Anomaly-based Intrusion Detection System for ICS

Prasanna S S
Dept of Computer Science and Engineering,
Thiagarajar College of Engineering,
Madurai, Tamil Nadu, India
ssprasannamdu@gmail.com

Dr. G. S. R. Emil Selvan
Assistant Professor, Dept of Computer Science and Engineering,
Thiagarajar College of Engineering,
Madurai, Tamil Nadu, India
emil@tce.edu

Dr. M. P. Ramkumar
Assistant Professor, Dept of Computer Science and Engineering,
Thiagarajar College of Engineering,
Madurai, Tamil Nadu, India
ramkumar@tce.edu

2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) | 979-8-3503-3509-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCCNT56998.2023.10307058

Abstract—**Industrial Control Systems (ICS) become a crucial target for hackers as these devices are unsupported in terms of storage, complex computations, and security. On the other hand, providing security for these devices are very difficult. Because small downtime of these devices will lead to financial loss and reputation loss for the industry. Sometimes, even it may lead to a disaster. We should also ensure that there are no heavy workloads present in this Operational Technology (OT) network. Hence, the intrusion detection systems for ICS should operate with high levels of accuracy utilizing resources as low as possible. In this paper, an anomaly-based ICS intrusion detection system is proposed. The proposed model uses Pearson Correlation for feature selection and Deep Neural Network for detection. The suggested solution is put to the test using an HIL-based Augmented ICS security dataset. The results show that the proposed model has a good fit and achieves a higher accuracy rate.**

Keywords— ICS, IDS, Anomaly Detection, Anomaly-based IDS.

I. Introduction

Industry operations like production, distribution, handling, and manufacturing are managed by industrial control systems (ICS). ICS also comprises Supervisory Control And Data Acquisition systems (SCADA) used to monitor geographically dispersed assets, in addition to distributed control systems and smaller control systems using programmable logic controllers to control localized activities. Operational Technology (OT), Industrial Internet of Things (IIoT) and ICS are closely related different terms. Controlling industrial equipment through hardware and software is termed OT. ICS is a subset or an example of the OT network. IIoT is the one that brings industrial machines, cloud computing, and analytics together to enhance industrial process productivity and performance. Although the attack surface of OT networks is too small when compared to IT networks, they are more challenging from the view of security operations. Because there were no specific or authorized teams or organizations for providing security updates. Even if the patch is available, frequent downtime of OT devices is not an option.

Implementation of an Intrusion Detection System (IDS) has two approaches. One is signature-based detection. It compares each traffic packet with the local database of existing attack patterns. This approach needs a huge storage capacity to store the attack patterns. Since the OT network lacks the support of huge storage, we move to the next approach of IDS implementation. Another approach is anomaly-based detection. This method of detection doesn't require any huge storage disks. It works on a principle – "Each protocol has a unique behavioral structure. Every attack traffic will have a deviated or malicious behavior. Hence, it is enough to identify the packets with the above-said behavior.".

II. Related Works

The works listed in the reference section use various kinds of datasets. A good dataset requires 3 conditions to be satisfied [4]. The fundamental requirement is the ratio of attack to normal traffic should lie between 1% and 25% and each transaction should have a timestamp. A special requirement is that the dataset should cover diverse attack possibilities and all the traffic entries should be labeled. The third condition is the real-time nature of the dataset. A machine learning and a deep learning approach have been proposed in [6] where Adaboost performs well in machine learning algorithms and Convolutional Neural Network (CNN) performs better than other deep learning algorithms. The author of [10] proposed an anomaly detection technique using Light Gradient Boosting Machine (LGBM), one-class Support Vector Machine (SVM), and Isolation Forest algorithms. The work in [12] uses BiGAN (GAN with encoder). Even though BiGAN is inferior to existing methods, it doesn't require examples for anomaly detection which makes it efficient in real-time detection. Another anomaly detection system is developed using LSTM in [13] and it outperforms other traditional models in detecting anomalies in public datasets.

