applied sciences

MDPI

Article

Anomaly Detection Using Deep Neural Network for IoT Architecture

Zeeshan Ahmad [1,2], Adnan Shahid Khan [1,*], Kashif Nisar [3,4,*], Iram Haider [3], Rosilah Hassan [5], Muhammad Reazul Haque [6], Seleviawati Tarmizi [1] and Joel J. P. C. Rodrigues [7,8]

[1] Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia; zayshan@kku.edu.sa (Z.A.); swati@unimas.my (S.T.)
[2] Department of Electrical Engineering, College of Engineering, King Khalid University, Abha 62529, Saudi Arabia
[3] Faculty of Computing and Informatics, Universiti Malaysia Sabah, Jalan UMS, Kota Kinabalu 88400, Malaysia; iramhaider765@yahoo.com
[4] Department of Computer Science and Engineering, Hanyang University, Seoul 04763, Korea
[5] Centre for Cyber Security, Faculty of Information Science and Technology (FTSM), Universiti Kebangsaan Malaysia, Bangi 43600, Malaysia; rosilah@ukm.edu.my
[6] Faculty of Computing & Informatics, Multimedia University, Persiaran Multimedia, Cyberjaya 63100, Malaysia; reazul@ieee.org
[7] Post-Graduation Program on Electrical Engineering, Federal University of Piauí (UFPI), Teresina 64049-550, PI, Brazil; joeljr@ieee.org
[8] Covilhã Delegation, Instituto de Telecomunicações, 6201-001 Covilhã, Portugal
* Correspondence: skadnan@unimas.my (A.S.K.); kashif@ums.edu.my (K.N.)

check for updates

Citation: Ahmad, Z.; Shahid Khan, A.; Nisar, K.; Haider, I.; Hassan, R.; Haque, M.R.; Tarmizi, S.; Rodrigues, J.J.P.C. Anomaly Detection Using Deep Neural Network for IoT Architecture. *Appl. Sci.* **2021**, *11*, 7050. https://doi.org/10.3390/app11157050

Academic Editor: Juan Francisco De Paz Santana

Received: 9 May 2021
Accepted: 12 July 2021
Published: 30 July 2021

Abstract: The revolutionary idea of the internet of things (IoT) architecture has gained enormous popularity over the last decade, resulting in an exponential growth in the IoT networks, connected devices, and the data processed therein. Since IoT devices generate and exchange sensitive data over the traditional internet, security has become a prime concern due to the generation of zero-day cyberattacks. A network-based intrusion detection system (NIDS) can provide the much-needed efficient security solution to the IoT network by protecting the network entry points through constant network traffic monitoring. Recent NIDS have a high false alarm rate (FAR) in detecting the anomalies, including the novel and zero-day anomalies. This paper proposes an efficient anomaly detection mechanism using mutual information (MI), considering a deep neural network (DNN) for an IoT network. A comparative analysis of different deep-learning models such as DNN, Convolutional Neural Network, Recurrent Neural Network, and its different variants, such as Gated Recurrent Unit and Long Short-term Memory is performed considering the IoT-Botnet 2020 dataset. Experimental results show the improvement of 0.57–2.6% in terms of the model's accuracy, while at the same time reducing the FAR by 0.23–7.98% to show the effectiveness of the DNN-based NIDS model compared to the well-known deep learning models. It was also observed that using only the 16–35 best numerical features selected using MI instead of 80 features of the dataset result in almost negligible degradation in the model's performance but helped in decreasing the overall model's complexity. In addition, the overall accuracy of the DL-based models is further improved by almost 0.99–3.45% in terms of the detection accuracy considering only the top five categorical and numerical features.

Keywords: IoT architecture; deep neural network; anomaly detection; deep learning; network-based intrusion detection system

1. Introduction

IoT is a revolutionary computing paradigm that has evolved rapidly over the last decade in almost every technological domain, such as smart homes, smart industries, smart transportation, smart healthcare [1–4], use of sensors [5–8], smart cities, and satellites [9], to name a few [10]. It comprises many IoT devices (Things) equipped with different sensors,