IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 21 October 2023, accepted 8 November 2023, date of publication 13 November 2023,
date of current version 17 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3332213

RESEARCH ARTICLE

Automated Threat Detection Using Flamingo Search Algorithm With Optimal Deep Learning on Cyber-Physical System Environment

MASOUD ALAJMI[1], (Member, IEEE), HANAN ABDULLAH MENGASH[2], HAMED ALQAHTANI[3], SUMAYH S. ALJAMEEL[4], MANAR AHMED HAMZA[5], AND AHMED S. SALAMA[6]

[1]Department of Computer Engineering, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
[2]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[3]Department of Information Systems, College of Computer Science, Center of Artificial Intelligence, Unit of Cybersecurity, King Khalid University, Abha, Saudi Arabia
[4]SAUDI ARAMCO Cybersecurity Chair, Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia
[5]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[6]Department of Electrical Engineering, Faculty of Engineering and Technology, Future University in Egypt, New Cairo 11845, Egypt

Corresponding authors: Manar Ahmed Hamza (ma.hamza@psau.edu.sa) and Ahmed S. Salama (a.salama@fue.edu.eg)

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/ 159 /44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R114), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. We Would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444). This study is partially funded by the Future University in Egypt (FUE).

ABSTRACT Threat detection in a Cyber-Physical System (CPS) platform is a key feature of ensuring the reliability and security of these connected methods, but digital elements interface with the physical world. CPS platforms are popular in sectors like healthcare, industrial automation, smart cities, and transportation making them vulnerable to different cyber-attacks. Threat detection in CPS contains the detection and mitigation of cybersecurity risks, which disrupt physical processes, compromise data integrity, and potentially cause safety concerns. Machine learning (ML) and deep learning (DL) systems are exploited for detecting anomalies by learning the normal behaviour forms of the CPS and recognizing deviations. This study presents an Automated Threat Detection using the Flamingo Search Algorithm with Optimal Deep Learning (ATD-FSAODL) technique in a CPS environment. Initially, the ATD-FSAODL technique applies FSA-based feature subset selection to elect the better group of features. In addition, the ATD-FSAODL technique makes use of a modified Elman Spike Neural Network (MESNN) model for threat recognition and classification. Finally, the slime mold algorithm (SMA) is used for the optimal selection of the parameters related to the MESNN approach to ensure that the threat detection rate is improved. To estimate the solution of the ATD-FSAODL technique, a sequence of simulations can be carried out on benchmark databases. The performance values portray the capable solution of the ATD-FSAODL methodology with other methods with a maximum accuracy of 99.58%, precision of 99.58%, recall of 99.58%, F-score of 99.58%, and MCC of 99.16%.

INDEX TERMS Cyber-physical system, industry 4.0, threat analysis, feature selection, deep learning.

I. INTRODUCTION

With the fast development of information and technologies, network security is developing major importance over time accordingly the attention that enterprises, businesses, and industries are positioned on systems namely cyber-physical security systems [1]. Cybersecurity professionals detect the importance of making an efficient network intrusion detection system (IDS) for providing safety networks [2]. Cyber-physical systems (CPSs) embedded sensing, computing,

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

control, and networking into physical components and frameworks, connecting them to the Internet and each other [3]. IDS is a foundational layer that should rapidly assess, detect, and respond to risky cyber traffic [4]. Network intrusion detection has been significant in detecting and monitoring possible attacks [5]. There is frequently the main asymmetrical information in open databases for intrusion detection [6]. The management of a massive quantity of information in a difficult network framework has been another problem that these approaches generally fail to address [7]. As a result, conventional IDSs that depend on traditional machine learning (ML) techniques usually have some disadvantages, namely lower real-time performance, and poor generalization capability [8]. In recent years, researchers have proposed various IDSs using deep learning (DL), ML, and other statistical methods [9].

A recent study on intrusion detection designs in work determines the improved performance of ML methods [10]. The IDS utilizes software and hardware for detecting intrusions from the networks [11]. The utilization of an embedded method allows the network-level execution of safety regulation. IDS are categorized into host- and network-based [12]. The virtual data are employed to feature extracts for classification-based IDSs. The ML approaches comprise unsupervised and supervised techniques and DL techniques are often used in IDSs [2]. Monitoring every packet from the network traffic would be computationally intensive and time-consuming due to the rising network traffic and various types of attacks. The DL is a robust device for detecting attacks and monitoring entire packets. The DL is to detect automatically correlations in data [13]; hence, it could be used for detecting zero-day attacks and obtaining a higher detection rate. Latest advances in DL methods are leading to breakthroughs in long-term AI tasks such as cybersecurity image, text, and speech detection and language translation [14].

This study presents an Automated Threat Detection using the Flamingo Search Algorithm with Optimal Deep Learning (ATD-FSAODL) technique in a CPS environment. The ATD-FSAODL technique applies FSA-based feature subset selection to elect the better group of features. In addition, the ATD-FSAODL technique makes use of a modified Elman Spike Neural Network (MESNN) model for threat recognition and classification. Finally, the slime mold algorithm (SMA) is used for the optimal selection of the parameters related to the MESNN approach to ensure that the threat detection rate is higher. To estimate the solution of the ATD-FSAODL technique, a sequence of simulations can be carried out on a benchmark database. In short, the key contributions are given as follows.

- Design a new ATD-FSAODL technique comprising FSA-based feature subset selection, MESNN-based classification, and SMA-based parameter tuning has been developed. This innovative approach is designed to improve the accuracy and efficiency of threat recognition, ultimately contributing to the cybersecurity and reliability of CPS.
- Develop FSA which optimizes the selection of the most relevant features, enhancing the efficiency of the threat detection process by reducing the dimensionality of the data and focusing on critical information.
- MESNN is adapted to handle the specific challenges of CPS environments, ensuring accurate threat detection in real-time scenarios. The design of the SMA for the optimal selection of parameters related to the MESNN approach ensures that the model is fine-tuned for maximum effectiveness in identifying and classifying threats, enhancing overall system security.

II. RELATED WORKS

Catillo et al. [3] examined a novel intrusion detection methodology CPS-GUARD depends on a single semi-supervised AE and the method to set the threshold utilized for discriminating normal activities in threats. CPS-GUARD was estimated using direct testing with intrusion and normal data points relating to separate sensing tools. The authors [15] developed a novel hybrid method for intrusion prediction in CPS communication networks. The authors utilize a bio-inspired hyper-parameter search algorithm for making an improved DNN structure depending on the core hyper-parameters of an NN. In [16], the authors suggested an innovative federated DL technique (DeepFed). Primarily, DL-based IDS for industrial CPSs by utilizing CNN and GRU. Secondarily, a federated learning approach is designed to enable several industrial CPSs to make comprehensive IDS.

