

TRUSTWORTHY AND RELIABLE DEEP-LEARNING-BASED CYBER ATTACK DETECTION

K.Venkatesh¹, A.Madhu Sri², B.Madhulika³

¹Assistant Professor, Department of IOT, Malla Reddy Engineering College For Women (Autonomous Institution), Maisammaguda, Dhulapally, Secunderabad, Telangana-500100

^{2,3}UG Scholar, Department of IOT, Malla Reddy Engineering College for Women, (Autonomous Institution), Maisammaguda, Dhulapally, Secunderabad, Telangana-500100

Email: venkatesh.kummara@gmail.com

ABSTRACT

The IIoT plays an important role in the betterment of industrial automation and operational efficiency, but inherent weaknesses pose significant risks to critical infrastructure systems. Conventional security measures are generally inadequate because of protocol inconsistencies and outdated adaptations, which expose IIoT networks to cyberattacks. This paper introduces a novel approach based on deep learning for the detection of cyberattacks on IIoT-enabled networks, with emphasis on SCADA systems. The proposed method combines PRU with DT and makes use of ensemble learning techniques to enhance the accuracy in the detection process. This will allow PRUs to have nonlinear learning capabilities and robustness in ensemble decision trees. As a result, detection rates are high because it is less affected by the irrelevant features. The method was tested on 15 SCADA datasets and was proven to perform better than traditional detection methods and machine learning-based methods. This approach improves the detection of cyberattacks but strengthens security and reliability in IIoT networks, making critical industrial operations resilient and safe.

Keywords-Industrial Internet of Things (IIoT), Cyberattack Detection, Supervisory Control and Data Acquisition (SCADA), Deep Learning, Pyramidal Recurrent Units (PRU), Decision Trees (DT), Ensemble Learning

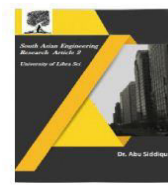
I. INTRODUCTION

The IIoT is changing industrial environments by connecting a wide range of smart devices, which provides significant operational benefits such as flexibility, agility, and improved resource efficiency. At the heart of many IIoT networks are control and data acquisition systems that monitor and control industrial processes. These SCADA-based IIoT networks are connected with enterprise networks through the Internet, thereby creating a huge communication infrastructure. But

connectivity has exposed IIoT systems to multiple cyber threats and vulnerabilities that make the whole system unreliable. The reliability of IIoT systems is of paramount importance in ensuring that they serve their purpose while fulfilling significant demands on safety, privacy, security, reliability, and resilience. SCADA-based IIoT networks are challenging to secure because conventional security protocols, such as Distributed Network Protocol (DNP 3.0), often only address partial security issues, such as



2581-4575



authentication and data integrity, leaving a big gap that potential attackers can exploit. Moreover, even with the comprehensive risk management frameworks like ISO 27005:2018, IIoT systems are still vulnerable due to the dynamic nature of cyber threats. In this regard, this project presents a new approach to detect cyberattacks on SCADA-based IIoT networks using an ensemble detection mechanism that combines deep learning (DL) and decision trees (DT). This model integrates pyramidal repetitive units (PRUs) with DT to exploit their nonlinear learning capabilities and handle the complexity of industrial protocols. The proposed approach is aimed at addressing the shortcomings of traditional security measures for improving detection accuracy, scalability, and efficiency. This sensing framework is scalable, deployable across multiple IIoT domains, and capable of overcoming protocol incompatibilities commonly encountered in industrial networks. Our approach helps improve the security, reliability, and dependability of SCADA-based IIoT systems, thus providing a greater level of protection against cyber threats. The proposed solution is easily integrated into existing systems, providing a convenient and effective way to protect critical industrial infrastructure.

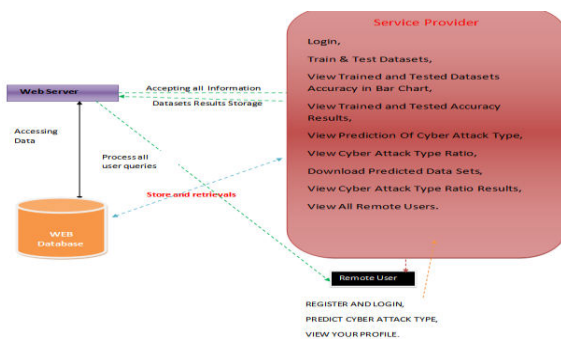


Fig 1: System Architecture

II. RELATED WORK

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

Author:Y. Luo, Y. Duan, W. Li, P. Pace, and G. Fortino, 2018.

This paper introduces a mobile and hierarchical data transmission architecture specifically designed for smart factories. It addresses the challenge of effective data communication across industrial environments where large-scale networks require reliable and low-latency data transmission. The approach focuses on enhancing the flexibility and security of data communication in industrial networks.

