Received: 8 February 2023 | Revised: 2 May 2023 | Accepted: 25 May 2023

DOI: 10.1002/ett.4810

RESEARCH ARTICLE

WILEY

MS-ADS: Multistage Spectrogram image-based Anomaly Detection System for IoT security

Zeeshan Ahmad[1,2] | **Adnan Shahid Khan**[1] | **Kartinah Zen**[1] | **Farhan Ahmad**[3]

[1]Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan, Malaysia

[2]Department of Electrical Engineering, College of Engineering, King Khalid University, Abha, Kingdom of Saudi Arabia

[3]Expleo Group UK, Derby, United Kingdom

Correspondence
Zeeshan Ahmad and Adnan Shahid Khan, Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia.
Email: zayshan@kku.edu.sa and skadnan@unimas.my

Funding information
Universiti Malaysia Sarawak

Abstract

The innovative computing idea of Internet-of-Things (IoT) architecture has gained tremendous popularity over the last decade, resulting in an exponential increase in the connected devices and the data processed in the IoT networks. Since IoT devices collect a massive amount of sensitive information exchanged over the traditional internet, security has become a prime concern due to the more frequent generation of network anomalies. A network-based anomaly detection system can provide the much-needed efficient security solution to the IoT network by detecting anomalies at the network entry points through constant traffic monitoring. Despite enormous efforts by researchers, these detection systems still suffer from lower detection accuracy in detecting anomalies and generate a high false alarm rate and false-negative rate in classifying network traffic. To this end, this paper proposes an efficient Multistage Spectrogram image-based network Anomaly Detection System (MS-ADS) using a deep convolution neural network that utilizes a short-time Fourier Transform to transform flow features into spectrogram images. The results demonstrate that the proposed method achieves high detection accuracy of 99.98% with a reduction in the false alarm rate to 0.006% in classifying network traffic. Also, the proposed scheme improves predicting the anomaly instances by 0.75% to 4.82%, comparing the benchmark methodologies to exhibit its efficiency for the IoT network. To minimize the computational and training cost for the model re-training phase, the proposed solution demonstrates that only 40500 network flows from the dataset suffice to achieve a detection accuracy of 99.5%.

1 | INTRODUCTION

The Internet-of-Things (IoT) has emerged as a novel, revolutionary, and ground-breaking computing idea over the previous few years that has been widely welcomed by the technological sectors, such as smart cities having smart homes, smart healthcare, smart industries, smart grids, smart transportation, etc. to name a few.[1] It contains many IoT devices (called Things) that have limited storage, computation, and communication capabilities and are embedded with various types of