Umer et al. [17] introduced the CPS model as a layered method comprising the physical, network, and application layers with respect to functionality. Later, various cyber-physical attacks on every layer were enhanced. Subsequently, DL methods are examined for intrusion detection and malicious URLs in CPSs. In [18], the authors recommended a technique to extract valuable features from particular features and later employ a DL approach for categorizing the intrusions. A distinctive Generic-Specific AE design is developed, where the specific ones learn features that can be related only to that domain, and the generic one learns the features, which are general around every type of network intrusion. The authors [19] suggested a knowledge distillation technique that depends on Triplet CNN to higher the solution of the method and dramatically increase the anomaly detection speed for industrial CPS.

Almutairi et al. [20] recommended a Quantum Dwarf Mongoose Optimizer with Ensemble DL-based Intrusion Detection (QDMO-EDLID) approach from the CPS platform. The introduced QDMO-EDLID method objectives are to detect the existence of intrusions by ensemble learning and the FS method. The QDMO-EDLID approach uses the QDMO method for feature subset selection purposes. Duhayyim et al. [21] present a novel Stochastic Fractal

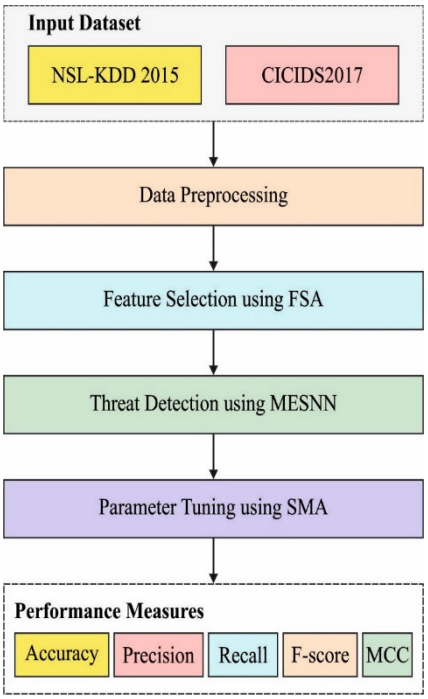

FIGURE 1. Workflow of ATD-FSAODL system.

Search Algorithm with DL Driven IDS (SFSA-DLIDS). The SFSA was used for selecting feature subsets. Further, a chicken swarm optimizer (CSO) with a deep stacked AE (DSAE) approach is employed to detect and classify the intrusions.

CPSs contain a wide range of applications in industrial control systems to smart cities and are characterized by difficult connections among physical and digital modules. Existing threat detection methods frequently fall short in adjusting to the unique data sources and real-time desires of CPS, necessitating new methods for FS to extract vital data and hyperparameter tuning to optimize detection accuracy. Besides, resource constraints, dynamic operating conditions, and safety-critical implications underscore the resolve of emerging robust and effectual approaches, which improve the reliability and security of CPS in the face of developing cyber-attacks. Bridging this research gap is paramount to advancing the recent CPS security and ensuring the continued safe process of essential structures.

III. THE PROPOSED MODEL

In this manuscript, we have derived a novel ATD-FSAODL approach for the automated detection and classification of threats from the CPS platform. The ATD-FSAODL technique aims to exploit feature selection and classification processes for automated threat detection. To accomplish this, the ATD-FSAODL technique incorporates FSA-based feature subset selection, MESNN-based classification, and SMA-based parameter tuning. Fig. 1 demonstrates the entire flow of the ATD-FSAODL algorithm.

A. FEATURE SELECTION USING FSA

For an effectual selection of features, the FSA is used. Due to the high capability of global search and high applicability with minimal parameters, Optimization is commonly used in various applications [22]. Flamingos are migratory birds that acquire food from small worms, algae, small shrimps, clams, and larvae.

The major feature of FSA is to calculate the optimum feature for the classification model. The foraging and migratory behaviours are used to develop the optimum features of FSA. The features of the flamingos are inhabitant in the region of food available and after foraging, it moves towards another location using the migration process. The features of the flamingo are given in the following:

1. The changing position can be evaluated by the foraging and migration behaviours of flamingos. As the foraging behavior includes two features namely flamingo foot movement and foraging behavior.
2. For local communication, flamingo sings to one another on food accessibility.
3. The flamingo population does not alert of the existing search region food accessibility. Rather, to find the high food region interacts with one another.

The procedure in FSA is discussed in the following: The food source could not be identified to the flamingo; it is required for spreading the data regarding position and alters in location. The global optimum was dependent upon the availability and position of food sources for assessment to develop the optimum performance from the searching region. Consider the food source from *the* j^{th} dimensional of x_{bj}.

The beak scanning behavior can be assessed by the i^{th} flamingo location from the j^{th} dimensional population as x_{ij} to each flamingo. However, the foraging behavior was exposed to the error based on the data broadcast in smaller probability values. The maximum foraging behaviour dependent upon maximal distance was represented by $|G1 \times xbj + \varepsilon_2 \times xij|$, with the arbitrary integer of -1 or 1. The scanning behavior is assessed by the uniform distribution-based variation curve with a beak scan range of G2 $\times |G1 \times$ xbj $+\varepsilon 2 \times$ xij, whereas $G2$ refers to the arbitrary value of normal distributions.

The flamingos are foraging and scanning their beak and claws toward the food in large ranges for an entire population, The food position is referred to as x_{bj} with the distance taken as $\varepsilon 1 \times x_{bj}$, the arbitrary integer $\varepsilon 1$ is represented as -1 or 1 enhances dependent upon the searching space. The iteration of the flamingo in the foraging distance is evaluated by the following expression:

$$b_{ij}^{t} = \varepsilon_1 \times xb_j^t + G_2 \times \left| G_1 \times xb_j^t + \varepsilon_2 \times x_{ij}^t \right| \tag{1}$$

The position updating of the flamingo foraging behavior is shown below:

$$x_{ij}^{r+1} = x_{ij}^t + \varepsilon_1 \times xb_j^t + G_2 \times \frac{\left| G_1 \times xb_j^t + \varepsilon_2 \times x_{ij}^t \right|}{G} \tag{2}$$

