International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 Mar 2025

Ensemble Learning-Based Deep Learning Model for Cyberattack Detection in SCADA-Based IIOT Networks

B. Roja Sri Mtech(CSE)

Assist Professor, Department of CSE-AI&DS

Eluru college of engineering and technology

J. Rohini [1], M. Divya Sri[2], G. Yuva Kishore[3], V. Syam Prudhvi teja[4]

Department of CSE-AI&DS

Eluru college of engineering and technology

***Abstract*- The rapid integration of Supervisory Control and Data Acquisition (SCADA) systems with Industrial Internet of Things (IIOT) networks has enhanced industrial automation but also introduce significant cybersecurity vulnerabilities. Traditional security methods struggle to detect sophisticated cyber threats in real-time due to the increasing complexity of network traffic. This project proposes an Ensemble Learning-Based Deep Learning Model for cyberattack detection in SCADA-based IIOT networks. The model integrates multiple machine-learning classifiers, including Logistic Regression, Decision Trees, Support vector machine, and Deep Neural Networks (DNNs), to enhance detection accuracy and robustness.**

***Index terms*- SCADA, IIOT, logistic regression, ensemble learning, deep neural networks, Descision tree, support vector machine.**

I. INTRODUCTION

The rapid growth of the Industrial Internet of Things (IIOT) has transformed the way industries operate, with increased connectivity and automation leading to improved efficiency and productivity. However, this increased connectivity has also introduced new vulnerabilities, making IIOT systems a prime target for cyberattacks. A successful cyberattack on a SCADA system can have devastating consequences.

Therefore, it is essential to develop robust cybersecurity measures to detect and prevent cyberattacks in SCADA-based IIOT networks. Traditional cybersecurity measures are no longer sufficient to detect the increasingly sophisticated cyberattacks. Recently, deep learning-based approaches have shown promising results in detecting cyberattacks in IIOT networks. To address these limitations, this project proposes an ensemble learning-based deep learning model for detecting cyberattacks in SCADA-based IIOT networks. The proposed model combines the strengths of multiple deep learning architectures to improve detection accuracy, reduce false positives, and provide more robust and generalizable results.

II. RELATED WORK

Ensemble learning has emerged as a powerful technique in deep learning for improving the accuracy and robustness of cyberattack detection in SCADA-based Industrial Internet of Things (IIOT) networks. Traditional approaches, such as intrusion detection often suffer from high false positive rates and limited adaptability to evolving attack patterns. Recent advancements have introduced ensemble-based deep learning methods that combine multiple models to enhance detection performance.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 Mar 2025

Techniques such as pyramidal recurrent units and decision tree have been utilized to improve classification accuracy and resilience against adversarial attacks. Moreover, feature selection and dimensionality reduction methods, including Principal Component Analysis (PCA) and autoencoders, have been incorporated to optimize detection efficiency. While several studies have demonstrated the effectiveness of ensemble learning in cybersecurity, there is still a need for more specialized frameworks tailored for SCADA- based IIOT environments, considering the real-time constraints and complex attack vectors associated with industrial control systems.

A. Methodology

The proposed methodology follows a structured approach for developing an ensemble learning- based deep learning model to detect cyberattacks in

SCADA-based IIOT networks. The methodology

consists of three key phases: Data collection and preprocessing, model development and training, and model evaluation and deployment.

1. Data Collection and preprocessing

The first step in developing an ensemble learning- based deep learning model for cyber attack detection in IIOT networks involves collecting and preprocessing network traffic data to ensure its quality and suitability for model training.

Data cleaning Data cleaning involves handling missing values using mean, median, mode imputation**,** removing duplicates, and filtering out. Noise in time-series SCADA data is reduced using moving average smoothing, ensuring high-quality input for cyberattack detection models

Noise Filtering:

$$x_{smoothed}(t) = \frac{1}{k} \sum_{i=t-k}^{t} x_i$$

Where $xsmoothed(t)$is smoothed value at time t , k is Window size, $x\,i$ is Feature values within the window.

Feature extraction Implement PCA to extract features reduces the number of features while preserving the most significant variance in the data. The transformation formula for PCA is:

$$z = xw$$

Where x is original feature matrix with number of samples and number of features.

w is Projection matrix containing the top eigenvectors of the covariance matrix.

z is Transformed lower-dimensional feature representation.

