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 **Engineer**
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 has introduced significant security challenges, particularly in protecting these networks from cyberattacks. This thesis presents an advanced Intrusion Detection System (IDS) that combines machine learning, rule-based classification, and Complex Event Processing (CEP) to detect and respond to network intrusions in real-time. The IDS is built using the Edge-IIoTset dataset, which contains a variety of cyberattack scenarios relevant to IoT/IIoT environments.

A hybrid deep learning model, incorporating Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Gated Recurrent Units (GRU), was developed to label and classify the dataset, achieving an accuracy of 96.68%. The IDS further incorporates rule-based classifiers, such as PART, for rule extraction. These rules were deployed within the Esper CEP engine, enabling real-time detection and alerting.

The IDS is complemented by a web-based dashboard built using AdminLTE, which provides real-time insights into the types and frequency of detected attacks, enhancing network security management. This approach effectively balances high detection accuracy with interpretability, making it suitable for real-time deployment in resource-constrained IoT environments.

Finally, the thesis discusses the limitations of the proposed system and suggests future research directions, including the exploration of federated learning, multi-stage attack detection, and adaptive IDS models to further improve security in evolving IoT ecosystems.

Keywords— IoT Security, Intrusion Detection System, Edge-IIoTset, Machine Learning, Rule-Based Classification, PART, Complex Event Processing, Esper, CNN-LSTM-GRU, Real-Time Detection, Network Security.

الملخص

أدى التوسع السريع في أنظمة إنترنت الأشياء (IoT) وإنترنت الأشياء الصناعي (IIoT) إلى ظهور تحديات أمنية كبيرة، خاصة فيما يتعلق بحماية هذه الشبكات من الهجمات السيبرانية. تقدم هذه الأطروحة نظام كشف التسلل (IDS) متقدم يجمع بين التعلم الآلي، التصنيف القائم على القواعد، ومعالجة الأحداث المعقدة (CEP) للكشف عن التسللات الشبكية والاستجابة لها في الوقت الفعلي. يعتمد نظام IDS على مجموعة بيانات Edge-IIoTset، التي تحتوي على مجموعة متنوعة من سيناريوهات الهجمات السيبرانية ذات الصلة ببيئات IIoT/IoT.

تم تطوير نموذج تعلم عميق هجين، يدمج بين الشبكات العصبية التلافيفية (CNN)، والذاكرة طويلة المدى (LSTM)، ووحدات التكرار المبوّبة (GRU)، لتسمية وتصنيف مجموعة البيانات، وحقق دقة تصل إلى 96.68%. كما يتضمن نظام IDS مصنفات تعتمد على القواعد، مثل PART، لاستخراج القواعد. تم نشر هذه القواعد داخل محرك Esper CEP، مما أتاح الكشف في الوقت الفعلي وتوليد التنبيهات.

يُكمل نظام IDS لوحة معلومات مبنية على الويب باستخدام AdminLTE، توفر رؤى في الوقت الفعلي حول أنواع الهجمات المكتشفة وتكرارها، مما يعزز إدارة أمان الشبكة. توازن هذه الطريقة بشكل فعال بين الدقة العالية في الكشف والقابلية للتفسير، مما يجعلها مناسبة للتطبيق في الوقت الفعلي في بيئات IoT محدودة الموارد.

أخيرًا، تناقش الأطروحة حدود النظام المقترح وتقترح اتجاهات بحث مستقبلية، بما في ذلك استكشاف التعلم الفيدرالي، الكشف عن الهجمات متعددة المراحل، ونماذج IDS التكيفية لتحسين الأمان في أنظمة IoT المتطورة.

الكلمات المفتاحية: أمن إنترنت الأشياء، نظام كشف التسلل، Edge-IIoTset، التعلم الآلي، التصنيف القائم على القواعد، الجزء، معالجة الأحداث المعقدة، إسبر،CNN-LSTM-GRU، الكشف في الوقت الحقيقي، أمن الشبكات.

Résumé

L'expansion rapide des écosystèmes de l'Internet des objets (IoT) et de l'IoT industriel (IIoT) a introduit des défis de sécurité importants, notamment dans la protection de ces réseaux contre les cyberattaques. Cette thèse présente un système de détection d'intrusion (IDS) avancé combinant l'apprentissage automatique, la classification basée sur des règles et le traitement d'événements complexes (CEP) pour détecter et répondre aux intrusions réseau en temps réel. L'IDS est construit à partir du jeu de données Edge-IIoTset, qui contient une variété de scénarios de cyberattaques pertinents pour les environnements IoT/IIoT.

Un modèle d'apprentissage profond hybride, incorporant des réseaux neuronaux convolutifs (CNN), des mémoires à long terme (LSTM) et des unités récurrentes à portes (GRU), a été développé pour étiqueter et classifier le jeu de données, atteignant une précision de 96,68 %. L'IDS intègre également des classificateurs basés sur des règles, tels que PART, pour l'extraction de règles. Ces règles ont été déployées dans le moteur CEP Esper, permettant une détection et des alertes en temps réel.

L'IDS est complété par un tableau de bord web développé avec AdminLTE, offrant des informations en temps réel sur les types et la fréquence des attaques détectées, améliorant ainsi la gestion de la sécurité réseau. Cette approche équilibre efficacement une haute précision de détection avec une interprétabilité, la rendant adaptée pour un déploiement en temps réel dans des environnements IoT à ressources limitées.

Enfin, la thèse discute des limites du système proposé et suggère des pistes de recherche futures, notamment l'exploration de l'apprentissage fédéré, la détection d'attaques en plusieurs étapes et les modèles IDS adaptatifs pour améliorer la sécurité dans des écosystèmes IoT en évolution.

Keywords— Sécurité de l'IoT, Système de détection d'intrusion, Edge-IIoTset, Apprentissage automatique, Classification fondée sur des règles, PART, Traitement d'événements complexes, Esper, CNN-LSTM-GRU, Détection en temps réel, Sécurité des réseaux.