

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

Ecole Nationale Supérieure en Informatique  
-08 Mai 1945- Sidi Bel Abbès (ESI-SBA)



# MÉMOIRE

En vue de l'obtention du diplôme du **Master**

Filière : **Informatique**

Spécialité : **Ingénierie des Systèmes Informatiques (ISI)**

## Thème

---

**Une étude comparative sur les méthodes de  
détection d'intrusion basées sur l'apprentissage  
automatique**

---

Présenté par :

Mlle. BENKADDOUR Zoubida Imene

Soutenu le : 03/07/2023

Devant le jury composé de :

- Dr. ANANI Djihed  
- Dr. KHALDI Miloud  
- Dr. MAHAMMED Nadir  
- Dr. BABA-AHMED Manel

Président  
Encadreur  
Co-Encadreur  
Examineur

*Année Universitaire : 2022 / 2023*

## *Remerciements*

Je tiens d'abord à remercier ALLAH le Tout-Puissant de m'avoir donné la force, la volonté, la santé et la patience pour réaliser ce travail.

J'adresse mes sincères remerciements tout particulièrement à mon encadrant, M. KHALDI Miloud, pour son encadrement de qualité, ses précieuses suggestions scientifiques, sa disponibilité et sa patience tout au long de ce travail. Ses immenses contributions, ses critiques constructives et sa compréhension ont été des éléments essentiels pour m'aider à progresser.

Je souhaite exprimer mes sincères remerciements à mon co-encadrant, M. MAHAMMED Nadir, pour sa précieuse contribution et son soutien durant cette période. Vos conseils éclairés et votre patience ont été d'une grande valeur pour moi.

J'adresse mes remerciements infinis à mes parents qui ont fait d'innombrables sacrifices pour moi, pour leur soutien et leurs encouragements.

Je tiens à remercier ma chère sœur Sarrah et mon cher frère Khalil. Leur présence et leur soutien constants ont été une source d'inspiration et de réconfort inestimables pour moi.

Je tiens également à remercier tous mes enseignants qui ont joué un rôle important dans ma formation au cours des cinq dernières années.

# *Résumé*

L'IoMT, ou Internet des objets médicaux, permet la collecte de données physiologiques à l'aide de capteurs intégrés dans le corps humain, formant ainsi un réseau corporel sans fil appelé WBAN. Ces données sont ensuite transmises à des serveurs distants pour une analyse continue par les professionnels de la santé.

Les avantages de cette technologie sont multiples, notamment la détection précoce des maladies et l'administration automatique de médicaments aux patients atteints de maladies chroniques. Cependant, l'IoMT présente des risques de sécurité importants, allant de la violation de la vie privée des patients aux attaques d'interception des données sans fil. Les données collectées sont particulièrement attractives pour les attaquants en raison de leur caractère sensible et privé. De plus, l'application de mesures de sécurité traditionnelles, telles que la cryptographie, sur des équipements médicaux ayant des capacités de calcul, de stockage et d'énergie limitées, associée à une communication hétérogène, représente un défi majeur. Ces méthodes de protection se révèlent également inefficaces contre les nouvelles attaques et les attaques zero-day.

Il est donc crucial de mettre en place des mesures de sécurité garantissant l'intégrité, la confidentialité et la disponibilité des données tout au long du processus de collecte, de transmission, de stockage et de traitement. C'est dans ce contexte que l'utilisation de systèmes de détection d'intrusion (IDS) basés sur l'apprentissage automatique (ML) peut offrir une solution de sécurité complémentaire adaptée aux caractéristiques spécifiques des systèmes IoMT.

Notre étude se concentre sur une analyse approfondie de la manière dont les IDS basés sur ML abordent ces problématiques de sécurité et de confidentialité.

**Mots-clés :** IDS, Apprentissage automatique, WBAN, IoMT.

# *Abstarct*

The IoMT, or Internet of Medical Things, enables the collection of physiological data through sensors integrated into the human body, forming a wireless body area network (WBAN). These data are then transmitted to remote servers for continuous analysis by healthcare professionals.

The advantages of this technology are numerous, including early disease detection and automatic medication administration for patients with chronic illnesses. However, the IoMT poses significant security risks, ranging from privacy violations to wireless data interception attacks. The collected data is particularly appealing to attackers due to its sensitive and private nature. Furthermore, implementing traditional security measures, such as cryptography, on medical devices with limited computing, storage, and energy capabilities, along with heterogeneous communication, presents a major challenge. These protection methods also prove ineffective against new and zero-day attacks.

Therefore, it is crucial to implement security measures that ensure the integrity, confidentiality, and availability of data throughout the collection, transmission, storage, and processing process. In this context, the use of Intrusion Detection Systems (IDS) based on Machine Learning (ML) can provide a complementary security solution tailored to the specific characteristics of IoMT systems.

Our study focuses on an in-depth analysis of how ML-based IDS addresses these security and privacy issues.

**Keywords:** WBAN, IoMT, IDS, machine learning, healthcare.