Effective Industrial Internet of Things Vulnerability Detection Using Machine Learning

Cosmas Ifeanyi Nwakanma [1], Love Allen Chijioke Ahakonye [2], Judith Nkechinyere Njoku [2],
Joy Eze [3], and Dong-Seong Kim [2],
[1] ICT Convergence Research Center, Kumoh National Institute of Technology, Korea
(cosmas.ifeanyi@kumoh.ac.kr)
[2] IT-Convergence Engineering, Kumoh National Institute of Technology, Korea
(loveahakonye, judithnjoku24, dskim@kumoh.ac.kr)
[3] Goldsmiths, University of London, United Kingdom
(j.eze@gold.ac.uk)

***Abstract*—Protecting the industrial internet of things (IIoT) devices through vulnerability detection is critical as the consequences of attacks can be devastating. Machine learning (ML) has assisted several works in this regard, improving vulnerability detection accuracy. Based on established vulnerability assessment, development and performance comparison of various ML detection algorithms is essential. This work presents a description of the IIoT protocols and their vulnerabilities. The performance of the ML-based detection system was developed using the WUSTL-IIoT-2018 dataset for industrial control systems (SCADA) cybersecurity research. The approach was validated using the ICS-SCADA and CICDDoS2019 datasets, a recent dataset that captures new dimensions of distributed denial of service (DDoS) attacks on networks. The evaluation and validation results show that the proposed scheme could help with high vulnerability detection and mitigation accuracy across all evaluated datasets.**

***Index Terms*—Detection, IIoT, Machine Learning, Smart Factory, Vulnerability assessment.**

I. Introduction

THE growth in modern technologies and design requirements of fifth-generation (5G) and beyond has given rise to heterogeneous sensor connectivity to provide additional benefits to industries. Industries are deploying more IoT sensors to meet the demand for massive connectivity of devices. The heterogeneity of IIoT devices (such as actuators and sensors) and their connectivity capabilities have increased IIoT's vulnerability to attacks, necessitating a robust and efficient machine learning-based detection system. Traditionally, industrial control systems (ICSs) operate as stand-alone systems with little attack vulnerability. ICSs are mission-critical systems utilized for real-time collection and analysis of data in IIoT and, as such, place high availability constraints on industrial systems. A breakdown due to an attack can be devastating and lead to a monumental loss of revenue by manufacturing companies and smart factories.

IIoT environments have been aided by AI and big data analytics, which have recently attracted much research work. Several machine learning (ML) schemes provide for the security and enhancement of the IIoT. One such scheme is the intrusion detection systems (IDS) and vulnerability detection systems based on various ML and available datasets. However, challenges such as accuracy, computation cost, time complexity, and the need for a testbed for up-to-date datasets have become critical as the dynamics of cyber attacks continue to change. AI is a rapidly growing trend across several industries, such as smart factories, security, and surveillance. Using pattern recognition and improved applications of neural processing, AI is helping these companies become more efficient in attack mitigation. The purpose of AI projects is to make decisions based on meaningful information. An IDS identifies or verifies network traffic for anomalies. The system simultaneously matches the input against the entire database rather than by individual elimination. It can also be used to retain it in the event of any incorrect input and disallow any future use of this input through machine learning.

Distributed denial of service (DDoS) threats, for instance, are undoubtedly critical security challenges to the Internet of Things (IoT) and, indeed, all forms of networks. Attacks by DDoS aim at overburdening the target IoT devices or networks by sending continuous and malicious traffics [1]. Reducing or mitigating security attacks on IIoT has attracted research attention due to the devastating effect and possible economic loss should they break down. In recent years, several ML approaches have employed traditional techniques for feature selection. However, one of the challenges with these approaches, is the limitation of the amount of data needed for feature learning and the burden of dataset balancing [2]. The reason is that as the volume of data increases to an exceedingly high level, the false alarm rate (FAR) is noticeably high. Second, most relied on the accuracy and $F-1$ score as classification evaluation metrics. These metrics perform poorly in the face of extensive data or where the data is not balanced. Thus, Selecting an efficient detection system is needed to secure networks. More importantly, such a detection system should focus on recent data or data from test beds. In addition, such an efficient ML scheme should provide alternative metrics such as Mathews correlation coefficient (MCC) [3]. Based on the aforementioned, the following contributions were made by

this work:

1) The first contribution of this article is a comprehensive description of the IIoT protocols and exposing the inherent vulnerabilities. Such information forms the basis for appreciating the need for security in IIoT systems.
2) Second, leveraging on the vulnerability assessment of [4], this work compared several ML-based IIoT vulnerability detection systems to take care of intrusion problems in IIoT. It is to determine the most efficient of them based on MCC and other metrics.
3) To validate the proposed ML algorithm, we investigated state-of-the-art ML techniques using WUSTL-IIoT-2018, ICS-SCADA, and CICDDoS2019 datasets to show the efficiency of the algorithms in terms of accuracy, feature extraction, computation complexity, MC Nemar's test, and time taken to train and test each classifier.

The organization of the paper is as follows: Following this Section I (Introduction) is Section II, which is a review of recent related works in ML-based vulnerability detection for IIoT. The pipeline of the proposed ML-based system and typical IIoT setup is described in Section III. Section IV presents the performance evaluation and the results. The study concludes in section V with recommendations for future research.

