IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 5 January 2024, accepted 16 February 2024, date of publication 26 February 2024, date of current version 5 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3370436

RESEARCH ARTICLE

Comparison and Investigation of AI-Based Approaches for Cyberattack Detection in Cyber-Physical Systems

MUJAHEED ABDULLAHI[1], (Graduate Student Member, IEEE), HITHAM ALHUSSIAN[1], (Senior Member, IEEE), NORSHAKIRAH AZIZ[1], SAID JADID ABDULKADIR[1], (Senior Member, IEEE), AYED ALWADAIN[2], AMINU AMINU MUAZU[1,3], AND ABUBAKAR BALA[4]

[1]Computer and Information Sciences Department, Faculty of Science and Information Technology, Universiti Teknologi PETRONAS, Seri Iskandar 32610, Malaysia
[2]Computer Science Department, Community College, King Saud University, Riyadh 145111, Saudi Arabia
[3]Computer Sciences Department, Faculty of Natural and Applied Science, Umaru Musa Yar'adua University, Katsina 820102, Nigeria
[4]Interdisciplinary Research Center for Communication Systems and Sensing (IRC-CSS), King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia

Corresponding author: Mujaheed Abdullahi (abdullahi_18001208@utp.edu.my)

This work was supported in part by Universiti Teknologi PETRONAS under Grant YUTP-FRG (015LC0-487); and in part by the Deputyship for Research and Innovation, Ministry of Education, Saudi Arabia, under Project IFKSUOR3–057-2.

ABSTRACT The demand for cyber-physical systems (CPSs) has recently increased in various domains, such as smart grids, intelligent transportation, and critical infrastructure. The massive data networks and communication layers generated make CPSs vulnerable to threats and cyberattacks. To mitigate these threats, artificial intelligence (AI) approaches are employed. However, AI models struggle to keep up with the constantly changing attack landscape. This study investigates the application of extreme gradient boosting (XGBoost) and long-short-term memory (LSTM) AI models for cyberattack detection in a CPS. Accuracy, precision, recall, and the F1-score validate the approach as evaluation metrics. The methods were tested on a gas pipeline industrial control system dataset and other benchmark datasets, such as NetML-2020 and IoT-23, which contain various cyberattacks. The performance of the two methods was found to be better than other models such as support vector machine (SVM) and artificial neural networks (ANN) on several evaluation metrics. Finally, we present recommendations for future research.

INDEX TERMS Artificial intelligence, attack detection, cyberattacks, cyber-physical systems, deep learning, machine learning, LSTM, XGBoost.

I. INTRODUCTION

Cyber-physical systems (CPSs) were introduced in 2006 by Helen Gill at the National Science Foundation (NSF) workshop in the United States (US) [1]. CPSs combine the integration of computational physical systems, including storage, sensors, and actuators for mission-critical tasks, to increase the efficiency of communication technologies. As an emerging defect in CPSs, data protection and data authentication are vulnerable to cyberattack threats. These attacks typically occur because CPSs are connected through wireless connections and the internet to transmit their data, making it easy for them to attack during regular network communication [2]. For example, in recent decades, there have been numerous threats to significant cyberattack issues within the CPS environment [3]. Data privacy concerns in network management and as sources for facility analysis of CPS security monitoring [4].

Figure 1 illustrates the holistic cyber-physical framework, where CPS applications are executed, including sensors and actuator networks. Additionally, CPS's framework encompasses three fundamental components: physical processes, interfaces, and cyber systems.

The term ''physical processes'' pertains to the observable and measurable natural phenomena that are subject to monitoring or regulation, while ''cyber systems'' pertains to a class

The associate editor coordinating the review of this manuscript and approving it for publication was Genoveffa Tortora.

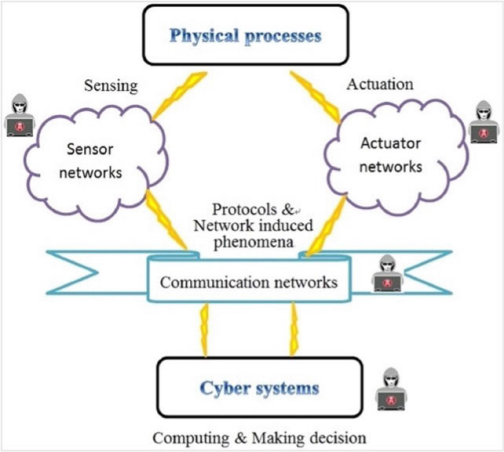

FIGURE 1. Holistic framework for cyber-physical systems [6].

of embedded devices that can process information. The physical world is connected to cyber systems through intermediate components, including sensors, actuators, and communication networks. Sensors and actuators convert energy into electricity and vice versa [5].

Due to the rapid growth of CPSs in many areas, such as smart buildings, smart grids, intelligent transportation, and critical infrastructure, huge amounts of data are being generated. This makes the system vulnerable to cyberattacks. With the increased demand for technology leading to the Fourth Industrial Revolution (IR 4.0), CPS sensors are often used for performing real-time analysis, monitoring, and forecasting system malfunctions. These data have an impact on the entire manufacturing system if they are contaminated or compromised because of cyberattacks, giving false predictions and insights and ultimately leading to catastrophic failures. The physical layer of CPSs is vulnerable to attacks involving the injection of false data into sensors and actuators, which can compromise the integrity of complex network systems [7]. Several cyberattacks have occurred in CPSs. For example, the Ukrainian power plant in 2016 and the Stuxnet worm, which targeted nuclear power plants, have been attributed to such methods [8].

Machine learning (ML) and deep learning (DL) techniques are subsections of artificial intelligence (AI) that are currently used for the detection of cyberattacks, such as threat detection, malware clarification, and intrusion detection. Extensive research has been conducted on the use of ML learning algorithms to enhance cyberattack issues in the CPS environment [9], [10]. The ML method can also be applied to detect and identify anomalies [11]. For example, XGBoost classifiers are used for intrusion detection in input datasets that contain normal and anomalous instances [12]. Gad et al. [13] proposed an XGBoost technique to detect and reduce malicious activity in IoT. Furthermore, a DL model based on Long short-term memory (LSTM) memories (LSTM) was used to detect cyberattacks in CPSs [14].

Moreover, AI and ML have significantly transformed the field of cybersecurity, especially CPS. They offer exceptional capabilities in detecting and minimizing cyberattacks that disrupt the interconnected infrastructure of vital systems, such as power grids, transportation networks, and industrial control systems [15]. However, traditional signature-based detection techniques frequently find it difficult to keep up with cybercriminals' increasingly complex techniques using advanced technology. In contrast, AI and ML algorithms can gain experience and continue to improve at identifying new threats. The ability to adapt is crucial for protecting CPS because it remains constantly changing and vulnerable to emerging threats. AI and ML algorithms can process and interpret these data with incredible speed and accuracy, allowing them to detect anomalies and suspicious patterns that may indicate a cyberattack. Furthermore, these intelligent models provide excellent performance in terms of their ability to analyze, detect, and adapt to new threats and evolving attack methods in real-time.

This study presents an approach that demonstrates greater efficiency in cyberattack detection for CPSs, and addresses cybersecurity concerns. The integration of LSTM and XGBoost has improved the detection of cyberattacks in gas pipeline systems. The temporal feature extraction capabilities of LSTM, combined with the robustness of XGBoost, improve the detection and classification of various cyberattacks. The model's effectiveness has been extended beyond the gas pipeline by including other domains, such as IoT datasets containing various cyberattacks. In addition, this study investigates the risks and threads associated with CPSs, as well as how to overcome them using potential AI approaches. This study's specific contributions are as follows:

a) We employed the XGBoost and LSTM models to detect sophisticated cyberattacks in CPS by examining temporal and context relations in the data.
b) The two models were tested on a gas pipeline system based on industrial control system (ICS) datasets and other available benchmark datasets, such as NetML-2020 and IoT-23, which contain various cyberattacks.

A. RISKS AND THREATS

The emergence of CPSs presents new challenges against cyberattack risks and threats. Ensuring data protection against security risks and cyberattacks is one of the most complex issues within the CPS environment [16], [17]. Such cyberattacks include denial of service (DoS), Trojans, worms, and buffer overflow. When these attacks succeed, they affect the CPS through breaches of confidentiality, privacy, integrity, availability, and safety, which can lead to failure. However, if the attacker had evaluated the encryption key, he could have illegally obtained access to the monitoring center and destroyed normal system operations.

Moreover, CPSs comprise both physical and cyber components through a range of integrated components. The ML and quantitative base risk assessment approaches play vital roles in the analysis and identification of threats to the CPS environment. These security-risk cybersecurity threads can

compromise security and privacy. An attacker's malicious activities can spread and could lead to failure, power failure, and security threats when using these devices [18]. As the number of devices increases, major problems continue to develop in real-world scenarios [19]. These problems include connectivity, security, trust, interoperability, scale, and the environment.

The remaining section of this paper is organized as follows. Section II provides a literature review based on related work on cyberattack detection techniques in CPSs using ML approaches. Section III presents the study methodology, which includes the data collection procedure, the proposed comparison method, and evaluation criteria. Section IV presents the implementation and result analysis, including the importance of their characteristics and comparison performance analysis. Section V provides an AI-based detection roadmap. Section VI provides a potential countermeasure. Finally, we present our conclusions and future directions in Section VII.

II. LITERATURE REVIEW

In this section, related studies are discussed. Various approaches have been proposed to solve cyberattacks using the ML method. For example, Almiani et al. [20] presented a fog system security and a fully automated intrusion detection system for cyberattacks by proposing a model using multilayer neural network designs that are very close to end users. To better understand the problem, the model was evaluated using typical varieties, Mathew's correlation, and Cohen's kappa coefficient. Mall et al. [21] demonstrated various ML models that can be used to identify distributed denial-of-service (DDoS) attacks in a software-defined CPS framework. This was achieved through the implementation of a flexible and scalable software-defined network (SDN) design. Bitirgen and Filik [22] proposed a new approach to improve the functionality of convolutional neural networks for long and short-term memory (CNN-LSTM) to detect fault detection, isolation, and accommodation (FDIA) in smart grid (SG) systems. Thapa et al. [23] conducted a comparative analysis of various ML and DL models using Coburg intrusion detection datasets (CIDDSs).

