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 Abbes

Thesis

To obtain the diploma of **Engineering 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
Djebarra Rabah Abderrazak
Deghbouche Abdelmoumen

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

Dr. Bensenane Hamdane	President of the Jury
Dr. Khaldi Miloud	Thesis Supervisor
Dr. Kechar Mohamed	Co-Supervisor & Incubator
Dr. Bendella Mohammed Salih	Examiner

Academic Year: 2024/2025

Abstract

The Internet of Medical Things (IoMT) revolutionises healthcare by providing remote patient monitoring, real-time diagnostics, and medical device communication. Integrated IoMT devices provide serious security risks to patient data, human lives, and healthcare infrastructure expenditures. The medical sector's digitalisation requires strong security to safeguard life-critical systems from sophisticated cyberattacks.

This research addresses the pressing need for IoMT-specific intrusion detection solutions. Developing an intrusion detection system and investigating metaheuristic algorithms in feature selection for threat identification are the main goals. We used CICIoMT2024 and NSL-KDD benchmark datasets and XGBoost, AdaBoost, LightGBM, Decision Tree, and Random Forest to achieve these goals.

Firefly algorithm, ROC-AUC analysis, CFS, and ReliefF are compared in our feature selection strategy. This work improves Particle Swarm Optimisation (PSO) convergence and feature selection by replacing uniform initialisation with the Well Equidistributed Long-period Linear (WELL1024) generator. Ney-Sec, a low-level, multi-threaded C++ system, offers real-time network monitoring and threat identification.

Demonstrating superior performance, AdaBoost with WELL-PSO excels on CICIoMT2024 and XGBoost with Firefly excels on NSL-KDD. Compared to other methods, including Lazrek et al.'s RFE/Ridge-ML/DL anomaly detection method, our WELL-PSO feature selection methodology works. Comprehensive testing in a controlled IoMT testbed proves the system's practicality.

This research provides an efficient, real-time intrusion detection solution that combines advanced machine learning techniques with optimised feature selection to protect critical healthcare infrastructure while meeting medical performance requirements.

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