الجمهورية الجزائرية الديمقراطية الشعبيةa

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث 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 **Master**
Field: **Computer Science**
Specialty: **Ingénierie Des Systèmes Informatique (ISI)**

Theme

Machine Learning-based Intrusion Detection System for IoT Applications : A State Of The Art

---

Presented by:

Dounia BRAHIMI **Khaoula KEBBATI**

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

Dr. Amina SOUYAH	Supervisor
Ing. Mohamed NEFFAH	Supervisor
Dr. Amina BELALIA	President
Dr. Manel BABA AHMED	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 master's thesis begins with a comprehensive exploration of the current state of the art in the field of intrusion detection systems with a specific focus on Machine Learning and Deep Learning techniques. The central objective of this project is twofold: firstly, to conduct a thorough review and analysis of various techniques and methodologies proposed in the IDS domain, and secondly, to present their respective outcomes and results.

The thesis delves into an extensive examination of existing intrusion detection techniques tailored explicitly for IoT environments. Through an in-depth evaluation of these methodologies, their strengths, weaknesses, and real-world applicability will be critically assessed. The study aims to identify emerging trends and advancements in ML and DL-based IDS, shedding light on their potential impact on cybersecurity practices.

Furthermore, this work seeks to provide valuable insights for researchers involved in enhancing the security of IoT ecosystems and critical infrastructure. By presenting a comprehensive overview of the state of the art, this master's thesis aims to serve as a foundational resource for informed decision-making and continued advancements in the dynamic field of intrusion detection within IoT environments.

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

Résumé

À une époque caractérisée par l'intégration omniprésente des applications de l'Internet des objets dans les infrastructures critiques, l'impératif de fortifier les mesures de cybersécurité n'a jamais été aussi pressant. Ce mémoire de master commence par une exploration complète de l'état actuel de l'art dans le domaine des systèmes de détection d'intrusion, avec un accent particulier sur les techniques d'apprentissage automatique et d'apprentissage profond. L'objectif central de ce projet est double : premièrement, effectuer un examen et une analyse approfondis des différentes techniques et méthodologies proposées dans le domaine des IDS, et deuxièmement, présenter leurs résultats respectifs.

La thèse se penche sur un examen approfondi des techniques de détection d'intrusion existantes conçues explicitement pour les environnements IoT. Grâce à une évaluation approfondie de ces méthodologies, leurs forces, leurs faiblesses et leur applicabilité dans le monde réel seront évaluées de manière critique. L'étude vise à identifier les tendances émergentes et les avancées dans les IDS basés sur la ML et la DL, en mettant en lumière leur impact potentiel sur les pratiques de cybersécurité.

En outre, ce travail vise à fournir des informations précieuses aux chercheurs impliqués dans l'amélioration de la sécurité des écosystèmes IoT et des infrastructures critiques. En présentant une vue d'ensemble de l'état de l'art, ce mémoire de maîtrise vise à servir de ressource fondamentale pour une prise de décision éclairée et des progrès continus dans le domaine dynamique de la détection des intrusions dans les environnements IoT.

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