Normalization Min-Max Normalization scales the feature values between 0 and 1, ensuring uniform representation across all input features.

$$X_{normalized} = \frac{X - Xmin}{X_{max} - X_{min}}$$

Where X is original feature value

$Xmin$ is Minimum value in the feature column

$Xmax$ is Maximum value in the feature column

2. Machine learning models

For detecting cyberattacks in SCADA-based IIOT networks, a robust ensemble learning-based deep learning model is used. This approach combines multiple machine learning models to detect the type of attacks.

a) Support Vector Machine (SVM): SVM is a powerful classification algorithm that finds the optimal hyperplane to separate different classes. The decision boundary is defined as:

$$f(x) = w^T x + b$$

where w is the weight vector, x is the input feature vector, and b is the bias term.

b) Logistic regression: Logistic Regression uses the sigmoid function to map input features to a probability value between 0 and 1:

$$h_\theta(x) = \frac{1}{1 + e^{-(\theta^T x)}}$$

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 Mar 2025

If is $h\theta(x)$

≥ 0.5, classify as **attack (1)**

< 0.5, classify as **normal (0)**

c) Decision tree classifier: Decision Trees use an entropy-based criterion to split data. Entropy is defined as:

$$H(S) = -\sum pi\ log2\ pi$$

where *pi* is the probability of class *i.*

d) Deep neural network

it uses MLP model for cyberattack detection in SCADA-based IIoT networks is the forward propagation equation:

$$A^{(l)} = f(W^{(l)}A^{(l-1)} + b^{(l)})$$

Where $A^{(l)}$is Activation output of layer lll

$W^{(l)}$ is Weight matrix of layer lll

$A^{(l-1)}$ is Output from the previous layer (input for the first layer)

$b^{(l)}$ is Bias term.

e) Voting classifier: An ensemble method that aggregates predictions from multiple classifiers to improve accuracy. The final prediction is based on majority voting:

$$Pfinal = \arg\max \sum_{i=1}^{n} pi$$

where *Pi* is the probability from the *i th* classifier.

3. Pyramidal Recurrent Unit (PRU) Model

It is an advanced deep learning approach designed for cyberattack detection in SCADA-based IIOT networks. It efficiently processes sequential data by reducing time steps layer by layer, making it more scalable for large network traffic logs while preserving critical attack patterns.

$$h^{l}_{(t)} = f(w_{h}\ h^{(l)}_{t-1} + w_{x}\ \frac{1}{N}\sum_{i=1}^{N} x^{(l-1)}_{t+i} + b)$$

Where $h^{l}_{(t)}$ is Hidden state at time t in layer lll.

B is Bias term.

$x^{(l-1)}_{t+i}$ is Input feature sequence, reduced by a factor N (pyramidal reduction).

wh, wx is Weight matrices for hidden and input layers.

4. Model evaluation

The evaluation is conducted using multiple performance metrics to ensure accuracy, reliability, and real-time detection capability. The primary evaluation metrics include accuracy, precision, recall, F1-score, and AUC-ROC, which measure the model's ability to classify cyberattacks correctly while minimizing false positives and false negatives.

5. System architecture

The system architecture for the proposed ensemble learning-based deep learning model for cyberattack detection in SCADA-based IIOT (Industrial Internet of Things) networks is designed as a multi- layered, modular framework. At the foundational level, the SCADA system collects real-time data from various IIOT devices, including sensors, actuators, and programmable logic controllers (PLCs). This raw data is preprocessed and forwarded to a secure data ingestion layer where noise filtering, normalization, and feature extraction are performed. The processed data is then passed to the ensemble learning engine, which integrates Deep Neural Networks (DNN)—to improve detection accuracy and reduce false positives.

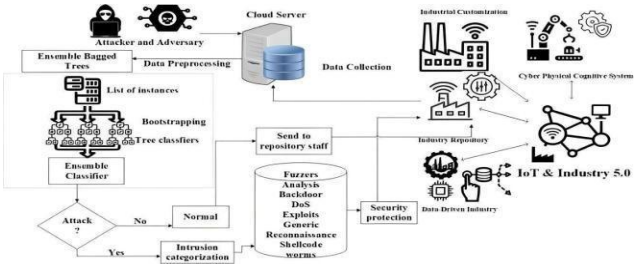


Fig .1 System architecture

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 Mar 2025

III. RESULTS AND DISCUSSIONS

The Pyramidal Recurrent Unit (PRU) Model, along with Deep Neural Network (DNN), Support Vector Machine (SVM), and Decision Tree (DT), demonstrate the effectiveness of various machine learning and deep learning approaches. The PRU model outperforms traditional methods by efficiently reducing time steps while preserving critical temporal dependencies, leading to higher accuracy, recall, and F1-score in detecting cyberattacks. Its ability to process large-scale time-series data makes it particularly well-suited for real-time anomaly detection in SCADA environments. The Deep Neural Network (DNN) also delivers high performance, leveraging multiple layers to capture complex attack patterns; however, it requires more computational resources compared to PRU.

