International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp1026-1031 Vol. 21, Issue 2, 2025

DEEP LEARNING-DRIVEN TRUSTWORTHY CYBERSECURITY FOR INDUSTRIAL IOT NETWORKS

[1]*Mandla Kiran Kumar*, *MCA Student, Department of MCA*

[2] *Emmanuel Raju A, M.Tech, Assistant Professor, Department of MCA*

[12]*Dr KV Subba Reddy Institute of Technology, Dupadu, Kurnool*

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 Due to outdated security mechanism modifications, restricted update choices, and protocol variations, the conventional security processes and mechanisms are unable to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 use 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.

I. INTRODUCTION

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 use 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

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp1026-1031 Vol. 21, Issue 2, 2025

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.

II. LITERATURE SURVEY

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

Much more data is sent via workshop networks in a smart industrial setting, which poses significant problems regarding data transfer capacity and energy efficiency. This paper suggests a mobile and hierarchical data transmission architecture to integrate the two main networks—wired/wireless fieldbus networks and wireless sensor networks—that are typically used in the workshop to collect and transmit data separately. It also makes use of the mobile intelligence already present in smart factories, like automatic guided vehicles (AGVs), to implement a novel data and materials delivery scheme that is well suited for contemporary industrial wireless sensor netwo In comparison to the separate networks without any mobile intelligence assistance, simulation testing showed that the suggested method, operating inside the IWSN, greatly improves data delivery efficiency and achieves better energy utilisation by a factor of four.

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

A cyber-physical paradigm for examining distributed control systems functioning inside smart-grid applications is presented in this study. Theoretical features of distributed intelligence in the smart grid are now the main emphasis of the research, but methods for testing and verifying such systems are either nonexistent or have extremely limited applicability. When evaluating these applications, three factors must be considered: (1) the communication system, (2) the distributed compute platform, and (3) the physical system. The communication system is either overlooked or oversimplified, the distributed computing component is ignored, or both are absent in the majority of earlier research. We provide an architecture that is based on a fleet of inexpensive single board computers and a real-time simulator in order to address all of these factors. Additionally, the data flow between multiple controllers is bent to simulate varied quality of service (QoS) situations via the use of network emulation and traffic management.

On a research example where 27 controllers self-coordinate to solve the distributed optimum power flow (OPF) algorithm in a dc network, the adaptability of the suggested framework is shown.

An overview of current developments and difficulties in modelling and controlling cyber-physical systems that are vulnerable to cyberattacks "

Nearly all locations include cyber physical systems (CPS), which are accessible and controllable from a distance. They are more susceptible to cyberattacks because of these characteristics. Attacking these systems might have serious repercussions since they provide essential functions. Regretfully, cyberattacks could be discovered after the harm has been done. As a result, creating a cyber system that is resilient to attacks is difficult. We are reviewing the research on the security features of CPSs in this study. We start by outlining a few of the current techniques for identifying cyberattacks. Second, we concentrate on three primary cyberattacks: replay, deception, and denial of service (DoS) assaults. We have reviewed various current models of these assaults, methods for filtering CPS that are vulnerable to

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp1026-1031 Vol. 21, Issue 2, 2025

them, and methods for controlling CPS that are vulnerable to them in our discussion.

III. SYSTEM ANALYSIS AND DESIGN

EXISTING SYSTEM

With its network of linked smart gadgets, the Internet of Things (IoT) has completely changed contemporary technology. These developments provide previously unheard-of possibilities, but they also present difficult security issues. An important issue for intrusion detection systems (IDS) is cybersecurity. Effectively identifying and stopping cyberattacks on Internet of Things devices has been shown to be possible using deep learning. Conventional IDS solutions have difficulties in the setting of the Internet of Things, despite the fact that IDS is essential for protecting sensitive data by detecting and stopping suspicious activity. This study explores the state-of-the-art, Deep Learning-based intrusion detection techniques for IoT security.

We examine the latest developments in IDS for IoT, emphasising the assessment criteria, related datasets, attack kinds, and underlying deep learning algorithms. We also go over the difficulties in using Deep Learning for IoT security and provide some directions for further study. This study will help academics and industry professionals use Deep Learning methods for intrusion detection and IoT security.

Disadvantages

• Data complexity: To identify cyberattacks, the majority of machine learning models now in use need to be able to correctly analyse large and intricate datasets.

• Data availability: In order to provide precise predictions, the majority of machine learning models need a lot of data. The accuracy of the model may degrade if data is not accessible in large enough amounts.

• Inaccurate labelling: The accuracy of the machine learning models that are now in use depends on how well the input dataset was used for training. Inaccurate labelling of the data prevents the model from producing reliable predictions.

PROPOSED SYSTEM

Taking into account the shortcomings of earlier methods, we use network characteristics of industrial protocols and provide an ensemble detection mechanism based on decision trees (DT) and pyramidal recurrent units (PRUs). Cyberattacks in any large industrial network might be detected using the suggested method. The suggested technique differs from earlier research in that it may be expanded to a larger industrial network with numerous locations and is compatible with other detection engines. The suggested detection technique may be used in a variety of IIoT fields. Additionally, our methodology may increase accuracy and efficiency while overcoming the drawbacks of earlier attempts and is simple to install and apply.

