

Conferences > 2024 IEEE 3rd International C...

ΑII

Enhancing Anomaly Detection of IoT using Knowledge-Based and Federated Deep Learning

Publisher: IEEE

Cite This



Tabassum Simra; Bharath Konatham; Fathi Amsaad; Mohamed I. Ibrahem; Noor Zaman Jhanjhi All Authors •••

55Full
Text Views



Q

ADVANCED SEARCH

Manage Content Alerts

Add to Citation Alerts

Abstract

٨

Downl

Document Sections

- I. Introduction
- II. Related Work
- III. Methodology and Experimental Setup
- IV. Results and Discussion
- V. Conclusion

Authors

Figures

References

Keywords

Metrics

More Like This

Abstract:

IoT encompasses an extensive range of sensors and physical devices that establish connections with diverse applications via networking technologies, enabling communicatio... **View more**

✓ Metadata

Abstract:

loT encompasses an extensive range of sensors and physical devices that establish connections with diverse applications via networking technologies, enabling communication with the Internet and other devices. Because of the increasing number of assaults on IoT applications, it is crucial to ensure strong cybersecurity as the number of users for IoT grows and new services appear. This article examines the importance of securing IoT applications and evaluates the effectiveness of integrating knowledge distillation and federated learning techniques with Deep Learning algorithms to enhance IDS for protecting IoT applications. The utilization of a combination of knowledge distillation and federated learning showcases the potential for achieving many advantages, including enhancing model performance, expediting the learning process, and safeguarding user data privacy. These advantages have been demonstrated to surpass conventional learning approaches.

Published in: 2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI)

Date of Conference: 13-14 April 2024 **DOI:** 10.1109/ICMI60790.2024.10585693

Date Added to IEEE Xplore: 11 July 2024 Publisher: IEEE

▶ ISBN Information: Conference Location: Mt Pleasant, MI, USA





I. Introduction

The Internet of Things (IoT) has made things like sensors and everyday objects connect to each other, changing how industries work by letting them gather data and control things remotely [1]. But this also makes things risky because many devices can be hacked [2]. This ignith the Contribution Restdirtion systems (IDS) come in. They watch over the network and devices all the time to find and stop any strange or unauthorized activities. This is important to keep data and devices safe. The mix of IoT and IDS is a big deal because it helps protect against cyber threats.

Authors	~
Figures	~
References	~
Keywords	~
Metrics	~

More Like This

Enhancing Accuracy in Gas-Water Two-Phase Flow Sensor Systems Through Deep-Learning-based Computational Framework

IEEE Sensors Journal Published: 2024

Enhancement of the Multiplexing Capacity and Measurement Accuracy of FBG Sensor System Using IWDM Technique and Deep Learning Algorithm Journal of Lightwave Technology

Published: 2020

Show More

IEEE Personal Account	Purchase Details	Profile Information	Need Help?	Follow
CHANGE USERNAME/PASSWORD	PAYMENT OPTIONS VIEW PURCHASED	COMMUNICATIONS PREFERENCES	US & CANADA: +1 800 678 4333	f ⊚ in □
	DOCUMENTS	PROFESSION AND EDUCATION	WORLDWIDE: +1 732 981 0060	
		TECHNICAL INTERESTS	CONTACT & SUPPORT	

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.

