Attack Detection Using Artificial Intelligence Methods for SCADA Security

Nesibe Yalçın, Semih Çakır, and Sibel Ünaldı

***Abstract*—Technological developments and transformations have rapidly risen since the Fourth Industrial Revolution. The prevalence of industrial devices interconnected over the wireless sensor networks and the provision of a sustainable data flow reveal the importance of the Industrial Internet of Things (IIoT). In the manufacturing industry, supervisory control and data acquisition (SCADA) systems are used to control IIoT for critical infrastructure. A cyberattack on the network-based communication structure embedded into the architecture of industrial equipment can significantly disrupt/sabotage product manufacturing and other industrial operations. The digitization of industrial control systems can expose the systems to malicious actors and therefore requires additional security solutions, such as intrusion detection systems (IDSs). Increasing sophistication of cyberattacks, industrial companies need to adopt innovative solutions like artificial intelligence (AI)-based attack detection to protect their valuable assets. In addition, AI-based approaches are more effective as they analyze network traffic, identify threats, and adapt to new attack techniques. This study aims to develop an AI-based IDS with high accuracy for SCADA security. In the study, cyberattacks that may occur against SCADA systems are examined. AI methods (including *K*-nearest neighbor, quadratic discriminant analysis, adaptive boosting, gradient boosting, and random forest) in different categories are used and AI models with various parameters are built. To improve the detection performance of the models, comprehensive experiments are carried out on two different SCADA data sets. As a result of experiments, the test accuracy rates exceeding 96.82% are achieved by all models: on the WUSTL-IIOT-2021 data set, the XGB model has outperformed with an accuracy of 99.99%.**

***Index Terms*—Artificial intelligence (AI), attack detection, cyber security, Industrial Internet of Things (IIoT), supervisory control and data acquisition (SCADA).**

I. Introduction

IN RECENT years, two initiatives have emerged with the potential to bring in an era of manufacturing change. The first is the Industry 4.0 vision, and the second is the Internet of Things (IoT), an internetworking of physical devices or "things" that can exchange information about their functions/roles and the network environment. Many areas, such as industry, health, agriculture, and energy, employ IoT technologies. The Industrial IoT (IIoT) refers to the application of IoT to industry and aids in the process of digital transformation in the industry. It also enables the networked connectivity of instruments, sensors, and other IoT devices in a manufacturing environment to provide computer-based data gathering, analysis, and control. Many traditional industry companies are embracing the digital transformation of IIoT. Critical infrastructure (gas, oil, manufacturing, transportation, and electricity) networks need to be constantly operated and monitored to ensure sustainability and security in industrial control systems (ICSs) [1], [2].

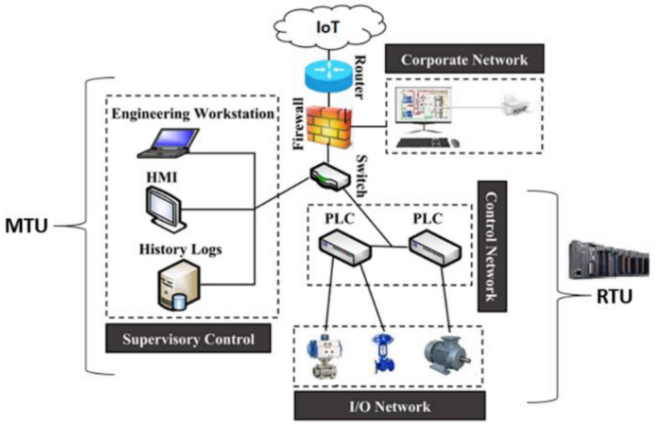


Fig. 1. Schematic representation of an ICS/SCADA system [1].

A supervisory control and data acquisition (SCADA) system is designed and implemented to increase energy efficiency, reduce energy losses, and monitor and analyze operational features within the specific industrial automation system [3]. Fig. 1 depicts the general structure of the ICS/SCADA system. Master terminal unit (MTU), remote terminal unit (RTU), human–machine interface (HMI), and programmable logic controllers (PLCs) are the main components of a classical SCADA system. MTU, the main command and control center of the entire SCADA system, is a supervisory computer with an HMI that enables real-time monitoring of the system status (data received from RTUs) and interaction with the field devices [4]. RTU provides storage of real-time data received from sensors and then transmits data upon request of MTU. PLCs are directly connected with edge devices. They are used to gather data from sensors and manage the actuators.

Manuscript received 17 March 2024; accepted 11 August 2024. Date of publication 22 August 2024; date of current version 6 December 2024. *(Corresponding author: Semih Çakır.)*

Nesibe Yalçın is with the Department of Computer Engineering, Erciyes University, 38030 Kayseri, Türkiye (e-mail: nesibeyalcin@erciyes.edu.tr).

Semih Çakır is with the Department of Computer Technologies, Zonguldak Bülent Ecevit University, 67100 Zonguldak, Türkiye (e-mail: semih.cakir@beun.edu.tr).

Sibel Ünaldı is with the Department of Electrical and Electronics Engineering, Bilecik Şeyh Edebali University, 11210 Bilecik, Türkiye (e-mail: sibel.unaldi@bilecik.edu.tr).

Digital Object Identifier 10.1109/JIOT.2024.3447876

SCADA systems automate the gathering of real-time data, the management of industrial processes, and the observation of distributed industrial machinery based on location. SCADA systems can communicate through wireless or cable. The ability to communicate is crucial for SCADA systems.

SCADA has experienced a significant evolution from an isolated environment to an interconnected network. Despite the advantages of this evolution, SCADA systems have become more vulnerable to cyberattacks (data theft, data manipulation, and data transfer over idle network traffic to different locations). Therefore, a cyberattack on a SCADA system can be disastrous: it may disrupt power, gas, and water supplies, damage important military facilities, and impact significantly public health and safety. As a result, analyzing cyber risks associated with the SCADA system is critically important [5].

The first cyber incident in the history of SCADA systems is thought of as the Siberian Gas Pipeline Explosion in 1982. Critical data was accessed through intrusions into the Salt River Project network in 1994. In 2003, Ohio's Davis Besse nuclear power plant was disabled for several hours due to a slammer worm. The Stuxnet worm detected in 2010, damaged the Iranian nuclear system [6]. The malware, called Triton, was used to take control of a safety shutdown system of Schneider Electric's Triconex Safety Controller in 2017 [7], [8]. This is the first publicly known cyberattack that particularly targeted an ICS/SCADA system [8], [9]. Over the years, the increased connectivity of Internet communication and technological developments have created more avenues for cyberattacks, such as Denial-of-Service (DoS), phishing, hijacking, SQL injection, man-in-the-middle (MiTM), reconnaissance, and password attacks on the SCADA systems.

Security countermeasures, such as firewalls, access control, and virtual private networks, are successfully adopted by SCADA systems [10], [11]. Traditional security approaches are no longer sufficient to detect increasingly sophisticated cyberattacks. Additionally, security countermeasures like authentication and cryptography may disrupt the operation of a time-sensitive SCADA system [12]. Artificial intelligence (AI) technologies are used to provide a dynamic and adaptive defense accelerating attack detection and response [13]. Furthermore, it helps the implementation of cyber security policies, improves the accuracy of security actions that organizations will take, and enables more effective protection of critical infrastructures like SCADA structures.

SCADA systems generally integrate components from different manufacturers and support complex interactions between logical and physical infrastructures [10]. It can be difficult to effectively integrate AI due to their infrastructure and interoperability. The use of standard rules and frameworks will ensure the effective use of new technologies such as AI. Operational continuity and data integrity may be jeopardized by threats to SCADA systems. In a case study presented by [14] for nuclear power plants, a cyberattack that attempts to send fake status data from a field device to the HMI has been examined. The study shows to extend the ability of attack detection models to the SCADA systems [12].

