffling » afin de renforcer la résistance face aux attaques par canaux auxiliaires (i.e., timing, SPA et DPA) ainsi qu'aux attaques quantiques hybrides. Une implémentation sur microcontrôleur ARM Cortex-M0 a démontré que la solution est adaptée aux dispositifs médicaux contraints, avec des coûts de calcul réduits et une meilleure efficacité que les travaux existants.

Le deuxième volet traite de la détection d'anomalies et d'attaques dans les environnements IoMT. Nous développons un nouveau jeu de données médicales, construit à partir de données physiologiques réelles et enrichi par des scénarios d'attaques représentatifs du domaine de la santé (i.e., attaques par falsification, déni de service et intrusions). Sur ces données, nous proposons un modèle d'apprentissage automatique par empilement « Stacking Ensemble » combinant « Random Forest », réseau de neurones artificiels et XGBoost. Les résultats montrent une précision de 98,02 % et une capacité robuste à détecter les anomalies en temps réel lors de transmissions de données médicales simulées.

Enfin, dans le troisième volet, nous concevons un cadre adaptatif pour l'authentification et le contrôle d'accès dans les systèmes de santé. Ce cadre repose sur un modèle dual-agent basé sur l'apprentissage par renforcement « Reinforcement Learning » (RL). L'agent d'authentification

intègre une analyse de risque contextuelle pour ajuster dynamiquement le niveau de sécurité, tandis que l'agent de contrôle d'accès évalue les comportements utilisateurs et les politiques organisationnelles. Pour l'évaluation, nous avons adapté le jeu de données « CERT Insider Threat » en contexte médical, afin de simuler des activités réalistes de professionnels de santé. Les résultats expérimentaux démontrent la supériorité de l'agent « Deep Q-Network » (DQN) par rapport à d'autres modèles RL et à plusieurs classificateurs d'apprentissage automatique traditionnels, grâce à une meilleure précision et un meilleur équilibre sur des données déséquilibrées.

En résumé, les travaux réalisés dans cette thèse apportent des contributions significatives à la cybersécurité des systèmes de santé intelligents. Ils offrent : (i) un schéma cryptographique léger et résistant aux menaces post-quantiques et aux attaques par canaux auxiliaires ; (ii) un nouveau jeu de données médical réaliste, associé à un modèle robuste de détection d'anomalies en temps réel ; et (iii) un cadre d'authentification et de contrôle d'accès adaptatif basé sur le RL. Ces contributions renforcent la confidentialité, l'intégrité, la disponibilité, ainsi que l'authentification et le contrôle d'accès des données médicales, tout en respectant les contraintes des environnements IoMT.

ABSTRACT

With the exponential growth of the « Internet of Medical Things » (IoMT) and the massive integration of connected devices in hospitals and smart healthcare systems, protecting medical data has become a major challenge. These devices, often constrained in terms of computation, memory, and energy, exchange sensitive information across dynamic environments exposed to multiple threats. In this context, medical data security must be ensured with respect to four fundamental dimensions: confidentiality, integrity, authentication and access control.

The main objective of this thesis is to design robust models to strengthen the security of smart healthcare systems. To achieve this objective, our work is divided into three complementary parts.

In the first part, we propose a lightweight post-quantum cryptographic scheme based on « Binary Ring Learning With Errors » (BRLWE). This scheme combines three-way decomposition Karatsuba for polynomial multiplication and random shuffling method to enhance resistance against side-channel attacks (i.e., timing, SPA and DPA) as well as hybrid quantum attacks. An implementation on the ARM Cortex-M0 microcontroller demonstrated that the solution is suitable for resource-constrained medical devices, with reduced computation costs and superior efficiency compared to existing approaches.

The second part addresses anomaly and attack detection in IoMT environments. We develop a new medical dataset built from real physiological data and enriched with healthcare-relevant attack scenarios (i.e., falsification, denial of service and intrusions). Using this dataset, we design a stacking ensemble machine learning model combining Random Forest, artificial neural network, and XGBoost as a meta-learner. The model achieved 98.02% accuracy and demonstrated strong robustness in real-time anomaly detection during simulated medical data transmissions.

Finally, in the third part, we propose an adaptive framework for authentication and access control in healthcare systems, based on Reinforcement Learning (RL). The authentication agent integrates contextual risk analysis to dynamically adjust security levels, while the access control agent evaluates user behaviors and organizational policies. For evaluation, we adapt the CERT Insider Threat dataset into a healthcare-specific behavioral dataset to simulate realistic activities of healthcare professionals. Experimental results show the superiority of the « Deep Q-Network » (DQN) agent compared to other RL models and traditional machine learning classifiers, achieving better accuracy and balanced performance on imbalanced datasets.

In summary, this thesis makes significant contributions to the cybersecurity of smart healthcare systems. It provides: (i) a lightweight cryptographic scheme resistant to post-quantum and side-channel threats; (ii) a realistic medical dataset combined with a robust real-time anomaly detection model; and (iii) an adaptive RL-based authentication and access control framework. Together, these contributions enhance confidentiality, integrity, availability, as well as authentication and access control of medical data, while meeting the constraints of IoMT environments.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

ABAC : Attribute-Based Access Control

AES : Advanced Encryption Standard

BDD : Bounded Distance Decoding

BRLWE : Binary Ring Learning With Errors

CERT : Computer Emergency Response Team (jeu de données d'insider threat)

CP-ABE : Ciphertext-Policy Attribute-Based Encryption

CVP : Closest Vector Problem

DPA : Differential Power Analysis

DQN : Deep Q-Network

DDQN : Double Deep Q-Network

DES : Deterministic Exploration Strategy

DS : Deterministic Strategy

DT : Decision Tree (Arbre de décision)

ECC : Elliptic Curve Cryptography

EHR : Electronic Health Records

EHS : Electronic Health Services

G-Mean : Geometric Mean

GANs : Generative Adversarial Networks

HIPAA : Health Insurance Portability and Accountability Act

HL7 FHIR : Health Level 7 – Fast Healthcare Interoperability Resources

IIoT : Industrial Internet of Things (IoT industriel)

IMDs : Implantable Medical Devices

InvRBLWE : Inverted Range Binary Ring Learning With Errors

IoMT : Internet of Medical Things

IoT : Internet of Things

LB-PKC : Lattice-Based Public-Key Cryptography

LB-RSA : Lattice-Based RSA

LSSS : Linear Secret Sharing Scheme

M-Santé : Mobile santé

M2M : Machine-to-Machine

MIM : Man-in-the-Middle

ML : Machine Learning

NB : Naive Bayes

NIST : National Institute of Standards and Technology

NTT : Number Theoretic Transform

PKI : Public Key Infrastructure

PMD : Personal Medical Devices

PQC : Post-Quantum Cryptography

RBAC : Role-Based Access Control

Ring-ExpLWE : Ring Exponential Learning With Errors

RL : Reinforcement Learning

ROC : Receiver Operating Characteristic

RSA : Rivest–Shamir–Adleman

S3VM : Semi-Supervised Support Vector Machine

SCA : Side-Channel Attacks

SPA : Simple Power Analysis

SPMA : Schoolbook Polynomial Multiplication Algorithm

SSSI : Systèmes de Soins de Santé Intelligents

SVM : Support Vector Machine

SVP : Shortest Vector Problem

TIC : Technologies de l'Information et de la Communication

uSVP : Unique Shortest Vector Problem

XAI : Explainable Artificial Intelligence

3-DMRKSh-BRLWE : 3-Decomposition Modular Reduction Karatsuba Shuffling Binary Ring Learning With Errors

3DKSh-BRLWE : 3-Decomposition Karatsuba Shuffling Binary Ring Learning With Errors

LISTE DES ANNEXES

CHAPITRE 1 INTRODUCTION

L'urbanisation de la population mondiale est devenue un enjeu majeur qui doit être traité. Dans les années 1950, seulement 30 % de la population mondiale vivait dans les villes; en 2014, le taux d'urbanisation atteint 54 %; et les Nations Unies prévoient qu'en 2050, ce chiffre augmentera à 66 % [1]. Ce qui nécessite une infrastructure intelligente et durable pour gérer les besoins des citoyens et offrir des services fondamentaux et plus avancés. Le concept de ville intelligente a été introduit pour répondre à ces besoins. Il est apparu pour la première fois au début des années 1990 où les chercheurs ont mis l'accent sur la technologie, l'innovation et la mondialisation dans le processus d'urbanisation.

Depuis l'émergence de divers types de réseaux, les objets connectés « Internet of Things » (*IoT*) sont devenus l'un des types d'infrastructure les plus importants dans les villes intelligentes [1]. Il s'agit d'un nouveau domaine intégrant le monde physique à Internet via l'infrastructure réseau existante. Cette technologie vise à connecter tous les appareils intelligents (e.g., les appareils physiques, les véhicules, les appareils d'électroménagers, etc.) en leur permettant de collecter et de partager des données de manière autonome via Internet. Selon le rapport annuel de Cisco, le nombre d'appareils connectés aux réseaux IP devrait atteindre 29,3 milliards d'ici 2023, soit environ 3,6 appareils par personne à l'échelle mondiale. Les connexions de type Machine-to-Machine (M2M), essentielles pour les applications IoT, constitueront 50 % de ces connexions.

L'*IoT* fournit un grand nombre d'applications pour améliorer la vie et les activités quotidiennes des gens, tels que la maison intelligente, le transport intelligent, l'agriculture intelligente, l'industrie intelligente, les soins des santés intelligent et d'autres [1].

La maison intelligente comprend une collection d'appareils intelligents (e.g., une serrure intelligente, un moniteur pour bébé, un détecteur, etc.) qui sont déployés à la maison et communiqués localement via des canaux sans fil [1]. Les appareils domestiques sont accessibles à distance via une passerelle domestique.

Le transport intelligent comprend un grand nombre de véhicules intelligents qui peuvent être communiqués entre eux (i.e., véhicule à véhicule), à la station extérieure (i.e., véhicule à infrastructure) et aux piétons (i.e., véhicule à piéton) via des réseaux sans fil [1]. Un véhicule

intelligent peut détecter l'état actuel de la circulation, gérer la vitesse et échanger des données, pour une conduite efficace et sûre.

L'agriculture intelligente permet de contrôler à distance la température, l'humidité, l'irrigation, l'humidité du sol et les conditions microclimatiques pour fournir une production de qualité élevée et éviter les pertes financières [1]. Dans un système agricole intelligent, des capteurs peuvent être attachés aux animaux pour suivre les comportements et les conditions de santé du bétail.

L'industrie intelligente, connue sous le nom de l'*IoT* industriel « Industrial IoT » (IIoT), utilise la technologie machine-à-machine pour automatiser le processus de fabrication avec une intervention humaine insignifiante [1]. L'IIoT vise à mieux contrôler le processus de production, les données et les problèmes pour fournir des produits finaux efficaces et fiables.

Les systèmes soins de santé intelligents (SSSI) reposent sur l'utilisation de capteurs biomédicaux, de dispositifs portables et de systèmes de communication interconnectés pour collecter, transmettre et stocker les informations physiologiques des patients [1]. Par exemple, la fréquence cardiaque peut être mesurée par des capteurs médicaux et transmise en temps réel aux professionnels de santé pour un diagnostic et un suivi à distance. Ces technologies sont particulièrement bénéfiques pour les personnes âgées, une population en croissance rapide et plus sujette aux maladies chroniques telles que les maladies cardiovasculaires, le diabète et le cancer [2]. Selon les projections des Nations Unies, la proportion de la population mondiale âgée de 65 ans et plus devrait passer de 9,3 % en 2020 à 16 % d'ici 2050 [3]. Cette augmentation significative souligne l'importance de solutions de santé innovantes pour répondre aux besoins spécifiques de cette tranche d'âge. En parallèle, les dépenses de santé associées aux personnes âgées sont en constante augmentation. Par exemple, aux États-Unis, les dépenses de santé par personne pour les individus de 65 ans et plus étaient de 22 356 $ en 2020, soit plus de cinq fois supérieures à celles des enfants et près de 2,5 fois celles des adultes en âge de travailler [4].

Les technologies de soins de santé intelligentes offrent des solutions prometteuses pour améliorer la qualité des soins tout en réduisant les coûts. En 2025, des dispositifs comme les montres connectées, les applications basées sur l’intelligence artificielle, ou encore les systèmes de détection et de prévention des chutes (via capteurs de mouvement ou caméras intelligentes) sont de plus en plus intégrés dans les environnements de soins à domicile et les établissements gériatriques. Ces

outils permettent une surveillance continue, une intervention rapide en cas d'accident et une réduction des hospitalisations, particulièrement chez les personnes âgées vivant seules.

Cependant, l'intégration de ces technologies soulève des défis majeurs en matière de cybersécurité. Il est essentiel de garantir la confidentialité, la préservation de la vie privée, ainsi que l'intégrité, la disponibilité, l'authentification et le contrôle d'accès aux données médicales. Cela implique la mise en place de mécanismes robustes pour prévenir les intrusions et protéger les systèmes contre les cyberattaques.

Pour répondre à ces exigences de sécurité dans les environnements connectés, notamment en santé intelligente, il est essentiel d'examiner les technologies capables de renforcer la résilience des systèmes. La sécurité des données présente un défi majeur dans les réseaux IoT, plus précisément dans les systèmes de soins de santé intelligents [5], [6]. Les données des patients sont critiques, et toute modification de ces données peut affecter leur vie et leur santé. Les approches classiques de sécurité, basées sur une architecture centralisée, montrent leurs limites face aux nouvelles menaces. Ainsi, des techniques avancées sont explorées, telles que l'utilisation de méthodes de cryptographie légère post-quantique, capables de résister aux attaques des futurs ordinateurs quantiques, la détection des attaques à l'aide d'algorithmes d'apprentissage automatique « Machine Learning » (ML), ainsi que des modèles d'authentification et de contrôle d'accès renforcés par l'apprentissage par renforcement. Ces solutions permettent de sécuriser efficacement les communications dans un contexte de ressources limitées, mais posent aussi des défis liés à la charge computationnelle, au temps de traitement et à la protection de la vie privée des patients.

Ce chapitre introductif définit les concepts fondamentaux nécessaires à la compréhension de cette thèse, à savoir les villes intelligentes, l'Internet des objets (IoT), les systèmes de soins de santé intelligents, le cryptage léger et l'apprentissage automatique. Ces notions constituent le socle sur lequel repose notre approche pour sécuriser les communications dans les environnements médicaux connectés.

Par la suite, nous exposons les éléments de problématique liés à la protection des données de santé dans un contexte fortement interconnecté, où les ressources des dispositifs sont limitées et les exigences de sécurité élevées. Nous poursuivons en présentant les objectifs de cette recherche, formulés à partir des besoins identifiés. Les contributions principales de cette thèse sont ensuite énoncées, en mettant en lumière leur caractère original et leur pertinence vis-à-vis des défis

contemporains de cybersécurité dans les soins intelligents. Enfin, ce chapitre se conclut par une vue d'ensemble des différents chapitres constituant ce travail de recherche.

1.1 Définition et concepts de base

Cette section est consacrée à la définition des concepts de base liés à la sécurité des réseaux *IoT* et des systèmes de soins de santé dans les villes intelligentes. Nous commencerons par la définition des villes intelligentes, l'*IoT*, les systèmes de soins de santé intelligents et la sécurité et les attaques dans les réseaux *IoT*. Ensuite, nous présenterons les concepts de base liés à la cryptographie légère et post-quantique, ainsi que les algorithmes d'apprentissage automatique et d'apprentissage par renforcement.

1.1.1 Villes intelligentes

La ville intelligente est définie par IBM [7] comme l'utilisation des technologies de l'information et de la communication dans le but de détecter, analyser et intégrer les informations clés des systèmes de base dans les villes en activité. Elle peut apporter une réponse intelligente à différents types de besoins, y compris les moyens de la protection de l'environnement, la subsistance quotidienne, la sécurité publique et les services de la ville intelligente, ainsi que les activités industrielles et commerciales.

La ville intelligente est l'approche actuelle de la planète intelligente s'appliquant à une région spécifique, réalisant la gestion informationnelle et intégrant des villes. Cependant, il s'agit d'une intégration efficace d'idées de planification intelligentes, de modes de construction intelligents, des méthodes de gestion intelligentes et d'approches de développement intelligentes. Grâce à la gestion du réseau numérique de la géographie urbaine, des ressources, de l'environnement, des systèmes économiques, sociaux et autres, ainsi que du traitement et des applications numériques et informatiques de l'infrastructure urbaine et de l'environnement de base, nous pouvons parvenir à une gestion de services urbains intelligents, favorisant ainsi un fonctionnement plus efficace, plus pratique et harmonieux des villes modernes [8].

La structure de la ville intelligente comprend une couche de perception, une couche de réseau et une couche d'application, qui peuvent rendre le monde futur de plus en plus appréciable, mesurable et intelligent avec plus d'interconnexion et d'interopérabilité [7].

1.1.2 Objets connectés « Internet of Things » (IoT)

La technologie des objets connectés « Internet of Things » (*IoT*) est un paradigme de communication récent qui considère la présence, dans l'environnement, d'une variété d'objets qui collaborent et communiquent à travers des connexions sans fil et filaires, ainsi que des systèmes d'adressage unique pour créer de nouveaux services. Le concept de l'*IoT* a été introduit la première fois par Kevin Ashton en 1999 [9]. L'objectif de l'*IoT* est de permettre aux objets d'être connectés à tout moment, de n'importe où, avec n'importe quoi et n'importe qui, idéalement en utilisant n'importe quel réseau et tout service [9]. Les objets dans l'*IoT* incluent des objets physiques de très petites à très grandes machines qui communiquent de manière transparente entre eux via Internet sans intervention humaine [10]. Les dispositifs *IoT* sont équipés de capteurs pour capturer les données et des actionneurs pour effectuer les actions, le tout de manière autonome et intelligente [11]. Le programme « Cluster of European Research Projects on the Internet of Things » (CERP-*IoT*) [12] définit l'*IoT* comme une infrastructure dynamique d'un réseau global. Ce réseau global a des capacités d'autoconfiguration basées sur des standards et des protocoles de communication interopérables. Dans ce réseau, les objets physiques et virtuels ont des identités, des attributs physiques, des personnalités virtuelles et des interfaces intelligentes, et ils sont intégrés dans le réseau d'une façon transparente. Actuellement, l'*IoT* a gagné une attention considérable, car il apporte des avantages potentiellement énormes à la vie des humains. Selon [13], plus de 8.4 milliards d'objets connectés ont rejoint ce réseau en 2017, qui ont augmenté de 31 % par rapport à 2016 et atteignent 20.4 milliards en 2020. Plusieurs applications sont développées après l'apparition du concept de l'*IoT*, tels que les villes intelligentes, l'industrie intelligente, le transport intelligent, l'énergie intelligente, etc. Ces applications ont des caractéristiques spécifiques. Elles génèrent d'énormes volumes de données et nécessitent de la connectivité et de l'énergie pour de longues périodes. Ceci, associé aux limitations de la mémoire, de la capacité des dispositifs, des réseaux et de l'énergie, pose un grand nombre de défis. L'énorme expansion de l'*IoT* doit être soutenue par des mécanismes et des protocoles standards pour réduire l'hétérogénéité existante dans le domaine. Cependant, en dehors des défis d'hétérogénéité et d'intégration présents dans l'*IoT*, la sécurité de ces données est également une question importante qu'on doit prendre en considération. En effet, la sécurité constitue un enjeu majeur dans les environnements connectés, en particulier lorsqu'il s'agit de données sensibles comme celles des systèmes de santé intelligents.

1.1.3 Systèmes de soins de santé intelligents

L'adoption des Technologies de l'Information et de la Communication (TIC) dans le secteur de la santé a conduit au concept de santé numérique (e-santé), qui contribue à réduire les coûts et à accroître l'efficacité. Suite à la consolidation de l'e-santé, l'utilisation généralisée d'appareils mobiles (i.e., téléphones intelligents « smartphone ») avec des capacités de positionnement a ouvert la porte à l'idée de la santé mobile (m-santé), qui pourrait être comprise comme la fourniture de services de santé via les dispositifs de communication mobiles [14]. La technologie de m-santé a un potentiel extraordinaire car elle ajoute aux avantages de la cybersanté tous les avantages liés à l'omniprésence des appareils mobiles (i.e., capacités de surveillance mondiales, large disponibilité et immédiateté). Bien que des progrès significatifs aient été réalisés, la technologie de m-santé est encore à ses débuts et évolue parallèlement à un autre concept très prometteur : les villes intelligentes. Ce concept est également fondé sur les TIC et vise à s'attaquer aux problèmes locaux, à l'économie locale et aux transports, à la qualité de la vie et à l'e-gouvernance [14].

Les soins de santé intelligents est une combinaison de diverses entités tels que les soins de santé traditionnels, les biocapteurs intelligents, les appareils portables, les TIC et les systèmes d'ambulance intelligents. La Figure 1.1 représente les éléments des systèmes de soins de santé intelligents, dont divers mécanismes sont utilisés, tels que le « Cloud Computing », les applications pour téléphones intelligents et les techniques avancées d'analyse de données [15].

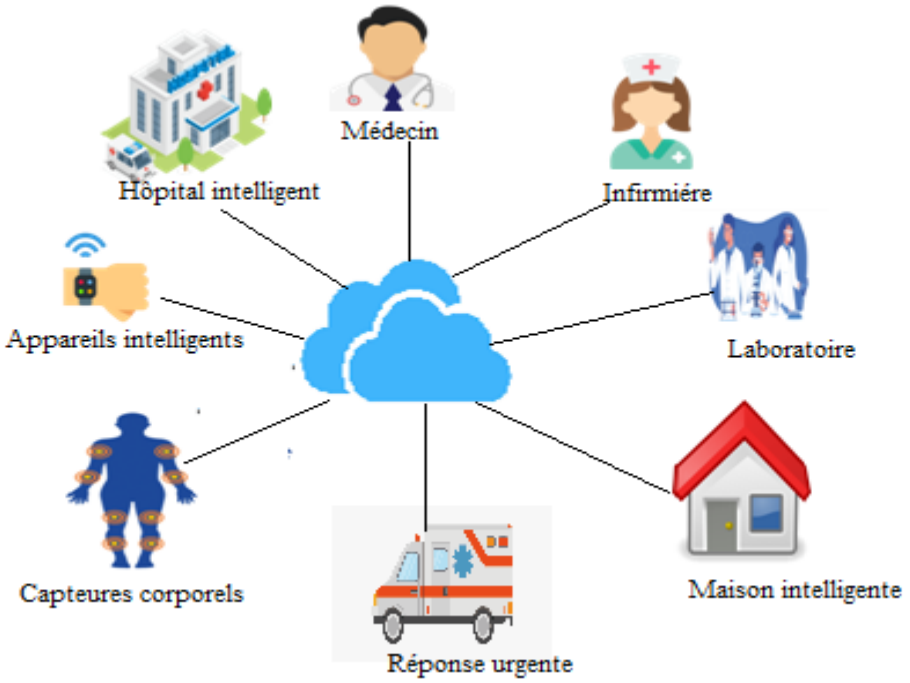


Figure 1.1 Les éléments des systèmes de soins de santé intelligents [15].

1.1.4 Dispositifs médicaux implantables (IMDs)

Les dispositifs médicaux implantables (IMDs) sont des dispositifs électroniques implantés dans le corps humain pour surveiller ou traiter divers types de maladies dans différents organes ou pour améliorer les fonctions médiocres de différentes parties du corps [16]. Ces appareils échangent des informations avec des appareils de surveillance ou de programmation à distance sur le réseau, ce qui les rend vulnérables aux attaques. De plus, la communication sans fil à longue portée et les contraintes de ressources de la batterie, du processeur et de la mémoire des IMDs rendent la sécurité de ces systèmes plus complexes [16].

Les IMDs sont classés en deux catégories [16] [17] :

- Boucle ouverte : où le patient peut contrôler l'actionnement de l'appareil tel que dans les pompes à insuline, les stimulateurs nerveux implantables, les simulateurs de vessie et les implants cochléaires;

- Boucle fermée : où les IMDs entièrement implantés sont des dispositifs médicaux où aucune intervention humaine n'est autorisée et dont l'actionnement est automatisé en fonction des mesures des capteurs tels que les simulateurs cardiaques.

Exemples des IMDs : il existe plusieurs types des dispositifs médicaux implantables, nous pouvons citer [16]:

- Implants cochléaires : il s'agit d'appareils électroniques implantés chirurgicalement pour améliorer l'audition des personnes qui ont des problèmes auditifs;

- Stimulateur gastrique : il est placé dans l'abdomen pour envoyer de légères impulsions électriques aux nerfs du bas de l'estomac, afin de diminuer les nausées et les vomissements;

- Pompes à insuline : elles sont implantées à l'intérieur du corps pour délivrer périodiquement de l'insuline;

- Stimulateurs cardiaques : ce sont des dispositifs alimentés par batterie placés sous la peau pour suivre la fréquence cardiaque et traiter les battements cardiaques irréguliers;

- Stimulateurs nerveux implantables : Ces appareils sont intégrés dans le corps et envoient un courant électrique pour traiter la douleur chronique.

1.1.5 La sécurité et les attaques dans les réseaux IoT

La sécurité est l'un des problèmes les plus importants dans les réseaux *IoT*. Pour échanger des messages en toute sécurité et pour garantir que les données critiques ne sont pas falsifiées ou interceptées par des attaquants, la sécurité du système *IoT* doit être assurée [6] [13].

Dans cette sous-section, nous présentons les attaques dans les réseaux *IoT*, les types d'attaques et les objectifs de sécurité qui doivent être satisfaits.

- Les attaques dans les réseaux IoT : une attaque peut être définie comme tout comportement anormal qui provient d'une entité qui a de mauvaises intentions, cette entité est appelée « un attaquant » [13]. Un attaquant est le nœud qui tente de lancer l'attaque sur le réseau, visant à voler ou à falsifier des informations, et à détruire ou à abattre le réseau. Les attaquants peuvent êtres catégorisés de la manière suivante [13]:

  - Insider vs Outsider (I/O) : l'insider se produit lorsque les entités légitimes se comportent de manière involontaire ou non autorisée. L'outsider est l'intrus avec une capacité d'attaque limitée.

- Malicieux vs Rationnel (M/R) : l'attaquant malveillant tente de nuire au réseau sans rechercher son avantage personnel, alors que l'attaquant rationnel anticipe ses propres avantages sur les attaques.
- Actif vs Passif (A/P) : un attaquant actif peut générer de nouveaux paquets pour endommager le réseau. En contrepartie, l'objectif d'un attaquant passif se résume en la détection et la découverte du réseau sans chercher à générer de nouveaux paquets.
- Local vs Etendu (L/E) : un attaquant local peut manipuler des entités limitées, tandis qu'un attaquant étendu peut contrôler plusieurs entités réparties sur le réseau.

- Types d'attaques dans les réseaux IoT*:* les communications entre les dispositifs IoT peuvent être menacées par plusieurs types d'attaques [13]. Parmi ces types d'attaques, nous pouvons citer :

- L'attaque par déni de service « Denial-of-service » (DoS) : l'attaquant tente de saturer le réseau en envoyant un grand nombre de faux messages pour rendre les services indisponibles pour les utilisateurs.
- L'attaque Sybil : un attaquant crée plusieurs fausses identités pour confondre d'autres entités en envoyant de mauvais messages pour gagner une grande influence. Ce type d'attaque est difficile à détecter et à corriger, surtout lorsque le nœud victime est isolé.
- L'attaque « Man in the Middle » (MIM) : un nœud malveillant intercepte la communication établie entre les dispositifs et renvoie des messages erronés.
- Le spam : un attaquant transmet des spams sur le réseau pour épuiser la bande passante du réseau et augmenter la latence de transmission;
- L'espionnage (Eavesdropping) : c'est une forme active de l'attaque MIM. Il vise à extraire des informations confidentielles des données protégées transmises sur le réseau et aux échanges dans les réseaux non-sécurisés.
- Falsification des messages : l'attaquant injecte des informations incorrectes ou fausses dans le réseau pour des avantages personnels. Ce type d'attaque consiste à modifier ou à supprimer une partie ou la totalité du message.

- Objectifs de sécurité : pour garantir un niveau de sécurité adéquat dans un système connecté, en particulier dans les environnements critiques tels que les systèmes de soins de santé intelligents, il est essentiel de satisfaire les objectifs suivants :

- Authentification : la nature critique des messages échangés entre les dispositifs impose une vérification rigoureuse de l'identité. L'authentification permet de s'assurer que chaque message provient bien d'un utilisateur ou d'un dispositif légitime.
- Confidentialité : les données sensibles doivent être protégées contre tout accès non autorisé. Cela implique le chiffrement des informations et la mise en place de mécanismes de contrôle d'accès limitant l'exposition des ressources.
- Non-répudiation : ce principe garantit qu'un émetteur ne peut pas nier avoir envoyé un message, et qu'un récepteur ne peut pas nier l'avoir reçu. Cela fournit une traçabilité essentielle, notamment dans le cadre de communications critiques ou juridiques.
- Intégrité : les données transmises doivent rester intactes. Toute modification non autorisée, accidentelle ou malveillante, doit pouvoir être détectée afin d'éviter des erreurs de diagnostic ou de traitement.
- Disponibilité : l'accès aux données et aux services doit être assuré en temps voulu pour les entités autorisées. Dans les systèmes de santé intelligents, un simple retard de transmission peut compromettre l'interprétation du message reçu, avec des conséquences potentiellement graves pour la santé du patient.

Le Tableau 1.1 résume les différents types d'attaques dans le réseau IoT ainsi que les services de sécurité menacés [5] [6] [13].

1.1.6 Cryptage léger

La cryptographie est un outil efficace pour garantir la confidentialité, l'intégrité et l'authentification [18]. Cependant, la plupart des appareils *IoT* ont des caractéristiques difficiles, telles que la limite de la mémoire, la puissance de la batterie et la capacité de traitement. Cependant, les algorithmes cryptographiques traditionnels ne conviennent pas aux appareils *IoT* à ressources limitées. Récemment, des primitives cryptographiques légères ont été proposées pour sécuriser les systèmes *IoT* tels que [18] :

- ECC (Elliptic Curve Cryptography) : c'est une technique cryptographique asymétrique légère qui offre le même niveau de sécurité que l'algorithme « Rivest-Shamir-Adleman » (RSA) avec une taille de clé plus petite.

- Les chiffrements par bloc : dans ces algorithmes, un bloc de texte en clair est chiffré à la fois.

- Les chiffrements en flux : ils chiffrent ou déchiffrent un seul bit ou octet de texte.

Tableau 1.1 Les types d'attaques dans les réseaux IoT [5] [6] [13].

Attaques	Services menacés	Type d'attaque	Solutions
DOS	Disponibilité	I/O,A,M,L/E	Signature digitale, protocoles de routages, et confiance des nœuds.
Attaque Sybil	Authentification Disponibilité	I,A,R/M,L/E	Autorité de validation centrale (VA), PKI pour la distribution/ révocation des clés.
MITM	Confidentialité Authentification Intégrité Non-répudiation	I,A/P,M/R,L	Méthodes d'authentification robustes, et cryptographie puissante.
Spamming	Disponibilité Confidentialité	I,A,M,L/E	Signature digitale des logiciels et des capteurs.
L'espionnage	Confidentialité	I,P,R,L	Cryptographie symétrique/Asymétrique des messages sécurisés.
Falsification de message	Intégrité Authentification	I/O,A,R/M,L	Algorithme de similarité, et système de gestion de la confiance et de la réputation.

- Les fonctions de hachage : elles sont utilisées pour assurer l'intégrité des données en générant un message de longueur fixe à partir d'un message de longueur arbitraire.

- Lattice-Based Public-Key Cryptography (LB-PKC) : elle représente l'ensemble de toutes les combinaisons linéaires entières de vecteurs de base. La fonction Lattice peut être définie sur une structure d'anneaux et de champs d'algèbre abstraite notée sur un ensemble L avec deux opérations + et -. Elle peut être écrite comme (L, +, -). Mathématiquement, elle est désignée par [19] :

$$\boldsymbol{L} = \{\sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} a_i v_i \,|a_i \in \mathbf{Z^n}\},$$

Où, $\{v_1, v_2 \ldots\ldots v_n\}$ est le vecteur de base et $\{a_1, a_2 \ldots\ldots a_n\}$ sont les coefficients entiers de l'équation polynomiale. La fonction *Lattice* présente les avantages recommandés par l'institut national des normes et de la technologie « National Institute of Standards and Technology » (NIST) pour les réseaux *IoT* [20]: sécurisée contre les attaques des canaux, résistante aux falsifications quantiques et aux attaques de collusion. De plus, elle utilise des clés de petites tailles, ce qui rend le cryptage et le décryptage avec *Lattice* léger. Cependant, il existe deux problèmes majeurs associés à cette fonction qui sont le problème vectoriel le plus court « Shortest Vector Problem » (SVP) et le

problème vectoriel le plus proche « Closest Vector Problem » (CVP) [21]. Où, SVP est associé à la recherche des vecteurs non nuls les plus courts dans un vecteur de *Lattice* n-dimensionnel donné, et CVP est associé à la recherche d'un vecteur dans L qui est le plus proche du vecteur non-*Lattice* donné, c'est-à-dire le vecteur qui se trouve à l'extérieur de l'espace vectoriel du *Lattice* à n-dimensions. Ces deux problèmes sont considérés comme des problèmes NP-difficiles [21].

Sur la base de ces deux problèmes, plusieurs solutions ont été proposées dans la littérature pour trouver une solution contre ces problèmes. La Figure 1.2 montre une taxonomie des solutions LB-PKC [19].

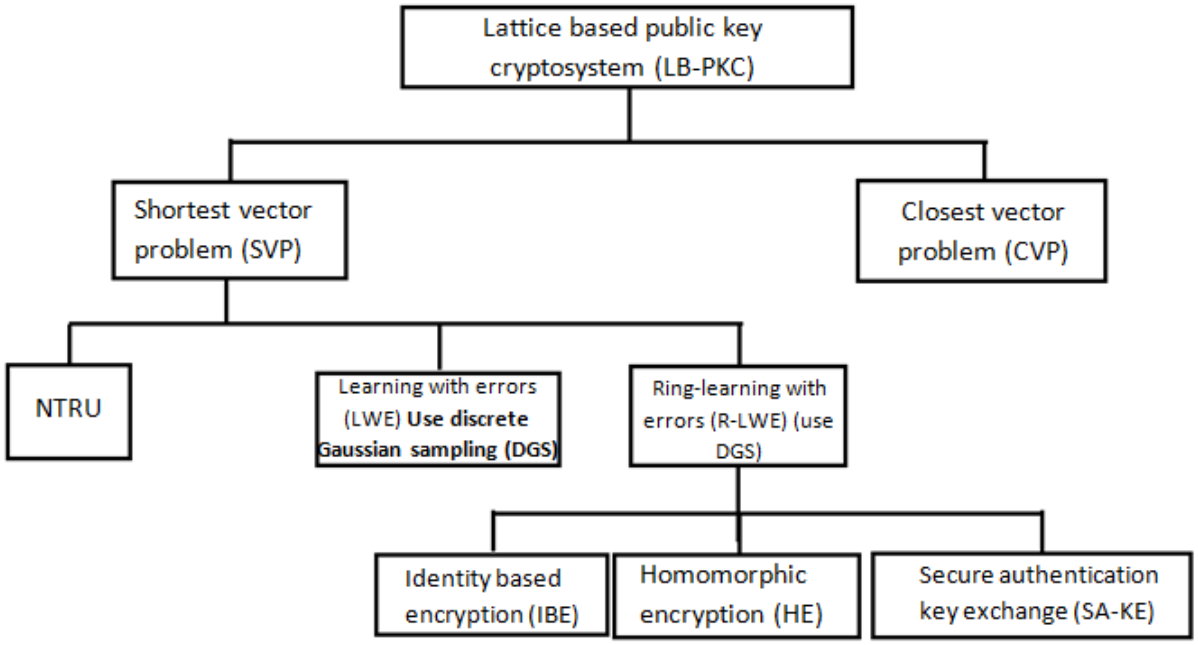


Figure 1.2 Taxonomie de LB-PKC [19].

1.1.7 Apprentissage automatique

L'apprentissage automatique « Machine Learning » (ML) fait référence à des méthodes intelligentes utilisées pour optimiser les critères de performance à l'aide d'exemples de données ou d'expériences passées grâce à l'apprentissage [22]. Plus précisément, les algorithmes *ML* construisent des modèles de comportements à l'aide de techniques mathématiques sur d'énormes ensembles de données. Le *ML* permet également d'apprendre sans être explicitement programmé. Ces modèles sont utilisés comme base pour faire des prévisions futures basées sur les nouvelles données d'entrée. Le *ML* est de nature interdisciplinaire et hérite de ses racines de nombreuses

disciplines de la science et de l'ingénierie qui incluent l'intelligence artificielle, la théorie de l'optimisation, la théorie de l'information et les sciences cognitives [22].

L'apprentissage automatique est utilisé lorsque l'expertise humaine n'existe pas ou ne peut pas être utilisée, comme la navigation dans un endroit hostile où les humains sont incapables d'utiliser leur expertise, plus spécifiquement dans le domaine de la robotique, la reconnaissance vocale, etc. Il est également appliqué dans des situations où la solution d'un problème spécifique change dans le temps (i.e., routage dans un réseau informatique, recherche de code malveillant dans un logiciel ou une application). De plus, il peut être utilisé dans des systèmes intelligents pratiques. Par exemple, Google utilise le *ML* pour analyser les menaces contre les points de terminaison mobiles et les applications qui fonctionnent sur Android. Le *ML* est également utilisé pour identifier et supprimer les logiciels malveillants des combinés infectés [23].

Les algorithmes de Machine Learning (ML) peuvent être classés en quatre grandes catégories [23], comme le montre la Figure 1.3 : apprentissage supervisé, apprentissage non supervisé, apprentissage semi-supervisé et apprentissage par renforcement.

- Apprentissage supervisé : l'apprentissage supervisé est utilisé lorsque des objectifs spécifiques sont fixés à partir d'un ensemble d'entrées connues. Les données sont étiquetées, c'est-à-dire qu'à chaque entrée est associée une sortie attendue. Le modèle apprend à partir de ces correspondances pour ensuite prédire la classe d'un nouvel élément. Ce type d'apprentissage nécessite généralement des ressources importantes en termes de stockage et de puissance de calcul. Parmi les algorithmes supervisés couramment utilisés, on retrouve : « Support Vector Machine » (SVM), « Naïve Bayes » (NB), Arbres de décision « Decision Tree » (DT) et XGBoost (eXtreme Gradient Boosting) [23].

- Apprentissage non supervisé : dans l'apprentissage non supervisé, les données ne sont pas étiquetées. Le système tente de découvrir des structures cachées ou des regroupements dans les données sans indication préalable. Cela permet, par exemple, de regrouper des comportements similaires dans les réseaux. Exemples des algorithmes non supervisés, on cite: « K-means » et « Hierarchical Clustering » [23].

- Apprentissage semi-supervisé : l'apprentissage semi-supervisé combine les deux approches précédentes. Il utilise un petit ensemble de données étiquetées et un grand volume de données non étiquetées. Ce type d'apprentissage est particulièrement utile lorsque l'étiquetage est coûteux ou difficile, comme c'est souvent le cas dans la détection d'attaques réseau. Il permet de réduire la

dépendance aux données annotées, tout en améliorant la précision des modèles. Parmi les méthodes semi-supervisées les plus courantes, on trouve le « Self-training », le « Co-training », les algorithmes à base de graphes tels que « Label Propagation », ainsi que des extensions comme les « Support Vector Machines semi-supervisés » (S3VM). Plus récemment, les GANs semi-supervisés ont montré un fort potentiel pour améliorer les performances en présence de données limitées [23].

- Apprentissage par renforcement : dans l'apprentissage par renforcement « Reinforcement Learning » (RL), l'agent apprend à interagir avec un environnement en recevant des récompenses ou des punitions. L'objectif est de maximiser la récompense cumulative. Ce paradigme, inspiré de l'apprentissage comportemental, est adapté aux situations dynamiques et complexes, comme l'authentification adaptative ou la gestion des accès réseau. Le choix de la fonction de récompense est critique, car il conditionne le comportement optimal de l'agent [23].

La Figure 1.3 illustre une classification des algorithmes ML et leurs applications typiques pour la détection et la prévention des attaques sur les réseaux IoT [23].

1.2 Éléments de la problématique

Dans les systèmes de soins de santé, les données sont critiques et toute modification de ces données peut affecter la vie et la santé des patients [24] [25] [26] [27]. Vu la criticité de ces données, la sécurité des données est un aspect très important dans les systèmes de soins de santé intelligents. Cependant, l'échange de ces données peut être menacé par plusieurs types d'attaques réseau (e.g., DoS, MIM, Attaque Sybil, falsification des messages et usurpation d'identité, etc.). De ce fait, l'authentification, l'intégrité, la confidentialité, la non-répudiation, la disponibilité et le contrôle d'accès sont des critères très importants pour assurer la sécurité d'un système de soins de santé intelligent et pour protéger les données médicales, tout en prenant en compte la protection de la vie privée des utilisateurs (i.e., patients, médecins).

La petite taille des dispositifs médicaux pose des contraintes sur la puissance de traitement, l'énergie et la capacité de stockage [28] [29] [30] [31] [32] [33]. De plus, le besoin d'une opération chirurgicale pour changer ou implanter quelques types des dispositifs médicaux, tels que les simulateurs cardiaques, nécessite une très faible consommation d'énergie. Pour réduire la consommation d'énergie on a besoin de minimiser le coût de calcul et donc avoir une cryptographie légère pour crypter les données collectées par les dispositifs médicaux. De plus, la transmission des

messages nécessite une bonne quantité d'énergie pour transmettre les données aux destinataires [28] [29], on doit alors avoir une courte portée de transmission pour conserver l'énergie.

