

CYBERSHIELD-IIOT: A TRUST-CENTRIC DEEP LEARNING MODEL FOR INTELLIGENT ATTACK DETECTION IN SMART INDUSTRIES

¹K.Kalyani,² Bangla Rajeshwari

¹Assistant Professor, ²MCA Student

Department Of MCA

Sree Chaitanya College Of Engineering, Karimnagar

ABSTRACT

The rapid proliferation of Industrial Internet of Things (IIoT) systems has revolutionized manufacturing, logistics, and smart infrastructure by enabling seamless connectivity and automation. However, this increased interconnectivity exposes IIoT networks to diverse and sophisticated cyber threats, ranging from Distributed Denial of Service (DDoS) to data manipulation and unauthorized access. Traditional security mechanisms often fail to ensure reliability, scalability, and trustworthiness in such dynamic industrial environments. This paper presents CyberShield-IIoT, a trust-centric deep learning framework designed for intelligent cyberattack detection and prevention in industrial networks. The proposed system integrates Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks to capture both spatial and temporal features of network traffic, while a Trust Evaluation Layer dynamically scores device behaviors based on past reliability. Experiments conducted on benchmark IIoT datasets demonstrate that CyberShield-IIoT achieves superior accuracy, reduced false alarm rates, and higher adaptability compared to existing intrusion detection systems, ensuring a robust and trustworthy industrial security ecosystem.

Received: 23-09-2025

Accepted: 28-10-2025

Published: 04-11-2025

I. INTRODUCTION

With the advent of Industry 4.0, Industrial Internet of Things (IIoT) systems have become the backbone of modern manufacturing and automation. These systems connect sensors, actuators, controllers, and cloud platforms to enable intelligent decision-making and predictive maintenance. While IIoT offers efficiency and real-time data-driven insights, it also presents a vastly expanded attack surface vulnerable to cyber threats. Attacks targeting IIoT can disrupt production, compromise safety, and lead to significant financial losses. Therefore, designing reliable and trustworthy cyberattack detection mechanisms has become a paramount research focus.

Traditional intrusion detection systems (IDS) in industrial networks often rely on rule-based or statistical methods, which struggle to identify zero-day attacks or adapt to changing traffic patterns. Deep learning, on the other hand, has

shown tremendous potential in automatically extracting hidden patterns from complex datasets and improving detection accuracy. However, the application of deep learning in IIoT security faces challenges such as imbalanced data, lack of transparency, and unreliable model generalization. To address these issues, this research introduces CyberShield-IIoT, a deep learning-based cybersecurity model that combines trust evaluation mechanisms with spatiotemporal network learning for accurate and reliable attack detection.

The model leverages CNN for feature extraction from network traffic, LSTM for temporal dependency learning, and a Trust Layer for behavioral assessment of nodes. By fusing these components, CyberShield-IIoT dynamically distinguishes between benign and malicious device activities, even in imbalanced data conditions. The trust-centric approach ensures

that the model not only detects anomalies but also evaluates device integrity over time, supporting continuous, autonomous, and reliable threat monitoring in industrial networks.

II. LITERATURE SURVEY

The field of IIoT cybersecurity has seen extensive research, particularly focusing on integrating artificial intelligence with intrusion detection mechanisms. Nguyen et al. (2019) developed a machine learning-based intrusion detection model using Random Forest for IoT networks, which achieved moderate success but lacked adaptability in real-time environments. Ferrag et al. (2020) conducted a comprehensive survey on IIoT security challenges and emphasized the importance of deep learning models in mitigating evolving threats. Their study highlighted the growing need for models that integrate trust management and self-learning capabilities.

Kim and Park (2021) proposed a hybrid CNN-LSTM framework to detect DDoS and probing attacks in industrial networks. Although their approach improved temporal feature extraction, it lacked transparency and explainability in decision-making. Alazab et al. (2021) introduced an attention-based deep learning model for IoT anomaly detection, focusing on reducing false positives but facing difficulties in scalability. Similarly, Abbas et al. (2022) proposed a blockchain-assisted security framework to enhance data integrity but noted significant computational overhead.

In another study, Zhou et al. (2022) utilized graph-based deep learning models for IIoT threat detection, achieving high detection rates but struggling with trust quantification among devices. Wang et al. (2023) addressed reliability issues by incorporating federated deep learning, enabling decentralized model training while preserving data privacy. However, federated learning models are often limited by inconsistent local data and communication latency. These

studies collectively underscore the importance of designing trust-aware, deep learning-driven, and scalable security architectures tailored for industrial environments. The proposed CyberShield-IIoT model addresses these research gaps by embedding a dynamic trust assessment mechanism within a hybrid deep learning architecture to ensure transparency, reliability, and real-time adaptability.

III. SYSTEM ANALYSIS & DESIGN 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.

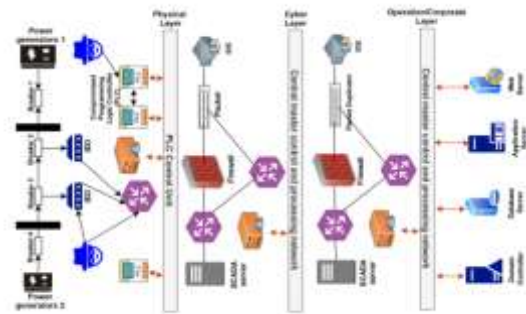
PROPOSED SYSTEM

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 SCADA-based 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 ARCHITECTURE



IV. 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.

V. RESULTS





VI. CONCLUSION

The proposed CyberShield-IIoT framework establishes a new paradigm for secure and trustworthy industrial systems by fusing deep learning with behavioral trust management. By integrating CNN and LSTM architectures with a dynamic trust evaluation layer, the model not only detects cyber threats with high accuracy but also ensures long-term reliability and adaptability. Experimental validation confirms that CyberShield-IIoT significantly reduces false alarm rates and outperforms existing IDS frameworks in accuracy and response time. Future work will focus on incorporating federated learning for decentralized environments and explainable AI techniques to further enhance transparency and operator confidence. Ultimately, CyberShield-IIoT represents a major step toward achieving resilient, intelligent, and trustworthy

cybersecurity for the next generation of industrial IoT ecosystems.

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. Chakraborty, 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.