DEEP LEARNING FOR TRUSTWORTHY AND RELIABLE CYBERATTACK DETECTION IN INDUSTRIAL IOT SYSTEMS

[1]D. Saikrishna, [2]Yalam Bhavana Reddy
[1]Assistant Professor, [2]MCA Student
Department Of MCA Student
Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT

The reliability and sustainability of the Industrial Internet of Things (IIoT) to prevent fatalities while carrying out vital tasks is a basic requirement of the stakeholders. Basic security features like trust, privacy, security, dependability, resilience, and safety are all included in a reliable IIoT-enabled network. Due to outdated security mechanism modifications, restricted update choices, and protocol variations, the conventional security processes and mechanisms are unable to safeguard these networks. Because of this, these networks need new methods to improve security and privacy measures and raise the degree of trust. In order to increase the credibility of IIoT-enabled networks, we thus suggest an innovative strategy in this study. We provide a precise and trustworthy method for detecting cyberattacks in these networks using supervisory control and data acquisition (SCADA) networks. The suggested plan integrates SCADA-based IIoT networks with deep learning-based pyramidal recurrent units (PRU) and decision trees (DT). In order to identify cyberattacks in SCADA-based IIoT networks, we also employ an ensemble-learning technique. High detection rates are made possible by the ensemble DT's and PRU's nonlinear learning capabilities, which reduce the sensitivity of irrelevant features. Fifteen datasets derived from SCADA-based networks are used to assess the suggested approach. The experimental findings demonstrate that the suggested methodology works better than both conventional techniques and machine learning-based detection strategies. The suggested plan enhances IIoT-enabled networks' security and related trustworthiness metrics.

1. INTRODUCTION

THE Industrial Internet of Things (IIOT) is a pervasive network that connects a diverse set of smart appliances in the industrial environment to deliver various intelligent services. In IIOT networks, a significant amount of industrial control systems (ICSs) premised on supervisory control and data acquisition(SCADA) are linked to the corporate network through the Internet [1]. Typically, these SCADA-based IIOT networks consist of a large number of field devices [2], for instance, intelligent electronic devices, sensors, and actuators, connected to an enterprise network via heterogeneous communications [3]. This integration provides the industrial networks and systems with supervision and a lot of flexibility and agility [2]–[4], resulting in greater production and resource efficiency. On the other hand, this integration exposes SCADA-based IIOT networks to serious

security threats and vulnerabilities, posing a significant danger to these networks and the trustworthiness of the systems [5]. The trustworthiness of an IIOT-enabled system ensures that it performs as expected while meeting a variety of security requirements, including trust, security, safety, reliability, resilience, and privacy [6]–[8]. Fig. 1 depicts the fundamental aspects of trustworthiness in an IIoT-enabled network. The basic goal of the IIOT-enabled system is to increase trustworthiness by safeguarding identities, data, and services, and therefore to secure SCADA-based IIOT networks from cybercriminals [8], [9].

Several protocol updates have been proposed to meet this purpose, including the distributed network protocol (DNP 3.0) [10]. However, it covers authentication and data integrity aspects only, leaving numerous holes for attackers to use known flaws like hash collision to carry out serious attacks [11]. Information Technology and Industrial Operational technology bodies build a typical risk management plan utilizing ISO 27005:2018 [10] to recognize, rank, and implement alleviation techniques in automated or semi automated enterprises. A comprehensive risk management plan and adequate preventive measures may not ensure absolute security against growing risks and attacks. This consequently offers a difficult research challenge for industrial and cyber security control researchers to 1) obtain the maximum degree of attack detection, 2) report malicious behavior as soon as it appears, and 3) isolate the afflicted subsystems as soon as possible. In recent years, there has been a surge toward the utility of artificial intelligence (AI) methods in evolving cyber security approaches, including attack prediction [12], privacy preservation [13], forensic exploration [14], and malware disclosure [15]. Deep learning (DL) is an AI approach that incorporates better learning models with considerable success in various disciplines [16]. However, designing a reliable and trustworthy AI, particularly a DL-based cyber attack detection model for the IIOT platforms, remains a research problem.