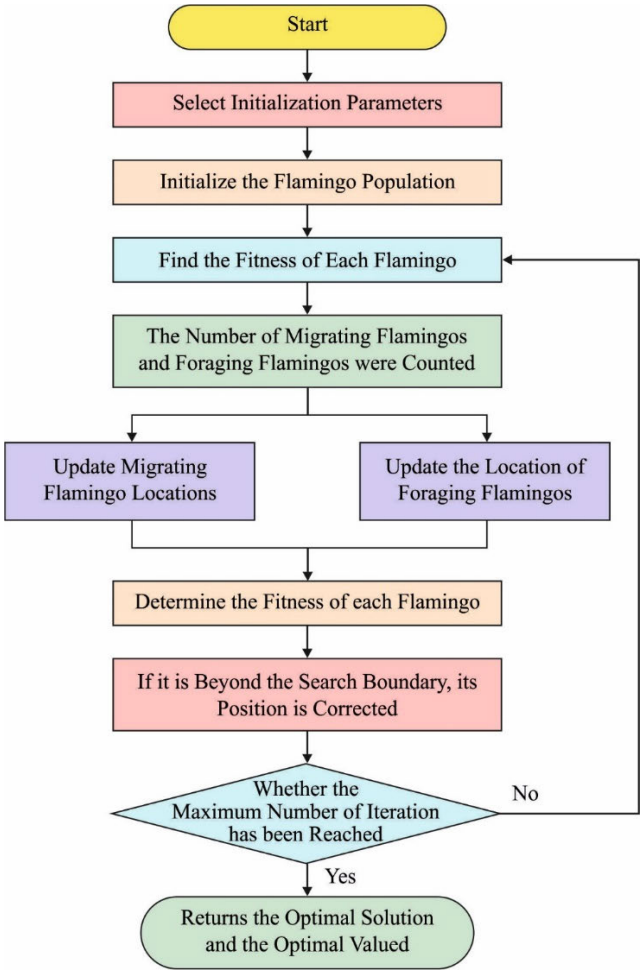

FIGURE 2. Flowchart of FSA.

where x_{ij}^{t+1} represents the i^{th} flamingos and j^{th} population dimension for $t+1$iteration. The flamingo location is indicated as x_{ij}^{t} for the t overall amount of iteration. The optimum fitness value for the flamingos from the populations at t iteration is signified as xb_j^t with a chi-square distribution with a degree of freedom. Fig. 2 describes the flowchart of FSA.

The flamingo population migrated to the next region with high food accessibility. The migration behaviors of flamingo populations are shown below

$$x_{ij}^{r+1} = x_{ij}^{t} + \omega \times \left(xb_j^t - x_{ij}^t\right) \tag{3}$$

where he x_{ij}^{t} shows the location of flamingos at t iterations. The optimum fitness function (FF) for the population is represented by $\omega = N(0,n)$ with a Gaussian arbitrary integer with the degree of freedom value for an increase in searching space.

The FF deployed in the FSA approach was intended to take a balance among the count of FSs in every outcome (minimal) and classifier accuracy (maximal) attained by employing these FSs, Eq. (4) signifies the FF for evaluating performances.

$$Fitness = \alpha\gamma_R(D) + \beta\frac{|R|}{|C|} \tag{4}$$

whereas $\gamma_R(D)$ demonstrates the classifier rate of errors of a provided classifier. $|R|$ denotes the cardinality of the elected subset and $|C|$ stands for the whole feature counts from the database, α and β are 2 parameters equal to the impact of subset length and classifier quality.

B. CLASSIFICATION USING MESNN MODEL

In this work, the MESNN system can be deployed for the automated threat detection process. The presented MESNN is an adapted version of ENN as a partial recurrent spike NN model [23]. The invisible, input, context, and output layers are four different layers of the presented architecture. During the training process, this architecture takes self-feedback with variables obtained from the context layers, whereas the feedback in the invisible to-context layers has feedback weight, W^{hc} that is adaptive. The spike criteria of the trained method accelerated the training method for an active node that reaches the threshold value should be upgraded. The dynamics of the MESNN are discussed.

$$X(k) = f\left(W^{xc}X^c(k), W^{xu}U(k)\right) \tag{5}$$

$$X^c(k) = \alpha(k)X^c(k-1) + W^{hc}X(k-1) \tag{6}$$

$$Y^m(k+1) = W^{yx}X(k) \tag{7}$$

where, X^ck and $X(k)$ denote the node layer vector of context and invisible layers, correspondingly. Y^mk and $U(k)$ show the output and input of MESNN. $f(\cdot)$ refers to a non-linear function. W^{xu}, W^{xc}, and W^{yx} represent the weight vectors among the input and invisible layers, among the context and invisible layers, and the invisible and output layers, correspondingly. During the context layer, the self-feedback α is updated until it attains an accurate value.

C. PARAMETER TUNING USING SMA

At this stage, the SMA can be utilized for the better choice of the MESNN parameters. The SMA is based on the morphological changes and foraging behaviours of Physarum polycephalum [24]. Simultaneously, in the foraging, the negative and positive feedback produced is inspired by the weight in SMA, thereby forming 3 dissimilar SM morphological varieties. The organic mass in SM searches for food during the active feeding stage surrounds it, and secrete enzymes for digesting it. They form connected venous networks using different food sources based on the properties of SM. Once the venous network of SM systems a food source, its biological oscillator produces a propagating wave to raise cytoplasmic flow by the veins. Decreased flow constricts veins that consecutively shrink vein diameter, while increased cytoplasmic flow extends vein diameter. SM can establish a strong path but food concentration is maximum, thereby ensuring rich nutrient concentration. With the fusion of positive and negative feedback, SM establishes the best path to interconnect food

in a better way. Simultaneously, it utilizes food sources due to the unique biology of SM. If the SM determines a low-density food source, it leaves to search for another one.

Based on the smell from the air, SM approaches food, and the contraction mode can be inspired by the subsequent equation:

$$\overrightarrow{X\left(t+1\right)}=\begin{cases}\overrightarrow{X_b\left(t\right)}+\overrightarrow{vb}\cdot\left(\overrightarrow{VV}\cdot\overrightarrow{X_A\left(t\right)}-\overrightarrow{X_B\left(t\right)}\right), r<p\\ \overrightarrow{vc}\cdot\overrightarrow{X\left(t\right)}, r\geq p\end{cases} \tag{8}$$

where $\overrightarrow{vb}$ denotes the parameter within $[-a, a]$; $\overrightarrow{vc}$ reduces linearly in [1-0], t shows the existing iteration; r obtains an arbitrary integer within [0, 1], $\overrightarrow{X_b}$ indicates the single $\rightarrow$ position with the high odor concentration; $\overrightarrow{X}$ indicates the location of SM; $\overrightarrow{X_A}$ and $\overrightarrow{X_B}$ denote the two individuals selected randomly from SM; $\overrightarrow{W}$ shows the weighted of SM; Parameter p is demonstrated as:

$$p=\tanh\left|S\left(i\right)-DF\right|, i=1,2,\ldots,N_{pop} \tag{9}$$

where N_{pop} refers to the size of populations $S(i)$ denotes the fitness of $\overrightarrow{X}$ DF indicates the better fitness attained in all the iterations. vb and a parameters are described as follows:

$$\overrightarrow{vb}=[-a,a] \tag{10}$$

$$a=arctanh\left(-\left(\frac{t}{\max_t}\right)+1\right) \tag{11}$$

Now $\max_t$ signifies the maximal amount of iterations:

