Trustworthy and Reliable Deep-Learning-Based Cyberattack Detection in Industrial IoT

ABSTRACT

A fundamental expectation of the stakeholders from the Industrial Internet of Things (IIoT) is its trustworthiness and sustainability to avoid the loss of human lives in performing a critical task. A trustworthy IIoT-enabled network encompasses fundamental security characteristics, such as trust, privacy, security, reliability, resilience, and safety. The traditional security mechanisms and procedures are insufficient to protect these networks owing to protocol differences, limited update options, and older adaptations of the security mechanisms. As a result, these networks require novel approaches to increase trust level and enhance security and privacy mechanisms. Therefore, in this article, we propose a novel approach to improve the trustworthiness of IIoT-enabled networks. We propose an accurate and reliable supervisory control and data acquisition (SCADA) network-based cyberattack detection in these networks. The proposed scheme combines the deep learning- based pyramidal recurrent units (PRU) and decision tree (DT) with SCADA-based IIoT networks. We also use an ensemble-learning method to detect cyberattacks in SCADA-based IIoT networks. The nonlinear learning ability of PRU and the ensemble DT address the sensitivity of irrelevant features, allowing high detection rates. The proposed scheme is evaluated on 15 datasets generated from

SCADA-based networks. The experimental results show that the proposed scheme outperforms traditional methods and machine learning-based detection approaches. The proposed scheme improves the security and associated measure of trustworthiness in IIoT-enabled networks.

**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.

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.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**SOFTWARE REQUIREMENTS:**

* **Operating system :** Windows 7 Ultimate.
* **Coding Language :** Python.
* **Front-End :** Python.
* **Back-End :** Django-ORM
* **Designing :** Html, css, javascript.
* **Data Base :** MySQL (WAMP Server).