Our study aims to detect various attacks on a SCADA system. Eleven different AI methods, namely, decision tree (DT), quadratic discriminant analysis (QDA), linear discriminant analysis (LDA), *K*-nearest neighbor (KNN), Bernoulli Naïve Bayes (BNB), bagging with KNN (Bag-KNN), bagging with DT (Bag-DT), RF, adaptive boosting (AdaBoost), gradient boosting (GB), and extreme GB (XGB), have been applied to two different SCADA data sets. Hyperparameters of the methods have been tuned and the attack detection efficacy has been analyzed.

SCADA systems automate the gathering of real-time data, the management of industrial processes, and the observation of distributed industrial machinery based on location. SCADA systems can communicate through wireless or cable. The ability to communicate is crucial for SCADA systems. Therefore, a cyberattack on a SCADA system can be disastrous. SCADA systems are vulnerable to data theft, manipulation, and transfer over idle network traffic to different locations. Public health and safety are significantly impacted by the continuous and dependable operation of SCADA systems. Therefore, any vulnerability could jeopardize public health and safety. For instance, a cyber-attacker may breach the SCADA system and disrupt power, gas, and water supplies or damage important military facilities.

In the last few decades, the increased connectivity of Internet communication and technological developments have created more avenues for cyberattacks, such as DoS, phishing, hijacking, SQL injection, MiTM, reconnaissance, and password attacks on the SCADA systems. Our study aims to detect reconnaissance attacks on a SCADA system. It has applied 11 different AI methods, namely, DT, QDA, LDA, KNN, BNB, Bag-KNN, Bag-DT, RF, AdaBoost, GB, and XGB. Hyperparameters of the methods have been tuned and the attack detection efficacy has been analyzed.

The organization of our study: the related works are highlighted in Section II. Section III explains the data set, the used AI methods, and performance metrics. Section IV presents experimental results and performance comparisons with the literature. Section V concludes this study.

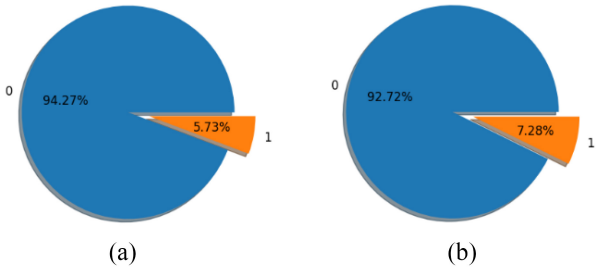
II. Related Works

Network security solutions, such as antivirus programs, firewalls, and intrusion detection systems (IDSs), are also used for ICS/SCADA security but are not robust enough to deal with emerging cyberattacks [15]. A study [16] has focused on Distributed DoS (DDoS) attack classification with the intent of improving low-complexity capability and accuracy rate for low-latency IIoT requirements. In the study, XGB (feature selection) and a hybrid CNN-LSTM method (classification) have been applied to the CICDDoS2019 data set. In [17], the effectiveness of six machine learning (ML) methods has been investigated for the detection of DDoS attacks. Another study [18] has achieved Adversarial ML attacks on an Iterative Dichotomiser 3 and GB model with an average classification accuracy of 87%. Research on SCADA security assessment focuses on areas, such as system simulation [19], [20], [21], penetration testing, vulnerability evaluation [21], [22], detection, and prevention of attacks [23], [24], [25] in SCADA systems. Therefore, AI methods have been widely used to detect, prevent, and mitigate numerous cyberattacks. Teixeira et al. [19] have developed a test environment to investigate

the effects of attacks on SCADA systems and analyze their consequences. The test environment has been exposed to sophisticated cyberattacks and then the attacks have been detected by traditional ML methods. The results have been obtained in offline and online phases. The performance of the methods in the online phase is very close to the offline results. An IDS based on temporal pattern recognition has been proposed and considered a time factor for the detection of anomalies in SCADA systems [20]. The suggested system using artificial neural networks and hidden Markov models is successful in detecting hard-to-detect anomalies that use legitimate commands but have an abnormal time duration. In [21], two laboratory-scale SCADA systems (water storage tank and gas pipeline systems) have been used to collect data and real data sets including various cyberattacks have been obtained. Some ML and deep learning methods, including the support vector machine (SVM), XGB, and RF, have been investigated to detect attacks on these systems. In [25], several ML models have been developed in order to show that the data set is useful for the detection of anomalies and attacks. In another study [26], deep neural network and DT classifier models have been presented for attack detection. To assess the performance of the models, the ten fold cross validation method has been applied to real ICS data sets. Deep-learning-based network IDSs have been also presented for SCADA networks [27], [28]. Realistic SCADA traffic data sets have been used and the well suited method is proposed for network intrusion detection in SCADA systems [28]. To identify the intrusions on a SCADA system, a hybrid classifier (normalized K-Means clustering and recurrent neural networks) has been studied in [29]. For SCADA-based power grids, [30] has developed a solution based on recursive feature elimination and XGB. Also, in another study related to intrusion detection [31], GB has been preferred for feature selection and different ML classifiers have been examined.

In [1], many ML algorithms have been used for vulnerability analysis of IIoT and applied to the WUSTL-IIOT-2018 data set. RF, DT, KNN, SVM, LR, and NB have presented Matthews correlation coefficient (MCC) of 96.81%, 94.26%, 93.44%, 80.84%, 66.20%, and 24.40%, respectively. Evaluating the same algorithms on the WUSTL-IIOT-2021 data set, Eid et al. [32] have achieved MCC values (%) of 99.97, 99.96, 99.89, 99.6, 99.37, and 87.42, respectively. Alani et al. [33] have proposed a deep-learning-based IDS and tested it on the WUSTL-IIOT-2021 data set. The IDS system based on multilayer perceptron (MLP) has performed low false alarm rates and accuracy exceeding 99%. With another deep learning approach using focal loss [34], an accuracy of 98.95% has been achieved for intrusion detection.

In this study, the "WUSTL-IIOT-2018 Data set" and "WUSTL-IIOT-2021 Data set" have been used for SCADA security. The reconnaissance attacks on the control system of a water storage tank have been detected with high performance using RF, logistic regression (LR), KNN, NB, and DT learning methods [19]. The studies on this data set for attack detection in SCADA systems are detailed in Table V.



(a) (b)

Fig. 2. Rate of data corresponds with the normal and abnormal traffic for (a) WUSTL-IIOT-2018 and (b) WUSTL-IIOT-2021.

TABLE I
CHARACTERISTICS OF THE WUSTL-IIOT-2018 DATA SET

Feature	Type	Description
Sport	Integer	Source port number
TotPkts	Integer	Total packets
TotBytes	Integer	Total bytes
SrcPkts	Integer	The count of source packets
DstPkts	Integer	The count of destination packets
SrcBytes	Integer	Source bytes
Target	String	The status of traffic (with or without attack)

III. MATERIAL AND METHODS

A. Data Set Description

In this study, WUSTL-IIOT-2018 [35] and WUSTL-IIOT-2021 [36] public data sets have been used for SCADA systems. These SCADA data sets are cleaned and preprocessed. The WUSTL-IIOT-2018 data set includes records for five reconnaissance attacks: 1) port scanner; 2) address scan; 3) exploit; 4) device identification; and 5) device identification (aggressive mode). There are 7 037 983 instances in this data set, 6 634 581 instances for normal traffic (without any attack), and 403 402 for abnormal traffic (with attacks). The WUSTL-IIOT-2021 data set has records for four attacks: 1) command injection; 2) DoS; 3) reconnaissance; and 4) backdoor/other. There are 1 194 464 instances in the data set: 1 107 448 for normal traffic and 87 016 for abnormal traffic. The rate of the instances corresponding with the status of traffic is presented in Fig. 2. The normal traffic has been represented by "0" and the abnormal traffic by "1."