II. Theoretical Background and Related Works

A. Industrial Internet of Things (IIoT)

Historically, this describes the IoT's application to manufacturing, production, and general industrial applications. The overall benefit is that it rewards efficiency and reliability in the company's operations. They constitute an essential part of the industrial ecosystem needed to transform factories into smart factories where there is seamless data capture, transmission, and smart decision-making by humans and machines. Moreover, IIoT allows for optimized usage of a company's assets, predicts points of failure, and draws attention to cases needing maintenance. In addition to the above, the novel virus COVID-19 created more need for remote work, which changed the threat landscape as more activities moved online and networked. According to [5], a more comprehensive definition of IIoT is "a system comprised of networked smart objects, cyber-physical assets, associated generic information technologies, and optional cloud or edge computing platforms that enables real-time, intelligent, and autonomous access, collection, analysis, communications, and exchange of process, product, and service information within the industrial environment in order to optimize overall production value. This value could include improving product or service delivery; increasing productivity; lowering labor costs; lowering energy consumption; and shortening the build-to-order cycle."

B. Vulnerabilities in IIoT Protocols and Impact on Industry Operation

The consensus is that the communication protocols used by ICS lack sufficient security by traditional IDSs [4]. Some of the protocols include MODBUS, building automation and control network (BACnet), message queuing telemetry transport (MQTT), and distributed network protocol version 3 (DNP3). A flooding attack can affect the availability of MODBUS, while a denial of service (DOS) attack can halt BACnet. Details of the vulnerabilities of these protocols are in [4]. Thus, the operational technology environment and ICS must be secured to protect critical infrastructures. According to the Siemen/Ponemon Institute study 2019 report, around 56% of gas, wind, water, and solar utilities worldwide faced at least one cyberattack in 2018 alone, causing a shutdown or loss of operation data [6]. The necessity for remote access, office utility connectivity, use of public networks, and growing use of IoT components enabled by the grid and enterprise IT are all contributing factors. As shown in Fig.1, the impact of cyber attacks on the operations of industries is better imagined as there can be a devastating impact on loss of confidential information, revenue, manufacturing or production line breakdown [6].

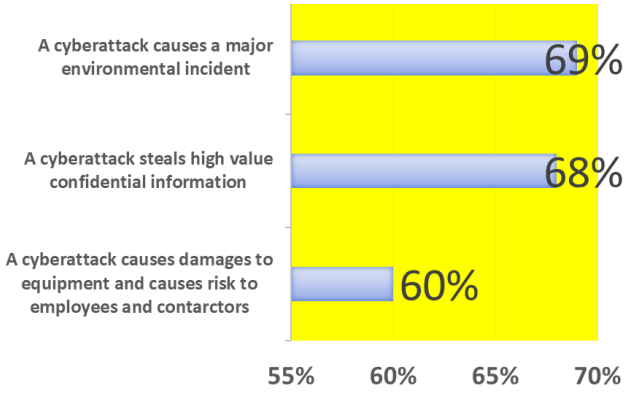

Figure 1. How Attacks on Operational Technology (an example is IIoT) affect Operations on Industries [6]

Understanding the changing nature of the IIoT attacks is the right step to security and vulnerability assessment needed for the countermeasure. Since IIoT no longer operates in isolation, the attack surface is more extensive. It raises the challenge of putting strategies in place to secure the IIoT despite exposure to the threat of increased connectivity and the internet. In order to secure the IIoT, there is a need for efficient mechanisms, which include ML approaches.

C. Machine Learning for IIoT Security

The application of ML for IIoT security has been well documented in recent years. Table I is a summary of the recent works in IoT and IIoT protection using various datasets and ML approaches. ML is used for feature extraction, outlier detection, value prediction, and pattern recognition in IIoT traffic/data, all of which are essential elements in securing IIoT networks and devices. The objective of applying ML to IIoT security is to identify security flaws (anomaly detection, intrusion, and malware detection).

However, one case of grave concern is the continuous need for human intervention, which reduces the efficiency of the

Table I
SUMMARY OF RECENT ML FOR VULNERABILITY DETECTION IN IIOT

Ref	Year	Algorithms	Dataset
[4], [7]	2019, 2018	DT and RF	WUSTL-IIoT
[8]	2020	ς-Classifier	KDD CUP'99
[9]	2020	Several	T-IIoT
[10]	2020	HADIoT	ISCX-2012
[11]	2020	DNN+DT	SWAT+GP
[12]	2020	RS+RT	ICS [13]
[14]	2021	DT	CIRA-CIC-DoHBrw-2020 [15]

ML systems. One factor responsible for human interaction is the challenge of handling imbalanced attack classes since a new attack class arises from time to time. To handle the imbalance introduced by the new attack category, authors in [16] proposed a novel algorithm that leverages optimized weight for each class to increase the accuracy of attack kinds that are rarely (or barely) discernible. By so doing, classification performance improves, and detection accuracy increases.

