كشف التسلل في إنترنت الأشياء باستخدام التعلم العميق

اسم الباحث

علاء محمد احمد باناعمه

بحث مقدم لنيل درجة الماجستير في تقنية المعلومات

إشراف

د. افتخار احمد خان

كلية الحاسبات وتقنية المعلومات

جامعة الملك عبدالعزيز

جدة،المملكة العربية السعودية

جمادى الآخر١٤٤٤ هـ - يناير٢٠٢٣ م

المستخلص

يستخدم الأمن السيبراني على نطاق واسع في العديد من التطبيقات، مثل الأنظمة الصناعية الذكية، والمنازل، والأجهزة الشخصية، والسيارات، وعليه شهد تطورات وابتكارات، لكنها لم تزل تواجه تحديات في حل المشكلات المتعلقة بأساليب الأمان لأجهزة إنترنت الأشياء. تم تقديم طرق أمنية فعالة، مثل التعلم العميق لاكتشاف التسلل، وركزت الأبحاث الحديثة على تحسين خوارزميات التعلم العميق لتحسين الأمان في إنترنت الأشياء.

يستكشف هذا البحث طرق اكتشاف التطفل التي يتم تنفيذها باستخدام التعلم العميق، ويقارن أداء طرق التعلم العميق المختلفة، ويحدد أفضل طريقة لتنفيذ اكتشاف التسلل في إنترنت الأشياء. يتم إجراء هذا البحث باستخدام نماذج التعلم العميق القائمة على الشبكات العصبية التلافيفية (CNN) والذاكرة طويلة المدى (LSTM) والوحدات المتكررة ذات البوابات (GRUs). وتم مقارنة أربع مجموعات بيانات، وهي IoT - Bot وUNSW - NB15 وCICIDS 2017 و٢٣ - IoT، لتحديد حدود كل مجموعة بيانات كما تم استخدام ثلاثة مصنفات لتحديد درجات الدقة والدقة و F1 لكل مجموعة بيانات.

تم التوصل من خلال نتائج البحث لأنسب مجموعات البيانات التي تستخدم لتحسين اكتشاف البرامج الضارة وخروقات البيانات وأنشطة الشبكة غير الطبيعية في إنترنت الأشياء، ومن بين جميع مجموعات البيانات، تم اعتبار نموذج LSTM هو الأكثر دقة، يليه GRU وCNN. المرجو هو أن يساعد البحث في تحسين الأمان في أجهزة إنترنت الأشياء ومساعدة الباحثين في تحديد أفضل طريقة لتنفيذ طرق اكتشاف التسلل في شبكات إنترنت الأشياء.

الكلمات المفتاحية: تعلم عميق؛ كشف التسلل؛ إنترنت الأشياء. الشبكات العصبية التلافيفية. ذاكرة طويلة المدى ؛ الوحدات المتكررة ذات البوابات ؛ الأمن الإلكتروني

Intrusion detection in IoT using deep learning.

By

Alaa Mohammed Banaamah

A thesis submitted for the requirements of the degree of Master of Science in Information Technology

Advisor

Dr. Iftikhar Ahmad Khan

Faculty of Computing and Information Technology
King Abdulaziz University
Jeddah, Saudi Arabia
Jumada Al-Akher 1444 H - January 2023 G

Abstract

Cybersecurity has been widely used in various applications, such as intelligent industrial systems, homes, personal devices, and cars, and has led to innovative developments that continue to face challenges in solving problems related to security methods for IoT devices. Effective security methods, such as deep learning for intrusion detection, have been introduced. Recent research has focused on improving deep learning algorithms for improved security in IoT.

This research explores intrusion detection methods implemented using deep learning, compares the performance of different deep learning methods, and identifies the best method for implementing intrusion detection in IoT. This research is conducted using deep learning models based on convolutional neural networks (CNNs), long short-term memory (LSTM), and gated recurrent units (GRUs). Four datasets, namely, Bot-IoT, CICIDS 2017, UNSW-NB15, and IoT-23, are compared to identify the boundaries of each dataset. Three classifiers are used to determine the accuracy, precision, and F1 scores of each dataset.

The research results reveal the suitable datasets for improving the detection of malware, data breaches, and abnormal network activities in IoT. For all the datasets, the LSTM model is the most accurate, followed by GRU and CNN. The research is expected to help improve security in IoT devices and assist researchers in identifying the best method for implementing intrusion detection methods in IoT networks.

Key Word: Deep Learning; Intrusion Detection; IoT; Convolutional Neural Networks; Long Short-term Memory; Gated Recurrent Units; Cybersecurity; Bot-IoT, CICIDS 2017, UNSW-NB15, IoT-23.