The SCADA data set includes seven continuous features (see Table I) obtained during normal and attack traffic. Fig. 3 shows the correlation between the features in the data set. The WUSTL-IIOT-2021 data set contains 49 features. In this study, the selected 41 features (including the features given in Table I), such as source load, source rate, total rate, destination loss, and transaction protocol, have been used.

B. Artificial Intelligence Methods

In this study, 11 AI methods in different categories (five of classical, three of bagging, and three of boosting) are selected for detection of the reconnaissance attacks. The classical AI methods used in this study are summarized as follows.

1) KNN [37], a well-known AI method, is memory-based and it does not require any training phase for model

	Sport	TotPkts	TotBytes	SrcPkts	DstPkts	SrcBytes	Target
Sport	1.000000	-0.073211	-0.060883	-0.072275	-0.081843	-0.083695	-0.445907
TotPkts	-0.073211	1.000000	0.861992	0.999973	0.945947	0.999611	-0.006477
TotBytes	-0.060883	0.861992	1.000000	0.862074	0.788766	0.861411	-0.002168
SrcPkts	-0.072275	0.999973	0.862074	1.000000	0.945072	0.999398	-0.004478
DstPkts	-0.081843	0.945947	0.788766	0.945072	1.000000	0.948104	-0.038170
SrcBytes	-0.083695	0.999611	0.861411	0.999398	0.948104	1.000000	-0.004679
Target	-0.445907	-0.006477	-0.002168	-0.004478	-0.038170	-0.004679	1.000000

Fig. 3. Correlation between the features in the WUSTL-IIOT-2018 data set.

building [38]. It labels the output depending on the number of nearest neighbors k for prediction.

2) LDA [39] is applied widely for classification in [40]. It assumes that the classes are separated linearly and maximizes the distance between classes while minimizing the variance within classes [41].
3) QDA is a type of LDA that uses nonlinear data separation [42]. It divides the classes by a hyperplane defined using a quadratic function within an n-dimensional coordinate system [43].
4) DT builds a classification tree based on the features in the data set and their values. The nodes stand the features and the root node representing the dominant feature is always on top. The internal nodes are created depending on the importance order of the features. The leaf nodes represent labels [44]. The classification starts from the root node, proceeds from the branches to other nodes according to the values of the properties, and finally, the leaf nodes are reached. Thus, if-else statements are created [45].
5) NB is based on Bayes' theorem [46] given in (1) and finding the maximum posterior probability $P(c_i|DS)$. In this method, each feature is assumed to be independent of the class. DS is the training data and P(DS), a priori probability of DS, is equal for all classes and does not calculate in NB. c_i denotes the ith class ($i = 1, 2, \ldots, n$ and n is the total number of classes). $P(ci)$ is a priori probability of c_i and $P(DS|c_i)$ is the probability of the NB method given a c_i. BNB is based on Bernoulli distribution [47] and is well suited for binary classification [48], [49], [50]

$$P\ (c_i|DS) = \frac{P(DS|c_i) \cdot P(c_i)}{P(DS)}\ . \tag{1}$$

Ensemble learning is an increasingly popular AI technique. It creates multiple individual classifiers (base learners) and combines the outputs of these learners to produce a better prediction result. Bagging and boosting are the two most popular ensemble methods. Bagging iteratively generates random subsets from the original/main training data set (bootstrapping) [51]. The base learners are trained on subsets (bootstrapped samples) and independently run in parallel. The same learner is used in bagging. Then the outputs of the learners are combined with the arithmetic mean or majority voting and the final prediction is produced. In boosting, base learners are interdependent, each learner runs sequentially. Boosting learns from the errors of the previous predictor (weak learner) to get more generalizable results [52].

In this study, KNN and DT methods are used as base learners in bagging and these methods are named Bag-KNN and Bag-DT, respectively.

1) RF [53], a popular bagging method, generates a large number of DTs based on random training samples and features selected from the data set. The model weights according to the predictions produced by each DT to make a comprehensive prediction. The weighting approach in the classification problem is performed by majority/weighted voting on the prediction results and the obtained result is presented as the final prediction.

Some popular boosting methods presented below are used to obtain more accurate detection results in the study.

1) AdaBoost is a statistical classification algorithm [54]. It builds a stronger learner by combining multiple weak learners. It manipulates training samples to achieve performance improvements. Its performance depends on a probability distribution value on the training data [44]. The weight distributions of misclassified samples are adjusted in subsequent iterations [55]. Each model tries to minimize the previous model's training error.
2) GB includes weak learners and a loss function. It aims to create an additive model to reduce the loss function's residuals iteratively [56]. Misclassifications are penalized considering classification probability [57].
3) XGB [58] is an efficient and flexible method based on GB and DT. It further generalizes the GB method and uses additional techniques, such as extra randomization and automatic feature selection [24]. XGB demonstrates good prediction performance in SCADA networks, despite the differing circumstances [56], [59], [60].

C. Performance Evaluation Metrics

The accuracy (Acc) metric is widely used to evaluate prediction/classification performance, however, using it alone may not be effective for data sets with an imbalanced distribution of the classes. Precision (P), recall (R), F1-score (F1), and false positive (FP) rate (FPR) metrics are commonly applied to evaluate the imbalanced data set. These metrics detailed in Table II are calculated by confusion matrix (CM). CM is also helpful for illustrating the performance of the model and summarizes true and false predictions as a table [61].

D. Methodology

The SCADA data sets have been normalized using the minimum and maximum value of features then each data set has been split into two subsets. AI methods in different categories are used for attack detection and their classification performance is evaluated in terms of various metrics. The framework of our study is illustrated in Fig. 4.

IV. Results and Discussion

Each SCADA data set has been normalized using the MinMaxScaler technique and then partitioned into two subsets: 1) the training data set 70% and 2) the test data set 30%. Table III quantifies this distribution.

All AI models have been built using the Python programming language. Pandas, NumPy, Sklearn, XGBoost,

TABLE II
PERFORMANCE METRICS

Metric	Formula
Acc	$\frac{TP+TN}{TP+TN+FP+FN} \times 100\%$
FPR	$\frac{FP}{TN+FP} \times 100\%$
P	$\frac{TP}{TP+FP}$
R	$\frac{TP}{TP+FN}$
F1	$2 \times \frac{P \times R}{P+R}$

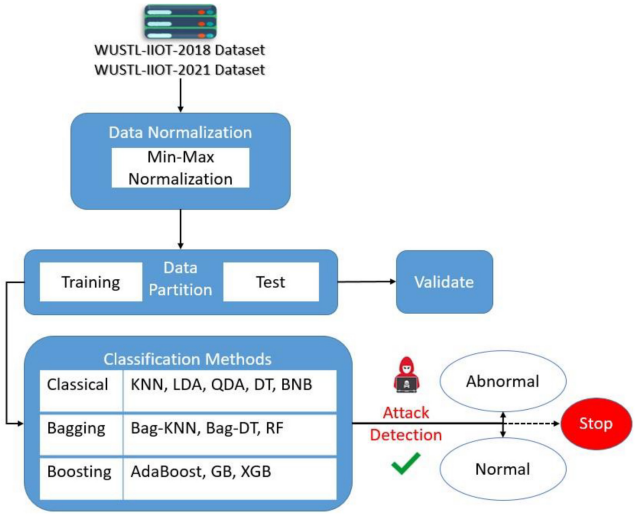


Fig. 4. Flowchart of the study.

Matplotlib, and MLxtend libraries. Google Colab resources are used in the study. Comprehensive experiments have been carried out to obtain AI models with better generalization ability. In KNN, k is determined as 5 using the Elbow method with fivefold cross validation. As a result of intensive experiments, the n_estimators (the max. number of estimators/models) hyperparameter values of the AdaBoost, GB, and XGB models in the training phase are given as 40, 50, and 10, respectively. This parameter is determined as 40 for the training of bagging models. The hyperparameter max_depth (the max. depth of the tree) [62] is 5 for DT, Bag-DT, and RF models and the max_samples (the number of samples used for training of each base learner) is 500 for Bag-KNN and Bag-DT models. The tenfold cross-validation method is also utilized for improving the performance of the models.