Additionally, the authors of [11] developed an ensemble deep learning solution for ICS cyber threat detection. They combined deep neural networks with decision tree classifiers to detect attacks. The proposed scheme performed comparatively well when tested using the safe water treatment (SWAT) and gas pipeline (GP) datasets while taking care of the imbalance dataset and reducing feature engineering technicalities. In like manner, authors in [12] proposed a random subspace(RS)-based random tree (RT) ensemble model to enhance the detection of attacks on SCADA while striking a tradeoff between model complexity, classification accuracy, and reliability. However, they created an additional problem with the ensemble model because the execution time of the proposed model was more than that of a single RT classifier. Moreover, the RSRT model could not optimize random feature selection when there was a small number of features.

D. Recent Testbed Attempts on Vulnerability Detection in IIoT

Therefore, to lend credence to the rising and dynamic nature of attacks on IIoT, recent efforts aim at developing datasets from testbeds to assist the research work in the area of detection and optimized countermeasures to IIoT attacks. This attempt is in response to the dearth of real-world datasets for the IoT and IIoT application domains. The authors of [9] developed what they termed a new generation dataset for IoT and IIoT data-driven intrusion detection systems (T-IIoT Dataset). The advantage of this dataset over the KDDCUP99, NSL-KDD, or UNSW-NB15 is that these datasets lack sensors' reading data and network traffic data. It consists of nine (9) attack types, such as distributed denial of service (DDoS), ransomware, backdoor, data injection, denial of service (DoS), scanning, and Man-in-the-Middle (MITM). The data sources are from seven (7) IIoT and IoT sensors as described in [9]. The dataset includes network traffic from IoT networks, operating system logs, and telemetry data from IIoT services.

In [4], [7], authors developed a test-bed for SCADA IDS. The selected IIoT system testbed monitors a water storage tank's water level and turbidity quantity. With the sensors' aid, the testbed ensures the water level is within predefined levels. After that, the authors subjected the testbed to various attack scenarios to gather data. The resulting dataset is code-named WUSTL-IIoT-2018 SCADA-IDS and is used in our simulation.

E. Summary of Related Works

In summary, Table I is a detailed analysis of recent research efforts in IIoT vulnerability detection using ML. The need to efficiently handle computation costs using feature selection techniques such as principal component analysis (PCA) or Pearson correlation coefficient (PCC) is one common lesson from these works. Also, most authors relied on only accuracy and F1 score, which has been mathematically proven not to be reliable in cases of imbalanced dataset [2]. In this work, therefore, we adopted the appropriate alternative MCC to validate the ML algorithms' classification. We also adopted PCC and PCA for top feature selection. In addition, we have adopted the WUSTL-IIoT-2018, ICS-SCADA, and CICDDoS2019 datasets for our evaluation since they captured the attacks for IIoT and are considered recent.

III. ML SYSTEM MODEL AND DATASET DESCRIPTION

A. ML Vulnerability System Model

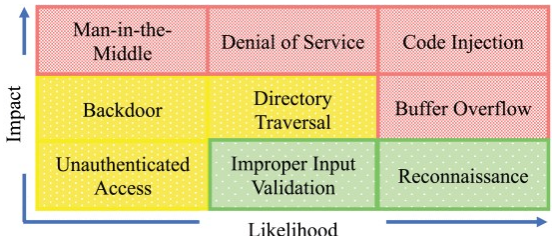

Figure 2. A matrix of risk assessment of most critical IIoT Vulnerabilities [4]

In this work, we have leveraged the vulnerability analysis of IIoT as captured by [4] where the authors have classified various attacks into three categories based on a combination of the likelihood of attack occurrence and the severity of the impact of such attacks. From Fig. 2, the red code is considered the most critical since it can be of devastating effect when it occurs. Some examples are DoS, Code injection, and MITM. The yellow codes are moderate since they fall in between the two extremes. Backdoor, directory traversal, and unauthenticated access attacks are examples of such. Finally, the attacks with the least likelihood and most negligible impact are the green-coded areas, representing their non-critical nature.

Fig. 3 below shows our ML-based model for efficient vulnerability detection in the IIoT.

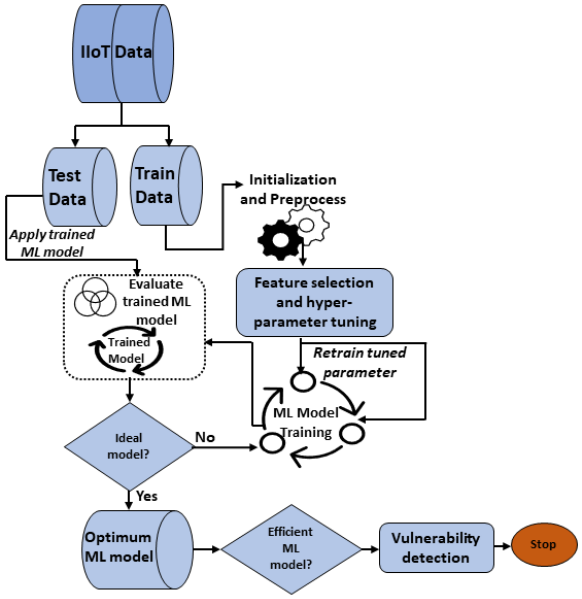

Figure 3. This is the Machine learning model adopted in this study. It demonstrates the process flow of arriving at an efficient model for vulnerability detection in the IIoT.

