R-IDPS: Real time SDN based IDPS system for IoT security

Publisher: IEEE

Cite This PDF

Noman Mazhar ; Rosli Salleh ; Muhammad Zeeshan ; M. Muzaffar Hameed ; Nauman … **All Authors**

115
Full
Text Views

Alerts

Manage Content Alerts

Add to Citation Alerts

More Like This

Q-DATA: Enhanced Traffic Flow Monitoring in Software-Defined Networks applying Q-learning
2019 15th International Conference on Network and Service Management (CNSM)
Published: 2019

Combining software-defined networking with Internet of Things: Survey on security and performance aspects
2017 International Conference on Engineering & MIS (ICEMIS)
Published: 2017

Show More

Downl
PDF

Abstract: Internet of things increases the automation pace of the world but at the same time, IoT poses many security challenges for the industry. Intrusion detection and preventio... **View more**

Metadata

Abstract:

Internet of things increases the automation pace of the world but at the same time, IoT poses many security challenges for the industry. Intrusion detection and prevention systems have dominated the market for security in conventional networks. The challenge to IDPS is huge resource utilization and imparting performance penalties. Also, real-time training of detection machine learning models has been an issue. In this research, we develop an agent-based IDPS system using software-defined networking (SDN) technology at its core. The system develops a baseline profile for the IoT network by analyzing data from all the devices under normal conditions. Based on this profile, we extract the network traffic features. Using these features, we construct our dataset for anomaly detection in the network. For detection, we use a support vector machine to detect ICMP flood and TCP SYN flood attacks. The R-IDPS machine learning model is capable of real-time training. The proposed model (R-IDPS) is fully capable of mitigating attacks using SDN technology. The main objective of the research is to analyze the accuracy of the proposed SDN-

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

Keywords

Metrics

More Like This

based intrusion detection system especially under the stress conditions of DDoS attacks. Simulation results show 97 % to 99 % of attack detection accuracy with no false positives. The R-IDPS is scalable for both large and heterogeneous IoT networks.

Published in: 2021 IEEE 18th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)

Date of Conference: 11-13 October 2021

INSPEC Accession Number: 21509640

Date Added to IEEE *Xplore*: 30 November 2021

DOI: 10.1109/HONET53078.2021.9615449

▸ **ISBN Information:**

Publisher: IEEE

▸ **ISSN Information:**

Conference Location: Karachi, Pakistan

▸ **Funding Agency:**

Contents

I. Introduction

A great number of applications are based on Internet of Things (IoT) devices, this results in the development and customization of related conventional technologies. This makes the IoT devices prone to cyber-attacks; and has become very challenging these days to guard IoT devices from these attacks. Formally, the conventional IDSs are not suitable for deployment in IoT devices because of resource constraints in terms of storage, processing power, and energy consumption. However, almost most of the mobile traffic data will originate from smart devices by the end of 2022 [1]. One of the limitations of Signature based approach is to detect new kinds of attacks. However anomaly detection systems using statistical techniques are more effective to detect the new attacks, the problem of the high false-positive rate is one of the main challenges [2], [3].

Sign in to Continue Reading

Authors

Figures

References

Keywords

Metrics

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

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

© Copyright 2022 IEEE - All rights reserved.

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 2022 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close