الجمهورية الشعبية الديمقراطية الجزائرية

République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي **.08** ماي **1945.** بسيدي بلعباس

École Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbès

THESIS

To obtain the diploma of **State Engineer**
Field: **Computer Science**
Specialty: **Ingénierie Des Systèmes Informatique (ISI)**

Theme

Machine Learning-based Intrusion Detection System for IoT Applications

---

Presented by:

Khaoula KEBBATI

Submission Date : **September, 2023** In front of the jury composed of

Dr. Amina SOUYAH	Supervisor
Ing. Mohamed NEFFAH	Supervisor
Dr. XXXXXXXXXXXXXX	President
Dr. XXXXXXXXXXXXX	Examiner

Academic Year : 2022/2023

Abstract

The exponential growth of IoT (Internet of Things) devices has initiated a period of unparalleled interconnectivity and convenience, revolutionizing multiple facets of our everyday existence. Nevertheless, the interconnectivity of IoT ecosystems also renders them vulnerable to a multitude of security risks. The primary objective of this FYP thesis is to enhance the security of Internet of Things (IoT) applications by designing and implementing sophisticated Intrusion Detection Systems (IDS).

The crux of this study is around the development and implementation of a novel Intrusion Detection System (IDS) specifically designed for Internet of Things (IoT) deployments. Through a clever integration of machine learning (ML) and deep learning (DL), the Intrusion Detection System (IDS) reaches a height of accuracy and adaptability. The model undergoes extensive training using vast datasets of Internet of Things (IoT) traffic, allowing it to accurately differentiate between typical activity and potentially harmful actions with exceptional accuracy.

This thesis represents a significant milestone in the field of Internet of Things (IoT) security. By integrating machine learning (ML) and deep learning (DL) techniques into a hybrid Intrusion Detection System (IDS) model, it provides a robust and effective protection mechanism against emerging attacks that specifically aim at compromising Internet of Things (IoT) applications.

Key words : Internet of Things, Machine Learning, Deep Learning, IoT Attacks, Hybrid Detection, Intrusion Detection.

Résumé

La croissance exponentielle des dispositifs IoT (Internet des objets) a initié une période d'interconnectivité et de commodité inégalée, révolutionnant de multiples facettes de notre existence quotidienne. Néanmoins, l'interconnectivité des écosystèmes IoT les rend également vulnérables à une multitude de risques de sécurité. L'objectif principal de cette thèse PFE est d'améliorer la sécurité des applications de l'Internet des objets (IoT) en concevant et en mettant en œuvre des systèmes de détection d'intrusion (IDS) sophistiqués

L'essentiel de cette étude porte sur le développement et la mise en œuvre d'un nouveau système de détection d'intrusion (IDS) spécialement conçu pour les déploiements de l'Internet des objets (IoT). Grâce à une intégration intelligente de l'apprentissage automatique (ML) et de l'apprentissage profond (DL), le système de détection d'intrusion (IDS) atteint un niveau de précision et d'adaptabilité inégalé. Le modèle subit un entraînement intensif à l'aide de vastes ensembles de données du trafic de l'Internet des objets (IoT), ce qui lui permet de différencier avec précision les activités typiques des actions potentiellement nuisibles avec une précision exceptionnelle.

Cette thèse représente une étape importante dans le domaine de la sécurité de l'Internet des objets (IoT). En intégrant des techniques d'apprentissage automatique (ML) et d'apprentissage profond (DL) dans un modèle hybride de système de détection d'intrusion (IDS), elle fournit un mécanisme de protection robuste et efficace contre les attaques émergentes qui visent spécifiquement à compromettre les applications de l'Internet des objets (IoT).

Mots clés : Internet des objets, Apprentissage Automatique, Apprentissage Profond, Attaques IoT, Détection Hybride, Détection d'intrusion.