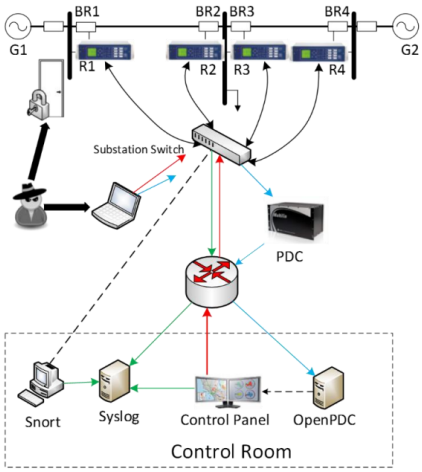

Figure 4. Configuration of the Power System SCADA Network used to generate the SCADA dataset [18]

B. Description of the Power System SCADA Network (ICS-SCADA Dataset)

A convenient method for remote monitoring and control of renewable energy sources is offered by the power SCADA system. It increases effectiveness and is utilized frequently in many industrial applications. Data is gathered and processed in accordance with the needs of various substations. The central system is informed by the close monitoring of substation components by the programmable logic controllers in the substations. It is in charge of enhancing efficiency by ensuring a reasonable power factor range [17]. Fig. 4 depicts the diagram of the power system network configuration used to generate the dataset. It consists of various parts, the first of which are power generators G1 and G2. R1 to R4 are Intelligent Electronic Devices (IEDs) that control the breakers (on or off). The breakers are BR1 to BR4. In addition, there are two lines, line one connects breaker one (BR1) to breaker two (BR2), and line two connects breaker three (BR3) to breaker four (BR4). Each IED is programmed to control one breaker. R1 controls BR1, and R2 controls BR2, respectively [18]. Since they lack internal validation, IEDs use a distance protection technique that trips the breaker on detecting anomalies regardless of whether they are valid or contrived. The constituents and configuration of the power grid SCADA network define its peculiarity in terms of data generated, vulnerability, and attack types. Hence, it requires an efficient IDS. The data is from twenty-nine (29) types of measurements from different phasor measurements (PMU). A PMU is a device that measures electrical waves on a power grid while synchronizing with an expected time source. This network comprises four PMUs that each measure 29 features, for a total of 116 PMU measurement columns in the dataset. Each column's index is in the form "R#-Signal Reference," indicating the type of measurement from a PMU designated by "R#." The dataset contains 128 features. For more details, see the dataset description.

C. WUSTL-IIoT-2018 Dataset for ICS(SCADA) Cybersecurity Research

The WUSTL-IIoT-2018 dataset for ICS (SCADA) cyber security research by [7] focuses on reconnaissance attacks on SCADA. A reconnaissance involves hackers using scan tools to locate network devices and possible spots for vulnerabilities. Port scan, address scan, device identification attacks, and exploits were all conducted against the testbed as reconnaissance assaults. Details can is in [7]. Although the raw data had 25 networking features, the authors carried out feature selection; thus, the following top features emerged for the creation of the dataset: total transaction packet count (Totpkts), total transaction bytes (TotBytes), Source/destination packet count (SrcPkts), Destination/Source packet count (DstPkts), Source/Destination transaction bytes (SrcBytes) and port number of the source (Sport). These features served as a guide in our evaluation of machine learning candidates and model evaluation. They used audit record generation and utilization system tools to monitor all network traffic, with 93.93% regular traffic and 6.07% attacked traffic, respectively.

D. CICDoS2019 Description

The CICDDoS2019 [19] final dataset includes 12 DDoS attacks, namely NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, and TFTP in the training day, and seven (7) attacks including PortScan, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag and SYN in the testing day. A cutting-edge dataset, CICDDoS2019, was utilized to train and test the suggested model for performance assessment. To the best of the author's knowledge, this dataset for DDoS is the most latest and sophisticated one and consists of

benign and other typical DDoS attacks. The different DDoS attack types are categorized into reflection-based threats and exploitation-based threats in the dataset. SYN, UDP, and UDP-Lag DDoS are exploitation-based threats, whereas reflection-based attacks target NetBIOS, MSSQL, and TFTP. Over 80 features make up CICDDoS2019 [19].

180,000 samples of benign and many other DDoS attack classes were included in the CICDDoS2019 dataset. Each class has a total of 14,000 to 18,000 attacks. Here, caution was taken to avoid creating an unrepresentative dataset by either over-representing or under-representing one class. Each class has around 18,000 samples, with the only benign class having about 4,000 fewer samples. The dataset was divided using Scikit Learn's train_test_split, with 25% set aside for model testing and 75% used for training [1].