$$\overrightarrow{W\left(SmellIndex\left(i\right)\right)}=\begin{cases}1+r\cdot log\left(\dfrac{bF-S\left(i\right)}{bF-wF}+1\right),\\ condition\\ 1-r\cdot log\left(\dfrac{bF-S\left(i\right)}{bF-wF}+1\right),\\ others\end{cases} \tag{12}$$

$$SmellIndex=sort\left(S\right) \tag{13}$$

Eq. (12) inspires the negative as well as positive feedback mechanisms among the explored food concentration and the width of the SM venous network. The weight near the region becomes larger once the food concentration is higher. r denotes the random integer with [0 1]. bF indicates the optimum fitness attained in the existing iteration. wF shows the worse fitness attained from the existing iteration and $SmellIndex$ denotes the fitness value order (in ascending for the minimized problem and descending order for the maximization problem) [24]:

$$\overrightarrow{X^*}=\begin{cases}rand\cdot\left(UB-LB\right)+LB, rand<z\\ \overrightarrow{X_b\left(t\right)}+\overrightarrow{vb}\cdot\left(\overrightarrow{W}\cdot\overrightarrow{X_A\left(t\right)}-\overrightarrow{X_B\left(t\right)}\right), r<p\\ \overrightarrow{vc}\cdot\overrightarrow{X\left(t\right)}, r\geq p\end{cases} \tag{14}$$

TABLE 1. Description of two databases.

Dataset	NSLKDD2015	CICIDS2017
No. of Instances	50000	50000
Attribute Count	41	80
Class Count	2	2
Normal	25000	25000
Anomaly	25000	25000

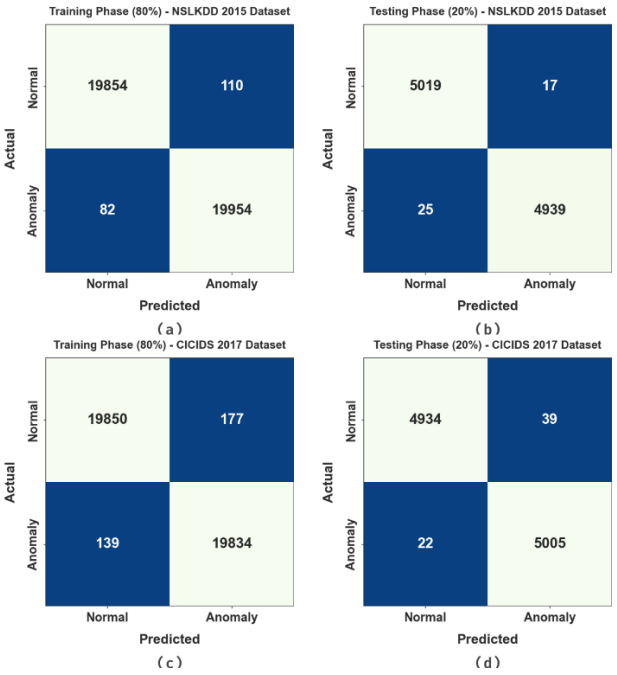

FIGURE 3. Confusion matrices of (a-b) 80:20 of TR set/TS set on the NSLKDD2015 database and (c-d) 80:20 of TR set/TS set on the CICIDS2017 database.

where UB and LB represent the upper as well as lower boundaries of the searching range. $rand$ and r show the randomly generated integer within $[0, 1]$.Z indicates the parameter value defined that ranges between $[0, 0.1]$. Generally, z= 0.03 is suggested because it maintains the between balance exploiting known areas and SM exploring new areas. The SMS primarily consists of the process of initialization, fitness estimation, ranking, weight, and position upgrade. N signifies the cell counts of SM, D signifies the dimension of the function, and T signifies the maximal iteration count. The SMA system develops an FF for gaining improved classifier solutions. It explains a positive integer for illustrating the good solution of candidate performances. In this work, the reduction of the classifier rate of errors is considered FF.

$$\begin{aligned}fitness\left(x_i\right)&=Classifier\ Error\ Rate\left(x_i\right)\\&=\frac{No.of\ misclassified\ instances}{Total\ No.of\ instances}*100\end{aligned} \tag{15}$$

IV. RESULTS AND DISCUSSION

The proposed model is simulated using the Python 3.8.5 tool on PC i5-8600k, GeForce 1050Ti 4GB, 16GB RAM, 250GB

TABLE 2. Threat detection outcome of ATD-FSAODL technique on NSLKDD2015 database.

NSLKDD 2015 Dataset					
Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	MCC
TR set (80%)					
Normal	99.45	99.59	99.45	99.52	99.04
Anomaly	99.59	99.45	99.59	99.52	99.04
Average	99.52	99.52	99.52	99.52	99.04
TS set (20%)					
Normal	99.66	99.50	99.66	99.58	99.16
Anomaly	99.50	99.66	99.50	99.58	99.16
Average	99.58	99.58	99.58	99.58	99.16

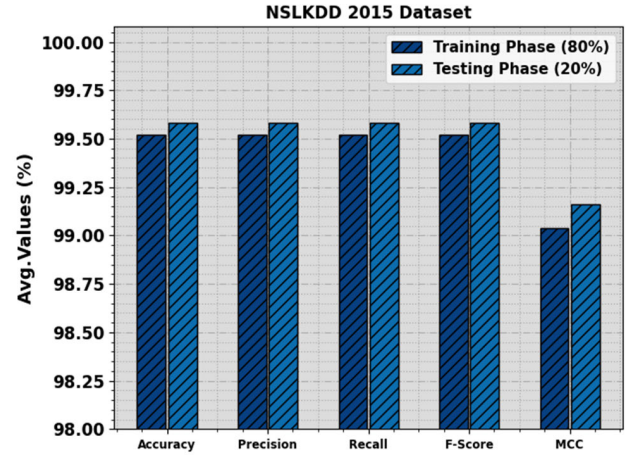

FIGURE 4. Average result of ATD-FSAODL technique on NSLKDD2015 database.

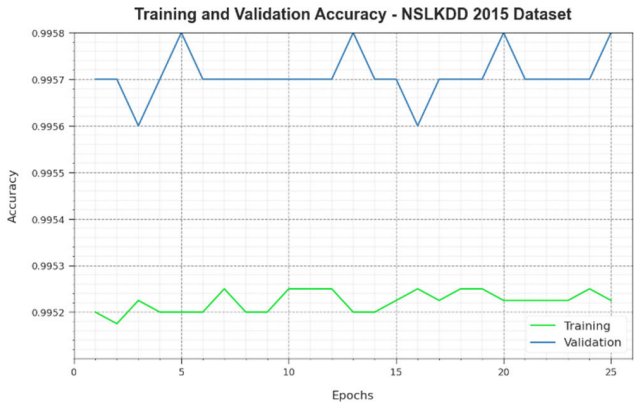

FIGURE 5. $Accu_y$ analysis of ATD-FSAODL technique on the NSLKDD2015 database.