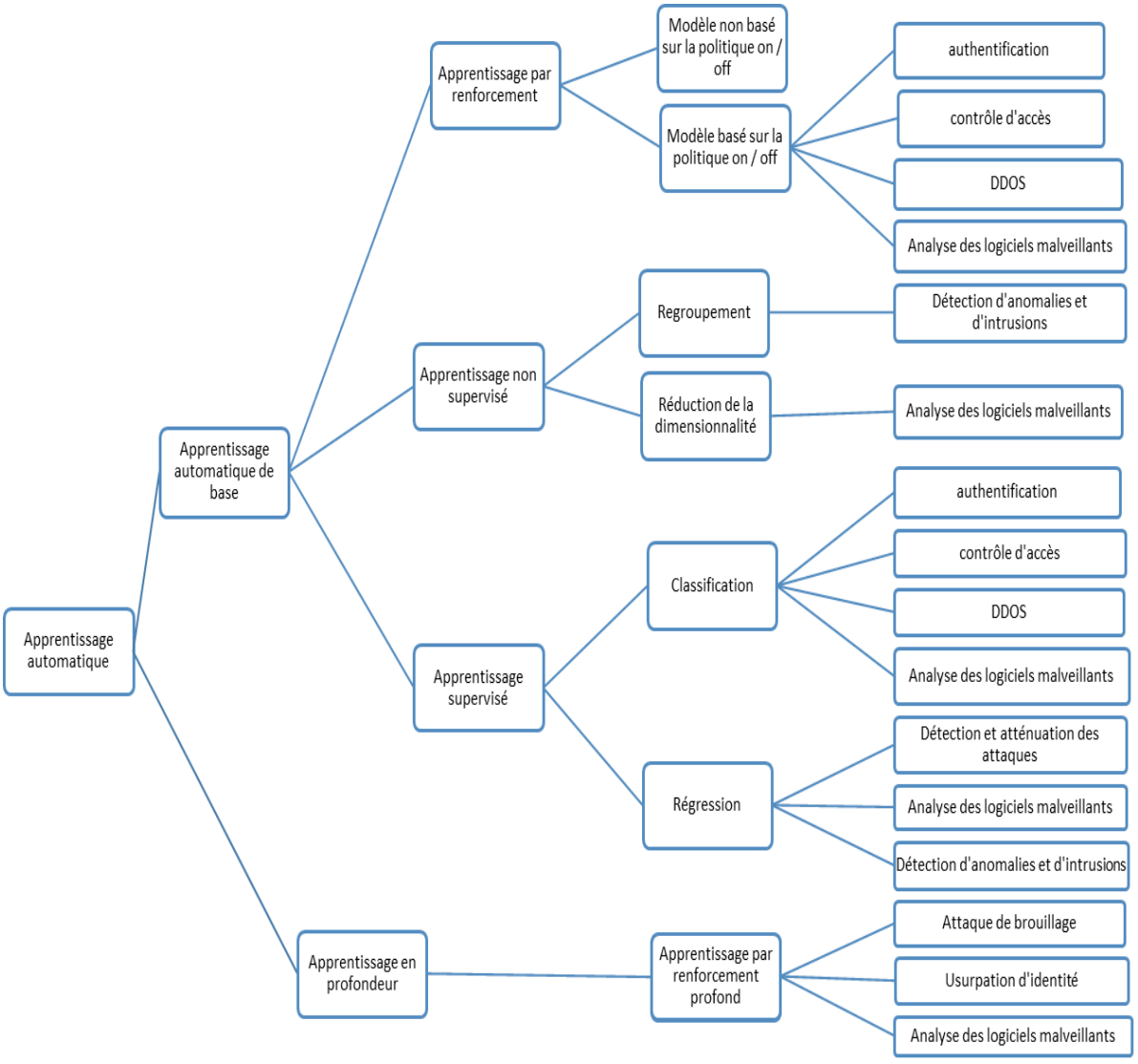


Figure 1.3 Les classes des algorithmes ML et leurs applications typiques [23].

Pour assurer la confidentialité des données nous avons besoin d'une cryptographie, symétrique ou asymétrique. La cryptographie symétrique nécessite des calculs légers mais elle est faible et elle peut être cassée facilement par des attaques, cependant la cryptographie asymétrique nécessite des calculs complexes mais elle est plus fiable et assure un niveau plus élevé de sécurité. Dans les systèmes de soins de santé intelligents nous avons besoin d'un algorithme de cryptage robuste

contre tout type d'attaques avec un coût de calcul minimal, ce qui nous conduit aux algorithmes de cryptage légers tels que ECC.

Dernièrement, les ordinateurs quantiques ont la capacité de résoudre des équations de cryptographie classique incroyablement complexes, notamment pour décoder les clés secrètes cryptées et rendre le réseau vulnérable au piratage. Ils peuvent résoudre des problèmes mathématiques complexes presque instantanément par rapport aux milliards d'années de calcul nécessaires aux machines informatiques traditionnelles. Par conséquence, les algorithmes de cryptage classique tels que RSA, ECC deviendront inutile face à cette percée technologique. Donc, une solution robuste et résistante contre ce type d'attaque est primordiale pour assurer la sécurité.

L'intégration des algorithmes d'apprentissage automatique dans les systèmes de soins de santé intelligents permet la prédiction et la détection des attaques réseau. Cependant, cette intégration soulève plusieurs problèmes [34] [35] [36] [37] [38] [39] [40] [41] [42]. Les algorithmes d'apprentissage automatique nécessitent des ensembles de données authentiques provenant de l'environnement physique réel pour l'entraînement et les tests, ce qui est difficile à obtenir dans le domaine médical à cause des contraintes liées à la protection de la vie privée des patients. De plus, ces algorithmes sont parfois limités en termes d'évolutivité, d'extraction automatique de caractéristiques et de précision dans des environnements complexes.

Par ailleurs, les systèmes de soins de santé intelligents exigent une communication sécurisée, en temps réel et sans interruption. Tout retard dans la détection d'une attaque ou dans la vérification d'une identité peut avoir un impact direct sur la santé du patient. Les approches classiques d'authentification et de contrôle d'accès sont souvent statiques et mal adaptées à des environnements IoT hétérogènes et dynamiques.

Les algorithmes d'apprentissage par renforcement offrent une solution prometteuse à ces contraintes. Ils permettent d'élaborer des politiques d'accès adaptatives et intelligentes, capables de réagir à l'évolution du comportement des entités du réseau, tout en respectant les contraintes temps réel. Malgré cela, ces algorithmes présentent eux aussi des défis, notamment un temps de convergence plus long, qui peut rendre leur intégration difficile dans des applications très sensibles.

Face à ces limites, cette recherche vise à proposer une architecture de sécurité basée sur des techniques légères de cryptographie post-quantique, combinées à des algorithmes d'apprentissage automatique pour la détection des attaques, et à l'apprentissage par renforcement pour

l'authentification et le contrôle d'accès. Cette approche permet d'adresser les contraintes spécifiques des dispositifs médicaux connectés, tout en assurant la fiabilité et la réactivité du système.

Ces éléments de la problématique nous ont permis de dériver une question de recherche générale qui se décompose en question secondaires que nous citons comme suit :

- *Question principale*

Comment peut-on assurer la sécurité des données et la protection de la vie privée des utilisateurs dans les systèmes de soins de santé dans les villes intelligentes ?

- *Questions secondaires*

1- Comment peut-on réduire les problèmes liés à la capacité des *IMD* (i.e., calcul, stockage et énergie), tout en assurant la sécurité des données dans les systèmes de soins de santé intelligents ?

2- Comment peut-on prédire et détecter les vulnérabilités, les attaques et les logiciels malveillants dans les systèmes de soins de santé intelligents?

3- Comment peut-on assurer une authentification et un contrôle d'accès adaptatifs pour protéger les données privées des patients dans un environnement de soins de santé intelligent ?

1.3 Objectifs de recherche

L'objectif principal de cette thèse est de proposer une architecture sécurisée pour préserver la vie privée des utilisateurs et sécuriser l'accès et les échanges des données au sein des systèmes de soins de santé dans les villes intelligentes. Plus spécifiquement, nous visons à :

1- Concevoir un algorithme qui ne nécessite pas des calculs complexes au niveau des IMD pour éliminer les problèmes liés à la capacité de ces derniers et assurer la sécurité des données.

2- Proposer un modèle de sécurité pour prédire les attaques et détecter les vulnérabilités dans les systèmes de soins de santé intelligents.

3- Concevoir un modèle d'authentification et de contrôle d'accès adaptatif afin d'assurer la protection des données privées des patients dans un environnement de soins de santé intelligent.

4- Implémenter l'algorithme et les modèles proposés.

5- Évaluer les performances de l'algorithme et des modèles proposés en termes de sécurité.

1.4 Plan de la thèse

Dans ce chapitre introductif, nous présentons le contexte général de la thèse, les motivations scientifiques et les objectifs poursuivis. Nous commençons par définir les concepts fondamentaux liés aux villes intelligentes, aux réseaux IoT médicaux, ainsi qu'aux problématiques de sécurité qui y sont associées. Ensuite, nous exposons les éléments de problématique, formulons les questions de recherche et définissons les objectifs ainsi que les principales contributions de cette thèse. La suite de ce document est structurée en huit chapitres.

Le chapitre 2 est consacré à une revue critique de la littérature sur les approches existantes de sécurisation des systèmes de soins de santé intelligents. Nous y analysons les travaux récents liés à la cryptographie légère, à la détection d'attaques dans les réseaux IoT, ainsi qu'aux modèles d'authentification et de contrôle d'accès.

Le chapitre 3 présente la méthodologie adoptée pour mener les travaux de cette thèse. Nous y expliquons comment les différents axes de recherche sont interconnectés et comment ils répondent aux objectifs définis. Ce chapitre inclut également un aperçu des publications issues de cette recherche.

Le chapitre 4 est consacré à la première contribution, portant sur la conception d'un algorithme de cryptographie légère basé sur les réseaux euclidiens « *lattice-based cryptography* ». Cette solution vise à répondre aux contraintes strictes des dispositifs médicaux implantables en termes de calcul, stockage et énergie.

Le chapitre 5 traite de la deuxième contribution, centrée sur la détection des attaques et la préservation de l'intégrité des données dans les systèmes de santé intelligents. Un modèle d'apprentissage automatique y est proposé pour détecter de manière proactive les vulnérabilités et comportements malveillants dans le réseau.

Le chapitre 6 présente la troisième contribution de cette thèse. Il s'agit de la conception d'un modèle d'authentification et de contrôle d'accès basé sur l'apprentissage par renforcement. Ce modèle vise à fournir une solution adaptative capable de s'ajuster dynamiquement au contexte du réseau et aux profils des utilisateurs.

Le chapitre 7 propose une discussion générale des résultats obtenus. Nous y confrontons les apports de cette thèse aux travaux de la littérature, et analysons les avantages, limites et perspectives d'amélioration des solutions proposées.

Enfin, le chapitre 8 conclut cette thèse. Il résume les contributions majeures, revient sur les objectifs atteints, et propose des pistes pour les travaux futurs.

CHAPITRE 2 REVUE DE LITTERATURE

Ce chapitre est consacré à une revue critique de la littérature. Dans un premier temps, nous présentons les travaux scientifiques portant sur la sécurité des systèmes de soins de santé intelligents, en mettant l'accent sur les vulnérabilités inhérentes à ces environnements et aux dispositifs médicaux qui y sont intégrés. Ensuite, nous passons en revue les solutions existantes pour améliorer la confidentialité et la protection de la vie privée au sein de ces systèmes. Enfin, nous nous intéressons aux approches basées sur l'intelligence artificielle, en particulier aux techniques d'apprentissage automatique utilisées pour détecter les anomalies et les attaques, ainsi qu'aux méthodes d'apprentissage par renforcement visant à renforcer l'authentification des utilisateurs et à assurer un contrôle d'accès adapté aux données médicales sensibles.

2.1 La sécurité des systèmes de soins de santé intelligents

La sécurité des données dans les systèmes de soins de santé intelligents joue un rôle primordial dans la protection de la vie et de la santé des patients. De nombreux travaux ont été menés afin de renforcer ces systèmes face aux risques croissants liés aux cybermenaces.

Tanwar *et al.* [24] ont conçu un système sécurisé et efficace de partage des services de santé électroniques (EHS), intégrant des mécanismes renforcés de protection de la vie privée. Ce système repose sur des autorisations à clé cryptographique et l'implémentation d'un algorithme de politique de contrôle d'accès automatisé. Toutefois, il présente des limites importantes en matière d'authentification, d'anonymat et de non-répudiation. En outre, sa lourdeur computationnelle nuit à une intervention médicale en temps réel.

Chen *et al*. [25] ont proposé un modèle de cryptage interrogeable permettant l'extraction et le partage sécurisé des dossiers médicaux à l'aide d'expressions booléennes complexes et d'indexation. Ce modèle vise à garantir l'équité entre les détenteurs de données et les utilisateurs, mais souffre d'un manque d'évolutivité.

Biswas *et al.* [26] ont introduit une approche d'intégration progressive des EHS vers un modèle unifié, facilitant les échanges sécurisés d'actifs numériques entre entités médicales. Le contrôle d'accès est géré à travers des clés composées, permettant une gestion fluide des droits sans modifications fréquentes des règles d'accès. Cependant, ce modèle n'assure pas de garanties suffisantes en matière d'anonymat, d'authentification, et de protection des informations sensibles.

Sun *et al.* [27] ont développé un modèle de signature décentralisée fondé sur les attributs pour améliorer le contrôle d'accès aux données de santé. Ce modèle permet un partage sécurisé entre différents organismes de soins tout en préservant une partie de la confidentialité, mais reste limité par des contraintes sur les certificats d'attributs et les capacités de stockage.

Au-delà des solutions centrées sur la gestion des données et le contrôle d'accès, plusieurs travaux se sont intéressés à la détection des attaques visant les dispositifs médicaux connectés ainsi que la transmission des données qu'ils génèrent. Ces dispositifs, souvent limités en ressources, présentent des vulnérabilités particulières qui nécessitent des approches de sécurité spécifiques et adaptées. Thamilarasu *et al.* [28] ont proposé un système de détection d'intrusion pour les objets connectés médicaux. De plus, ils ont développé un mécanisme de détection d'attaques hiérarchique et distribué dans les dispositifs de santé connectés à l'aide d'agents mobiles autonomes., Dans ce réseau, chaque nœud agit comme un nœud informatique, et les agents mobiles migrent, apprennent et effectuent en collaboration la détection des attaques. Les auteurs ont utilisé des algorithmes d'apprentissage automatique et de régression pour détecter les intrusions au niveau du réseau, ainsi que les anomalies dans les données des capteurs. Cependant, ils n'ont pas pris en charge le traitement du problème de consommation d'énergie, la préservation de la vie privée des patients, ainsi que la confidentialité et l'intégrité des données.

Newaz *et al.* [29] ont présenté un nouveau système de détection d'intrusion pour surveiller le trafic des dispositifs médicaux personnels et détecter les attaques. Ce système se connecte passivement à la communication des dispositifs médicaux personnels « Personal Medical Devices » (PMD) et génère des n-grammes de différentes tailles à partir de différentes caractéristiques de trafic, tels que les types de PDU, les modèles de trafic séquentiels, etc. Ces caractéristiques sont transmises à différentes techniques d'apprentissage automatique « Machine Learning » (ML) pour détecter les modèles de flux de trafic irréguliers dans la communication PMD. En revanche, ce système ne préserve pas la vie privée des patients et ne prend pas en considération le problème de consommation d'énergie des PMD.

Pinisetty *et al.* [30] ont proposé une solution pour sécuriser les stimulateurs cardiaques à l'aide de la vérification d'exécution. Cette solution est basée sur un système de détection des attaques utilisant une technologie de détection d'électrocardiogramme (ECG) combinée à des méthodes formelles. De plus, les auteurs ont proposé un dispositif portable qui permet de détecter de manière

non invasive les signaux ECG familiers, afin de déterminer si un stimulateur cardiaque a été compromis et un ensemble de politiques temporisées a été développé pour surveiller les signaux ECG au moment de l'exécution. Cette solution ne préserve pas la vie privée des patients, la confidentialité et l'intégrité des données. En outre, elle est testée en utilisant l'ECG d'un seul patient, ce qui rend les données non réelles.

Zhang *et al.* [31] ont proposé un système pour sécuriser les dispositifs médicaux grâce à la surveillance sans fil et à la détection d'anomalies, afin de détecter et prévenir les événements anormaux en espionnant toutes les transactions sans fil. Les auteurs ont adopté un moniteur de sécurité médicale « Medical Monitor » (MedMon) qui espionne toutes les communications radiofréquences sans fil vers/depuis les dispositifs médicaux. De plus, ils ont utilisé la détection d'anomalies multicouches pour identifier les transactions potentiellement malveillantes. Lors de la détection d'une transaction malveillante, *MedMon* prend les mesures de réponse appropriées, qui peuvent aller de passive (i.e., notifier l'utilisateur) à active (i.e., bloquer les paquets pour qu'ils n'atteignent pas le dispositif médical). Cependant, les auteurs n'ont pas pris en charge la préservation de la vie privée des patients, ainsi que la confidentialité et l'intégrité des données.

Bu *et al.* [32] ont proposé une solution de sécurisation des canaux de communication des dispositifs médicaux implantables pour faire face aux attaques existantes et potentielles de type Man-In-The-Middle sur la communication sans fil des dispositifs médicaux. Les auteurs ont utilisé un chiffrement authentifié avec un vecteur aléatoire et un horodatage encodé par des codes robustes ou « Algebraic Manipulation Detection » (AMD) pour assurer la confidentialité et l'intégrité des paquets transmis et reçus. Les codes robustes avec moins de complexité matérielle sont utilisés si les attaquants ont une connaissance minimale du contenu des paquets transmis. Les codes AMD avec un coût matériel plus élevé sont utilisés pour se protéger contre des attaquants plus avertis. En revanche, cette solution proposée ne préserve pas de la vie privée des patients.

Gibson *et al.* [33] ont présenté une solution qui authentifie l'opérateur des programmeurs de stimulateur cardiaque et qui applique un accès sécurisé à l'appareil implanté selon le consentement éclairé du patient. Basant sur la Blockchain qui fournit une authentification et une autorisation en fonction du consentement du patient. Les auteurs conçoivent des protocoles qui permettent aux médecins d'obtenir des licences médicales numériques. Ces protocoles permettent aux patients d'obtenir et de vérifier le consentement numérique du patient et des informations d'identification de

l'opérateur. Cette solution ne préserve pas de la vie privée des patients et ne prend pas en charge le problème de consommation d'énergie des stimulateurs cardiaques.

Par ailleurs, Plusieurs travaux ont été menés autour de la conception d'architectures intelligentes visant à renforcer la sécurité, la gestion et le traitement des données dans les systèmes de soins de santé connectés.

Singh *et al.* [43] ont proposé une architecture à quatre couches, incluant une couche des appareils intelligents destinée à produire un volume massif de données, une couche Edge Intelligence chargée de l'analyse du trafic des dispositifs de détection, une couche Fog Intelligence pour le traitement intermédiaire, et une couche Cloud Intelligence assurant le stockage des données. Cette architecture vise à combiner de manière efficace l'intelligence en périphérie avec les technologies émergentes pour optimiser le traitement des données dans les environnements IoT médicaux. Toutefois, elle ne prend pas en considération les contraintes de calcul, de stockage et d'énergie propres aux dispositifs embarqués, ce qui limite son applicabilité en temps réel.

Dans une perspective similaire, les auteurs de [44] ont proposé une autre architecture à trois couches pour le partage sécurisé des dossiers médicaux électroniques entre les différents acteurs du domaine de la santé. La première couche, située au niveau des dispositifs, génère des modèles d'apprentissage locaux et initie les contrats de traitement. La couche Edge Computing regroupe ensuite ces modèles, tandis que la couche Cloud Server assure le stockage centralisé. Cette architecture inclut un mécanisme d'authentification robuste fondé sur la cryptographie Lattice, ainsi qu'un module de prédiction des maladies basé sur les données EHR. Malgré ces apports, elle souffre d'un temps de traitement élevé et ne prévoit ni mécanisme efficace de contrôle d'accès, ni solution de détection proactive des attaques.

Dans le même esprit, Rathore *et al.* [45] ont présenté une architecture de quatre couches incluant une couche de captage pour la collecte de données, une couche « Edge Computing » pour le traitement initial, une couche « Fog Computing » pour l'analyse approfondie et la détection des anomalies, et une couche « Cloud Computing » dédiée au stockage. Cette architecture tire parti du réseau défini par logiciel « Software-Defined Networking » (SDN) pour assurer une surveillance continue des flux de données. Cependant, elle nécessite une puissance de calcul importante, ce qui limite également son efficacité en contexte temps réel.

Enfin, Nguyen *et al.* [46] ont proposé une architecture en deux couches, avec une passerelle locale chargée de collecter les données des patients à l'échelle locale, et une couche « Cloud Computing » assurant la gestion, la sécurité et le contrôle d'accès. Cette approche met en œuvre des mécanismes de partage sécurisé basés sur des politiques d'accès dynamiques, dans le but de garantir une distribution fiable des données entre patients et professionnels de santé. Toutefois, cette solution ne traite pas suffisamment les problématiques liées à la protection de la vie privée des patients ni la sécurité des données transmises depuis les capteurs corporels.

2.2 Approches de cryptographie pour améliorer la confidentialité des SSSI

La confidentialité des données de santé, notamment celles transmises par les dispositifs médicaux connectés, représente un défi central. Ces dispositifs étant souvent limités en capacité de calcul, de stockage et d'énergie, ils nécessitent des solutions de protection légères et adaptées, capables d'assurer un haut niveau de confidentialité sans compromettre leur performance ni leur autonomie. Face aux exigences croissantes en matière de confidentialité des données médicales, notamment celles transmises par les dispositifs connectés à ressources limitées, il devient essentiel d'adopter des mécanismes de chiffrement adaptés. Les schémas classiques tels que le standard de chiffrement avancée « Advanced Encryption Standard » (AES) [47], « Rivest–Shamir–Adleman » (RSA) [48] et la cryptographie à courbes elliptiques « Elliptic Curve Cryptography » (ECC) [49], bien que efficaces dans des environnements standards, requièrent des opérations mathématiques complexes et une mémoire importante, ce qui les rend peu compatibles avec les dispositifs médicaux embarqués. De surcroît, les schémas de cryptographie à clé publique reposant sur la factorisation d'entiers ou les logarithmes discrets sont vulnérables aux attaques en temps polynomial rendues possibles par les algorithmes quantiques de Shor [50], [51]. L'augmentation de la taille des clés ne suffit pas à garantir leur sécurité face aux capacités croissantes des ordinateurs quantiques. Pour anticiper cette menace, l'institut national des normes et de la technologie « National Institute of Standards and Technology » (NIST) a lancé un projet de standardisation des algorithmes de cryptographie post-quantique « Post-Quantum Cryptography » (PQC). Parmi les nombreuses propositions reçues, quatre algorithmes ont été retenus pour la phase finale : Le classic McEliece, La suite cryptographique pour les réseaux algébriques « Cryptographic Suite for Algebraic Lattices » (CRYSTALS-Kyber), les unités de polynômes tronqués du N-ième degré « N-th degree Truncated Polynomial Ring Units » (NTRU) et le schéma d'apprentissage modulaire par arrondi LWR « Modulaire Learning With Rounding LWR Scheme » (SABER). Ces schémas s'appuient

sur des problèmes mathématiques réputés difficiles au sein des réseaux euclidiens, tels que le problème du vecteur le plus proche « Closest Vector Problem » (CVP), le plus court vecteur « Shortest Vector Problem » (SVP) et l'apprentissage avec erreurs (LWE). Cinq autres algorithmes : L'encapsulation de clé par retournement de bits « Bit Flipping Key Encapsulation » (BIKE), le mécanisme d'encapsulation de clé basé sur l'apprentissage avec erreurs « A Learning With Errors Key Encapsulation Mechanism » (FrodoKEM), le code quasi-cyclique de Hamming « Hamming Quasi-Cyclic » (HQC), NTRU Prime et l'encapsulation de clé par isogénies supersingulières « Supersingular Isogeny Key Encapsulation » (SIKE), sont encore à l'étude en tant qu'alternatives potentielles. Les schémas de chiffrement fondés sur les réseaux sont aujourd'hui reconnus pour leur résistance aux attaques quantiques, et plusieurs travaux récents s'en sont inspirés pour renforcer la sécurité des algorithmes existants. Dans [52], un nouveau schéma d'attribution de clés basé sur les attributs (CP-ABE) utilisant la cryptographie sur réseaux est proposé. Ce modèle améliore la résistance aux attaques quantiques en combinant l'approche CP-ABE avec un partage de secrets linéaire (LSSS) et une technique de randomisation des clés privées. Une autre variante post-quantique du RSA, appelée LB-RSA (Lattice-Based RSA), a été proposée dans [53] pour sécuriser les échanges de données dans les applications cloud basées sur l'IoT. Elle augmente la sécurité en agrandissant les dimensions des clés, sans en accroître la taille.

D'autres études ont également optimisé les performances de l'algorithme SABER basé sur les réseaux, en utilisant la multiplication polynomiale via la transformée arithmétique des nombres « Number Theoretic Transform » (NTT), comme dans [54] et [55], ou encore l'algorithme de Karatsuba pour en alléger le coût de calcul dans [56].

Par ailleurs, Lyubashevsky *et al*. [57] ont introduit le Ring-LWE, une variante du LWE appliquée aux anneaux polynomiaux, qui permet de réduire la taille des clés tout en conservant un niveau de sécurité élevé. Malgré ses avantages, le Ring-LWE reste difficile à implémenter efficacement à cause de la complexité du générateur Gaussien et du coût élevé de la multiplication polynomiale.

Des travaux comme [58] ont proposé des méthodes alternatives pour éviter ce générateur, tandis que Howe *et al*. [59] ont évalué différentes techniques de génération Gaussienne, en proposant des architectures matérielles optimisées pour des échantillonnages tels que CDT, Bernoulli, Knuth-Yao, ou encore Ziggurat. Une autre variante, le Binary Ring-LWE (BRLWE), remplace la distribution Gaussienne par une distribution binaire pour réduire à la fois la taille des textes chiffrés

et le coût des opérations. Il a été mis en œuvre sur des microcontrôleurs 8 et 32 bits, adaptés aux contraintes de l'IoT. À partir du BRLWE, Aydin *et al.* [60] ont développé une implémentation matérielle avec contre-mesures contre les attaques par canaux auxiliaires (DPA), en utilisant la randomisation des états intermédiaires et un décodage masqué. Une autre version [61] introduit un masquage matériel sans générateur pseudo-aléatoire, améliorant ainsi la rapidité et l'efficacité.

L'étude [62] présente une architecture matérielle efficace pour BRLWE, optimisée pour les applications légères, capable d'exécuter l'opération arithmétique $AB + C$ sur des anneaux polynomiaux tout en réduisant la consommation énergétique.

Dans [63], Ebrahimi *et al.* ont proposé des implémentations logicielles résilientes aux fautes de BRLWE, testées sur des microcontrôleurs à faibles ressources (AVR ATxmega128A1 et ARM Cortex-M0). L'étude analyse la vulnérabilité des versions antérieures du BRLWE face à divers types d'attaques par faute, notamment la randomisation, la mise à zéro et l'omission d'instructions. En parallèle, une nouvelle variante appelée Ring-ExpLWE a été proposée dans [64], où les vecteurs d'erreurs sont issus d'une distribution exponentielle. Cette approche renforce la sécurité tout en optimisant les performances et le compromis surface/temps.

2.3 Approches d'intelligence artificielle pour la détection des anomalies dans les systèmes de soins de santé intelligents

Cette section présente les principales contributions portant sur l'utilisation de l'apprentissage automatique et l'apprentissage par renforcement pour la détection d'anomalies dans les systèmes de santé intelligents. Ces approches visent à identifier les comportements suspects ou malveillants afin de préserver l'intégrité des données, authentifier les utilisateurs et contrôler l'accès aux données des patients.

2.3.1 Détection des anomalies basée sur l'apprentissage automatique pour garantir l'intégrité des données dans SSSI

L'apprentissage automatique est de plus en plus utilisé dans les systèmes de santé intelligents afin d'assurer l'intégrité des données en détectant de manière proactive les comportements anormaux ou malveillants. De nombreux travaux ont ainsi exploré diverses approches pour identifier les anomalies dans les flux de données issues de dispositifs médicaux ou d'environnements IoT.

Dans [65], cinq algorithmes d'apprentissage automatique ont été évalués sur le jeu de données MIT-BIH pour la détection d'anomalies du rythme cardiaque. Bien que les résultats aient été prometteurs, l'étude définissait les anomalies comme toute valeur en dehors de la plage fixe de 60 à 100 bpm, ce qui limite son applicabilité dans des contextes réels. Les algorithmes Local Outlier Factor (LOF) et Random Forest ont obtenu les meilleures performances, mettant en avant le potentiel des données simulées pour l'entraînement.

Park *et al.* [66] ont utilisé les GANs pour générer des étiquettes de fraude dans des jeux de données dépourvus de classes, en appliquant la régression logistique et XGBoost pour la classification, avec une analyse SHAP pour identifier les caractéristiques déterminantes. Dans [67], un clustering non supervisé (K-means et K-medoids) a été appliqué à des données de capteurs portables ; K-means a légèrement surpassé K-medoids, bien que les détails sur les jeux de données utilisés soient insuffisants. Le système DIB proposé dans [68] s'appuie sur R-FCVM (une combinaison de la théorie des ensembles flous et des machines à vecteurs cœurs) pour détecter les comportements illégaux dans l'IoT médical, mais sans prendre en compte les anomalies de données.

Alsolami *et al.* [69] ont exploré l'apprentissage par ensemble (Bagging, Boosting, Stacking) pour la détection d'anomalies dans l'IoMT, en s'appuyant sur le jeu de données WUSTL-EHMS-2020 [70], mais la petite taille du jeu et la faible diversité des attaques ont limité la portée de l'évaluation.

Dans le contexte IoT, Ullah *et al.* [71] ont utilisé des réseaux de neurones convolutifs (CNN) pour la détection multi-classes d'anomalies, obtenant de bons résultats sur les jeux de données BoT-IoT et IoT-23. Das *et al*. [72] ont proposé une méthode hybride par ensemble pour détecter les attaques DDoS connues et zero-day, atteignant une précision de 99,1 % sur les jeux NSL-KDD et UNSW-NB15.Gu *et al.* [73] ont introduit un algorithme semi-supervisé basé sur K-means pour la classification DDoS, sans toutefois fournir de mesures de précision. Meidan *et al.* [74] ont développé N-BaIoT, utilisant des autoencodeurs profonds pour des dispositifs IoT ; le modèle est efficace, bien que les résultats chiffrés soient absents. Ravi *et al.* [75] ont proposé une machine d'apprentissage extrême profonde semi-supervisée (SDELM) pour mitiger les attaques DDoS, mais se sont limités aux attaques de type inondation UDP sur le jeu UNB-ISCX. Doshi *et al*. [76] ont développé une pipeline en quatre étapes pour la détection d'anomalies avec des résultats solides, bien que reposant sur des données synthétiques. Maseer *et al.* [77] ont comparé 31 modèles

d'apprentissage automatique, identifiant k-NN, les arbres de décision et Naive Bayes comme les plus performants sur le jeu CICIDS2017.

D'autres travaux ont ciblé des problématiques spécifiques: Choi *et al.* [78] ont comparé des modèles de détection d'anomalies pour des séries temporelles ; Luo *et al.* [79] ont utilisé des autoencodeurs empilés (SAE) pour la détection précoce de pannes dans des machines CNC ; Abdelmoumin et al. [80] ont exploré l'utilisation de l'ACP et des machines à vecteurs de support à classe unique (One-Class SVM) pour le développement d'un IDS évolutif ; Poornima *et al.* [80] ont proposé une approche par régression pour réduire la complexité de calcul dans les réseaux de capteurs sans fil ; Kavitha *et al*. [82] ont comparé la régression logistique et les réseaux de neurones artificiels pour la détection d'anomalies dans l'IoT, l'ANN surpassant la régression sur le jeu DS2OS ; Alsamiri *et al.* [83] ont testé sept algorithmes sur Bot-IoT, améliorant les performances de détection via de nouvelles caractéristiques. Hasan *et al.* [84] ont intégré l'explicabilité (XAI) à des classifieurs ensemblistes pour la détection d'anomalies dans le domaine des cryptomonnaies, en proposant XGBCLUS pour équilibrer les données, qui surpassent les méthodes classiques.

2.3.2 Apprentissage par renforcement pour l'authentification et le contrôle d'accès dans SSSI

L'authentification et le contrôle d'accès représentent deux piliers essentiels dans la protection des dossiers médicaux électroniques, des dispositifs de l'Internet des objets médicaux (IoMT) et des plateformes de santé hébergées dans le cloud. Traditionnellement, les systèmes de santé s'appuient sur le contrôle d'accès basé sur les rôles (RBAC) ou les attributs (ABAC), afin de gérer les droits d'accès en fonction des rôles des utilisateurs ou de certaines caractéristiques spécifiques [85], [86], [87]. Bien que largement déployés et relativement simples à mettre en œuvre, ces modèles présentent une rigidité structurelle. Ils reposent sur des politiques statiques et prédéfinies, qui ne tiennent pas compte des niveaux de risque évolutifs ni des contextes opérationnels en temps réel. Afin de surmonter ces limites, plusieurs travaux ont exploré la décentralisation du contrôle d'accès à travers l'usage de la blockchain et des contrats intelligents. Par exemple, les modèles SmartAccess [88] et Fortified-Chain [89] ont automatisé les décisions d'accès en combinant ABAC et données issues de l'IoMT.

Haritha *et al.* [90] ont introduit des règles de sécurité multiniveaux pour gérer des structures d'utilisateurs hiérarchisées. Ying *et al.* [91] ont proposé un mécanisme de partage de DME basé

sur le chiffrement par attributs dans le cloud, permettant de définir des politiques cryptographiques personnalisées et plus fines. De leur côté, Zhang *et al*. [92] ont développé un système d'accès décentralisé basé sur les attributs et intégré à une blockchain, garantissant l'auditabilité et l'intégrité des journaux d'accès. Nguyen *et al*. [93] ont introduit un modèle de contrat intelligent basé sur la confiance pour le partage de DME dans des environnements de cloud mobile, visant à automatiser le contrôle d'accès tout en protégeant la vie privée des utilisateurs. Xu *et al.* [94] ont conçu un modèle fondé sur les capacités d'accès, activé par la blockchain, pour des scénarios IoT avec un contrôle fin. Enfin, Novo *et al.* [95] ont proposé une architecture blockchain évolutive adaptée aux systèmes IoT critiques, en optimisant les performances et les délais d'accès.

Des contributions complémentaires telles qu'Ancile [96] et MedRec [97] ont introduit des cadres pour le partage sécurisé et décentralisé des données médicales, accordant un contrôle direct aux patients sur leur vie privée. Si les solutions basées sur la blockchain renforcent la sécurité et la décentralisation des données de santé, leurs mécanismes de contrôle d'accès restent fondamentalement rigides. Une fois déployés, les contrats intelligents ne peuvent pas s'adapter dynamiquement à l'évolution des comportements, au contexte ou aux niveaux de risque sans intervention manuelle. De plus, leur coût computationnel et leur latence rendent ces approches peu adaptées aux scénarios critiques de santé en temps réel, notamment en cas d'urgence.

Dans cette optique, plusieurs chercheurs se sont tournés vers des techniques d'apprentissage automatique pour introduire davantage de souplesse dans la gestion des accès et la détection d'anomalies. Sangeetha *et al.* [98] ont ainsi proposé un système d'accès sécurisé intégrant l'apprentissage automatique pour détecter des comportements suspects et renforcer la résilience face aux menaces internes. Des modèles d'authentification basés sur le risque, tels que celui présenté dans [99], utilisent des arbres de décision et des réseaux neuronaux pour évaluer dynamiquement les variables contextuelles et ajuster les niveaux d'exigence lors de l'authentification. L'introduction de l'IA explicable (XAI) dans la sécurité des soins, comme explorée dans [100], contribue également à renforcer la confiance des utilisateurs grâce à une meilleure transparence des décisions. Cependant, les systèmes basés sur l'apprentissage supervisé demeurent souvent réactifs, dépendent fortement de données étiquetées, et manquent d'autonomie dans la prise de décision. Ils sont donc limités dans des environnements complexes ou évolutifs.

Face à ces limites, l'apprentissage par renforcement (RL) émerge comme une alternative prometteuse. Contrairement aux modèles supervisés, les agents RL apprennent à prendre des décisions optimales à travers des interactions directes avec leur environnement, permettant la mise en place de politiques d'accès adaptatives qui évoluent dans le temps. Le modèle RLAuth [101] a ainsi démontré la faisabilité de l'apprentissage profond par renforcement pour l'authentification basée sur le risque, en ajustant dynamiquement la force des politiques selon les indicateurs de risque environnemental. Il a montré de meilleures performances en termes de classification et de réactivité par rapport aux modèles statiques ou heuristiques. Toutefois, RLAuth reste limité à l'authentification, sans intégrer les mécanismes de contrôle d'accès ou de contextualisation des rôles utilisateurs, éléments pourtant essentiels dans les environnements cliniques où la sensibilité des données et l'urgence varient fortement selon les profils et les situations.

CHAPITRE 3 DÉMARCHE DE L'ENSEMBLE DU TRAVAIL DE RECHERCHE

Cette thèse a pour objectif de concevoir une architecture sécurisée visant à préserver la vie privée des utilisateurs et à protéger l'accès ainsi que les échanges de données au sein des systèmes de soins de santé intelligents. Nous avons proposé une architecture à quatre couches, comme le montre la Figure 3.1. Notre travail s'inscrit dans une démarche d'amélioration progressive de la sécurité de cette architecture, en renforçant les mécanismes de protection à chaque niveau.

Afin d'atteindre cet objectif global, nous avons formulé quatre objectifs spécifiques détaillés dans la Section 1.3. Ce chapitre présente la démarche méthodologique adoptée dans l'ensemble de nos travaux de recherche, tout en soulignant la cohérence entre les objectifs poursuivis et la structure des chapitres qui suivent.

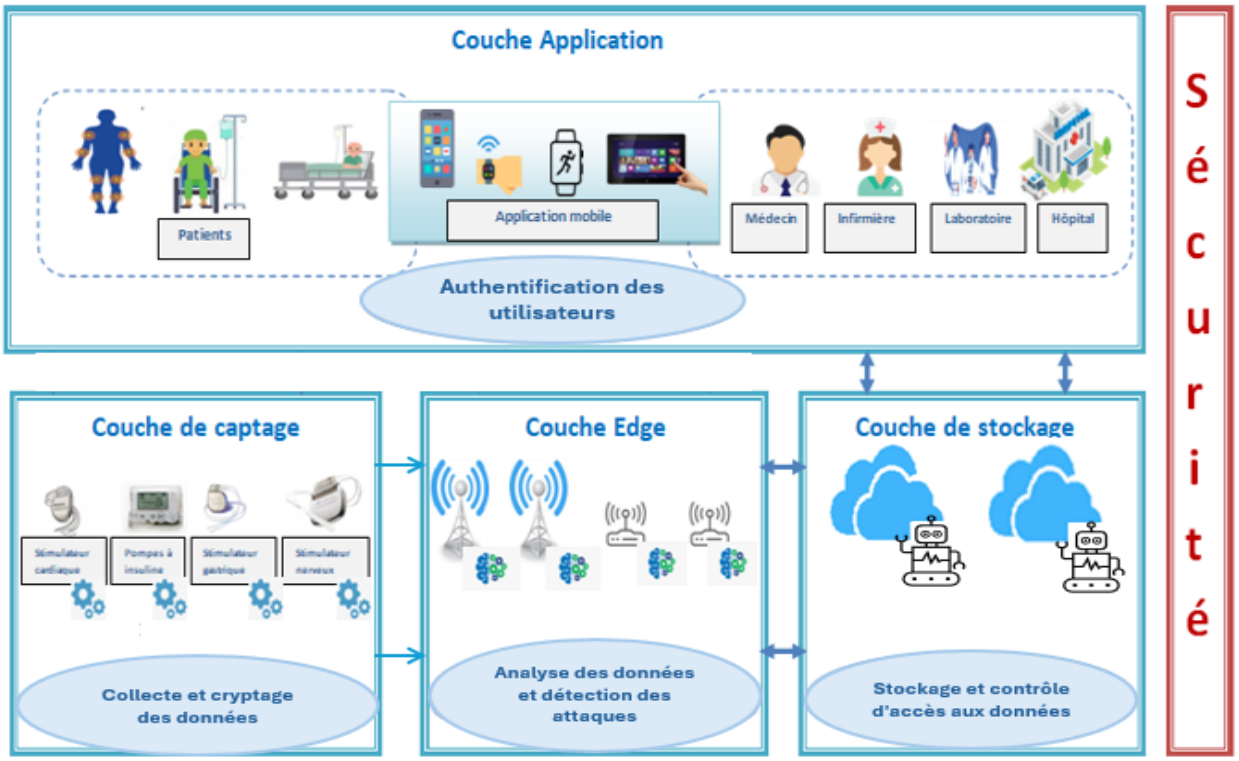


Figure 3.1 Architecture proposée

De manière générale, nos contributions se répartissent en trois volets principaux, chacun ayant donné lieu à un article scientifique. Le premier volet concerne la conception d'un algorithme de chiffrement léger visant à garantir la confidentialité des données dès leur collecte, au niveau de la

couche de captage. Le second volet porte sur la mise en place d'un système de détection des attaques et des anomalies afin d'assurer l'intégrité et la disponibilité des données, en particulier au niveau de la couche « Edge Computing ». Enfin, le troisième volet s'intéresse à la conception d'un mécanisme de détection des anomalies comportementales dans le but de renforcer l'authentification des utilisateurs et le contrôle d'accès aux données sensibles au niveau de la couche application. Dans le cadre de cette architecture, nous faisons l'hypothèse que la couche cloud est sécurisée et ne constitue pas un vecteur direct de menace.

3.1 Volet 1 : Confidentialité des données au niveau de la couche de captage

Le premier volet de cette thèse porte sur la confidentialité des données médicales sensibles dès leur point de collecte, au sein de la couche de captage de l'architecture proposée. Cette couche est composée de dispositifs médicaux connectés (IoMT), et notamment de dispositifs implantables (IMD), qui présentent des contraintes strictes en matière de calcul, d'énergie et de mémoire. L'objectif principal dans ce contexte est donc de concevoir un mécanisme de chiffrement léger, capable de garantir la sécurité des données sans imposer une charge computationnelle excessive sur ces équipements. Dans ce contexte, le premier objectif spécifique de cette thèse consiste à :

Concevoir un algorithme qui ne nécessite pas des calculs complexes au niveau des IMD, afin d'éliminer les problèmes liés à la capacité limitée de ces dispositifs tout en assurant la sécurité des données. Cet objectif a été atteint à travers la première publication scientifique, intitulée : « A Novel Approach to Enhance the Security and Efficiency of Binary Ring-LWE for IoT Resource-Constrained » et présentée au chapitre 4.

3.1.1 Technique cryptographique adoptée

L'approche proposée repose sur une amélioration du schéma BRLWE (Binary Ring Learning With Errors), une variante de la cryptographie post-quantique sur réseaux euclidiens. Ce schéma est reconnu pour sa résistance aux attaques quantiques ainsi que pour ses exigences faibles en ressources, ce qui le rend particulièrement adapté aux dispositifs IoMT.

Cependant, malgré ses avantages, le BRLWE classique reste vulnérable aux attaques physiques, notamment les attaques par canaux auxiliaires (i.e., Side-Channel Attacks et SCA), et présente encore un coût de calcul non négligeable pour les IMD.

Pour surmonter ces limitations, nous avons proposé une nouvelle stratégie de multiplication polynomiale optimisée basée sur la multiplication de Karatsuba en trois décompositions « 3-Decomposition Karatsuba » et un mécanisme de permutation aléatoire « Radom Shuffling » des opérations internes, afin de perturber les fuites d'information exploitables par les attaquants.

Cette technique permet de réduire significativement le temps de chiffrement et de déchiffrement, tout en renforçant la sécurité contre les attaques physiques et hybrides (classiques + quantiques).

3.1.2 Évaluation de la sécurité

La sécurité de l'approche proposée a été évaluée selon deux axes :

- La résistance aux attaques hybrides combinant des techniques classiques et quantiques.
- La résilience face aux SCAs, en s'appuyant sur des tests d'analyse de consommation de temps et d'énergie et de détection de fuites.