E. ICS-SCADA Dataset Description

The ICS-SCADA dataset from the Oak Ridge National Laboratories (ORNL) was a result of establishing a power grid testbed [18]. The dataset is from the power grid SCADA system testbed and contains computations associated with disturbance, cyber-attack exploits, and normal and control obtained during electrical transmission. This study evaluated the dataset's binary and three (3) classes. It consists of 128 features with responses as a natural, attack, and no event for the 3 class and attack and no event for the binary class. "Attack", as the name implies, depicts the attack state; "no event" is the Benign state or no attack, while the natural represents a zero-day or ground truth. These features came from 4 Phasor Measurement Units (PMUs), which compute energy signals of the substation with a regular schedule source for competent time simultaneity. Each PMU calculates 29 features; thus, 116 PMU measurements are in all. These features are referred to as R# (signal Reference), indicating the ratio of PMU and type of analysis. For instance, R1-PA1:VH denotes the Phase A voltage phase angle calculated by PMU R1 [18]. Additional 16 columns by snort alerts, control panel logs, and relay logs alongside a combination of relay and PMU. The last column represents the marker to label different events. Furthermore, each batch of the 15 batches comprises 3711 attack vectors, 294 no event occurrences, and 1221 natural events through the analysis patterns.

F. Feature Selection and hyper-parameter Settings

1) Feature Description: In order to extract features, it is vital to have good background knowledge of network traffic features. The first step involves preprocessing the network traffic data to extract bidirectional transmission control protocol (TCP) flows identified by their source and destination internet protocol (IP) addresses and ports. Long TCP connections are divided into many bidirectional flows using a timeout. The statistics on the size of the first N packets transmitted and received, as well as the related inter-arrival periods, are the features describing the bidirectional TCP flows (IAT). The count is the proportion of non-zero-sized packets among the first N packets. It represents the actual number of packets transmitted or received, in other words. Due to the timeout to divide lengthy TCP connections, it could be less than N. For instance, the count is equal to that amount if the total number of packets sent during the timeout length is less than N. It is equal to N if not. For the IAT to exist, N needs to be equal to or larger than 2. The statistics that cannot be calculated, such as the mean and standard deviation of the IAT between packets, are all set to 0 if a communication only contains one packet transmitted or received. Application independence characterizes the attributes used to describe network traffic. The TCP protocol can be used with any application. It should be noted that features can still be extracted even if network connection is encrypted. As all the devices utilized for the research use HTTP/HTTPS for communication, this study only focuses on TCP protocols. It makes sense because TCP is the most common network protocol used by IoT malware [20].

2) Feature Selection: Feature selection is an enabler for enhancing the performance of ML models, especially for classification. The reason for this is that it eliminates the dimensionality curse, characterized by having more features than samples and, in most circumstances, resulting in overfitting of the model, which prevents it from generalizing to new data. Moreover, ensuring a simple and explainable model of controllable features is desirable, which is only made possible by avoiding too many undesired and redundant features. In order to achieve this goal, this work implements the Pearson correlation coefficient (PCC). PCC is depicted mathematically as follows:

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}}, \tag{1}$$

where n is the sample/dataset size, x_i, y_i are the individual sample points indexed as i. At the end of the PCC iteration, i.e., when $i == n$, the top features are selected and used for the model. The top 10 features selected from CICDDoS2019 dataset are listed in the Table II while Table III shows top 5 features from WUSTL-IIoT-2018 dataset.

Table II
TOP TEN FEATURES CHOSEN FROM THE CICDDOS2019 DATASET, LISTED IN ORDER OF IMPORTANCE

No.	Name of Feature
1	Forward packet length max
2	Flow packets/seconds
3	Average packet size
4	Subflow forward bytes
5	Average forward segment size
6	Standard deviation of flow inter-arrival time
7	Min packet length
8	Total forward packets
9	Packet length variance
10	Protocol

3) Hyperparameters: Hyperparameters are used to regulate and track a model's learning process across all phases of training, helping to increase the efficiency and effectiveness of the learning process. The Keras-tuner Library was used to tune the hyperparameters in this study.

Table III
TOP 5 FEATURES FROM THE WUSLT-IIOT-2018 DATASET

No.	Name of Feature
1	Source Port (Sport)
2	Mean flow (Mean)
3	Total percentage loss (pLoss)
4	Source loss(SrcLoss)
5	Destination Port (Dport)

4) Feature Scaling and Dimension Reduction: Data preparation includes processes like feature scaling and dimension reduction. This stage involves preparing the dataset to make it easier for the machine learning algorithm to read the data more efficiently and accurately, as well as adhering to the machine learning algorithm that will be employed. Different features in the dataset have different ranges, and most of the time, the range is simply too wide; for instance, a specific characteristic can have a value between 10 and 100 or even between 10 and 10,000. In this situation, normalization or feature scaling using the Min-Max Scaling function of sci-kit learn is required when the range of a feature is small, such as between 0 and 1.