SSD, and 1TB HDD. The parameter settings are given as follows: learning rate: 0.01, dropout: 0.5, batch size: 5, epoch count: 50, and activation: ReLU. In this study, the simulation outcome of the ATD-FSAODL approach was tested on two databases as NSLKDD2015 and the CICIDS2017 database. Table 1 demonstrates a detailed explanation of two databases.

The confusion matrices of the ATD-FSAODL system are depicted in Fig. 3. The outcomes show that the

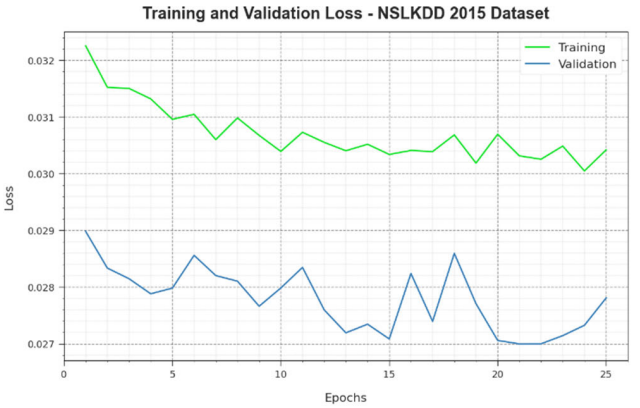

FIGURE 6. Loss curve of ATD-FSAODL technique on NSLKDD2015 database.

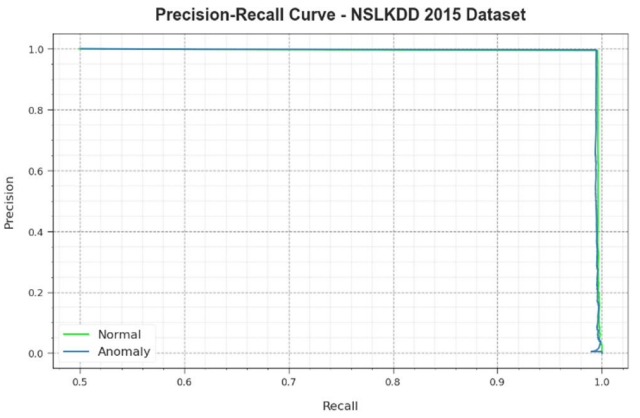

FIGURE 7. PR curve of ATD-FSAODL technique on NSLKDD2015 database.

ATD-FSAODL methodology appropriately categorizes the normal and anomaly instances.

In Table 2 and Fig. 4, the overall threat detection outcome of the ATD-FSAODL approach is tested on the NSLKDD2015 database. The results represented that the ATD-FSAODL approach reaches effective performances. On 80% of the TR set, the ATD-FSAODL technique offers average $accu_y$, $prec_n$, $reca_l$, F_{score}, and MCC of 99.52%, 99.52%, 99.52%, 99.52%, and 99.04% respectively. Also, on 20% of the TS set, the ATD-FSAODL method offers average $accu_y$, $prec_n$, $reca_l$, F_{score}, and MCC of 99.58%, 99.58%, 99.58%, 99.58%, and 99.16% respectively.

Fig. 5 demonstrates the training accuracy TR_accu_y and VL_accu_y of the ATD-FSAODL system on the NSLKDD2015 database. The TL_accu_y is defined by the estimation of the ATD-FSAODL method on the TR database whereas the VL_accu_y is calculated by evaluating the performance on an individual testing dataset. The outcomes revealed that TR_accu_y and VL_accu_y rise with an upsurge in epochs. Therefore, the performance of the ATD-FSAODL technique gets enhanced on the TR and TS dataset with an increase in the number of epochs.

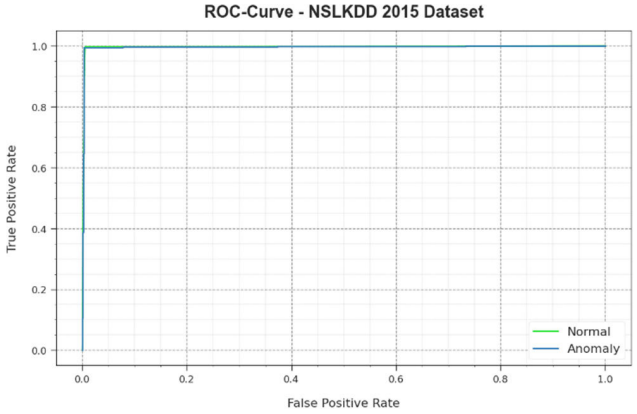

FIGURE 8. ROC curve of ATD-FSAODL method on NSLKDD2015 database.

TABLE 3. Threat detection outcome of ATD-FSAODL technique on the CICIDS2017 database.

CICIDS2017 Dataset					
Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	MCC
TR set (80%)					
Normal	99.12	99.30	99.12	99.21	98.42
Anomaly	99.30	99.12	99.30	99.21	98.42
Average	99.21	99.21	99.21	99.21	98.42
TS set (20%)					
Normal	99.22	99.56	99.22	99.39	98.78
Anomaly	99.56	99.23	99.56	99.39	98.78
Average	99.39	99.39	99.39	99.39	98.78

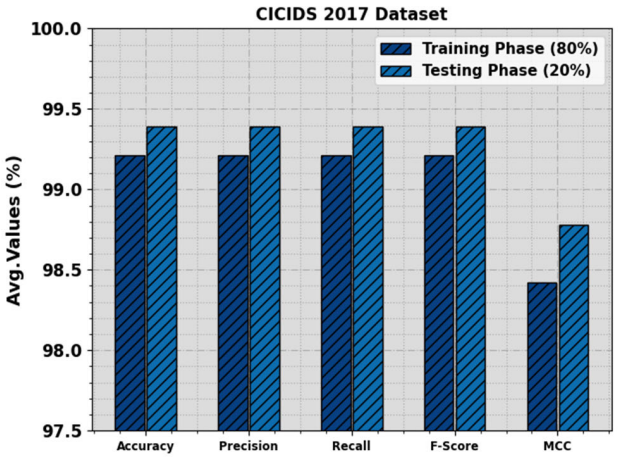

FIGURE 9. Average result of ATD-FSAODL approach on the CICIDS2017 database.