Les résultats montrent que la méthode de randomisation couplée au Karatsuba 3-Decomposition augmente la complexité pour un attaquant souhaitant extraire des informations à partir des traces physiques. De plus, les évaluations face aux attaques de type Ring-LWE Breaker confirment que notre schéma conserve un niveau de sécurité post-quantique équivalent voire supérieur aux versions améliorées du BRLWE existantes.

3.1.3 Évaluation des performances

L'évaluation des performances de l'algorithme proposé vise à démontrer sa faisabilité dans un environnement contraint, tel que celui des dispositifs médicaux implantables (IMD), où les ressources en calcul, en énergie et en mémoire sont particulièrement limitées. Pour cela, nous avons défini trois facteurs d'évaluation principaux :

- Le coût de calcul, mesuré en millisecondes, correspond au temps nécessaire pour exécuter les différentes opérations de chiffrement et de déchiffrement. Cette métrique permet d'évaluer la capacité de l'IMD à exécuter l'algorithme dans un délai compatible avec son fonctionnement temps réel.

- Le coût mémoire, exprimé en octets, désigne la quantité de mémoire requise pour stocker les éléments nécessaires au fonctionnement du schéma, tels que les clés, les polynômes intermédiaires

ou les paramètres cryptographiques. Cette mesure permet d'estimer la compatibilité de l'algorithme avec les capacités mémoires limités des dispositifs ciblés.

- La consommation énergétique, qui reflète la quantité d'énergie consommée lors de l'exécution des opérations cryptographiques. Cette métrique est essentielle dans le contexte des IMD, où la longévité de la batterie est un critère critique de déploiement.

L'ensemble de ces indicateurs permet de juger de l'efficacité de l'algorithme proposé sur le plan computationnel, tout en respectant les contraintes matérielles propres aux environnements médicaux embarqués.

3.2 Volet 2 : Intégrité et disponibilité des données au niveau de la couche Edge

Le second volet de la thèse concerne la conception d'un système de détection des attaques et des anomalies visant à assurer l'intégrité et la disponibilité des données dans les systèmes de soins de santé intelligents, notamment au niveau de la couche Edge de notre architecture. Cette démarche s'inscrit dans notre objectif de recherche 2, qui consiste à proposer un algorithme de sécurité capable de prédire les attaques et de détecter les vulnérabilités, en tenant compte des spécificités de l'environnement IoMT. Le travail réalisé dans ce cadre a donné lieu à la rédaction de l'article intitulé « Real-Time Anomaly Detection in IoMT Networks Using Stacking Model and a Healthcare-Specific Dataset », présenté dans le chapitre 5.

3.2.1 Approche proposée

Pour répondre aux besoins d'une détection rapide et fiable des cybermenaces affectant les dispositifs médicaux connectés, nous avons conçu un modèle d'apprentissage automatique en temps réel reposant sur une approche d'ensemble stacking. Cette approche combine la force de trois algorithmes supervisés : Random Forest, Artificial Neural Network (ANN), et XGBoost, ce dernier jouant le rôle de méta-apprenant. Ce choix permet de bénéficier à la fois de la robustesse des forêts aléatoires, de la capacité d'apprentissage non linéaire des réseaux de neurones, et de la puissance prédictive du gradient boosting. Le modèle proposé vise à détecter différentes catégories d'attaques affectant l'intégrité ou la disponibilité des données transmises, telles que les attaques de falsification et de type déni de service (DoS), tout en maintenant une faible latence afin de répondre aux contraintes des environnements médicaux temps réel.

3.2.2 Ensemble de données

Afin d'évaluer efficacement notre système, nous avons conçu un nouvel ensemble de données médicales pour la détection d'anomalies, inspiré de la structure du jeu de données UNSW-NB15, tout en l'enrichissant par des scénarios réalistes propres au domaine médical. Ce jeu de données comprend 253 680 enregistrements, dont 60 % de données anormales, réparties entre différentes catégories d'attaques spécifiques à l'IoMT. Contrairement à de nombreux travaux antérieurs qui s'appuient sur des jeux de données peu contextualisés ou artificiels, notre jeu de données reflète des menaces pertinentes, comme la modification des signaux vitaux ou l'interruption des transmissions critiques. L'objectif est de fournir un cadre de test plus exigeant et plus fidèle aux réalités du terrain médical connecté.

3.2.3 Évaluation des performances

L'évaluation du système de détection proposé a été menée en deux phases complémentaires : une phase de pré-entraînement visant à comparer la performance de plusieurs algorithmes sur des données historiques, et une phase de prédiction en temps réel, destinée à tester la robustesse et la réactivité du modèle dans un contexte dynamique et continu.

- Phase 1 : Évaluation en pré-entraînement

Lors de cette phase, nous avons comparé les performances de sept algorithmes d'apprentissage automatique : « Random Forest » (RF), XGBoost, k-Nearest Neighbors (KNN), Support Vector Machine (SVM), Logistic Regression (LR), Artificial Neural Network (ANN) et Isolation Forest (ISOF). Ces algorithmes ont été évalués à la fois sur le jeu de données UNSW-NB15 et sur notre nouveau jeu de données médical enrichi, afin de mesurer à la fois l'efficacité du modèle et la pertinence du jeu de données proposé dans un contexte IoMT.

Pour chaque modèle, nous avons mesuré les indicateurs de performance suivants :

- Exactitude « Accuracy » : la proportion d'échantillons correctement classifiés parmi l'ensemble des prédictions. Elle donne une vue d'ensemble de la qualité du modèle mais peut être trompeuse en cas de classes déséquilibrées.
- Précision « Precision » : le rapport entre le nombre de vraies détections positives et l'ensemble des prédictions positives. Elle mesure la fiabilité des alertes émises.

- Rappel « Recall » : la capacité du modèle à détecter effectivement les anomalies (i.e., vrais positifs sur l'ensemble des anomalies). C'est une métrique clé dans les systèmes de sécurité pour minimiser les attaques non détectées.
- Le score F1 « F1-score » : la moyenne harmonique entre la précision et le rappel, utile pour évaluer les performances dans un contexte de classes déséquilibrées.
- Taux de faux positifs « False Positive Rate » (FPR) : le taux de faux positifs, c'est-à-dire la proportion de données normales incorrectement détectées comme anormales. Un faible FPR est essentiel pour éviter les alertes inutiles dans les systèmes médicaux.
- Courbe ROC « Receiver Operating Characteristic » : utilisées pour comparer la capacité discriminante des modèles à différents seuils de classification.

En plus des performances de classification, nous avons mesuré deux indicateurs importants pour l'efficacité opérationnelle du système :

- Temps d'entraînement « Training Time » : durée nécessaire à chaque algorithme pour apprendre sur les jeux de données, mesurant la scalabilité du modèle.
- Temps de test « Testing Time » : durée nécessaire à chaque modèle pour faire des prédictions sur de nouveaux échantillons, indicateur critique pour l'intégration en temps réel.

- Phase 2 : Prédiction en temps réel

Afin de valider l'efficacité du modèle dans des conditions proches du déploiement réel, nous avons ensuite conduit une série d'expérimentations en temps réel. Dans ce scénario, le modèle reçoit 100 messages successifs, simulant des transmissions issues d'appareils médicaux connectés. Chaque message était classifié de manière binaire (i.e., normal ou anormal), permettant d'évaluer la réactivité immédiate du système face à des flux continus de données.

En complément, nous avons effectué une classification multi-classes pour identifier précisément le type d'attaque détectée, et pas seulement sa présence. Nous avons ainsi mesuré pour chaque modèle le nombre d'attaques correctement prédites par type, ce qui permet de tester la granularité et la précision contextuelle du modèle dans des environnements complexes.

Cette double évaluation, binaire et multiclasses, démontre la capacité du système à non seulement signaler les anomalies en temps réel, mais également à fournir des informations précises sur la nature des menaces, ce qui est essentiel pour un traitement efficace dans les architectures de soins de santé intelligents.

3.3 Volet 3 : Authentification et contrôle d'accès au niveau de la couche Application

Dans les systèmes de soins de santé intelligents, l'accès aux données sensibles des patients nécessite des mécanismes de sécurité à la fois robustes et dynamiques. La couche Application de notre architecture est particulièrement critique, car elle constitue le point de jonction entre les utilisateurs (e.g., professionnels de santé, administrateurs, etc.) et les données cliniques. Garantir une authentification fiable et un contrôle d'accès contextuel est essentiel pour prévenir les intrusions, les abus internes ou les violations de confidentialité.

C'est dans cette optique que s'inscrit notre troisième objectif de recherche, qui vise à concevoir un modèle d'authentification et de contrôle d'accès adaptatif afin d'assurer la protection des données privées des patients dans un environnement de soins de santé intelligent. Cet objectif a donné lieu à la rédaction de l'article intitulé : « Reinforcement Learning Framework for Adaptive Authentication and Access Control in Healthcare Systems » présenté dans le Chapitre 6.

3.3.1 Approche proposée

Nous proposons une architecture duale basée sur l'apprentissage par renforcement « Reinforcement Learning » (RL) composée de deux agents intelligents :

- Agent d'authentification adaptative : il ajuste dynamiquement les décisions d'accès en analysant les variables comportementales et contextuelles (e.g., heure, périphérique, niveau de risque, etc.). Il repose sur une logique d'authentification basée sur le risque « Risk-Based Authentication ».

- Agent de contrôle d'accès comportemental : il surveille en continu les activités des utilisateurs déjà authentifiés, détecte les comportements anormaux (i.e., changement soudain d'usage et accès inhabituel) et adapte les politiques d'accès en conséquence.

Contrairement aux modèles classiques (i.e., RBAC et ABAC) [85], [86], [87], cette approche permet de s'adapter aux évolutions contextuelles en temps réel, en prenant en compte à la fois le comportement passé, le profil métier, et la dynamique de l'environnement médical.

3.3.2 Ensemble de données

Afin de simuler un environnement médical réaliste, nous avons adapté le jeu de données « CERT Insider Threat », initialement conçu pour analyser les menaces internes en entreprise.

Pour le module d'authentification, nous avons extrait et sélectionné les caractéristiques liées au comportement identitaire (e.g., moment de connexion, rôle, type d'accès sollicité, fréquence d'utilisation d'applications critiques, etc.). Ces variables permettent de modéliser un profil d'accès pour chaque rôle médical (e.g., médecin, infirmier, technicien, etc.).

Pour le module de contrôle d'accès, nous avons extrait des comportements post-authentification : changement de fréquence d'envoi de courriels, navigation web excessive, ouverture de pièces jointes inhabituelles et d'autres. Ces actions sont ensuite croisées avec les règles de politique d'accès afin de détecter les comportements anormaux ou les abus potentiels.

Cette adaptation du set de données nous a permis de simuler des interactions réalistes dans un système de santé, tout en exploitant des données comportementales crédibles et hétérogènes.

3.3.3 Évaluation des performances

L'évaluation de notre approche a été structurée autour de deux scénarios distincts mais complémentaires, correspondant aux deux volets fonctionnels du système proposé :

- l'authentification adaptative des utilisateurs;
- le contrôle d'accès comportemental aux données sensibles.

Dans ces deux scénarios, les performances des agents d'apprentissage par renforcement ont été analysées à l'aide d'un ensemble cohérent et commun de métriques, ce qui permet une comparaison uniforme et une meilleure évaluation de la robustesse du modèle global. Ces métriques couvrent à la fois la précision, la capacité à détecter les comportements anormaux, l'équilibre entre les classes, ainsi que l'efficacité temporelle et la stabilité des politiques apprises. Les détails de cette évaluation sont présentés dans les paragraphes suivants.

Dans chaque scénario, nous avons testé cinq modèles d'apprentissage par renforcement [101] : DS « Deterministic Strategy » (on-policy), DES « Deterministic Exploration Strategy » (on-policy et off-policy), DQN « Deep Q-Network » et DDQN « Double DQN » selon les métriques suivantes :

- Exactitude « Accuracy » : pourcentage d'actions correctement classées (autorisation/refus).
- Rappel « Recall » (ALLOW / DENY) : taux de détection des cas positifs (ALLOW) et négatifs (DENY), afin d'équilibrer les erreurs de type I et II.
- Moyenne géométrique « G-Mean » : moyenne géométrique entre les deux rappels, utilisée pour mieux refléter la robustesse du modèle face à des classes déséquilibrées.
- Temps d'apprentissage et de test « Training & Testing Time » : mesure des temps d'apprentissage et d'inférence, essentiels pour juger de la faisabilité dans un contexte de soins en temps réel.
- Courbe de récompense lissée « Smoothed Reward Curve » (200 épisodes) : permet de suivre la stabilité et la convergence des politiques apprises par les agents.
- Récompense cumulée « Accumulated Reward » : évalue la performance du modèle en phase de déploiement sur des données temps réel simulées.
- Comparaison avec les modèles ML classiques
  Pour renforcer l'analyse, nous avons également comparé les performances du modèle DQN, qui a obtenu les meilleurs résultats parmi les algorithmes RL testés, avec cinq modèles d'apprentissage automatique classiques (i.e., XGBoost, Random Forest, SVM, ANN et KNN).

Cette comparaison a été réalisée sur les deux scénarios : l'authentification et le contrôle d'accès, en mesurant l'exactitude et la moyenne géométrique. Cette comparaison vise à confirmer que le RL n'est pas seulement adapté à l'exploration adaptative, mais qu'il surpasse aussi des modèles supervisés bien établis.

CHAPITRE 4 ARTICLE 1: A NOVEL APPROACH TO ENHANCE THE SECURITY AND EFFICIENCY OF BINARY RING-LWE FOR IOT RESOURCE-CONSTRAINED

Hadjer Goumidi and Samuel Pierre (Senior Member, IEEE)

Department of Computer and Software Engineering, Polytechnique Montréal, Montreal, QC H3T 1J4, Canada

E-mail: hadjer.goumidi@polymtl.ca; samuel.pierre@polymtl.ca;

Revue : Accepté et publié dans le journal *Computer Networks and Communications*, volume *3, numéro* 1, pages 19–42, 19 décembre 2024.

Abstract

The rapid expansion of the Internet of Things (IoT) brings a vast proliferation of network connections. This surge in connectivity significantly increases the risk of private data exposure during transmission and processing. Traditional public key encryption schemes face considerable challenges due to their high computational complexity and vulnerability to quantum attacks. Recently, Lattice-based cryptography, particularly the Binary Ring Learning With Errors (BRLWE) paradigm, has garnered significant attention for its quantum resistance and lightweight computational requirements. However, BRLWE remains vulnerable to physical attacks, especially Side-Channel Attacks (SCA). This paper proposes a novel 3-Decomposition Karatsuba multiplication-based random shuffling scheme to enhance both the efficiency and security of BRLWE. We evaluate the security performance of our proposed scheme against quantum hybrid attacks and SCAs. We assess the performances of different Karatsuba multiplication techniques in terms of computation cost, energy consumption and memory usage to make choose which Karatsuba technique is suitable for our proposal. Our experimental results show that our proposed approach provides the lowest encryption computation time of 18.97 ms and decryption computation time of 9.53 ms compared to the BRLWE and its improved versions. Furthermore, it improves the

security level while it decreases the computation time of the original BRLWE by 32.49% and 20.58%, for the encryption and decryption phases, respectively.

Keywords: Internet of things security, post-quantum cryptography, lattice-based cryptography, binary ring learning with errors, shuffling and karatsuba multiplication.

4.1 Introduction

The Internet of Things (IoT) is a well-established area of study that connects the physical world to the Internet through existing network infrastructures. This technology enables smart devices, such as physical devices, vehicles, household appliances, and more, to autonomously collect and share data via the Internet. The 'Cluster of European Research Projects on the Internet of Things' (CERP-IoT) program [102] defines IoT as a dynamic infrastructure within a global network, characterized by self-configuring capabilities based on standardized and interoperable communication protocols. Physical and virtual objects within this network possess unique identities, physical attributes, virtual personalities, and intelligent interfaces, facilitating seamless integration into the network.

The emergence of the IoT concept has led to the development of various applications, such as smart cities, smart industries, smart transportation, smart energy, etc. These applications exhibit specific characteristics, generating vast volumes of data while requiring sustained connectivity and energy for extended periods. However, they face challenges related to memory limitations, device capacity, network constraints, and power consumption. Ensuring the security and privacy of the transmitted data within the IoT network is a primordial task. Besides, a robust security measure must take into consideration the limitations of the IoT devices in terms of memory, device capacity and power consumption.

To ensure the secure communication of critical and private data between IoT nodes, it is crucial to implement appropriate encryption primitives. However, conventional encryption schemes like AES [47], RSA [48], and ECC [49] typically involve complex mathematical operations and require significant memory, making them unsuitable for resource-constrained IoT devices. Moreover, classical public key encryption schemes relying on mathematical problems like large integer factorization and discrete logarithms are vulnerable to polynomial-time methods through Shor's quantum algorithms [50], [51]. Simply increasing the key size of existing classical public key encryption schemes will not enhance security against available quantum computers. Unfortunately, the rapid advancement of quantum computing puts at risk the security of these classic encryption

schemes, leading to substantial resource overhead. Therefore, there is a pressing need for quantum-resistant and lightweight alternatives to address these challenges effectively. This need has prompted several researchers and organizations to initiate the standardization process of post-quantum cryptography. Fig. 4.1 depicts a taxonomy of different post-quantum cryptography algorithms suggested by different researchers [57, 103].

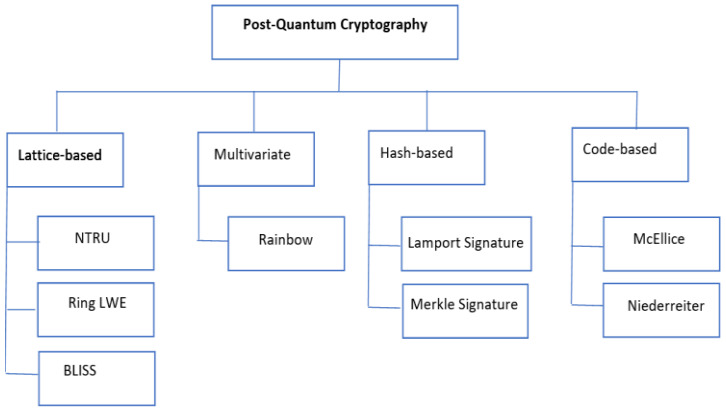


Figure 4.1 Taxonomy of different post-quantum cryptography algorithms.

Among current post-quantum cryptosystems, lattice-based cryptography, particularly the Learning With Errors (LWE) problem [51] and its variants, such as ring learning with error (Ring-LWE) [57] and BRLWE [103], have gained significant attention of researchers. Lattice-based cryptography demonstrates superior efficiency and faster execution times compared to other cryptographic approaches, and unlike code-based cryptography, it does not suffer from large key sizes. Moreover, it provides a robust resistance against attacks leveraging quantum computers, which makes lattice-based public key encryption an ideal choice for resource-constrained IoT nodes [57], [104], [105], [106]. Especially the BRLWE, researchers in [103] and [60] proved that the BRLWE is practical for ultralightweight and resource-constrained IoT devices.

Over the last decade, IoT devices have encountered a range of SCA, including timing [107], fault injection attacks [108], [63], Simple Power Analysis (SPA), and Differential Power Analysis (DPA) attacks [105], [60], [109], [110].

Side-channel analysis of BRLWE differs from RLWE because parts of the secret key (i.e., coefficients of the secret-key polynomial) in BRLWE are drawn from a binary distribution, resulting in only two possible values: '0' or '1'. On the other hand, RLWE keys are sampled from a

larger set with a Gaussian distribution. Therefore, the evaluation of side-channel analysis for BRLWE is very important since unprotected proposals could be vulnerable to SCA.

Several efforts have been made in the literature to enhance the security of BRLWE against SCA. However, many of these approaches focus only on introducing complex computations to reinforce the algorithm's resilience, often without considering methods to minimize unnecessary computations. In this paper, we present an advanced version of BRLWE that establishes a delicate balance between efficiency and security against timing, SPA and DPA side-channel attacks, while optimizing the overall computation cost. Our approach aims to achieve a more robust and practical approach, addressing the crucial challenge of mitigating side-channel vulnerabilities while maintaining the algorithm's performance. We propose a new random shuffling method designed to enhance the security of the BRLWE algorithm against SCA, specifically against timing SPA and DPA. Moreover, we intend to optimize the polynomial multiplication using the 3-Decomposition Karatsuba multiplication [111], in order to minimize the computation cost. To the best of our knowledge, this combination of the random shuffling method with the 3-Decomposition Karatsuba multiplication, which aims to make a balance between security and efficiency, did not exist in the literature before. We formally prove the security of our approach against quantum hybrid attacks, timing, SPA and DPA attacks. In terms of efficiency, we have evaluated the computation cost, the memory usage and the energy consumption of the proposed approach using a resource-constrained microcontroller, 32-b ARM Cortex-M0. This microcontroller has limited computation resources to prove that our approach can be practical and scalable to even tiny and low-power IoT devices.

The main contributions of this paper are as follows:

1) Enhance the security level of BRLWE using a random shuffling method, which provides timing, SPA and DPA-resistant. Moreover, we provide security analysis against the mentioned attacks and quantum hybrid attacks.
2) Propose a lightweight approach 3DKSh-BRLWE with an optimized polynomial multiplication suitable for resource-constrained IoT nodes, which provides a lower computation time than the original BRLWE.
3) Prove that 3DKSh-BRLWE dominates related works in terms of speed and efficiency on ARM Cortex M0 microcontroller.

The originality of this paper is based on the random shuffling method that is used on the 3-Decomposition Karatsuba multiplication's sub-polynomials to enhance the BRLWE security and efficiency.

The remainder of this paper is organized as follows. In Section II, we detail the technical background. In Section III, we present an overview of the existing methods to resist timing, SPA and DPA attacks, as well as to improve the lattice-based security and efficiency. We describe the proposed approach in Section IV. In Section V, we discuss the security analysis of the proposed approach. We analyze the complexity between the original BRLWE and our proposed 3DKSh-BRLWE approach in Section VI. In Section VII, we detail the implementation and discuss the results. Finally, we conclude the paper in Section VIII.

4.2 Background

In this section, we present the BRLWE encryption algorithm with uSVP problem that will be used in the security analysis section to evaluate the security level of the proposed approach. Next, we describe the Karatsuba multiplication algorithm. Finally, a notation table summarizing the key symbols and terms used in the paper is provided in Table 1.

4.2.1 Binary Ring Learning With Errors (BRLWE)

The Binary Ring-LWE (BRLWE) is a relatively new variant of the Ring-LWE scheme. It was recently introduced in [103] with rigorous security analysis. The BRLWE scheme uses binary errors instead of Gaussian distributed errors used in the original LWE scheme to reduce the key size and corresponding area complexity. It has great potential for standardization in the future for lightweight applications, despite not being a NIST candidate yet [112]. The BRLWE involves mainly operations over the ring $\mathbb{Z}q\ /f\ (x)$, where $f(x)=x^n+1$, and a polynomial of degree $n-1$ with integer coefficients modulo q is considered one typical element in the ring. The scheme can be secured with equivalent class and quantum securities of 190/140 and 84/73 bits, respectively, for n = 512 and n = 256 [103], [57]. It is based on the hardness of the Ring-LWE problem, which involves finding the secret key given a set of noisy polynomial equations. The security of the scheme relies on the assumption that the underlying problem is hard to solve, even with the use of quantum computers. The BRLWE-based post-quantum cryptography has three main phases [103], as shown in Fig. 4.2. The scheme in Fig. 4.2 represents a use case of BRLWE in IoT applications, where

devices encrypt the collected data and transmit it to the edge or cloud for data analysis or storage after the decryption process.

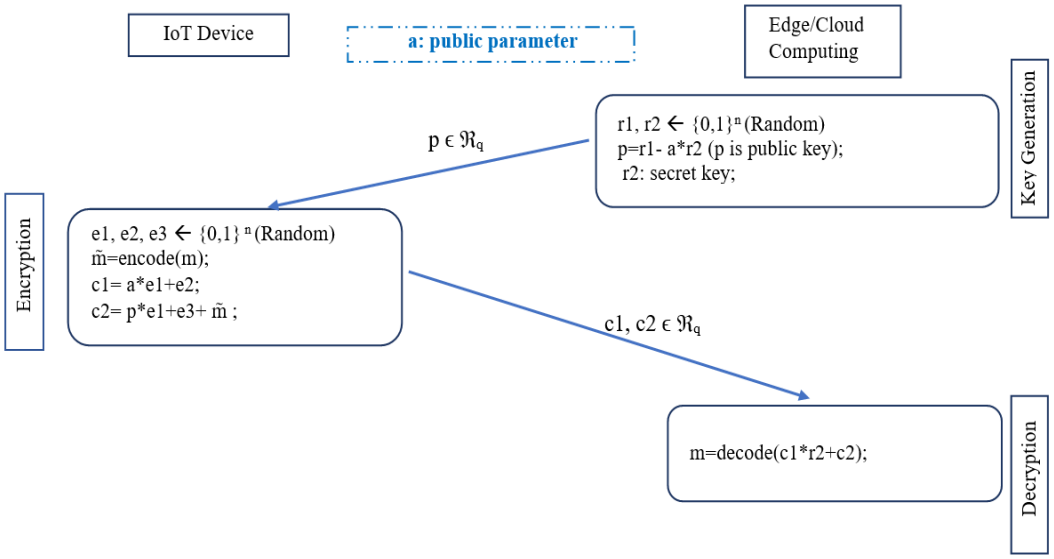


Figure 4.2 BRLWE phases.

For hardware implementation, as suggested by the authors in [105], coefficients of the polynomials within the ring are adjusted to lie within an inverted range compared to the original. Here, each coefficient is represented in the interval (−q/2, q/2−1), which aligns with the range used in the two's complement representation. This approach allows modular additions and subtractions of coefficients to occur seamlessly, eliminating the need for further reductions. Moreover, we proceed to the LWE problem, the lattice framework, the unique Shortest Vector Problem (uSVP), and the Bounded Distance Decoding problem (BDD). These foundations are essential as we need to convert the LWE problem to the uSVP problem [64] and then evaluate the security level as described in Section V. Consider positive integers *m, n,* and *q*, where A ∈ $\mathbb{Z}_q^{mxn}$ represents randomly and uniformly a selected matrix. We denote $e \in \mathbb{Z}_q^m$ as the error vector, drawn from a specific probability distribution, and $s \in \mathbb{Z}_q^n$ as the secret vector. The crux of the LWE problem is to deduce the secret vector *s* from the given samples (l,A), where $l = As + e$.

Furthermore, we define the lattice structure and the lattice basis L, which serve as a discrete subset of $\mathbb{R}^m$. A set of vectors constitutes a lattice ℓ if it adheres to the expression:

$$\ell(L) = \{x \in \mathbb{R}^m \mid x = \sum_{i=1}^{m} \alpha_i \, l_i, \ \alpha_i \in \mathbb{Z}\}, \qquad (1)$$

where *x* represents any point in the lattice defined by L; *m* is the dimension of the lattice, indicating the number of linearly independent vectors; and $\alpha_i \in \mathbb{Z}$ are integer coefficients used in the linear combination of the basis vectors l_i. For a linearly independent vector ensemble $L = \{l_1, \ldots, l_m\} \subset \mathbb{R}^m$, such a collection is termed the basis of the lattice ℓ. It is important to note that lattice bases are not unique, encompassing numerous permutations. To assess the quality of Lattice basis L, we use the Hermitian delta δ, with $||l_1|| = \delta^m \det(\ell)^{1/m}$.

The uSVP challenge involves finding the shortest nonzero vector *t* in a lattice, which is distinctly shorter than any other vectors that are not integer multiples of *t*. In contrast, the BDD problem uses a lattice basis L, a distance threshold α, and a target vector *t*. The goal in BDD is to identify a vector *e* such that $||e|| < \alpha\lambda$ and the difference *t* - *e* lies within the lattice ℓ.

4.2.2 Karatsuba Multiplication in BRLWE

Karatsuba multiplication is a fast algorithm for multiplying two large polynomials, it works by recursively splitting each polynomial into half-size polynomials until the base case of single-digit multiplication is reached. Then, it combines the partial products to obtain the final product. It improves the computational complexity of schoolbook multiplication by reducing the number of elementary operations from $O(n^2)$ to about $O(n^{1.585})$, where n is the number of digits of the operands. It can help optimize memory usage by computing partial products and combining them as needed. This can be advantageous when dealing with limited memory resources or when performing polynomial multiplication on devices with memory constraints [111], [113].

The conventional Schoolbook Polynomial Multiplication Algorithm (SPMA) for two polynomials of length *n* requires n^2 coefficient products. However, the Karatsuba algorithm can be adapted to polynomial multiplication to reduce the number of coefficient multiplications at the cost of more coefficient additions. This adjustment involves the decomposition of A(x) and B(x) into two distinct components, which are designated by:

$$A(x) = A_1(x) * X^{n/2} + A_0(x) \quad (2)$$

$$B(x) = B_1(x) * X^{n/2} + B_0(x), \quad (3)$$

where A(x) and B(x) are the original polynomials we aim to multiply; X represents the polynomial variable and acts as the placeholder for terms raised to powers of X; n is the length (or degree) of

the polynomials; $A_0(x)$ and $B_0(x)$ are the low-order n/2 coefficients of A(x) and B(x); and $A_1(x)$ and $B_1(x)$ are the high-order n/2 coefficients, which are denoted by:

$$A_0(x) = \sum_{i=0}^{n/2-1} a_i X^i, \quad A_1(x) = \sum_{i=0}^{n/2-1} a_{i+n/2} X^i. \qquad (4)$$

$$B_0(x) = \sum_{i=0}^{n/2-1} b_i X^i, \quad B_1(x) = \sum_{i=0}^{n/2-1} b_{i+n/2} X^i \qquad (5)$$

The Karatsuba formula enables computing P(x) and is denoted by:

$$P(x) = x^n * P_2(x) + x^{n/2} * (P_1(x) - P_0(x) - P_2(x)) + P_0(x), \qquad (6)$$

where *P(x)* represents the resulting polynomial product of A(x) and B(x); $P_0(x)$, $P_1(x)$ and $P_2(x)$ are intermediate polynomial products computed as follows:

$$P_0(x) = A_0(x) * B_0(x) \qquad (7)$$

$$P_1(x) = (A_0(x) + A_1(x)) * (B_0(x) + B_1(x)) \qquad (8)$$

$$P_2(x) = A_1(x) * B_1(x) \qquad (9)$$

For conciseness, '(*x*)' is omitted from the notations if no ambiguity occurs. In (112), (103), we can see that only three polynomial multiplications of length *n*/2 are required. Consequently, these formulas reduce the number of coefficient multiplications from n^2 to $3(n/2)^2 = 3n^2/4$.

4.3 Related Work

In this section, we review the existing lattice-based methods to improve the security and efficiency.

One of the challenges provided by the development of quantum computing is its potential threat to classical public-key encryption schemes. To address this issue, NIST initiated a project to standardize post-quantum cryptography (PQC) algorithms [114]. Out of the many candidates submitted, only four public key encryption and key establishment algorithms have been chosen for the final round: Classic McEliece [115], CRYSTALSKyber [116], NTRU [117], and SABER [118]. These three algorithms are based on hard problems on lattices, such as the closest vector problem (CVP) [119], the shortest vector problem (SVP) [120], and learning with errors (LWE) [57]. Another five algorithms, namely BIKE [121], FrodoKEM [122], HQC, NTRU Prime and SIKE [123], are still under consideration as alternatives.

Table 4.1 Notations Table

Notation	Description
$\mathbb{Z}q$	Ring of integers modulo q.
f(x)	Polynomial defining the ring.
$A \in \mathbb{Z}_q^{mxn}$	Randomly and uniformly selected matrix in the LWE problem.
s	Secret vector.
e	Error vector.
l	Samples in the LWE problem, combining the matrix, secret vector, and error.
ℓ(L)	Lattice defined by basis L.
$\boldsymbol{\alpha_i}$	Integer coefficients used in the linear combination of basis vectors in the lattice.
δ	Hermitian delta, used to assess the quality of a lattice basis.
$\boldsymbol{\rho}$	Success probability of the quantum hybrid attack.
p	Public key.
r_2	Private key.
r_1	Intermediate random polynomial.
Sh( )	Random shuffling function.
c_1, c_2	Ciphertext components.
m	Message to be encrypted.
T_{mul}	Timing complexity of classical polynomial multiplication.
T_{sub}	Timing complexity of polynomial subtraction.
T_{add}	Timing complexity of polynomial addition.
T_{kmul}	Timing complexity of Karatsuba polynomial multiplication.
T_{Sh}	Timing complexity of the shuffling method.

Lattice-based encryption schemes rely on the hardness of lattice problems, which are believed to be resistant to quantum attacks. Several related works used Lattice cryptography to improve the existing security algorithms to resist quantum attacks. In [52], a new scheme for Ciphertext-Policy Attribute-Based Encryption (CP-ABE) based on the Lattice problem is proposed, in which the authors combined the known CP-ABE algorithm with the Lattice cryptography to resist quantum attacks. The main advantage of this scheme is that it reduces the computation and communication overhead of existing lattice-based CP-ABE schemes, it uses a Linear Secret Sharing Scheme (LSSS) to represent monotone access policies and applies a private key randomization technique to ensure resistance against collision attacks. A variant of pre-quantum RSA called a post-quantum lattice-based RSA (LB-RSA) is proposed in [53] to secure the shared data and information for IoT-

based cloud applications. It improves the security level by increasing key dimensions instead of increasing key size. On the other hand, several related works have been proposed to improve Lattice encryption in terms of security and efficiency. In [54] and [55] authors improve the complexity and the computation cost of a post-quantum lattice-based SABER algorithm using Number Theoretic Transform (NTT) polynomial multiplication. In [56], a new hardware architecture is proposed to improve the computation cost of post-quantum lattice-based SABER algorithm based on an efficient Karatsuba multiplication algorithm. On the other hand, Lyubashevsky *et al.* [57] introduced a new variant of the Learning With Errors (LWE) problem that applies the ideal lattices in the LWE, this variant is called ring-LWE. The polynomial ring is used for all operations, and the error polynomials are sampled from a discrete Gaussian distribution. Ring-LWE reduces the public key and the private key size by n times while keeping the same security level as standard LWE instances. The ring-LWE has been used for key exchange, homomorphic encryption, digital signature, public key encryption, etc. However, it faces challenges in efficient deployment due to the complexity of its Gaussian sampler and the high cost of polynomial multiplication in terms of time and resources [124]. A shuffling method is proposed in [58] to avoid the expensive constant-time Gaussian sampler. Many hardware and software implementations in the literature aim to optimize these aspects of polynomial multiplication. Howe *et al.* [59] presented a comprehensive evaluation of different methods for sampling from a discrete Gaussian distribution. They proposed novel optimized hardware architectures for several sampling techniques, such as the Cumulative Distribution Table (CDT), the Bernoulli, the Knuth-Yao and the discrete Ziggurat samplers. Moreover, the authors presented the first constant-time hardware designs for some of these samplers, which offer protection against timing analysis. They concluded that the CDT sampler is the most suitable for a balanced performance, achieving a high throughput and a low area consumption for both encryption and signature applications. Another work that tries to improve the Ring LWE is the Binary Ring LWE (BRLWE) [103]. The authors proposed a new public-key encryption scheme using the binary noise distribution instead of the Gaussian one, which reduces the size of the ciphertexts and the computational cost of encryption and decryption. It presents efficient implementations of the scheme on 8-bit and 32-bit microcontrollers, which are suitable for low-power and low-cost scenarios such as the IoT.

Based on BRLWE, Aydin *et al.* [60] proposed a hardware implementation of BRLWE along with low-cost power side-channel countermeasures, they use a randomization of intermediate states and

masked threshold decoding to improve the security against DPA. Another hardware implementation of BRLWE is presented in [61], it is based on masking countermeasures against differential power analysis (DPA) attacks without employing any pseudo-random number generator (PRNG) module on lightweight implementations, which improves the speed and efficiency. In [62], authors proposed an efficient hardware architecture for the BRLWE-based cryptographic scheme, targeting lightweight applications. The architecture computes the arithmetic operation $AB + C$, which includes polynomial multiplication and addition over the polynomial ring. It reduces resource utilization, increases frequency, and lowers power consumption compared to existing BRLWE-based schemes. Ebrahimi *et al.* [63] proposed fault-resilient implementations of BRLWE for IoT Devices. The paper analyzes the vulnerability of previous BRLWE implementations to different types of fault attacks, such as randomization, zeroing, and skipping faults, and shows how they can be easily broken by an adversary. Moreover, it proposes new fault-resilient software implementations of BRLWE on two resource-constrained microcontrollers, namely AVR ATxmega128A1 and ARM Cortex-M0, which are suitable for IoT devices.

A variant of Ring-LWE, known as the Ring-ExpLWE scheme [64], has been introduced, where the error vector is drawn from an exponential distribution. This makes the noise distribution more discrete and increases the security level of the scheme. Its security level is evaluated by comparing and analyzing the runtime of BRLWE and Ring-ExpLWE when subjected to quantum hybrid attacks, as well as examining the noise polynomials in each scheme. The Ring-ExpLWE scheme has a high performance, and a low area-time product compared to BRLWE while maintaining a strong security level.

All the previous proposed works that aim to improve the BRLWE try to improve the security of the algorithm against SCA by adding more computation tasks. They tried to present lightweight methods, but it was still not enough. The computation time was always higher than the computation time of the original BRLWE. In this paper, we aim to enhance the security of the BRLWE algorithm against SCA, including timing, SPA, and DPA, and to optimize the polynomial multiplication process which is a complex task within the BRLWE algorithm. The combination of adding computation tasks to improve the security and at the same time optimize the polynomial multiplication helps us to create a balance between security efficiency.

4.4 Proposed Approach

In this section, we present the different variants of Karatsuba multiplication algorithms then, we display the new shuffling method-based Karatsuba multiplication and how it enhances the security of BRLWE and improves its computation cost. Moreover, we exhibit the main approach including a detailed description of each phase of the proposed BRLWE.

4.4.1 Karatsuba Polynomial Multiplication

Figure 4.2 depicts a summary of all the arithmetic operations involved with each phase of the BRLWE. In the key generation phase, polynomial multiplication and polynomial subtraction are performed to generate the public key *p*. The encryption phase involves polynomial multiplication and polynomial addition to compute the first part of the ciphertext, *c1*, and requires additional polynomial multiplication and two polynomial additions to generate *c2.* Finally, in the decryption phase, polynomial multiplication and polynomial addition are used to recover the original message.

We can see that the major arithmetic complexity of each phase of the BRLWE scheme lies mainly in the polynomial multiplication (Polynomial addition and substruction are just point-wise operations). To improve the BRLWE computation cost we need to optimize the polynomial multiplication.

SPMA is a highly efficient method for multiplying polynomials due to its straightforward computational structure. Its folded architecture is simple to implement, consumes a small hardware area and has a low throughput performance. The complexity of the SPMA is $O(n^2)$. On the other hand, the NTT is an advanced method that can achieve high-speed polynomial multiplication with a complexity of $O(nlogn)$. However, NTT requires complicated pre-computation and array re-ordering to achieve high speed, requiring much higher memory usage and area consumption compared to SPMA.

The Karatsuba algorithm offers a middle ground between these two extremes. It has a computational complexity of $O(n^{log_2 3})$, which is lower than SPMA but higher than NTT. This makes Karatsuba a favorable choice for balanced implementations of resources-constrained Lattice-Based Cryptography (LBC). Furthermore, in the round 3 submission to the NIST Post-Quantum Cryptography (PQC) standardization process, the authors of the Saber cryptographic scheme advised against using NTT for polynomial convolution. The primary reason is that the ring structure

used in Saber, typically does not facilitate a straightforward implementation of NTT due to the difficulty in finding appropriate roots of unity and ensuring compatibility with the modulus [56]. Similarly, in the context of BRLWE, which often involves rings with binary coefficients, implementing NTT can be challenging. The absence of suitable roots of unity and the specific modulus requirements make NTT impractical for such schemes. Therefore, alternatives like Karatsuba are preferred for their more manageable complexity and compatibility with the ring structures used in BRLWE.

Besides the reduced computation cost of Karatsuba and its simplicity to implement, it can provide another layer of security for BRLWE. By recursively splitting polynomials and shuffling each sub-polynomial separately, even if an attacker discovers the shuffling factors, they will only gain partial information about the secret key rather than the entire key.

1- Decompositions of Karatsuba multiplication

In Karatsuba multiplication, increasing the decomposition factor can further decrease the number of coefficient multiplications, thus lowering computational costs. When $A(x)$ and $B(x)$ are divided into three segments, each of length $n/3$ rather than two, their product P(x) can be represented as:

$$P(x) = P_0(x) + P_1(x)x^{n/3} + P_2(x)x^{2n/3} + P_3(x)x^{n} + P_4(x)x^{4n/3} \quad (10)$$

It can be computed according to [48] as follows:

$$P_0(x) = A_0(x)B_0(x) \quad (11)$$

$$P_1(x) = (A_0(x) + A_1(x))(B_0(x) + B_1(x)) - A_1(x)B_1(x) - A_0(x)B_0(x) \quad (12)$$

$$P_2(x) = (A_0(x) + A_1(x) + A_2(x))(B_0(x) + B_1(x) + B_1(x)) - ((A_0(x) + A_1(x))(B_0(x) + B_1(x)) - A_1(x)B_1(x)) - ((A_1(x) + A_2(x))(B_1(x) + B_2(x)) - A_1(x)B_1(x)) \quad (13)$$

$$P_3(x) = (A_1(x) + A_2(x))(B_1(x) + B_2(x)) - A_1(x)B_1(x) - A_2(x)B_2(x) \quad (14)$$

$$P_4(x) = A_2(x)B_2(x) \quad (15)$$

Using three segments, six multiplications between polynomials of length $n/3$ are required, leading to a total of $6(n/3)^2 = 2n^2/3$ coefficient multiplications. For a four-segment decomposition, ten multiplications are needed between polynomials of length $n/4$, resulting in $10(n/4)2 = 5n^2/8$ coefficient multiplications. The formulas for two-segment decompositions, as shown in (6), (7),

(8), and (9), and for three-segment decompositions in (10) through (15), can be iteratively applied to achieve higher decompositions and further minimize the number of coefficient multiplications.

2- Karatsuba Polynomial Multiplication with Integrated Modular Reduction

The Karatsuba algorithm aims to reduce the number of coefficient multiplications, but the intermediate segment products must be assembled appropriately to compose the final polynomial product. This assembly process needs more storage for intermediate results and supplementary additions and subtractions. These can cause problems, especially for applications with limited memory.

The works [125] and [126] proposed to apply the integrated modular reduction by x^n+1 directly on the segment products during Karatsuba multiplication before adding them up. This technique optimizes the assembly process before the final addition/ substruction of segments, thereby reducing the number of additions/ substructions without increasing multiplication complexity. Furthermore, the shared terms help to minimize the memory size, which stores intermediate results and accounts for a significant portion of the silicon area required for polynomial multiplication as shown in Figure 4.3.