By considering the limitations of previous techniques, we employ network attributes of industrial protocols and propose a pyramidal recurrent unit (PRUs)- and decision tree (DT)-based ensemble detection mechanism. The proposed mechanism has the potential to detect cyber attacks in any extensive industrial network. The interoperability with other detection engines and expandability for a wider industrial network with multiple areas distinguishes the proposed mechanism from previous studies. The proposed detection method is disseminable across many IIOT domains. Furthermore, our model is straightforward to implement and deploy and can improve efficiency and accuracy while overcoming the shortcomings of previous efforts. The following capabilities can characterize the novelty and contribution of our article.

1) We propose a scalable and efficient DL- and DT-based ensemble cyber-attack detection framework to resolve trustworthiness issues in the SCADA-based IIOT networks.

2) We present an efficient probing approach by the SCADA based network data to solve

the protocol mismatch limitations of traditional security solutions for the IIOT platform. Fig. 2 . SCADA-based industrial IOT network .

3) A statistical analytic approach for ensuring the trustworthiness and reliability of the proposed model for SCADA based IIOT networks.

The rest of the article is organized as follows. In Section II, we have discussed the basics of problem formulation. In Section III, we have given details of our proposed work, followed by the results and discussion in Section IV. Finally, Section V concludes this article.

2. LITERATURE SURVEY

"A novel mobile and hierarchical data transmission architecture for smart factories"

In a smart factory environment, a much larger amount of data are transmitted in the workshop networks bringing big challenges to data transfer capability and energy usage efficiency. In the workshop, two main networks, i.e., wired/wireless fieldbus networks and wireless sensor networks, are usually used to collect and transmit data separately; thus, this paper proposes a mobile and hierarchical data transmission architecture to integrate these two networks also taking advantages from the existing mobile intelligence in smart factories, such as automatic guided vehicles (AGVs), to implement a novel data and materials delivery scheme well suited for modern industrial wireless sensor networks (IWSNs). Simulation experiments demonstrated how the proposed approach, running within the IWSN, significantly increases data delivery efficiency along with achieving better energy usage, by 4 times, with respect to the separated networks without any mobile intelligence support.

"Cyber-physical framework for emulating distributed control systems in smart grids"

This paper proposes a cyber-physical framework for investigating distributed control systems operating in the context of smart-grid applications. At the moment, the literature focuses almost exclusively on the theoretical aspects of distributed intelligence in the smart-grid, meanwhile, approaches for testing and validating such systems are either missing or are very limited in their scope. Three aspects need to be taken into account while considering these applications: (1) the physical system, (2) the distributed computation platform, and (3) the communication system. In most of the previous works either the communication system is neglected or oversimplified, either the distributed computation aspect is disregarded, either both elements are missing. In order to cover all these aspects, we propose a framework which is built around a fleet of low-cost single board computers coupled with a real-time simulator. Additionally, using traffic control and network emulation, the flow of data between different controllers is shaped so that it replicates various quality of service (QoS) conditions.

The versatility of the proposed framework is shown on a study case in which 27 controllers self-coordinate in order to solve the distributed optimal power flow (OPF) algorithm in a dc network.

"Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges"

Cyber Physical Systems (CPS) are almost everywhere; they can be accessed and controlled remotely. These features make them more vulnerable to cyber attacks. Since these systems provide critical services, having them under attack would have dangerous consequences. Unfortunately, cyber attacks may be detected, but after the damage is done. Therefore, developing a cyber system that can survive an attack is a challenge. In this paper, we are surveying the literature on security aspects of CPSs. First, we present some of existing methods for detecting cyber attacks. Second, we focus on three main cyber attacks, which are: Denial of service (DoS), deception, and replay attacks. In our discussion, we have surveyed some exiting models of these attacks, approaches of filtering CPS subject to these attacks, and approaches of control CPS subject to these attacks.

3. EXISTING SYSTEM

The Internet of Things (IoT) has revolutionized modern tech with interconnected smart devices. While these innovations offer unprecedented opportunities, they also introduce complex security challenges. Cybersecurity is a pivotal concern for intrusion detection systems (IDS). Deep Learning has shown promise in effectively detecting and preventing cyberattacks on IoT devices. Although IDS is vital for safeguarding sensitive information by identifying and mitigating suspicious activities, conventional IDS solutions grapple with challenges in the IoT context. This paper delves into the cutting-edge intrusion detection methods for IoT security, anchored in Deep Learning.

We review recent advancements in IDS for IoT, highlighting the underlying deep learning algorithms, associated datasets, types of attacks, and evaluation metrics. Further, we discuss the challenges faced in deploying Deep Learning for IoT security and suggest potential areas for future research. This survey will guide researchers and industry experts in adopting Deep Learning techniques in IoT security and intrusion detection.