The confusion matrices of the AI models are demonstrated for both SCADA data sets in Figs. 5 and 6. As can be seen in Fig. 5, the results of confusion matrices show that AdaBoost achieves high values of true positives (TPs) and true negatives (TNs). In addition to boosting models, DT and RF present the other best results for false negatives. As shown in Fig. 6, KNN and XGB have best performance in detecting abnormal traffic. DT, KNN, Bag-DT, and boosting methods have produced low FPs.

Here, this study explores the best performing AI models. Since the SCADA data sets are imbalanced, P, R, and F1 performance metrics have been also considered. A comparative

TABLE III
STATISTICAL INFORMATION ABOUT THE DATA SETS

Dataset	Target	The number of instances		
		Training dataset	*Test dataset*	*Total*
WUSTL-IIOT-2018	0, normal traffic	4,644,485	1,990,096	6,634,581
	1, abnormal traffic	282,103	121,299	403,402
	All traffic	4,926,588	2,111,395	7,037,983
WUSTL-IIOT-2021	0, normal traffic	775,152	332,296	1,107,448
	1, abnormal traffic	60,972	26,044	87,016
	All traffic	836,124	358,340	1,194,464

analysis of the obtained results is presented in Table IV. From the table, it can be found that all used AI models present good results for both studied data sets. According to the obtained results for the WUSTL-IIOT-2018 data set, the highest detection Acc values are achieved using AdaBoost. AdaBoost, GB, and XGB methods have finally obtained the best prediction with a test Acc of approximately 100%. The lowest results are obtained by BNB with a training Acc about of 96.84% and a test Acc of 96.82%. BNB has the worst performance of misclassification for abnormal traffic. The bagging method that gives the highest results is RF. Bagging methods are not as effective as the boosting methods in both the training and the test phases. DT and RF have achieved a recall of 1.0. AdaBoost, GB, and XGB have shown the best performance with an F1 of 0.9996 and above. Also, the AdaBoost has outperformed all other investigated methods in terms of FPR. For the WUSTL-IIOT-2021 data set, KNN, DT, and boosting models have exhibited better performance. XGB, GB, and DT are the most successful models in terms of FPR.

The performance of the AI models has been compared with FPR. The obtained test FPR values for WUSTL-IIOT-2018 and WUSTL-IIOT-2021 are given in Figs. 7 and 8, respectively. Comparative experimental results depict that the used AI methods achieved high detection rates and low FPRs. KNN, DT, bagging (Bag-DT and RF), and three boosting models have presented lower FPRs. The higher FPRs are obtained by LDA, QDA, BNB, and BAG-KNN models.

Tables V and VI highlight the recent studies on the same SCADA data sets and compare the accuracies of different prediction models. Only the most efficient classifiers in our study are presented in these tables. Performance results given in Table V reveal that the developed AdaBoost model has a high detection Acc of 100% with a very low FPR (0.0020%). XGB has shown the second-best performance with an Acc of 100% and an FPR of 0.0023%. GB, DT, and RF have achieved FPRs of 0.0031, 0.0188, and 0.0212, respectively. The proposed models in this study have presented high detection rates when compared with the results of [63] (without feature selection), [60], [64], and [65] which have a similar data partition. Reference [19] has used a data split rate of 80/20, presented high Acc rates, and achieved a very low FPR.

As shown in Table VI, XGB is proven to be the best among the used models with the highest Acc and the lowest FPR.

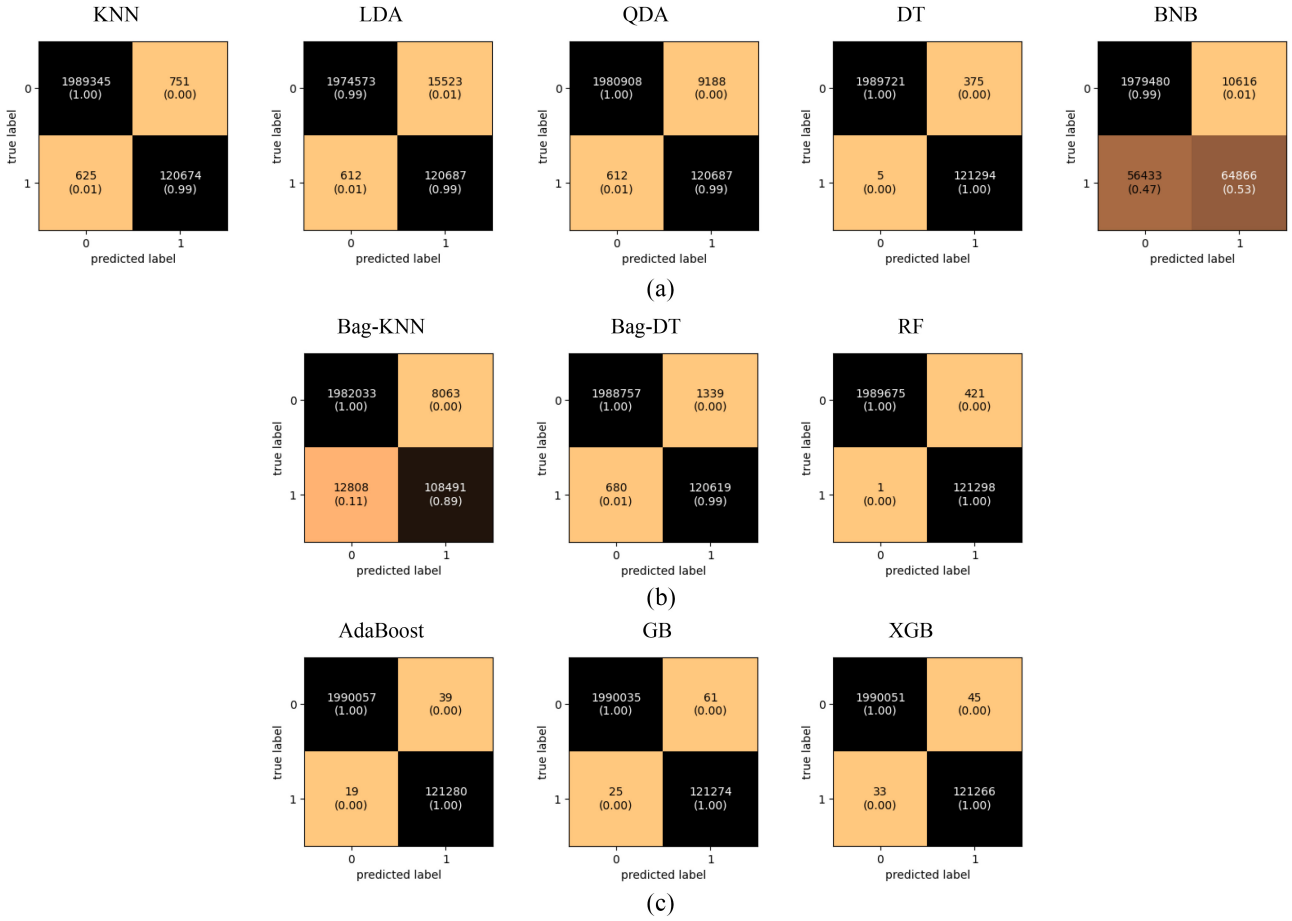


Fig. 5. WUSTL-IIOT-2018—the confusion matrices of (a) classical, (b) bagging, and (c) boosting models.