In a major advance in 2022, [24] conducted a comprehensive survey on the use of DL for detecting cyber-physical system attacks, which represents a significant advancement in cybersecurity. The authors employed a modified methodology that encompasses CPS scenario analysis, identification of cyber-attacks, formulation of ML problems, customization of DL models, acquisition of training data, and performance evaluation. The reviewed studies demonstrate significant promise in identifying cyber-attacks on CPSs using DL modules. In [25], the authors developed an innovative method called PRO-DLBIDCPS, which is a poor and rich optimization with DL for blockchain-enabled intrusion detection in a CPS environment. The PRO-DLBIDCPS technique introduces an adaptive harmony search algorithm (AHSA) for selecting feature subsets. The CPS-GUARD system was developed using an innovative intrusion detection method that relies on a single semi-supervised autoencoder. In addition, a technique has been implemented to establish a threshold that distinguishes normal operations from attacks. The technique is designed to be aware of outliers, i.e., it uses outlier detection to address the inherent imperfections present in the training data [26]. Several authors have investigated the impact of the DL model on cyberattack detection in CPS. For instance, [27] conducted a comparative analysis of various state-of-the-art deep learning techniques for the classification and categorization of malicious applications. The proposed method involves using an ensemble dynamic weighted voting model to accurately detect and categorize a diverse range of malicious applications using the CCCS-CIC and Mal-2020 datasets. A DL approach for identifying and analyzing time delay attacks (TDA) has been introduced. This approach involves the development of a hierarchical long short-term memory model. The model is designed to handle real-time data streams from relevant CPS sensors with an understanding of any embedded signals that may indicate an attack [28].

Moreover, the authors of [29], [30], and [31] explained the potential of ML techniques to detect various attacks on CPS, including smart grids, power grids, and cyber-physical power systems. Lin et al. [29] used deep reinforcement learning (DRL), propose a model for false data injection attacks and counter-detection techniques. Jahangir et al. [30] proposed a novel approach for the identification and localization of high-resolution. This method uses a multi-output network that includes a two-dimensional neural network classifier and a reconstruction decoder. Presekal et al. [31] introduced a novel technique for identifying anomalies in time-series data using classification. This approach uses a hybrid DL model that integrates graph convolutional long and short-term memory (GC-LSTM) with a deep convolutional network. Almuqren et al. [32] developed a technique known as the Explainable Artificial Intelligence Enabled Intrusion Detection Technique for Secure Cyber-Physical Systems (XAIID-SCPS). Furthermore, the XAIID-SCPS technique incorporates the XAI methodology known as local interpretable model-agnostic explanation (LIME) to enhance the comprehension and interpretability of the black-box algorithm, thereby facilitating accurate intrusion classification.

More recent evidence by Tertytchny et al. [33] demonstrates that CPS classifies network abnormalities as faults and attaches them to the IoT using ML. The authors established a formal definition of the issues arising from component failures and network attacks, considering the impact of communication behavior. They demonstrated the correlation between these two abnormal sources and presented a framework based on ML. A concept paper on the adaptation of ML and blockchain techniques in CPS to address security issues related to cyberattacks was presented [34]. Sowmya and Mary Anita [35] presented a comprehensive taxonomy of the extant literature on ML, DL, and ensemble learning. The analysis includes 72 research papers and

TABLE 1. Summary of the findings of the related studies.

Ref.	Model Used	Contribution	Challenges/Gaps
[20]	DRNN	The main contribution of this study is the development of an innovative intrusion detection system for Fog security, that uses a multi-layered recurrent neural network-based approach.	The study's limitation is that it was evaluated using a single dataset; further study is required to evaluate its performance on other datasets.
[21]	DL	This study contributes to the field of DDoS attack detection by introducing a scalable and adaptable SDN-based framework using DL to achieve a high level of accuracy in categorizing binary and multiclass data across unknown network traffic.	This study is limited to the use of two recent security datasets; additional investigation is required to evaluate the proposed architecture's performance in a wider range of attack scenarios.
[22]	CNN-LSTM	This study contribution proposes a novel approach for identifying false data injection attacks (FDIA) in smart grid (SG) systems. In addition, the model has been optimized by applying particle swarm optimization (PSO).	This limitation is that it only detects FDIA using PMU measurements and does not consider other types of data that could be used to improve detection accuracy.
[23]	ML, DL	This study presents a novel IDS that uses various ML and DL models. The proposed IDS demonstrates high accuracy, a minimal rate of false alarms, and a low cost for training on the CIDDS dataset.	This study is limited by its use of both the KDD99 and NSL-KDD datasets, which do not adequately represent recent attacks and suffer from network biases.
[29]	DRL	The study's contributions encompass a model for conducting false data injection attacks, a detection method based on deep reinforcement learning, and an approach to enhance efficiency in addressing sparse reward problems.	The study's limitations include the assumption of unrestricted attack resources, complete topology information, and the potential for future advancements in the detection method's perception capabilities.
[30]	2DR-CNN	The main contribution of this study is the development of an innovative technique called 2DR-CNN, which can accurately detect and identify dynamic load-altering attacks (D-LAAs) with high resolution.	The study's testing on IEEE 14- and 39-bus systems is its main drawback.
[33]	ML	The framework developed in this study uses machine learning to distinguish between network attacks and component failures in Energy Aware Smart Home (EASH) systems.	The focus of this research is limited to a specific EASH system; therefore, it's findings may not apply to other CPSs. The analysis also indicates that the classification results can be enhanced by including or excluding features from the descriptive datasets.
This work	ML, DL	This study compares and investigates AI methods that use XGBoost and LSTM for cyberattack detection in a CPS environment. In addition, we investigate and analyze the proposed approach using other available benchmark datasets, such as NetML-2020 and IoT-23, which contain various cyberattacks. However, this work has some similarities to prior studies. For example, [20], [21], and [23] use various ML techniques for IDS in Fog systems and SDN-based framework.	This study is limited to the use of one ICS gas pipeline security dataset. Future research could involve exploring other ensemble methods or optimizing hyperparameters to improve the model's performance.

considers detection-related factors such as the algorithm and performance metrics. Finally, a comprehensive review was conducted, which involved categorization, classification, and examination of the existing literature on artificial intelligence (AI) techniques used to identify cyberattacks in the Internet of Things (IoT) settings [36].

This study compares and investigates existing DL and ML algorithms for cyberattack detection in CPSs. Based on our knowledge, this study is different from other studies because we focused on critical industrial control systems, i.e., gas pipeline cyberattack detection using LSTM and XGBoost models. However, our work added value by understanding the various AI models from empirical studies to overcome current trends in cybersecurity attacks in CPSs and IoT environments. We also analyzed and validated the models using the available benchmark datasets that containing cyberattacks. Table 1 summarizes the findings based on the related studies.

In addition, our comparable contribution attempts to address key limitations of existing approaches. For example, [20] evaluated there DRNN model for intrusion detection systems using a single dataset. The authors in [23] use both the KDD99 and NSL-KDD datasets, which appear to have network biases. In addition, [21] limits the capabilities of their proposed DL model to a single DDoS attack in the SDN-based domain. To overcome these limitations, our study uses a variety of datasets from various domains, including gas pipelines, NetML-2020, and IoT-23, which contain a variety of cyberattack scenarios. We also investigate the capability of combining LSTM and XGBoost to detect cyberattack scenarios in industrial control systems.

III. MATERIALS AND METHODS

This section provides details of the study methodology, implementation, and design of the proposed methods for intrusion detection systems in CPS. The proposed framework combines several independent processes and comprises data collection and observation. During this process, datasets were collected and observed in detail based on the type of data. The entire dataset was processed, consisting of cleaning the data, visualizing the data using vectorization steps, and feature engineering. The training of the dataset used ML. An optimization method was used to create the final model. The study will use the XGBoost classification, which is based on

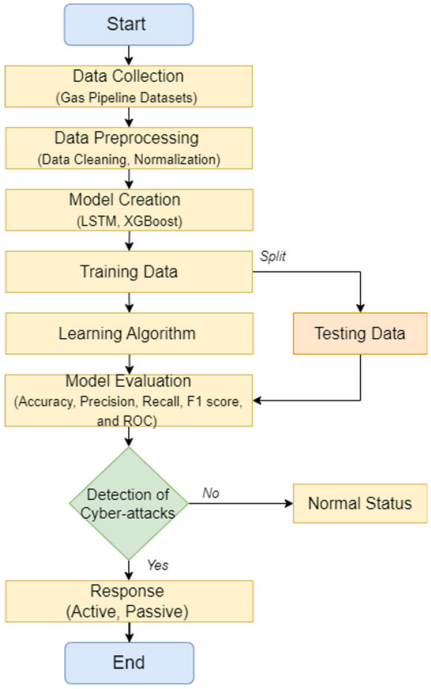

FIGURE 2. Overall methodology flowchart.

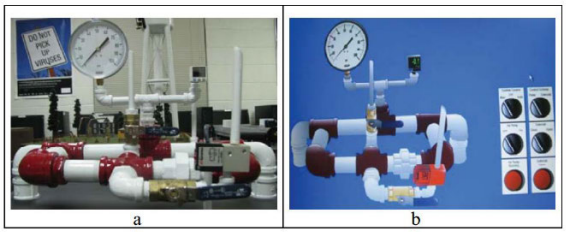

FIGURE 3. The gas pipeline system is shown on the left (a), and the right HMI is shown on the right (b) [37].

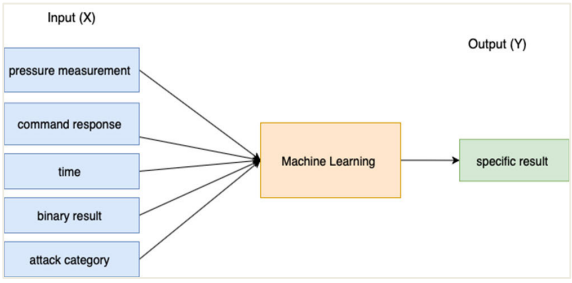

FIGURE 4. Machine learning data flow for the input and output of selected features.

the decision tree algorithm (DT), and the LSTM, which is based on the recurrent neural network (RNN) and uses the conventional gradient descent technique.

Figure 2 presents the research methodology flowchart. First, data collection from a real-world gas pipeline system contains various cyberattacks. Followed by data preprocessing, which involves data cleaning and normalization. Model creation consists of the LSTM and XGBoost algorithms. The sampling data were split into training and testing, followed by the learning algorithms. The model evaluation would be based on the ACC. After evaluation, the model would predict if there were cyberattacks or if it was in normal status. Cyberattacks are predicted based on anomalous activities in the input data. Finally, anomalous activity can be classified as active or passive.

A. DATASETS EXPLANATION

The datasets were obtained from a gas pipeline system based on an industrial control system (ICS) at Mississippi State University. The dataset comprised various components, including sensors equipped with actuators from a gas pipeline. The dataset contained seven different categories of cyberattacks [37]. There are two actuator components for gas pipelines in conjunction with a pressure sensor, which are components of the SCADA system. Actuators, comprising solenoids and pumps, are used to regulate the physical processes of the system, thereby ensuring that the pressure set by the SCADA is maintained. The modes of the gas pipeline system were classified into three distinct groups: manual, automatic, and off. The components of a communication network refer to the protocols used in a serial Modbus remote terminal unit (RTU). Each packet transmitted through this system comprises a header and a payload. The components responsible for supervisory control encompass the master terminal unit (MTU) and the human-machine interface (HMI). The MTU is configured in various setups where each subordinate device functions as a RTU that receives directives from the MTU, and subsequently, the RTUs react to the MTU's commands.