Disadvantages

• The complexity of data: Most of the existing machine learning models must be able to accurately interpret large and complex datasets to detect Cyber Attacks.

• Data availability: Most machine learning models require large amounts of data to create accurate predictions. If data is unavailable in sufficient quantities, then model accuracy may suffer.

• Incorrect labeling: The existing machine learning models are only as accurate as the data trained using the input dataset. If the data has been incorrectly labeled, the model cannot make accurate predictions.

4. PROPOSED SYSTEM

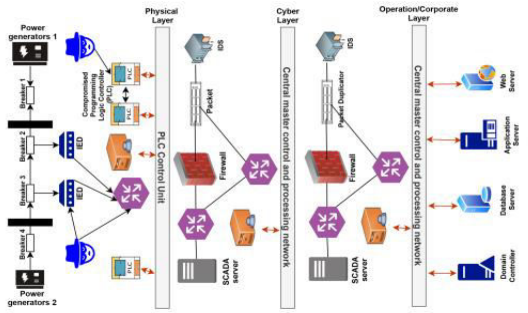
By considering the limitations of previous techniques, we employ network attributes of industrial protocols and propose a pyramidal

recurrent unit (PRUs)- and decision tree (DT)-based ensemble detection mechanism. The proposed mechanism has the potential to detect cyberattacks in any extensive industrial network. The interoperability with other detection engines and expandability for a wider industrial network with multiple areas distinguishes the proposed mechanism from previous studies. The proposed detection method is disseminable across many IIoT domains. Furthermore, our model is straightforward to implement and deploy and can improve efficiency and accuracy while overcoming the shortcomings of previous efforts.

Advantages

1) We propose a scalable and efficient DL- and DT-based ensemble cyber-attack detection framework to resolve trustworthiness issues in the SCADA-based IIoT networks.
2) We present an efficient probing approach by the SCADAbased network data to solve the protocol mismatch limitations of traditional security solutions for the IIoT platform.
3) A statistical analytic approach for ensuring the trustworthiness and reliability of the proposed model for SCADA based IIoT networks.

5. SYSTEM ARCHITECTURE



6. IMPLEMENTATION

Modules

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Train & Test Datasets, View Trained and Tested Datasets Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of Cyber Attack Type, View Cyber Attack Type Ratio, Download Predicted Data Sets, View Cyber Attack Type Ratio Results, View All Remote Users.

View and Authorize Users

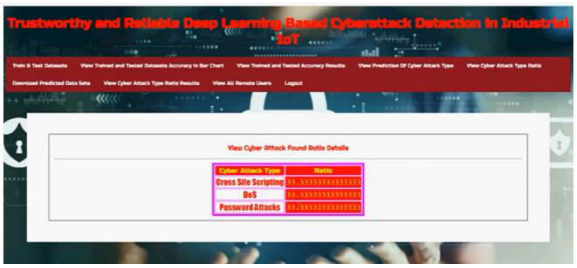
In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user

will do some operations like REGISTER AND LOGIN, PREDICT CYBER ATTACK TYPE, VIEW YOUR PROFILE.

7. RESULTS




Trustworthy and Reliable Deep Learning Based Cyberattack Detection in Industrial IoT


Trustworthy and Reliable Deep Learning Based Cyberattack Detection in Industrial IoT
PREDICT CYBER ATTACK TYPE
VIEW YOUR PROFILE
LOGOUT
YOUR PROFILE DETAILS !!!
USER NAME = Manjunath
EMAIL = tmksmanju199@gmail.com
PASSWORD = Manjunath
MOBILE NO = 9535866270
COUNTRY = India
STATE = karnataka
CITY = Bangalore


Trustworthy and Reliable Deep Learning Based Cyberattack Detection in Industrial IoT


Trustworthy and Reliable Deep Learning Based Cyberattack Detection in Industrial IoT
View Cyber Attack Type Prediction Details !!!


Trustworthy and Reliable Deep Learning Based Cyberattack Detection in Industrial IoT
VIEW ALL REMOTE USERS !!!