IV. RESULTS, ANALYSIS, AND PERFORMANCE EVALUATION

A. Evaluation Metrics

For a fair comparison, some considered traditional performance metrics are true positive (TP), true negative(TN), false negative (FN), false positive (FP), false alarm rate (FAR), precision, F1-measure, recall, the area under receiver operating characteristics (AUC), executive time, Mc-Nemar's test, sensitivity, and Mathew's correlation coefficient (MCC). While it is not the goal of this paper to explain these metrics in detail, suffice it to say that a suitable detection system should have high accuracy, precision, recall, and F1 score with a low false alarm rate. The accuracy is (2):

$$Accuracy = \frac{TP + TN}{(TP + TN + FN + FP)}, \tag{2}$$

On the other hand, FAR is given as (3):

$$FAR = \frac{FP}{(TN + FP)}, \tag{3}$$

Precision, recall, F1- measures, and sensitivity are given as (4), (5), (6), and (7):

$$Precision = \frac{TP}{(TP + FP)}, \tag{4}$$

$$Recall = \frac{TP}{(TP + FN)}, \tag{5}$$

$$F1 - measure = \frac{2 * (Precision * Recall)}{(Precision + Recall)}, \tag{6}$$

$$sensitivity = 100 * Recall(\%) \tag{7}$$

The MCC is used to evaluate the quality of the classification. It finds usefulness when it is needed to have a metric not affected by the unbalanced datasets [3]. The drawback of relying only on the F1 score is that it can lead to overoptimistic inflated results, especially on an imbalanced dataset. To solve this, authors in [3] gave a comprehensive analysis and justification for MCC as a veritable alternative. The MCC values range -1 and +1, representing cases of perfect misclassification and perfect classification, respectively. Mathematically, MCC is in (8)

$$MCC = \frac{TP.TN - FP.FN}{\sqrt{(TP + FP).(TP + FN).(TN + FP).(TN + FN)}}, \tag{8}$$

The Confusion Matrix (CM): The diagonal in the confusion matrix represents accurate predictions, and the non-diagonal represents false predictions. See the table below for the confusion matrix based on the ICS-SCADA dataset, which contains three (3) classes of traffic events, including, attack, natural, and no events.

Table IV
DESCRIPTION AND FEATURES OF A CONFUSION MATRIX

		Predicted class		
		No events	Attack	Natural
2*Actual Class	No events	992	107	46
	Attack	114	1098	4
	Natural	1	1	1243

B. Performance comparison of ML algorithm candidates

In this study, the ML-based IDS is for attack detection and classification to determine if a given traffic sample is malicious or benign. The three chosen datasets are inputs to the IDS, and the output is either benign or attack traffic. The dataset was also divided into training and testing sets in a 70/30 split.

The study used and tested six distinct techniques: random forest (RF), decision tree (DT), extreme gradient boosting (XGB), gradient boosting (GB), Adaboost (AD), and the recurrent neural network (RNN). The IDS learning models emerged using the Keras library [21] and the scikit-learn library [22]. The models are trained and tested on the three datasets, and their performance is in Figs. 5, 6 and 7. The time comparison is in Fig. 8.

The experimental results demonstrate the efficiency of the ML algorithms for vulnerability detection in the IIoT. The combined advantage of the accuracy and computation time-cost demonstrates the performance of the ML classifiers over the RNN. It confirms its suitability for the IIoT scenario.

C. Mc-Nemer Test analysis

In addition to the metrics mentioned above, Mc-Nemar's test is an essential criterion for comparing the performance of two ML algorithms. Mc-Nemar's test is a non-parametric pairwise test showing that an algorithm has achieved a statistically significant increase over the other. When the z-value of Mc-Nemar's test >1.96 (p-value is less than 0.05), the conclusion is that there is a significant difference between the two

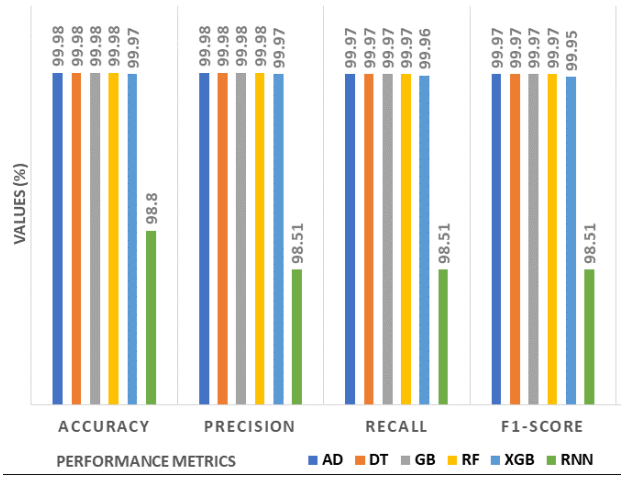

Figure 5. Model performance of the six compared models on the WUSTL-IIoT-2018 dataset.

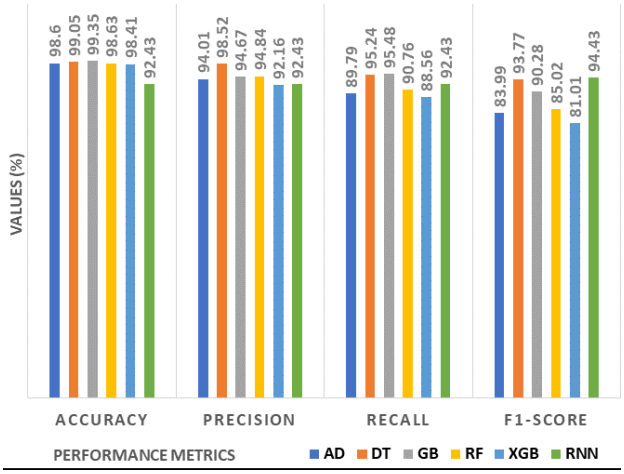

Figure 6. Model performance of the six compared models on the ICS-SCADA Dataset.

