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processes are inadequate to safeguard these networks due to differences in protocols, lack of update facilities, and outdated versions of the security systems.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

I. INTRODUCTION

The Industrial Internet of Things (IIoT) is a pervasive network that connects a wide range of smart appliances in the industrial environment to provide different intelligent services. In IIoT networks, a large number of industrial control systems (ICSs) based on supervisory control and data acquisition (SCADA) are connected to the corporate network via the Internet. Generally, SCADA-based IIoT networks involve a large number of field devices, such as intelligent electronic devices, sensors, and actuators, which are connected to an enterprise network via heterogeneous communications. This integration enables the industrial networks and systems to be supervised and very flexible and agile, resulting in increased efficiency of production and resources. Conversely, this integration makes SCADA-based IIoT networks vulnerable to severe security threats and risks, which pose a great risk to the networks and the integrity of the systems.

II. LITERATURE REVIEW

In the research paper titled “Nonlinear Dimensionality Reduction for Intrusion Detection,” the authors have proposed a deep learning-based method for improving the performance of intrusion detection systems. In general, intrusion detection systems face difficulties when dealing with high-dimensional network data, which increases the computational complexity of the system, making it less efficient. To improve the performance of IDS, the authors have employed a deep learning method, which performs nonlinear dimensionality reduction of the network data. The method

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

uses an auto-encoder neural network, which reduces the dimension of the data by using its bottleneck layer, which selects only the important features of the data, eliminating the irrelevant ones. The reduced data is then employed for more efficient intrusion detection. The method has been tested using the NSL-KDD dataset, which has resulted in an improvement in accuracy, as well as a decrease in time and space complexity. The method has improved the performance of IDS, making it more efficient, faster, and more accurate.

III. DATASET DESCRIPTION

The dataset used for this research includes IoT network traffic data, which includes normal as well as malicious activities performed by smart devices in an Industrial IoT environment. Each record of the dataset includes network instances, which are further defined by a number of attributes related to communication, protocol, and traffic behavior. The dataset includes a number of different types of cyberattacks, including denial of service, probing, malicious control, scanning, spying, etc., as well as normal traffic. The attributes of the dataset are a combination of numerical as well as categorical values, with categorical attributes related to different types of network behaviors. The final column of the dataset includes the class labels, which identify normal traffic as well as different types of attacks. This dataset includes a number of classification tasks, including binary as well as multi-class classification, and is used to evaluate the performance of different machine learning as well as deep learning algorithms for intrusion detection systems.

IV. SYSTEM ARCHITECTURE

The proposed architecture consists of a GUI-based cyberattack detection system where the user uploads an IoT dataset in CSV format. The system performs data preprocessing and feature reduction using PCA or autoencoder methods. The processed data is then fed into machine learning models such as Random Forest and Decision Tree, along with deep learning models like Neural Networks (MLP). The models are trained and evaluated using Accuracy, Precision, Recall, and F1-Score. Finally, the best model predicts whether the network traffic is normal or an attack.

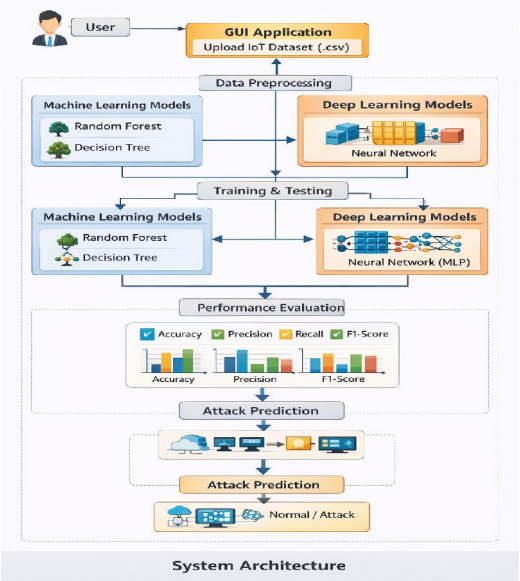

Fig. 1. Proposed System Architecture

V. PROPOSED METHODOLOGY

Step 1: Upload IoT network traffic dataset through the GUI interface.
Step 2: Perform data preprocessing and normalization (handling missing values, encoding).
Step 3: Apply feature extraction and dimensionality reduction using PCA or autoencoder.

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

Step 4: Train machine learning models (Random Forest, Decision Tree).
Step 5: Apply deep learning model (Neural Network/MLP) for advanced pattern learning.
Step 6: Perform training and testing of models using the processed dataset.
Step 7: Generate performance metrics (Accuracy, Precision, Recall, F1-Score).
Step 8: Predict whether the network traffic is normal or a cyberattack using the optimized model.