The work in [5] proposed five Deep Neural Network (DNN) models - InterFusion, RANSynCoder, GDN, LSTM-ED, and USAD. These 5 models are developed using Autoencoder (AE), Hierarchical Variational Autoencoder (Hierarchical AVE), Graph Attention Network (GAN), and Long Short-Term Memory-based Encoder-Decoder (LSTM-ED). This work uses 2 datasets – SWaT and HAI v2.0. The interfusion model works well with the SWaT dataset and the RANSynCoder model works better for HAI v2.0 dataset. The work detailed in [7] is a 3-step process. First, they normalized the dataset using SMOTE method and used Pearson Correlation for feature selection, and used Decision Tree (DT), K-Nearest Neighbors (KNN), and Random Forest (RF) for classification. RF outperforms the other two algorithms. The work in [28] analyses the performance of various algorithms with the Gas pipeline dataset. Lasso and Logistic Regression algorithms are poorly suited. Support Vector Machine (SVM) doesn't attain acceptable accuracy. DT performance becomes overfitting. Hence, they implemented advanced algorithms such as RF, Adaptive Boosting, Gradient Boosting, Recurrent Neural Network (RNN) based on LSTM, Fully Connected Neural Network (FCNN), and Gated Recurrent Unit (GRU). RF produced better results. And there we not much difference in the performances of LSTM-based RNN and GRU. FCNN outperformed other algorithms. The work in [34] uses SWaT, GP, IUNO, BATADAL, WST, POWER, WADI, FESTO, HAIv1.0, TEP, and TLIGHT datasets. And done a detailed comparative analysis of IDS algorithms on these datasets. All these datasets are concentrated on Fault Data Injection attack only.

TABLE I. EXISTING WORKS

S No	Ref	Feature Selection	Classification	Dataset used
1	[7]	Pearson Correlation	KNN, RF, DT	HAI v1.0
2	[9]	PCA	RF, GBM, ANN, LSTM, LSTM-AE	HAI v1.0
3	[15]	AE	DCNN	KDDCUP99
4	[18]	PCA, ICA, CCA	Bloom Filter, KNN	Gas Pipeline
5	[25]	PCA	SVM, RF, Naïve Bayes	normal SCADA network traffic, BATADAL, ICS cyber-attack dataset, power systems dataset

Among several algorithms, only RF, DT, and DNN achieve over 99% accuracy. ICS systems have implemented Ethernet-based interconnections that combines OT network with IT network to reduce cost and maintainance complexity. But this integration becomes a vulnerable point to attack OT systems. The work in [16] states that anomaly-based IDS are well-suited for OT environments and introduces a threat-based assessment method to evaluate the anomaly-based network IDS configurations. As a continuation, they applied the proposed methodology on a full-scale ICS testbed by simulating actual attacks [20]. Another anomaly-based IDS approach is introudced [21] which uses RF for training and detection. Comparision between traditional and modern IDS systems is done in [30]. Also, several IDS are compared and the numerical results are dicussed in detail. The work in [32] presented a detailed analysis of several IDS (both signature-based and anomaly-based) and commonly used datasets. They also stated that an effective IDS should accurately detect all kinds of intrusions including those with evading techniques. Some of the works are summarized in Table I.

III. PEARSON CORRELATION

Pearson Correlation is a bivariate analysis that evaluates the degree of association and the direction of the link between two variables. The correlation coefficient, which represents the strength of the association, ranges from -1 to +1. If the value tends toward zero, the relationship is weak and if the value tends towards either end, i.e., -1 or +1, then the relationship is strong, otherwise known as a high correlation. When two or more independent features are highly correlated, then they can be removed as they are considered duplicate features. The result of the correlation is viewed through a heatmap.