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

Author:C. Gavriluta, C. Boudinet, F. Kupzog, A. Gomez-Exposito, and R. Caire, 2020.

The authors present a cyber-physical framework to simulate distributed control systems in smart grids. This will improve the monitoring and control mechanisms of energy distribution systems by combining physical devices with computational models, thus trying to reach the optimal scenario of energy distribution and fault or cyber threat resilience.

"Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges"

Author:M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, 2019.

This survey focuses on the modeling and control of cyber-physical systems in the face of increasing cyber attacks. The authors review



2581-4575



recent developments in CPS security, pointing out methods for detecting and mitigating cyber threats while maintaining system reliability. It also discusses the challenges that industries face in protecting their critical infrastructure from cyber vulnerabilities.

"A novel trust mechanism based on fog computing in sensor–cloud systems"

Author: T. Wang, G. Zhang, M. Z. A. Bhuiyan, A. Liu, W. Jia, and M. Xie, 2020.

The authors propose a trust mechanism by integrating fog computing into sensor-cloud systems for the purpose of improving data processing and security. By utilizing fog computing, the proposed model will reduce latency and increase the reliability of data gathered from the IoT devices. This is particularly relevant in environments where real-time data analysis and decision-making are critical.

"MDMaaS: Medical-assisted diagnosis model as a service with artificial intelligence and trust"

Author: K. Guo et al., 2020.

This paper presents the Medical-assisted Diagnosis Model as a Service, MDMaaS, which combines artificial intelligence with trust mechanisms to support medical diagnoses. The authors stress that the reliability and accuracy of AI models in healthcare must be guaranteed, since trust in diagnostic outcomes is critical for patient safety and decision-making.

"Developing a security testbed for industrial Internet of Things"

Author: M. Al-Hawawreh and E. Sitnikova, 2021.

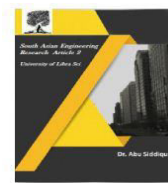
The authors describe the development of a security testbed intended to simulate the Industrial Internet of Things (IIoT) environments. This testbed would be used for the testing and evaluation of several different security measures in protecting the IIoT systems against cyber threats, considering unique challenges in industrial networks of interconnected devices.

III. IMPLEMENTATION

The implementation of the proposed cyber attack detection system involves several steps. First, network traffic data from SCADA-based IIoT networks is collected, pre-processed and cleaned to remove irrelevant information. This data includes network attributes such as packet size, communication frequency, timestamps and error rates, which are essential for training models. Feature extraction techniques are being used to identify more relevant Now the system is built by a mechanism of ensemble detection by integration of pyramid recurrent units PRUs and decision trees DTs. PRUs that involve modeling sequential patterns were put to use to capture time series nature of SCADA network data, such as irregular bursts or unusual command sequences which give a sign of a probable cyber attack. DTs, on the other hand, are used for classification, to classify the normal and malicious activity. These DTs are working in conjunction with PRU to enhance the system's accuracy and also fix non-functional functionality issues. The ensemble approach improves the overall detection rate and also prevents overfitting. After training the



2581-4575



model, it is deployed to monitor SCADA network data in real-time. The system continuously monitors network traffic for anomalies and reports any potential threats. If an attack is detected, the system generates real-time alerts, which are then sent to network administrators for further investigation. Metrics for evaluation of the system performance are precision, accuracy, recall, F1 score, and confusion matrix to estimate its effectiveness in the detection of cyber attacks. The web user interface was designed to access alerts and the system status. For the backend, Django ORM has been used in the building to store network traffic and attack logs in the MySQL database. This system can be seamlessly integrated with other security tools for enhancement of overall industrial cybersecurity. A statistical analysis module is further implemented to monitor the time evolution of the reliability of detection over time, so as the system continues to be effective at times when new attack patterns surface. This process ensures a scalable, efficient, and reliable system for the detection of cyberattacks on SCADA-based IIoT networks.

IV. ALGORITHM

Decision Tree Classifier Algorithm: The Decision Tree classifier algorithm works by recursively splitting the data set into subsets based on the most informative features. It starts by checking if all objects in the data set belong to the same class. If that is true, a leaf node is formed with that class. Otherwise, a test is selected to split the data set based on different outcomes. This test is going to be the root of the tree, and the process is being carried out recursively on each subset. This gives a structure to the tree, wherein each internal node will symbolize a decision made

through a feature, and leaf nodes represent class labels.

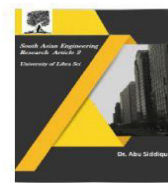
Gradient Boosting Algorithm: Gradient Boosting basically goes by constructing a number of weak models, typically decision trees, in a stage wise fashion. The first step involves training the first tree on the dataset. The model at the end of each stage adjusts itself in order to minimize the residual error of the previous stage, that is, to focus on the misclassified instances. Each model corrects errors made by the previous models, which means improving overall prediction accuracy. This goes on until a predetermined number of models are built or desired accuracy level is reached. The final prediction can be obtained by aggregating the results of all models that typically use a weighted average.