In addition, the MTU was linked to the HMI to provide human operators with a means to oversee the system and the supervisory controls. However, the fault has been simulated because of the huge network traffic and imbalanced data in the SCADA system, where system commands and responses are being manipulated. Figure 3 shows the gas pipeline system and HMI.

Figure 4 shows the comprised input datasets, which consist of the five most important features that describe the possibility of cyberattacks. Hence, the XGBoost model classifies all numeric input features as simple binary classification problems. The LSTM model learns from a function consisting of a sequence of past observations as input (x) to an output observation (y). Furthermore, one feature output indicates whether a specific attack has occurred after training and testing.

Table 2 shows that datasets consist of seven separate types of attacks, comprising both normal and attack samples, which have been identified as follows:

The attack values range from 0 to 7, which is accomplished by establishing a parameterization. This range was created to provide updates on all attack possibilities that can be executed using a specific parameter. The dataset is a comma-separated value (CSV) text file consisting of 19 features of network field states provided by one packet delivered by the MTU or RTU as shown in Table 3. Each dataset for MTUs or RTUs includes information on network traffic and payload. The

TABLE 2. Seven types of categories from the datasets.

Attack Type	Attack abbreviation	Threat type
Naïve Malicious Response Injection	NMRI (1)	Modification
Complex Malicious Response Injection	CMRI (2)	Modification
Malicious State Command Injection	MSCI (3)	Modification
Malicious Parameter Command Injection	MPCI (4)	Modification
Malicious Function Code Injection	MFCI (5)	Modification
Denial of Service	DoS (6)	Interruption
Reconnaissance	Recon (7)	Interception

TABLE 3. Dataset features.

S/N	Feature name	Description
1	address	Station address of the MODBUS slave device.
2	function	MODBUS function code.
3	length	The length of the MODBUS packet.
4	setpoint	Pressure set point when the system is in automatic system mode.
5	Gain	PID gain.
6	reset rate	PID reset rate.
7	deadband	PID dead band.
8	cycle time	PID cycle time.
9	Rate	PID rate.
10	system mode	The system mode is automatic (2), and manual (1).
11	control scheme	The control scheme is either pump (0) or solenoid (1).
12	pump	Pump control; on (1) or off (0).
13	solenoid	Relief valve control; opened (1) or closed (0).
14	pressure measurement	Pressure measurement.
15	command response	Command (1) or response (0).
16	time	Timestamp.
17	binary result	Binary class; attack (1) or normal (0).
18	attack category	Category of attack (0-7).
19	specific result	Specific attack (0-35)

payload contains crucial data related to the state, parameters, and settings of the gas pipeline. This information is essential for comprehending the system's behavior and identifying any deviations from normal operation.

B. ALGORITHM THEORETICAL CONSIDERATIONS

1) LONG SHORT-TERM MEMORY (LSTM)

LSTM is based on a recurrent neural network (RNN) and aims to capture sequence-dependent behavior or model time in a range of applications, such as IDS for detecting intrusions in network traffic. The process involved in this study involved providing the output of the neural network layer at a specific time point T as input to the subsequent layer at time T + 1. The LSTM model is an extension of the RNN architecture. It incorporates memory components that facilitate the transmission of acquired knowledge from a given time step T to subsequent time steps, including T + 1, T + 2, and T + 3. Moreover, an important attribute of the LSTM model is its ability to selectively discard irrelevant components of the prior state while simultaneously selecting the updated state and producing pertinent components of the state that

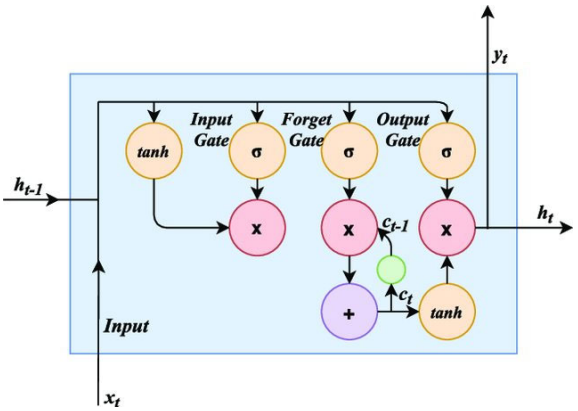

FIGURE 5. Illustration of the LSTM cell architecture.

are pertinent to future predictions. The LSTM cell shown in Figure 5 indicates the use of input features xt, which correspond to input data x at a given time t. The input gate is responsible for regulating the flow of input data into the cell.

In addition, the LSTM cell consists of three primary components: the input gate, forget gate, and output gate. They are responsible for regulating the flow of information within the cell.

a) Input gate: The input gate determines which parts of the current input (X) will be incorporated into the cell state (Ct). It also serves as a filter, that identifies valuable elements of the new memory vector.
b) Forget gate: The forget gate regulates the extent to which the previous cell state (Ct-1) is forgotten. Also, determine the relevant components of the cell state by considering the previous hidden state and the new input data.
c) Output gate: The output gate determines the amount of the LSTM cell's state (Ct) that is output. It also determines the LSTM network's final hidden state.

The i_t define the input/output of gate activation, where f_t determine forget gate activation, while o_t finds control flow to output gate activation. The c_t determines cell state and h_{t-1} define the hidden state, while σ sigmoid acts as an activation function. The components of the LSTM equation cell functions are indicated below.

$$i_t = \sigma\left(U_i x_t + W_i h_{t-1} + b_i\right) \tag{1}$$

where i_t is the function that determines which information from the current input should be stored in the cell state, h_{t-1} represent the previous hidden state, x_t denotes the current input, and *Wi,* and bi represent the weight and bias for the input gate, respectively.

$$f_t = \sigma\left(U_f x_t + W_f h_{t-1} + b_f\right) \tag{2}$$

where ft decides what information in the cell state should be forgotten or retained, h_{t-1} represent the previous hidden state, x_t denotes the current input, and *Wf*, bf represent weight and bias for the forget gate, respectively.

$$O_t = \sigma\left(U_a x_t + W_o h_{t-1} + b_o\right) \tag{3}$$

TABLE 4. Summary of Important Symbols/Notations.

Symbol/Notation	Description
x_t	Input at the time step t
h_{t-1}	Hidden state at the time step $t-1$
h_t	Hidden state at the time step t
C_{t-1}	Cell state at the time step $t-1$
C_t	Cell state at the time step t
i_t	Input gate
f_t	Forget gate
O_t	Output gate
W_i, W_f, W_C, W_o	Weight matrices for the gates
b_i, b_f, b_C, b_o	Bias terms for gates
σ	Sigmoid activation function
$tanh$	Hyperbolic tangent activation function
Obj(θ)	Objective function
Ω	Regularization term
L	Loss function
$f(x)$	Complexity function of the model
W	Vector

Meanwhile, for the output gate, Ot determines the output based on the current input and the updated cell state, h_{t-1} denotes the previous hidden state, x_t denotes the current input, *Wo, bo* represent the weight and bias for the output gate, respectively.

$$g_t = \sigma\left(U_g x_t + W_g h_{t-1} + b_g\right) \tag{4}$$

$$C_t = g_t i_t + f_t C_{t-} \tag{5}$$

Here, after *gt* the *Ct updates* the cell state by combining the candidate cell state update and the previous cell state *Ct-1,* using the input it and forget gates *f t,* respectively.

$$h_t = O_t tanh\,(c_t) \tag{6}$$

ht function produces the new hidden state based on the updated cell state and the output gate, *ht* represents gate output, and *ct*denotes the cell state.

The LSTM architecture has the capability to detect cyber-attacks by learning to identify patterns in network traffic that are indicative of attacks. To control how the LSTM network learns these patterns, use the input gate, forget gate, and output gate. For example, the input gate can be used to direct the network's attention to specific aspects of network traffic, such as the IP addresses of the source and destination hosts, packet size and frequency, and protocol type. The forget gate can be used to prevent the network from forgetting previously learned important patterns. The output gate can be used to regulate how much of the network's output is used to forecast the possibility of a cyber-attack.

2) EXTREME GRADIENT BOOSTING (XGBOOST)

XGBoost is rooted in the concept of gradient boosting as introduced in Friedman's "A Gradient Boosting Machine" for function approximation [26]. XGBoost is a supervised learning algorithm used to solve problems by treating data with multiple features xi to predict the value of the target variable yi. The model's objective functions are training loss and regulation with *yi* by a various of tasks such as ranking, classification, and regression. The training task is to find the parameter θ that best fits the training of data *xi* and labels *yi*.

TABLE 5. XGBoost classifier parameters.

Model	Parameters	Tunned parameters
XGBoost	{booster='gbtree' 'max_depth': 4, 'alpha': 10, 'learning_rate': 1.0, 'n_estimators':100}	{colsample_bylevel=1, learning_rate=1.0, max_depth=4, min_child_weight=1, missing=None, n_estimators=100, n_jobs=1, subsample=1, verbosity=1, booster='gbtree'}

Table 4 summarizes the symbols and notations used in this study. Table 5 provides the XGBoost classifier parameters. The silent characteristics of the objective function consist of XGBoost classifier parameters.

The silent characteristics of the objective function consist of two parts: training loss and a regularization term.

$$\text{obj}(\theta) = \text{L}(\theta) + \Omega(\theta) \tag{7}$$

where L is the training loss function and Ω is the regularization term. Training loss measures how the predictive model respects the training data, where a common choice of L is the squared error.

$$\boldsymbol{L}(\theta) = \sum_i (\boldsymbol{yi} - \hat{\boldsymbol{y}}\boldsymbol{i})^2 \tag{8}$$

The chosen XGBoost model is based on DT ensembles and consists of a classification and regression tree (CART). Tree-boosting training is based on supervised learning models that satisfy the objectives.

$$\boldsymbol{obj} = \sum_{i=1}^{n} \boldsymbol{l} \tag{9}$$

The complexity of the model is important in the regularization term, where the complexity of the tree, $\Omega(f)$, is also defined as $f(x)$.

$$f_t(x) = w_{q(x),w}, \text{R}^{\text{T}}, q : \text{R}^{\text{d}} \rightarrow \{1, 2, \cdots, T\} \tag{10}$$

where W is the vector of scores for the leaves, q is the function assigned to each data point on the corresponding leaf, and T is the level number. The XGBoost complexity is defined as

$$\Omega(f) = \gamma T + \frac{1}{2}\lambda \sum_{j=1}^{T} \boldsymbol{w}_j^2 \tag{11}$$

Figure 6 shows the structure of the XGBoost model, which involves the iterative process of fitting decision trees to the data and updating the model parameters using the loss function gradient. This process is repeated until convergence, providing a model that is both highly accurate and scalable. Moreover, XGBoost has demonstrated its efficacy as a machine learning algorithm in diverse cyber security domains, encompassing intrusion detection, malware detection, and phishing detection.