IV. DEEP NEURAL NETWORKS

Artificial intelligence has a subfield called "Deep Learning" that focuses on developing algorithms to give computers intelligence by drawing inspiration from the biological structure and operation of the brain. A hierarchical (layered) layout of neurons with connections to other neurons is how a Deep Neural Network (DNN) is conceptualized in its most basic form. Fig 1 depicts the DNN architecture. Each layer computes a value known as Activation Function, which is responsible for deciding whether a node should be activated or not. This value decides whether the input value from the node is needed or not in the process of detection using some simple mathematical computations. Generally, the most commonly used activation function in neural networks is Rectified Linear Unit (ReLU). The hidden layers' activation function in this work is the Parametric Rectified Linear Unit (PReLU). Since our output is binary, the activation function of the output layer always remains linear. Since the sigmoid function has the vanishing gradient problem, ReLU was developed. An improvised ReLU, named LeakyReLU is introduced. This function does not zero out the negative inputs as ReLU does. Instead, it leaves the positive input at its current value and multiplies the negative input by a little number (such as 0.02). Yet, this has only slightly improved the accuracy of our models. What if, through training, we can learn that tiny number that will let our activation function more effectively adjust to the other parameters? (like weights and biases). Herein lies the role of PReLU. With a minimal increase in training costs, backpropagation allows us to learn the slope parameter. PReLU can be mathematically defined as,

$$f(p_i) = \max(0, p_i) + q_i \min(0, p_i) \qquad (1)$$

where, pi is the input parameter of the ith channel, and qi is the negative slope which becomes the learnable parameter. ReLU, LeakyReLU, and PReLU share the same mathematical formula, where the changes lie with the parameter qi. If qi =0, then f becomes ReLU. If qi >0, then f becomes LeakyReLU. If qi <0, it becomes the learnable parameter and f becomes PReLU.

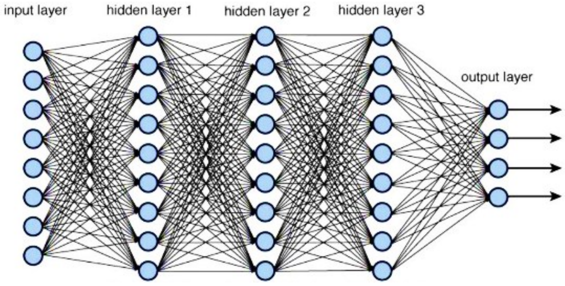

Fig. 1. DNN Architecture

V. DATASET

HAI 3.0 also known as HIL-based Augmented ICS Security Dataset (HAI 22.04) [1] is taken as the dataset for this work. This dataset consists of four CSV files comprising both attack and normal traffic entries with timestamps. All four files are combined into a single CSV file of 361,200 traffic entries (rows) and 86 features (columns). The Hardware-In-the-Loop (HIL) simulator that mimicked the production of steam turbine power and pumped-storage hydropower was added to an ICS testbed, which served as the source of the HAI dataset. According to the dataset requirements listed in [4], our dataset meets all the criteria. Out of 361,200 traffic entries, 12,030 entries are attack traffic, which is 3% of the whole dataset. And this dataset contains timestamps as said above. Also, this dataset has diverse attack entries labeled with attack names. As said above, this dataset is developed in a real-time testbed. Hence, this dataset meets all criteria for a good dataset listed in [4].

VI. Proposed Methodology

A three-staged approach is proposed as the methodology. Pre-processing of the data is the initial stage. The second stage is feature selection, and the final action is model training and validation.

A. *Pre-processing*

Each CSV file's time-series data complies with time continuity. The first column lists the observed time in the following format: "yyyy-MM-dd hh:mm:ss," whereas the subsequent columns provide the observed SCADA data points. As a first step, the timestamp column is removed from the dataset. Then the whole dataset is checked for any empty cells, and string values. Those values are changed to appropriate numeric values. The last column is represented in 1s and 0s, indicating whether the corresponding row data is an attack sequence or not.

B. *Feature Selection*

Out of 86 data points, it is necessary to filter out the unnecessary or irrelevant to the target column from the dataset. For this process, Pearson Correlation is used in this work.

