الكشف عن هجمات إنترنت الأشياء باستخدام التعلم الآلي

اعداد: جادل مرزوق السميري

اشراف: د.خالد الصبحي

المستخلص

يجمع انترنت الأشياء (IoT) بين مئات الملايين من الأجهزة القادرة على التفاعل مع بعضها مع الحد الأدنى من التفاعل البشري. إنترنت الأشياء هي واحدة من أسرع المناطق نمواً في مجال الحوسبة؛ ومع ذلك، فإن الواقع هو أنه في بيئة معادية للغاية للإنترنت، فإن إنترنت الأشياء عرضة لأنواع عديدة من الهجمات الإلكترونية. لحل هذه المشكلة، يجب اتخاذ تدابير مضادة عملية لتأمين شبكات إنترنت الأشياء، مثل اكتشاف الشذوذ في الشبكة. بغض النظر عن أنه لا يمكن تجنب الهجمات تمامًا إلى الأبد، فإن الاكتشاف المبكر للهجوم أمر أساسي للدفاع العملي. نظرًا لأن أجهزة إنترنت الأشياء ذات سعة تخزين منخفضة وقدرة معالجة منخفضة، فإن حلول الأمان التقليدية المتطورة لحماية نظام إنترنت الأشياء ليست مناسبة. أيضًا، أجهزة إنترنت الأشياء متصلة الآن دون تدخل بشري لفترات أطول .هذا يعني انه يجب تطوير حلول أمنية ذكية قائمة على الشبكة مثل حلول التعلم الآلي .على الرغم من أن العديد من الدراسات التي تمت في السنوات الأخيرة ناقشت استخدام حلول التعلم الآلي في مشاكل اكتشاف الهجمات، إلا أنها لم يتم إيلاء اهتمام كبير لاكتشاف الهجمات على وجه التحديد في شبكات انترنت الاشياء .في هذه الدراسة ،نهدف الى المساهمة في الادب من خلال تقييم خوارزميات التعلم الآلي المختلفة التي يمكن استخدامها للكشف بسرعة وفعالية هجمات شبكة إنترنت الأشياء .تم استخدام مجموعة بيانات جديدة ،Bot-IoT، لتقييم خوارزميات الكشف المختلفة. في مرحلة التنفيذ، تم استخدام سبع خوارزميات مختلفة للتعلم الآلي، وحقق معظمها أداءً عالياً. تم استخراج ميزات جديدة من مجموعة بيانات Bot-IoT أثناء التنفيذ ومقارنتها بدراسات من الأدب ،الميزات الجديدة أعطت نتائج أفضل.

IoT Cyber Attacks Detection Using Machine Learning

By: Jadel Marzouq Alsamiri
Supervised By
Dr. Khalid Ateatallah Alsubhi

ABSTRACT

The Internet of Things (IoT) combines hundreds of millions of devices which are capable of interact with each other with minimum human interaction. IoT is one of the fastest- growing areas in of computing; however, the reality is that in the extremely hostile environment of the internet, IoT is vulnerable to numerous types of cyberattacks. To resolve this, practical countermeasures need to be established to secure IoT networks, such as network anomaly detection. Regardless that attacks cannot be wholly avoided forever, early detection of an attack is crucial for practical defense. Since IoT devices have low storage capacity and low processing power, traditional high-end security solutions to protect an IoT system are not appropriate. Also, IoT devices are now connected without human intervention for longer periods. This implies that intelligent network-based security solutions like machine learning solutions must be developed. Although many studies in recent years have discussed the use of Machine Learning (ML) solutions in attack detection problems, little attention has been given to the detection of attacks specifically in IoT networks. In this study, we aim to contribute to the literature by evaluating various machine learning algorithms that can be used to quickly and effectively detect IoT network attacks. A new dataset, Bot-IoT, is used to evaluate various detection algorithms. In the implementation phase, seven different machine learning algorithms were used, and most of them achieved high performance. New features were extracted from the Bot-IoT dataset during the implementation and compared with studies from the literature, and the new features gave better results.