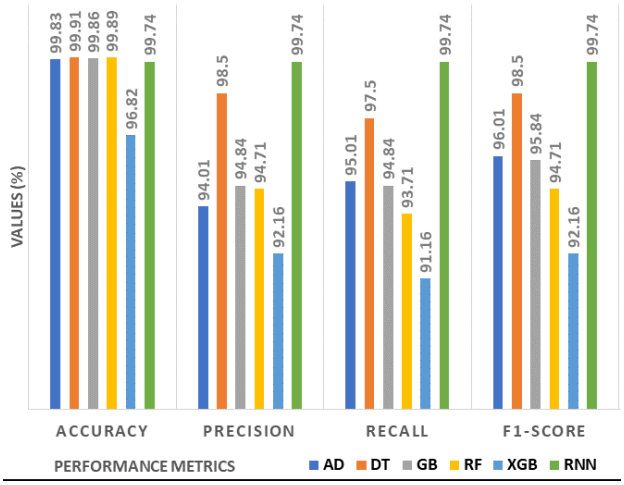

Figure 7. Model performance of the six compared models on the CICIDS2019 dataset.

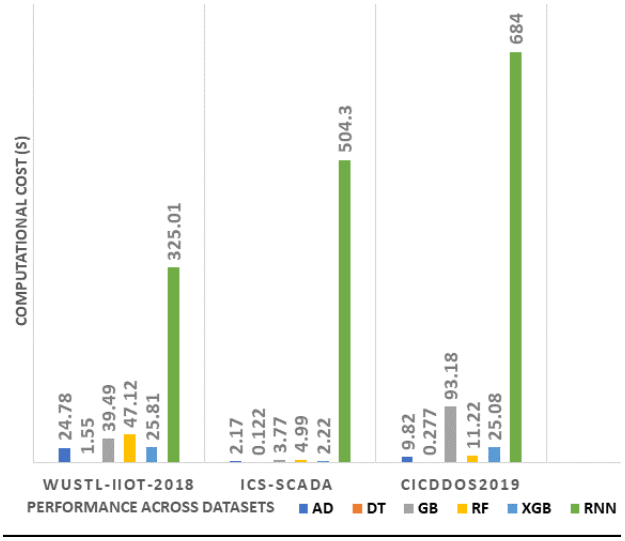

Figure 8. Time model performance of the six compared models all evaluated datasets.

algorithms. Z-score is used to show the confidence levels [23]. Z-score is presented mathematically as in (9)

$$Z = \frac{(\beta - \delta) - 1}{\sqrt{(\beta + \delta)}}, \tag{9}$$

where β is the number of times, the first algorithm succeeded in the classification, and the second failed. Also, δ represents the number of times when the second algorithm succeeded in the classification and the first one fails.

The Mc-Nemer test of the least performed model RNN is a p-value (1-tail and 2-tail test) of 0.000, which is less than 0.05. Thus, we rejected the null hypothesis and accepted the alternative stating that the *"intrusion type, target system, and dataset type* ***does have a significant impact on the performance of ML models."*** Table V contains the Mc-Nemer's χ^2 values for WUSTL-IIoT-2018, ICS-SCADA, and CICDDoS2019 datasets, respectively.

Table V
MCC RESULTS ON THE THREE DATASETS

Dataset	Mc-Nemer's Test Statistic χ^2	ρ-value	Odd Ratio	MCC
WUSTL-IIoT-2018	387764.6948	0.000	13.2861	0.86
ICS-SCADA	707.8278	0.000	61.9161	0.9682
CICDDoS2019	207531.6327	**0.000**	**1149.5912**	**0.9965**

D. MCC Test of RNN Algorithm

The previous results show that the RNN algorithm had a minor performance across metrics. The RNN model had poor classification ability for the WUSTL-IIoT-2018 dataset, as corroborated by the previous accuracy, precision, and recall results. However, to verify the quality of classification of the least performed model, this section gives the MCC test results of RNN for the three datasets categories. For binary classification, Table V shows that the RNN had a minimum MCC value

of 0.86 for WUSTL-IIoT-2018, 0.9682 for ICS-SCADA, and 0.9965 for the CICDDoS2019 dataset, respectively.

V. Conclusion

The discovery of vulnerabilities in the IIoT network is crucial. Big data analytics and ML approaches have greatly aided in the development of IDSs to assure secure protection. However, the current cyber-risks of industrial critical systems and conventional systems differ due to primary variances and differential priorities. There is a significant gap in ensuring proper security for these systems, which is why focusing on critical industrial systems is vital. As a result, there should be great care in ensuring IIoT security. The experimental analysis in this paper illustrates the effectiveness of ML-based strategies for system security.