C. EVALUATION CRITERIA

The metric used to evaluate the model's performance is ACC. The evaluation of classification models involves the use of the Model ACC metric, which assesses a limited portion

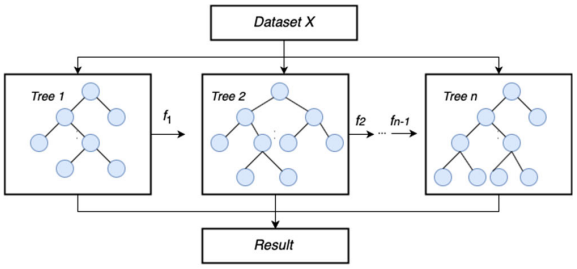

FIGURE 6. Architecture of the of XGBoost model.

of the model's overall performance. Additionally, performance metrics included confusion matrix, precision, recall, and F1-score, which summarizes the classification model's effectiveness. Furthermore, it comprises true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN) for the developed model.

1) CONFUSION MATRIX

A confusion matrix is a table that is used to summarizes the performance of a classification model. It shows the number of true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN) that the model produced by the model.

a) The TP are the instances that were correctly classified as normal.
b) The FP are the instances that were incorrectly classified as attacks.
c) The TN are the instances that were correctly classified as attacks.
d) The FN are the instances that were incorrectly classified as normal.

2) ACCURACY

The accuracy of a model represents only a portion of its overall performance. The accuracy metric is commonly employed in the evaluation of classification models. It is calculated as follows:

$$\boldsymbol{Accuracy} = \frac{\boldsymbol{TP} + \boldsymbol{TN}}{\boldsymbol{TP} + \boldsymbol{FP} + \boldsymbol{TN} + \boldsymbol{FN}} \tag{12}$$

3) PRECISION

Precision is the positive predictive value. The metric quantifies the ratio of correctly identified positive instances by the model to the total number of positive instances identified by the model. In addition, precision is the fraction of instances that were classified as attacks. It is calculated as follows:

$$\boldsymbol{Precision} = \frac{\boldsymbol{TP}}{\boldsymbol{TP} + \boldsymbol{FP}} \tag{13}$$

4) RECALL

The recall metric, also referred to as the actual positive rate, quantifies the proportion of positive instances correctly identified by the model concerning the total number of positive instances present in the dataset. Additionally, recall is the fraction of instances that are attacked that were classified as attacks. It is calculated as follows:

$$\boldsymbol{Recall} = \frac{\boldsymbol{TP}}{\boldsymbol{TP} + \boldsymbol{FN}} \tag{14}$$

Algorithm 1 Pseudocode of the LSTM and XGBoost deployment processes

Require: Gas Pipeline Data $\mathcal{D} = (xi, +yi)\, i = 1^n$, Evaluation Metrics *MAE*
Ensure: Model $f\ (x;\theta)$, Detection of Cyberattacks
Preprocessing:
$\mathcal{D} \leftarrow$ Handle missing values, normalize, encode categorical variables, and split into train/test sets
Train:
$\theta \leftarrow$ Choose model/LSTM or XGBoost
$\theta \leftarrow$ Train on a train set using the Model
Evaluation:
$MAE_{train} \leftarrow$ Evaluate the model on the train set
$MAE_{test} \leftarrow$ Evaluate the model on the test set
Deploy:
If MAE_{test} is satisfactory, deploy the model $f\ (x;\theta)$
Set up monitoring to ensure that the model's performance is maintained over time
Update:
If necessary, retain the model using new data or update hyperparameters θ

5) F1 SCORE

The F1 score can also evaluate the performance of a model as well. The metric in question is a calculated value that combines the precision and recall of a given model, considering their respective weights. In addition, the F1 score is a measure of the accuracy of the classification model. It is calculated as the harmonic mean of precision and recall.

$$\boldsymbol{F1\ Score} = \boldsymbol{2X}\frac{(\boldsymbol{PrecisionXRecall})}{(\boldsymbol{Precision} + \boldsymbol{Recall})} \tag{15}$$

6) RECEIVER OPERATING CHARACTERISTIC CURVE

The receiver operating characteristic (ROC) curve is a widely used graph that summarizes a classifier's performance across all possible thresholds. In addition, the ROC curve is a plot of the true positive rate (TPR) against the false positive rate (FPR).

IV. IMPLEMENTATION AND RESULT ANALYSIS

A. EXPERIMENTAL SETUP

The experiment was conducted using Desktop-G7BDT90, with the operating system edition of Windows 10 Home 64-bit (22H2, Build 19045). The processor was Intel(R) Core (TM) i5-6400 CPU @ 2.70GHz, 2.70GHz. The memory for the desktop was 16.0 GB RM. In addition, for data analogy, we used Python (version 3.8.11) for the artificial neural network and the machine learning Keras library, along with its functionality on the back end, TensorFlow, to perform low-level operations using Keras. For data analysis, the Scikit-learn library was used; for data visualization the

TABLE 6. Statistics of the datasets used in the experiment.

S. No	Class	Sample size
1	Normal	274,628
2	Attack	60,048

FIGURE 7. Model accuracy comparison.

Matplotlib library and Seaborn library; and for data cleaning and feature engineering, the Pandas, and Numpy libraries were used.

B. RESULT ANALYSIS

This subsection provides details of the implementation and validation of the proposed methods mentioned in Section III. A feature selection method was used to improve the accuracy score. In addition, a comparative performance analysis was conducted, in which we trained and tested our employed models with other available benchmark datasets that contain various types of cyberattacks. Detailed statistics of datasets that only consist of binary classification tasks. Additionally, 274,628 are samples, while 60,048 are attack-related (See Table 6).

Figure 7 presents a comparative analysis of the LSTM and XGBoost models in terms of their accuracy in classifying cyberattacks. Following the completion of training and testing, the XGBoost model achieved a higher level of efficiency of 98%. This result represents a 1% improvement over the performance of the LSTM model.

The employed LSTM model for detecting cyber security attacks in cyber-physical systems (CPSs) achieved a training accuracy of 98.80% and a testing accuracy of 97.80%, as shown in Figure 8. This indicates that the model learned the patterns in the training data and generalized well to new data. The training loss was 0.4911, whereas the testing loss was 0.4796. This indicates that the model could effectively fit the training data and minimize the testing data prediction error. However, the LSTM model's high accuracy and low loss indicate that it is a promising approach for detecting cybersecurity attacks in CPSs. This is because the model was able to learn the patterns in the training data and generalize effectively to new data. Similar performance of the model on testing and training data that the model does not overfit the training data. In addition, the model accuracy and loss results are comparable to or better than those reported by other studies on the detection of cyber security attacks in CPSs using LSTM models. The performance of the model on testing data is comparable to its performance on training data, indicating that the model does not overfit the training data. Overall, the model accuracy and loss results indicate that the employed LSTM model is a promising technique for detecting cyber security attacks in CPSs.

Table 7 presents a comprehensive analysis of the outcomes obtained from the LSTM and XGBoost models for detecting CPS cyber security attacks. The LSTM model attained a classification accuracy of 97%, precision of 86%, recall of 97%, and F1-score of 91% when evaluated on the ICS Gas Pipeline dataset. This finding indicates that the LSTM model demonstrates efficacy in detecting cyber security attacks in CPSs; however, there is a possibility of generating false positive results. The XGBoost model demonstrated notable performance on the ICS gas pipeline dataset, achieving an accuracy of 98%, precision of 99%, recall of 98%, and F1-score of 98%. This finding proved that the XGBoost model demonstrated high efficacy in identifying cyber security attacks in CPSs while exhibiting minimal occurrence of false positives.

In terms of comparative analysis, it is evident that both the LSTM and XGBoost models have demonstrated a commendable level of accuracy when employed for detecting cybersecurity attacks in CPSs. In comparison, the XGBoost model exhibited marginally superior accuracy and precision compared with the LSTM model. This implies that the XGBoost model could offers advantages in the context of cyber security attack detection in CPSs, where the consequences of false positives are financially burdensome.

The findings obtained from the LSTM and XGBoost models demonstrate their capability to acquire knowledge regarding the characteristics of cyber security attacks in the ICS gas pipeline dataset. This phenomenon can be attributed to the capacity of both models to acquire intricate associations among sensor data. Furthermore, the findings derived from the LSTM and XGBoost models demonstrate the efficacy of both models in identifying cyber security attacks within CPSs. In comparison, the XGBoost model exhibited marginally superior accuracy and precision compared with the LSTM model. This implies that the XGBoost model could be a more favorable option for detecting cyber security attacks in CPSs when the consequences of false positives are significant. In general, the outcomes derived from the LSTM and XGBoost models exhibit promise and indicate the potential use of these models in the creation of efficient cyber security attack detection systems for CPSs.

The confusion matrix for the XGBoost model, as shown in Figure 9, provides valuable insights into its performance in classifying various types of cyber-attacks. The matrix shows that the model is highly accurate correctly identifying "Normal" and "Recon" attacks, with few misclassifications. However, some difficulties in distinguishing between similar attack types, such as "NMRI," "CMRI," and "MPCI," have been observed, resulting in a few misclassifications.

Overall, the XGBoost model performs well in cyber security attack detection, especially in detecting common and severe attack types. However, the confusion matrix of the LSTM model highlights its exceptional performance across all attack types. The model detects normal and recon attacks with near-perfect accuracy, with almost no misclassifications in these categories. Notably, the LSTM model excels at distinguishing between attack types that are closely related, such as ''NMRI,'' ''CMRI,'' and ''MPCI,'' resulting in few misclassifications. These findings highlight the robustness and effectiveness of the LSTM model in detecting cybersecurity attacks, making it a promising choice for protecting CPSs against various threats.

Furthermore, the employed model's results were directly compared with the other models, which are SVM and ANN. In terms of overall performance as measured by the F1-Score, the employed models, XGBoost and LSTM, outperformed the other models, SVM and ANN. The employed models achieved F1-Score of 0.94 on average, whereas the other models received F1-Score of 0.86 on average. However, the models also performed well in terms of accuracy, precision, and recall. The highest accuracy (0.98) was achieved by XGBoost, while the highest precision (0.99) and recall (0.97) were achieved by LSTM. The comparison indicates that the employed models, XGBoost and LSTM, outperform SVM and ANN for cyber-attack detection in cyber-physical systems.

