



All



ADVANCED SEARCH

Conferences > 2023 IEEE International Confe... ?

Cross Model Verification of Intrusion Detection System on IoT Using Convolutional Neural Network

Publisher: **IEEE**

[Cite This](#)

PDF

V. Surya ; C. Shanthi [All Authors](#) ...



28
Full
Text Views

Alerts

[Manage Content Alerts](#)
[Add to Citation Alerts](#)

Abstract



Downl
PDF

Document Sections

- I. Introduction
- II. Overview of Datasets
- III. Methodology
- IV. Experimental Results and Analysis
- V. Conclusion

Abstract:

The IDS to secure IoT devices have become so important with the tremendous growth in the field of IoT. The potential damage to the IoT network by different types of attac... [View more](#)

Metadata

Abstract:

The IDS to secure IoT devices have become so important with the tremendous growth in the field of IoT. The potential damage to the IoT network by different types of attacks is increasing rapidly with the increased use of IoT devices. Therefore, IDS has become an essential defense tool against the vulnerable attacks. These IoT devices are to be continuously monitored for attacks, hence IDS software is deployed to detect anomalies. Today ML and DL algorithms which are subset of Artificial Intelligence are widely used in the intrusion detection system to detect attacks. In this research work, the cross verification of the outputs of IDS using CNN on three different datasets namely NSLKDD, IDS2018 and IOTID20 are explored. Intrusion detection in the context of the IoT has become a critical concern due to the proliferation of connected devices and evolving attack techniques. Traditional IDS often struggle to adapt to the unique challenges posed by IoT environments. This article explores the application of CNNs for intrusion detection in IoT and discusses the significance of cross-model verification to enhance security and accuracy. The AUC score yielded an accuracy of more than 80-95% in 15 epochs in all the three datasets. Both binary and multiclassification are done. Further it is observed that the ROC curve is above the diagonal line signifying the model is excellent. Moreover, a new feature selection algorithm SELBEST is proposed based on Stochastic gradient descent, which significantly reduced the features. Also, the classification time is reduced and the performance is increased.

[Authors](#)

[Figures](#)

[References](#)

[Keywords](#)

[Metrics](#)

[More Like This](#)



Published in: 2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG)

Date of Conference: 08-09 December 2023

DOI: 10.1109/ICTBIG59752.2023.10456135

Date Added to IEEE Xplore: 19 March 2024

Publisher: IEEE

► ISBN Information:

Conference Location: Indore, India

 **Contents**

I. Introduction

The Internet of things technology provides enumerable services and forms a global infrastructure for the information society. It enables services to interconnect existing and evolving communication technologies. Also, the communication between the devices is done without human intervention. With the advancement in IoT technology, the cyber-attacks are also increased. The biggest challenge in IoT is to prevent the computer network from harmful attacks [1]. Some of the main security techniques are firewalls, antivirus software and IDSs. These techniques protect the network attacks. The IDS is a software mechanism, which when deployed, monitors and protects the IoT devices from attacks and signals an alarm when an unknown signal is recognised. IDS plays a vital role among other techniques in intrusion detection[2]. To overcome this problem, researchers started working constructing IDS using Artificial intelligence techniques namely ML and DL. Using ML and DL techniques, useful information can be extracted from massive datasets[3]. When the training dataset is available, the attack variants are easily detected using Machine learning based IDS. Deep Learning on the other hand can be used to achieve outstanding performance. In deep learning feature extraction is done hand in hand with model classification. There are multiple hidden layers in deep learning, hence the output is accurate. The process takes more time compared to Machine learning[4]. Both the techniques are widely employed in all fields of technology. In this paper, we explore on deep learning model - Convolutional Neural Network on three different datasets namely NSLKDD, IDS2018 and IOTID20. The cross-model verification of the output for all the data sources are analysed. It took a longer duration to measure the performance of the model, hence for better efficiency and to eventually increase the speed, a feature selection algorithm based on the SGD, a generic optimization algorithm SELBEST is proposed and its performance is measured. IoT devices, ranging from smart home gadgets to industrial sensors, are vulnerable to a wide array of cyber threats. Traditional IDS primarily designed for networks with conventional traffic patterns may not effectively detect IoT -specific attacks. CNNs, which have excelled in computer vision, exhibit promise for IoT intrusion detection by leveraging their ability to capture spatial patterns in data.

Sign in to Continue Reading

Authors	▼
Figures	▼
References	▼
Keywords	▼
Metrics	▼

More Like This

Cognitive Memory-Guided AutoEncoder for Effective Intrusion Detection in Internet of Things
IEEE Transactions on Industrial Informatics
Published: 2022

A Few-Shot-Based Model-Agnostic Meta-Learning for Intrusion Detection in Security of Internet of Things
IEEE Internet of Things Journal
Published: 2023

Show More

IEEE Personal Account

CHANGE
USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED
DOCUMENTS

Profile Information


COMMUNICATIONS
PREFERENCES
PROFESSION AND
EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800
678 4333
WORLDWIDE: +1 732
981 0060
CONTACT & SUPPORT

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#)  | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.

IEEE Account

- » [Change Username/Password](#)
- » [Update Address](#)

Purchase Details

- » [Payment Options](#)
- » [Order History](#)
- » [View Purchased Documents](#)

Profile Information

- » [Communications Preferences](#)
- » [Profession and Education](#)
- » [Technical Interests](#)

Need Help?

- » **US & Canada:** +1 800 678 4333
- » **Worldwide:** +1 732 981 0060
- » [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.