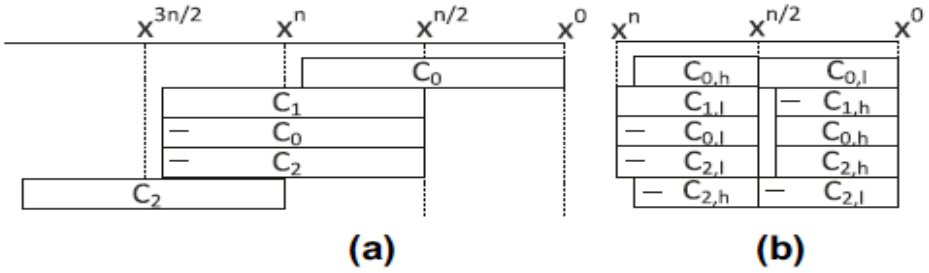


Figure 4.3 Segment products needed to be added up in Karatsuba multiplication with 2-decomposition: (a) original; (b) with integrated modular reduction by $x^n + 1$ [125].

4.4.2 The proposed Karatsuba multiplication based random shuffling method

The shuffling method aims to add randomness through permitting operations order. It effectively hides the correlation between the secret key and the ciphertext, making it harder for an attacker to extract information. The shuffling method provides strong security guarantees and can withstand attacks based on statistical analysis [127], [128]. However, typically, it produces additional

computation costs and memory usage. The effectiveness of the shuffling method and the exact computation cost relies on the shuffling algorithm used.

In this paper, we propose to use the Fisher-Yates Shuffle algorithm known as the Knuth shuffle [127]. It is a widely used algorithm for shuffling a finite sequence, due to its simplicity to understand and implement. This algorithm shuffles the element of the array in place without requiring additional memory or data structures and performs a linear number of permutations that make it efficient for IoT applications. Moreover, it produces uniformly random permutations and provides good randomness proprieties which make it efficient against Timing and SPA attacks.

However, in [127], the authors proved that the simple shuffling algorithm can not protect against DPA attacks. These attacks exploit the correlations in power consumption between different clock cycles, making it possible to infer sensitive information despite the simple shuffling.

To eliminate these correlations between the power consumption and the sensitive information, we propose to divide the polynomials into sub-polynomials during the polynomial multiplication and randomly shuffle the order of operations of each sub-polynomial multiplication. Each multiplication involves several smaller operations, and because these operations are performed in a random order, the overall power consumption pattern becomes more complex and less correlated with any specific sub-operation. Which reduces the ability of an attacker to combine information from different parts of the trace to deduce the key.

We propose to apply Karatsuba multiplication algorithm in polynomial multiplication. This algorithm is based on recursively splitting each polynomial into n-size sub-polynomials then combining the partial products to obtain the final product. The main objective of this algorithm is to optimize the polynomial multiplication cost, which improves the computation cost of the random shuffling method.

To determine the most efficient Karatsuba multiplication algorithm to enhance the computation cost and security of BRLWE. We implement the simple Karatsuba multiplication (2-Decompositions) based shuffling for BRLWE, 3-Decompositions Karatsuba based shuffling for BRLWE, 4-Decompositions Karatsuba based shuffling for BRLWE and 3-Decompositions Karatsuba with integrated modular reduction-based shuffling for BRLWE, as shown in Table 3 in Section (V). According to the results presented in Table 3, the 3-decomposition Karatsuba-based

shuffling for BRLWE gives the best results. Algorithm 4.1 represents the proposed 3-Decomposition Karatsuba-based random shuffling method.

Algorithm 4.1: 3-Decompositions Karatsuba based Shuffling

Input: *A(x), B(x)* ← $\{0,1\}^n$, *n is power of 3*
Output: *P(x)= A(x).B(x)*
N←*max(degree(A),degree(B))*
if *n=1 :*
  P(x)← *A(x).B(x)*
else if *n < 32:*
  P(x)←$Schoolbook\ Polynomial\ Multiplication\ (A, B)$
else*:*
  1- Pre-processing Phase
  m ← *n/3*
  $A_0(x)$ ← $A_0(x)[m-1:0]$;
  $A_1(x)$ ← $A_1(x)[2m-1:m]$;
  $A_2(x)$ ← $A_2(x)[n-1:2m]$;
  $B_0(x)$ ← $B_0(x)[m-1:0]$;
  $B_1(x)$ ← $B_1(x)[2m-1:m]$;
  $B_2(x)$ ← $B_2(x)[n-1:2m]$;
  2- Shuffling phase
  $A'_0(x)$ ← *Random Shuffling (* $A_0(x)$, *m);*
  $A'_1(x)$ ← *Random Shuffling (* $A_1(x)$, *m);*
  $A'_2(x)$ ← *Random Shuffling (* $A_2(x)$,*m);*
  $B'_0(x)$ ← *Random Shuffling (* $B_0(x)$,*m);*
  $B'_1(x)$ ← *Random Shuffling (* $B_1(x)$,*m);*
  $B'_2(x)$ ← *Random Shuffling (* $B_2(x)$,*m);*
  ❖ **Recursive and Polynomial multiplication**
  $P_0(x)$ ← *Karatsuba(*$A'_0(x)$, $B'_0(x)$, *m);*
  $P_1(x)$ ← *Karatsuba(* $A'_0(x) + A'_1(x)$, $B'_0(x) + B'_1(x)$, *m);*
  $P_2(x)$ ← *Karatsuba(*$A'_0(x) + A'_1(x) + A'_2(x)$, $B'_0(x) + B'_1(x) + B'_2(x)$, *m);*
  $P_3(x)$ ← *Karatsuba(*$A'_1(x) + A'_2(x)$, $B'_1(x) + B'_2(x)$, *m);*
  $P_4(x)$ ←*Karatsuba(*$A'_2(x)$, $B'_2(x)$, *m);*
  $P_5(x)$ ←*Karatsuba(*$A'_2(x)$, $B'_1(x)$, *m);*
  ❖ **Post-processing Phase**
  P1(x) ← *P1(x)* − *P5(x)* − *P0(x);*
  P2(x) ← *P2(x)*− *(P1(x)* − *P5(x))* – *(P3(x)* – *P5(x));*
  P3(x) ← *P3(x)*− *P5(x)*− *P4(x);*
  P(x) ← *x4n/3P4(x) + xnP3(x) + x2n/3P2(x) + xn/3P1(x)+P0(x);*
End if
Return P(x);

Generally, Karatsuba multiplication is particularly effective for multiplying large numbers. It gives better results than the SPMA only with big numbers because it requires more additions and digit

shifts. For this reason, as illustrated in Algorithm 1, we apply the Karatsuba algorithm only when the polynomial degree is more than 32.

Furthermore, to introduce additional noise and enhance randomization and to cancel the correlation between clock cycles, we propose to refresh the shuffling factor in each cycle. During each cycle, a new random number is used for shuffling, breaking the link between consecutive clock cycles. As a result, potential DPA attackers cannot extract any meaningful information from trace analysis across different cycles. By applying this approach, the shuffling method effectively obscures the actual sequence of operations, making it significantly more challenging for attackers to deduce sensitive information from side-channel leakage.

The polynomial splitting and the updates of the shuffling factor in each cycle provide an added layer of security, ensuring the resilience of the cryptographic scheme against DPA attacks.

Algorithm 4.2 exhibits the random shuffling algorithm for each sub-polynomial. The proposed random shuffling algorithm generates a random number *r* between <1, n/3−k>, called shuffling factor, where *n* is the length of the polynomial in each cycle and *k* is the number of elements already processed in the cycle. We divide *n* by 3 because we used 3-Decomposition Karatsuba multiplication (see (14), (15), (17) and (18)), and we shuffle each sub-polynomial separately to add more noise and make it harder for an attacker to predict the whole polynomial of the secret key. In the first iteration, the algorithm swaps the last element of the sub-polynomial with the *r-th* element, and the iteration continues to reduce the size of the sub-polynomial by 1 until the first element is reached. This made the time complexity O(n) with space complexity O(1) for the random function.

Algorithm 4.2: The proposed Random shuffling algorithm

***Input**: sub-polynomial of coefficients c, sub-polynomial degree m;*
***Output:** Shuffling c*
***For** each Karatsuba cycle:*
  m ← n/3;
  ***For** j from (m-1) down to 1:*
    random integer r between 0 and j;
    Swap c[j] and c[r];
  End
End
Return (c);

4.4.3 Main Approach

In this paper, we focus primarily on data confidentiality and encryption to secure transmitted data within the 3DKSh-BRLWE scheme. We assume that IoT devices are pre-authenticated on the Cloud/ Edge side, and the Cloud/ Edge infrastructure itself is treated as a secure entity. This assumption allows us to ensure that data is only encrypted and transmitted by verified devices, while enabling our efforts to be dedicated to developing a robust encryption approach to protect data confidentiality during transmission.

In this section, we present the main components and functions of the proposed robust encryption approach, as shown in Fig. 4.4. First, we present the two components of the proposed approach which are: IoT device and cloud/edge computing.

- Cloud / Edge COMPUTING: This entity is responsible for generating both the public and private keys. It generates and securely stores the private key, while the public key is shared with authenticated devices. Additionally, cloud/edge computing performs decryption operations using the private key, which is retained solely within the cloud infrastructure and not distributed.

- IoT Device: This entity is tasked with encrypting the data it collects using the public key provided by the cloud.

Second, we present the main three functions of the proposed approach which are, key generation, encryption and decryption.

- Key generation: this phase is responsible for generating the public and the private keys. In this phase, two binary polynomials, r1 and r2, are randomly selected, where r2 is the secret key. Therefore, the main operation is to produce the public key using (10).

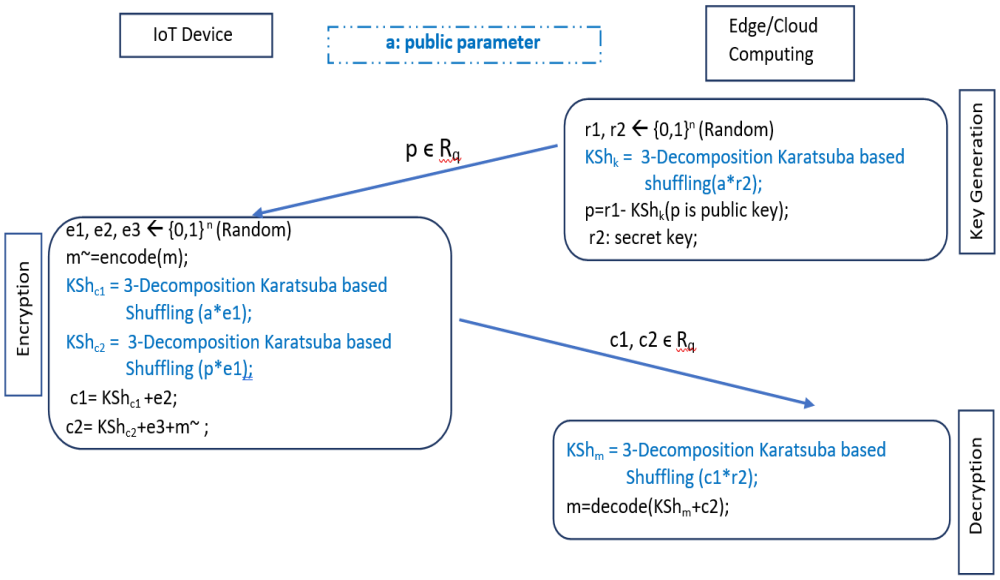


Figure 4.4 The proposed 3DKSh-BRLWE phases.

$$p = r1 - Sh(a*r2), \qquad (16)$$

where a is the public polynomial of the integer, Sh( ) is the random shuffling function, and the operation (*) is the 3-Decomposition Karatsuba polynomial multiplication. The size of public key p and private key $r2$ is different, private key $r2$ is composed of n bits while the public key p consists of n _ log2 q bits, and the polynomial $r1$ will be ignored after the public key calculation. To optimize the polynomial multiplication and to protect the secret key from timing and power analysis attacks (SPA and DPA), we apply a 3-Decomposition Karatsuba-based random shuffling on the public key computation to protect sensitive information such as a secret key.

- Encryption: this phase is responsible for the encryption of n−bit message m. Firstly, the message is mapped to a polynomial $m \in \Re q$ using (17), and secondly, it generates the ciphertexts $c1$ and $c2$ from the message using (18) and (19). The polynomials $c1$ and $c2$ are computed using the public key (p) and the random vector errors $e1$, $e2$ and $e3 \in \Re_q$ are uniformly and randomly selected from $\{0,1\}^n$. To add noise and reduce the computation time of the ciphertexts, we apply the proposed 3DKSh algorithm on $c1$ and $c2$ computation. We apply the 3-Decomposition Karatsuba multiplication (*) and randomly shuffle (Sh) each sub-polynomials in the polynomial multiplication of $c1$ and $c2$.

$$\boldsymbol{m} = \text{ENCODE}(m)$$

$$(m_0,\ldots,m_{n-1}) \rightarrow \sum_{i=0}^{n-1} m_i \left(-\frac{q}{2}\right)x^i, \qquad (17)$$

where $(m_0,\ldots,m_{n-1})$ represents the message as a vector of coefficients, m_i denotes the i-th coefficient of the message, q is a prime number related to the modulus used in the cryptographic scheme and x^i represents the power of x corresponding to the position of each coefficient.

$$c1 = Sh(a * e1) + e2 \qquad (18)$$

$$c2 = Sh(p * e1) + e3 + m \qquad (19)$$

It is worth noting that in (17), we use the new variant proposed by [17]. This variant used the two's complement range to manage the reduction operation and eliminate individual reduction checks using natural overflow. The range of polynomial coefficient values is adjusted from $(-\lfloor q/2 \rfloor + 1, \lfloor q/2 \rfloor)$ *to* $(-\lfloor q/2 \rfloor, \lfloor q/2 \rfloor - 1)$.

- Decryption: this phase is responsible for ciphertext decryption and message recovery. It uses the secret key *r2* and the ciphertexts *c1* and *c2* to generate the decryption polynomial $d \in \mathfrak{R}_q$ calculated by (20). In this phase, we also apply the proposed 3DKSh algorithm in the polynomial multiplication of *c1* and *r2*. Using the random shuffling method (Sh) and the 3-Decomposition Karatsuba multiplication (*), to protect the secret key while reducing the computation time. The threshold decoder in (22) processes each coefficient separately. It outputs a binary '0' if the calculated polynomial's coefficient falls outside the range of (q/4, 3q/4), otherwise, it outputs a '1'. The application of the BRLWE decryption function directly can cause half of the decoding failure, thus it is necessary to take into consideration the boundary overflow problem under the discrimination condition [17].

$$d = Sh(c1 * r2) + c2 \qquad (20)$$

$$\text{DECODE} : \mathfrak{R}_q \rightarrow \{0, 1\}^n,$$

$$\sum_{i=0}^{n-1} d_i\, x^i \rightarrow (m_0,\ldots,m_{n-1}), \qquad (21)$$

$$m_i = \begin{cases} 0, & \left| d_i - i - \left\lfloor \frac{n-3}{2} \right\rfloor \right| > \frac{q}{4} \\ 1, & else \end{cases} \qquad (22)$$

4.5 Security Analysis

In this section, we formally analyze the security of 3DKSh-BRLE against quantum hybrid attacks and timing, SPA and DPA attacks.

4.5.1 Quantum hybrid attack

To analyze the security level of our approach against a quantum hybrid attack and compare it with BRLWE, we evaluate the runtime for both schemes under the same parameter set. Initially, we explore the runtime for our approach using a quantum hybrid attack, which is suitable for evaluating both BRLWE and our enhanced version due to their sparse secret and error vectors [57]. Hybrid attacks consist of classical and quantum versions [129]. The quantum hybrid attack replaces the classical meet-in-the-middle technique [130] with a quantum search algorithm for faster guessing. In the quantum hybrid attack [129], we first convert the LWE instance into a uSVP problem using (23):

$$\ell = \{x \in \mathbb{Z}^d : (A\ |I_m|\ -\ b)\ x = \ 0\ mod\ q\}, \qquad (23)$$

where ℓ is a *d*-dimensional lattice, in which $d = n+m+1$; $(A\ |I_m|\ -\ b)$ is an augmented matrix that includes: A$\in \mathbb{Z}_q^{m\times n}$ a randomly chosen matrix representing the public part of the LWE instance, I_m the identity matrix of size m×m, which ensures that the error vector e is incorporated into the lattice structure; and $-b$ which is a column vector representing the negation of the known vector b from the LWE instance. This component links the lattice definition directly to the original LWE instance. The vector $\boldsymbol{v} = (\boldsymbol{s}, \boldsymbol{e}, 1)$ is an element of the lattice ℓ, because of $\boldsymbol{s} \in \mathbb{Z}_q^n$ and $\boldsymbol{e} \in \mathbb{Z}_q^m$.

The second step is to solve the uSVP problem using (17):

$$\acute{L} = \begin{pmatrix} L & C \\ 0 & I_r \end{pmatrix} \in \mathbb{Z}^{d\times d}, \qquad (24)$$

where Ĺ is a basis for lattice ℓ, $L \in \mathbb{Z}^{(d-r)\ x\ (d-r)}$, $r \in \mathbb{N}$ and $r < m, n$. We can represent the short vector $\boldsymbol{v} = (\boldsymbol{v}_l, \boldsymbol{v}_g)$ by lattice basis Ĺ as it belongs to the lattice ℓ using (15):

$$\boldsymbol{v} = \begin{pmatrix} \boldsymbol{v_l} \\ \boldsymbol{v_g} \end{pmatrix} = \acute{L} \begin{pmatrix} h \\ v_g \end{pmatrix} = \begin{pmatrix} Lh + CV_g \\ v_g \end{pmatrix}, \qquad (25)$$

where $Lh \in \mathbb{Z}^{d-r}$ is a vector in Lattice $\ell' \in \mathbb{Z}^{d-r}$ and $v_l - Lh = Cv_g$, $h \in \mathbb{Z}^{d-r}$. Therefore, by solving the BDD problem with Cv_g as the target vector, we can recover the vector $v_l \in \mathbb{Z}^{d-r}$, provided that $v_g \in$

$\mathbb{Z}^r$ is guessed. To enhance the efficiency of solving the BDD problem using the Nearest Plane algorithm [51], it is necessary to precompute a high-quality lattice basis $L \in \mathbb{Z}^{(d-r) \times (d-r)}$ for the Lattice ℓ. The total runtime of the quantum hybrid attack is denoted by:

$$T = \frac{T_h + T_r}{\rho}, \qquad (26)$$

where $Th = l \cdot (d - r)^2/2^{1.06}$ is the runtime for the hybrid attack, Tr is the lattice reduction runtime and ρ is the quantum hybrid attack success probability [49], which is designated by:

$$\rho \approx \prod_{i=0}^{d-r} \left(1 - \frac{2}{B\left(\frac{(b-r)-1}{2}, \frac{1}{2}\right)} \int_{-1}^{max(-r_i-1)} (1-t^2)^{\frac{(d-r)-3}{2}} dt\right), \quad (27)$$

where B(·, ·) denotes the Euler beta function. We define r_i as $R_i/2\ \|v_l\|$, where i ∈ {1, . . . , d−r} and R_i is the length of the Gram-Schmidt basis vectors [49] corresponding to the basis L . Here, $\|v_l\|$is the Euclidean norm of the vector v_l. The runtime of lattice basis reduction depends on both the basis quality δ the lattice dimension $d−r$. Therefore, optimizing the total runtime for a quantum hybrid attack is dependent on the attack parameters r and δ. Hence, it is crucial to optimize the total runtime across all possible choices of attack parameters is crucial for performance. Given the same attack parameters (r, δ) in both schemes, the runtime T_r for BRLWE and our proposal remains consistent since their lattice dimensions remain the same. T_h denotes the runtime of the hybrid attack, where l is the number of guessing cycles for v_g. The computational complexity of a single run of the Nearest Plane algorithm is $(d - r)^2/2^{1.06}$. Based on this analysis, the Nearest Plane algorithm's runtime is equivalent in both our scheme and BRLWE, given the same d and r. For a structured search space, Q-search yields more efficient search cycles. When distributed over a set $S = \{-16, \ldots, 16\}^r$, using the more generalized Grover's search algorithm [130], the search cycles l is designated by:

$$1 = \left(\left(\sum_{i=0}^{32} \rho^{\frac{3}{2}} i\right)^r\right)^{\frac{3}{2}} \approx 2^{1.85r}, \rho_i = \binom{32}{i} 2^{-32} \qquad (28)$$

We apply a generalized version of Grover's search algorithm across both schemes, resulting in identical cycles required for guessing the vector v_g. Thus, the runtime T_h remains the same for both schemes. However, when evaluating the success probability ρ, it's crucial to recognize that the vector v_l in our approach exhibits a larger Euclidean norm compared to BRLWE. This is due to the error vector e. In our approach, we hide the error vector by shuffling the order of operations and

refreshing the shuffling factor which adds more noise. As a result, when computing the integral in the attack success probability (27), the value of r_i for our scheme is smaller than that of BRLWE. As a result, the integral term in the success probability ρ increases for our approach due the upper bound of the integral being $– r_i$. This increase in the integral's result causes each factor in the continuous multiplication in Equation (27) to be smaller, thereby reducing the quantum hybrid attack's success probability for our scheme relative to BRLWE, and consequently leading to a larger total runtime. Furthermore, this conclusion assumes that both schemes employ identical attack parameters. In a more general scenario, when both schemes are evaluated across the complete set of attack parameters, the total runtime of our approach is higher than that of BRLWE (before applying 3-Decopsition Karatsuba algorithm). Thus, our approach exhibits higher runtime complexity, before reducing the polynomial multiplication cost, when optimized on the attack parameter set. This observation also indicates that it offers a stronger security level compared to BRLWE.

4.5.2 Timing and Power analysis countermeasures

An encryption scheme is considered robust and reliable when it not only provides sufficient security at the algorithmic level but also demonstrates resistance to side-channel attacks [130]. NIST specifically requires practical evaluations of submitted schemes for resilience against such attacks, especially in IoT infrastructures where long-term security is critical [114]. Attackers often have physical access to devices that store secret cryptographic keys. Without specific countermeasures, side-channel attacks, such as timing and power analysis, can be exploited to extract these keys, compromising the security of the entire system.

In this section, we discuss how timing, SPA and DPA side channel attacks can infect the BRLWE and how can our enhanced approach improve the security to resist these attacks. Precisely, we analyze the decryption phase because of the direct dependency of each round's behavior on the secret key. In the proposed scheme, the parameter set (n, q) offers flexibility and extensibility. By increasing the values of n and q, the security level improves, when (n, q) takes the value (256, 256), the scheme achieves 84-bit and 73-bit classical and quantum security, respectively. On the other hand, for (n, q) = (512, 256), the security level reaches 190-bit and 140-bit, respectively [103], [57]. However, increasing the values of n and q demands more computing resources.

In our approach, and because we use the 3-Decomposition Karatsuba polynomial multiplication, the polynomials of the ciphertext and the secret key are divided into three sub-polynomials with degree *n/3*. The polynomial multiplication is computed using (11), (12), (13), (14) and (15). To explain how our approach can resist timing, SPA and DPA attacks, we give the following example:

C1= (90,50,30,120,80,150,20,60,70,59,85,94)

R2 = (1,1,1,0,1,0,1,1,0,0,1,1)

Two polynomials with n=12 and q=256. First, we split the polynomials into three sub-polynomials with n=4 and q=85, which gives: $C1_0$= (90,50,30,120), $C1_1$= (80,150,20,60), $C1_2$= (70,59,85,94), $R2_0$= (1,1,0,1), $R2_1$= (1,1,1,0) and $R2_2$= (0,0,1,1).

Second, we randomly shuffle each sub-polynomial using different shuffling factors to eliminate the correlation between the sub-polynomials, where: $C1_0$= (50,90,120,30), $C1_1$= (60,150,80,20), $C1_2$= (85,94,70,59), $R2_0$= (1,1,0,1), $R2_1$= (1,1,0,1) and $R2_2$= (0,1,0,1).

By using these steps, we added a new security layer against Timing, SPA and DPA attacks by eliminating any correlation between the sub-polynomials. Consequently, if an attacker manages to determine the shuffling factor of a sub-polynomial multiplication, they would only be able to detect a portion of the secret and not the entire secret message. This significantly enhances the security of the BRLWE scheme by compartmentalizing the information and making it substantially more difficult for an attacker to reconstruct the full secret.

To eliminate the correlation during the polynomial multiplication, we randomly shuffle each multiplication cycle using different shuffling factors. Fig. 4.5 shows the polynomial multiplication of the first sub-polynomials $C1_0$ and $R2_0$.

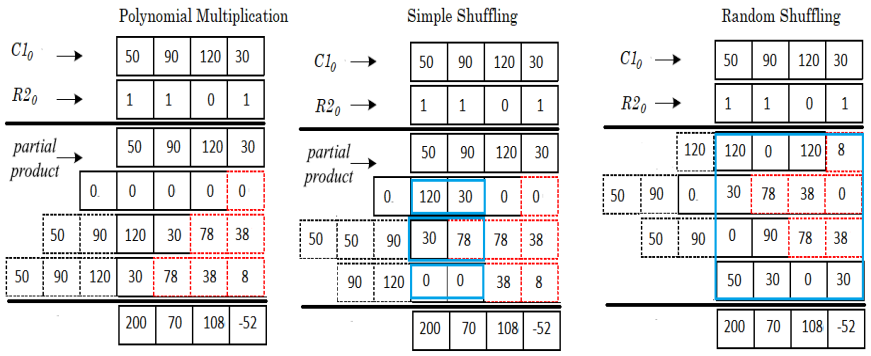


Figure 4.5 The difference between: (a) simple polynomial multiplication. (b) polynomial multiplication with simple shuffling. (c) polynomial multiplication with random shuffling.

The calculation involving the private key $R2_0$ entails polynomial multiplication. Notably, when $R2_0$ is 0, the corresponding partial product becomes 0, as shown in Figure 4.5 (a). A crucial concern arises when performing the addition operation directly, as one input of the adder is 0. This leads to distinct spikes in the measured power trace, which allows the adversary to analyze the power differences caused by these operations. Yet, the attacker could attempt a Simple Power Analysis (SPA) attack, extracting the private key with only a few measurements. Such attacks rely on interpreting power trace variations due to specific operations like addition and memory updates, which do not occur by default.

Using the shuffling method enables the manipulation of the order of operations during polynomial multiplication without affecting the result. This introduces randomness and confusion, making it significantly more challenging for adversaries to extract sensitive information from side-channel leakage. Moreover, using Karatsuba multiplication and especially dividing the polynomial into three sub-polynomial and shuffling the sub-polynomial multiplications will add more noise and protect the secret key.

As shown in Figure 4.5 (a), each addition row is computed in one cycle, so to generate the first-row addition it will compute: (30+0), (120+0), (90+0), and (50+0). Using the simple shuffling method, as shown in Figure 4.5 (b), the first-row addition can be generated as follows: (30+0), (120+0), (90+30), and (50+120). This adds confusion to the attacker to detect the position of the zero and in which the vector exists. Here, our proposed approach resists the simple power analysis (SPA) attacks. Furthermore, it enhances resistance against timing attacks. Each clock cycle now yields different operations, disrupting any correlation between the computation time of each cycle

and the processed data. In the example illustrated in Figure 4.5 (a), the computation time for each cycle might be distinguishable due to the consistent order of operations in each cycle. The shuffling method, however, disrupts this regularity, making the timing attack ineffective in capturing meaningful timing differences.

On the other hand, the simple shuffling method has been shown vulnerable to DPA attack, as demonstrated in [127]. This differential attack leverages a random input during decryption and formulates hypotheses on an intermediate addition. Subsequently, the attack validates these hypotheses through power trace analysis on each cycle, enabling the detection of the shuffling factor's value and facilitating the recovery of the first part of the secret key ($R2_0$).

Therefore, it is hard for a DPA attacker to make a hypothesis and recover the two other parts of the secret key ($R2_1$), ($R2_2$) but it is still possible. In response to this DPA vulnerability, we propose to refresh the shuffling factor's value in each cycle in sub-polynomial multiplication. This strategic refreshment aims to break any correlation between consecutive cycles, rendering hypothesis-making and power trace analysis ineffective. The constant alteration of the shuffling factor during each cycle completely changes the order of operations, preventing any meaningful correlation between consecutive cycles, as shown in Figure 4.5(c). Consequently, the lack of correlation between the shuffling factors in successive cycles introduces substantial noise, effectively thwarting the DPA attacker's efforts to recover the first sub-polynomial of the secret key $R2_0$.

4.6 Complexity Analysis

In this section, we present a comprehensive comparison between the original BRLE scheme and our proposed enhanced version, 3DKSh-BRLWE in terms of complexity analysis. As illustrated in Table 4.2, our 3DKSh-BRLWE presents better complexity than the original BRLWE even if we added the shuffling computation. This is because we have optimized the most costing operation (i.e., polynomial multiplication).

Table 4.2 Time complexity analysis of the proposed approach.

Phases	**BRLWE**	**3DKSH-BRLWE**
Key Generation	$T_{mul} + T_{sub} \rightarrow O(n^2)$	$Tk_{mul} + xT_{Sh} + T_{sub} \rightarrow O(n^{\log_3(6)})$
Encryption	$2T_{mul} + 3T_{add} \rightarrow 2O(n^2)$	$2\,Tk_{mul} + xT_{Sh} + 3T_{add} \rightarrow 2O(n^{\log_3(6)})$
Decryption	$T_{mul} + T_{add} \rightarrow O(n^2)$	$Tk_{mul} + xT_{Sh} + T_{add} \rightarrow O(n^{\log_3(6)})$

T_{mul}, T_{sub}, T_{add}, Tk_{mul}, T_{Sh} represent the timing complexity of classical polynomial multiplication, Polynomial Substruction, Polynomial addition, Karatsuba polynomial multiplication and Shuffling method, respectively. x represents the number of random shuffling operations.

Table 4.3 Comparaison of polynomial multiplication techniques based random shuffling Binary Ring LWE.

Scheme	Computation Time (ms)		Energy consumption(mJ)		Memory usage (bytes)	
	Enc	**Dec**	**Enc**	**Dec**	**Enc**	**Dec**
SPMA-Sh for BRLWE	49.8	29.5	1.83	1.07	180	132
2-DKSh for BRLWE	29.3	14.4	1.05	0.51	180	120
3-DKSh for BRLWE*	18.97	9.53	0.7	0.35	168	132
4-DKSh for BRLWE	33.4	16.3	1.16	0.57	168	132
3-DMRKSh for BRLWE	25.8	12.7	1.41	0.69	160	128

The primary operations in our scheme include polynomial addition, subtraction, and multiplication, with multiplication being the most computationally intensive. Below is a detailed explanation of each operation's efficiency and its impact:

- Polynomial Addition and Subtraction: These operations have a time complexity of O(n), where n is the degree of the polynomial. Due to their linear complexity, they contribute minimally to the overall computational load and thus have a limited impact on performance.

- Standard Polynomial Multiplication*:* Standard polynomial multiplication has a time complexity of $O(n^2)$, While this method can be effective for small polynomials, it becomes computationally demanding as the polynomial degree increases, making it less suitable for larger polynomials, especially in resource-constrained IoT environments.

- 3-Decomposition Karatsuba Polynomial Multiplication: To address the limitations of standard multiplication, we employ 3-Decomposition Karatsuba polynomial multiplication, which reduces the computational cost from $O(n^2)$ to $O(n^{\log_3 6})$, which is approximately $O(n^{1.464})$ [111], [113]. This

reduction represents a significant improvement over the standard Karatsuba algorithm (2-decomposition) with complexity $O(n^{1.585})$.

- Shuffling Method: The shuffling method is used to enhance security by obfuscating data, but it has a relatively low impact on overall time complexity compared to polynomial multiplication. This method operates in linear time, adding minimal computational overhead.

4.7 Implementation and Experimental Results

In this section, we provide device-specific optimization of the proposed method. To emphasize the relevance of the scheme for the Internet of Things, we choose a widely used and resource-constrained microcontroller as the target platform for our implementation, namely the ARM Cortex-M0. To assess the effectiveness of our approach, we conducted a comprehensive comparison against the original BRLWE [103] algorithm and the enhanced versions [63], [64] of the BRLWE that are implemented on the same platform.

The ARM Cortex-M0 is a 32-bit microcontroller processor core designed for low-power, cost-sensitive, and resource-constrained applications. It offers a compact and efficient architecture, making it ideal for various embedded systems,

IoT devices, and other applications that require energy efficiency and real-time processing capabilities, such as:

- Healthcare: Wearable health monitoring devices, such as heart rate monitors and fitness trackers, which require low power consumption and efficient processing.

- Smart Home: Home automation sensors, such as temperature, humidity and motion sensors, operate on limited computational resources while ensuring reliable data transmission.

- Industrial IoT (IIoT): Environmental monitoring sensors used in factories and warehouses to track parameters like air quality and machine vibration, often deployed in large numbers and optimized for energy efficiency.

- Agriculture: Soil moisture sensors and environmental monitoring devices in precision agriculture, which rely on battery-powered devices, must be highly energy-efficient and reliable.

To benefit from the advantage of the 32-bit architecture, we applied the same vectorizing method proposed by [9] to optimize the polynomial multiplication in our Karatsuba multiplication

implementation. This method enables storing two coefficients into one data word, thereby reducing the time required for each multiplication operation by 50%.

We implemented the proposed 3DKSh-BRLWE cryptographic scheme on a resource-constrained, 32-bit ARM Cortex M0 microcontroller, specifically using the Arduino Zero platform and its integrated development environment (IDE). This setup enabled us to evaluate the efficiency of our scheme in terms of computation time, memory usage, and energy consumption, three critical metrics for Internet of Things (IoT) applications where resources are highly limited.

Table 4.4 Implementation results compared with previous software implementations in ARM Cortex-M0

Scheme	Parameters Set	Resistance			Freq. MHz	Clock Cycle (1K)		Time (ms)	
		Timing	SPA	DPA		Enc	Dec	Enc	Dec
InvRBLWE [63]	(p=256, q=256)	✓	X	X	--	1755	3404	52.3	101.4
Ring-ExpLWE [64]	(p=256, q=256)	✓	✓	X	32	1567	792	49.0	24.7
This research work* 3DKSh-BRLWE	(p=256, q=256)	✓	✓	✓	32	621	307	18.97	9.53

To assess the benefits of our approach, we implemented the baseline BRLWE with a proposed random shuffling algorithm using standard polynomial multiplication (referred to as SPMA-Sh for BRLWE). We then extended this with several variations of Karatsuba polynomial multiplication techniques to improve computational efficiency, including: 2-Decomposition Karatsuba-based shuffling for BRLWE, (2-DKSh), 3-Decomposition Karatsuba-based shuffling for BRLWE (3-DKSh), 4-Decomposition Karatsuba-based shuffling for BRLWE (4-DKSh), and 3-Decomposition Karatsuba with integrated modular reduction-based shuffling for BRLWE (3-DMRKSh). Each variation allowed us to investigate the trade-offs between computational cost, memory usage, and energy consumption, with particular attention to the suitability of each approach for the ARM Cortex M0 microcontroller.

The primary goal of introducing Karatsuba decomposition methods was to reduce the time complexity of polynomial multiplication, which is the most computationally demanding operation in BRLWE. As summarized in Table 4.3, the results demonstrate a clear advantage of using

Karatsuba-based methods over standard polynomial multiplication. Among the variations, the 3DKSh-BRLWE approach demonstrated the best computation times, requiring only 18.97 ms for encryption and 9.53 ms for decryption. This represents a significant improvement over the SPMA-Sh method and even outperforms other Karatsuba decomposition methods. The 2-DKSh for BRLWE requires 23.9 ms for encryption and 14.4 ms for decryption. While this approach achieves faster computation than SPMA-Sh due to fewer polynomial multiplications, it is less efficient than 3DKSh-BRLWE because the 2-Decomposition structure has a lower degree of decomposition, resulting in a higher number of coefficient multiplications. Conversely, 4-DKSh for BRLWE requires 33.4 ms for encryption and 16.3 ms for decryption. Although it has a higher decomposition factor, the 4-Decomposition method performs more addition operations and intermediate calculations, which exceed the processing capabilities of the ARM Cortex M0. This limits its efficiency on this microcontroller and makes it less suitable for resource-constrained environments. Meanwhile, 3-DMRKSh for BRLWE requires 25.8 ms for encryption and 12.7 ms for decryption. While modular reduction in this variation reduces memory usage (discussed below), the additional operations required for integrated modular reduction increase computation time, making it less efficient than standard 3-Decomposition (3DKSh-BRLWE).

Memory usage is another critical factor for IoT devices with limited storage, such as the ARM Cortex M0. As shown in Table 3, each variation of the scheme impacted memory usage differently, based on the decomposition method and the addition of modular reduction. The SPMA-Sh for BRLWE consumes 180 bytes for encryption and 132 bytes for decryption. By contrast, 2-DKSh for BRLWE requires 180 bytes for encryption but reduces the decryption memory to 120 bytes, achieving modest memory savings during decryption. In 3-DKSh for BRLWE, the scheme uses 168 bytes for encryption and 132 bytes for decryption, offering a small reduction in encryption memory usage compared to SPMA-Sh while maintaining similar decryption memory requirements. In 4-DKSh for BRLWE, the memory requirements are 168 bytes for encryption and 132 bytes for decryption, similar to 3-DKSh, although it incurs higher computation costs. The 3-DMRKSh for BRLWE further reduces memory usage to 160 bytes for encryption and 128 bytes for decryption. This approach provides the most memory-efficient solution, achieving a 4.8% reduction in encryption memory and a 3% reduction in decryption memory compared to standard 3-DKSh for BRLWE. However, as noted earlier, this memory savings is accompanied by increased computation time due to additional modular reduction operations.

Energy consumption is also a key metric for IoT devices operating on limited power sources, such as batteries. Energy usage is determined by the power required for each operation in combination with the overall computation time. In our analysis, we observed that the power needed for 2-DKSh, 3-DKSh, and for 4-DKSh schemes for BRLWE is consistent at approximately 35 W. However, the 3-DMRKSh for BRLWE approach, which integrates modular reduction, has a higher power consumption of approximately 54 W. This increased power demand results from the additional operations required for modular reduction, which, when combined with the extended computation time, significantly increases energy consumption.

Overall, our results indicate that 3DKSh-BRLWE offers the best balance of low computation time, manageable memory usage, and energy efficiency, making it the optimal choice among the evaluated approaches for resource-constrained IoT applications. While the 3-DMRKSh for the BRLWE variant achieves minor memory savings, its increased computation and energy costs make it less favorable for devices with strict power and performance limitations.

To demonstrate the effectiveness of our proposed 3DKSh-BRLWE scheme, we conducted a comparative analysis of computation time in both the encryption and decryption phases against the original BRLWE scheme [103], as illustrated in Fig.4.6. The results indicate that 3DKSh-BRLWE achieves a 32.49% reduction in computation time for encryption and a 20.58% reduction for decryption compared to the original BRLWE scheme. This substantial improvement in computation efficiency highlights the advantage of using our 3-Decomposition Karatsuba approach for lightweight encryption schemes. The significant reduction in computation time, combined with the enhanced security features of our approach, positions 3DKSh-BRLWE as a highly promising solution for securing resource-constrained applications, especially IoT devices where computational resources are limited, and efficiency is crucial.

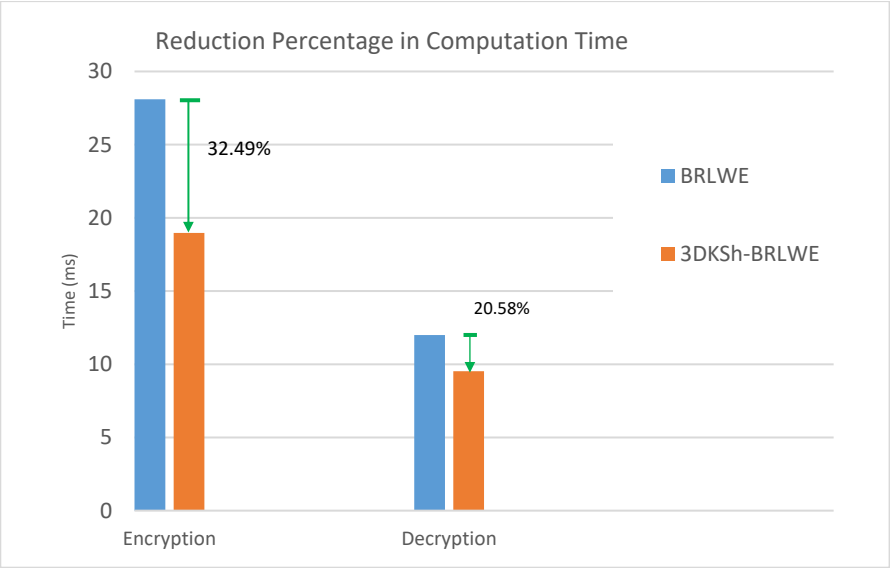


Figure 4.6 The reduction percentage of the original BRLWE and the proposed 3DKSh-BRLWE in the computation time.

Additionally, we conducted a comparative study against the schemes presented in [19] and [46], which were implemented using the same ARM Cortex M0 microcontroller and aimed to enhance BRLWE security. Our findings, summarized in Table 4, reveal that 3DKSh-BRLWE achieves the lowest computation time among the schemes tested, while also withstanding timing attacks, Simple Power Analysis (SPA), and Differential Power Analysis (DPA) attacks. By demonstrating resilience against these specific types of side-channel attacks, our proposed scheme achieves a higher level of security compared to the schemes in [63] and [64], which are more susceptible to timing and power-based attacks due to longer computation times and less efficient shuffling methods.

Overall, these results confirm that 3DKSh-BRLWE offers a unique combination of low computation time and robust security against side-channel attacks, providing a clear advantage over alternative schemes on the same ARM Cortex M0 platform. This makes it particularly well-suited for secure IoT applications, where efficient and resilient encryption is critical.

4.8 Conclusion

In this paper, we proposed an improved version of BRLWE using the random shuffling method and the 3-Decomposition Karatsuba multiplication to improve the security and optimize the polynomial multiplication cost.

We formally proved that 3DKSh-BRLWE resists the hybrid quantum attacks and the timing, SPA and DPA Side-Channel attacks. Moreover, we provide a software implementation using ARM Cortex-M0. In our evaluation, we examined the SPMA-based random shuffling for BRLWE with various Karatsuba multiplication techniques to demonstrate the advantages of Karatsuba multiplication and to determine the most suitable Karatsuba variant for our implementation. Furthermore, we compared our results with the original BRLWE and the existing software implementations that aim to improve it. Our approach requires only 18.79 ms and 9.53 ms for the encryption and the decryption respectively, which makes it a very good candidate for lightweight and resource-constrained IoT devices.

As future work, we aim to enhance the proposed approach to resist other types of side-channel attacks (SCAs), such as fault attacks. Our algorithm is currently optimized for polynomials of degree 256 and below on the Cortex M0, making it suitable for lightweight applications. However, for higher polynomial degrees, scalability needs to account for the increased cost of the random shuffling phase. To address this, implementing an adapted j-decomposition Karatsuba algorithm on more capable microcontrollers could help reduce computational overhead while maintaining efficiency in larger and more demanding cryptographic scenarios.

ACKNOWLEDGMENT

The authors would like to thank Dr. Franjieh El Khoury for her valuable comments and proofreading of this paper.

This research work was funded by the Natural Sciences and Engineering Research Council of Canada (NSERC), Prompt, Flex Group, and ISAME.

