الجمهورية الشعبية الديمقراطية الجزائرية
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
Ecole Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbes

MEMOIRE

En vue de l'obtention du diplôme de **Master**

Filière : **Informatique**

Spécialité : **Systèmes d'Information et Web (SIW)**

Thème

Anomaly-based Intrusion Detection System for IoT network using machine learning and deep learning techniques

---

Présenté par **:**

- Melle Houria RAFAA
- Mr Ayoub MEKKAOUI

Soutenu le : **21/09/2020** Devant le jury composé de :

-	Mr BENSLIMANE Sidi Mohamed	Professeur	Président
-	Mr MALKI Mimoun	Professeur	Encadreur
-	Mr MALKI Abdelhamid	Docteur	Encadreur
-	Mr BENABDERRAHMANE Sid Ahmed	Docteur	Encadreur
-	Mr AMAR BENSABER Djamel	Docteur	Examinateur
-	Mr BENDAOUD Fayssal	Docteur	Examinateur

Année Universitaire : 2019 / 2020

Abstract

The Internet of Things (IoT) is a system of interconnected objects that enables the communication of humans with different devices. It has expanded into several areas such as health, agriculture. However, the nature of the IoT architecture has created new security challenges, especially in the IoT network which presents the largest scale of an IoT system.

Anomaly-based intrusion detection systems (IDSs) are an effective way to prevent abnormal traffic in the IoT network. It is known that the IoT architecture is getting more complicated day by day, which makes traditional methods like statistical-based or knowledge-based for anomaly detection face difficulties detecting unknown attacks in real-time. Therefore, machine learning and deep learning technique show excellent performance in detecting small anomalous data over time. These advanced techniques give resilient mechanisms to prevent novel attacks due to its high-level of discovering hidden patterns in the data.

The goal of this work is to provide a set of research that proposes anomaly-based intrusion detection system using machine learning and deep learning techniques. We then thoroughly discuss the advantages and the shortcoming of each approach. Our report also presents via a summary table a comparison of the presented approaches. Finally, our conclusion and future work are identified.

Keywords: Internet of Things, Anomaly detection, Machine learning, Deep learning, security.

Résumé

L'internet des objets (IoT) est un système d'objets interconnectés qui permet la communication des humains avec différents appareils. Il a pu s'étendre à plusieurs domaines tels que la santé, l'agriculture. Cependant, la nature de l'architecture Iot a a créé de nouveaux défis de sécurité, en particulier la sécurité du réseau Iot qui présente la plus grande échelle d'un système IoT.

Les systèmes de détection d'intrusion (IDS) à base d'anomalies sont un moyen efficace de prévenir le trafic anormal dans le réseau Iot. Il est connu que l'architecture IoT se complique de jour en jour, ce qui rend les méthodes traditionnelles comme les méthodes basées sur les statistique ou basées sur la connaissance pour la détection d'anomalies confrontent des difficultés de détection d'attaques inconnues en temps réel. Par conséquent, l'apprentissage automatique et l'apprentissage profond montrent des performances excellentes de détection de petites anomalies au fil du temps. Ces techniques avancées offrent un mécanisme résilient pour empêcher de nouvelles attaques grâce à la grande aptitude de découverte de patterns cachés dans les données.

L'objectif de ce travail est de fournir un ensemble de recherches qui ont proposé un système de détection d'intrusions à base d'anomalies en utilisant des techniques d'apprentissage automatique et d'apprentissage profond. Nous discutons ensuite en profondeur des avantages et des inconvénients de chaque approche. Notre rapport présente également via un tableau récapitulatif une comparaison des approches présentées. Une conclusion et nos future perspectives sont identifiées.

Mot Clé: Internet des objets,Détection d'anomalie,apprentissage automatique,apprentissage profond,sécurité

مُلخص

إنترنت الأشياء)IoT(هو نظام مِن الأشياء المُترابطة التي تُمكّن مِن التّواصل بينَ البشر ومختلف الأجهزة. ولقد توسّعت لتشمل العديد مِن المجالات مثل الصّحة والزّراعة. لكن في المقابل، خلقت طبيعة بُنية إنترنت الأشياء تحديّات أمان جديدة ، خاصة في شبكة إنترنت الأشياء التي تُعتبر أهم وأكبر جزء في هذا النظام.

تُعد أنظمة كشف التسلل والاختراق)SDI(القائمة على كشف العناصر الدّخيلة وغير المألوفة طريقةً فعّالة لمنع مرور بيانات غير طبيعيّة في شبكة إنترنت الأشياء. ومِن المعروف أنَّ بُنية إنترنت الأشياء تزدادُ تعقيدًا يومًا بعد يوم ، مِمَّا يجعل الطُرق التّقليدية في كشف العناصر الدَّخيلة استنادًا إلى الإحصائيات أو المعرفة تواجه صُعوباتٍ في الكشف عن الهجمات غير المعروفة في الوقت الحقيقيّ. غير أنَّ تقنيات تعلُّم الآلة و التَّعلم العميق يُظهران أداءً مُتازًا في الكشف عن البيانات الصَّغيرة غير المألوفة والمُتغيِّرة مع الزمن. تُوفر هذه التقنيات المُتقدِّمة آلياتٍ مرنة لمنع الهجمات الجديدة نظرًا لامتلاكها مُستوى عالٍ مِن اكتشاف الأنماط المَخفيّة في البيانات.

الهدف من هذا العمل هو توفير مجموعة مِن الأبحاث الّتي تقترح أنظمةً لكشف التّسلل والاختراق قائمة على كشف العناصر غير المألوفة باستخدام تقنيات تعلُّم الآلة و التّعلم العميق. نُناقِش بدقّة في هذا التقرير مزايا وعيوب كل مقاربة ونَعرضُ أيضًا مِن خلال جدول موجز مُقارنة للمقاربات المعروضة. أخيرًا سنقدّم استنتاجًا ختاميًا و وموجزًا عن أعمالنا المقبلة في هذا الصدد.

كلمات مفتاحيّة: : إنترنت الأشياء، كشف العناصر غير المألوفة، تعلم آلة، تعلم عميق، أمن معلوماتي.