KNN Algorithm: The KNN algorithm classifies the test instance by finding out the K-nearest data points in the training set about the feature space. The distance between the test point and the training points is obtained, often using Euclidean distance. The class that appears most frequently among those neighbors is assigned to the test point after identifying the K nearest neighbors. KNN is a lazy learning algorithm, meaning it does not learn a model during training but instead makes predictions during testing by looking at the nearest neighbors of the test instance.

Logistic Regression Algorithm: Logistic Regression is used for binary or multinomial classification problems. It calculates the probability that an instance belongs to a given class by applying the logistic, also called sigmoid function. In case of two-class classification, it outputs the probability of the instance belonging to the positive class, and



2581-4575



this output is mapped to class 0 or class 1. For multinomial logistic regression, it calculates probabilities for each class, and it assigns to the class which has a higher probability. Maximum likelihood estimation is a technique of estimating the coefficients for a given model. This algorithm maximizes the likelihood of getting the observed data.

Naive Bayes Algorithm: It is based on Bayes' Theorem. Given class label, all the features are assumed to be independent. It calculates the probability of an instance of data belonging to a particular class by multiplying conditional probabilities of each feature given a class. It picks up the class having the maximum posterior probability. Even with the naive assumption of independence, Naive Bayes often works pretty well, especially in the classification tasks of text and is quite famous for its simplicity and efficiency.

Random Forest Algorithm: Random Forest is an ensemble learning method where multiple decision trees are trained on different subsets of the data. Each tree in the forest is trained on a random subset of features and data points, which helps to reduce overfitting. In prediction, each tree makes a classification, and the final result is determined by majority vote or averaging the predictions of all trees in the forest. This method improves accuracy and robustness, especially for complex datasets, and handles both classification and regression tasks well.

Support Vector Machine (SVM) Algorithm: SVM is a supervised machine learning algorithm that finds a hyperplane that best separates data points belonging to different classes in a high-dimensional space. It aims to maximize the margin between the classes,

ensuring the greatest separation. SVM can handle linear and non-linear data by using different kernel functions, such as linear, polynomial, and radial basis function (RBF). It has a very high generalization ability as it minimizes classification error while maximizing the margin. SVM is especially powerful for high-dimensional spaces and clear margin separation between classes.

RESULT



Fig:1: User Login

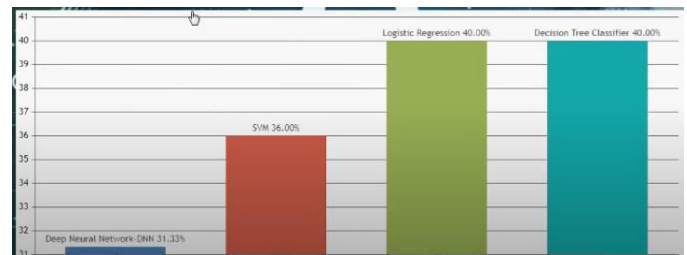


Fig:2: Algorithms Accuracy



Fig:3: Accuracy Results

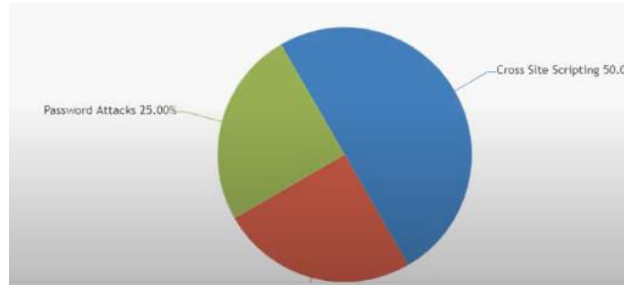


Fig:4:Pie chart Accuracy Results

CONCLUSION

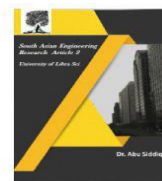
This paper presents an enhanced cyber attack detection mechanism for SCADA-based IIoT networks using deep learning and ensemble learning techniques. The approach combined pyramid recurrent units and decision trees in an ensemble model that improved detection accuracy significantly more than the traditional method. Evaluation of 15 data sets generated by the SCADA network showed a considerable increase in classification accuracy by the proposed model. and a better balance between reliability, trustworthiness and model complexity. The results show that the ensemble model is very effective in detecting cyber attacks and improving the security of IIoT networks. This approach addresses the limitations of existing security methods and presents a promising solution for protecting industrial networks. Future work would optimize the model with more advanced deep learning techniques and test it in real-world scenarios to further improve its applicability and practical effectiveness. Moreover, future work will look into feature selection strategies that would help in data-limited scenarios and ensure that the proposed mechanism continues to be effective

.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



2581-4575



- 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.