TABLE IV
PERFORMANCE RESULTS

Dataset	Method		Training Acc (%)	Test Acc (%)	FPR (%)	P	R	F1
WUSTL-IIOT-2018	Classical	KNN	99.9357	99.93	0.0377	0.9938	0.9948	0.9943
		LDA	99.2412	99.24	0.7800	0.8860	0.9950	0.9373
		QDA	99.5427	99.54	0.4617	0.9293	0.9950	0.9610
		DT	99.9821	99.98	0.0188	0.9969	1.0000	0.9984
		BNB	96.8351	96.82	0.5334	0.8594	0.5348	0.6593
	Bagging	KNN	99.4569	99.01	0.4052	0.9308	0.8944	0.9123
		DT	99.8893	99.90	0.0673	0.9890	0.9944	0.9917
		RF	99.9799	99.98	0.0212	0.9965	1.0000	0.9983
	Boosting	AdaBoost	99.9972	100.00	0.0020	0.9997	0.9998	0.9998
		GB	99.9965	100.00	0.0031	0.9995	0.9998	0.9996
		XGB	99.9961	100.00	0.0023	0.9996	0.9997	0.9997
WUSTL-IIOT-2021	Classical	KNN	99.9877	99.99	0.0027	0.9997	0.9990	0.9993
		LDA	99.1212	99.12	0.6702	0.9186	0.9648	0.9411
		QDA	99.5031	99.51	0.5230	0.9374	0.9990	0.9672
		DT	99.9938	99.99	0.0009	0.9999	0.9988	0.9993
		BNB	97.9235	97.94	2.1755	0.7818	0.9948	0.8756
	Bagging	KNN	98.5200	98.37	1.4508	0.8385	0.9609	0.8955
		DT	99.9075	99.91	0.0090	0.9988	0.9887	0.9938
		RF	99.9091	99.99	0.0581	0.9993	0.9989	0.9991
	Boosting	AdaBoost	99.9871	99.98	0.0027	0.9997	0.9980	0.9988
		GB	99.9861	99.99	0.0003	1.0000	0.9982	0.9991
		XGB	99.9933	99.99	0.0000	1.0000	0.9990	0.9995

We have compared the Acc, P, R, F1, and FPR values of all models to identify the best among them. In [66], the data sets with different numbers of features have been applied to the training of several AI methods. RF and DT methods have achieved Acc $\geq$ %99.97 using 41 and 11 features. When using 11 features, the scores obtained with LR and NB are lower

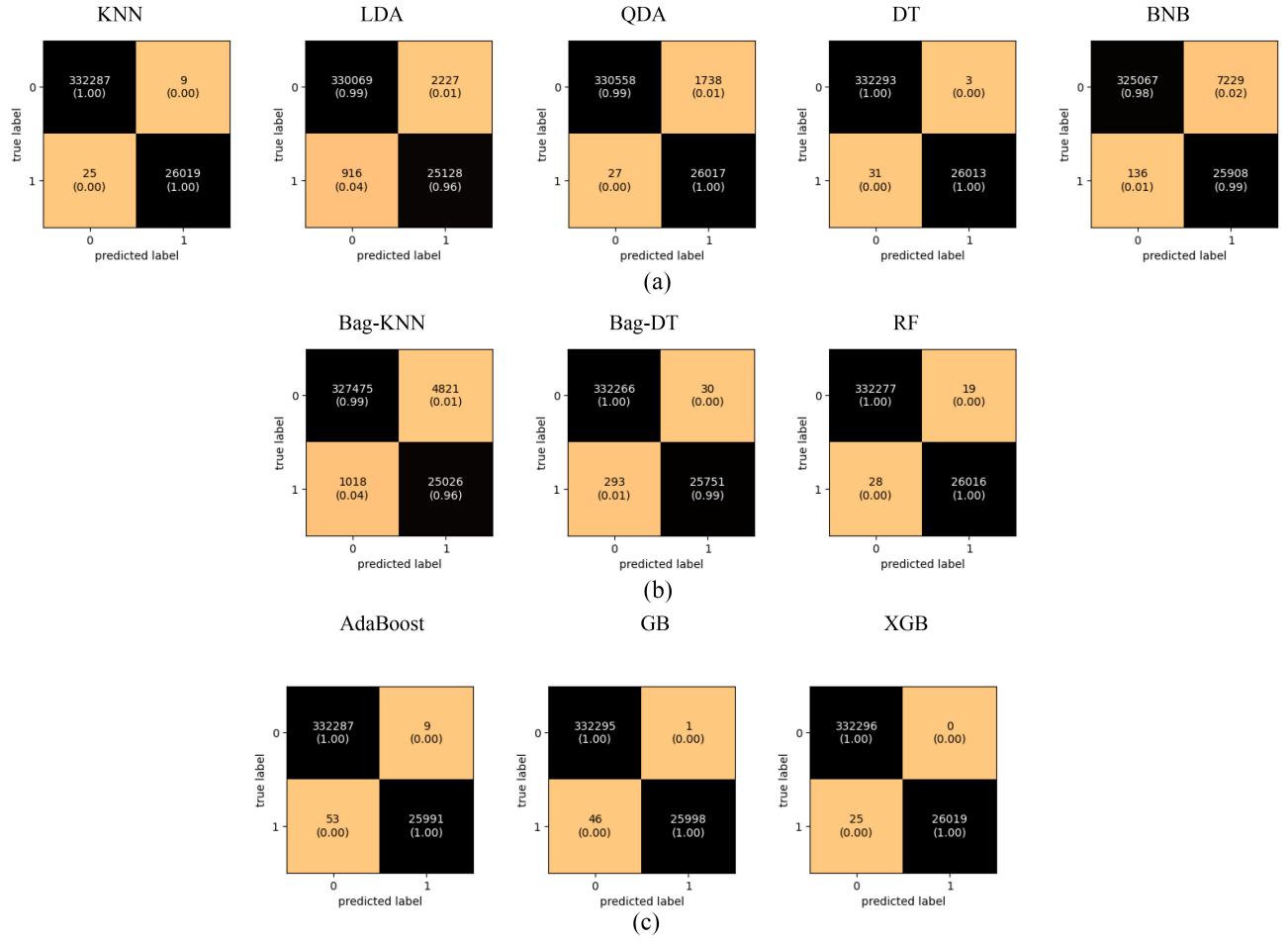


Fig. 6. WUSTL-IIOT-2021—the confusion matrices of (a) classical, (b) bagging, and (c) boosting models.

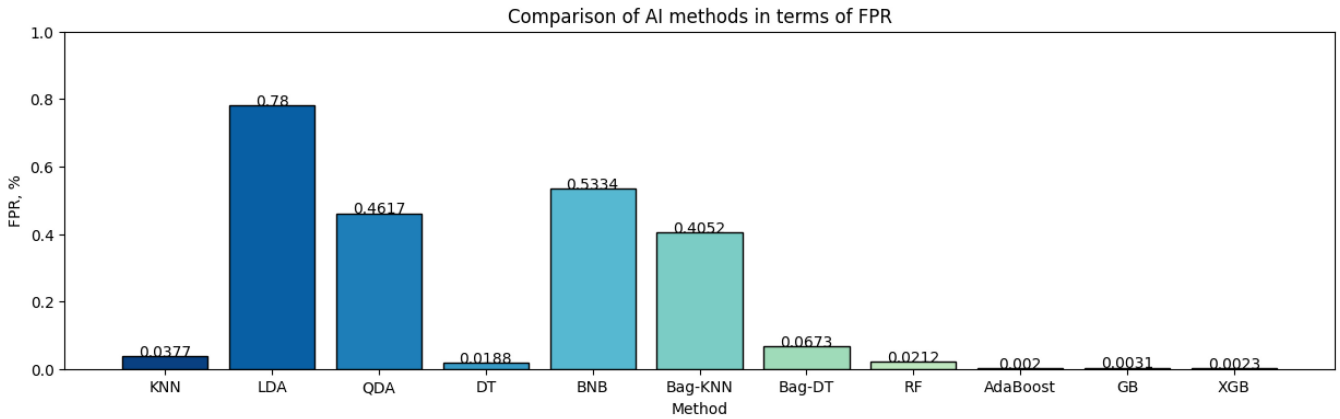


Fig. 7. Comparison of FPR (%) for WUSTL-IIOT-2018.

compared to the use of 41 features. Although the methods proposed by [34] have high Acc rates, they have presented weak performance in terms of P, R, and F1. MLP model in [33] and the RF model in [32] have provided attack detection with Acc equal to 99.94% and 99.97%, respectively. Finally, our study outlines six AI methods that achieve very high performance for cyberattack detection.