We proposed an ML algorithm for efficient IIoT intrusion detection and classification in this work. We provided a comparative study of efficient ML algorithms focusing on typical candidates such as RF, DT, AD, XGB, GB, and RNN. We evaluated the algorithms using WUSTL-IIoT-2018 and ICS-SCADA datasets for industrial control systems (SCADA) cybersecurity research and validated their performance using the CICDDos2019 dataset. Feature selection and dimensionality reduction were with the Pearson correlation coefficient (PCC), which aided the ML algorithms' accuracy since it helped eliminate redundant and data considered not helpful.

The proposed algorithm consistently outperformed other compared algorithms in a combined advantage of model accuracy and computation time-cost, which is a critical factor in IIoT. It is pertinent to say that the proposed algorithm is apt for vulnerability detection and attack classification, particularly in a real-time IIoT environment.

Acknowledgment

This research work was supported by Priority Research Centers Program through NRF funded by MEST (2018R1A6A1A03024003) and the Grand Information Technology Research Center support program (IITP-2022-2020-0-01612) supervised by the IITP by MSIT, Korea.

References

[1] G. Amaizu, C. Nwakanma, S. Bhardwaj, J. Lee, and D. Kim, "Composite and Efficient DDoS Attack Detection Framework for B5G Networks," *Computer Networks*, vol. 188, p. 107871, 2021. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128621000438

[2] M. Zolanvari, M. A. Teixeira, and R. Jain, "Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning," in *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2018, pp. 112–117.

[3] D. Chicco and G. Jurman, "The Advantage of the Mathews Correlation Coefficient (MCC) over F1 Score and Accuracy in Binary Classification Evaluation," *BMC Genomics*, vol. 21, no. 6, pp. 1–13, 2020.

[4] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6822–6834, 2019.

[5] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in Industry*, vol. 101, pp. 1–12, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166361517307285

[6] L. Simonovich, *Caught in the Crosshairs: Are Utilities Keeping up with the Industrial Cyber Threat? Assessing Operational Readiness of the global Utilities Sector*, ser. 3. Houston: Siemens Gas and Power, 2019, a collaboration work between Ponemon Institute and Siemens.

[7] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. SamaKa, "SCADA System Testbed for Cybersecurity Research using Machine Learning Approach," *Future Internet*, vol. 10, no. 76, pp. 1–15, 2018.

[8] M. Sayad Haghighi, F. Farivar, and A. Jolfaei, "A Machine Learning-based Approach to Build Zero False-Positive IPSs for Industrial IoT and CPS with a Case Study on Power Grids Security," *IEEE Transactions on Industry Applications*, pp. 1–1, 2020.

[9] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems," *IEEE Access*, vol. 8, pp. 165 130–165 150, 2020.

[10] H. Chang, J. Feng, and C. Duan, "HADIoT: A Hierarchical Anomaly Detection Framework for IoT," *IEEE Access*, vol. 8, pp. 154 530–154 539, 2020.

[11] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "An ensemble deep learning-based cyber-attack detection in industrial control system," *IEEE Access*, vol. 8, pp. 83 965–83 973, 2020.

[12] 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 Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6154–6162, 2020.

[13] *Industrial Control System (ICS) Cyber Attack Datasets*, 2019. [Online]. Available: https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets

[14] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Efficient Classification of Enciphered SCADA Network Traffic in Smart Factory Using Decision Tree Algorithm," *IEEE Access*, vol. 9, pp. 154 892–154 901, 2021.

[15] M. MontazeriShatoori, L. Davidson, G. Kaur, and A. H. Lashkari, "Detection of DoH Tunnels using Time-Series Classification of Encrypted Traffic," in *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. IEEE, 2020, pp. 63–70.

[16] Z. Chkirbene, A. Erbad, R. Hamila, A. Gouissem, A. Mohamed, M. Guizani, and M. Hamdi, "A Weighted Machine Learning-Based Attacks Classification to Alleviating Class Imbalance," *IEEE Systems Journal*, pp. 1–12, 2020.

[17] K. Sayed and H. A. Gabbar, "Chapter 18–SCADA and Smart Energy Grid Control Automation," in *Smart Energy Grid Engineering*. Academic Press, 2017, pp. 481–514. [Online]. Available: https://doi.org/10.1016/B978-0-12-805343-0.00018-8

[18] U. Adhikari, S. Pan, T. Morris, R. Borges, and J. Beave, "Industrial Control System (ICS) Cyber Attack Datasets," *datasets used in the experimentation.[Online]. Available: https://sites. google. com/a/uah. edu/tommy-morris-uah/ics-data-sets*, 2019.

[19] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*, 2019, pp. 1–8.

[20] M. R. Shahid, G. Blane, Z. Zhang, and H. Debar, "Anomalous Communications Detection in IoT Networks Using Sparse Autoencoders ," *arXiv*, pp. 1–5, 2019. [Online]. Available: https://arxiv.org/pdf/1912.11831v1.pdf

[21] J. Moolayil, J. Moolayil, and S. John, *Learn Keras for Deep Neural Networks*. Springer, 2019.

[22] E. Bisong, "Introduction to Scikit-learn," in *Building machine learning and deep learning models on Google cloud platform*. Springer, 2019, pp. 215–229.

[23] M. Latah and L. Toker, "Towards an Efficient Anomaly-Based Intrusion Detection for Software Defined Networks," *IET Networks*, vol. 7, no. 6, pp. 453–459, 2018.