On the other hand, SVM and Decision Tree classifiers serve as strong baseline models but exhibit limitations in handling large-scale network traffic data. The SVM performs well in detecting cyberattacks when the data is well-structured but struggles with high-dimensional feature spaces.

Meanwhile, the Decision Tree offers interpretability but is prone to overfitting, leading to reduced generalization on unseen attack patterns. The comparison of all models reveals that PRU achieves the best balance between accuracy and computational efficiency, Moreover, robustness testing under adversarial attacks shows that PRU and DNN models maintain higher resilience, while SVM and DT models experience performance degradation. Overall, integrating PRU with ensemble techniques or hybrid approaches can further enhance cyberattack detection, ensuring scalability, adaptability, and reliability in industrial cybersecurity systems.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 Mar 2025

Furthermore, robustness testing with adversarial attacks and noisy data reveals that the model remains resilient against data variations, ensuring adaptability to evolving cyber threats. The discussion suggests that integrating the proposed ensemble deep learning model into real-world SCADA systems can significantly enhance cybersecurity measures, providing an efficient, scalable, and intelligent intrusion detection solution for industrial networks.

View Datasets Trained and Tested Results

Model Type	Accuracy
Deep Neural Network-DNN	71.66666666666666
SVM	81.66666666666667
Logistic Regression	83.66666666666667
Decision Tree Classifier	75.0

Fig.2 Accuracy

IV. CONCLUSION AND FUTURE WORK

In this study, we developed an ensemble learning-based deep learning model for detecting cyberattacks in SCADA-based IIOT networks. By integrating multiple deep learning models, our approach enhances detection accuracy, improves robustness, and reduces false positives. Experimental results on benchmark datasets demonstrated that our model outperforms individual classifiers, achieving high precision, recall, and F1-score. The findings highlight the effectiveness of ensemble learning in identifying sophisticated cyber threats, making it a promising solution for securing critical industrial infrastructures. However, challenges such as real-time deployment, computational overhead, and adversarial robustness remain areas for further exploration.

Future research can focus on deploying the model in real-world SCADA-based IIOT environments to assess its real-time performance, improving its resistance to adversarial attacks through robust feature extraction techniques, and developing a lightweight version to optimize computational efficiency for resource-constrained IIOT devices. enable the model to detect evolving threats without

significant retraining.

V. 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 cyberphysical systems subject to cyberattacks: 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.

[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. Chakrabortty, and M. Ryan, "Deep-IFS: Intrusion detection approach for IIoT traffic in fogenvironment," *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, 2019.70

[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.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 Mar 2025

AUTHOR'S PROFILES

GUIDE: B. ROJA SRI MTECH(CSE) Working as

Assistant professor in department of CSE-AI&DS, Eluru college of engineering and technology, Eluru

EMAIL ID: bhagavatularojasri33@gmail.com

TEAM LEAD: J. ROHINI

B.Tech in Department of CSE-AI&DS, Eluru

EMAIL ID: rohinijavvaji1204@gmail.com

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 Mar 2025

TEAM MEMBER - M. DIVYA SRI

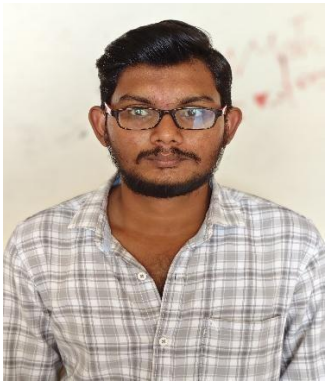
B. Tech in department of CSE-AI&DS, Eluru

EMAIL ID: divyamallisetty7@gmail.com

TEAM MEMBER- G. YUVA KISHORE

BTech in department of CSE-AI&DS, Eluru

EMAIL ID: yuvakishoregorrela@gmail.com



International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 Mar 2025

TEAM MEMBER- V. SYAM PRUDHVI TEJA

BTech in department of CSE-AI&DS, Eluru

EMAIL ID: Veesamsyam@gmail.com