V. Conclusion

SCADA systems may serve as the groundwork for making industrial digital transformation. Digital transformation includes both opportunities and challenges for cybersecurity. Cybersecurity approaches, such as detecting potential attacks, protecting data, and mitigating cybersecurity risks, must be integrated into digital transformation strategies.

Our study expands the existing AI-based attack detection research. Various AI methods have been applied to analyze and detect cyberattacks on SCADA systems. It has focused on 11 AI methods in three different categories and provided a comparative study of efficient AI methods.

The study has evaluated the classification performance for two SCADA data sets in terms of Acc, FPR, P, R, and F1. All

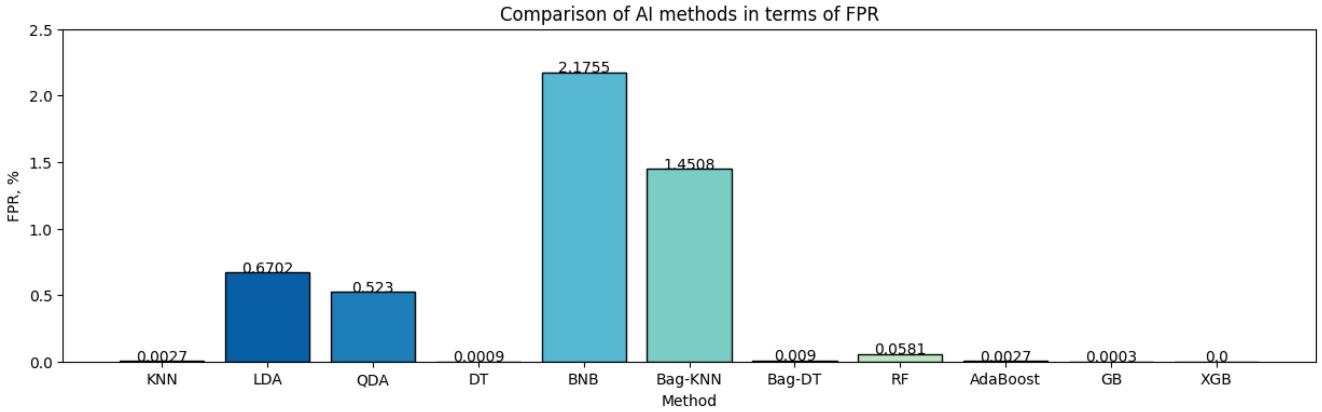


Fig. 8. Comparison of FPR (%) for WUSTL-IIOT-2021.

TABLE V
COMPARISON OF THE STATE-OF-THE-ART TECHNIQUES FOR THE WUSTL-IIOT-2018 DATA SET

Reference	Model	Training/Test Acc (%)	P (%)	R (%)	F1 (%)	FPR (%)
[19]	RF	99.98	-	-	-	0.01
	DT	100				0
	LR	99.86				0.12
	NB	99.51				0.50
	KNN	100				0
[60]	DT	99.98	99.98	99.97	99.97	-
	RF	99.98	99.98	99.97	99.97	
	RNN	98.80	98.51	98.51	98.51	
	AdaBoost	99.98	99.98	99.97	99.97	
	GB	99.98	99.98	99.97	99.97	
	XGB	99.97	99.97	99.96	99.95	
[63]	Modified DT	89.00	-	-	-	-
	RF	87.31				
	AdaBoost	86.47				
	XGB	86.47				
	GB	87.31				
[64]	Proposed CH-DT	99.98	-	-	-	-
	Agnostic Chi-square+RF	99.98				
	Agnostic Chi-square+CNN	93.63				
	Agnostic Chi-square+AdaBoost	99.97				
	Agnostic Chi-square+LSTM	93.06				
	Agnostic Chi-square+XGB	99.98				
	Agnostic Chi-square+GB	99.98				
	Agnostic Chi-square+Bi-LSTM	95.67				
	Agnostic Chi-square+CNN+LSTM	93.00				
[65]	GSFTNN	98.54	98.70	98.42	98.61	-
	ResNet	97.70	98.10	97.54	97.89	
	RNN	94.22	93.64	93.73	94.38	
	LSTM	95.98	96.30	95.78	96.17	
This study	KNN	99.93	99.38	99.48	99.43	0.0377
	DT	99.98	99.69	100	99.84	0.0188
	RF	99.98	99.65	100	99.83	0.0212
	AdaBoost	100	99.97	99.98	99.98	0.0020
	GB	100	99.95	99.98	99.96	0.0031
	XGB	100	99.96	99.97	99.97	0.0023

AI models with high test Acc of about 96.82% and above have been built for both data sets. Furthermore, the results have also confirmed that attack detection can be performed with high Acc using AI methods on different data sets. Overall, results show that the boosting models are the most efficient AI models in the study. AdaBoost model for the WUSTL-IIOT-2018 data set has outperformed Acc of 100%, P of 99.97%, R of 99.98%, F1 of 99.98%, and FPR of 0.002%. XGB model for the WUSTL-IIOT-2021 data set has outperformed Acc of 99.99%, P of 100%, R of 99.90%, F1 of 99.95%, and FPR of 0%. The attack detection results obtained have been analyzed by comparing them with studies using the same data sets. The proposed AI models enable for detection of abnormal traffic vectors and the classification of potential cyberattacks in a real-time IIoT environment.

The integration of different Internet and network technologies with SCADA systems has led to the need to protect the system against cyberattacks. To ensure the safety and productivity of ICSs against cyberattacks, it is essential to design an IDS that is both accurate and sensitive.

TABLE VI
COMPARISON OF THE STATE-OF-THE-ART TECHNIQUES FOR THE WUSTL-IIOT-2021 DATA SET

Reference	Model	Training/Test Acc (%)	P (%)	R (%)	F1 (%)	FPR (%)
[32]	RF	99.97	-	-	-	-
[33]	MLP	99.94	-	-	99.94	0.069
[34]	FNN-focal	98.95	77.22	64.06	68.48	-
	CNN-focal	98.21	88.54	66.51	70.50	
[66]	RF	99.99	99.99	99.99	99.99	-
	LR	79.92	87.24	69.87	71.95	
	DT	99.98	99.98	99.98	99.98	
	NB	95.37	95.83	93.69	94.65	
[66]	RF (with 11 features)	99.98	99.98	99.98	99.98	-
	LR	67.04	83.51	50.08	40.29	-
	DT	99.97	99.98	99.97	99.97	0.01
	NB	78.17	85.41	67.42	68.92	-
This study	KNN	99.99	99.97	99.90	99.93	0.0027
	DT	99.99	99.99	99.88	99.93	0.0009
	RF	99.99	99.93	99.89	99.91	0.0581
	AdaBoost	99.98	99.97	99.80	99.88	0.0027
	GB	99.99	100	99.82	99.91	0.0003
	XGB	99.99	100	99.90	99.95	0.0000

REFERENCES

[1] 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 Things J.*, vol. 6, no. 4, pp. 6822–6834, Aug. 2019.

[2] Y. Wu, H. N. Dai, and H. Tang, "Graph neural networks for anomaly detection in Industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9214–9231, Jun. 2022.

