





Article

A White Shark Equilibrium Optimizer with a Hybrid Deep-Learning-Based Cybersecurity Solution for a Smart City Environment

Latifah Almuqren ¹, Sumayh S. Aljameel ² , Hamed Alqahtani ³ , Saud S. Alotaibi ⁴ , Manar Ahmed Hamza ^{5,*} and Ahmed S. Salama ⁶ 

¹ Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

² SAUDI ARAMCO Cybersecurity Chair, Computer Science Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia

³ Department of Information Systems, College of Computer Science, Unit of Cybersecurity, King Khalid University, Abha 61421, Saudi Arabia

⁴ Department of Information Systems, College of Computing and Information System, Umm Al-Qura University, Mecca 24382, Saudi Arabia

⁵ Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam Bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia

⁶ Department of Electrical Engineering, Faculty of Engineering & Technology, Future University in Egypt, New Cairo 11845, Egypt; a.salama@fue.edu.eg

* Correspondence: ma.hamza@psau.edu.sa

Abstract: Smart grids (SGs) play a vital role in the smart city environment, which exploits digital technology, communication systems, and automation for effectively managing electricity generation, distribution, and consumption. SGs are a fundamental module of smart cities that purpose to leverage technology and data for enhancing the life quality for citizens and optimize resource consumption. The biggest challenge in dealing with SGs and smart cities is the potential for cyberattacks comprising Distributed Denial of Service (DDoS) attacks. DDoS attacks involve overwhelming a system with a huge volume of traffic, causing disruptions and potentially leading to service outages. Mitigating and detecting DDoS attacks in SGs is of great significance to ensuring their stability and reliability. Therefore, this study develops a new White Shark Equilibrium Optimizer with a Hybrid Deep-Learning-based Cybersecurity Solution (WSEO-HDLCS) technique for a Smart City Environment. The goal of the WSEO-HDLCS technique is to recognize the presence of DDoS attacks, in order to ensure cybersecurity. In the presented WSEO-HDLCS technique, the high-dimensionality data problem can be resolved by the use of WSEO-based feature selection (WSEO-FS) approach. In addition, the WSEO-HDLCS technique employs a stacked deep autoencoder (SDAE) model for DDoS attack detection. Moreover, the gravitational search algorithm (GSA) is utilized for the optimal selection of the hyperparameters related to the SDAE model. The simulation outcome of the WSEO-HDLCS system is validated on the CICIDS-2017 dataset. The widespread simulation values highlighted the promising outcome of the WSEO-HDLCS methodology over existing methods.

Keywords: smart grids; DDoS attacks; cybersecurity; feature selection; deep autoencoder; smart cities



Citation: Almuqren, L.; Aljameel, S.S.; Alqahtani, H.; Alotaibi, S.S.; Hamza, M.A.; Salama, A.S. A White Shark Equilibrium Optimizer with a Hybrid Deep-Learning-Based Cybersecurity Solution for a Smart City Environment. *Sensors* **2023**, *23*, 7370. <https://doi.org/10.3390/s23177370>

Academic Editor: Maurizio Mongelli

Received: 23 July 2023

Revised: 14 August 2023

Accepted: 15 August 2023

Published: 24 August 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Smart grids (SGs) are an evolving technology, which provides intelligent monitoring, inters connectivity of multiple modes of generation, two-way data transmission, and improved resource utilization [1]. By raising the number of connected devices, it is tedious for the SG to access the distributed network. Therefore, the Internet of Things (IoT) is being

used in the energy sector to enable bidirectional data transmission [2]. It involves the deployment of sensors, actuators, Radio-frequency Identification (RFID), and microcontrollers for communication and computation, to accomplish a two-way communication process [3]. If IoT is combined with SGs, it creates a widespread network of a cyber-physical system, which can be used to monitor and control connected devices remotely. Several countries have already implemented this technology, but approaches to implementation might differ based on the goals and policies of a country [4,5].