C. *Model Training and Validation*

In this step, as a first part, two of the above-resulted features are removed from the dataset. The dataset is split into training and testing data in the ratio of 7:3 with random data as None, which indicates that it results in different portions of data for each execution of this statement, which means the dataset is shuffled wisely and then the resulting data is split in the above-said ratio. The next part is data standardization. This process transforms the dataset such that the mean and variance of the dataset becomes 0 and 1 respectively. This is mainly done to develop an unbiased model. fit_transform method from the sklearn package is used to do standardization on the training dataset. transform method from the same package is used on the testing dataset to change the testing data based on the mean and variance computed for the training set. The DNN model is now developed with one input layer of input dimension 83, three hidden layers, and an output layer. Input and hidden layers use PReLU as the activation function. This model uses the hinge method to compute the loss and adam algorithm as the optimizer. The model is inputted with training data with a split of validation data in the ratio 7:3 and runs for 100 epochs. Then the model is evaluated with the testing dataset.

VII. Results And Discussion

As a result of the feature selection process, we got 3 irrelevant data points from the dataset – P2_MASW_Lamp, P2_ManualGO, and P2_AutoGO. It indicates that these 3 data points are almost similar to each other and hence any two of them can be removed before entering to next step. Using the seaborn package, a heatmap is developed (Fig 2) to showcase the correlation among the data points. In the final step, the dataset is split into testing and training data on a ratio of 3:7. Out of a total of 361,200 records, Table II shows the number of records that are present in the training and testing datasets.

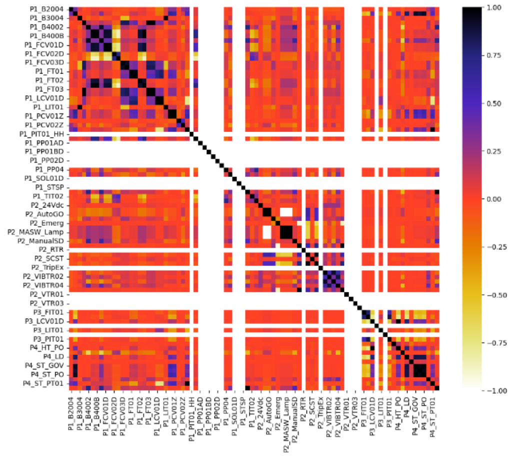

Fig. 2. Heatmap for features correlation

TABLE II. Test-Train Data Split Count

Data	Count of records	Total records in the dataset
Training Data	252,840	361,200
Testing Data	108,360	

During the training phase, accuracy and validation accuracy are calculated and plotted in the graph as Learning Curve (Fig 3). The y-axis limits of the graph lie between 0.9900 and 0.9930. We can infer from the graph that the training and validation scores are closely mapped as the variation between them is too small, i.e., the scores have changes in the one-thousandth digit. It indicates that the proposed model is well-trained. The testing stage is then carried out.

