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 **Engineering**
Field: **Computer Science**
Specialty: **Ingénierie Des Systèmes Informatique (ISI)**

Theme

Machine Learning-based Intrusion Detection System for IoT Applications

---

Presented by:

Dounia BRAHIMI

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

Dr. Amina SOUYAH	Supervisor
Ing. Mohamed NEFFAH	Supervisor
Dr. Belaila Amina	President
Dr. BABA Ahmed Manel	Examiner

Academic Year : 2022/2023

Abstract

In an era characterized by the pervasive integration of Internet of Things applications into critical infrastructure, the imperative to fortify cybersecurity measures has never been more pressing. This work endeavors to address this challenge through the development of a novel Machine Learning-based Intrusion Detection System tailored explicitly for IoT environments. Our approach revolves around the amalgamation of Machine Learning and Deep Learning techniques, leveraging Convolutional Neural Networks architectures for time series data analysis.

Our proposed solution focuses on the integration of ML and DL, with a particular emphasis on Convolutional Neural Networks for time series data analysis tailored to IoT environments. The central aim of this project revolves around two key objectives: firstly, to enhance the accuracy and efficacy of intrusion detection within IoT applications, and secondly, to fortify Threat Intelligence capabilities by identifying complex and evolving threat patterns with precision.

By Incorporating ensemble learning through concatenation into our hybrid approach we aim to create a versatile and resilient solution capable of effectively identifying intricate temporal and spatial patterns within IoT networks. The primary goal of this methodology is to overcome the limitations commonly associated with conventional IDS approaches.

Furthermore, the project seeks to highlight the potential of this ML-based IDS. We aim to explore its promise as a means to enhance intrusion detection and threat recognition in IoT ecosystems.These objectives extend to the broader realms of IoT security and safeguarding critical infrastructure, serving as a foundation for further investigation, scalability, and resource optimization.

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

Résumé

À une époque caractérisée par l'intégration généralisée des applications de l'internet des objets dans les infrastructures critiques, l'impératif de renforcer les mesures de cybersécurité n'a jamais été aussi pressant. Ce travail s'efforce de relever ce défi en développant un nouveau système de détection des intrusions basé sur l'apprentissage automatique et conçu explicitement pour les environnements IOT. Notre approche s'articule autour de l'amalgame des techniques d'apprentissage automatique et d'apprentissage profond, en tirant parti des architectures de réseaux neuronaux convolutifs pour l'analyse des données de séries temporelles.

La solution que nous proposons se concentre sur l'intégration de l'apprentissage automatique et de l'apprentissage profond, en mettant particulièrement l'accent sur les réseaux neuronaux convolutifs pour l'analyse des données de séries temporelles adaptées aux environnements IoT. Le but principal de ce projet tourne autour de deux objectifs clés : premièrement, améliorer la précision et l'efficacité de la détection d'intrusion dans les applications IoT, et deuxièmement, renforcer les capacités de renseignement sur les menaces en identifiant avec précision des modèles de menaces complexes et évolutifs.

En incorporant l'apprentissage d'ensemble par concaténation dans notre approche hybride, nous visons à créer une solution polyvalente et résiliente capable d'identifier efficacement des schémas temporels et spatiaux complexes au sein des réseaux IoT. L'objectif principal de cette méthodologie est de surmonter les limites communément associées aux approches IDS conventionnelles.

En outre, ce projet vise à mettre en évidence le potentiel de cet IDS basé sur l'apprentissage automatique. Ces objectifs s'étendent aux domaines plus larges de la sécurité de l'IoT et de la sauvegarde des infrastructures critiques, servant de base à des recherches plus approfondies, à l'évolutivité et à l'optimisation des ressources.

Mots clés: Internet des objets, Apprentissage Automatique, Apprentissage Profond, Attaques IoT, System de Détection des intrusions.