CHAPITRE 5 ARTICLE 2: REAL-TIME ANOMALY DETECTION IN IOMT NETWORKS USING STACKING MODEL AND A HEALTHCARE-SPECIFIC DATASET

Hadjer Goumidi and Samuel Pierre (Senior Member, IEEE)

Department of Computer and Software Engineering, Polytechnique Montréal, Montreal, QC H3T 1J4, Canada

E-mail: hadjer.goumidi@polymtl.ca; samuel.pierre@polymtl.ca;

Revue : Accepté et publié dans le journal *IEEE Access* volume 1*3,* pages 70352-70365, 2025, 14 avril 2025.

Abstract

The Internet of Medical Things (IoMT) connects medical devices to enable real-time monitoring and personalized care, significantly enhancing patient health and well-being. However, this connectivity also introduces substantial cybersecurity risks, including various attack types that compromise data integrity and availability, jeopardizing patient safety and healthcare service reliability. This study addresses these challenges by proposing a real-time anomaly detection model based on machine learning (ML) techniques, designed to detect and mitigate diverse cyber threats effectively. This paper proposes a new medical dataset for anomaly detection, inspired by the UNSW-NB15 dataset, and enriched with healthcare-relevant attack types, including falsification and DoS attacks, to reflect real-world IoMT scenarios. The dataset comprises 253,680 records, with 60% anomalous data distributed across multiple attack types, offering a more challenging and realistic environment for evaluating ML models. Seven machine learning algorithms, including Random Forest, XGBoost, and Artificial Neural Networks (ANN), were rigorously tested, leading to the development of a novel stacking ensemble model. This model integrates XGBoost as the meta-learner with Random Forest and ANN as base models, leveraging their strengths to optimize anomaly detection. The proposed model was evaluated on both the UNSW-NB15 and the new medical dataset, achieving significant improvements across key metrics such as accuracy,

precision, recall, and F1-score. A real-time prediction analysis further demonstrated its ability to detect anomalies efficiently during live data transmission, validating its suitability for detecting anomalies in real-time scenarios.

Keywords: Anomaly detection, Intrusion Detection System, Internet of Medical Things, medical dataset with anomalies, machine learning, healthcare security.

5.1 Introduction

The Internet of Medical Things (IoMT) has revolutionized modern healthcare by seamlessly connecting medical devices, wearable sensors, and healthcare IT systems [131]. This interconnected ecosystem enables real-time patient monitoring, personalized treatment plans, and efficient care delivery, significantly enhancing healthcare quality and patient outcomes. Devices such as smart infusion pumps, wearable health monitors and connected diagnostic tools empower healthcare providers to make timely interventions and deliver tailored care strategies. Beyond clinical benefits, IoMT reduces costs, improves operational efficiency, and increases accessibility to medical services, holding immense potential to redefine healthcare systems globally [131,132].

However, the integration of IoMT devices into healthcare networks introduces significant cybersecurity challenges. These devices often operate with limited computational resources and lack robust security features, making them vulnerable to cyberattacks such as data falsification, denial of service (DoS) attacks, and message tampering [133,134]. Such threats can compromise the integrity and availability of critical healthcare systems, with severe consequences. For instance, a falsified message from an insulin pump could lead to incorrect dosages, or a DoS attack could disrupt vital monitoring systems during emergencies, endangering patient lives [135].

Traditional security measures, including cryptographic techniques like hashing and encryption, are essential but often impose computational demands that exceed the capabilities of resource-constrained IoMT devices [135,136]. For example, ensuring message integrity through hashing can be computationally expensive for medical devices. Moreover, even encrypted data remains vulnerable to integrity and availability threats. To address these limitations, machine learning (ML)-based anomaly detection systems have emerged as a promising solution, enabling real-time analysis of incoming data to identify tampering, disruptions, or malicious activity.

To support this effort, we developed a new medical dataset for anomaly detection that reflects real-world healthcare scenarios and addresses the limitations of existing datasets. By incorporating features and attacks inspired by the UNSW-NB15 dataset [137] and introducing attacks that significantly impact healthcare systems, such as falsification and DoS attacks, this dataset provides a comprehensive foundation for evaluating Intrusion Detection Systems (IDS) solutions. It includes diverse normal and anomalous data, balancing complexity and practicality for IoMT security research. Using this dataset, we evaluated seven ML algorithms, XGBoost [138], Random Forest [139], ANN [140], Support Vector Machines (SVM) [141] , K-Nearest Neighbors (KNN) [142], Logistic Regression (LR) [143], and Isolation Forest (IF) [143], and selected XGBoost, Random Forest, and ANN as base learners for their strong accuracy and efficiency. These algorithms were integrated into a novel stacking ensemble model, with XGBoost serving as the meta-learner, to achieve robust and efficient anomaly detection tailored to IoMT environments.

This research addresses the cybersecurity challenges of IoMT, particularly data integrity and availability, through a real-time anomaly prediction model. The model dynamically adapts to incoming messages and newly detected anomalies or attack types. To overcome the lack of specialized datasets for healthcare systems, we developed a new medical dataset combining medical data with IoT network attacks (e.g., Fuzzers, Shellcode, Worms, Exploit) and healthcare-relevant attacks (e.g., Data Falsification and DoS). Additionally, we proposed a stacking ensemble model that demonstrates superior accuracy and efficiency, offering a reliable solution for real-time anomaly detection in healthcare environments.

To guide this research work, the study is driven by the following research questions:

- How can a synthetic medical dataset that integrates healthcare data with diverse network attack types improve the development and evaluation of anomaly detection models for IoMT?
- Which machine learning algorithms are most suitable for detecting and classifying both generic and healthcare-specific attacks (such as data falsification and DoS) with high accuracy and reliability?
- Can a stacking ensemble model enhance the detection performance across multiple attack categories?
- How effective is the proposed model in performing real-time anomaly prediction during live data transmission, and what levels of accuracy can be achieved in such a setting?

The key contributions of this research are as follows:

1) We proposed a real-time anomaly detection model based on machine learning, capable of pre-training datasets and dynamically predicting attacks in real time.
2) We developed a new medical dataset for anomaly detection that integrates medical data with known IoT network attacks inspired by UNSW-NB15 dataset and healthcare-relevant attack types such as falsification and DoS attacks to address real-world IoMT challenges.
3) We evaluated the performance of seven machine learning algorithms across both the UNSW-NB15 and the new medical datasets to identify the most effective models for anomaly detection.
4) Based on the evaluation results, we designed a novel stacking ensemble model that integrates the best-performing algorithms to enhance anomaly detection and real-time prediction capabilities.
5) We conducted a real-time prediction analysis by sending 100 sequential messages containing normal and anomalous data and performed real-time anomaly detection during live data transmission.

Our proposed stacking model demonstrated superior performance, significantly improving accuracy and efficiency, and demonstrating reliable performance across diverse attack types.

The originality of this paper lies in developing a real-time anomaly detection model that dynamically detects anomalies during live data transmission, creating a medical dataset enriched with real-world attack types, and proposing a high-performing stacking model with superior accuracy and efficiency for real-time IoMT applications.

This paper is organized as follows. Section II provides an overview of related works, focusing on machine learning methods and anomaly detection systems for IoT networks and IoMT. Section III explains the methodology, describing the proposed anomaly detection model and stacking algorithm. Section IV discusses experiments, including the feature selection and the creation of the new dataset, as well as presenting the results including the performance of ML models and the proposed stacking algorithm on both datasets and the real-time prediction analysis. Finally, Section V concludes the paper and suggests future directions for improving anomaly detection systems in IoMT environments.

5.2 Related Work

The increasing use of machine learning for anomaly detection in IoMT and IoT networks has led to diverse approaches, datasets, and methodologies. This section reviews key contributions, focusing on anomaly detection techniques, ensemble frameworks, and their applications in healthcare and IoT security. A comparison of prior works is provided in Appendix A.

In [65], five machine learning algorithms were evaluated on the MIT-BIH dataset for heart rate anomaly detection. While effective, the study defined variables outside the fixed range (60–100 bpm) as anomalies, which limited its real-world applicability. Local Outlier Factor (LOF) and Random Forest performed best, highlighting the potential of simulated data for training. Park *et al.* [66] used GANs to generate fraud labels for datasets lacking them, applying logistic regression and XGBoost for classification, with SHAP analysis identifying key features. In [67], unsupervised clustering (K-means and K-medoids) was used to detect anomalies in wearable sensor data, with K-means slightly outperforming K-medoids. However, dataset details were lacking. In [68], the DIB system used R-FCVM (rough set theory and fuzzy core vector machine) to detect illegal device behavior in medical IoT but did not address data anomalies. Alsolami *et al*. [69] explored ensemble learning (Bagging, Boosting, Stacking) for IoMT anomaly detection using the WUSTL-EHMS-2020 dataset [70], though its small size and limited attack types hindered comprehensive evaluation. In IoT, Ullah *et al.* [71] used CNNs for multiclass anomaly detection, achieving high accuracy with BoT-IoT and IoT-23 datasets. Das *et al.* [72] introduced a hybrid ensemble method for detecting known and zero-day DDoS attacks, achieving 99.1% accuracy on NSL-KDD and UNSW-NB15 datasets. Gu *et al.* [73] proposed a semi-supervised k-means algorithm for DDoS classification, though it lacked accuracy benchmarks. Meidan *et al.* [74] developed N-BaIoT using deep autoencoders for IoT devices, effective but without accuracy metrics. Ravi *et al.* [75] proposed a semi-supervised deep extreme learning machine (SDELM) for DDoS mitigation, though limited to UDP flooding attacks on the UNB-ISCX dataset. Doshi *et al.* [76] presented a four-stage anomaly detection pipeline with high accuracy but relied on synthetic data. Maseer *et al.* [77] evaluated 31 ML models, identifying k-NN, Decision Trees, and Naive Bayes as top performers on CICIDS2017.

Other works addressed domain-specific challenges. Choi *et al.* [78] compared deep anomaly detection models for time-series data. Luo *et al.* [79] used stacked autoencoders (SAE) for early

fault detection in CNC machines. Abdelmoumin *et al*. [80] explored PCA and one-class SVM for scalable IDS development. Poornima *et al*. [81] proposed a regression-based approach to reduce computational complexity in Wireless Sensor Networks. Kavitha *et al*. [82] used logistic regression and ANN for IoT anomaly detection, with ANN outperforming logistic regression on DS2OS. Alsamiri *et al*. [83] evaluated seven ML algorithms on Bot-IoT, improving detection with new features. Hasan *et al*. [84] integrated XAI with ensemble classifiers for Bitcoin anomaly detection, proposing XGBCLUS for data balancing, which outperformed traditional methods.

Existing literature highlights limitations, such as the lack of comprehensive medical datasets and real-time intrusion detection evaluation. While ensemble methods like voting and stacking have been explored, their real-time application in IoMT remains underdeveloped. To address these gaps, this research introduces a new medical anomaly detection dataset combining medical data with UNSW-NB15-inspired attacks, enriched with healthcare-relevant threats. A novel stacking ensemble model (XGBoost, Random Forest, ANN) is proposed. The evaluation of the proposed model is performed in real-time scenarios, demonstrating robustness and efficiency in practical healthcare settings.

5.3 Methodology

This section presents the proposed real-time anomaly detection model and the stacking ensemble model, along with the machine learning (ML) algorithms analyzed in this work.

5.3.1 The proposed Real-Time Anomaly Detection model

Healthcare systems operate in dynamic environments where vast amounts of data are continuously generated and transmitted by connected devices. Real-time anomaly detection is critical in this context, as delays in identifying malicious activity can lead to severe consequences, including unauthorized access, falsification of patient data, and disruption of healthcare services. To enhance healthcare system security, we propose a real-time anomaly detection model, as illustrated in Fig. 5.1. The model consists of two primary components: Medical Devices and Edge Computing.

1- Medical devices: This component represents the data collection process involving devices, such as wearables and medical sensors. We assume the collected data is encrypted using a lightweight and efficient encryption algorithm to ensure confidentiality. However, during transmission to the edge layer, attacks may compromise the integrity and availability of the ciphertext.

2- Edge computing: This component plays a crucial role in data analysis and system security. In this paper, the edge computing layer was simulated using a local machine (PC), which acted as a lightweight edge node responsible for both model pretraining and real-time data stream processing. It operates in two main phases:

- Pretraining Phase: Before deployment, the model is trained on the new medical dataset, which includes both normal and anomalous data. This phase enables the model to understand typical network behavior and detect unusual activity.
- Real-Time Data Processing Phase: Once deployed, the model dynamically processes incoming data streams in real-time. Each data point is analyzed immediately after decryption, allowing instant classification as normal or anomalous. This capability ensures timely identification and response to potential threats.

The model continuously adapts by learning from new patterns, enhancing its ability to detect and predict previously unseen anomalies. This ensures robust network monitoring, enabling the system to identify and mitigate emerging threats, thereby maintaining healthcare system security and integrity.

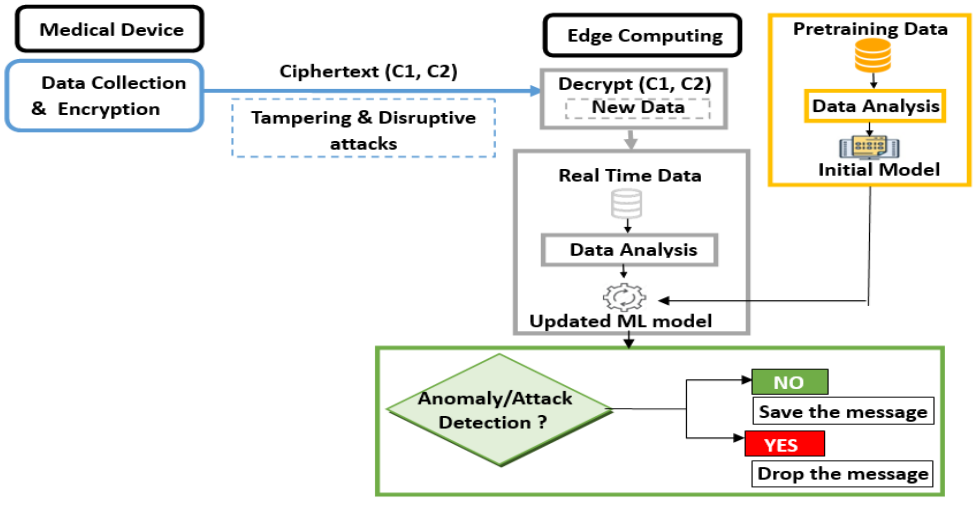


Figure 5.1 The proposed real-time anomaly prediction model.

5.3.2 The proposed Stacking-Ensemble Learning model

Based on the literature review, seven ML algorithms were selected. These models were analyzed to identify the best performers and integrated into a stacking-based ensemble learning model to enhance real-time prediction accuracy and efficiency.

1) ML selected algorithms: to evaluate the performance of diverse learning strategies in anomaly detection, we selected seven machine learning models widely adopted in the literature for their effectiveness in classifying and predicting anomalies.

- K-Nearest Neighbors (KNN): A simple, effective method for pattern detection, chosen for its ability to classify data based on proximity [142].

- Support Vector Machine (SVM): A robust classifier for high-dimensional data, selected for its effectiveness in separating complex patterns [141].

- Logistic Regression (LR): A straightforward binary classifier, preferred for its simplicity and interpretability in distinguishing anomalies [143].

- Random Forest: An ensemble model that reduces overfitting, chosen for its accuracy and reliability in classification tasks [139].

- Isolation Forest (IF): An unsupervised algorithm ideal for anomaly detection, selected for its efficiency with high-dimensional data [143].

- XGBoost: A high-performance gradient boosting method, chosen for its ability to handle large datasets and complex tasks [138].

- ANN: A powerful model for non-linear data, selected for its capability to detect intricate attack patterns [140].

2) Stacking-ensemble learning: our proposed ensemble model uses a stacking-based methodology [34] to improve intrusion detection system performance by leveraging the strengths of multiple ML algorithms. The model integrates three base learners, XGBoost, Random Forest, and ANN, with XGBoost serving as the meta-learner to refine and optimize final predictions. Fig.5.2 illustrates the stacking ensemble framework.

The base learners were selected based on their demonstrated effectiveness during evaluation (see Section 4.C). XGBoost excels at modeling non-linear relationships and addressing

misclassifications through iterative refinement. Random Forest enhances robustness with its bagging-based approach, reducing variance and ensuring stability. ANN complements these models by capturing intricate, non-linear patterns, improving the ensemble's ability to differentiate between normal traffic and various attack types. These algorithms consistently delivered high accuracy, precision, recall, and F1-scores, along with strong AUC values.

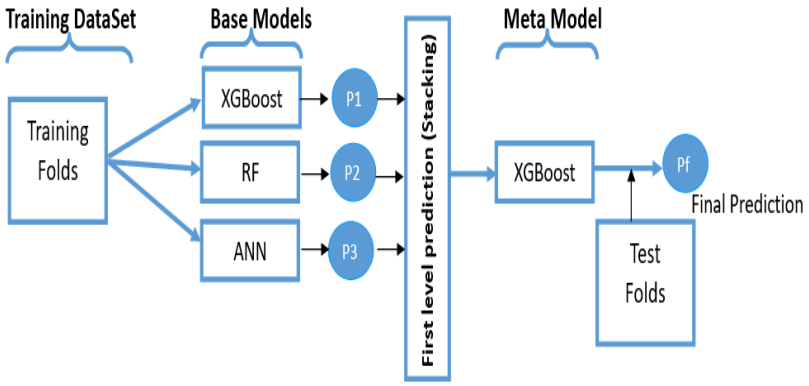


Figure 5.2. Stacking ensemble learning algorithm.

They also exhibited faster testing times compared to other algorithms like SVM and KNN, which, despite acceptable performance, were computationally expensive for real-time detection.

In the stacking framework, the outputs from the base learners are passed to the meta-learner (XGBoost), which combines their predictions to produce the final classification. Each base learner is independently trained, and its predictions are used as input features for the meta-model. This architecture enables the meta-learner to mitigate individual model weaknesses and leverage their combined strengths for more accurate predictions, as detailed in Algorithm 5.1.

By integrating the strengths of XGBoost, Random Forest, and ANN, the proposed stacking ensemble model provides a reliable and efficient solution for anomaly detection, capable of detecting a wide range of attacks while remaining suitable for real-time deployment.

5.4 Experiments

This section outlines the data analysis process, as depicted in Fig. 5.3. It begins with a description of the datasets used, followed by data pre-processing steps, attack generation methods, and evaluation metrics for assessing the performance of the machine learning (ML) algorithms and the proposed stacking model. Finally, the results are presented and discussed.

Algorithm 5.1: Ensemble Stacking Model With Multiple Base Models and K-Fold Cross-Validation

***Input**:* Dataset features X, numerical and categorical features from the UNSW-NB15 dataset/Medical dataset with attacks.
Target variable y: attack labels indicating normal or various attack types.

Step 1: Select a K-fold split of the dataset.

Step 2: Select M base models.
Base Models: Define M = {M_1, M_2, M_3}
M_1: XGBoost;
M_2: Random Forest;
M_3: Artificial Neural Network (ANN).

Step 3: Train Base Models:

For each base model $M_i \in M$:

Evaluate using K-Fold Cross-Validation.

Store the out-of-fold predictions for each instance.

Train M_i on the full training set (X_{train}, y_{train}) for final use.

Step 4: Train meta-learner*:*

Combine the out-of-fold predictions from all base models into a new feature matrix P={P_1,P_2,P_3}, where:
P_1,P_2,P_3 are predicted from M_1, M_2, M_3 respectively.

Step 5: Train the meta-learner (XGBoost) using the combined feature matrix P and the corresponding attack labels y_{train}.

Output: The evaluation metrics & the predicted attack classes ($\hat{y}$) for each instance in real-time data.

The experiments were conducted on a system with an Intel(R) Core(TM) i7-8650U CPU @ 1.90 GHz, 16 GB of RAM, and Windows 10 (64-bit). All tasks, including model implementation and feature engineering, were performed using Python 3 within the Anaconda environment. Data transmission was simulated using an Arduino, representing the medical device, while the edge computing component was executed on the machine running the Python code.

To ensure optimal model performance, hyperparameters were meticulously selected and fine-tuned, as detailed in Table 5.1.

5.4.1 Datasets description

In this paper. we have used two public datasets : The UNSW-NB15 dataset [137] and the Behavioral Risk Factor Surveillance System (BRFSS) dataset for 2015 [145]. In this section. we describe both datasets and their pre-processing phase.

1- UNSW-NB15 Dataset: the UNSW-NB15 dataset [137], introduced by the Australian Centre for Cyber Security (ACCS), provides a modern representation of synthetic network traffic, including

normal and abnormal activities. It contains 2.5 million records, with one normal class and nine attack categories: Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode, and Worms. The dataset is organized into six feature groups (flow, basic, content, time, additional generated, and labeled features), comprising 49 features in total [137].

For this study, a 10% cleaned subset of the UNSW-NB15 dataset, consisting of 175,341 training records and 82,332 test records, was used. The dataset includes 47 features with numeric, nominal, and categorical data types labeled for both binary and multi-class classification. Fig.5.4 depicts the distribution of each attack type in the training and testing sets.

2- Medical Dataset: publicly available medical datasets incorporating anomalies and simulated attacks are scarce. While some datasets, such as heart rate monitors, exist, they are limited in scope and lack comprehensive medical data or diverse attack types. The WUSTL-EHMS-2020 dataset [70], containing approximately 16,000 records, includes IoMT-specific attacks but is small and lacks diversity in attack scenarios.

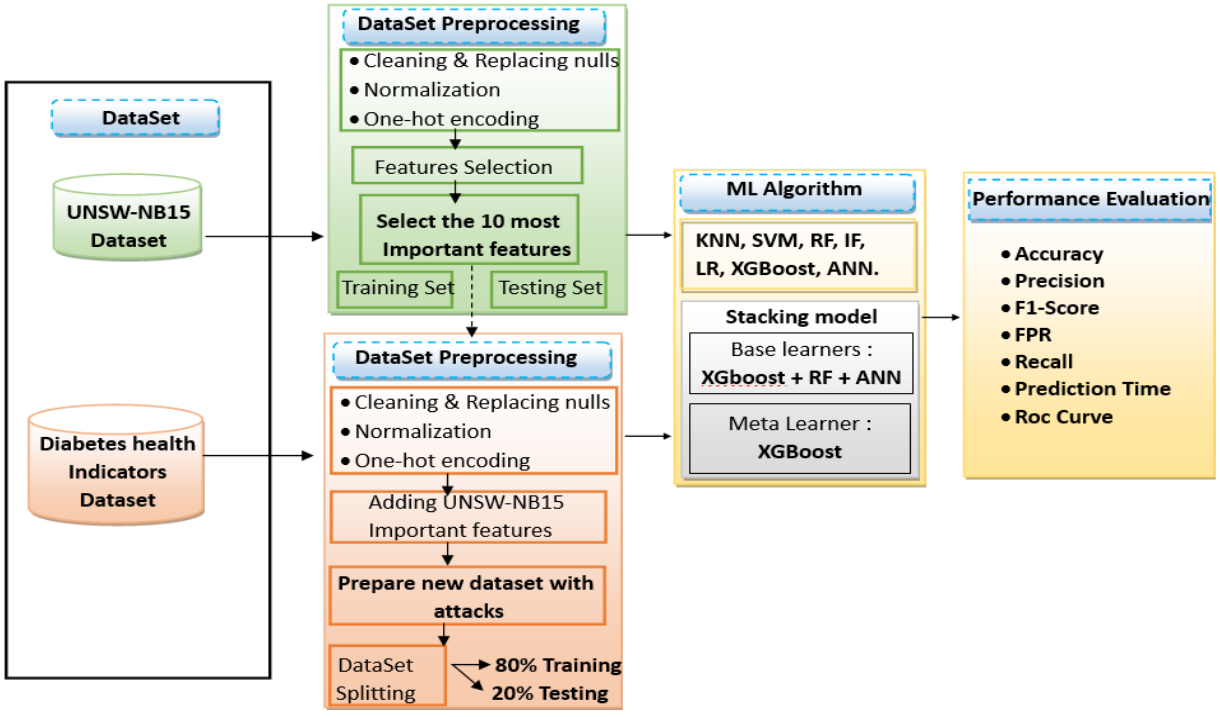


Figure 5.3 The workflow of the proposed methodology for anomaly detection in IoMT

Table 5.1 The hyperparameter values of the analysed ML models

Model	Hyperparametres
XGBoost	n_estimators=500, learning_rate=0.01, max_depth=5, min_samples_split=8, min_samples_leaf=4, subsample=0.8, random_state=42
RF	n_estimators=200, max_depth=15, min_samples_split=10, min_samples_leaf=5, max_features='sqrt', random_state=42
LR	random_state=42, max_iter=1000, solver='saga', penalty='l2', C=1.0
ISOF	contamination=0.6, random_state=42
KNN	n_neighbors=3, weights='distance', metric='minkowski'
ANN	hidden_layer_sizes=(100, 50, 20), max_iter=1000, random_state=42, learning_rate_init=0.001, activation='relu'
SVM	kernel='rbf', probability=True, random_state=42, C=5.0, gamma='scale'
Stacking model	(n_estimators=100, max_depth=5, learning_rate=0.01, random_state=42), cv=5

To address these limitations, we modified the BRFSS dataset for 2015, which contains physiological medical data. The BRFSS [145] is an annual health survey conducted by the CDC, collecting responses from over 400,000 Americans on health behaviors, chronic conditions, and preventive services. It includes 253,680 records and 22 features representing various health indicators, such as lifestyle choices, physical conditions, and medical history.

3- Data pre-processing: data pre-processing is crucial to ensure clean, consistent, and suitable datasets for anomaly and attack detection. This phase involved cleaning, transforming, and organizing the data to improve its quality and compatibility with ML algorithms.

- Handling Missing and Invalid Values: Missing or invalid values were replaced with appropriate substitutes to preserve data integrity.
- Encoding Categorical Features: Categorical features were converted into numerical representations using ordinal encoding and one-hot encoding.

Ordinal encoding assigned unique integer values to each category, while one-hot encoding created binary vectors to represent distinct categories without introducing unintended ordinal relationships.

- Data Normalization: Normalization was applied to scale features, particularly for algorithms like SVM, LR, ANN, and KNN, which are sensitive to input feature scales. Min-Max Scaling was used to rescale features to a range of 0 to 1 using the formula:

$$X_{new} = \frac{(X_i - X_{min})}{(X_{max} - X_{min})}, \qquad (1)$$

where X_i is the original feature value; and X_{min} and X_{max} are the minimum and maximum values of the feature, respectively.

- Feature Selection: XGBoost was employed for feature selection on the UNSW-NB15 dataset due to its ability to handle numerical and categorical features while capturing complex, non-linear patterns. Feature importance scores were calculated to identify and retain the most impactful features, reducing dimensionality and improving model efficiency. For the medical dataset, all 22 physiological features were retained, as any could be targeted by attacks like falsification.

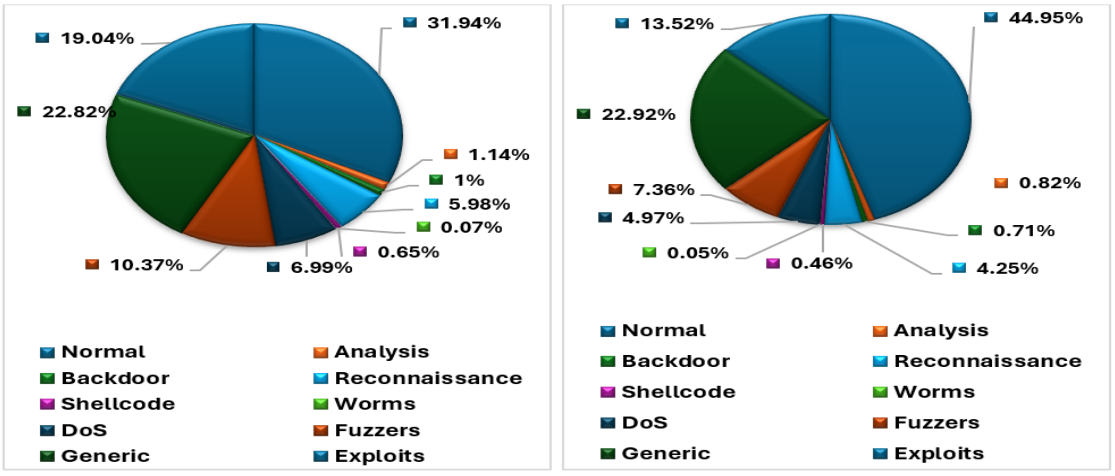


Figure 5.4 Data Distribution by normal and attack types in the UNSW-NB15 Dataset: (a) Training Set and (b) Testing Set.

To address the significant class imbalance observed across different attack types, we applied the Synthetic Minority Over-Sampling Technique (SMOTE) to the training set. This approach was used to artificially generate new samples for under-represented classes, helping to improve the learning capacity of the model, especially for minority attack categories such as Worms and Shellcode.

5.4.2 The new medical dataset with attacks

The new medical dataset for anomaly detection was created by drawing inspiration from the UNSW-NB15 dataset. Attack scenarios were generated and incorporated into the dataset to simulate real-world threats, ensuring a comprehensive foundation for evaluating intrusion detection systems.

1- UNSW-NB15 Attacks selection: the original goal of the BRFSS (Behavioral Risk Factor Surveillance System) dataset is diabetes prediction, in this paper, we restructured it to simulate cybersecurity attack scenarios within healthcare data. Guided by the UNSW-NB15 dataset, we evaluated attack types for relevance to our case study, as illustrated in Table 5.2.

Attacks like Backdoor, Analysis, Generic, and Reconnaissance, which primarily impact data confidentiality, were excluded as they fall outside our scope. We retained normal data and attack types affecting data integrity and availability, which are critical in healthcare settings. To enhance the BRFSS dataset, we integrated the 10 most relevant features from UNSW-NB15 (illustrated in Fig. 5.5) and introduced new features for simulating network attacks. Normal data was used as a baseline, with features systematically modified to simulate attacks inspired by UNSW-NB15.

Table 5.2 Attacks type description in UNSW-NB15 dataset

Attack Type	**Description**	**Affected Services**
DoS	Overloads network services	**Availability**
Backdoor	Gains illegal system access	Confidentiality, integrity
Analysis	Probes for application vulnerabilities	Confidentiality
Exploits	Exploits network vulnerabilities	**Integrity, Confidentiality**
Fuzzers	Tests for system weaknesses	**Integrity, Availability**
Generic	Breaks cryptographic systems	Confidentiality, integrity
Reconnaissance	Gathers network information	Confidentiality
Shellcode	Executes malicious code	**Integrity**
Worms	Spreads self-replicating malware	**Availability, Integrity**

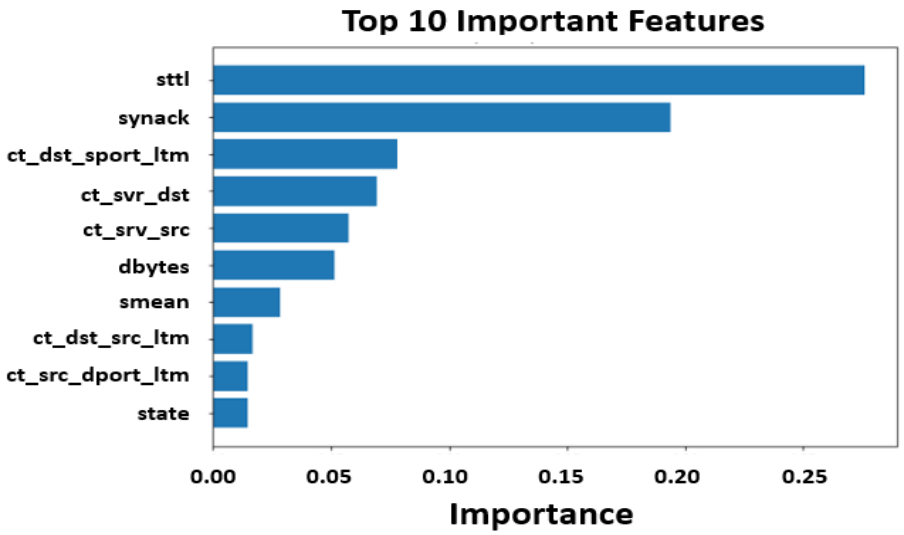


Figure 5.5 The most ten important features on the UNSW-NB15 dataset.

2- Attacks generation: to improve dataset realism, we focused on two critical healthcare threats: falsification attacks and Denial of Service (DoS) attacks. Falsification attacks compromise data integrity by altering or injecting false information, while DoS attacks disrupt service availability by overwhelming network resources. Since UNSW-NB15 lacks falsification attacks and has limited DoS samples, we enriched our dataset with realistic instances of these attacks.

A real-world-inspired scenario was designed, simulating data transmission from an Arduino (i.e., medical device) to a laptop (i.e., edge computing system). For falsification attacks, Ettercap was used to intercept and modify encrypted medical data during transmission, simulating tampering with sensitive information. For DoS attacks, HPING3 generated high-volume traffic floods (e.g., ICMP, TCP SYN, UDP floods, etc.), overwhelming network resources and disrupting communication. These additions provide critical examples of data integrity breaches and resource-based disruptions, enhancing the dataset's ability to reflect real-world medical network threats.

3- New medical dataset for anomaly detection: the new medical dataset integrates patient health data with network anomaly features and simulated attack scenarios, offering a comprehensive resource for evaluating anomaly detection systems in healthcare. It contains 253,680 rows, each representing normal activity or an attack, with 32 features blending medical and network-related attributes.

- Medical Features: 22 indicators (e.g., cholesterol, blood pressure, BMI) from the original BRFSS dataset, retained to reflect real-world healthcare scenarios.
- Network Features: 10 relevant features from UNSW-NB15 (see Fig. 5.5), were selected for their importance in predicting attacks that harm data integrity and availability.

The dataset includes six attack types alongside normal traffic; Normal activity accounts for 40% of the dataset, while the remaining 60% comprises various attacks: Falsification attacks (20.3%), which represent data integrity breaches by manipulating encrypted medical information during transmission; Denial of Service (DoS) attacks (15%), which simulate resource exhaustion and communication disruptions; Fuzzers (11%), which inject random data to exploit vulnerabilities; Exploits (12%), targeting system weaknesses for unauthorized access; Worms (1%), representing self-replicating malware; and Shellcode (1%), involving malicious code execution. Attack distributions were inspired by UNSW-NB15, with adjustments to emphasize critical healthcare threats like falsification and DoS.

This dataset provides a unique combination of medical data and network anomaly scenarios, offering a valuable resource for developing robust anomaly detection systems tailored to secure healthcare networks against real-world threats.

4- Evaluation metrics: the evaluation metrics for the machine learning models were derived from the confusion matrix, as detailed in Table 3. The confusion matrix organizes the four possible classification outcomes in a binary classifier: True Positive (TP), where the model correctly identifies attacks; True Negative (TN), where it correctly classifies benign data; False Positive (FP), where benign data is incorrectly classified as an attack; and False Negative (FN), where an attack is incorrectly classified as benign, potentially leading to undetected threats. In this study, several standard evaluation metrics were used to assess model performance, as outlined in Table 5.4. Additionally, training and testing times were measured for each model to evaluate computational efficiency, which is critical for real-time anomaly detection in healthcare applications where rapid decision-making is essential.

In this paper, reliability refers to the consistency and robustness of a model's performance across a wide range of attack categories and scenarios. Efficiency refers to the model's ability to process and classify data quickly, which is especially important for real-time anomaly detection.

Table 5.3 Confusion Matrix.

	Predicted Normal	**Predicted Attack**
Attack actual	FN	TP
Normal actual	TN	FP

Table 5.4 Evaluation Metrics for Model Performance

Metric	**Description**	**Formula**
Accuracy	Measures overall correctness.	$\frac{(TP + TN)}{Total}$
Precision	Identifies true attacks precisely.	$\frac{TP}{(FP + TP)}$
False Positive Rate (FPR)	Tracks misclassified normal instances.	$\frac{FP}{(FP + TP)}$
Recall	Captures all true attacks.	$\frac{TP}{(FN + TP)}$
F1 score	Balances precision and recall.	$\frac{2 * (Precision * Recall)}{(Precision + Recall)}$
ROC-AUC Score	Assesses model's separability.	

5.4.3 Performance Evaluation and Discussion

The performance evaluation was conducted in two phases: the pretraining phase and the real-time prediction phase.

1- Pretraining phase: during the pretraining phase, models were trained and validated on the UNSW-NB15 dataset and a new medical dataset for anomaly detection, as shown in Fig.5.6 (a) and (b), respectively. The results revealed significant improvements in model performance on the medical dataset compared to UNSW-NB15. XGBoost achieved the highest accuracy, improving from 93.81% on UNSW-NB15 to 97.17% on the medical dataset. Random Forest and ANN also showed notable improvements, with their accuracy increasing from 93.78% to 96.38% and from 92.21% to 93.41%, respectively. These results validated the selection of XGBoost, Random Forest, and ANN as base models for the proposed stacking model, with XGBoost serving as the meta-learner.

The stacking model outperformed all other models, achieving 98.02% accuracy on the medical dataset compared to 94.32% on UNSW-NB15. SVM and Logistic Regression showed moderate improvements, while KNN experienced a slight decline in performance due to the inclusion of falsification attacks, which disrupted proximity-based relationships. Isolation Forest consistently

performed poorly, reflecting its unsupervised nature and inability to effectively capture structured patterns in the datasets.

To further evaluate model performance, ROC curves and AUC values were analyzed (see Fig.5. 7). XGBoost, Random Forest, and ANN achieved AUCs of 0.99, 0.99, and 0.98, respectively, on both datasets, confirming their ability to rank anomalies accurately and handle complex features. The stacking model achieved an AUC of 0.99, leveraging the complementary strengths of its base models for enhanced anomaly detection. In contrast, models like KNN, SVM, and Logistic Regression exhibited slightly lower AUC values, while Isolation Forest recorded the lowest AUC of 0.76, reflecting its limited ability to handle structured datasets.

The evaluation of model accuracy for predicting specific attack types across the two datasets highlighted the strengths of the proposed stacking model, as displayed in Fig. 5.8. It consistently achieved high accuracy across all attack types, particularly on the new medical dataset, where it excelled in detecting the falsification attack. KNN also demonstrated strong accuracy in identifying various attacks, though its high testing time limited its real-time applicability. Random Forest, ANN, and XGBoost consistently delivered robust accuracy across both datasets. In contrast, Logistic Regression and SVM showed moderate performance, with lower accuracy on complex attack types like Exploit.

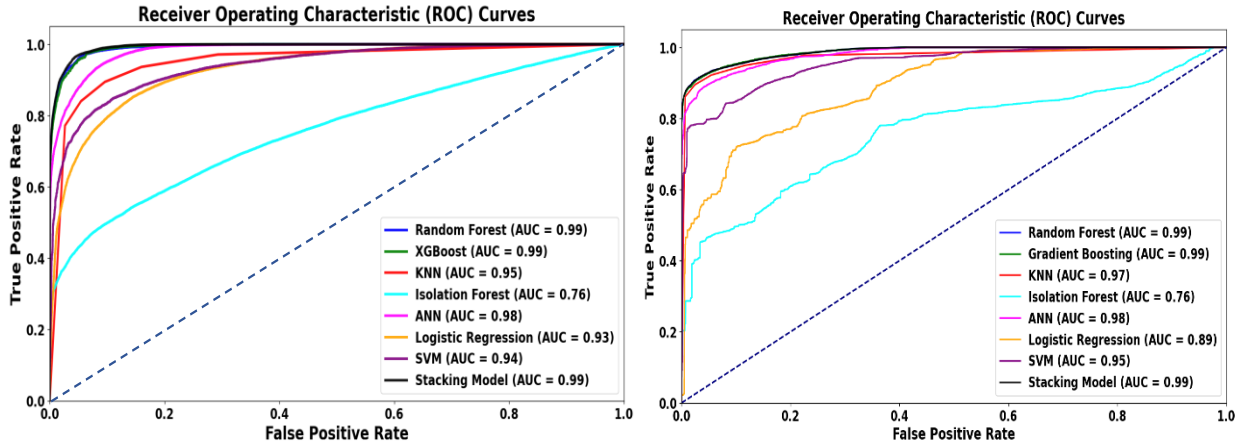
	XGBoost	RF	LR	KNN	IF	ANN	SVM	Proposed
Accuracy	0,9381	0,9378	0,8047	0,9317	0,5094	0,9221	0,8401	0,9432
Precision	0,9408	0,9425	0,7992	0,9328	0,3116	0,9415	0,8115	0,9502
Recall	0,9374	0,9358	0,7794	0,9206	0,4994	0,9159	0,8001	0,9397
F1-Score	0,9391	0,9391	0,7892	0,9267	0,3838	0,9285	0,8058	0,9449
FPR	0,0372	0,036	0,23	0,0547	0,0086	0,0923	0,079	0,0254

(a)

	XGBoost	RF	LR	KNN	IF	ANN	SVM	Proposed
Accuracy	0,9717	0,9638	0,8874	0,9081	0,4703	0,9341	0,9015	0,9802
Precision	0,9685	0,9628	0,8772	0,9202	0,2617	0,9552	0,8548	0,9846
Recall	0,9725	0,9597	0,8074	0,8981	0,4703	0,9343	0,8891	0,9722
F1-Score	0,9705	0,9612	0,8409	0,9090	0,3363	0,9446	0,8716	0,9784
FPR	0,0365	0,0293	0,2045	0,1263	0,0041	0,0934	0,057	0,021

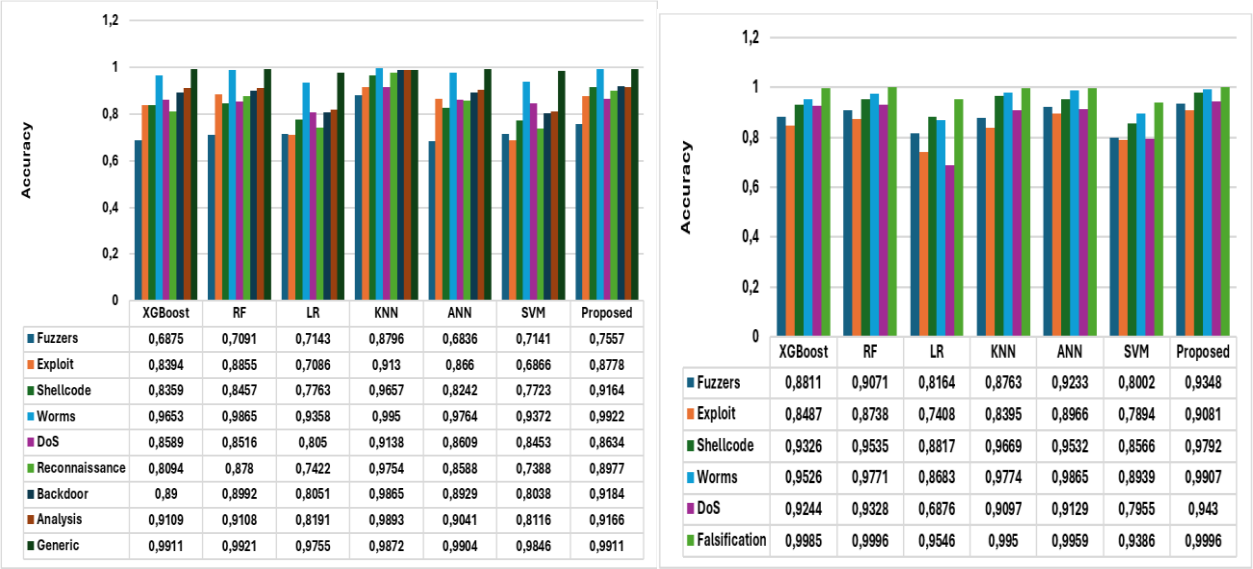
(b)

Figure 5.6 Performance analysis of the ML anomaly prediction models running on: (a) UNSW-NB15 dataset, (b) the new medical dataset for anomaly Prediction



(a) (b)

Figure 5.7 Roc Curve of the ML anomaly prediction models running on: (a) UNSW-NB15 dataset, (b) the new medical dataset for anomaly prediction.