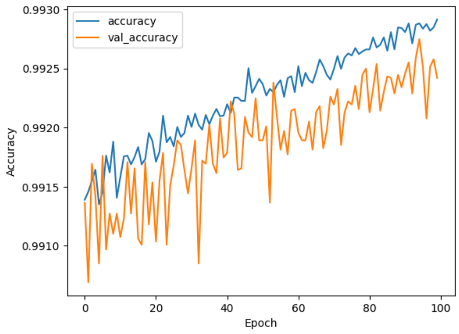

Fig. 3. Learning Curve

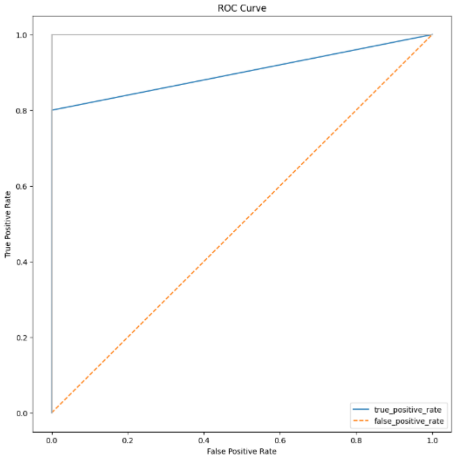

Fig. 4. ROC Curve

The Receiver Operating Characteristic Curve (ROC Curve) is plotted using the findings of this testing section (Fig 4). The trade-off between True Positive Rate and False Positive Rate, also known as sensitivity and specificity, is shown in this ROC curve graph. The curve bends toward the top-left corner. This shows that the proposed model gives better performance. The proposed approach uses as few resources as possible to reach a greater accuracy of 99.24%.

Conclusion

In this Industry 4.0 age, securing OT networks should be the highest priority for the security team of any organization. Although the area susceptible to attack is small, the process of providing security to OT networks is way more difficult. Managing and securing OT networks with no proper patches and without making a small downtime is challenging. This work proposes an anomaly-based IDS for ICS which incorporates the Pearson Coefficient and DNN algorithms. The findings show that the suggested model works effectively and yields a greater accuracy rate.

References

[1] Shin, Hyeok-Ki, et al. "HAI 1.0: HIL-based augmented ICS security dataset." Proceedings of the 13th USENIX Conference on Cyber Security Experimentation and Test. 2020.

[2] Tushkanova, Olga, et al. "Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation." Algorithms 16.2 (2023): 85.

[3] Wang, Xuelei, and Ernest Foo. "Assessing industrial control system attack datasets for intrusion detection." Proceedings of the 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC 2018). Institute of Electrical and Electronics Engineers Inc., 2018.

[4] Essop, Ismael, et al. "Generating datasets for anomaly-based intrusion detection systems in iot and industrial iot networks." Sensors 21.4 (2021): 1528.

[5] Kim, Bedeuro, et al. "A Comparative Study of Time Series Anomaly Detection Models for Industrial Control Systems." Sensors 23.3 (2023): 1310.

[6] Ribu Hassini, S., T. Gireesh Kumar, and S. Kowshik Hurshan. "A machine learning and deep neural network approach in industrial control systems." ICT Analysis and Applications. Springer Singapore, 2022.

[7] Mokhtari, Sohrab, et al. "A machine learning approach for anomaly detection in industrial control systems based on measurement data." Electronics 10.4 (2021): 407.

[8] Bian, Xingchao. "Detecting Anomalies in Time-Series Data using Unsupervised Learning and Analysis on Infrequent Signatures." Journal of IKEEE 24.4 (2020): 1011-1016.

[9] Tai, Johnathan, et al. "Machine Learning Methods for Anomaly Detection in Industrial Control Systems." 2020 IEEE International Conference on Big Data. IEEE, 2020.

[10] Kim, Janghoon, et al. "Study on anomaly detection technique in an industrial control system based on machine learning." Proceedings of the 2020 ACM International Conference on Intelligent Computing and its Emerging Applications. 2020.

[11] Wang, Weiping, et al. "Anomaly detection of industrial control systems based on transfer learning." Tsinghua Science and Technology 26.6 (2021): 821-832.

[12] S. K. Alabugin and A. N. Sokolov, "Applying of Generative Adversarial Networks for Anomaly Detection in Industrial Control Systems," 2020 Global Smart Industry Confer-ence (GloSIC), Chelyabinsk, Russia, 2020, pp. 199-203, doi: 10.1109/GloSIC50886.2020.9267878.

[13] de Riberolles, Theobald, et al. "Anomaly detection for ICS based on deep learning: a use case for aeronautical radar data." Annals of Telecommunications (2022): 1-13.

[14] Chang, Chun-Pi, Wen-Chiao Hsu, and I–En Liao. "Anomaly detection for industrial control systems using k-means and convolutional autoencoder." 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). IEEE, 2019.