C. FEATURE IMPORTANCE

The important features consisted of a bar graph visualization of the top ten important features sorted according to the highest score among all features to improve the model accuracy score. This achievement was achieved by calculating the frequency of the time division of the features in the boosting trees integrated within the model. A feature with a high-value score only contributes when predicting an attack. In addition, a technique for determining the importance of the characteristics was applied to assess the significance of each characteristic in the datasets. The feature importance technique was employed after every training session to modify the attributes of the datasets. The top ten features of the study are presented in Figure 10.

D. COMPARISON PERFORMANCE ANALYSIS

This section provides a comparative performance analysis of our proposed approach. ROC curves are used to evaluate our models' discriminatory capability and efficacy in differentiating between instances of attack and non-attack. We also further investigate the efficiency of our models using other available real-world benchmark datasets that contain different types of cyberattacks.

As shown in Figure 11, the XGBoost and LSTM model's exhibit a robust performance in identifying between attack and non-attack instances, as evidenced by the AUC-ROC value of 0.86. The findings indicate that the XGBoost model is effective in detecting cyber security attacks. After comparing the AUC-ROC values of the LSTM and XGBoost models, it becomes evident that the LSTM model exhibits superior performance in terms of its overall discriminative capability when compared with XGBoost. The LSTM model exhibits a higher AUC-ROC, which indicates its superior capability in accurately classifying attacks while minimizing the occurrence of false positives.

TABLE 7. Model performance results.

Datasets	Model	Accuracy	Precision	Recall	F1-Score
ICS Gas Pipeline	XGBoost	0.98	0.99	0.98	0.98
	LSTM	0.97	0.86	0.97	0.91
	SVM	0.90	0.91	0.90	0.87
	ANN	0.90	0.91	0.90	0.86

In addition, the receiver operating characteristic (ROC) curves provide a visual representation of the trade-offs in performance. The LSTM model consistently exhibits a superior true positive rate compared with XGBoost across different thresholds of false positive rates.

Figure 12 presents our model's comparative performance across various datasets containing different types of intrusions and cyberattacks. In addition, Table 8 provides details about the comparative performance and includes additional evaluation metrics. We also investigated the capabilities of AI techniques for cyberattack detection across real-world benchmark datasets. However, our proposed method has been evaluated using benchmark datasets adopted from [38], [39], [40], and [41]. Moreover, these targeted datasets enable a focused evaluation of our method's efficacy against diverse cyberattacks in these critical systems.

Table 9 provides a comparison of our study with other state-of-the-art studies. We also analyzed the compared studies based on the ML classifiers used, ACC score, predictive features, strengths, and limitations. The analysis findings indicate that ACC is competitive with other techniques for attack detection. However, they can be enhanced. Finally, these studies provide better performance toward various types of cyberattack detection using LSTM and XGBoost classifiers.

V. AI-BASED DETECTION ROADMAP AND THREAT MODEL ANALYSIS

In this section, we investigate the AI capabilities for detecting cybersecurity attacks in CPSs and understand their threat to analysis. The attacks were adapted from the several cyber-attacks included in our datasets, which are naïve malicious response injection (NMRI), complex malicious response injection (CMRI), malicious function code injection (MFCI), denial of service (DoS), and reconnaissance (Recon). Figure 13 shows the AI approaches for detecting attacks using a roadmap.

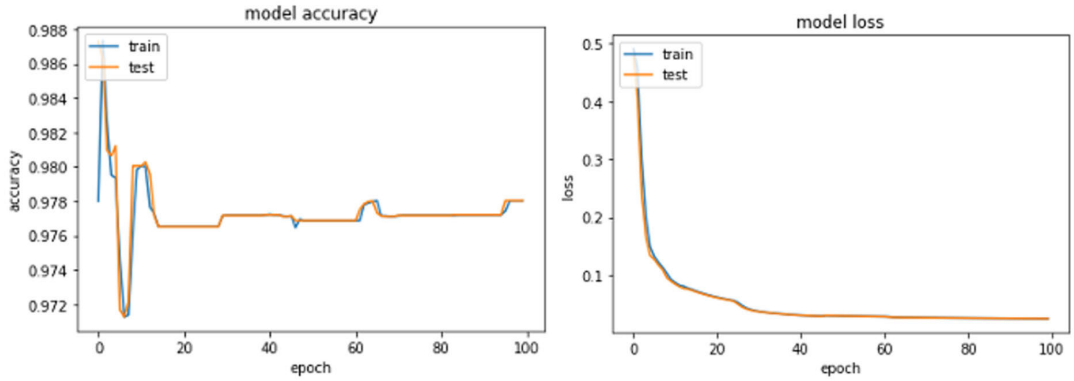

FIGURE 8. Model accuracy (left) and loss performance metric (right) for 100 epochs based on training and validation of an initial network (RNN-LSTM).

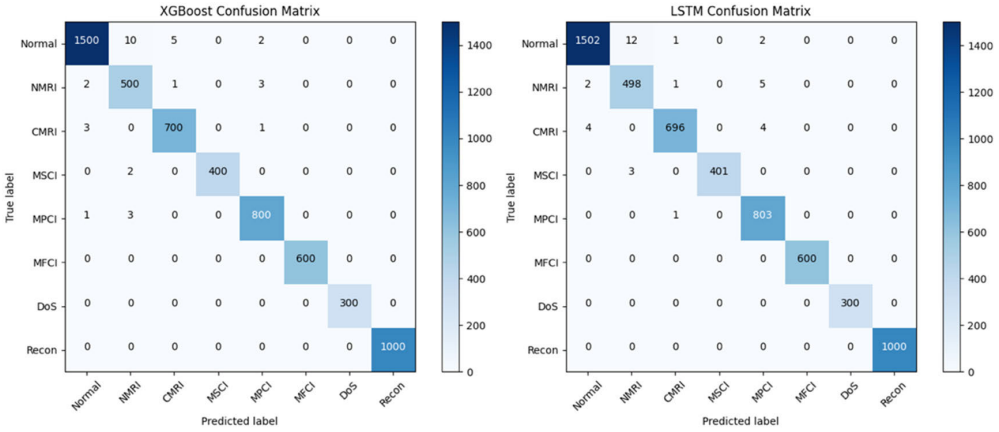

FIGURE 9. Confusion matrix of XGBoost and LSTM.

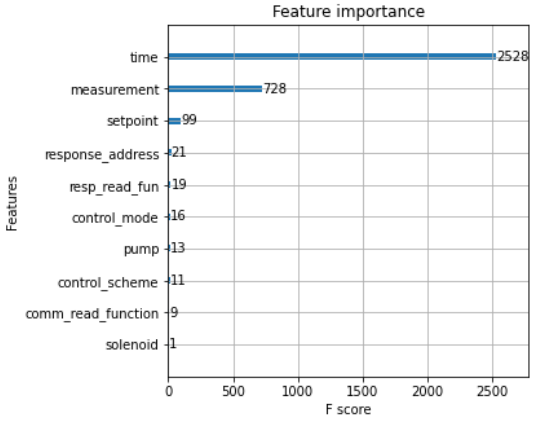

FIGURE 10. Selection of the top 10 features of importance (XGBoost).

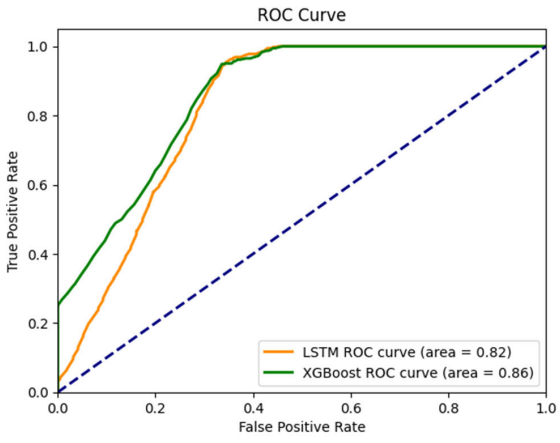

FIGURE 11. ROC curves for the XGBoost and LSTM models.

Naïve malicious response injection (NMRI) attacks are measured by a lack of knowledge regarding the physical system and its control logic. The effects of NMRI attacks are effective because of the attacker's ability to inject or modify response packets in the network. AI-based methods can be used to identify this attack. For example, Wang et al. [42] presented an approach for using a DNN with explanatory attributes for the purpose of intrusion detection in industrial control networks. In addition, support vector machines (SVM) and random forest (RF) have been employed as effective methods for ensuring the reliable detection of network attacks in SCADA systems [43].

Furthermore, NMRI attacks are a type of network-based threat that targets CPSs. These attacks exploit communication protocol vulnerabilities by injecting crafted responses into the network and manipulating the system's perception of physical process control. NMRI attacks can pose significant threats to

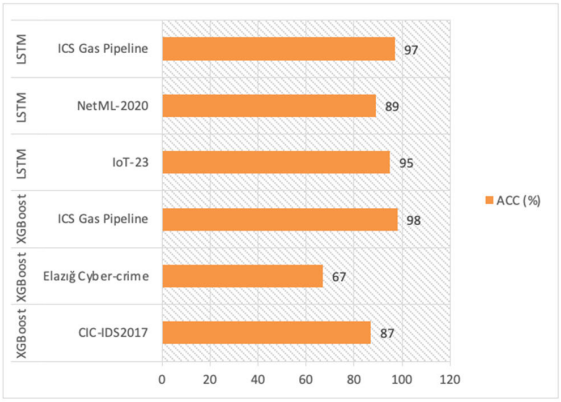

FIGURE 12. Comparison of AI models across various datasets.

ICS and SCADA systems. These attacks can disrupt control loops by injecting false or misleading information, resulting in equipment malfunctions, production outages, or even safety hazards. A comprehensive cybersecurity strategy is required to effectively mitigate NMRI attacks. This strategy should include network segmentation, intrusion detection and prevention systems (IDS/IPS), and vulnerability assessments.

Complex malicious response injection (CMRI) attacks encompass a category of response injection attacks that exploit vulnerabilities in industrial control systems. The effect of CMRI attacks hides the actual state of the physical process. The attack can be detected using AI-based techniques. Shitharth et al. [44] developed sophisticated machine-learning models to enhance the security of SCADA systems. These models are based on the Block Correlated Neural Network (BCNN) used to detect and classify attacks in SCADA systems. In addition, an architectural framework has been proposed to enhance malware detection using two ensembles: one employing a deep belief network (DBN) and the other using a standard classifier, specifically SVM [45].