(a) (b)

Figure 5.8 The overall performance of ML models based on different types of attacks running on: (a) UNSW-NB15 dataset, (b) the new medical dataset for anomaly prediction.

Table 5.5 Training and Testing time of LM anomaly prediction models.

	New medical dataset for anomaly detection		**UNSW-NB15 dataset**	
Model	Training time (s)	Testing time (s)	Training tine (s)	Testing time (s)
RF	12.1688	0.2473	8.7314	0.2338
XGBoost	62.8170	0.0327	41.9799	0.1548
KNN	0.9465	59.3154	0.3626	38. 0637
ISOF	1.3206	0.2821	1.0107	0.1428
ANN	110.4858	0.0298	78.0247	0.0396
LR	0.6420	0.0051	0.3793	0.0031
SVM	1059.96	54.5325	901.3636	32. 6092
Proposed	64.22	0.3016	52.657	0.3016

Finally, the computational efficiency of the models was analyzed through training and testing times (see Table5. 4). Testing time is critical for real-time applications, and XGBoost, ANN, and Random Forest stood out for their consistently low testing times across both datasets, making them practical choices for real-time anomaly prediction. The stacking model also demonstrated competitive testing times, combining efficiency with enhanced performance. Conversely, KNN and SVM exhibited significantly higher testing times, limiting their suitability for real-time scenarios. This higher computational cost was a key reason for excluding KNN and SVM from the stacking model, as the focus was on achieving a balance between speed and reliability.

2- Real-time prediction phase: in this phase, we assess the real-time prediction capabilities of machine learning models on medical messages from a newly developed medical dataset designed for anomaly detection. A total of 100 sequential messages were tested, comprising 25 normal messages and 75 anomalies distributed across six attack types: 10 Fuzzers attacks, 10 Exploit attacks, 10 Worm attacks, 10 Shellcode attacks, 15 DoS attacks, and 20 Falsification attacks. These messages were transmitted within the designed real-world-inspired scenario to replicate real-world conditions. For Falsification and DoS attacks, the attacks were dynamically generated during data transmission to mimic real-time scenarios where data streams are intercepted, altered, or overwhelmed. The remaining attacks were pre-prepared with attack values inspired by the UNSW-NB15 dataset and transmitted through the network. This comprehensive setup provided a realistic simulation of both normal and anomalous data exchanges, enabling a thorough evaluation of each model's ability to predict anomalies in real-time.

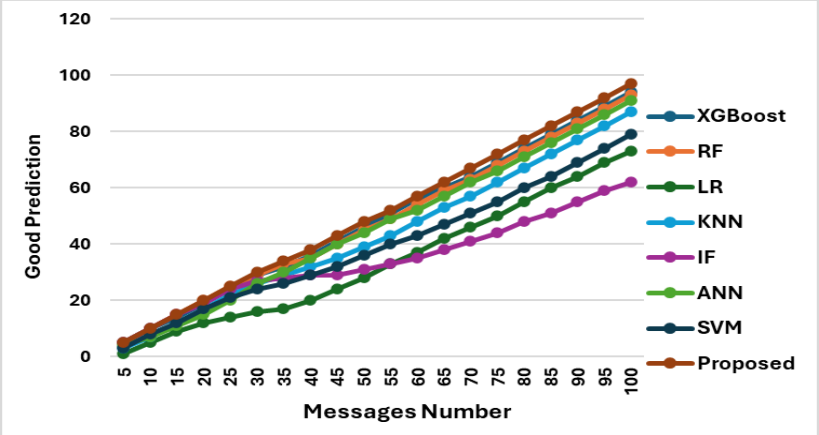


Figure 5.9 Number of good predicted messages by ML models in Real-time.

Fig. 5.9 illustrates the performance of the machine learning models in real-time binary classification, distinguishing between normal and anomalous data across the 100 messages. The proposed stacking model outperformed all others, correctly predicting 97 messages. This exceptional performance underscores its ability to integrate the strengths of its base models, ensuring accurate detection of both normal and anomalous patterns. XGBoost followed closely with 94 correct predictions, demonstrating robust handling of both normal and attack data. Similarly, Random Forest achieved 93 correct predictions, highlighting its reliability in real-time anomaly detection. KNN and ANN also delivered strong results. KNN excelled in identifying normal data, and accurately predicting all 25 normal messages, while ANN maintained consistent performance across all message types. These results position both models as promising candidates for real-time anomaly detection. In contrast, SVM struggled with predicting attack types, reflecting its limitations in handling diverse patterns. Logistic regression underperformed, correctly predicting only 73 messages. Its linear nature restricts its ability to model complex, non-linear relationships, which is evident in its weaker performance with anomalies. Isolation Forest also faced challenges, accurately detecting 24 out of 25 normal messages but identifying only 36 anomalies. Its reliance on outlier detection makes it less effective for subtle or nuanced attack patterns.

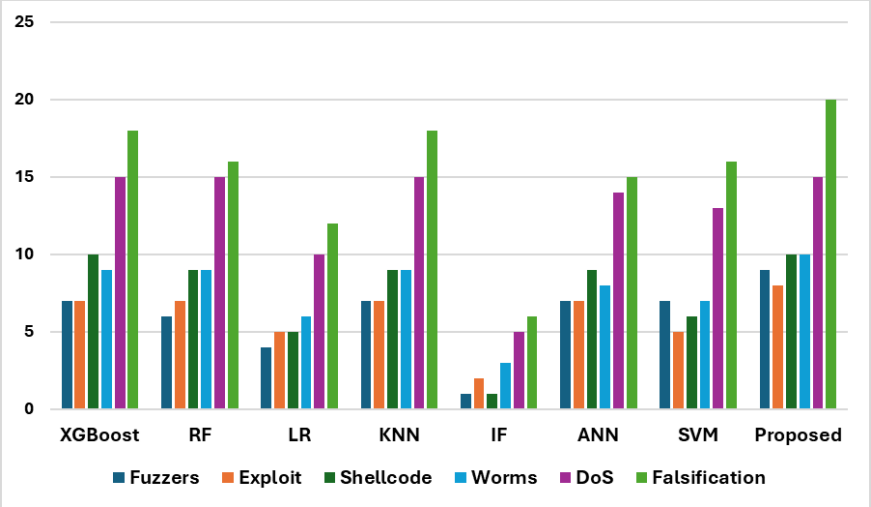


Figure 5.10 Number of correctly predicted attack types by ML models in Real-time.

For multiclass classification, the models were evaluated on their ability to predict anomalies across the six attack categories, as shown in Fig. 5.10. The proposed stacking model again emerged as the top performer, accurately detecting 9 Fuzzers, 8 Exploits, 10 Shellcodes, 10 Worms, 15 DoS attacks, and 20 Falsification attacks. Its superior performance stems from its ability to combine the strengths of its base models, enabling it to identify both straightforward and complex attack patterns effectively. XGBoost, Random Forest, and ANN also delivered robust results, demonstrating their capability to handle diverse attack types. KNN achieved prediction accuracy comparable to XGBoost and excelled in detecting closely grouped attack patterns, such as 15 DoS and 18 Falsification attacks. However, KNN's high computational cost during testing limits its suitability for real-time applications, as slower performance can hinder its effectiveness in dynamic environments. Logistic regression and Isolation Forest continued to struggle with complex attack patterns, further highlighting their limitations.

Overall, the results confirm the effectiveness of the proposed stacking model and the value of the newly developed medical dataset. During the pretraining phase, almost all the models showed better performance on the medical dataset compared to UNSW-NB15, demonstrating that the customized attack types improved the models' ability to detect anomalies more accurately. The stacking model consistently outperformed individual models, benefiting from the complementary strengths of XGBoost, Random Forest, and ANN. This trend held in the real-time prediction phase, where the stacking model successfully detected 97 out of 100 messages and achieved high accuracy across all six attack categories. These results not only highlight its robustness in complex, multiclass

scenarios but also prove its practical applicability in real-time healthcare environments. In contrast, simpler models like Logistic Regression and Isolation Forest struggled to generalize to nuanced attack patterns. These findings emphasize the importance of tailored datasets, ensemble learning, and efficient real-time processing in building reliable security systems for IoMT infrastructures.

5.5 Conclusion

This research presents a novel real-time anomaly detection model designed for Internet of Medical Things (IoMT) systems, addressing critical cybersecurity challenges through a machine learning-based approach. A new medical dataset was developed, combining physiological data from the BRFSS dataset and attack patterns inspired by the UNSW-NB15 dataset. Additionally, healthcare-relevant attacks were generated to simulate real-world anomalous scenarios in IoMT environments. The new dataset demonstrated superior effectiveness for anomaly detection, significantly improving model performance compared to the UNSW-NB15 dataset.

The proposed stacking ensemble model, integrating XGBoost as the meta-learner with Random Forest and ANN as base models, achieved outstanding results. On the new medical dataset, it attained an accuracy of 98.02%, outperforming other models' accuracy. Real-time prediction analysis further validated the model's robustness, with 97 out of 100 messages correctly classified. These findings underscore the value of the new medical dataset in enhancing anomaly detection capabilities. By incorporating healthcare-relevant attacks and leveraging key features from the UNSW-NB15 dataset, the dataset provides a realistic and challenging environment for training and testing machine learning algorithms. This study highlights the potential of ensemble learning techniques and tailored datasets to significantly advance IoMT security, offering a robust solution for real-time anomaly detection in critical healthcare systems.

This research work has a few limitations that open directions for future research. First, the dataset used includes a limited set of attack types, which may not reflect all possible or newly emerging threats. A possible future direction could be to expand the dataset with more recent attacks or to explore reinforcement learning techniques that allow the model to adapt dynamically to unknown or evolving attack patterns. Second, the evaluation was done only on a custom medical dataset, which limits the ability to assess how well the models perform in other environments. Future studies could involve evaluating the models on other public benchmark datasets to better assess their generalizability.

ACKNOWLEDGMENT

The authors would like to thank Dr. Franjieh El Khoury for her valuable comments and proofreading of this paper.

This work was funded by the Natural Sciences and Engineering Research Council of Canada (NSERC), Prompt, Flex Group, and ISAME

CHAPITRE 6 ARTICLE 3:REINFORCEMENT LEARNING FRAMEWORK FOR ADAPTIVE AUTHENTICATION AND ACCESS CONTROL IN HEALTHCARE SYSTEMS

Hadjer Goumidi and Samuel Pierre (Senior Member, IEEE)

Department of Computer and Software Engineering, Polytechnique Montréal, Montreal, QC H3T 1J4, Canada

E-mail: hadjer.goumidi@polymtl.ca; samuel.pierre@polymtl.ca;

Revue : Soumis pour publication dans le journal Engineering Applications of Artificial Intelligence, 03 november 2025

Abstract

The shift toward digital healthcare systems introduces pressing challenges around ensuring strong security without compromising user accessibility. Conventional static authentication and rule-based access control often fall short in adapting to the dynamic, risk-sensitive context of healthcare environments. To address this gap, we present a novel dual-agent framework leveraging reinforcement learning (RL) to secure both authentication and access control processes in e-health systems. The first agent applies risk-based adaptive authentication, adjusting its decision based on contextual behavioral features. The second agent implements behavior-driven access control by continuously evaluating user activity and enforcing dynamic policy responses to anomalies. We repurpose the insider threat dataset developed by the Computer Emergency Response Team (CERT) to reflect medical roles and behaviors, enabling realistic simulation of healthcare interactions. Five reinforcement learning models, Deterministic Strategy (DS), Deterministic Exploration Strategy (DES), Deep Q-Network (DQN), and Double Deep Q-Network (DDQN), are trained and assessed using key performance metrics, with a particular focus on the G-Mean to account for class imbalance. Among them, DQN emerges as the most effective model, balancing high accuracy (97.45% for authentication scenario and 92.95% for access control scenario), sensitivity to rare events, fast convergence, and decision stability. Its performance is further validated against five machine learning baselines, where DQN consistently outperforms, especially

in detecting minority class anomalies (90.35% for authentication scenario and 78.45% for access control scenario). These results highlight the potential of reinforcement learning as a scalable and autonomous solution for securing next-generation healthcare systems.

Keywords: Reinforcement learning, risk-based authentication, dynamic access control, anomaly detection, e-Health security.

6.1 Introduction

Modern healthcare systems are undergoing a rapid digital transformation aimed at improving the efficiency, scalability, and accessibility of medical services [146]. This shift is largely driven by the integration of intelligent technologies into clinical workflows, including electronic health records (EHRs), wearable biosensors, telemedicine platforms, and Internet of Things (IoT) devices. Collectively referred to as e-Health, these systems facilitate real-time patient monitoring, remote diagnosis, and personalized treatment, making healthcare more proactive and data-driven [147]. Particularly for patients with chronic conditions or those in remote areas, e-Health dramatically reduces hospital dependency and enhances the continuity of care.

Despite their benefits, e-Health systems also introduce critical security and privacy challenges. The sensitive nature of health data, ranging from biometric identifiers to mental health records, makes these systems highly vulnerable to cyberattacks, data breaches, identity theft, and misuse [148]. Beyond confidentiality, healthcare operations depend on the integrity and availability of data to ensure patient safety. A single unauthorized access or denial-of-service attack can lead to life-threatening consequences [149]. Therefore, robust cybersecurity mechanisms are indispensable. Two foundational pillars in protecting digital health ecosystems are authentication (verifying user legitimacy) and access control (defining who can do what, and under which conditions). These mechanisms ensure that only trusted entities can access or modify critical medical information or system functions [148], [149], [150].

Conventional solutions for authentication and access control often fall short in the dynamic, decentralized, and heterogeneous nature of modern e-Health environments. Static models such as Role-Based Access Control (RBAC) [85] offer simple implementation but lack flexibility in adapting to changing contexts, user behaviors, or system states. Blockchain and smart contract-based approaches [89] enhance decentralization and auditability but come with high computational overhead, rigidity, and limited adaptability to real-time decision contexts. On the other hand,

Machine Learning (ML)-based solutions [100] improve adaptability but often rely on offline training, static datasets, and do not support sequential learning from ongoing system interactions. These models are typically reactive rather than proactive, failing to evolve in real-time as new threats or behavioral patterns emerge. Furthermore, most solutions treat authentication and access control as disjoint components, ignoring the interdependencies between identity verification and privilege assignment.

To overcome these limitations, we propose a novel security framework for e-Health systems that leverages Deep Reinforcement Learning (DRL) to manage authentication and access control simultaneously. At the core of this framework are two intelligent agents trained using advanced Deep Q-Learning architectures, capable of learning optimal security policies through interaction with their environment. Unlike traditional systems, our approach dynamically adapts to contextual features such as access frequency, resource sensitivity, historical behavior, and anomaly patterns, enabling personalized, context-aware decisions. The agents continuously update their policies based on feedback from the environment, allowing the system to evolve in real-time without requiring manual reconfiguration. By integrating both authentication and access control into a unified, learning-based architecture, the proposed model provides robust, scalable, and adaptive protection for next-generation e-Health infrastructures.

The key contributions of this paper are as follows:

1) We develop a novel dual-agent framework for healthcare cybersecurity, introducing separate reinforcement learning-based agents for both risk-aware authentication and contextual access control.

2) We introduce a risk-based adaptive authentication system that tailors challenge levels to the -contextual threat level of each access attempt, enhancing both security and usability.

3) We propose a dynamic, behavior-driven access control model that evaluates user legitimacy based on real-time activity patterns, learned roles, and anomaly detection.

4) We repurpose and semantically adapt the CERT insider threat dataset [151] into a healthcare-specific behavioral context, enriching it with medically relevant roles and usage features.

5) We perform an extensive evaluation comparing five RL models and multiple ML baselines across training, testing, and deployment scenarios, demonstrating the superiority and robustness of the proposed DQN-based agent.

To the best of our knowledge, this paper introduces the first unified framework that leverages reinforcement learning to independently govern both authentication and access control in e-health systems based on real-time user behavior. Unlike traditional static policies or ML-based solutions, our dual-agent design continuously learns optimal security actions in dynamic healthcare environments. Furthermore, we uniquely adapt and semantically restructure a large-scale insider threat dataset (CERT) into a healthcare-specific behavioral domain, enabling realistic simulation and evaluation of human-centric security policies.

This paper is organized as follows. Section II reviews related works, with a focus on authentication and access control approaches that utilize smart contracts, machine learning algorithms, and reinforcement learning models. Section III presents the proposed methodology, detailing the design of the authentication and access control agents. Section IV outlines the experimental setup, including the transformation of the CERT dataset into a medical behavioral context, and reports the evaluation results of five RL models and several ML algorithms across both authentication and access control scenarios. Finally, Section V concludes the paper and outlines future research directions.

6.2 Related Work

As healthcare systems continue to evolve toward digital and interconnected environments, securing access to sensitive medical data has become a top priority. Authentication and access control are two foundational components in safeguarding electronic health records (EHRs), Internet of Medical Things (IoMT) devices, and cloud-based health platforms. This section reviews existing work on secure access management in healthcare by examining various techniques used across the literature.

Traditionally, healthcare systems have employed Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) to manage access based on user roles or specific attributes [85], [86], [87]. Although these approaches are widely implemented and straightforward, they remain fundamentally rigid, relying on static, predefined policies that fail to accommodate changing risk levels or adapt to real-time operational contexts.

Efforts to decentralize access control led to the exploration of blockchain and smart contracts. For instance, the SmartAccess model [88] and Fortified-Chain system [89] used smart contracts to automate access decisions based on ABAC and IoMT data, respectively. Similarly, Haritha et al. [90] applied multilevel security rules to support hierarchical user structures. Beyond these, Ying et al. [91] proposed a fine-grained electronic health record (EHR) sharing mechanism on the cloud using attribute-based encryption, offering enhanced privacy through user-defined cryptographic policies. Zhang et al. [92] developed an attribute-based, decentralized access system that leverages blockchain to ensure the auditability and integrity of access logs. Nguyen et al. [93] further contributed by building a trust-driven smart contract model for EHR sharing on mobile cloud platforms, aiming to preserve user privacy and automate access control across institutions. Xu et al. [94] designed a blockchain-enabled capability-based model that emphasized fine-grained control in IoT scenarios, while Novo et al. [95] presented a scalable blockchain framework for IoT-critical systems focusing on performance and access latency. Complementary efforts such as Ancile [96] and MedRec [97] introduced frameworks for secure and decentralized health data sharing, providing patient-controlled privacy through blockchain-integrated record management.

While blockchain-based systems enhance the decentralization and security of healthcare data sharing, their access control mechanisms remain inherently static. Once deployed, smart contracts lack the flexibility to adapt to evolving behaviors, risk levels, or contextual factors without manual updates. Additionally, the computational overhead and latency of blockchain operations limit their suitability for real-time healthcare scenarios, particularly during emergencies or dynamic access contexts. These constraints highlight the need for more adaptive, intelligent access control approaches that respond to user behavior and context in real time.

To improve responsiveness, researchers have turned to machine learning techniques for adaptive access control and anomaly detection. Sangeetha et al. [98] introduced a machine learning-based secure healthcare access control system capable of detecting suspicious patterns and improving resilience against insider threats. Risk-based authentication models, such as the one proposed in [99], employed decision trees and neural networks to evaluate contextual variables and adjust authentication challenges dynamically. The rise of explainable AI in healthcare security, as explored in [100], further enhances trust in such systems by providing transparency and interpretability in anomaly detection outcomes. However, ML-based systems typically function in an advisory capacity and rely heavily on labeled training data. Their reactive nature, lack of

autonomous decision-making, and limited enforcement capabilities often make them insufficient in highly dynamic or adversarial settings.

Reinforcement learning has emerged as a promising paradigm capable of addressing these shortcomings. Unlike supervised ML models, RL agents can learn optimal decision-making strategies through direct interaction with the environment, allowing for adaptive access policies that evolve over time. RLAuth [101] demonstrated the viability of deep RL for risk-based authentication by adjusting policy strength based on environmental risk indicators. It achieved superior classification metrics and policy responsiveness compared to static or heuristic-based models. However, RLAuth focused only on authentication and did not incorporate access control mechanisms or user-role contextualization, which are critical in clinical environments where the nature of data sensitivity and urgency varies significantly across user profiles and situations.

Despite advancements in rule-based, blockchain, and machine learning frameworks, existing solutions often treat authentication and access control separately, lack real-time adaptability, and overlook contextual factors like user roles and data sensitivity. Static smart contracts are rigid, and ML models rely on labeled data and reactive decision-making. In this work, we propose a reinforcement learning-based model that jointly manages authentication and access control in a dynamic, context-aware, and real-time manner. Our approach adapts continuously to changes in environmental conditions, aligns access decisions with user roles and data sensitivity, and eliminates the rigidity of predefined rules. By addressing these limitations, the proposed model aims to enhance both security and operational efficiency in complex healthcare environments.

6.3 Methodology

This section presents the proposed model for user authentication and access control in healthcare systems using reinforcement learning. The framework combines behavioral analysis, risk evaluation, and adaptive decision-making to enhance data security.

The proposed model is a two-stage security system designed to protect access to sensitive healthcare data by integrating user behavior analysis, contextual risk evaluation, and reinforcement learning. The system is organized into two primary contexts: authentication and access control (see Fig.6.1). Each context is governed by a dedicated reinforcement learning agent and is supported by specialized modules responsible for state construction, policy validation, and agent training.

6.3.1 Authentication Context

For the authentication context, we have three key entities: Authentication Agent, Risk Engine, Authentication Manager and Authentication Buffer.

- Risk engine: the Risk Engine in the proposed model is a core component responsible for calculating a real-time risk score associated with each login attempt. This score reflects the system's confidence in the legitimacy of the authentication request, and it directly influences the feedback given to the Authentication Agent. Rather than relying solely on binary labels, the risk score captures nuanced indicators derived from both historical identity trust and contextual familiarity.

The engine operates only when invoked by the Authentication Manager, ensuring that risk evaluation is context-sensitive and event-driven rather than continuous. Its structure comprises two analytical modules: the Identity Confidence Evaluator and the Context Confidence Evaluator, which contribute to a final composite score normalized within the range [0,1].

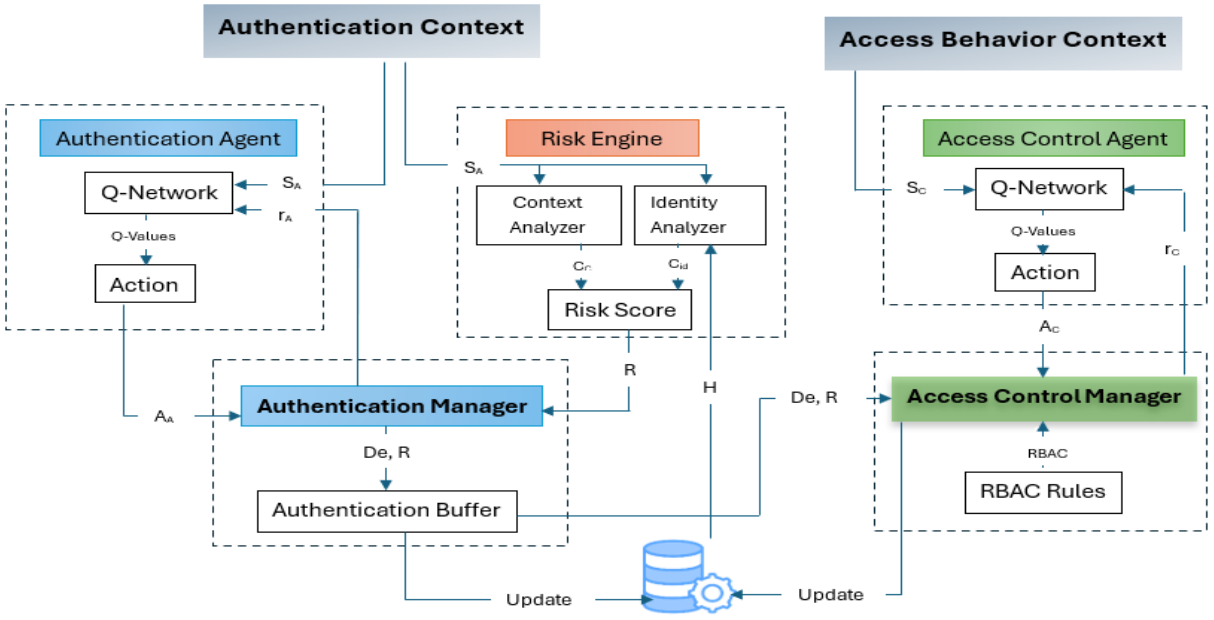


Figure 6.1 The proposed authentication and access control model.

- Identity Analyzer: this module quantifies how trustworthy the claimed identity is. It is computed using three main factors: the outcome of the most recent successful authentication, the user's historical failure rate, and the behavior during the current session (including inactivity and duration). To balance precision with interpretability, the confidence score combines a base

confidence component with a contextual adjustment that reflects session health dynamics. The identity confidence score $C_{id} \in [0,1]$ is calculated as:

$$C_{id} = \lambda_1 \cdot (C_{la} \cdot (1-H)) + \lambda 2 \cdot (\delta_a \cdot \delta_s) \quad (1)$$

where:

$C_{la} \in [0,1]$ is the confidence of the last successful authentication.

$H \in [0,1]$ is the historical failure rate, computed as the proportion of failed authentication attempts over total attempts.

$\delta_a \in [0,1]$ is the activity confidence, which decreases linearly based on user inactivity time:

- If the user stays inactive for ≤ 2 hours: $\delta_a = 1$,
- If the user stays inactive between 2 and 4 hours:

$$\delta_a = 1 - \frac{T_{idle} - 2}{2} \quad (2)$$

- If user stays inactive > 4 hours: $\delta_a = 0$.

$\delta_s \in [0,1]$ is the session confidence, reflecting the duration since last login:

- If session duration ≤ 8 hours: $\delta_s = 1$,
- If duration is between 8–12 hours:

$$\delta_s = 1 - \frac{T_{session} - 8}{4} \quad (3)$$

- If session duration > 12 hours: $\delta_s = 0$.

This formulation ensures that identity confidence remains within the [0,1] range, prioritizing recent authentication success and long-term behavioral history, while softly penalizing prolonged inactivity and extended sessions.

- Context confidence evaluator: the context confidence score C_{ctx} is a dynamic metric that quantifies the familiarity of the current access context based on the user's historical behavior. In the proposed framework, context encompasses environmental and situational features such as the device used for login, the temporal segment of access (e.g., shift-based login hours), and role-specific usage patterns. This mechanism ensures that even when the user's identity is

confidently verified, additional trust is granted only if the environmental conditions align with typical access behaviors.

To compute the context confidence, the system maintains a historical frequency table for each user, mapping previously encountered context tuples to their occurrence counts during successful authentications. Let f_{ctx} denote the number of times the current context has been observed for the user, and $MAX_{f_{ctx}}$ represent the frequency of the most encountered context. The context confidence is then defined as a normalized ratio:

$$C_{ctx} = \frac{f_{ctx}}{MAX_{f_{ctx}}} \quad (4)$$

This formulation ensures that confidence is maximized when the access context matches the most habitual pattern for the user and gradually decreases as the context deviates from their norm. The score is strictly bounded within the interval [0,1], allowing for seamless integration with other components of the risk engine. For example, a nurse accessing the system from her regular workstation during morning shift hours may yield a high C_{ctx}, whereas an attempt from an unknown terminal during off-hours would result in a significantly lower score.

This approach enables the model to balance usability with security: familiar contexts allow seamless access, while unfamiliar environments trigger heightened scrutiny or re-authentication prompts. By grounding context evaluation in empirical frequency data, the system adapts over time to evolving but legitimate behavior patterns without requiring manual rule updates.

- Risk Score evaluator: the final risk score $R \in [0,1]$ combines identity and context confidence through a weighted average:

$$R = (1 - (\mu \cdot C_c + (1 - \mu) \cdot C_{id})) \quad (5)$$

The weight μ reflects the system's relative trust in identity versus contextual consistency and can be tuned based on organizational policy.

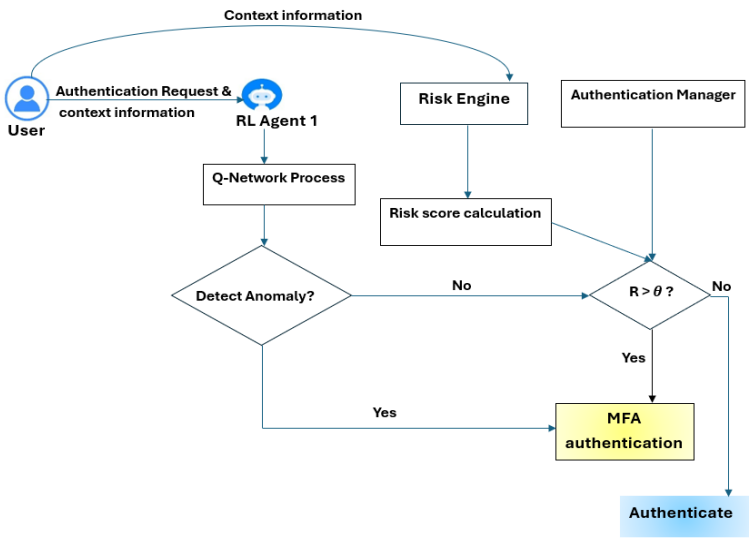


Figure 6.2 Authentication Process

- Authentication agent: The Authentication Agent is the core decision-making entity in the authentication layer, designed to autonomously determine whether a user should be granted access based on observed behavioral and contextual indicators, Fig.6.2 displays the authentication process of our agent. Implemented as a reinforcement learning agent, it continuously improves its decision policy by interacting with the environment and receiving feedback through a reward mechanism. This approach enables the agent to adapt over time to evolving patterns in user behavior, device usage, and contextual dynamics.

- State and Action: At each authentication attempt, the agent receives a structured input vector, representing the state of the system:

$\text{Auth-}s_t = [C_{la}, H, T_{session}, T_{idle}, \text{Role}, \text{Hour}]$

This vector integrates identity information (C_{la}, H), behavioral features ($T_{session}$, T_{idle}), and categorical identifiers (Role, Hour). It provides a rich representation of the current login scenario, allowing the agent to assess both behavioral norms and security relevance.

The agent outputs a binary action, either authenticate or deny, based on the current state. Once the action is executed, the Authentication Manager evaluates the outcome against the system's computed risk score and generates a reward signal. We designed our reward function to address the class imbalance issue in authentication decisions, inspired by the strategy in [101]. To enhance learning from the minority class (denial decisions), we introduce an imbalance correction factor λ.

Let:

- a = agent's action (0 = AUTH, 1 = DENY)
- a_e = expected action (based on R>θ)
- C = model's decision confidence
- R ∈ [0,1] = evaluated risk
- λ ∈ [0,1] = imbalance correction factor

Then:

$$\boldsymbol{Auth_r} = \begin{cases} 1 & if\ \ a = a_e\ and\ \ ae = 0 \\ \lambda & if\ \ a = a_e\ and\ \ ae = 1 \\ -|\ C - R\ | & if\ \ a \neq a_e\ and\ \ ae = 0 \\ -\lambda\ |\ C - R\ | & if\ \ a \neq a_e\ and\ \ ae = 1 \end{cases} \quad (6)$$

The reward function is designed to reflect both the correctness and the contextual impact of the agent's authentication decisions. When the agent's action matches the expected decision $a=a_e$, it receives a reward of +1 for low-risk (majority) cases and a weighted reward λ for high-risk (minority) cases, promoting fairness in imbalanced data. If the agent misclassifies, the penalty is proportional to the difference between its confidence C and the actual risk R. A false positive (incorrect allow) leads to a penalty of |C−R|, while a false negative (incorrect deny) incurs a stronger penalty −λ|C−R|, reflecting a greater cost on usability. This dynamic reward structure encourages precise, risk-aware decisions and improves the agent's ability to detect rare but critical anomalies.

- Deep Q-Network: The authentication agent leverages a Deep Q-Network (DQN) to approximate the Q-function, which predicts the expected cumulative reward for each action given a state. This Q-function is implemented using a fully connected feedforward neural network. It receives the user's behavioral state vector and outputs Q-values for the two possible actions: authenticate or deny. Formally, the output is:

$$Q\ (s_t\ ;\ \theta) = [Q(s_t\ ,\ \text{authenticate}),\ Q(s_t\ ,\ \text{deny})] \quad (7)$$

where θ denotes the network weights updated through training. The learning process minimizes the Bellman loss, defined as:

$$L(\theta)=E_{(s,a,r,s')}[(r+\gamma \cdot \max_{a'} Q(s',a';\bar{\theta}) - Q(s,a;\theta))^2] \quad (8)$$

Here, γ is discount factor and $\bar{\boldsymbol{\theta}}$ represents the weights of a target network updated periodically for stability.

To balance exploration and exploitation, the agent uses an $\boldsymbol{\epsilon}$-greedy policy: it selects a random action with probability ϵ, or the action with the highest Q-value otherwise. Initially, $\boldsymbol{\epsilon} = 1$ to encourage exploration, and it decays over time as learning progresses.

An experience replays buffer stores interactions in the form of tuples (s_t, a_t, r_t, s_{t+1}). Mini-batches sampled from this buffer enable stable and sample-efficient learning by breaking temporal correlations. To address class imbalance (e.g., rare insider threats), the buffer can be partitioned by class, ensuring that training batches reflect both normal and abnormal behaviors.

This design allows the agent to learn nuanced, context-aware policies that dynamically adjust authentication decisions in real-time, aligning security enforcement with operational realities in e-health environments.

- Authentication manager: the Authentication Manager acts as the intermediary that validates and formalizes the authentication outcome by combining the agent's proposed action with the risk score. Specifically, if the action is "Authenticate" and the risk score meets or exceeds a predefined threshold, access is granted. Otherwise, access is denied.

To support learning, the Authentication Manager issues a scalar reward signal based on the outcome, as defined in Equation (6). This reward is then used by the Authentication Agent to adjust its policy over time. A key system-level component maintained by the Authentication Manager is the Authentication Buffer, a persistent memory structure that logs recent authentication transactions. Each record in the buffer stores relevant metadata such as: User ID, R, C_{id}, C_{cxt}, Authentication timestamp, Agent's decision and outcome. This buffer serves multiple security-critical purposes. Most notably, it bridges the authentication and access control layers of the model. When a user attempts to access, write or modify healthcare data post-authentication, the Access Control Manager queries this buffer to verify whether the session is valid and trustworthy. The stored risk score and decision outcome become key contextual cues for validating whether the access request aligns with organizational policies and user behavior norms. The experience replay buffer not only supports stable learning but also enhances system intelligence by enabling auditing

for compliance, detecting anomalous session trends, correlating authentication with access behaviors, and enabling real-time access validation without repeated authentication. By maintaining this structured historical view of authentication behavior, the Authentication Buffer acts as a real-time memory module that enhances security decisions across the system lifecycle.

6.3.2 Access Control Context

The Access Control context governs user authorization after successful authentication, comprising two primary components: the Access Control Agent and the Access Control Manager.

- Access Control Agent: the Access Control Agent is a reinforcement learning entity responsible for deciding whether to allow or deny specific user actions after authentication, Fig.6.3 shows the access control process of our agent. Unlike the authentication layer, which evaluates the legitimacy of initial access, this agent analyzes real-time behavioral data within the session.

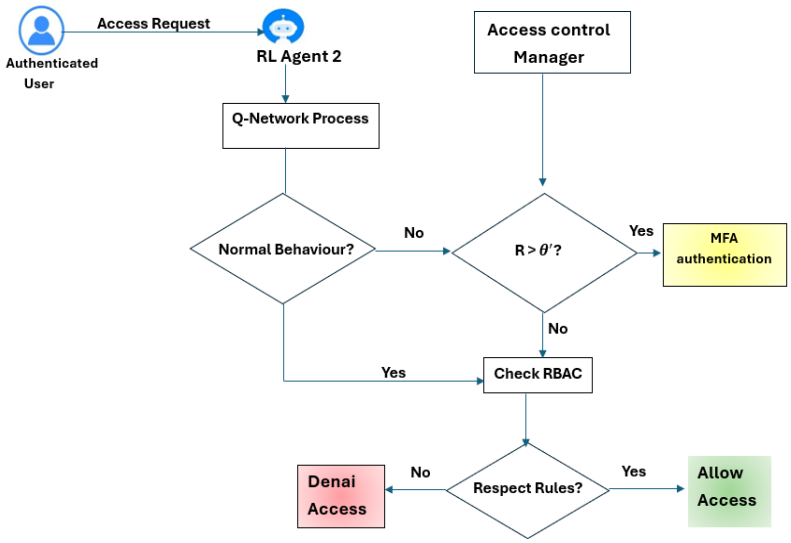


Figure 6.3 Access Control Process.

- State and Action: At each decision point, the Access Control Agent receives a structured state vector defined as:

$$ACC\text{-}st=[Role, N_{email}, S_{email}, N_{web}, N_{attach}, Hour, User\ ID, R]$$

Where:

- N_{email}: Number of emails exchanged,

- S_{email}: Total size of exchanged emails,
- N_{web}: Web access frequency,
- N_{attach}: Number of attachments sent,
- Hour: Current time segment,
- User ID: Unique session identifier,
- R∈[0,1] Risk score from the authentication phase.

This state formulation is tailored to the specific behavioral features available in our dataset, making it highly context-aware and role-sensitive. It is important to note that the structure of this vector is not fixed and can be adjusted depending on the behavioral dimensions present in the dataset used. This modularity allows the model to adapt seamlessly across different environments or application domains where the nature of user interactions may vary.

- Reward function: The reward function governs how the agent learns over time. It is designed to reinforce decisions that maintain system security while allowing behavioral flexibility when justified by context. The reward ACC-r is defined as:

$$\boldsymbol{ACC_r} = \begin{cases} 1 & if\ \ a = a_e\ and\ a_e\ = 0 \\ \lambda & if\ \ a = a_e\ and\ \ a_e\ = 1 \\ \lambda(1-R) & if\ a = a_e\ and\ a_e\ = 0\ and\ \ rare\ access \\ -|\ C-R\ | & if\ \ a \neq a_e\ and\ \ ae = 0 \\ -\lambda\ |\ C-R\ | & if\ \ a \neq a_e\ and\ \ ae = 1\ or\ rare\ access \end{cases} \quad (9)$$

Here, *rare access* as a scenario where the user is authorized to perform an action but exhibits this behavior infrequently based on their historical patterns. In such cases, access can be granted only if the associated risk score R remains below a strict threshold θ′ (with θ′<θ), ensuring the user is well authenticated despite the uncommon behavior. The reward function for the access control agent is structured to balance security enforcement with adaptive, behavior-aware flexibility. A reward of +1 is issued when the agent correctly allows legitimate access under typical conditions, while +λ is given for correctly denying unauthorized actions, boosting sensitivity to minority-class threats. For rare but legitimate access, where a user is permitted to perform an action they seldom use, the agent is rewarded +λ (1 – R), provided the risk score R remains below a defined threshold. This ensures flexibility while still requiring contextual justification. Misclassifications are penalized proportionally: –|C – R| when unauthorized access is wrongly allowed, and –λ |C – R|

when valid access is wrongly denied. This dynamic reward structure helps the agent learn nuanced access control decisions aligned with both policy and behavioral risk.

- Access control manager: the Access Control Manager validates the Access Control Agent's actions by comparing them against a set of role-based and context-aware behavioral rules. These rules are not rigid; they evolve in response to ongoing behavioral trends and are informed by historical access patterns.

The manager issues a reward or punishment based on (9). A penalty is given when the agent's action contradicts either policy constraints or dynamic context evaluation. This dynamic rule framework differentiates the system from static models, enabling more adaptive and intelligent access control in sensitive healthcare environments.

- Rules based access control: at deployment, the Access Control Manager is initialized with role-based access policies derived from:
- HL7 FHIR AuditEvent standards, which encode real healthcare roles and their allowed actions [152].
- Organizational security policies, such as HIPAA [153].

These rules might include for example:

- Admins can access web servers but not clinical data.
- Nurses may send emails but not download attachments.
- Doctors can access patient records and external web tools.

Unlike smart contracts or traditional ML classifiers, these rules are not hard-coded, they serve as initial behavior templates. The agent is free to violate rules, but only if risk and behavioral context justify it. Violations that lead to low-risk, safe outcomes are positively reinforced. This means the model can adapt to real-world variability, such as: shift pattern changes, emergency access scenarios and new workflow patterns. This flexibility supports real-time adaptability, which is critical in environments like hospitals, where user behavior is legitimate but non-static.

6.4 Experiments

This section presents the experimental framework used to evaluate the proposed authentication and access control model. The process flow is illustrated in Fig.6.4 and encompasses several key

phases: dataset selection and user-role mapping, data preprocessing, implementation of authentication and access control agents, and the application of performance metrics to assess anomaly detection and decision-making efficacy.

All experiments were executed on a workstation equipped with an Intel(R) Core(TM) i7-8650U CPU @ 1.90 GHz, 16 GB of RAM, running Windows 10 (64-bit). The entire development pipeline, including data transformation, feature engineering, model training, and evaluation, was implemented in Python 3 within the Anaconda environment.

To ensure robust and reproducible learning dynamics, model hyperparameters were carefully chosen and optimized through iterative experimentation. The final configuration is summarized in Table 6.1.

6.4.1 Dataset description

In the domain of healthcare cybersecurity, one of the major challenges is the scarcity of publicly available datasets that combine realistic behavioral activity logs with labeled anomalies or insider threats. Due to the sensitive nature of healthcare systems and the strict privacy regulations surrounding patient data, access logs and interaction histories are rarely shared for research. Most existing healthcare datasets are clinical in nature, focusing on medical records or physiological signals, and fail to capture the dynamic user behaviors necessary for modeling adaptive authentication and access control mechanisms. This data gap severely limits the ability to train and validate intelligent security models tailored to healthcare environments.

To address this limitation, we utilize the CERT Insider Threat Dataset v4.2 [151], developed by the Carnegie Mellon University Software Engineering Institute [154]. This dataset is a well-established benchmark in the cybersecurity community, frequently used in anomaly detection and insider threat modeling research [155]. Although it was not originally created for healthcare, CERT v4.2 offers an extensive multi-modal view of user behavior within a simulated corporate environment over 18 months, covering 1,000 synthetic employees, with total events of 32,7 million and 70 different anomalies.

Moreover, version 4.2 of CERT was selected over newer versions (e.g., v6.2) due to its higher proportion of labeled anomalies [155], providing a more balanced foundation for training and evaluation. The richness of user behavior logs combined with clearly marked attack traces makes

CERT v4.2 particularly valuable for modeling adaptive, behavior-aware security systems in sensitive domains like healthcare.