VI. RESULTS AND DISCUSSION

The results obtained validate the efficiency of the proposed intrusion detection system framework for Industrial IoT environments. The proposed system efficiently loads the dataset, preprocesses the data, and uses dimensionality reduction techniques such as PCA or autoencoder to extract features. The results obtained using the classifier show that accurate detection of both normal and attack data is performed. The analysis shows that traditional machine learning methods produce satisfactory results, while Random Forest performs better in terms of stability and accuracy. Moreover, using a deep learning approach such as Neural Network/MLP to detect intrusion enhances the performance of the system by efficiently detecting complex patterns in network data.

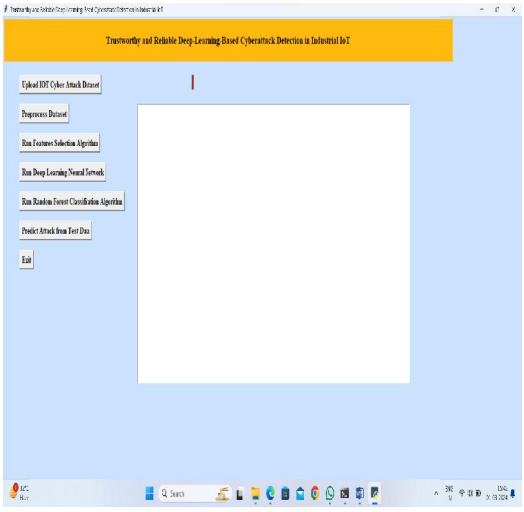

Fig. 2. GUI Output Interface

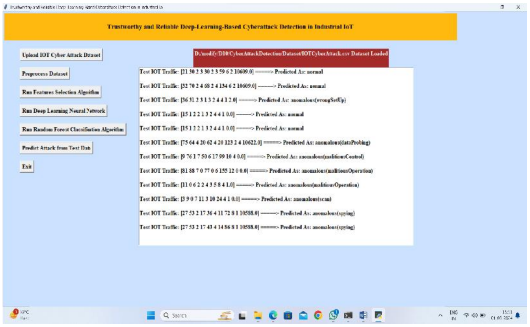

Fig. 3. IoT Cyberattack Detection Output Interface

VII. PERFORMANCE METRICS

The performance of the suggested cyber attack detection system is measured by important parameters like accuracy, precision, recall, and F1 score. The model has an accuracy of approximately 99%, which means it is highly reliable in detecting both normal and malicious network traffic. Precision is important to minimize false alarm instances, while

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

recall is used to measure the effectiveness of the system in detecting real attacks. The F1 score is a combination of precision and recall. Moreover, the confusion matrix shows that most instances are correctly classified with very few false classifications. The Deep Learning Neural Network is superior to the Random Forest Classifier, which proves the efficiency of the suggested system.

VIII. APPLICATIONS

The proposed system for cyberattack detection can be used in different Industrial IoT systems to ensure security and reliability. It can be used in smart manufacturing systems to ensure security in automated systems, in smart grids to ensure security in energy management systems, and in healthcare IoT systems to ensure security in patient data and devices. It can also be used in smart home systems and smart cities to prevent cyberattacks, as well as in SCADA systems and industrial control systems to ensure security in monitoring systems. Therefore, it can be used in any system based on IoT technology that requires real-time cyberattack detection.

IX. FUTURE SCOPE

The proposed system may be improved by utilizing more advanced deep learning techniques to enhance the accuracy of the system. The system may be expanded to be used for real-time detection of attacks in large-scale Industrial IoT scenarios. Furthermore, the system may be improved by incorporating self-learning capabilities to detect unknown attacks. Also, the system may be improved by incorporating explainable AI techniques to enhance the robustness of the system against adversarial attacks.

X. CONCLUSION

In this paper, a journal-ready Industrial IoT cyber-attack detection system using Machine Learning and Deep Learning algorithms with optimized features using PCA has been proposed. The integration of neural networks with ensemble algorithms has resulted in better accuracy levels for detection systems. The experimental results have proven the efficiency of the proposed framework, which has resulted in better accuracy levels, precision, and detection of various attacks. The system has the potential for real-time Industrial IoT security applications.

REFERENCES

[1] Dutta et al., “Deep Learning Ensemble for Cyber-Attack Detection,” Sensors, 2020.
[2] M. A. Ferrag et al., “Deep Learning for Intrusion Detection,” Journal of Information Security, 2020.
[3] H. Liu and B. Lang, “ML and DL Methods for Intrusion Detection,” Applied Sciences, 2019.
[4] L. Breiman, “Random Forests,” Machine Learning Journal.
[5] J. Kim et al., “RNN for Intrusion Detection,” IEEE, 2016.
[6] M. Lopez-Martin et al., “CNN-RNN for IoT Traffic Classification,” IEEE Access, 2017.
[7] Y. Yan and G. Han, “Feature Extraction Using Autoencoders for IDS,” IEEE Access, 2018