Advantages

1) To address trustworthiness concerns in SCADA-based IIoT networks, we provide an effective and scalable ensemble cyber-attack detection system based on DL and DT.

2) To address the protocol mismatch constraints of conventional security solutions for the IIoT platform, we provide an effective probing technique using SCADA-based network data.

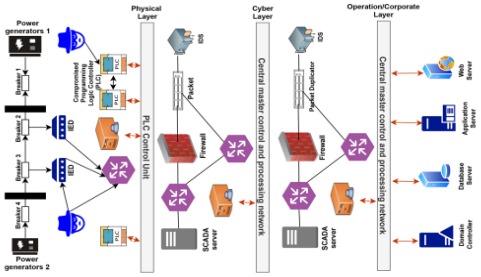
3) A statistical analytical method to guarantee the validity and dependability of the suggested model for IIoT networks based on SCADA.

SYSTEM ARCHITECTURE

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp1026-1031 Vol. 21, Issue 2, 2025



IV. IMPLEMENTATION

Modules

Service Provider

The Service Provider must use a working user name and password to log in to this module. He may do many tasks after successfully logging in, including Train & Test Data Sets, See the Accuracy of Trained and Tested Datasets in a Bar Chart View Accuracy Results for Trained and Tested Datasets, Download Predicted Data Sets, View Cyber Attack Prediction Status Ratio, and View Cyber Attack Prediction Status See the results of the Cyber Attack Prediction Status Ratio. See Every Remote User.

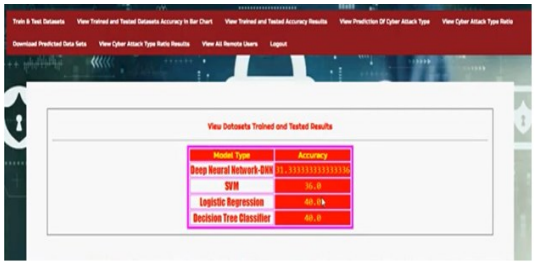
View and Authorize Users

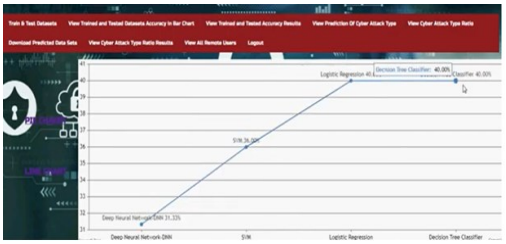
The administrator may see a list of all registered users in this module. Here, the administrator may see the user's information, like name, email, and address, and they can also grant the user permissions.

Remote User

A total of n users are present in this module. Before beginning any actions, the user needs register. Following registration, the user's information will be entered into the database. Following a successful registration, he must use his password and authorised user name to log in. Following a successful login, the user may do tasks including registering and logging in, predicting the status of cyberattacks, and seeing their profile.

V. SCREEN SHOTS

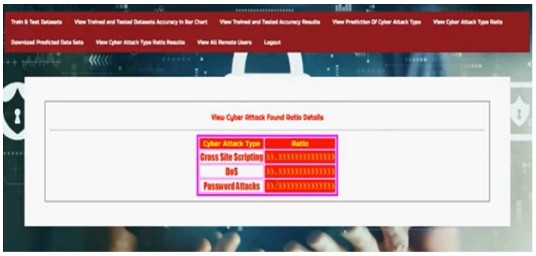




International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp1026-1031 Vol. 21, Issue 2, 2025



VI. CONCLUSION

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 using 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.*

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp1026-1031 Vol. 21, Issue 2, 2025

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.

[16] S. T. U. Shah, J. Li, Z. Guo, G. Li, and Q. Zhou, "DDFL: A deep dual function learning-based model for recommender systems," in *Proc. Int. Conf. Database Syst. Adv. Appl.*, 2020, pp. 590–606.

[17] R. C. B. Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyberattack discrimination," in *Proc. 7th Int. Symp. Resilient Control Syst.*, 2014, pp. 1–8.

[18] A. Derhab et al., "Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security," *Sensors*, vol. 19, no. 14, 2019, Art. no. 3119.

[19] S. Mehta, R. Koncel-Kedziorski, M. Rastegari, and H. Hajishirzi, "Pyramidal recurrent unit for language modeling," in *Proc. Conf. Empirical Methods Natural Lang. Process.*, 2018, pp. 4620–4630.

[20] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," 2014, *arXiv:1412.6980*.

[21] P. Refaeilzadeh, L. Tang, and H. Liu, "Cross-validation," *Encyclopedia Database Syst.*, vol. 5, pp. 532–538, 2009.

[22] G.W. Zeoli and T. S. Fong, "Performance of a two-sample Mann-Whitney nonparametric detector in a radar application," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-7, no. 5, pp. 951–959, Sep. 1971.