Furthermore, CMRI attacks target CPSs by injecting malicious responses that mimic normal process functionality. CMRIs are especially difficult to detect using this advanced technique because they effectively mask the true state of the system and negatively impact feedback control loops. CMRI attackers typically have extensive knowledge of the targeted system, allowing them to craft responses that blend in with legitimate data. These attacks can cause catastrophic consequences in critical infrastructure environments by manipulating sensor readings, controlling signals, or even deactivating safety mechanisms. A multi-layered approach to CMRI defense is required that combines intrusion detection systems, anomaly detection algorithms, and continuous monitoring of system behavior. ML techniques are capable of detecting patterns and anomalies that may indicate CMRI activity, enabling timely intervention and mitigation strategies.

Malicious function code injection (MFCI) attacks involve use inherent protocol functions that deviate from their intended purpose. For instance, a force listen-only mode attack is a type of cyber-attack that interrupts network transmission by a MODBUS server. Attacks on the MFCI can cause abnormalities in the system's time and control parameters, which affect its normal operation. Using AI capabilities, these attacks can be detected. For example, Wu [46] employed the C4.5 decision tree (DT), naive Bayes (NB), and CNN model to conduct an analysis and compare their respective impacts on intrusion detection. A more appropriate machine learning model for intrusion detection in industrial IoT is used through experimental analysis.

MFCI attacks pose a significant threat to the CPS cybersecurity. These attacks use communication protocol vulnerabilities to inject malicious commands into programmable logic controllers (PLCs). The attacker manipulates built-in protocol functions to achieve unintended consequences that could result in production process disruptions, safety hazards, and even financial losses. MFCI attacks can be classified into several types based on the specific functions targeted. For example, the "Force Listen Only Mode" attack disables a Modbus secondary device from transmitting data, effectively silencing it on the network. Combating MFCI attacks requires a multi-pronged approach involving multiple layers of defense. Network segmentation can be used to prevent unauthorized access to ICS devices, while firewalls and intrusion detection systems can be used to filter malicious traffic.

A denial-of-service (DoS) attack disrupts the services of a host on a network, rendering the connected resource unavailable to the intended users. DoS attacks have significant effects, including substantial response delays, excessive losses, and service interruptions. These effects directly impact the availability of a system or service. An AI detection model based on logistic regression (LR) and NB has been proposed as a method for detecting attacks as well as normal scenarios [47], [48]. The authors in [49] presented an intelligent agent system that incorporates the K-nearest neighbors (KNN) algorithm to detect distributed denial-of-service (DDoS) attacks. The system uses automatic feature extraction and selection techniques.

In addition, DoS attacks exploit vulnerabilities present in network protocols or system configurations to deplete substantial resources, including bandwidth, memory, or processing capacity. Consequently, the targeted system experiences a state of unresponsiveness or is overwhelmed, thereby impeding legitimate users from accessing crucial services or resources. DoS attacks can manifest in several forms, including volume-based attacks, protocol-based attacks, application-based attacks, and reflected DoS attacks. These attacks employ third-party servers to enhance the impact of the attack by redirecting the traffic back to the target. The detection of DoS attacks is necessitated by the implementation of a comprehensive strategy that encompasses various aspects such as network security, application security, traffic analysis, and incident response planning.

Reconnaissance (Recon) attacks are security attacks employed by an attacker to acquire comprehensive information about the target before initiating an actual attack. The effect of Recon attacks includes using the gathered

TABLE 8. Comparison analysis of AI models across datasets.

Model	Datasets	Accuracy	Precision	Recall	F1-Score
XGBoost	CIC-IDS2017 [38]	0.87	0.98	0.79	0.87
XGBoost	Elazığ Cyber-crime [39]	0.67	0.70	0.69	0.69
XGBoost	ICS Gas Pipeline	0.98	0.99	0.98	0.98
LSTM	IoT-23 [40]	0.95	0.75	1.00	0.85
LSTM	NetML-2020 [41]	0.89	1.00	0.86	0.92
LSTM	ICS Gas Pipeline	0.97	0.86	0.97	0.91

information to determine the precise location of the intended target. Furthermore, based on these data, a hacker can determine the type of infrastructure the target uses. AI-based techniques can detect this attack. Kwon et al. [50] presented a proposed intrusion detection system that incorporates reconnaissance to detect anomalous attacks in a CPS using RNN. In addition, an AI technique based on XGBoost and KNN has been proposed for detecting reconnaissance attacks [51].

Furthermore, recon-attack activities encompass the systematic exploration of the target's network infrastructure, where vulnerabilities are identified, network topology is mapped, and sensitive data are uncovered. Threat of enables proactive cybersecurity practices that aid organizations in anticipating and mitigating potential Recon threats. This is achieved by identifying potential attack scenarios, analyzing of vulnerabilities, and implementing of suitable countermeasures. The procedure entails the careful examination of multiple factors, including the capabilities of the attacker, the assets possessed by the target, and the potential consequences that would arise from a successful attack. Common reconnaissance techniques in the field of cybersecurity encompass a range of methods such as open-source intelligence (OSINT), footprinting, vulnerability scanning, and social engineering. The mitigation of Recon threats can be achieved through the implementation of robust cybersecurity measures, such as network segmentation, access control, vulnerability management, and security awareness training.

VI. POTENTIAL COUNTERMEASURES

This section presents several potential countermeasures for addressing cyber security attacks in the CPS. It is imperative to acknowledge that safeguarding a CPS against all forms of cyber security attacks cannot be achieved through the implementation of a single countermeasure. Nevertheless, it is imperative to adopt a multi-layered security strategy to effectively minimize the potential vulnerabilities and threats posed by malicious attacks. CPSs frequently exhibit intricate and decentralized characteristics that pose challenges in ensuring their security. Furthermore, CPSs are frequently employed in critical infrastructure contexts, making them attractive targets for malicious actors.

A. COUNTERMEASURES FOR NMRI AND CMRI ATTACKS

Remove potentially harmful characters and code from all user inputs through input validation. The use of prepared statements is recommended to execute database queries, as it aids in mitigating the risk of SQL injection attacks. A web application firewall (WAF) can be employed as a protective measure against prevalent web application attacks, including cross-site scripting (XSS) and NMRI attacks.

B. COUNTERMEASURES FOR THE MFCI ATTACK

Input validation entails checking the user input for malicious code and characters. The implementation of a allowlist can be employed to impose limitations on the range of functions that can be defined within the application. The use of a sandbox facilitates the segregation of functions, thereby preventing the potential impact of a compromised function on other functions.

C. COUNTERMEASURES FOR A DOS ATTACK

Using a firewall prevents DoS attacks from overwhelming the system and filters out malicious traffic. The use of a load balancer is recommended to evenly distribute network traffic among multiple servers, thereby mitigating the impact of a Denial of Service (DoS) attack on any individual server and ensuring the continued functionality of the remaining servers. A content delivery network (CDN) can be employed to cache static content and distribute it to users from servers near their locations. This approach can effectively mitigate the adverse effects of denial-of-service (DoS) attacks.

TABLE 9. Comparison with other related studies based on the LSTM and XGBoost models.

Ref.	Models	(ACC %)	Predictive features	Strengths
[52]	LSTM	98	41	Use LSTM for cyberattack detection and identification of attacks from signature databases. Other algorithms have been included such as KNN have been included.
[53]	LSTM	95	33	Detecting cyberattacks in wireless sensor networks (WSNs) is presented, using the DL method is presented.
[54]	LSTM	78	3	ML classifiers are used to identify security personnel who are vulnerable to increased absenteeism.
This work	LSTM	97	19	Detection of cyberattacks in CPSs using LSTM and XGBoost algorithms with comparison.
[38]	XGboost	100	80	Based on boosted ML classifiers, this is an effective method for identifying network intrusions and cyberattacks.
[55]	XGboost	99	20	The purpose of this study was to analyze the Bot-IoT dataset to categorize reconnaissance attacks in the context of the IoT.
[56]	XGboost	83	49	The authors used ML algorithms to detect and categorize system intrusions.
This work	XGboost	98	19	Detection of cyberattacks in CPSs using the XGBoost and XGBoost algorithms with comparison.

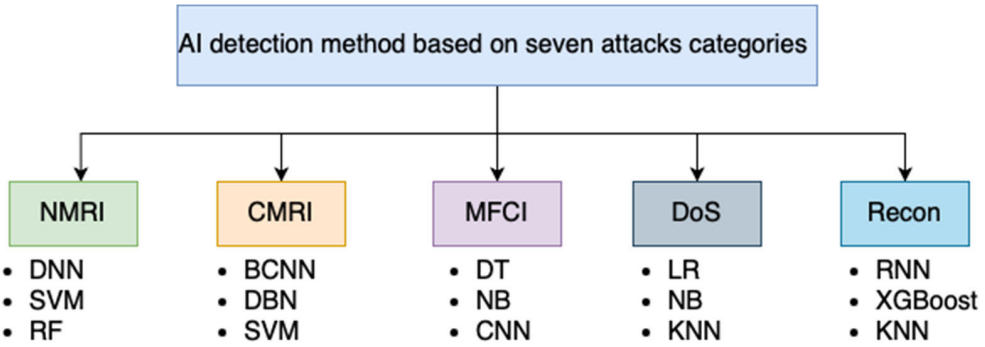

FIGURE 13. Illustration of artificial intelligence methods based on attack categories.

D. COUNTERMEASURES FOR THE RECON ATTACK

A firewall should be employed to impose access restrictions on the system and network, permitting only essential traffic to traverse. Intrusion detection and prevention systems (IDS/IPS) are security mechanisms designed to detect and prevent unauthorized access or malicious activities within a computer network. Using an intrusion detection system (IDS) or intrusion prevention system (IPS) to actively monitor both the system and network for potentially malicious activities, including but not limited to port scanning and reconnaissance attacks. It is imperative to ensure the regular updating of system and network software with the most recent security patches to maintain optimal security measures.

VII. CONCLUSION AND FUTURE DIRECTIONS

In conclusion, we have presented a comparison and investigation of AI approaches for cyberattack detection in a CPS environment. The LSTM and XGBoost classifiers were used to analyze the performance toward advanced cyberattack detection in the CPS network communication layer. The model was trained and tested using real-world benchmark datasets from gas pipelines. Due to the large number of datasets, we had to monitor ACC and validation trends for 100 training epochs. The prediction classification rate was ACC of 97.80% from LSTM and XGBoost 98.69%. The experiment confirmed that XGboost performed better by achieving higher accuracy scores and cyberattack classification rates in CPSs.