In Fig. 6, the *TR_loss* and *VR_loss* analysis of the ATD-FSAODL approach on the NSLKDD2015 database is presented. The *TR_loss* determines the error between the predicted performance and original values on the TR data. The *VR_loss* signifies the measure of the performance of the ATD-FSAODL system on separate validation data. The outcomes indicated that the *TR_loss* and *VR_loss* tend to reduce with increasing epochs. It depicted the improved performance of the ATD-FSAODL method and its ability

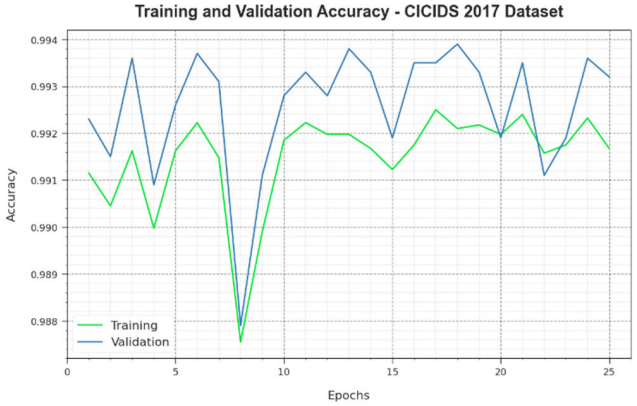

FIGURE 10. $Accu_y$ curve of ATD-FSAODL methodology on CICIDS2017 database.

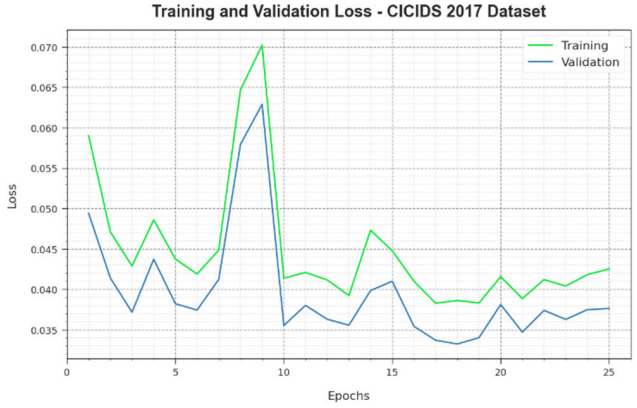

FIGURE 11. Loss curve of ATD-FSAODL methodology on CICIDS2017 database.

to generate accurate classification. The minimalized value of *TR_loss* and *VR_loss* shows the superior performance of the ATD-FSAODL technique in capturing relationships and patterns.

A comprehensive PR investigation of the ATD-FSAODL method is revealed in the NSLKDD2015 database in Fig. 7. The results stated that the ATD-FSAODL system outcomes in raising values of PR. Furthermore, the ATD-FSAODL algorithm can reach superior PR values on 2 class labels.

In Fig. 8, a ROC analysis of the ATD-FSAODL method is demonstrated on the NSLKDD2015 database. The simulation value defined that the ATD-FSAODL method has led to enhanced ROC values. Also, the ATD-FSAODL algorithm attained higher ROC values on 2 class labels.

In Table 3 and Fig. 9, the overall threat detection outcome of the ATD-FSAODL methodology is tested on the CICIDS2017 database. The outcome inferred that the ATD-FSAODL approach reaches effective results. On 80% of the TR set, the ATD-FSAODL algorithm offers average $accu_y$, $prec_n$, $reca_l$, F_{score}, and MCC of 99.21%, 99.21%, 99.21%, 99.21%, and 98.42% respectively. Further, on 20% of the TS set, the ATD-FSAODL method offers average $accu_y$, $prec_n$, $reca_l$, F_{score}, and MCC of 99.39%, 99.39%, 99.39%, 99.39%, and 98.78% correspondingly.

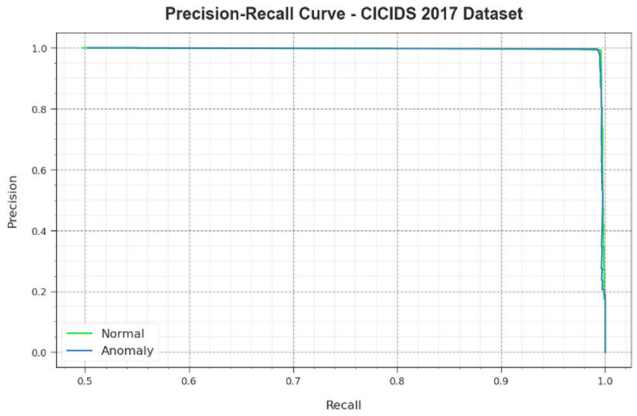

FIGURE 12. PR curve of ATD-FSAODL methodology on CICIDS2017 database.

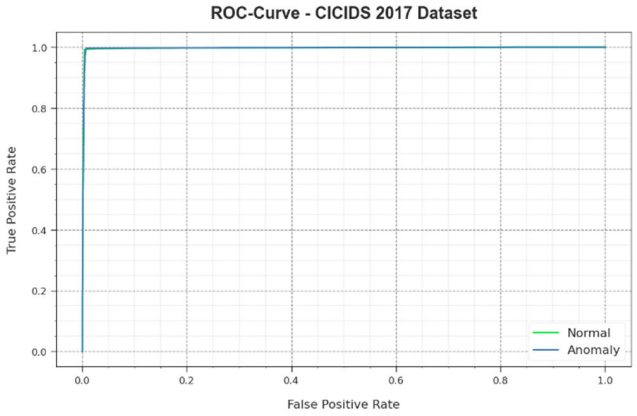

FIGURE 13. ROC curve of ATD-FSAODL methodology on CICIDS2017 database.

Fig. 10 illustrates the training accuracy TR_accu_y and VL_accu_y of the ATD-FSAODL method on the CICIDS2017 database. The TL_accu_y is determined by the estimation of the ATD-FSAODL algorithm on the TR dataset whereas the VL_accu_y is calculated by evaluating the performance on a separate testing dataset. The outcomes exhibited that TR_accu_y and VL_accu_y rise with an upsurge in epochs. Therefore, the performance of the ATD-FSAODL system gets enhanced on the TR and TS dataset with an increase in the number of epochs.

In Fig. 11, the *TR_loss* and *VR_loss* analysis of the ATD-FSAODL method on the CICIDS2017 database is demonstrated. The *TR_loss* defines the error between the predicted performance and original values on the TR data. The *VR_loss* denoted the measure of the performance of the ATD-FSAODL system on individual validation data. The outcomes represent that the *TR_loss* and *VR_loss* tend to reduce with increasing epochs. It revealed the improved performance of the ATD-FSAODL approach and its ability to generate accurate classification. The decreased value of *TR_loss* and *VR_loss* shows the greater performance of the ATD-FSAODL system in capturing patterns and relationships.

TABLE 4. Comparative outcome of ATD-FSAODL technique with other methodologies [20].

Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
ATD-FSAODL	99.58	99.58	99.58	99.58
QDMO-EDLTD	99.51	99.51	99.51	99.51
ATMMF-TDS	98.67	99.23	99.06	99.04
DBN	98.55	98.75	98.28	98.22
LSTM	98.37	98.52	98.18	98.11
RNN	98.71	97.74	98.41	98.05
OT	93.81	95.88	92.52	95.45
RF	95.99	97.6	93.46	95.98

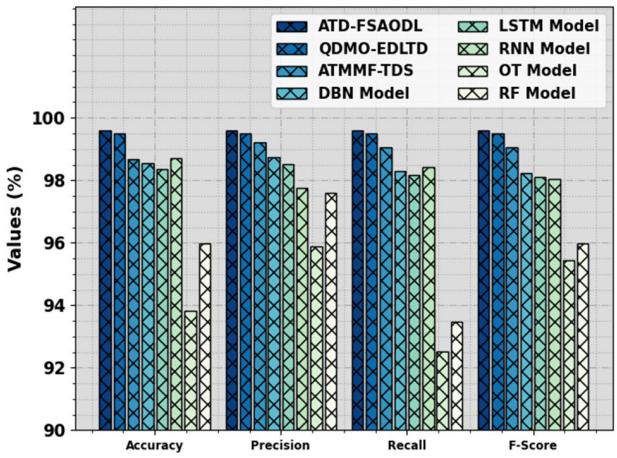

FIGURE 14. Comparative outcome of ATD-FSAODL technique with other methodologies.

TABLE 5. TRT and TST outcomes of ATD-FSAODL method with other algorithms [20].

Methods	Training Time(m)	Testing Time(m)
ATD-FSAODL	0.33	0.19
QDMO-EDLID	0.65	0.38
AIMMF-IDS	0.94	0.42
DBN	1.03	0.57
LSTM	1.14	0.56
RNN	1.14	0.59
DT	1.44	0.78
RF	1.44	0.85

A comprehensive PR analysis of the ATD-FSAODL system is revealed on the CICIDS2017 database in Fig. 12. The results inferred that the ATD-FSAODL algorithm outcome in raising values of PR. Also, it is noticeable that the ATD-FSAODL approach can reach greater PR values on 2 class labels.

In Fig. 13, a ROC analysis of the ATD-FSAODL algorithm is shown on the CICIDS2017 database. The outcome demonstrated that the ATD-FSAODL method has led to enhanced ROC values. Further, the ATD-FSAODL system can extend superior ROC values on 2 class labels.

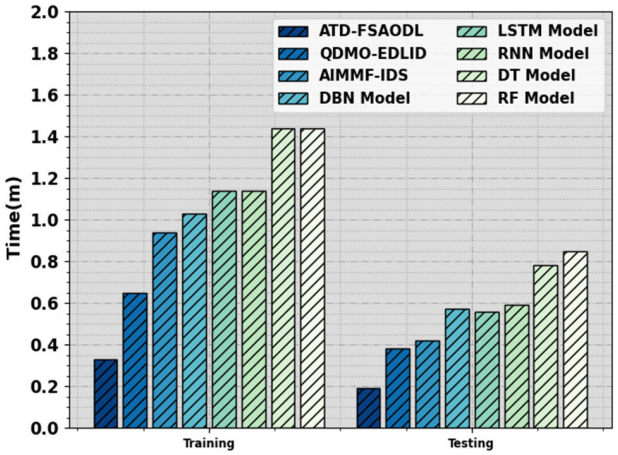

FIGURE 15. TRT and TST outcomes of ATD-FSAODL technique with other methodologies.

In Table 4 and Fig. 14, a comparative outcome of the ATD-FSAODL technique with other approaches is given [20]. The simulation value shows that the OT and RF models have shown worse results than the other ones. Next to that, the ATMMF-TDS, DBN, LSTM, and RNN models have accomplished closer performance. Meanwhile, the QDMO-EDLTD technique has shown moderate performance with $anaccu_y$ of 99.51%, $prec_n$ of 99.51%, $reca_l$ of 99.51%, and F_{score} of 99.51%. However, the ATD-FSAODL technique surpassed the existing models with a maximum $accu_y$ of 99.58%, $prec_n$ of 99.51%, $reca_l$ of 99.51%, and F_{score} of 99.51%.

The computation time examination of the ATD-FSAODL system with existing approaches is given in Table 5 and Fig. 15. The outcome indicates that the ATD-FSAODL methodology accomplishes better performance. Based on training time (TRT), the ATD-FSAODL technique provides a decreasing TRT of 0.33m while the QDMO-EDLID, AIMMF-IDS, DBN, LSTM, RNN, DT, and RF models offered increased TRT values. Besides, depending on testing time (TST), the ATD-FSAODL method provides a reducing TRT of 0.19m while the QDMO-EDLID, AIMMF-IDS, DBN, LSTM, RNN, DT, and RF techniques offered improved TRT values. These outcomes show the optimum solution of the ATD-FSAODL algorithm over other approaches.

The ATD-FSAODL approach gains scalability and robustness through an integration of new methodologies. Scalability is addressed by the FSA that optimizes feature selection, ensuring that only the most important features are assumed, thereby decreasing the computational burden once relating to wide data from large-scale CPS. Furthermore, the use of the SMA for parameter optimizer adjusts the system performance and adaptability to distinct data volumes. The ATD-FSAODL approach's robustness was obtained by its reliance on an MESNN and the optimized parameters determined by SMA, enabling it to efficiently classify and detect attacks across different conditions, even as the threat landscape evolves. This robust and scalable model empowers the process for maintaining its performance in safeguarding CPS, making it a useful tool for addressing security problems in real-world deployments.

V. CONCLUSION

In this manuscript, we have derived a novel ATD-FSAODL algorithm for the automated recognition and classification of threats from the CPS platform. The ATD-FSAODL technique aims to exploit feature selection and classification processes for automated threat detection. To accomplish this, the ATD-FSAODL technique incorporates FSA-based feature subset selection, MESNN-based classification, and SMA-based parameter tuning. In this work, the SMA is used for the optimal selection of the parameters related to the MESNN approach to ensure that the threat detection rate is improved. For estimating the solution of the ATD-FSAODL technique, a sequence of simulations is performed on the benchmark database. The simulation values portray the capable outcome of the ATD-FSAODL methodology with other approaches with a maximum accuracy of 99.58%, precision of 99.58%, recall of 99.58%, F-score of 99.58%, and MCC of 99.16%. In the future, outlier detection outcomes will be involved to better the rate of detection of the ATD-FSAODL system. In real-world deployment, the ATD-FSAODL approach can face challenges connected to data diversity and acquisition approaches, as CPS environments are extremely heterogeneous. Adapting to many data sources, formats, and quality levels but preserving consistent attack detection solutions is a vital challenge. Furthermore, the computational resources needed for DL approaches like MESNN, may pose limitations in resource-constrained CPS. Additionally, these method capabilities for addressing zero-day threats and novel attack vectors require continual monitoring and updates. However, by addressing these problems and acknowledging their limitations, the ATD-FSAODL algorithm is refined to offer a widespread and adaptable solution to secure difficult CPS ecosystems.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/ 159 /44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R114), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. We Would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444). This study is partially funded by the Future University in Egypt (FUE).

