IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 6, Issue 6, March 2026

Impact Factor: 8.2

Augmenting Reliability and Trustworthiness in Deep Learning-Driven Security Systems for Industrial IoT

Mrs. Suji Aparna, G. Shiva Sai, A. Srinitha, Ch. Supradhika

Assistant Professor, Dept. of CSE

UG Students, Dept. of CSE

CMR Technical Campus, Hyderabad, Telangana, India

Abstract: *One of the primary requirements of the stakeholders in the Industrial Internet of Things (IIoT) is its trustworthiness and sustainability to prevent the loss of human life in the execution of a critical task. A trustworthy IIoT-enabled network includes basic security attributes, including trust, privacy, security, reliability, resilience, and safety. The conventional security systems and processes are inadequate to safeguard these networks due to differences in protocols, lack of update facilities, and outdated versions of the security systems. Consequently, these networks demand new approaches to boost the trustworthiness level and improve the security and privacy processes. Thus, in this paper, we present a new approach to enhance the trustworthiness of IIoT-enabled networks.. The proposed approach integrates the deep learning-based pyramidal recurrent units (PRU) and decision tree (DT) with SCADA-based IIoT networks. We also employ an ensemble-learning approach to detect cyberattacks in SCADA-based IIoT networks. The nonlinear learning property of PRU and the ensemble DT mitigate the issue of irrelevant feature sensitivity, enabling high detection rates. The proposed approach is tested on 15 datasets created from SCADA-based networks.*

Keywords*:* Industrial Internet of Things (IIoT), SCADA Security, Cyberattack Detection, Deep Learning, Pyramidal Recurrent Unit (PRU), Ensemble Learning

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/568

ISSN
2581-9429
IJARSCT