We hope that further research can focus on real-time ICS system datasets to detect threats, such as DoS and DDoS attacks, using unsupervised learning. However, our analysis indicates that classification outcomes may be enhanced by including or excluding attributes from gas pipeline datasets or larger sample datasets. Finally, the findings from the ROC curve analysis highlight the effectiveness of both the LSTM and XGBoost models in cyber security attack detection. The implications of these findings are of great importance in the context of improving the security of cyber-physical systems. Additional potential future research could entail investigating ensemble methods or improving hyperparameters to enhance the model's performance. Finally, the nomenclature, which

includes symbols, notations, and their descriptions, has been provided (see Table 4).

ABBREVIATIONS

This manuscript uses the following abbreviations:

ACC	Accuracy.
ANN	Artificial Neural Network.
APT	Advanced Persistent Threats.
AHSA	Adaptive Harmony Search Algorithm.
CSV	Comma Separated Value.
CPS	Cyber-Physical System.
CPSs	Cyber-Physical Systems.
CMS	Cyber Manufacturing system.
CNN	Convolutional Neural Network.
DL	Deep Learning.
DT	Decision Tree.
DoS	Denial of Service.
DRL	Deep Reinforcement Learning.
DBN	Deep Belief Network.
DRNN	Deep Recurrent Neural Network.
FP	False Positive.
FN	False Negative.
FFDNN	Feed-Forward Deep Neural Network.
FDIA	False Data Injection Attacks.
EASH	Energy Aware Smart Home.
GC-LSTM	Graph Convolutional Long-Short-Term Memory.
IR 4.0	Fourth Industrial Revolution.
HMI	Human Machine Interface.
IoT	Internet of Things.
ICS	Industrial Control System.
IDS	Intrusion Detection System.
KNN	K-Nearest Neighbors.
LSTM	Long Short-Term Memory.
ML	Machine Learning.
MTU	Master Terminal Unit.
MLP	Multilayer Perceptrons.
NSF	National Science Foundation NSF.
OT	Operational Technology OT.
OSINT	Open-Source Intelligence.
PSO	Particle Swarm Optimization.
PLCs	Programmable Logic Controllers.
PMU	Phasor Measurement Unit.
US	United State.
RTU	Modbus Remote Terminal Unit.
RNN	Recurrent Neural Network.
RF	Random Forest
SQL	Structured Query Language
SDN	Software-Defined Network
SG	Smart Grid.
SVM	Support Vector Machine.
TP	True Positive.
TN	True Negative.
WFEU	Wrapper-Based Feature Extraction Unit.
XGBoost	eXtreme Gradient Boosting.

REFERENCES

[1] H. Gill, "A continuing vision: Cyber-physical systems," in *Proc. 4th Annu. Carnegie Mellon Conf. Electr. Ind. Future Energy Syst., Efficiency, Secur., Control*, 2008, pp. 1–28.

[2] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet Things*, vol. 7, Sep. 2019, Art. no. 100059, doi: 10.1016/j.iot.2019.100059.

[3] A. K. Tyagi and N. Sreenath, "Cyber physical systems: Analyses, challenges and possible solutions," *Internet Things Cyber-Phys. Syst.*, vol. 1, pp. 22–33, Jul. 2021, doi: 10.1016/j.iotcps.2021.12.002.

[4] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K. R. Choo, "A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5110–5118, Aug. 2020.

[5] V. Gunes, S. Peter, T. Givargis, and F. Vahid, "A survey on concepts, applications, and challenges in cyber-physical systems," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 12, pp. 4242–4268, 2014, doi: 10.3837/tiis.2014.12.001.

[6] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018, doi: 10.1016/j.neucom.2017.10.009.

[7] Y. Zhao, P. Gu, F. Zhu, T. Liu, and R. Shen, "Security control scheme for cyber-physical system with a complex network in physical layer against false data injection attacks," *Appl. Math. Comput.*, vol. 447, Jun. 2023, Art. no. 127908, doi: 10.1016/j.amc.2023.127908.

[8] *Attack That Hit Ukraine Power Grid Had Stuxnet-Like Capabilities*. Accessed: May 8, 2023. [Online]. Available: https://www.eweek.com/security/industroyer-cyber-attack-revealed-as-cause-of-ukraine-power-outage/

[9] C. S. Wickramasinghe, D. L. Marino, K. Amarasinghe, and M. Manic, "Generalization of deep learning for cyber-physical system security: A survey," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc.*, Oct. 2018, pp. 745–751, doi: 10.1109/IECON.2018.8591773.

[10] A. A. Alashhab, M. S. M. Zahid, A. Muneer, and M. Abdukkahi, "Low-rate DDoS attack detection using deep learning for SDN-enabled IoT networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 11, pp. 371–377, 2022, doi: 10.14569/ijacsa.2022.0131141.

[11] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Daphne Yao, "Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities," 2020, *arXiv:2003.13213*.

[12] J. L. Leevy, J. Hancock, R. Zuech, and T. M. Khoshgoftaar, "Detecting cybersecurity attacks using different network features with LightGBM and XGBoost learners," in *Proc. IEEE 2nd Int. Conf. Cognit. Mach. Intell. (CogMI)*, Oct. 2020, pp. 190–197, doi: 10.1109/CogMI50398.2020.00032.

[13] A. R. Gad, M. Haggag, A. A. Nashat, and T. M. Barakat. (2022). *A Distributed Intrusion Detection System Using Machine Learning for IoT Based on ToN-IoT Dataset*. [Online]. Available: https://www.ijacsa.thesai.org

[14] M. Abdullahi, H. Alhussian, N. Aziz, S. J. Abdulkadir, and Y. Baashar, "Deep learning model for cybersecurity attack detection in cyber-physical systems," in *Proc. 6th Int. Conf. Comput., Commun., Control Autom. (ICCUBEA*, Aug. 2022, pp. 1–5, doi: 10.1109/ICCUBEA54992.2022.10010717.

[15] P. Radanliev, D. de Roure, M. van Kleek, O. Santos, and U. Ani, "Artificial intelligence in cyber physical systems," *AI Soc.*, vol. 36, no. 3, pp. 783–796, Sep. 2021, doi: 10.1007/s00146-020-01049-0.

[16] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Comput. Ind.*, vol. 100, pp. 212–223, Sep. 2018, doi: 10.1016/j.compind.2018.04.017.

[17] M. Zahid, I. Inayat, M. Daneva, and Z. Mehmood, "Security risks in cyber physical systems—A systematic mapping study," *J. Softw., Evol. Process*, vol. 33, no. 9, p. e2346, Sep. 2021, doi: 10.1002/smr.2346.

[18] R. S. Devi and M. M. Kumar, "Cyber security affairs in empowering technologies," *Int. J. Innov. Technol. Exploring Eng.*, vol. 8, no. 10, pp. 1–7, 2019, doi: 10.35940/ijitee.J1001.08810S19.

[19] A. Ghosh, D. Chakraborty, and A. Law, "Artificial intelligence in Internet of Things," *CAAI Trans. Intell. Technol.*, vol. 3, no. 4, pp. 208–218, Dec. 2018, doi: 10.1049/trit.2018.1008.

[20] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simul. Model. Pract. Theory*, vol. 101, May 2020, Art. no. 102031, doi: 10.1016/j.simpat.2019.102031.

[21] R. Mall, K. Abhishek, S. Manimurugan, A. Shankar, and A. Kumar, "Stacking ensemble approach for DDoS attack detection in software-defined cyber-physical systems," *Comput. Electr. Eng.*, vol. 107, Apr. 2023, Art. no. 108635, doi: 10.1016/j.compeleceng.2023.108635.

[22] K. Bitirgen and Ü. B. Filik, "A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid," *Int. J. Crit. Infrastruct. Protection*, vol. 40, Mar. 2023, Art. no. 100582, doi: 10.1016/j.ijcip.2022.100582.

[23] N. Thapa, Z. Liu, D. B. Kc, B. Gokaraju, and K. Roy, "Comparison of machine learning and deep learning models for network intrusion detection systems," *Future Internet*, vol. 12, no. 10, p. 167, Sep. 2020, doi: 10.3390/fi12100167.

[24] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 3, pp. 377–391, Mar. 2022, doi: 10.1109/JAS.2021.1004261.

[25] R. F. Mansour, "Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment," *Sci. Rep.*, vol. 12, no. 1, p. 12937, Jul. 2022, doi: 10.1038/s41598-022-17043-z.

[26] M. Catillo, A. Pecchia, and U. Villano, "CPS-GUARD: Intrusion detection for cyber-physical systems and IoT devices using outlier-aware deep autoencoders," *Comput. Secur.*, vol. 129, Jun. 2023, Art. no. 103210, doi: 10.1016/j.cose.2023.103210.

[27] M. I. Sayed, S. Saha, and A. Haque, "Deep learning based malapps detection in Android powered mobile cyber-physical system," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2023, pp. 443–449, doi: 10.1109/ICNC57223.2023.10074208.

[28] P. Ganesh, X. Lou, Y. Chen, R. Tan, D. K. Y. Yau, D. Chen, and M. Winslett, "Learning-based simultaneous detection and characterization of time delay attack in cyber-physical systems," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3581–3593, Jul. 2021, doi: 10.1109/TSG.2021.3058682.

[29] X. Lin, D. An, F. Cui, and F. Zhang, "False data injection attack in smart grid: Attack model and reinforcement learning-based detection method," *Frontiers Energy Res.*, vol. 10, pp. 1–14, Jan. 2023, doi: 10.3389/fenrg.2022.1104989.

[30] H. Jahangir, S. Lakshminarayana, C. Maple, and G. Epiphaniou, "A deep-learning-based solution for securing the power grid against load altering threats by IoT-enabled devices," *IEEE Internet Things J.*, vol. 10, no. 12, pp. 10687–10697, 2023, doi: 10.1109/JIOT.2023.3240289.

[31] A. Presekal, A. Ştefanov, V. S. Rajkumar, and P. Palensky, "Attack graph model for cyber-physical power systems using hybrid deep learning," *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 4007–4020, Sep. 2023, doi: 10.1109/TSG.2023.3237011.

[32] L. Almuqren, M. S. Maashi, M. Alamgeer, H. Mohsen, M. A. Hamza, and A. A. Abdelmageed, "Explainable artificial intelligence enabled intrusion detection technique for secure cyber-physical systems," *Appl. Sci.*, vol. 13, no. 5, p. 3081, Feb. 2023, doi: 10.3390/app13053081.

[33] G. Tertytchny, N. Nicolaou, and M. K. Michael, "Classifying network abnormalities into faults and attacks in IoT-based cyber physical systems using machine learning," *Microprocessors Microsyst.*, vol. 77, Sep. 2020, Art. no. 103121, doi: 10.1016/j.micpro.2020.103121.

[34] M. Abdullahi, H. Alhussian, and N. Aziz, "Adaptation of machine learning and blockchain technology in cyber-physical system applications: A concept paper," in *Proc. Int. Conf. Artif. Intell. Smart Community*, R. Ibrahim, K. Porkumaran, R. Kannan, N. M. Nor, and S. Prabakar, Eds. Singapore: Springer, 2022, pp. 517–523.