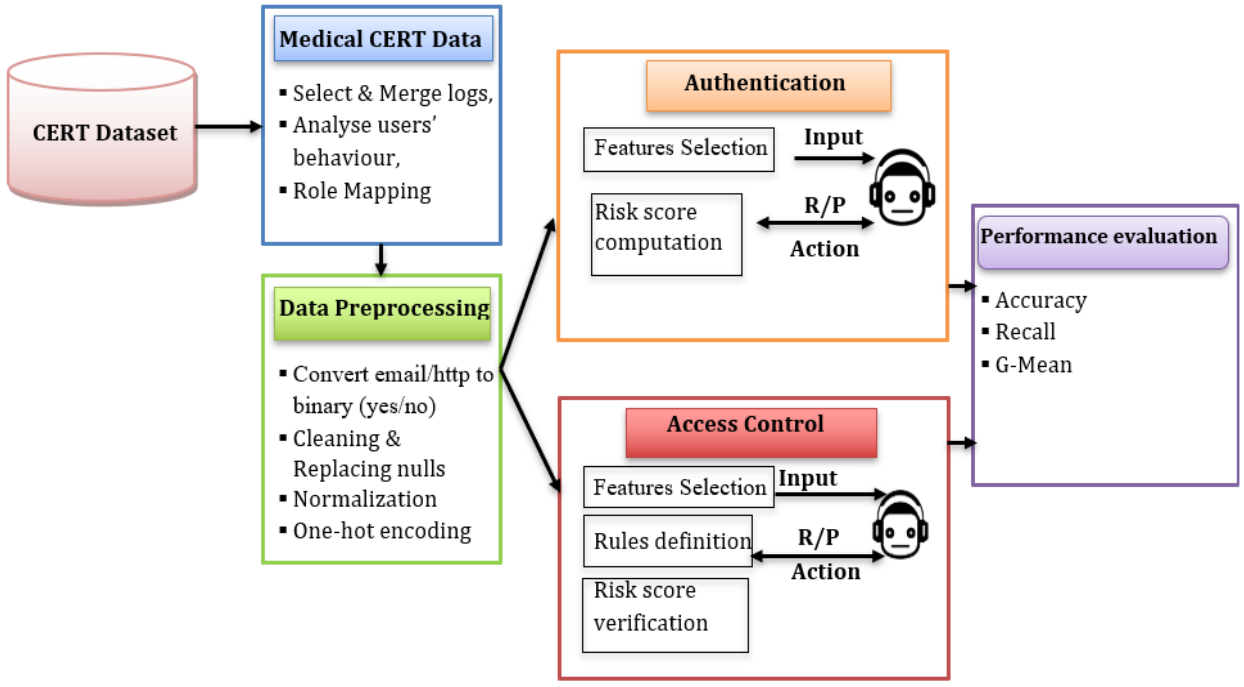


Figure 6.4 The workflow of the proposed methodology for authentication and access control

- Medical Dataset: To apply the CERT v4.2 dataset to the healthcare cybersecurity context, a key challenge lies in the absence of labeled, domain-specific roles that reflect the operational and behavioral dynamics of medical environments. To address this, we performed a systematic role-mapping and behavioral analysis process, aimed at realistically translating synthetic corporate roles into clinically relevant user profiles. The dataset in reality simulates activities for 1,000 users, but the roles metadata, extracted from the LDPA logs, is limited to just 15 distinct organizational roles.

For each of these 15 roles, we conducted a quantitative behavioral analysis that included:

- Login/logout timestamps to identify typical working hours and infer shift patterns (e.g., day-only, night shifts, rotating).
- Email and web access intensity, used to distinguish desk-based administrative roles from high-mobility or clinical positions.
- Activity distribution across services (email, web, device use), helping to characterize task types and system engagement.

Using these features, we generated behavioral profiles that were then aligned with functionally equivalent roles in the healthcare sector based on [152, 153]. For instance, a role exhibiting consistent morning logins and moderate email use was associated with a general practitioner or family doctor, while irregular activity with high web interactions suggested a more IT-intensive healthcare role such as a radiology technician. The full mapping process is presented in Appendix 6.1. which lists each original CERT role, its observed digital behavior, and the corresponding mapped healthcare role. This mapping ensures that the dataset is not arbitrarily relabeled, but instead reflects real-world clinical operations based on empirical system usage.

By embedding this role mapping into our experimental setup, we were able to simulate realistic healthcare workflows while leveraging the existing insider threat labels and behavioral depth of the CERT dataset. This transformation renders the dataset semantically consistent with healthcare information systems, enabling effective training and evaluation of our adaptive access control and authentication models.

- Medical CERT dataset construction: to construct a coherent and behaviorally rich dataset suitable for our reinforcement learning framework, we performed a series of data integration and preprocessing steps. The original CERT v4.2 dataset consists of multiple log files, each capturing distinct aspects of user activity [155]. Each user is identified by a unique ID, and every interaction, such as logon events, email transmission, web browsing, file access, or device use, is time-stamped, allowing for temporal alignment and user-level aggregation.

We defined a user session as the interval between a successful logon and its corresponding logoff, using records from the file *logon.csv*. In cases where multiple consecutive logons occur without an intervening logoff, the session is flagged for anomaly detection, as such patterns typically deviate from standard login behavior. Within each session, we examined all corresponding records from *email.csv*, *http.csv*, *file.csv*, and *device.cs*v files using timestamp and user ID alignment. All users were mapped to healthcare-equivalent roles using metadata from the LDPA files, allowing us to simulate realistic hospital workflows. The resulting CERT-Medical dataset includes approximately 1,1 million user-session records, each encoding both temporal and categorical behavioral data.

This structured dataset serves as the foundation for training and evaluating our adaptive authentication and access control agents, enabling anomaly detection and security decision-making aligned with healthcare operations.

Table 6.1 Parameter values of the RL agents

Parameters	Values
μ	0.25
$\boldsymbol{\gamma}$	0.1
$\boldsymbol{MAX_{f_{ctx}}}$	100
ε decay	0.999
$\boldsymbol{\lambda}$	1
θ	0.5
θ'	0.2

- Data pre-processing: following the integration of behavioral data into structured session records, we applied a series of standard preprocessing steps to ensure data quality and model compatibility. First, we addressed missing values and inconsistencies by discarding incomplete sessions and replacing null values in categorical fields with default labels. Numerical features were normalized using the min-max normalization method to ensure uniform input representation for the learning model. Categorical features were one-hot encoded, enabling the reinforcement learning model to process them effectively.

In terms of feature selection, relevant input attributes were chosen during dataset construction based on their contextual relevance to behavioral modeling. For the authentication scenario, selected features included: Access time segment (to reflect expected working hours), Device ID (used for consistency tracking), User role, Session duration, and Historical authentication status (captured via prior successful login metadata). These features are directly tied to the identity and context evaluation required for adaptive authentication.

For the access control scenario, additional behavioral features observed during the session were included to assess ongoing activity patterns. These comprised: Email activity, Web access, Attachment transmission, along with contextual attributes such as user role, access time, and the risk score computed during authentication.

This separation ensures that both agents, authentication and access control, are trained on behaviorally and contextually appropriate signals, while maintaining a coherent flow of information between system components.

- Evaluation metrics: to evaluate the performance of the proposed RL model in detecting anomalies and abnormal behaviors within healthcare access patterns. To assess the effectiveness of the proposed models, we evaluated standard classification metrics, specifically Accuracy, Recall for

the minority class (anomalies), and Recall for the majority class (normal behavior), as illustrated in Table 6.2. These metrics provide insight into the model's ability to correctly identify both typical and abnormal access patterns in healthcare environments. Given the class imbalance often present in anomaly detection tasks, where normal behavior dominates, the Geometric Mean (G-Mean) was used as a key performance metric. G-Mean provides a balanced measure by incorporating both sensitivity and specificity, helping to ensure that the model performs well across both classes.

Table 6.2 Evaluation Metrics for Model Performance

Metric	**Description**	**Formula**
Accuracy	Measures overall correctness.	$\frac{(TP + TN)}{Total}$
Recall (Majority)	Ability to correctly identify normal behavior	$\frac{TN}{(FP + TN)}$
Recall (Minority)	Sensitivity to detect actual anomalies.	$\frac{TP}{(FN + TP)}$
G-Mean	Balances recall both classes, robust to imbalance.	$\sqrt{Recall_{Maj} * Recall_{Min}}$

6.4.2 Performance Evaluation and Discussion

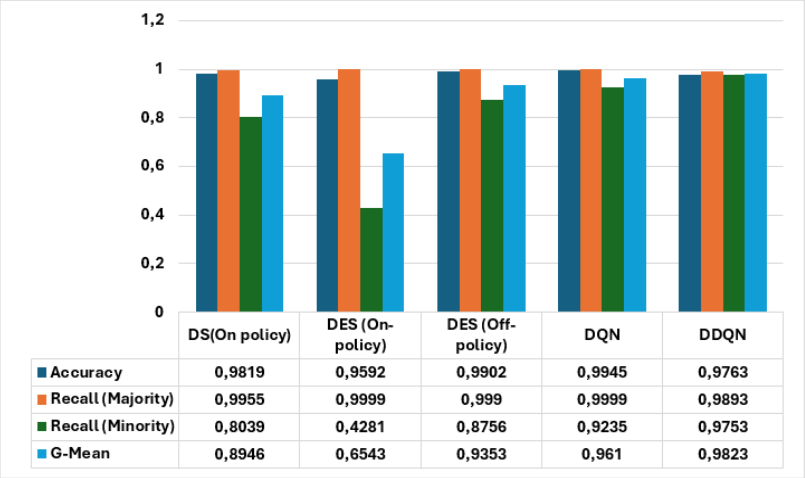
The performance evaluation was conducted in two scenarios: the authentication phase and the Access control phase.

- Authentication scenario: the authentication agent was evaluated using several reinforcements learning algorithms, including DS (on-policy), DES (on-policy and off-policy), DQN, and DDQN, see Fig.6.5. Across all models, accuracy remained consistently high, with most values exceeding 95%, and the best results were achieved by DES (off-policy) and DQN, both approaching or surpassing 99%. This suggests that these agents are generally reliable in classifying authentication attempts. However, accuracy alone does not provide a complete picture in imbalanced classification tasks such as anomaly detection, where the normal class dominates.

To better assess each model's behavior, recall values for both the majority (normal authentication behavior) and minority (anomalous behavior) classes were analyzed. All agents performed well on the majority class, with DES (on-policy), DES (off-policy), and DQN achieving near-perfect recall.

This indicates that legitimate access attempts were rarely misclassified, which is desirable in terms of user experience and system availability. In contrast, recall for the minority class showed substantial variation and proved to be more informative in comparing model effectiveness. DES (on-policy), for instance, detected less than half of the abnormal cases (recall = 0.4281), demonstrating limited utility in real-world applications where early and accurate anomaly detection is essential.

DQN and DDQN, on the other hand, showed significantly stronger performance in identifying abnormal access attempts, with recall values of 0.9235 and 0.9753 respectively. The high recall on the minority class is especially notable, indicating that these models can detect almost all anomalous behaviors without sacrificing overall accuracy. To capture the model's balance across classes, the geometric mean (G-Mean) was used as a key evaluation metric. G-Mean values mirrored the trends observed in recall: DES (on-policy) struggled with a G-Mean of only 0.6543, while DDQN and DQN achieved values of 0.9823 and 0.961, respectively.



	DS(On policy)	DES (On-policy)	DES (Off-policy)	DQN	DDQN
Accuracy	0,9819	0,9592	0,9902	0,9945	0,9763
Recall (Majority)	0,9955	0,9999	0,999	0,9999	0,9893
Recall (Minority)	0,8039	0,4281	0,8756	0,9235	0,9753
G-Mean	0,8946	0,6543	0,9353	0,961	0,9823

Figure 6.5 Performances comparison of different reinforcement learning algorithms (Authentication).

In addition to standard classification metrics, we further analyzed the learning performance of the RL models through smoothed reward measurements over 200 episodes. These smoothed reward curves offer critical insight into the long-term decision-making efficiency of each model. Fig.6.6 presents the smoothed reward obtained per episode during the training phase. In this context, an episode represents one complete simulation cycle, where the RL agent processes a batch of authentication interactions, each involving a decision step, and updates its policy based on received

rewards. This episodic framing allows the model to gradually refine its strategy over successive rounds of learning.

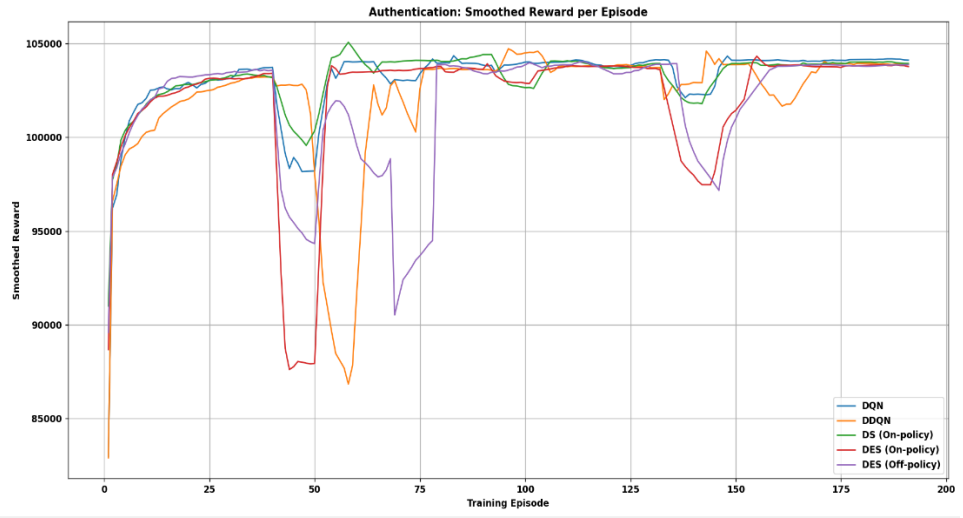


Figure 6.6 The smoothed Reward throughout Episodes for the Training Process (Authentication).

At the start of training, all models experience a sharp increase in reward, indicating effective initial learning. As training progresses, performance differences emerge. The plotted results indicate that DQN achieves fast and stable convergence, with its reward curve displaying minimal volatility after an initial learning phase. This stability suggests DQN is well-suited to the task and consistently learns effective policies. In contrast, the other algorithms, including DDQN, DS (On-policy), DES (On-policy), and DES (Off-policy), demonstrate higher variance in reward across episodes, marked by occasional sharp declines and recoveries. Such variability may reflect differences in exploration strategies, sensitivity to reward signals, or robustness to outliers. The results highlight DQN's advantage in learning stability, while alternative methods may benefit from further tuning to mitigate episodic reward drops.

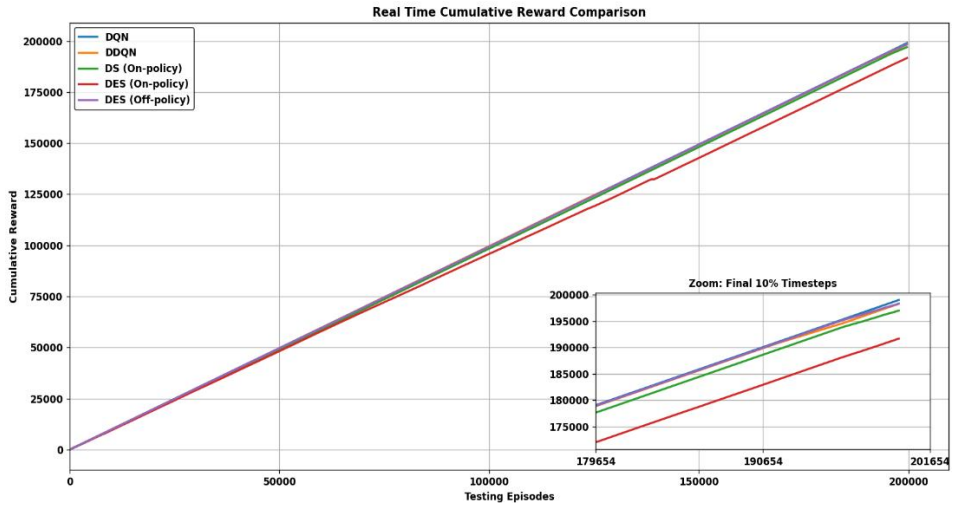


Figure 6.7. Cumulated reward during testing (real-time) episodes (Authentication).

To further evaluate the effectiveness of the trained reinforcement learning models, we assessed their cumulative reward on the testing set. Fig.6.7 compares the real-time cumulative reward across several algorithms during the testing phase. The x-axis represents the progression through testing episodes, while the y-axis denotes the accumulated reward, corresponding to the number of correct decisions over time. As observed, all models exhibit a consistent upward trend, with DQN and DDQN achieving slightly higher cumulative rewards compared to the other approaches. The inset provides a closer look at the final 10% of episodes, highlighting finer differences in performance and stability between models. This comparison illustrates the robustness and generalization ability of each model on unseen data.

To complement the evaluation, we measured training and testing times for each scenario as illustrated in table 6.3. In authentication scenario, all agents trained quickly, with DQN and DDQN being the fastest. On the test set, DQN again led (2.45 ms), closely followed by DDQN. These results confirm that all models are suitable for real-time use, with DQN achieving the best overall efficiency.

Across all experiments, the DQN agent consistently emerged as the most balanced and effective model. It demonstrated excellent classification accuracy, a high recall for both normal and abnormal behaviors, and a strong G-Mean, confirming its robustness in handling imbalanced healthcare authentication data. Its learning curve during training reflected fast convergence and sustained reward optimization, while its cumulative reward in real-time deployment was the highest among all agents, signaling superior long-term decision-making.

Table 6.3 Training and Testing time of RL anomaly detection models.

	Authentication Scenario		**Access Control Scenario**	
Model	Training time (ms)	Testing time (ms)	Training time (ms)	Testing time (ms)
DS(On-Policy)	56.01	3.271	72.71	4.15
DES (On-Policy)	55.98	2.24	71.48	3.10
DES (Off-Policy)	56.25	2.72	72.68	3.17
DQN	51.52	2.45	65.87	3.74
DDQN	51.48	2.63	68.3	3.96

Additionally, DQN demonstrated some of the lowest training and testing times, reinforcing its efficiency and making it particularly well-suited for our time-sensitive healthcare authentication scenario.

To demonstrate the superiority of our DQN-based authentication agent, we benchmarked its performance against widely used machine learning classifiers: Random Forest, XGBoost, KNN, ANN, and SVM. As shown in Fig. 6.8, DQN clearly outperforms all other models, achieving a remarkable accuracy of 99.45% and a G-Mean of 96.1%. This indicates not only high overall correctness but also a strong balance between detecting both legitimate (majority) and anomalous (minority) access attempts, a critical requirement in security-sensitive systems. In contrast, while Random Forest, XGBoost, and KNN offer solid accuracy, their G-Mean scores range between 76.19% and 77.23%, signaling a performance drop on minority class detection. ANN and SVM perform even lower, especially in terms of G-Mean. This highlights their vulnerability to class imbalance, a common issue in real-world intrusion and authentication data.

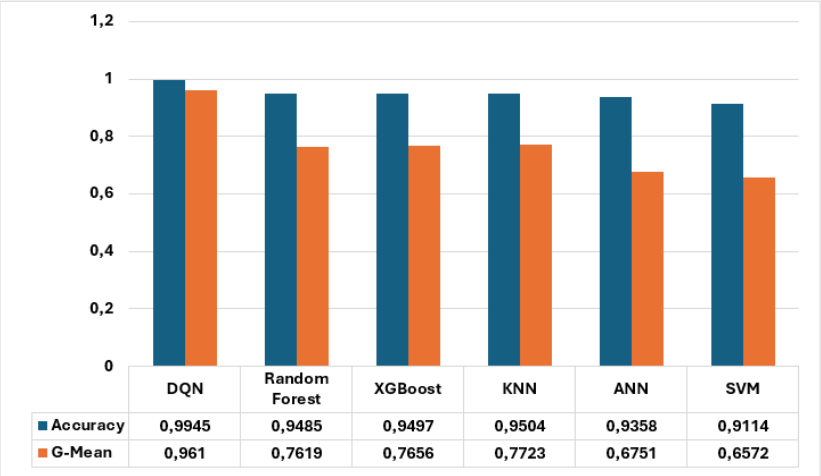
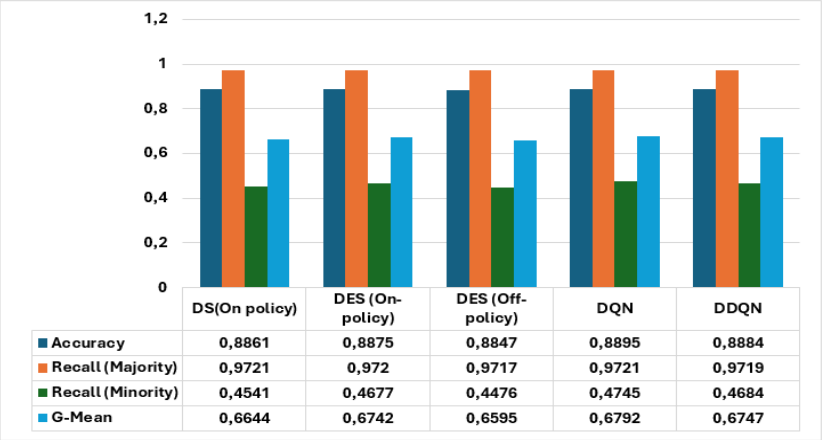


Figure 6.8 Performance comparison of different machine learning algorithms (Authentication).

As a result, DQN proved its effectiveness as a robust and adaptive model for dynamic, imbalanced authentication environments.

- Access control scenario: we passed now to the access control scenario, similar to the authentication agent. The access control scenario was evaluated using DS (on-policy), DES (on-policy and off-policy), DQN, and DDQN models, see Fig. 6.9. Although overall accuracy remains high (around 88–89% for all models), these results are slightly below those observed for authentication, reflecting the increased complexity of access control classification. Majority recall values are again very strong, showing that all models effectively identify regular access attempts, as in the authentication scenario. However, the recall for the minority class remains moderate, with no model exceeding 50%. DQN and DDQN achieve the best minority recall, suggesting a more balanced approach.

Notably, unlike in the authentication scenario, where a risk score enabled straightforward thresholding, here, access decisions are driven by a set of handcrafted rules, making adaptation more challenging. This rule-based setup adds complexity and explains the slightly lower performance, particularly for anomaly detection.



	DS(On policy)	DES (On-policy)	DES (Off-policy)	DQN	DDQN
Accuracy	0,8861	0,8875	0,8847	0,8895	0,8884
Recall (Majority)	0,9721	0,972	0,9717	0,9721	0,9719
Recall (Minority)	0,4541	0,4677	0,4476	0,4745	0,4684
G-Mean	0,6644	0,6742	0,6595	0,6792	0,6747

Figure 6.9 Performance comparison of different reinforcement learning algorithms (Access Control).

Building on the performance metrics discussed above, we now examine the smoothed training reward for the access control agent, as depicted in Figure 6.10. Compared to the authentication phase, where the learning curves were generally more stable, we observe greater instability and variance in the reward trajectories for all algorithms. This increased variability can be attributed to the rule-based nature of the access control task, which presents a more complex decision landscape than the single numerical threshold used in authentication. The need to satisfy multiple, often rare, access rules lead to frequent fluctuations in reward, especially when agents encounter uncommon access patterns.

Examining the curves, DQN again demonstrates strong learning behavior, achieving rapid and stable convergence after the initial training episodes, and showing less sensitivity to episodic fluctuations than the other agents. In contrast, the alternative algorithms, including DDQN, DS (on-policy), and both DES variants, display more pronounced oscillations and sharper drops in reward throughout training. This suggests that DQN is more robust in adapting to the increased complexity of rule-driven access decisions.

To complement the training analysis, Figure 6.11 presents the cumulative reward of each agent on the access control testing set. This evaluation provides insight into the real-time decision accuracy and generalization ability of the trained models. As observed, the cumulative reward curves for all algorithms increase steadily as more test episodes are processed, indicating a high frequency of correct decisions.

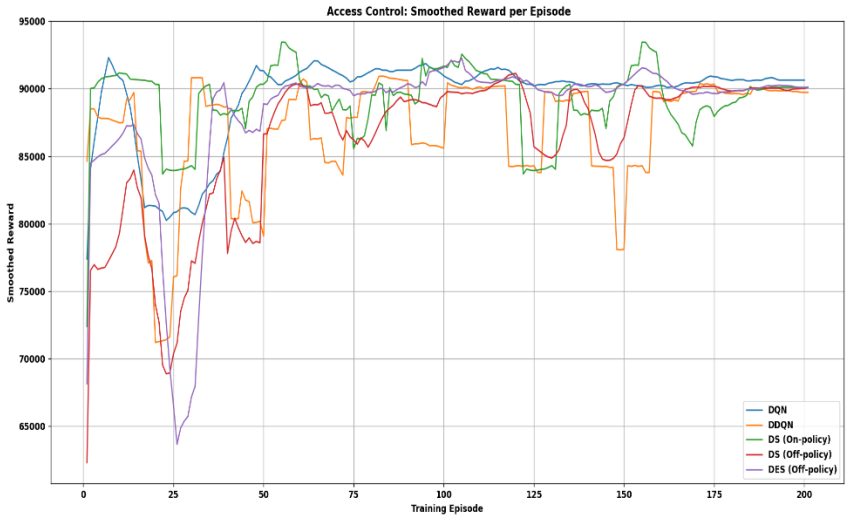


Figure 6.10. The smoothed Reward throughout Episodes for the Training Process (Access control).

Compared to the authentication scenario, the access control results show greater separation between agents, especially over the final portion of the test set (see the zoomed inset). DQN and DDQN outperform the other algorithms, maintaining the highest cumulative rewards and thus demonstrating superior generalization. This pattern reinforces previous findings: while all models perform well in general, DQN exhibits the most consistent and reliable performance across both training and testing phases, particularly in more complex, rule-driven environments.

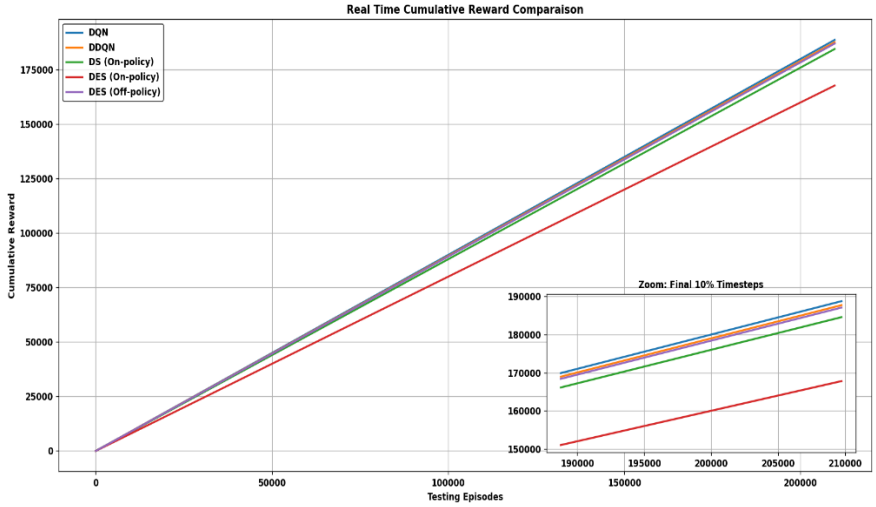


Figure 6.11 Cumulated reward during testing (real-time) episodes (Access Control).

To provide a broader perspective on model performance, Figure 6.12 reports the results of the DQN access control agent compared with several classical machine learning methods.

The classical ML models show considerably lower G-Mean values, with most models scoring below 0.5. This indicates a substantial weakness in detecting the minority class, namely, rare anomalous access attempts. While accuracy scores remain relatively high due to the predominance of normal cases in the dataset, these results mask the difficulty of identifying rare events, which is critical in access control scenarios. The nature of the dataset, where legitimate accesses are much more frequent than policy violations, and the presence of strict, domain-specific rules further complicate learning for standard classifiers, leading to suboptimal anomaly detection. In contrast, the DQN reinforcement learning agent stands out, achieving both the highest accuracy and the best G-Mean. This reinforces findings from the authentication agent, RL methods are more capable of adapting to the complex, rule-based structure of access control and are more robust to class imbalance. These results underline the challenges classical models face in such contexts and highlight the advantage of RL-based approaches for policy-driven anomaly detection tasks.

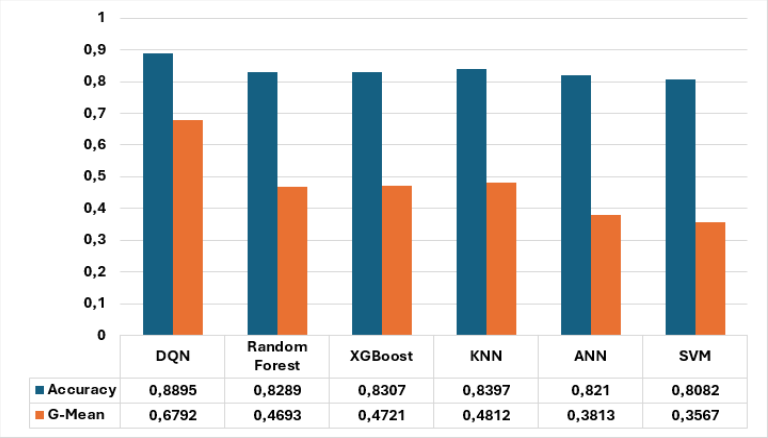


Figure 6.12. Performance comparison of different machine learning algorithms (Access Control).

6.5 CONCLUSION

This paper presents a novel dual-agent framework for authentication and access control in healthcare environments using reinforcement learning (RL). By integrating behavioral risk analysis and adaptive policy enforcement, the system addresses critical limitations of static, rule-based and machine learning models, especially in handling imbalanced and dynamic healthcare scenarios.

To enable realistic evaluation, we constructed a customized healthcare-specific version of the CERT insider threat dataset. This adaptation was achieved by analyzing user roles, activity patterns, and organizational policies to reflect authentic operational conditions in medical systems.

The proposed framework includes two core implementation scenarios, authentication and access control. In both, five RL models, DS, DES (on/off-policy), DQN, and DDQN, were trained and evaluated using multiple performance metrics: accuracy, class-specific recall, G-Mean, training/testing time, smoothed rewards over 200 episodes, and cumulative rewards during testing. Among these, the DQN agent emerged as the most reliable model, achieving the highest G-Mean, superior recall on minority classes, and efficient training behavior.

To reinforce these findings, DQN was benchmarked against five traditional ML classifiers, Random Forest, XGBoost, KNN, ANN, and SVM. In both authentication and access control settings, DQN outperformed all baselines, with G-Mean scores of 96% and 67%, respectively. These results validate the effectiveness of our reward function design and reinforce the value of reinforcement learning for imbalanced classification in security-critical systems.

While the authentication scenario showed strong and consistent results, the access control agent faced slightly more challenges. Its reliance on manually defined access rules introduces added complexity and may affect sensitivity to anomalous behavior. Future improvements could include defining a more stable and quantifiable access score, like the risk score in the authentication setup, to guide the agent's decisions with greater precision.

ACKNOWLEDGMENT

The authors would like to thank Dr. Franjieh El Khoury for her valuable comments and proofreading of this paper.

This work was funded by the Natural Sciences and Engineering Research Council of Canada (NSERC), Prompt, Flex Group, and ISAME

CHAPITRE 7 DISCUSSION GÉNÉRALE

Ce chapitre est consacré à la discussion des travaux réalisés dans cette thèse. Dans un premier temps, nous présentons les choix méthodologiques qui ont guidé la définition et l'atteinte des objectifs de recherche. Dans un second temps, nous procédons à l'analyse des résultats obtenus.

7.1 Aspects méthodologiques

La thématique principale abordée dans cette thèse est la sécurité des données dans les systèmes de soins de santé intelligents. Pour traiter cette problématique, un travail préalable de revue de la littérature a été mené afin d'identifier les principales faiblesses des solutions existantes, notamment en ce qui concerne la confidentialité, l'intégrité et le contrôle d'accès dans des environnements contraints et dynamiques.

De cette analyse, il ressort que les problèmes de sécurité dans les systèmes de soins de santé intelligents peuvent être regroupés autour de trois axes principaux : la protection de la confidentialité des données médicales, la détection en temps réel des menaces et anomalies, et l'authentification et contrôle d'accès adaptés aux environnements médicaux complexes.

En fonction de ces trois axes, la thèse a été structurée en trois volets complémentaires :

- Le premier volet s'attaque aux défis liés à la confidentialité et à la protection de la vie privée des patients, en proposant un schéma cryptographique léger basé sur la décomposition en trois parties de Karatsuba et la technique de permutation aléatoire, conçu pour les dispositifs médicaux contraints en ressources.
- Le deuxième volet aborde la question de l'intégrité et de la détection des menaces, à travers la création d'un nouveau jeu de données médicales et le développement d'un modèle d'ensemble d'apprentissage automatique capable de détecter les anomalies en temps réel.
- Le troisième volet se concentre sur l'authentification et le contrôle d'accès, en introduisant un cadre adaptatif basé sur l'apprentissage par renforcement, apte à gérer les comportements dynamiques et les risques d'usurpation d'identité dans les environnements hospitaliers.

La méthodologie adoptée dans chacun de ces volets suit un même fil conducteur :

1. Une revue critique de la littérature, afin de mettre en évidence les limites des solutions actuelles ;

2. La conception d'une approche novatrice répondant aux faiblesses identifiées ;
3. L'implémentation et l'évaluation expérimentale de la solution proposée sur des environnements réalistes (dispositifs IoT médicaux, jeux de données médicaux, et scénarios hospitaliers).

La méthodologie adoptée dans chacun de ces volets suit un même fil conducteur :

Une revue critique de la littérature, afin de mettre en évidence les limites des solutions actuelles ;

La conception d'une approche novatrice répondant aux faiblesses identifiées ;

L'implémentation et l'évaluation expérimentale de la solution proposée sur des environnements réalistes (dispositifs IoT médicaux, jeux de données médicaux, et scénarios hospitaliers).

7.2 Analyse des résultats

Les résultats obtenus au terme de cette thèse contribuent à renforcer la sécurité des données dans les systèmes de soins de santé intelligents.

Pour protéger la confidentialité des informations médicales échangées entre dispositifs connectés et infrastructures de soins de santé intelligents, nous avons proposé un schéma cryptographique léger, 3DKSh-BRLWE. L'intégration de la multiplication de Karatsuba en trois décompositions, associée au procédé de permutation aléatoire « random shuffling », a permis d'optimiser la multiplication polynomiale tout en renforçant la résistance aux attaques par canaux auxiliaires (timing, SPA, DPA), tout en assurant une sécurité contre les menaces quantiques et hybrides. L'évaluation expérimentale sur microcontrôleur ARM Cortex-M0 montre un temps d'exécution très réduit (18,79 ms pour le chiffrement et 9,53 ms pour le déchiffrement), confirmant la pertinence du schéma pour des dispositifs médicaux contraints en ressources. Ces résultats mettent en évidence un compromis optimal entre robustesse cryptographique et efficacité pratique.

Pour garantir l'intégrité des flux médicaux et la détection en temps réel des menaces, nous avons construit un nouveau jeu de données médicales, intégrant des données physiologiques et des scénarios d'attaques spécifiques au domaine de la santé (falsification, DoS, intrusions réseau). Sur ce jeu de données, nous avons développé un modèle d'ensemble par empilement (stacking ensemble), combinant Random Forest et réseaux de neurones artificiels avec XGBoost en tant que méta-apprenant (meta-learner). Les résultats expérimentaux démontrent une précision de 98,02 %

et une capacité de prédiction en temps réel validée par 97 messages correctement classés sur 100 lors d'une simulation. Notre approche montre une amélioration notable en termes de réalisme et d'efficacité pour la détection des anomalies dans les environnements médicaux.

Enfin, pour répondre aux défis liés à l'authentification et au contrôle d'accès adaptatif, nous avons proposé un cadre basé sur l'apprentissage par renforcement. Ce cadre introduit deux agents distincts : l'un dédié à l'authentification contextuelle et l'autre au contrôle d'accès dynamique. L'utilisation d'un jeu de données adapté du CERT Insider Threat a permis d'entraîner et d'évaluer cinq algorithmes RL (i.e., DS, DES, DQN et DDQN). Les résultats montrent que DQN surpasse les autres agents, avec une meilleure capacité à gérer les classes déséquilibrées, un G-Mean élevé et une convergence rapide et stable. Par rapport aux modèles classiques de machine learning (e.g., Random Forest, ANN, SVM, etc.), l'approche par renforcement se distingue par sa capacité d'adaptation aux comportements dynamiques et aux risques d'usurpation d'identité dans les environnements hospitaliers.

En conclusion, les objectifs de recherche fixés en début de thèse ont été atteints à travers ces trois volets. Chaque contribution a permis d'apporter une solution innovante et validée expérimentalement à un défi majeur de la sécurité dans les systèmes de soins de santé intelligents: la confidentialité, l'intégrité, et l'authentification/contrôle d'accès. L'ensemble de ces résultats a donné lieu à trois articles scientifiques, présentés dans les chapitres 4, 5 et 6. Le chapitre suivant est consacré à la discussion des limites et aux perspectives futures.

CHAPITRE 8 CONCLUSION

Ce chapitre présente une synthèse des travaux réalisés dans le cadre de cette thèse. Dans un premier temps, nous proposons une vue d'ensemble des travaux réalisées. Ensuite, nous rappelons les principales contributions obtenues, avant d'aborder les limites identifiées. Enfin, nous présentons les perspectives de recherche qui pourraient constituer des pistes pour des travaux futurs.

8.1 Synthèse des travaux

L'objectif principal de cette thèse est de concevoir des approches robustes pour renforcer la sécurité des données dans les systèmes de soins de santé intelligents. Avec la numérisation croissante des pratiques médicales, la protection des informations médicales, en termes de confidentialité, d'intégrité d'authentification et de contrôle d'accès, constitue un enjeu fondamental. Dans cette optique, les travaux réalisés dans cette thèse sont organisés en trois volets complémentaires. Le premier introduit un algorithme de chiffrement post-quantique léger pour garantir la confidentialité des données médicales. Le deuxième volet présente un système de détection d'anomalies en temps réel pour assurer l'intégrité et la disponibilité des données. Le troisième volet met en œuvre un modèle d'authentification et de contrôle d'accès adaptatif capable d'ajuster dynamiquement les politiques de sécurité selon le comportement des utilisateurs et le contexte opérationnel. L'ensemble de ces contributions permet d'établir une architecture de sécurité unifiée, évolutive et adaptée aux contraintes réelles des environnements médicaux connectés.

8.2 Contributions de la thèse

À l'issue de ce travail doctoral, plusieurs contributions majeures ont été apportées à l'amélioration de la sécurité des systèmes de soins de santé intelligents. Elles se résument comme suit :

- Proposition d'un schéma cryptographique post-quantique léger (3DKSh-BRLWE) adapté aux dispositifs médicaux contraints. Le schéma combine la décomposition en trois parties de Karatsuba et la technique de permutation aléatoire « Random Shuffling », renforçant ainsi la résistance face aux attaques par canaux auxiliaires (i.e., timing, SPA et DPA) et aux menaces quantiques hybrides. L'évaluation sur microcontrôleur ARM Cortex-M0 a démontré la rapidité et l'efficacité de la solution par rapport aux variantes existantes.

- Optimisation de la multiplication polynomiale dans le schéma BRLWE, permettant une réduction significative des coûts de calcul tout en maintenant un haut niveau de sécurité. Cette optimisation confirme la faisabilité du schéma dans des environnements médicaux à ressources limitées.

- Conception d'un nouveau jeu de données médicales orienté cybersécurité, intégrant des données physiologiques réelles issues de bases médicales et des scénarios d'attaques représentatifs des environnements IoMT (i.e., attaques par falsification, DoS et intrusions). Ce jeu de données pallie l'absence de bases de données médicales publiques adaptées aux problématiques de la détection des anomalies.

- Développement d'un modèle pour la détection des intrusions en temps réel basé sur un ensemble par empilement « Stacking Ensemble ». Le modèle intègre « Random Forest », réseaux de neurones artificiels et XGBoost comme méta-apprenant. Les résultats expérimentaux montrent une précision de 98,02 % et une robustesse confirmée lors de transmissions médicales simulées en conditions réelles.

- Proposition d'un « Framework dual-agent » pour l'authentification et le contrôle d'accès adaptatif, reposant sur l'apprentissage par renforcement. Le « Framework » introduit deux agents distincts : un agent d'authentification basé sur le risque et un agent de contrôle d'accès contextuel. Pour un réalisme accru, le « CERT Insider Threat Dataset » a été adapté et restructuré dans un contexte médical, reflétant les rôles et comportements des utilisateurs hospitaliers.

- Évaluation comparative entre les modèles d'apprentissage par renforcement et les modèles classiques d'apprentissage automatique, démontrant la supériorité de l'agent « DQN ». Ce dernier surpasse les autres modèles RL (i.e., DS, DES et DDQN) et les algorithmes classiques (e.g., Random Forest, ANN, SVM, etc.) en termes de précision, rappel sur classes minoritaires, « G-Mean » et rapidité de convergence, confirmant son adaptabilité aux environnements médicaux dynamiques.

8.3 Limitations des travaux réalisés

L'identification des limites de tout travail est nécessaire à l'avancement des connaissances. Les limites des travaux réalisés dans le cadre de cette thèse sont présentées comme suit :

- Le schéma cryptographique léger 3DKSh-BRLWE proposé est optimisé pour des polynômes de degré limité (≤256). Cette restriction engendre des problèmes de passage à l'échelle pour des paramètres cryptographiques plus élevés, nécessaires dans certains scénarios post-quantiques.

- La sécurité du schéma n'a pas encore été évaluée face à des attaques avancées par canaux auxiliaires, telles que les attaques par injection de fautes. De telles attaques pourraient réduire la robustesse dans des environnements hostiles.

- Le jeu de données médicales conçu inclut un ensemble limité de types d'attaques. Cette limitation peut réduire sa capacité à représenter de nouvelles menaces émergentes ou des attaques multi-étapes sophistiquées.

- L'évaluation du modèle de détection des anomalies a été principalement réalisée sur le jeu de données personnalisé développé et sur le jeu CICIDS2017. L'absence de validation sur d'autres jeux de données publics spécifiquement conçus pour la détection des attaques dans les systèmes de soins de santé limite la généralisation des résultats à des environnements médicaux variés.

- Les modèles d'apprentissage par renforcement reposant sur des règles limitent la capacité du système à s'adapter rapidement aux nouveaux comportements anormaux et réduisent sa flexibilité, notamment en comparaison avec l'agent d'authentification fondé sur un score de risque.

- Les agents d'apprentissage par renforcement peuvent souffrir de lenteurs de convergence dans des environnements hautement dynamiques. Cette contrainte peut freiner leur efficacité lors d'une mise en œuvre à grande échelle dans des systèmes médicaux en temps réel.