The interconnection of several devices from the domestic to the commercial level creates a communication network in the SGs. The physical component includes highly predictable, less technical, and few challenging issues, because of tedious human access and organized maintenance intervening with the faults instigated by material and equipment damage. At the same time, the challenging issues posed by the cyber network are highly complex, recurrent, and less predictable. Therefore, cyber-security has been regarded as a major power industry security target [6]. Cyber security in SGs is needed, as the embedded and general-purpose systems linked to it should be secure from cyber-attacks. Utilities need to ensure that cybersecurity in SGs for preserving the massive data flow and control signals indispensable to the SG for reaping the operational benefits derived from its implementation [7]. As SGs are a critical national infrastructure, cybersecurity in SGs should manage every possible threat from user errors and equipment failures.

Intrusion Detection is a technique for detecting attacks before or after they attain access to a security network. Integrating this method as to gateway is the fastest manner to combine it [8]. Deep Learning (DL), data mining, Machine Learning (ML), fuzzy logic (FL), evolutionary techniques, and other related approaches are comprised in Artificial Intelligence (AI). ML has become increasingly significant to researchers for risk recognition [9]. Researchers have utilized ML techniques, namely neural networks (NNs), support vector machines (SVMs), and random forests (RFs), for identifying jamming attacks. Researchers have used the ML approach for detecting social engineering attacks [7]. This method employs unsupervised learning; hence, it does not need that used for cyber-attacks in order to detect them.

This study develops a new White Shark Equilibrium Optimizer with a Hybrid Deep-Learning-based Cybersecurity Solution (WSEO-HDLCS) technique for a Smart City Environment. The goal of the WSEO-HDLCS technique is to recognize the presence of DDoS attacks, in order to ensure cybersecurity. In the presented WSEO-HDLCS technique, the high-dimensionality data problem can be resolved by the use of a WSEO-based feature selection (WSEO-FS) approach. In addition, the WSEO-HDLCS technique employs a stacked deep autoencoder (SDAE) model for DDoS attack detection. Moreover, the gravitational search algorithm (GSA) is utilized for the optimal selection of the hyperparameters related to the SDAE model. The experimental evaluation of the WSEO-HDLCS algorithm is validated on the CICIDS-2017 database. The widespread simulation values highlighted the promising outcome of the WSEO-HDLCS method over existing approaches.

2. Related Works

Ali and Li [10] introduced an effective DDoS attack detection method that depends on multi-level AE-based feature learning. The authors learned of multiple levels of shallow and DAE in unsupervised learning that can be utilized for encoding the trained and test information in feature generation. The ultimate combined identification technique is learned by integrating multiple-level features utilizing an effective multiple kernel learning (MKL) method. Monday et al. [11] proposed a technique for detecting DDoS attacks on the SG framework. Continuous wavelet transform (CWT) has been employed in the proposed method to transform 1D traffic data to a 2D time-frequency domain scalogram as the input to a wavelet CNN (WavCovNet) for detecting anomalous performance, with information by differentiating attack features in standard outlines. Diaba and Elmusrati [12] suggested a hybrid DL approach, which focused on DDoS attacks on the transmission framework of SGs. The recommended technique is hybridized by the GRU and CNN

methods. Nagaraj et al. [13] introduce graph learning techniques to identify and detect DDoS attacks in SDN_SGC systems (GLASS). Network model statistics have been applied to model SDN_SGC graphs that are trained GCN for extracting hidden representations caused by DDoS attacks.

Ebojoh and Yeboah-Ofori [14] introduced an agent-based model of offensive botnet connections in an SG method, and studied the amplification attack strategy of FDIA and DDoS on SGs. Primarily, the authors examine that botnet agent attacks methods utilizing ABS influence collaborative protection in FDIA and DDoS attacks. Secondly, the authors implemented an attack model utilizing the GAMA tool for determining offensive botnet interactions within an SG system. Lastly, the authors suggested control methods for preventing offensive botnets on the SG network. In [15], a model that depends on ML to identify SG DDoS attacks was suggested. The model initially gathers network information, then FS, applies PCA for reducing the data size and, lastly, utilizes the SVM approach to detect the abnormality.