[15] Doraswamy, B., and K. Lokesh Krishna. "A Deep Learning Approach for Anomaly Detection in Industrial Control Systems." 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS). IEEE, 2022.

[16] Gillen, Robert E., and Stephen L. Scott. "Method for assessment of security-relevant settings in anomaly-based intrusion detection for industrial control systems." 2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS). Vol. 1. IEEE, 2020.

[17] Aldweesh, Arwa, Abdelouahid Derhab, and Ahmed Z. Emam. "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues." Knowledge-Based Systems 189 (2020): 105124.

[18] Khan, Izhar Ahmed, et al. "HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems." IEEE Access 7 (2019): 89507-89521.

[19] Sabari, K. K., and Saurabh Shrivastava. "Anomaly-based Intrusion Detection using GAN for Industrial Control Systems." 2022 10th International Conference on Reliability, Info-com Technologies and Optimization (Trends and Future Directions)(ICRITO). IEEE, 2022.

[20] Gillen, Robert E., et al. "Assessing Anomaly-Based Intrusion Detection Configurations for Industrial Control Systems." 2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM). IEEE, 2020.

[21] Maniriho, Pascal, et al. "Anomaly-based intrusion detection approach for iot networks using machine learning." 2020 international conference on computer engineering, network, and intelligent multimedia (CENIM). IEEE, 2020.

[22] Eskandari, Mojtaba, et al. "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices." IEEE Internet of Things Journal 7.8 (2020): 6882-6897.

[23] Colelli, Riccardo, et al. "Anomaly-based intrusion detection system for cyber-physical system security." 2021 29th Mediterranean Conference on Control and Automation (MED). IEEE, 2021.

[24] Radoglou-Grammatikis, Panagiotis I., and Panagiotis G. Sarigiannidis. "An anomaly-based intrusion detection system for the smart grid based on cart decision tree." 2018 global information infrastructure and networking symposium (GIIS). IEEE, 2018.

[25] Almehmadi, Abdulaziz. "SCADA networks anomaly-based intrusion detection system." Proceedings of the 11th International Conference on Security of Information and Networks. 2018.

[26] Shaikh, Mrs, and Dr Sita. "Anomaly Based Intrusion Detection System Using Deep Learning Methods." Proceedings of the International Conference on Recent Advances in Computational Techniques (IC-RACT). 2020.

[27] Zhang, Jiazhen, et al. "Federated Learning for Distributed IIoT Intrusion Detection using Transfer Approaches." IEEE Transactions on Industrial Informatics (2022).

[28] Sokolov, Alexander N., Ilya A. Pyatnitsky, and Sergei K. Alabugin. "Applying methods of machine learning in the task of intrusion detection based on the analysis of industrial process state and ICS networking." FME Transactions 47.4 (2019): 782-789.

[29] Khan, Izhar Ahmed, et al. "Efficient behaviour specification and bidirectional gated re-current units ‑ based intrusion detection method for industrial control systems." Electronics Letters 56.1 (2020): 27-30.

[30] Gaiceanu, Marian, et al. "Intrusion detection on ics and scada networks." Recent Developments on Industrial Control Systems Resilience (2020): 197-262.

[31] Li, Huiping, Bin Wang, and Xin Xie. "An improved content-based outlier detection method for ICS intrusion detection." EURASIP Journal on Wireless Communications and Networking 2020.1 (2020): 1-15.

[32] Khraisat, Ansam, et al. "Survey of intrusion detection systems: techniques, datasets and challenges." Cybersecurity 2.1 (2019): 1-22.

[33] Ortega-Fernandez, Ines, et al. "Network intrusion detection system for DDoS attacks in ICS using deep autoencoders." Wireless Networks (2023): 1-17

[34] Khan, Izhar Ahmed, et al. "Efficient behaviour specification and bidirectional gated recurrent units ‑ based intrusion detection method for industrial control systems." Electronics Letters 56.1 (2020): 27-30.