REFERENCES

[1] P. Ramadevi, K. N. Baluprithviraj, V. A. Pillai, and K. Subramaniam, "Deep learning based distributed intrusion detection in secure cyber physical systems," *Intell. Autom. Soft Comput.*, vol. 34, no. 3, pp. 2067–2081, 2022.

[2] X. Zhou, W. Liang, S. Shimizu, J. Ma, and Q. Jin, "Siamese neural network based few-shot learning for anomaly detection in industrial cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5790–5798, Aug. 2021.
[3] 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.
[4] A. Kamble and V. S. Malemath, "Adam improved rider optimization-based deep recurrent neural network for the intrusion detection in cyber physical systems," *Int. J. Swarm Intell. Res.*, vol. 13, no. 3, pp. 1–22, Jul. 2022.
[5] G. Kamdem De Teyou and J. Ziazet, "Convolutional neural network for intrusion detection system in cyber physical systems," 2019, *arXiv:1905.03168*.
[6] S. M. Nagarajan, G. G. Deverajan, A. K. Bashir, R. P. Mahapatra, and M. S. Al-Numay, "IADF-CPS: Intelligent anomaly detection framework towards cyber physical systems," *Comput. Commun.*, vol. 188, pp. 81–89, Apr. 2022.
[7] J. Goh, S. Adepu, M. Tan, and Z. S. Lee, "Anomaly detection in cyber physical systems using recurrent neural networks," in *Proc. IEEE 18th Int. Symp. High Assurance Syst. Eng. (HASE)*, Jan. 2017, pp. 140–145.
[8] D. Wu, H. Zhu, Y. Zhu, V. Chang, C. He, C.-H. Hsu, H. Wang, S. Feng, L. Tian, and Z. Huang, "Anomaly detection based on RBM-LSTM neural network for CPS in advanced driver assistance system," *ACM Trans. Cyber-Physical Syst.*, vol. 4, no. 3, pp. 1–17, Jul. 2020.
[9] F. S. Mozaffari, H. Karimipour, and R. M. Parizi, "Learning based anomaly detection in critical cyber-physical systems," in *Security of Cyber-Physical Systems*. 2020, pp. 107–130.
[10] Z. Sun and J. Li, "Anomaly detection for CPS via memory-augmented reconstruction and time series prediction," in *Proc. IEEE 19th Int. Conf. Mobile Ad Hoc Smart Syst. (MASS)*, Oct. 2022, pp. 530–536.
[11] V. Ravi, T. D. Pham, and M. Alazab, "Attention-based multidimensional deep learning approach for cross-architecture IoMT malware detection and classification in healthcare cyber-physical systems," *IEEE Trans. Computat. Social Syst.*, vol. 10, no. 14, pp. 1597–1606, Aug. 2023.
[12] A. M. Hilal, S. Al-Otaibi, H. Mahgoub, F. N. Al-Wesabi, G. Aldehim, A. Motwakel, M. Rizwanullah, and I. Yaseen, "Deep learning enabled class imbalance with sand piper optimization based intrusion detection for secure cyber physical systems," *Cluster Comput.*, vol. 26, no. 3, pp. 2085–2098, Jun. 2023.
[13] Q. Lin, R. Ming, K. Zhang, and H. Luo, "Privacy-enhanced intrusion detection and defense for cyber-physical systems: A deep reinforcement learning approach," *Secur. Commun. Netw.*, vol. 2022, pp. 1–9, Oct. 2022.
[14] A. Sharma, S. Rani, S. H. Shah, R. Sharma, F. Yu, and M. M. Hassan, "An efficient hybrid deep learning model for denial of service detection in cyber physical systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2419–2428, Sep./Oct. 2023.
[15] A. E. Ibor, O. B. Okunoye, F. A. Oladeji, and K. A. Abdulsalam, "Novel hybrid model for intrusion prediction on cyber physical systems' communication networks based on bio-inspired deep neural network structure," *J. Inf. Secur. Appl.*, vol. 65, Mar. 2022, Art. no. 103107.
[16] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021.
[17] M. Umer, S. Sadiq, H. Karamti, R. M. Alhebshi, K. Alnowaiser, A. A. Eshmawi, H. Song, and I. Ashraf, "Deep learning-based intrusion detection methods in cyber-physical systems: Challenges and future trends," *Electronics*, vol. 11, no. 20, p. 3326, Oct. 2022.
[18] S. Thakur, A. Chakraborty, R. De, N. Kumar, and R. Sarkar, "Intrusion detection in cyber-physical systems using a generic and domain specific deep autoencoder model," *Comput. Electr. Eng.*, vol. 91, May 2021, Art. no. 107044.
[19] Z. Wang, Z. Li, D. He, and S. Chan, "A lightweight approach for network intrusion detection in industrial cyber-physical systems based on knowledge distillation and deep metric learning," *Exp. Syst. Appl.*, vol. 206, Nov. 2022, Art. no. 117671.
[20] L. Almutairi, R. Daniel, S. Khasimbee, E. L. Lydia, S. Acharya, and H.-I. Kim, "Quantum dwarf mongoose optimization with ensemble deep learning based intrusion detection in cyber-physical systems," *IEEE Access*, vol. 11, pp. 66828–66837, 2023.
[21] M. A. Duhayyim, K. A. Alissa, F. S. Alrayes, S. S. Alotaibi, E. M. T. El Din, A. A. Abdelmageed, I. Yaseen, and A. Motwakel, "Evolutionary-based deep stacked autoencoder for intrusion detection in a cloud-based cyber-physical system," *Appl. Sci.*, vol. 12, no. 14, p. 6875, Jul. 2022.
[22] V. Vijaypriya and M. Uma, "Facial feature-based drowsiness detection with multi-scale convolutional neural network," *IEEE Access*, vol. 11, pp. 63417–63429, 2023.
[23] N. A. S. Al-Jamali and H. S. Al-Raweshidy, "Modified Elman spike neural network for identification and control of dynamic system," *IEEE Access*, vol. 8, pp. 61246–61254, 2020.
[24] C. Peng, Z. Che, T. W. Liao, and Z. Zhang, "Prediction using multi-objective slime mould algorithm optimized support vector regression model," *Appl. Soft Comput.*, vol. 145, Sep. 2023, Art. no. 110580.