**INTRODUCTION**

**T**HE 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.