[35] T. Sowmya and E. A. Mary Anita, "A comprehensive review of AI based intrusion detection system," *Meas., Sensors*, vol. 28, Aug. 2023, Art. no. 100827, doi: 10.1016/j.measen.2023.100827.

[36] M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L. F. Capretz, and S. J. Abdulkadir, "Detecting cybersecurity attacks in Internet of Things using artificial intelligence methods: A systematic literature review," *Electronics*, vol. 11, no. 2, p. 198, Jan. 2022, doi: 10.3390/electronics11020198.

[37] T. H. Morris, Z. Thornton, and I. Turnipseed, "Industrial control system simulation and data logging for intrusion detection system research," in *Proc. 7th Annu. Southeastern Cyber Secur. Summit*, 2015, p. 6. [Online]. Available: https://www.semanticscholar.org/paper/Industrial-Control-System-Simulation-and-Data-for-Morris-Thornton/bb9714e0c661576f5df19fb54e0e26567ca37372

[38] O. D. Okey, S. S. Maidin, P. Adasme, R. L. Rosa, M. Saadi, D. C. Melgarejo, and D. Z. Rodríguez, "BoostedEnML: Efficient technique for detecting cyberattacks in IoT systems using boosted ensemble machine learning," *Sensors*, vol. 22, no. 19, p. 7409, Sep. 2022, doi: 10.3390/s22197409.

[39] A. Bilen and A. B. Özer, "Cyber-attack method and perpetrator prediction using machine learning algorithms," *PeerJ Comput. Sci.*, vol. 7, p. e475, Apr. 2021, doi: 10.7717/peerj-cs.475.

[40] S. Garcia, A. Parmisano, and M. J. Erquiaga, (Jan. 2020), "IoT-23: A labeled dataset with malicious and benign IoT network traffic," *Zenodo*, doi: 10.5281/zenodo.4743746.

[41] O. Barut, Y. Luo, T. Zhang, W. Li, and P. Li, "NetML: A challenge for network traffic analytics," 2020, *arXiv:2004.13006*.

[42] Z. Wang, Y. Lai, Z. Liu, and J. Liu, "Explaining the attributes of a deep learning based intrusion detection system for industrial control networks," *Sensors*, vol. 20, no. 14, p. 3817, Jul. 2020, doi: 10.3390/s20143817.

[43] R. L. Perez, F. Adamsky, R. Soua, and T. Engel, "Machine learning for reliable network attack detection in SCADA systems," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 633–638, doi: 10.1109/TrustCom/BIGDATASE.2018.00094.

[44] S. Shitharth, K. M. Prasad, K. Sangeetha, P. R. Kshirsagar, T. S. Babu, and H. H. Alhelou, "An enriched RPCO-BCNN mechanisms for attack detection and classification in SCADA systems," *IEEE Access*, vol. 9, pp. 156297–156312, 2021, doi: 10.1109/ACCESS.2021.3129053.

[45] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, "Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks," *Appl. Soft Comput.*, vol. 71, pp. 66–77, Oct. 2018, doi: 10.1016/j.asoc.2018.06.017.

[46] Y. Wu, "Basic intrusion technology of industrial Internet of Things—Based on machine learning," *J. Phys., Conf. Ser.*, vol. 1738, no. 1, Jan. 2021, Art. no. 012094, doi: 10.1088/1742-6596/1738/1/012094.

[47] K. Kumari and M. Mrunalini, "Detecting denial of service attacks using machine learning algorithms," *J. Big Data*, vol. 9, no. 1, p. 56, Dec. 2022, doi: 10.1186/s40537-022-00616-0.

[48] Y. Yan, D. Tang, S. Zhan, R. Dai, J. Chen, and N. Zhu, "Low-rate DoS attack detection based on improved logistic regression," in *Proc. IEEE 21st Int. Conf. High Perform. Comput. Commun., IEEE 17th Int. Conf. Smart City, IEEE 5th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Aug. 2019, pp. 468–476, doi: 10.1109/HPCC/SmartCity/DSS.2019.00076.

[49] R. Abu Bakar, X. Huang, M. S. Javed, S. Hussain, and M. F. Majeed, "An intelligent agent-based detection system for DDoS attacks using automatic feature extraction and selection," *Sensors*, vol. 23, no. 6, p. 3333, Mar. 2023, doi: 10.3390/s23063333.

[50] S. Kwon, H. Yoo, and T. Shon, "IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system," *IEEE Access*, vol. 8, pp. 77572–77586, 2020, doi: 10.1109/ACCESS.2020.2989770.

[51] K. A. Dhanya, S. Vajipayajula, K. Srinivasan, A. Tibrewal, T. S. Kumar, and T. G. Kumar, "Detection of network attacks using machine learning and deep learning models," *Proc. Comput. Sci.*, vol. 218, pp. 57–66, Jan. 2023, doi: 10.1016/j.procs.2022.12.401.

[52] M. S. Alzahrani and F. W. Alsaade, "Computational intelligence approaches in developing cyberattack detection system," *Comput. Intell. Neurosci.*, vol. 2022, Mar. 2022, Art. no. 4705325, doi: 10.1155/2022/4705325.

[53] S. M. Naser, Y. H. Ali, D. Al-Jumeily, and D. Al-Jumeily, "Deep learning model for cyber-attacks detection method in wireless sensor networks," *Original Res.*, vol. 10, no. 2, pp. 251–259, 2022.

[54] E. Lima, T. Vieira, and E. de Barros Costa, "Evaluating deep models for absenteeism prediction of public security agents," *Appl. Soft Comput.*, vol. 91, Jun. 2020, Art. no. 106236, doi: 10.1016/j.asoc.2020.106236.

[55] J. L. Leevy, J. Hancock, T. M. Khoshgoftaar, and N. Seliya, "IoT reconnaissance attack classification with random undersampling and ensemble feature selection," in *Proc. IEEE 7th Int. Conf. Collaboration Internet Comput. (CIC)*, Dec. 2021, pp. 41–49, doi: 10.1109/CIC52973.2021.00016.

[56] J. Sarraf, Vaibhaw, S. Chakraborty, and P. K. Pattnaik, "Detection of network intrusion and classification of cyberattack using machine learning algorithms: A multistage classifier approach," in *Proc. Int. Conf. Smart Comput. Cyber Secur.*, P. K. Pattnaik, M. Sain, A. A. Al-Absi, and P. Kumar, Eds. Singapore: Springer, 2021, pp. 285–295.

MUJAHEED ABDULLAHI (Graduate Student Member, IEEE) received the B.Sc. degree in information technology from Infrastructure University, Kuala Lumpur, Malaysia, in 2018, and the M.Sc. degree in information technology from Universiti Teknologi PETRONAS, Malaysia, in 2022, where he is currently pursuing the Ph.D. degree in information technology. He is a Graduate Research Assistant. His research interests include machine learning, data analytics, cybersecurity, and the Internet of Things.

HITHAM ALHUSSIAN (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in computer science from the School of Mathematical Sciences, Khartoum University, Sudan, and the Ph.D. degree from Universiti Teknologi PETRONAS, Malaysia. He is currently a Senior Lecturer with the Department of Computer and Information Sciences and a Core Research Member of the Centre for Research in Data Science (CERDAS), Universiti Teknologi PETRONAS. His current research interests include real-time parallel distributed systems, cloud computing, big data mining, machine learning, and secure computer-based management systems.

NORSHAKIRAH AZIZ received the Diploma degree in management technology, the bachelor's and M.Sc. degrees in information technology (IT), and the Ph.D. degree in e-business(e-SCM). She is currently a Senior Lecturer with Universiti Teknologi PETRONAS, Malaysia. She is also a Researcher with the UTP Centre of Research in Data Sciences (CeRDaS) and the Data Governance Leader with the High-Performance Cloud Computing Data Centre (HPCCC). She is a Qualified Technologist. She has a total experience of 19 years in both academic institutions and industry. Her industry working experience is related to business intelligence, e-business, and IT project management. Her research interests include business intelligence, data analytics, data governance, and digital addiction.

SAID JADID ABDULKADIR (Senior Member, IEEE) received the B.Sc. degree in computer science from Moi University, the M.Sc. degree in computer science from Universiti Teknologi Malaysia, and the Ph.D. degree in information technology from Universiti Teknologi PETRONAS. He is currently a Senior Lecturer with the Department of Computer and Information Sciences, Universiti Teknologi PETRONAS. His current research interests include supervised machine learning and predictive and streaming analytics. He is currently serving as a Journal Reviewer for *Artificial Intelligence Review*, IEEE Access, and *Knowledge-Based Systems*.

AYED ALWADAIN received the Ph.D. degree from the Queensland University of Technology, Brisbane, QLD, Australia, in 2014. He is currently an Associate Professor with the Computer Science Department, Community College, King Saud University, Riyadh, Saudi Arabia. He has published his work at many international conferences and journals. His research interests include enterprise architecture, service management and engineering, business process management, requirement engineering, machine learning, and big data.

AMINU AMINU MUAZU received the B.Sc. degree in computer science from Umaru Musa Yar'adua University, Katsina, Nigeria, in 2011, and the M.Sc. degree in software engineering from Universiti Malaysia Pahang (UMP), Malaysia, in 2017. He is currently pursuing the Ph.D. degree in information technology (software engineering) with the Computer and Information Science Department, Universiti Teknologi PETRONAS (UTP), Malaysia.

He has been an Academic Staff with the Computer Science Department, Umaru Musa Yar'adua University, since 2020, where he is holding a post as a Lecturer II. He held different positions, such as the Undergraduate Project Coordinator, the Examination Officer, and the Level Advisor. His research interests include software engineering, combinatorial t-way software testing, and optimization algorithms.

Mr. Muazu received the Award of the Best Student of Master's Final Year Project Competition at Universiti Malaysia Phang, in 2016, and the Merit Award of Recognition as a Community Volunteer (Computer Application Instructor) at EC Computer Ltd., Katsina, in 2014.

ABUBAKAR BALA received the bachelor's degree (Hons.) in computer engineering from Bayero University, Kano, Nigeria, in 2011, the master's degree in computer engineering from the King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia, in 2015, and the Ph.D. degree in electrical engineering from Universiti Teknologi PETRONAS (UTP), Malaysia, in 2022. He is currently a Postdoctoral Fellow with the Interdisciplinary Research Center for Communication Systems and Sensing (IRC-CSS), KFUPM. He is developing new algorithms to optimize deep learning models for the detection and classification of unauthorized drones. His research interests include optimization, artificial neural networks, computer vision, and metaheuristics.