[3] A.G. Finogeev, A. Finogeev, "Information attacks and security in wireless sensor networks of industrial SCADA systems," *J. Ind. Inf. Integr.*, vol. 5, pp. 6–16, Mar. 2017.

[4] S. Cakir, E. Bozacioglu, and N. Bozacioglu, "Endüstriyel nesnelerin İnternetinde IIoT PLC Makinelerinin SCADA Sisteminde Oluşturduğu Zafiyetler ve Siber Saldırılar," in *Proc. 4th Int. Conf. Appl. Eng. Natural Sci.*, Konya, Türkiye, 2022, pp. 1–26.

[5] M. Alanazi, A. Mahmood, and M. J. M. Chowdhury, "SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues," *Comput. Secur. J.*, vol. 125, Feb. 2023, Art. no. 103028.

[6] B. Miller and D. Rowe, "A survey of SCADA and critical infrastructure incidents," in *Proc. 1st Annu. Conf. Res. Inf. Technol.*, 2012, pp. 51–56.

[7] J.-M. Lee and S. Hong, "Keeping host sanity for security of the SCADA systems," *IEEE Access*, vol. 8, pp. 62954–62968, 2020.

[8] D. Silverman, Y. H. Hu, and M. Hoppa, "A study on vulnerabilities and threats to SCADA devices," *J. Colloq. Inf. Syst. Secur. Educ.*, vol. 7, no. 1, pp. 1–8, 2020.

[9] A. Di Pinto, Y. Dragoni, and A. Carcano, "TRITON: The first ICS cyber attack on safety instrument systems," presented at the Black Hat USA, Las Vegas, NV, USA, 2018, pp. 1–26.

[10] Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur. J.*, vol. 56, pp. 1–27, Feb. 2016.

[11] S. Patel, R. Tantalean, P. Ralston, and J. Graham, "Supervisory control and data acquisition remote terminal unit testbed," Intell. Syst. Res. Lab., College Station, TX, USA, Rep. TR-ISRL-05-01, 2005.

[12] R. D. Larkin, J. Lopez, J. W. Butts, and M. R. Grimaila, "Evaluation of Security Solutions in the SCADA Environment," *ACM SIGMIS Database*, vol. 45, no. 1, pp. 38–53, 2014.

[13] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial Intelligence for cybersecurity: Literature review and future research directions," *Inf. Fusion*, vol. 97, Sep. 2023, Art. no. 101804.

[14] R. Campbell and J. Rrushi, "Detecting cyber attacks on nuclear power plants," 'in *Critical Infrastructure Protection II*, (IFIP Advances in Information and Communication Technology), vol. 290. Boston, MA, USA: Springer, 2008, pp. 41–54.

[15] S. Ghosh and S. Sampalli, "A survey of security in SCADA networks: Current issues and future challenges," *IEEE Access*, vol. 7, pp. 135812–135831, 2019.

[16] A. Zainudin, L. A. C. Ahakonye, R. Akter, D. S. Kim, and J. M. Lee, "An efficient hybrid-DNN for DDoS detection and classification in software-defined IIoT networks," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8491–8504, May 2023.

[17] G. Qaiser, S. Chandrasekaran, R. Chai, and J. Zheng, "Classifying DDoS attack in industrial Internet of services using machine learning," in *Proc. 15th Int. Conf. Comput. Autom. Eng.*, 2023, pp. 546–550.

[18] S. Trivedi, T. A. Tran, N. Faruqui, and M. M. Hassan, "An exploratory analysis of effect of adversarial machine learning attack on IoT-enabled industrial control systems," in *Proc. Int. Conf. Smart Comput. Appl.*, Hail, Saudi Arabia, 2023, pp. 1–8.

[19] 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. 8, p. 76, 2018.

[20] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "SCADA cyber security testbed development," in *Proc. 38th North Am. Power Symp.*, 2006, pp. 483–488.

[21] A. Tesfahun and D. L. Bhaskari, "A SCADA testbed for investigating cyber security vulnerabilities in critical infrastructures," *Autom. Control Comput. Sci.*, vol. 50, pp. 54–62, Jan. 2016.

[22] S. Krishnan and M. Wei, "SCADA testbed for vulnerability assessments, penetration testing and incident forensics," in *Proc. 7th Int. Symp. Digit. Forensics Secur.*, Barcelos, Portugal, 2019, pp. 1–6.

[23] M. Kalech, "Cyber-attack detection in SCADA systems using temporal pattern recognition techniques," *Comput. Secur. J.*, vol. 84, pp. 225–238, Jul. 2019.

[24] W. Wang, F. Harrou, B. Bouyeddou, S. M. Senouci, and Y. Sun, "Cyber-attacks detection in industrial systems using artificial intelligence-driven methods," *Int. J. Crit. Infrastruct. Prot.*, vol. 38, Sep. 2022, Art. no. 100542.

[25] A. Dehlaghi-Ghadim, M. H. Moghadam, A. Balador, and H. Hansson, "Anomaly detection dataset for industrial control systems," 2023, *arXiv:2305.09678*.

[26] 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. 83965–83973, 2020.

[27] W. Wang, F. Harrou, B. Bouyeddou, S. M. Senouci, Y. Sun, "A stacked deep learning approach to cyber-attacks detection in industrial systems: Application to the power system and gas pipeline systems," *Clust. Comput.*, vol. 25, pp. 561–578, Feb. 2022.

[28] H. Yang, L. Cheng, and M. C. Chuah, "Deep-learning-based network intrusion detection for SCADA systems," in *Proc. IEEE Conf. Commun. Netw. Security*, Washington, DC, USA, 2019, pp. 1–7.

[29] Y. Justindhas and P. Jeyanthi, "Attack detection and prevention in IoT-SCADA networks using NK-classifier," *Soft Comput.*, vol. 26, pp. 6811–6823, Jul. 2022.

[30] D. Upadhyay, J. Manero, M. Zaman, and S. Sampalli, "Intrusion detection in SCADA based power grids: Recursive feature elimination model with majority vote ensemble algorithm," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2559–2574, Sep. 2021.

[31] D. Upadhyay, J. Manero, M. Zaman, and S. Sampalli, "Gradient boosting feature selection with machine learning classifiers for intrusion detection on power grids," *Trans. Netw. Service Manag.*, vol. 18, no. 1, pp. 1104–1116, Mar. 2021.

[32] A. M. Eid, A. B. Nassif, B. Soudan, and M. N. Injadat, "IIoT network intrusion detection using machine learning," in *Proc. 6th Int. Conf. Intell. Robot. Control Eng. (IRCE)*, Jilin, China, 2023, pp. 196–201.

[33] M. M. Alani, E. Damiani, and U. Ghosh, "DeepIIoT: An explainable deep learning based intrusion detection system for industrial IoT," in *Proc. IEEE 42nd Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, Bologna, Italy, 2022, pp. 169–174.

[34] A. S. Dina, A. B. Siddique, and D. Manivannan, "A deep learning approach for intrusion detection in Internet of Things using focal loss function," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100699.

[35] Jan. 2022, "WUSTL-IIOT-2018 dataset for ICS (SCADA) cybersecurity research," Dataset, Wustl, Accessed: Jan. 2022. https://www.cse.wustl.edu/∼jain/iiot/index.html

[36] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "WUSTL-IIOT-2021 dataset for IIoT cybersecurity research," Washington Univ. St. Louis, MO, USA, Oct. 2021, Access: Jan. 2024. https://www.cse.wustl.edu/∼jain/iiot2/index.html

[37] E. Fix and J. L. Hodges, "Discriminatory analysis. nonparametric discrimination: Consistency properties," USAF School Aviat. Med., Randolph Field, TX, USA, Rep. 4, 1951.