Trustworthy and Reliable Deep Learning Based Cyberattack Detection in Industrial IoT
View Cyber Attack Found Ratio Details
Cyber Attack Type
DoS
Password Attacks


Register


Trustworthy and Reliable Deep Learning Based Cyberattack Detection in Industrial IoT


Trustworthy and Reliable Deep Learning Based Cyberattack Detection in Industrial IoT
VIEW ALL REMOTE USERS !!!


Trustworthy and Reliable Deep Learning Based Cyberattack Detection in Industrial IoT

8. CONCLUSION AND FUTURE ENHANCEMENT

The credibility of SCADA-based IIOT networks is enhanced by their capacity to fend against cyberattacks. When it came to safeguarding IIOT networks, the current security techniques and machine learning algorithms were unreliable and ineffective. In this paper, we suggested a method for detecting cyberattacks in a SCADA-based IIOT network by utilising improved deep and ensemble learning. Because the PRU and DT were combined to create an ensemble detection model, the suggested method is accurate and dependable. A significant improvement in classification accuracy was achieved when the suggested approach was tested on 15 datasets produced by a SCADA-based network. The results of our approach demonstrated a solid balance between classification accuracy, dependability, trustworthiness, and model complexity, leading to enhanced performance when compared to state-of-the-art methodologies.

In the future, we will use more potent deep learning models to precisely identify cyberattacks, significantly enhancing trustworthiness. Furthermore, we will attempt to develop and evaluate its effectiveness in practical situations. Additionally, when the features are insufficient, we will work on choosing the best features.

REFERENCES

[1] Y. Luo, Y. Duan, W. Li, P. Pace, and G. Fortino, "A novel mobile and hierarchical data transmission architecture for smart factories," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3534–3546, Aug. 2018.

[2] C. Gavriluta, C. Boudinet, F. Kupzog, A. Gomez-Exposito, and R. Caire, "Cyber-physical framework for emulating distributed control systems in smart grids," *Int. J. Elect. Power Energy Syst.*, vol. 114, 2020, Art. no. 105375.

[3] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101–115, 2019.

[4] T. Wang, G. Zhang, M. Z. A. Bhuiyan, A. Liu, W. Jia, and M. Xie, "A novel trust mechanism based on fog computing in sensor–cloud system," *Future Gener. Comput. Syst.*, vol. 109, pp. 573–582, 2020.

[5] K. Guo et al., "MDMaaS: Medical-assisted diagnosis model as a service with artificial intelligence and trust," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2102–2114, Mar. 2020.

[6] M. Al-Hawawreh and E. Sitnikova, "Developing a security testbed for industrial Internet of Things," *IEEE Internet of Things J.*, vol. 8, no. 7, pp. 5558–5573, Apr. 2021.

[7] M. A. Shahriar et al., "Modelling attacks in blockchain systems using petri nets," in *Proc. IEEE 19th Int. Conf. Trust Secur. Privacy Comput. Commun.*, 2020, pp. 1069–1078.

[8] M. Abdel-Basset, V. Chang, H. Hawash, R. K. Chakrabortty, and M. Ryan, "Deep-IFS: Intrusion detection approach for IIoT traffic in fog environment," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7704–7715,

Nov. 2021.
[9] S. Huda, J. Abawajy, B. Al-Rubaie, L. Pan, and M. M. Hassan, "Automatic extraction and integration of behavioural indicators of malware for protection of cyber–physical networks," *Future Gener. Comput. Syst.*, vol. 101, pp. 1247–1258, 2019.
[10] Information Technology-Security Techniques-Information Security Risk Management, ISO/IEC 27005:2018, 2018.
[11] X. Yan, Y. Xu, X. Xing, B. Cui, Z. Guo, and T. Guo, "Trustworthy network anomaly detection based on an adaptive learning rate and momentum in IIoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6182–6192,
Sep. 2020.
[12] D. Wu, Z. Jiang, X. Xie, X. Wei, W. Yu, and R. Li, "LSTM learning with Bayesian and Gaussian processing for anomaly detection in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5244–5253, Aug. 2020.
[13] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf.*, 2015, pp. 1–6.
[14] M. M. Hassan, A. Gumaei, S. Huda, and A. Almogren, "Increasing the trustworthiness in the industrial IoT networks through a reliable cyberattack detection model," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6154–6162, Sep. 2020.
[15] A. N. Jahromi et al., "An improved two-hidden-layer extreme learning machine for malware hunting," *Comput. Secur.*, vol. 89, 2020, Art. no. 101655.