

الجمهورية الشعبية الديمقراطية الجزائرية
People's Democratic Republic of Algeria
وزارة التعليم العالي و البحث العلمي
Ministry of Higher Education and Scientific Research
المدرسة العليا للإعلام الآلي 8 ماي 1945 - سيدي بلعباس
Higher School of Computer Science
8 Mai 1945 - Sidi Bel Abbès



Thesis

To obtain the diploma of **Master's Degree**

Field of Study: **Computer Science**

Specialization: **Artificial Intelligence and Data Sciences**

Theme

**AI-Driven Intrusion Detection based on Feature
Selection for IoMT**

Presented by
Deghbouche Abdelmoumen
Djebbar Rabah Abderrazak

Defended on: **09 July 2025**
In front of the jury composed of

Dr. Bensenane Hamdane
Dr. Khaldi Miloud
Dr. Kechar Mohamed
Dr. Bendella Mohammed Salih

President of the Jury
Thesis Supervisor
Co-Supervisor & Incubator
Examiner

Academic Year: 2024/2025

Abstract

Due to limitations in device capabilities and data complexity, traditional Intrusion Detection Systems (IDS) are unable to mitigate the serious security vulnerabilities posed by the Internet of Medical Things' (IoMT) rapid proliferation. AI-driven security for the Internet of Medical Things (IoMT) is thoroughly examined in this thesis, with a focus on the challenge of balancing computational efficiency and detection accuracy. Sophisticated Feature Selection (FS) is essential to modern Intrusion Detection Systems' (IDS) ability to mitigate the "curse of dimensionality." The study thoroughly evaluates the effectiveness of wrapper-based feature selection techniques, specifically metaheuristic algorithms like Particle Swarm Optimization (PSO), in locating the best feature subsets within high-dimensional network data. The analysis reveals that while machine learning offers a powerful solution, there is still a significant gap in the development of powerful yet lightweight models. In order to create a strong security framework and guarantee patient safety in networked healthcare settings, this paper lays out the fundamental analysis for "Neye Sec," a proposed intrusion detection system (IDS) that will use the sophisticated metaheuristic WELL-PSO.

Keywords: Internet of Medical Things (IoMT), Intrusion Detection System (IDS), Machine Learning, Feature Selection, Metaheuristics, Particle Swarm Optimization (PSO), Cybersecurity, Resource-Constrained Systems.

Résumé

En raison des contraintes liées aux capacités des dispositifs et à la complexité des données, les systèmes de détection d'intrusion traditionnels (IDS) se révèlent incapables de contrer efficacement les importantes vulnérabilités de sécurité engendrées par la rapide expansion de l'Internet des objets médicaux (IoMT). Cette thèse examine de manière approfondie la sécurité pilotée par l'IA pour l'Internet des objets médicaux (IoMT), en se concentrant sur le défi de concilier l'efficacité computationnelle et la précision de la détection. Le processus de sélection de caractéristiques sophistiqué (FS) est crucial pour permettre aux systèmes actuels de détection d'intrusions (IDS) de contrer la "malédiction de la dimensionnalité". L'étude examine de manière approfondie l'efficacité des méthodes de sélection de caractéristiques basées sur des wrappers, en mettant l'accent sur l'utilisation d'algorithmes métaheuristiques tels que l'optimisation par essaims particuliers (PSO), afin d'identifier les sous-ensembles de caractéristiques les plus pertinents dans des données réseau de grande dimension. L'analyse met en évidence que malgré les avantages offerts par l'apprentissage automatique, il persiste une disparité notable dans la conception de modèles efficaces tout en étant légers. Dans le but d'établir un cadre de sécurité robuste et d'assurer la protection des patients au sein des milieux de soins de santé connectés, cette étude expose une analyse approfondie du système de détection d'intrusion (IDS) nommé "Neye Sec," qui fera appel à la métaheuristique avancée WELL-PSO.

Mots-clés : Internet des objets médicaux (IoMT), Système de détection d'intrusion (IDS), Apprentissage automatique, Sélection de caractéristiques, Métaheuristiques, Optimisation par essaim de particules (PSO), Cybersécurité, Systèmes à ressources limitées.

الملخص

نظراً للقيود المفروضة على قدرات المعالجة وتعقيد البيانات، أصبحت أنظمة الكشف التقليدية غير قادرة على التعامل بفعالية مع التهديدات السيبرانية المتزايدة الناتجة عن التوسع السريع لإنترنت الأشياء الطبية. تسلط هذه الأطروحة الضوء على دور الذكاء الاصطناعي في تعزيز أمن شبكات إنترنت الأشياء الطبية، مع التركيز على التحدي المتمثل في تحقيق التوازن بين الكفاءة الحاسوبية ودقة الكشف. وتعدّ عملية اختيار الميزات خطوة جوهرية لتمكين أنظمة كشف الهجمات من التغلب على مشكلة "لعنة الأبعاد". تتناول الدراسة بعمق فعالية أساليب اختيار الميزات المعتمدة على نماذج الأغلفة، مع التركيز على استخدام خوارزميات ميتاهيرستية مثل خوارزمية تحسين سرب الجسيمات، بهدف تحديد المجموعات الفرعية الأكثر أهمية من الميزات ضمن بيانات الشبكة عالية الأبعاد. ويبرز التحليل أنه، على الرغم من إمكانات التعلم الآلي، لا تزال هناك فجوة قائمة في تصميم نماذج تجمع بين الكفاءة والفعالية وخفة الوزن. ومن أجل تطوير إطار أمني متكامل يضمن حماية المرضى ضمن بيئات الرعاية الصحية المتصلة، تقدم هذه الدراسة تحليلاً معمقاً لنظام ذكي لكشف الهجمات يُعرف باسم "العين الآمنة"، ويعتمد على خوارزمية تحسين متقدمة تُسمى "تحسين سرب الجسيمات المعزز بالوزن الخطي".

الكلمات المفتاحية: إنترنت الأشياء الطبية، كشف الهجمات، التعلم الآلي، اختيار الميزات، الخوارزميات الميتاهيرستية، تحسين بواسطة السرب، الأمن السيبراني، الأنظمة محدودة الموارد.