[38] S. Ünaldı and N. Yalçın, "Prediction of air pollution based on machine learning methods: A case study for Başakşehir, İstanbul," *J. Eng. Sci. Res.*, vol. 4, no. 1, pp. 35–44, 2022.

[39] R. A. Fisher, "The use of multiple measurements in taxonomic problems," *Ann. Eugenics*, vol. 7, no. 2, pp. 179–188, 1936.

[40] P. P. Markopoulos, "Linear discriminant analysis with few training data," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, New Orleans, LA, USA, 2017, pp. 4626–4630.

[41] G. A. Giraldi, P. S. Rodrigues, E. C. Kitani, J. R. Sato, and C. E. Thomaz, "Statistical learning approaches for discriminant features selection," *J. Brazilian Comput. Soc.*, vol. 14, pp. 7–22, Jun. 2008.

[42] P. Naveen and B. Diwan, "Relative analysis of ML algorithm QDA, LR and SVM for credit card fraud detection dataset," in *Proc. 4th Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, 2020, pp. 976–981.

[43] J. Bakker, B. Ng, W. K. Seah, and A. Pekar, "Traffic classification with machine learning in a live network," in *Proc. IEEE Symp. Integr. Netw. Service Manag.*, 2019, pp. 488–493.

[44] A. S. Bangari, "A comparative evaluation of machine learning models and EDA through tableau using CICIDS2017 dataset," M.S. thesis, Dept. Comput., Nat. College Ireland, Dublin, Ireland, 2023.

[45] A. Nafees et al., "Forecasting the mechanical properties of plastic concrete employing experimental data using machine learning algorithms: DT, MLPNN, SVM, and RF," *Polymers*, vol. 14, no. 8, p. 1583, 2022.

[46] I. Rish, "An empirical study of the naive Bayes classifier," in *Proc. Workshop Empir. Methods Artif. Intell.*, 2001, pp. 41–46.

[47] L. Segurola-Gil, F. Zola, X. Echeberria-Barrio, and R. Orduna-Urrutia, "Nbcoded: Network attack classifiers based on encoder and naive Bayes model for resource limited devices," in *Proc. Joint Eur. Conf. Mach. Learn. Knowl. Discovery Databases*, 2021, pp. 55–70.

[48] A. McCallum and K. Nigan, "A comparison of event models for naive Bayes text classification," in *Proc. AAAI-98 Workshop Learn. Text Categorization*, 1998, p. 752.

[49] M. Artur, "Review the performance of the bernoulli Naïve Bayes classifier in intrusion detection systems using recursive feature elimination with cross-validated selection of the best number of features," *Procedia Comput. Sci.*, vol. 190, no. 2019, pp. 564–570, 2021.

[50] S. Ismail and H. Reza, "Evaluation of Naïve Bayesian algorithms for cyber-attacks detection in wireless sensor networks," in *Proc. IEEE World AI IoT Congr.*, Seattle, WA, USA, 2022, pp. 283–289.

[51] L. Wen and M. Hughes, "Coastal wetland mapping using ensemble learning algorithms: A comparative study of bagging, boosting and stacking techniques," *Remote Sens.*, vol. 12, no. 10, p. 1683, 2020.

[52] T. T. Akano and C. C. James, "An assessment of ensemble learning approaches and single-based machine learning algorithms for the characterization of undersaturated oil viscosity," *Beni-Suef Univ. J. Basic Appl. Sci.*, vol. 11, p. 149, Dec. 2022.

[53] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, pp. 5–32, Oct. 2001.

[54] Y. Freund and R. E. Schapire, "A decision-theoretic generalization of on-line learning and an application to boosting," in *Proc. Eur. Conf. Comput. Learn. Theory*, Berlin, Germany, 1995, pp. 23–37.

[55] D. Lee and K. Kim, "Improved noise-filtering algorithm for adaboost using the inter-and intra-class variability of imbalanced datasets," *J. Intell. Fuzzy Syst.*, 2022, pp. 5035–5051.

[56] M. Timken, O. Gungor, T. Rosing, and B. Aksanli, "Analysis of machine learning algorithms for cyber attack detection in SCADA power systems," in *Proc. Int. Conf. Smart Commun. Netw.*, İstanbul, Türkiye, 2023, pp. 1–6.

[57] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, "Anomaly detection model based on gradient boosting and decision tree for IoT environments security," *J. Rel. Intell. Environ.*, 2022, pp. 1–12.

[58] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in *Proc. 22nd ACM SIGKDD Int. Conf. Knowl. Discovery Data Min.*, 2016, pp. 785–794.

[59] U. Singh and M. Rizwan, "SCADA system dataset exploration and machine learning based forecast for wind turbines," *Results Eng.*, vol. 16, Dec. 2022, Art. no. 100640.

[60] C. I. Nwakanma, L. A. C. Ahakonye, J. N. Njoku, J. Eze, and D. S. Kim, "Effective Industrial Internet of Things vulnerability detection using machine learning," in *Proc. 5th Inf. Technol. Educ. Develop.*, Abuja, Nigeria, 2022, pp. 1–8.

[61] N. Yalçın and S. Ünaldı, "Symptom based COVID-19 prediction using machine learning and deep learning algorithms," *J. Emerg. Comput. Technol.*, vol. 2, no. 1, pp. 22–29, 2022.

[62] "Scikit-Learn." Accessed: Jun. 23, 2023. [Online]. Available: https://scikit-learn.org/stable/

[63] L. A. C. Ahakonye, C. I. Nwakanma, J. M. Lee, and D. S. Kim, "SCADA intrusion detection scheme exploiting the fusion of modified decision tree and chi-square feature selection," *Internet Things*, vol. 21, Apr. 2023, Art. no. 100676.

[64] L. A. C. Ahakonye, C. I. Nwakanma, J. M. Lee, and D. S. Kim, "Agnostic CH-DT technique for SCADA network high-dimensional data-aware intrusion detection system," *IEEE Internet Things J.*, vol. 10, no. 12, pp. 10344–10356, Jun. 2023.

[65] S. Y. Diaba et al., "SCADA securing system using deep learning to prevent cyber infiltration," *Neural Netw.*, vol. 165, pp. 321–332, Aug. 2023.

[66] M. M. Alani, "An explainable efficient flow-based industrial IoT intrusion detection system," *Comput. Electr. Eng.*, vol. 18, May 2023, Art. no. 108732.

Nesibe Yalçın received the B.S. degree (First Place) and the M.S. degree in computer engineering from the Selçuk University, Konya, Türkiye, in 2009 and 2012, respectively, and the Ph.D. degree from Sakarya University, Serdivan, Türkiye, in 2017.

She is an Assistant Professor of Computer Engineering with Erciyes University, Kayseri, Türkiye. Her research interests include information security, IoT, AI applications, indoor air quality, and mathematical modeling.

Semih Çakır received the B.S. degree (First Place) from Anadolu University, Eskişehir, Türkiye, in 2010, the M.S. degree in computer engineering from Bilecik Şeyh Edebali University, Bilecik, Türkiye, in 2012, and the Ph.D. degree in electrical, electronics, and computer engineering from Düzce University, Düzce, Türkiye, in 2020.

He is an Assistant Professor and the Director of the Karaelmas Cyber Security Application and Research Center, Zonguldak Bülent Ecevit University. His research interest IoT, cyber security, computer networks, and deep learning.

Sibel Ünaldı received the M.Sc. degree from Yıldız Technical University, Istanbul, Türkiye, in 2015, and the Ph.D. degree from Sakarya University, Serdivan, Türkiye, in 2019.

She is an Assistant Professor with the Department of Electrical and Electronics Engineering, Bilecik Şeyh Edebali University, Bilecik, Türkiye. Her research interests include metamaterials, frequency-selective surfaces, reflectarray antennas, RCS reduction of microstrip antennas, AI applications, and IoT.