8.4 Travaux futurs

Pour conclure cette thèse, nous faisons des recommandations sur des directions de recherche futures, dont certaines émanent des limites relevées à la section précédente. Ces recommandations sont les suivantes :

- Renforcement du schéma cryptographique 3DKSh-BRLWE : concevoir et intégrer des contre-mesures supplémentaires pour renforcer la résistance contre des attaques avancées par canaux auxiliaires, telles que les attaques par injection de fautes.

- Extension de l'algorithme de multiplication polynomiale : adapter le schéma proposé afin de supporter des polynômes de degré plus élevé sur des microcontrôleurs plus puissants, tout en maintenant un coût de calcul léger.

- Enrichissement du jeu de données médical : élargir le jeu de données en intégrant de nouveaux scénarios d'attaques émergentes et complexes, afin de mieux représenter les menaces évolutives auxquelles les systèmes de santé sont exposés.

- Validation croisée sur plusieurs benchmarks : évaluer le modèle de détection d'anomalies sur des jeux de données publics et hétérogènes, et explorer des techniques d'apprentissage par renforcement pour améliorer l'adaptabilité de la détection face à des environnements variés.

- Amélioration du cadre d'accès adaptatif : définir un score de risque quantifiable et stable, similaire à celui utilisé dans le scénario d'authentification, pour guider les décisions de l'agent de contrôle d'accès de manière plus précise.

- Accélération de la convergence des agents RL : explorer des approches hybrides combinant apprentissage par renforcement et modèles d'apprentissage automatique traditionnels, afin d'accélérer l'entraînement et d'améliorer la réactivité tout en conservant la robustesse dans des environnements dynamiques.

RÉFÉRENCES

[1] United Nations, Department of Economic and Social Affairs. World urbanization prospects: the 2014 revision. https://www.un-ilibrary.org/content/books/9789210043144/read, consulté le 01-12-2021

[2] W. H. Organization and Others, "Noncommunicable diseases country profiles 2014," 2014, [Online]. Available: https://apps.who.int/iris/bitstream/handle/10665/128038/9789241?sequence=1

[3] U. N. D. of E. A. S. Affairs and United Nations Department of Economic and Social Affairs, "World Population Ageing 2013," 2013.

[4] A. Chatterjee, Chronic Disease and Wellness in America: Measuring the Economic Burden in a Changing Nation. Santa Monica, CA, USA: Milken Institute, 2014.

[5] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and its integration with *IoT*. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, 2018.

[6] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[7] K. Su, J. Li, and H. Fu, "Smart city and the applications," in *2011 International Conference on Electronics, Communications and Control (ICECC)*, Sep. 2011, pp. 1028–1031.

[8] R. R. Harmon, E. G. Castro-Leon, and S. Bhide, "Smart cities and the Internet of Things," in *2015 Portland International Conference on Management of Engineering and Technology (PICMET)*, Aug. 2015, pp. 485–494.

[9] O. Vermesan and P. Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. River Publishers, 2013.

[10] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, and A. Refoufi, "A review of security in internet of things," *Wirel. Pers. Commun.*, vol. 108, no. 1, pp. 325–344, 2019.

[11] I. Saif, S. Peasley, and A. Perinkolam, "Safeguarding the Internet of Things," *Deloitte Review*, 2015.

[12] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and challenges for realising the Internet of Things," *Cluster of European research projects on the internet of things, European Commision*, vol. 3, no. 3, pp. 34–36, 2010.

[13] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, 2018.

[14] C. Butpheng, K.-H. Yeh, and H. Xiong, "Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review," *Symmetry* , vol. 12, no. 7, p. 1191, 2020.

[15] C. Konstantinou, "Toward a Secure and Resilient All-Renewable Energy Grid for Smart Cities," *IEEE Consumer Electronics Magazine*, vol. 11, no. 1, pp. 33–41, 2022.

[16] A. Tabasum, Z. Safi, W. AlKhater, and A. Shikfa, "Cybersecurity Issues in Implanted Medical Devices," in *2018 International Conference on Computer and Applications (ICCA)*, Aug. 2018, pp. 1–9.

[17] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT Malware Detection Approaches: Analysis and Research Challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019.

[18] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight cryptography: A solution to secure IoT," Wirel. Pers. Commun., vol. 112, no. 3, pp. 1947–1980, 2020.

[19] R. Chaudhary, G. S. Aujla, N. Kumar, and S. Zeadally, "Lattice-Based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions," IEEE Internet of Things Journal, vol. 6, no. 3. pp. 4897–4909, 2019.

[20] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a Quantum World," IEEE Communications Magazine, vol. 55, no. 2. pp. 116–120, 2017.

[21] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," Journal of Network and Computer Applications, vol. 84. pp. 25–37, 2017.

[22] J. Qiu, Q. Wu, G. Ding, Y. Xu, and S. Feng, "A survey of machine learning for big data processing," EURASIP J. Adv. Signal Process., vol. 2016, no. 1, p. 67, 2016.

[23] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, “Machine Learning in IoT Security: Current Solutions and Future Challenges,” IEEE Communications Surveys Tutorials, vol. 22, no. 3, pp. 1686–1721, 2020.

[24] S. Tanwar, K. Parekh, and R. Evans, “Blockchain-based electronic healthcare record system for healthcare 4.0 applications,” Journal of Information Security and Applications, vol. 50, p. 102407, 2020.

[25] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, “Blockchain based searchable encryption for electronic health record sharing,” Future Gener. Comput. Syst., vol. 95, pp. 420–429, 2019.

[26] S. Biswas, K. Sharif, F. Li, I. Alam, and S. Mohanty, “DAAC: Digital Asset Access Control in a Unified Blockchain Based E-Health System,” IEEE Transactions on Big Data, pp. 1–15, 2020.

[27] Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, “A Decentralizing Attribute-Based Signature for Healthcare Blockchain,” in 2018 27th International Conference on Computer Communication and Networks (ICCCN), Jul. 2018, pp. 1–9.

[28] G. Thamilarasu, A. Odesile, and A. Hoang, “An Intrusion Detection System for Internet of Medical Things,” IEEE Access, vol. 8, pp. 181560–181576, undefined 2020.

[29] A. I. Newaz, A. K. Sikder, L. Babun, and A. S. Uluagac, “HEKA: A Novel Intrusion Detection System for Attacks to Personal Medical Devices,” in 2020 IEEE Conference on Communications and Network Security (CNS), Jun. 2020, pp. 1–9.

[30] S. Pinisetty, P. S. Roop, V. Sawant, and G. Schneider, “Security of Pacemakers using Runtime Verification,” in 2018 16th ACM/IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE), Oct. 2018, pp. 1–11.

[31] M. Zhang, A. Raghunathan, and N. K. Jha, “MedMon: securing medical devices through wireless monitoring and anomaly detection,” IEEE Trans. Biomed. Circuits Syst., vol. 7, no. 6, pp. 871–881, Dec. 2013.

[32] L. Bu, M. G. Karpovsky, and M. A. Kinsy, “Bulwark: Securing implantable medical devices communication channels,” Comput. Secur., vol. 86, pp. 498–511, Sep. 2019.

[33] A. Gibson and G. Thamilarasu, “Protect Your Pacemaker: Blockchain based Authentication and Consented Authorization for Implanted Medical Devices,” Procedia Comput. Sci., vol. 171, pp. 847–856, Jan. 2020.

[34] P. Mamoshina et al., “Converging Blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare,” Oncotarget, vol. 9, no. 5, pp. 5665–5690, 2018.

[35] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, “DeepChain: Auditable and privacy-preserving deep learning with Blockchain-based incentive,” IEEE Trans. Dependable Secure Comput., pp. 1–1, 2019.

[36] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, “HealthGuard: A Machine Learning-Based Security Framework for Smart Healthcare Systems,” in 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS), Oct. 2019, pp. 389–396.

[37] J. Cañedo and A. Skjellum, “Using machine learning to secure IoT systems,” in 2016 14th Annual Conference on Privacy, Security and Trust (PST), Dec. 2016, pp. 219–222.

[38] G. Han, L. Xiao, and H. V. Poor, “Two-dimensional anti-jamming communication based on deep reinforcement learning,” in 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Mar. 2017, pp. 2087–2091.

[39] M. Signorini, M. Pontecorvi, W. Kanoun, and R. Di Pietro, “BAD: Blockchain Anomaly Detection,” arXiv [cs.CR], Jul. 10, 2018. [Online]. Available: http://arxiv.org/abs/1807.03833

[40] A. Besir Kurtulmus and K. Daniel, “Trustless Machine Learning Contracts; Evaluating and Exchanging Machine Learning Models on the Ethereum Blockchain,” arXiv [cs.CR], Feb. 27, 2018. [Online]. Available: http://arxiv.org/abs/1802.10185

[41] J. Yu, H. Lee, M.-S. Kim, and D. Park, “Traffic flooding attack detection with SNMP MIB using SVM,” Comput. Commun., vol. 31, no. 17, pp. 4212–4219, Nov. 2008.

[42] R. Agrawal et al., “Continuous Security in IoT Using Blockchain,” in 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Apr. 2018, pp. 6423–6427.

[43] A. Deshpande, M. S. Deshpande, and D. N. Kayatanavar, "FPGA implementation of AES encryption and decryption," *International Conference on Control and Automation*, pp. 1–6, Jun. 2009.

[44] Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," *IEEE Xplore*, Aug. 01, 2011. https://ieeexplore.ieee.org/abstract/document/6021216 (accessed May 28, 2020).

[45] Hamad Marzouqi, Mahmoud Al-Qutayri, and K. Salah, "Review of Elliptic Curve Cryptography processor designs," *Microprocessors and Microsystems*, vol. 39, no. 2, pp. 97–112, Mar. 2015, doi: https://doi.org/10.1016/j.micpro.2015.02.003.

[46] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, doi: https://doi.org/10.1109/sfcs.1994.365700.

[47] A. Deshpande, M. S. Deshpande, and D. N. Kayatanavar, "FPGA implementation of AES encryption and decryption," *International Conference on Control and Automation*, pp. 1–6, Jun. 2009.

[48] Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," *IEEE Xplore*, Aug. 01, 2011. https://ieeexplore.ieee.org/abstract/document/6021216 (accessed May 28, 2020).

[49] Hamad Marzouqi, Mahmoud Al-Qutayri, and K. Salah, "Review of Elliptic Curve Cryptography processor designs," *Microprocessors and Microsystems*, vol. 39, no. 2, pp. 97–112, Mar. 2015, doi: https://doi.org/10.1016/j.micpro.2015.02.003.

[50] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, doi: https://doi.org/10.1109/sfcs.1994.365700.

[51] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997, doi: https://doi.org/10.1137/s0097539795293172

[52] X. Qian and W. Wu, "An Efficient Ciphertext Policy Attribute-Based Encryption Scheme from Lattices and Its Implementation," 2021 IEEE 6th International Conference

on Computer and Communication Systems (ICCCS), Apr. 2021, doi: https://doi.org/10.1109/icccs52626.2021.9449182.

[53] I. Mustafa *et al.*, "A Lightweight Post-Quantum Lattice-Based RSA for Secure Communications," *IEEE Access*, vol. 8, pp. 99273–99285, 2020, doi: https://doi.org/10.1109/access.2020.2995801

[54] A. Abdulrahman, J.-P. Chen, Y.-J. Chen, V. Hwang, M. J. Kannwischer, and B.-Y. Yang, "Multi-moduli NTTs for Saber on Cortex-M3 and Cortex M4," IACR transactions on cryptographic hardware and embedded systems, pp. 127–151, Nov. 2021, doi: https://doi.org/10.46586/tches.v2022.i1.127-151.

[55] C.-M. M. Chung et al., "NTT multiplication for NTT-unfriendly rings," IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 159–188, Feb. 2021. doi:10.46586/tches.v2021.i2.159-188.

[56] Z.-Y. Wong, Denis, W.-K. Lee, Kai Meng Mok, W.-S. Yap, and A. Khalid, "KaratSaber: New Speed Records for Saber Polynomial Multiplication using Efficient Karatsuba FPGA Architecture," IEEE Transactions on Computers, pp. 1–13, Jan. 2023, doi: https://doi.org/10.1109/tc.2023.3238129.

[57] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," *Proceeding Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2010, pp. 1–23.

[58] A. Khalid, T. Oder, F. A. Valencia, Maire O' Neill, T. Güneysu, and F. Regazzoni, "Physical Protection of Lattice-Based Cryptography," Research Portal (Queen's University Belfast), May 2018, doi: https://doi.org/10.1145/3194554.3194616.

[59] Centers for Disease Control and Prevention (CDC) (2015) Behavioral Risk Factor Surveillance System (BRFSS) dataset. Available at: https://www.cdc.gov/brfss/ (Accessed: [Decembre 2024]).

[60] Aydin Aysu, M. Orshansky, and M. Tiwari, "Binary Ring-LWE hardware with power side-channel countermeasures," *Design, Automation & Test in Europe Conference & Exhibition (DATE), IEEE*, pp. 1253–1258, Mar. 2018, doi: https://doi.org/10.23919/date.2018.8342207ss

[61] S. Ebrahimi and Siavash Bayat-Sarmadi, “Lightweight and DPA-Resistant Post-Quantum Cryptoprocessor based on Binary Ring-LWE,” 2020 20th International Symposium on Computer Architecture and Digital Systems (CADS), Rasht, Iran, Aug. 2020, doi: https://doi.org/10.1109/cads50570.2020.9211858.

[62] Shaik Ahmadunnisa and Sudha Ellison Mathe, “CNC: A lightweight architecture for Binary Ring-LWE based PQC,” Microprocessors and microsystems, vol. 106, pp. 105044–105044, Apr. 2024, doi: https://doi.org/10.1016/j.micpro.2024.105044.

[63] S. Ebrahimi and S. Bayat-Sarmadi, “Lightweight and Fault Resilient Implementations of Binary Ring-LWE for IoT Devices,” IEEE Internet of Things Journal, pp. 1–1, 2020, doi: https://doi.org/10.1109/jiot.2020.2979318.

[64] D. Xu *et al.*, “Ring-ExpLWE:A High-performance and Lightweight Post-quantum Encryption Scheme for Resource-constrained IoT Devices,” *IEEE Internet of Things Journal*, pp. 1–1, 2022, doi: https://doi.org/10.1109/jiot.2022.3189210.

[65] E. Šabić, D. Keeley, B. Henderson, and S. Nannemann, “Healthcare and anomaly detection: using machine learning to predict anomalies in heart rate data,” AI & SOCIETY, May 2020, doi: https://doi.org/10.1007/s00146-020-00985-1.

[66] S. Park, K. H. Lee, B. Ko, and N. Kim, “Unsupervised anomaly detection with generative adversarial networks in mammography,” Scientific Reports, vol. 13, no. 1, Feb. 2023, doi: https://doi.org/10.1038/s41598-023-29521-z.

[67] M. Kavitha, S. Srinivas, P. S. Latha Kalyampudi, C. S. F, and Singaraju Srinivasulu, “Machine Learning Techniques for Anomaly Detection in Smart Healthcare,” in Proc. 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), Sep. 2021,

[68] L. Fang, Y. Li, Z. Liu, C. Yin, M. Li, and Z. J. Cao, “A Practical Model Based on Anomaly Detection for Protecting Medical IoT Control Services Against External Attacks,” IEEE Transactions on Industrial Informatics, vol. 17, no. 6, pp. 4260–4269, Jun. 2021, doi: https://doi.org/10.1109/tii.2020.3011444.

[69] Theyab Alsolami, B. Alsharif, and M. Ilyas, “Enhancing Cybersecurity in Healthcare: Evaluating Ensemble Learning Models for Intrusion Detection in the Internet of Medical

Things," Sensors, vol. 24, no. 18, pp. 5937–5937, Sep. 2024, doi: https://doi.org/10.3390/s24185937.

[70] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study," IEEE Access, vol. 8, no. 1, pp. 106576–106584, 2020, doi: https://doi.org/10.1109/access.2020.3000421.

[71] I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," IEEE Access, vol. 9, pp. 103906–103926, 2021, doi: https://doi.org/10.1109/access.2021.3094024.

[72] S. Das, M. Ashrafuzzaman, F. T. Sheldon, and S. Shiva, "Ensembling Supervised and Unsupervised Machine Learning Algorithms for Detecting Distributed Denial of Service Attacks," Algorithms, vol. 17, no. 3, p. 99, Feb. 2024, doi: https://doi.org/10.3390/a17030099.

[73] Y. Gu, K. Li, Z. Guo, and Y. Wang, "Semi-Supervised K-Means DDoS Detection Method Using Hybrid Feature Selection Algorithm," IEEE Access, vol. 7, pp. 64351–64365, 2019, doi: https://doi.org/10.1109/access.2019.2917532.

[74] Y. Meidan et al., "N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, Jul. 2018, doi: https://doi.org/10.1109/mprv.2018.03367731.

[75] N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," in IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3559-3570, April. 2020, doi: 10.1109/JIOT.2020.2973176.

[76] R. Doshi, N. Apthorpe, and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," in Proc. 2018 IEEE Security and Privacy Workshops (SPW), May 2018.

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

[78] K. Choi, J. Yi, C. Park and S. Yoon, "Deep Learning for Anomaly Detection in Time-Series Data: Review, Analysis, and Guidelines," in IEEE Access, vol. 9, pp. 120043-120065, 2021, doi: 10.1109/ACCESS.2021.3107975.

[79] B. Luo, H. Wang, H. Liu, B. Li, and F. Peng, “Early Fault Detection of Machine Tools Based on Deep Learning and Dynamic Identification,” IEEE Transactions on Industrial Electronics, vol. 66, no. 1, pp. 509–518, Jan. 2019, doi: https://doi.org/10.1109/TIE.2018.2807414.

[80] G. Abdelmoumin, D. B. Rawat and A. Rahman, "On the Performance of Machine Learning Models for Anomaly-Based Intelligent Intrusion Detection Systems for the Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4280-4290, March 2022, doi: 10.1109/JIOT.2021.3103829.

[81] I. G. A. Poornima and B. Paramasivan, “Anomaly detection in wireless sensor network using machine learning algorithm,” Computer Communications, vol. 151, pp. 331–337, Feb. 2020, doi: https://doi.org/10.1016/j.comcom.2020.01.005.

[82] M. Kavitha, S. Srinivas, P. S. Latha Kalyampudi, C. S. F, and Singaraju Srinivasulu, “Machine Learning Techniques for Anomaly Detection in Smart Healthcare,” in Proc. 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), Sep. 2021,

[83] J. Alsamiri and K. Alsubhi, “Internet of Things Cyber Attacks Detection using Machine Learning,” International Journal of Advanced Computer Science and Applications, vol. 10, no. 12, 2019, doi: https://doi.org/10.14569/ijacsa.2019.0101280.

[84] M. Hasan, Mohammad Shahriar Rahman, H. Janicke, and I. H. Sarker, “Detecting Anomalies in Blockchain Transactions using Machine Learning Classifiers and Explainability Analysis,” Blockchain. Research and applications, pp. 100207–100207, May. 2024, doi: https://doi.org/10.1016/j.bcra.2024.100207.

[85] K. Seol, Y.-G. Kim, E. Lee, Y.-D. Seo, and D.-K. Baik, “Privacy-Preserving Attribute-Based Access Control Model for XML-Based Electronic Health Record System,” IEEE Access, vol. 6, pp. 9114–9128, 2018, doi: https://doi.org/10.1109/access.2018.2800288.

[86] A. Sahi, D. Lai, and Y. Li, ‘‘A review of the state of the art in privacy and security in the eHealth cloud,’’ IEEE Access, vol. 9, pp. 104127–104141, 2021, doi: 10.1109/ACCESS.2021.3098708.

[87] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren, ‘‘d-MABE: Distributed multilevel attribute-based EMR management and applications,’’ IEEE Trans. Services Comput., vol. 15, no. 3, pp. 1592–1605, May 2022, doi:10.1109/TSC.2020.3003321.

[88] M. Tuler De Oliveira, L. H. A. Reis, Y. Verginadis, D. M. F. Mattos, and S. D. Olabarriaga, “SmartAccess: Attribute-Based Access Control System for Medical Records Based on Smart Contracts,” IEEE Access, vol. 10, pp. 117836–117854, 2022, doi: https://doi.org/10.1109/access.2022.3217201.

[89] B. S. Egala, A. K. Pradhan, V. R. Badarla, and S. P. Mohanty, “Fortified-Chain: A Blockchain Based Framework for Security and Privacy Assured Internet of Medical Things with Effective Access Control,” IEEE Internet of Things Journal, pp. 11717–11731, 2021, doi: https://doi.org/10.1109/jiot.2021.3058946.

[90] T Haritha and A Anitha, “Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain- Based Smart Contracts System,” IEEE Access, vol. 11, pp. 114322–114340, Jan. 2023, doi: https://doi.org/10.1109/access.2023.3324740.

[91] Z. Ying, L. Wei, Q. Li, X. Liu, and J. Cui, “A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud,” IEEE Access, vol. 6, pp. 53698–53708, 2018, doi: https://doi.org/10.1109/access.2018.2871170.

[92] Y. Zhang, D. He, and K.-K. R. Choo, “BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT,” Wireless Communications and Mobile Computing, vol. 2018, pp. 1–9, Nov. 2018, doi: https://doi.org/10.1155/2018/2783658.

[93] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems,” IEEE Access, vol. 7, pp. 66792–66806, 2019, doi: https://doi.org/10.1109/access.2019.2917555.

[94] R. Xu, Y. Chen, E. Blasch, and G. Chen, “BlendCAC: A Smart Contract Enabled Decentralized Capability-Based Access Control Mechanism for the IoT,” Computers, vol. 7, no. 3, p. 39, Jul. 2018, doi: https://doi.org/10.3390/computers7030039.

[95] O. Novo, “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT,” IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184–1195, Apr. 2018, doi: https://doi.org/10.1109/jiot.2018.2812239.

[96] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, “Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology,” Sustainable Cities and Society, vol. 39, pp. 283–297, May 2018, doi: https://doi.org/10.1016/j.scs.2018.02.014.

[97] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management,” 2016 2nd International Conference on Open and Big Data (OBD), vol. 1, no. 1, pp. 25–30, Aug. 2016, doi: https://doi.org/10.1109/obd.2016.11.

[98] S. K. B. Sangeetha, C. Selvarathi, S. K. Mathivanan, J. Cho and S. V. Easwaramoorthy, "Secure Healthcare Access Control System (SHACS) for Anomaly Detection and Enhanced Security in Cloud-Based Healthcare Applications," in IEEE Access, vol. 12, pp. 164543-164559, 2024, doi: 10.1109/ACCESS.2024.3492024.

[99] M. Misbahuddin, B. S. Bindhumadhava and B. Dheeptha, "Design of a risk based authentication system using machine learning techniques," 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), San Francisco, CA, USA, 2017, pp. 1-6, doi: 10.1109/UIC-ATC.2017.8397628.

[100] Menatalla Abououf, S. Singh, Rabeb Mizouni, and Hadi Otrok, “Explainable AI for Event and Anomaly Detection and Classification in Healthcare Monitoring Systems,” IEEE Internet of Things Journal, pp. 1–1, Jan. 2023, doi: https://doi.org/10.1109/jiot.2023.3296809.

[101] C. Picard and S. Pierre, “RLAuth: A Risk-Based Authentication System Using Reinforcement Learning,” IEEE access, vol. 11, pp. 61129–61143, Jan. 2023, doi: https://doi.org/10.1109/access.2023.3286376.

[102] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, “Vision and challenges for realising the Internet of Things,” Cluster of European research projects on the internet of things, European Commision, vol. 3, no. 3, pp. 34–36, 2010.

[103] J. Buchmann, F. Göpfert, T. Güneysu, T. Oder, and T. Pöppelmann, “High-Performance and Lightweight Lattice-Based Public-Key Encryption,” *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, May 2016, doi: https://doi.org/10.1145/2899007.2899011

[104] R. Chaudhary, G. S. Aujla, N. Kumar, and S. Zeadally, “Lattice based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions,” IEEE Internet of Things Journal, pp. 1–1, 2018, doi: https://doi.org/10.1109/jiot.2018.2878707

[105] S. Ebrahimi, S. Bayat-Sarmadi, and H. Mosanaei-Boorani, “Post-Quantum Cryptoprocessors Optimized for Edge and Resource-Constrained Devices in IoT,” IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5500–5507, Jun. 2019, doi: https://doi.org/10.1109/jiot.2019.2903082.

[106] C. Peikert, “Public-key cryptosystems from the worst-case shortest vector problem,” Symposium on the Theory of Computing, May 2009, doi: https://doi.org/10.1145/1536414.1536461.

[107] P. C. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,” Advances in Cryptology — CRYPTO ’96, pp. 104–113, 1996, doi: https://doi.org/10.1007/3-540-68697-5_9.

[108] T. Schneider, A. Moradi, and T. Güneysu, “ParTI - Towards Combined Hardware Countermeasures against Side-Channel and Fault-Injection Attacks.,” IACR Cryptology ePrint Archive, vol. 2016, p. 648, Jan. 2016

[109] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, “Introduction to differential power analysis,” Journal of Cryptographic Engineering, vol. 1, no. 1, pp. 5–27, Mar. 2011, doi: https://doi.org/10.1007/s13389-011-0006-y.

[110] O. Reparaz, Sujoy Sinha Roy, F. Vercauteren, and I. Verbauwhede, “A Masked Ring-LWE Implementation,” Springer eBooks, pp. 683–702, Jan. 2015, doi: https://doi.org/10.1007/978-3-662-48324-4_34.

[111] A. Karatsuba, Yu. Ofman, 'Multiplication of many-digital numbers by automatic computers', Dokl. Akad. Nauk SSSR, 145:2 (1962), 293–294," www.mathnet.ru. https://www.mathnet.ru/eng/dan26729 (accessed Aug. 09, 2023).

[112] L. Chen *et al.*, "Report on Post-Quantum Cryptography," *Report on Post-Quantum Cryptography*, Apr. 2016, doi: https://doi.org/10.6028/nist.ir.8105.

[113] P. He, Y. Tu, J. Xie, and H. Jacinto, "KINA: Karatsuba Initiated Novel Accelerator for Ring-Binary-LWE (RBLWE)-based Post-Quantum Cryptography," INDIGO (University of Illinois at Chicago), Aug. 2022, doi: https://doi.org/10.36227/techrxiv.20407134 .

[114] "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process." 2020. [Online]. Available: https://csrc.nist.gov/Projects/post-quantumcryptography/publications (accessed Aug. 09, 2023).

[115] M.-S. Chen and T. Chou, "Classic McEliece on the ARM Cortex-M4," IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 125–148, Jul. 2021, doi: https://doi.org/10.46586/tches.v2021.i3.125-148.

[116] J. Bos et al., "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM," 2018 IEEE European Symposium on Security and Privacy (EuroS&P), Apr. 2018, doi: https://doi.org/10.1109/eurosp.2018.00032.

[117] M. Albrecht et al., "Estimate all the {LWE, NTRU} schemes!," IACR Cryptology ePrint Archive, vol. 2018, p. 331, Jan. 2018.

[118] M. V. Beirendonck, J.-P. D'anvers, A. Karmakar, J. Balasch, and I. Verbauwhede, "A Side-Channel-Resistant Implementation of SABER," ACM Journal on Emerging Technologies in Computing Systems, vol. 17, no. 2, pp. 1–26, Apr. 2021, doi: https://doi.org/10.1145/3429983.

[119] D. Micciancio, "The hardness of the closest vector problem with preprocessing," IEEE Transactions on Information Theory, vol. 47, no. 3, pp. 1212–1215, Mar. 2001, doi: https://doi.org/10.1109/18.915688.

[120] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem: Extended abstract," in Proc. 41st Annu. ACM Symp. Theory Comput., 2009, pp. 333–342.

[121] J. Richter-Brockmann, J. Mono, and T. Guneysu, “Folding BIKE: Scalable Hardware Implementation for Reconfigurable Devices,” IEEE Transactions on Computers, vol. 71, no. 5, pp. 1204–1215, May 2022, doi: https://doi.org/10.1109/tc.2021.3078294.

[122] J. Howe, T. Oder, M. Krausz, and T. Güneysu, “Standard Lattice-Based Key Encapsulation on Embedded Devices,” IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 372–393, Aug. 2018, doi: https://doi.org/10.46586/tches.v2018.i3.372-393.

[123] H. Seo, M. Anastasova, A. Jalali, and R. Azarderakhsh, “Supersingular Isogeny Key Encapsulation (SIKE) Round 2 on ARM Cortex-M4,” IEEE Transactions on Computers, vol. 70, no. 10, pp. 1705–1718, Oct. 2021, doi: https://doi.org/10.1109/tc.2020.3023045.

[124] A. Sarker, M. M. Kermani, and R. Azarderakhsh, “Error Detection Architectures for Ring Polynomial Multiplication and Modular Reduction of Ring-LWE in $\boldsymbol{\frac{\mathbb{Z}/p\mathbb{Z}[x]}{x^{n}+1}}$ Benchmarked on ASIC,” IEEE Transactions on Reliability, vol. 70, no. 1, pp. 362–370, Mar. 2021, doi: https://doi.org/10.1109/tr.2020.2991671.

[125] X. Zhang and K. K. Parhi, “Reduced-Complexity Modular Polynomial Multiplication for R-LWE Cryptosystems,” ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Toronto, ON, Canada, 2021, pp. 7853-7857, doi: 10.1109/ICASSP39728.2021.9414005.

[126] X. Zhang, Zheang Huai, and K. K. Parhi, “Polynomial Multiplication Architecture with Integrated Modular Reduction for R-LWE Cryptosystems,” Journal of signal processing systems for signal, image, and video technology, vol. 94, no. 8, pp. 799–809, Apr. 2022, doi: https://doi.org/10.1007/s11265-022-01746-7.

[127] D. E. Knuth, The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1997.

[128] P. Pessl, “Analyzing the Shuffling Side-Channel Countermeasure for Lattice-Based Signatures,” Cryptology–INDOCRYPT 2016: 17th International Conference on Cryptology in India, Kolkata, India, pp. 153–170, Dec. 2016, doi: https://doi.org/10.1007/978-3-319-49890-4_9.

[129] T. Wunderer, “Revisiting the Hybrid Attack: Improved Analysis and Refined Security Estimates,” Cryptology ePrint Archive, 2016, Accessed: Mar. 08, 2023. [Online]. Available: https://eprint.iacr.org/2016/733

[130] Florian Göpfert, Christine van Vredendaal, and T. Wunderer, “A Hybrid Lattice Basis Reduction and Quantum Search Attack on LWE,” Lecture Notes in Computer Science, pp. 184–202, Jan. 2017, doi: https://doi.org/10.1007/978-3-319-59879-6_11

[131] D. V. Dimitrov, “Medical Internet of Things and Big Data in Healthcare,” Healthcare Informatics Research, vol. 22, no. 3, p. 156, 2021, doi: https://doi.org/10.4258/hir.2016.22.3.156.

[132] P. Manickam et al., “Artificial Intelligence (AI) and Internet of Medical Things (IoMT) Assisted Biomedical Systems for Intelligent Healthcare,” Biosensors, vol. 12, no. 8, p. 562, Jul. 2022, doi: https://doi.org/10.3390/bios12080562.

[133] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, “Security and Privacy in the Medical Internet of Things: A Review,” Security and Communication Networks, vol. 2018, pp. 1–9, 2018, doi: https://doi.org/10.1155/2018/5978636.

[134] T. Yaqoob, H. Abbas, and M. Atiquzzaman, ``Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices_ A review," IEEE Commun. Surveys Tuts., vol. 21, no. 4, pp. 3723_3768, 4th Quart., 2019, doi: 10.1109/COMST.2019.291409.

[135] T. Levy-Loboda, E. Sheetrit, I. F. Liberty, A. Haim, and N. Nissim, “Personalized insulin dose manipulation attack and its detection using interval-based temporal patterns and machine learning algorithms,” Journal of Biomedical Informatics, vol. 132, p. 104129, Aug. 2022, doi: https://doi.org/10.1016/j.jbi.2022.104129.

[136] P. Sharma, S. Jain, S. Gupta, and V. Chamola, “Role of machine learning and deep learning in securing 5G-driven industrial IoT applications,” Ad Hoc Networks, vol. 123, p. 102685, Dec. 2021, doi: https://doi.org/10.1016/j.adhoc.2021.102685.

[137] N. Moustafa and J. Slay, “UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” IEEE Xplore, Nov. 01, 2015. https://ieeexplore.ieee.org/document/7348942

[138] G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, and T.-Y. Liu, ‘‘LightGBM: A highly efficient gradient boosting decision tree,’’ in Proc. Adv. Neural Inf. Process. Syst., 2017, pp. 3146–3154.

[139] N. Farnaaz and M. A. Jabbar, ``Random forest modeling for network intrusion detection system," Procedia Comput. Sci., vol. 89, pp. 213-217, 2016.

[140] A. Gelbukh, F. C. Espinoza, and S. N. Galicia-Haro, ``The best neural network architecture," in Nature-Inspired Computation and Machine Learning (Lecture Notes in Computer Science: Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8857. Jul. 2014.

[141] S. A. Mulay, P. R. Devale, and G. V. Garje, “Intrusion Detection System Using Support Vector Machine and Decision Tree,” International Journal of Computer Applications, vol. 3, no. 3, pp. 40–43, Jun. 2010, doi: https://doi.org/10.5120/758-993.

[142] T. Cover and P. Hart, “Nearest neighbor pattern classification,” *IEEE Transactions on Information Theory*, vol. 13, no. 1, pp. 21–27, Jan. 1967, doi: https://doi.org/10.1109/tit.1967.1053964.

[143] G. J. M. Rosa, “The Elements of Statistical Learning: Data Mining, Inference, and Prediction by HASTIE, T., TIBSHIRANI, R., and FRIEDMAN, J.,” Biometrics, vol. 66, no. 4, pp. 1315–1315, Dec. 2010, doi: https://doi.org/10.1111/j.1541-0420.2010.01516.x.

[144] Y. Alotaibi and M. Ilyas, “Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things’ Devices Security,” Sensors, vol. 23, no. 12, pp. 5568–5568, Jun. 2023, doi: https://doi.org/10.3390/s23125568.

[145] Centers for Disease Control and Prevention (CDC) (2015) Behavioral Risk Factor Surveillance System (BRFSS) dataset. Available at: https://www.cdc.gov/brfss/ (Accessed: [Decembre 2024]).

[146] A. Alagha, S. Singh, R. Mizouni, J. Bentahar, and H. Otrok, “Target localization using Multi-Agent Deep Reinforcement Learning with Proximal Policy Optimization,” Future Generation Computer Systems, vol. 136, pp. 342–357, Nov. 2022, doi: https://doi.org/10.1016/j.future.2022.06.015.

[147] H.-N. Dai, H. Wang, G. Xu, J. Wan, and M. Imran, “Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies,” Enterprise Information Systems, vol. 14, no. 9–10, pp. 1–25, Jun. 2019, doi: https://doi.org/10.1080/17517575.2019.1633689.

[148] S. Li et al., “Efficient Data Retrieval Over Encrypted Attribute-Value Type Databases in Cloud-Assisted Ehealth Systems,” IEEE Systems Journal, vol. 16, no. 2, pp. 3096–3107, Jun. 2022, doi: https://doi.org/10.1109/jsyst.2021.3073169.

[149] H. Deng, Z. Qin, L. Sha, and H. Yin, “A Flexible Privacy-Preserving Data Sharing Scheme in Cloud-assisted IoT,” IEEE Internet of Things Journal, vol. 7, no. 12, pp. 1601–11611, 2020, doi: https://doi.org/10.1109/jiot.2020.2999350.

[150] M. Masud, G. S. Gaba, K. Choudhary, R. Alroobaea, and M. S. Hossain, “A robust and lightweight secure access scheme for cloud based E-healthcare services,” Peer-to-Peer Networking and Applications, vol. 14, no. 5, pp. 3043–3057, May 2021, doi: https://doi.org/10.1007/s12083-021-01162-x.

[151] Insider Threat Test Dataset; Software Engineering Institute: Pittsburgh, PA, USA, 2016.

[152] HL7 International, “FHIR Release 4 (R4),” [Online]. Available: https://hl7.org/fhir/R4/index.html. [Accessed: July 16, 2025].

[153] U.S. Department of Health and Human Services, “HIPAA Security Rule,” [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html. [Accessed: July 16, 2025].

[154] J. Glasser and B. Lindauer, “Bridging the Gap: A Pragmatic Approach to Generating Insider Threat Data,” IEEE Xplore, May 01, 2013. doi: https://ieeexplore.ieee.org/document/6565236.

[155] B. B. Sarhan and N. Altwaijry, “Insider Threat Detection Using Machine Learning Approach,” Applied Sciences, vol. 13, no. 1, p. 259, Dec. 2022, doi: https://doi.org/10.3390/app13010259.

ANNEXE A COMPARAISON DES SYSTÈMES DE DÉTECTION D'ANOMALIES UTILISANT DES APPROCHES D'APPRENTISSAGE AUTOMATIQUE POUR LES RÉSEAUX IOT ET IOMT

L'annexe présentée dans cette section fait partie intégrante de l'article 2, inclus dans cette thèse. Conformément à la version publiée de l'article, le titre et le contenu de tableau est conservés en anglais afin de préserver l'exactitude terminologique et la cohérence scientifique.

Table A. 1 Comparison of anomaly detection systems based on ML approaches on IoT and IoMT networks

Ref	Algorithms or Models	DataSet	IoT Application	Detected Attacks	Effectiveness					Efficiency		Real-time Prediction
					Accuracy	Precision	Recall	F1-Score	FPR	Trainin Time (s)	Testing Time (s)	
[8]	RF, LOF, IF, SVM, KNN	MIT- BIH	Healthcare	-	-	-	-	-	-	-	-	-
[9]	LR, XGBoost, RF, DT	Medicare Dataset(CMS) PrivateDataset (COIDA)	Healthcare	-	Yes	Yes	Yes	-	-	-	-	-
[10]	K-means, K-medoids partitioning	Collect its own dataset	Healthcare	-	Yes	-	-	-	-	Yes	Yes	-
[11]	R-FCVM	Collect its own dataset	Medical IoT	Replay attacks, Shoulder-surfing attacks, Malware attacks.	Yes	-	-	-	-	-	Yes	-
[12]	Ensemble learning (Stacking, Bagging, Boosting)	WUSTL-EHMS-2020	Medical IoT	Spoofing, Data injection	Yes	Yes	Yes	Yes	-	-	-	-

[14]	CNN1D, CNN2D,CNN3D	BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, IoT-23 intrusion detection datasets	IoT	DoS, DDoS, Scan, Theft, Mirai, MITM, MQTT Brute-Force, Sparta SSH Brute-Force, Agressive Scan, UDP Scan, File download, Heartbeat, C&C, Torri, Port Scan, Okiru	Yes	Yes	Yes	Yes	-	-	-	-
[15]	LR, SVM, NB, DT, NN, OCSVM_P, OCSVM_P, EE, ISOF, LOF	NSL-KDD, UNSW-NB15, CICIDS2017	IoT	DDoS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-
[17]	Deep autoencoder	Detection of IoT Botnet attacks	IoT	DDoS: UDP, TCP, SYN	-	-	-	-	Yes	-	-	-
[18]	semi-supervised deep extreme learning machine (SDELM)	UNB-ISCX	IoT	DDoS: UDP Floodign attacks	Yes	Yes	Yes	-	Yes	-	-	-
[19]	KNN, SVM, DT, RF, DNN	Synthetic Dataset	IoT	DDoS: TCP SYN Flood, UDP Flood, HTTP GET Flood	Yes	Yes	Yes	-	Yes	-	-	-
[20]	ANN, DT, KNN, NB, RF, SVM, CNN, EM, k means, SOM	CICIDS2017	IoT	BENIGN, Brute Force, XSS, SQL Injection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-
[23]	SVM_PCA, SVM_NN, SVM_PCA_NN	IoT_Botnet, IoT_Fridje	IoT, SmartHome	DoS, DDoS, XSS, Backdoor, Injection	Yes	Yes	Yes	Yes	-	-	-	-
[24]	LR, SVM, DT, RF,	collected in Intel Berkeley	IoT		Yes	Yes	Yes	Yes	-	-	-	-

	ANN, OLWPR	Research Lab (IBRL) from 54 mica sensors.		-								
[25]	LR, ANN	DS2OS traffic traces	IoT	DoS, Data Type Probing, Malicious Control, Malicious Operation, Scan, Spying, Wrong Setup	Yes	Yes	Yes	Yes	-	-	-	-
[26]	KNN, QDA, Iterative Dichotomiser ID3, RF, AdaBoost, MLP, NB	Bot-IoT	IoT	Probing attacks, DoS, Information Theft.	Yes	Yes	Yes	-	-	Yes	Yes	-
[27]	DT, Adaboost, RF, Gboost, Ensemble learning	Bitcoin transaction data	-	-	Yes	Yes	Yes	-	Yes	-	-	-
Our	**XGBoost, ANN, RF, IF, LR, KNN, SVM, STACKING**	**UNSW-NB15, New medical dataset with attacks**	**Medical IoT**	**Fuzzers, Exploit, Shellcode,Worms ,Reconnaissance, DoS, Backdoor, Analysis, Generic, Falsification**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

ANNEXE B ATTRIBUTION DES RÔLES À PARTIR DU JEU DE DONNÉES CERT INSIDER THREAT

L'annexe présentée dans cette section fait partie intégrante de l'article 3, inclus dans cette thèse. Conformément à la version soumise de l'article, le titre et le contenu de tableau est conservé en anglais afin de préserver l'exactitude terminologique et la cohérence scientifique.

Table B.1 Role Mapped from CERT insider threat dataset.

CERT Role	**Observed Behavior**	**Email/Web Usage**	**Mapped Healthcare Role**	**Justification**
Administrative Assistant	Starts mainly Afternoon/Evening	Low to medium	Hospital Receptionist	Typical front-desk staff profile—limited system use, regular hours, focused on patient intake.
Assembly Supervisor	Mostly Evening/Night	Low	ER Nurse	Always on late shifts, active emergency presence.
Computer Programmer	Irregular starts, many night ends	Low	ICU Nurse	Works across shifts, handling critical care data irregularly across 24 hours.
Electrical Engineer	Evening start, ends by Night	Low	On-call cardiologist	Frequent night shifts, aligns with emergency specialists.
Engineer	Evening work, some night activity	Low	Lab Technician	Balanced day/night shifts, lab roles are similar.
IT Admin	Massive late-day activity	High	Health IT Specialist	Heavy IT interaction and overnight work.
Management Trainer	Evening sessions, occasional nights.	Low	ER Doctor	Works during late hours, aligns with emergency roles.
Manager	Only morning starts, no variability	Medium	Family Doctor	Day-only work, regular schedules.
Physicist	Only morning starts, no variability	Low	Anesthesiologist	Day-only like scheduled procedures.
ProductionLineWorker	Extensive multi-shift, high activity	High	Nurse	All-hour shifts, essential care staff.
Salesman	Heavy late afternoon/evening use	Very High	Clinical Pharmacist	Pharmacists often work outside core hours, responding to medication needs across shift.

Scientist	Only morning work	Medium	Surgeon	Day shifts like scheduled procedures.
SoftwareEngineer	High usage, late ends	Very High	Radiology Technician	Mixed shifts, high availability needed.
SystemsEngineer	Evenly distributed logins	High	Sonographer	Split shifts, similar to imaging techs.
Technician	Night activity frequent	Medium	ICU Doctor	Early starts and evening ends, matches rehab roles.