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 **Master**
Field: **Computer Science**
Specialty: **Ingénierie des Systèmes Informatiques (ISI)**

Theme

Intrusion Detection System based on Deep learning and Complex event processing for IoT environments

---

Presented by:
Ilyes Dhiaeddine Belmiloud

Submission Date: **October, 2024**
In front of the jury composed of:

Mr. AZZA Mohamed	Président
Mr. KHALDI Miloud	Examinateur
Ms. KECHAR Mohamed	Incubateur
Ms. Amina Souyah	Supervisor
Mr. Mohamed Neffah	Co-Supervisor

Academic Year : 2023/2024

Abstract

The rapid expansion of the Internet of Things (IoT) and Industrial IoT (IIoT) ecosystems presents significant security challenges, particularly in safeguarding these networks from cyber threats. This thesis explores the use of Artificial Intelligence (AI) in enhancing Intrusion Detection Systems (IDS) for IoT environments. Specifically, the research investigates the application of advanced AI techniques, such as deep learning and Complex Event Processing (CEP), to improve the detection of network intrusions. Through an extensive literature review, this thesis highlights the potential of hybrid AI models, including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Gated Recurrent Units (GRU), in capturing complex patterns in network traffic. Furthermore, the integration of CEP offers real-time detection and response capabilities. The study concludes with a discussion of the challenges, opportunities, and future research directions for AI-based IDS in IoT security, focusing on emerging techniques like federated learning and adaptive IDS models.

Keywords— IoT Security, Intrusion Detection System, Machine Learning, Deep Learning, Complex Event Processing, AI in IoT, Cybersecurity.

الملخص

تواجه شبكات إنترنت الأشياء (IoT) وإنترنت الأشياء الصناعي (IIoT) تحديات كبيرة في مجال الأمان، خاصة فيما يتعلق بالحماية من التهديدات السيبرانية. تهدف هذه الأطروحة إلى استكشاف استخدام الذكاء الاصطناعي (AI) في تعزيز أنظمة الكشف عن التطفل (IDS) في بيئات إنترنت الأشياء. تركز الدراسة على استقصاء تقنيات الذكاء الاصطناعي المتقدمة، مثل التعلم العميق ومعالجة الأحداث المعقدة (CEP)، لتحسين اكتشاف التطفل على الشبكات. من خلال مراجعة الأدبيات، تسلط الأطروحة الضوء على إمكانات النماذج الهجينة للذكاء الاصطناعي، بما في ذلك الشبكات العصبية التلافيفية (CNN) وذاكرة المدى الطويل (LSTM) ووحدات البوابات التكرارية (GRU)، في تحليل الأنماط المعقدة في حركة مرور الشبكات. كما تناقش الأطروحة التحديات والفرص واتجاهات البحث المستقبلية لأنظمة الكشف عن التطفل القائمة على الذكاء الاصطناعي في مجال أمن إنترنت الأشياء، مع التركيز على تقنيات جديدة مثل التعلم الفيدرالي والنماذج التكيفية لأنظمة الكشف

الكلمات المفتاحية: أمان إنترنت الأشياء، نظام كشف التطفل، التعلم الآلي، التعلم العميق، معالجة الأحداث المعقدة، الذكاء الاصطناعي في إنترنت الأشياء، الأمن السيبراني

Résumé

L'expansion rapide des écosystèmes de l'Internet des objets (IoT) et de l'IoT industriel (IIoT) présente d'importants défis de sécurité, notamment dans la protection de ces réseaux contre les cybermenaces. Cette thèse explore l'utilisation de l'intelligence artificielle (IA) pour améliorer les systèmes de détection d'intrusion (IDS) dans les environnements IoT. En particulier, la recherche examine l'application de techniques avancées d'IA, telles que l'apprentissage profond et le traitement d'événements complexes (CEP), pour améliorer la détection des intrusions réseau. À travers une revue de littérature approfondie, cette thèse met en lumière le potentiel des modèles hybrides d'IA, y compris les réseaux neuronaux convolutifs (CNN), les mémoires à long terme (LSTM) et les unités récurrentes à portes (GRU), dans la capture de modèles complexes dans le trafic réseau. De plus, l'intégration du CEP offre des capacités de détection et de réponse en temps réel. L'étude conclut par une discussion des défis, opportunités et pistes de recherche future pour les IDS basés sur l'IA dans la sécurité IoT, avec un accent particulier sur des techniques émergentes telles que l'apprentissage fédéré et les modèles IDS adaptatifs.

Keywords— Sécurité IoT, Système de détection d'intrusion, Apprentissage automatique, Apprentissage profond, Traitement d'événements complexes, IA dans l'IoT, Cybersécurité.