Ma et al. [16] recommended an innovative DDoS attack identification technique that only applies unlabeled abnormal network traffic information to make the recognition system. This approach primarily utilizes the Balanced Iterative Reducing and Clustering utilizing the Hierarchies technique (BIRCH) for pre-clustering the anomalous network traffic data and, after examining AE, to make the identification method in unsupervised learning depends on clustering subsets. Khoei et al. [17] present a CNN-based approach, a ResNet with 50 layers. In this method, the tabular information is modified to images for enhancing the model performance.

3. The Proposed Model

In this study, we have designed and developed a WSEO-HDLCS methodology for cybersecurity in an SG environment. The major purpose of the WSEO-HDLCS system is to recognize the presence of DDoS attacks, in order to ensure cybersecurity. In the proposed WSEO-HDLCS system, three main sub-processes are contained in the WSEO-FS technique, SDAE-based classification, and GSA-based hyperparameter selection. Figure 1 exemplifies the overall flow of the WSEO-HDLCS method.

3.1. Design of WSEO-FS Technique

To choose a subset of features, the WSEO-FS technique is used. The WESO algorithm is derived by the use of a White Shark Optimizer (WSO) with an equilibrium optimizer (EO) [18]. In this work, the EO was used to increase the population of the worse solution and improve the WSO's searching abilities. Due to its higher performance, the EO is applied to deeply search in the rugged search space by maintaining the balance among local as well as global searches. The study implements the EO to improve the worse solution by arranging the population and allowing for the second half as its population. The EO enhances the worse half of the population and returns it to the WSO for re-evaluating the population and selecting the better solution.

Initialization of parameters *WSO* and *EO*: This step is used for initializing the *WSO* and *EO* parameters. For *EO*, the parameters are *GP* and *V*. For the *WSO*, the parameters are *v*, *u*, *l*, τ , f_{\min} , f_{\min} , p_{\min} , and p_{\max} .

Initially, the initial population is produced. The population is randomly produced similar to other swarm-based optimizers, which consider the starting time *st* and the number of SAs (*m*).

$$Population = \begin{bmatrix} st_1^1 & st_1^2 & \dots & st_m^1 \\ st_2^1 & st_2^2 & \dots & st_m^2 \\ \vdots & \vdots & \dots & \vdots \\ st_1^N & st_2^N & \dots & st_m^N \end{bmatrix}, \quad (1)$$

Next, the fitness value (FV) of the solution is assessed. Consequently, the *WSO* assigned the fittest outcome with the best values to $\omega_{g_{best}}$. The searching agent of the *WSO*

is used for updating the solution from the population and searching for the best schedule for the FS. Once it evaluates the FV for each solution from the population and allocates the fittest outcome to $\omega_{g_{best}}$, the WSO operation can upgrade and produce novel solutions based on the $\omega_{g_{best}}$. If they have optimum FV, then a new solution will replace the worst solution. Next, based on the FV, the solution from the population was ranked, where the best solution was highly ranked, and the worst solution was lowly ranked. After ranking the solution, the EO takes the solution with the low rank from the WSO population for additional improvement. The low-ranking solution is utilized as an initial population for the EO. The EO allocates the fittest four solutions to $\vec{C}_{eq(1)}$, $\vec{C}_{eq(2)}$, $\vec{C}_{eq(3)}$, and $\vec{C}_{eq(4)}$ for generating $\vec{C}_{eq.pool}$. Consequently, the EO updates the population to enhance the FV and search for the best schedule. Consequently, the EO returns the novel solution to the WSO population. The fitness function (FF) assumes the classifier accuracy and the FS counts. It maximizes the classifier accuracy and minimizes the fixed size of FSs. Then, the following FF can be employed for measuring individual performances, as expressed in Equation (2).

$$Fitness = \alpha * ErrorRate + (1 - \alpha) * \frac{\#SF}{\#All_F} \quad (2)$$

whereas *ErrorRate* stands for the classifier rate of errors employing the FSs. *ErrorRate* denotes the measured percentage of incorrect classification to the count of classifiers made, expressed as a value among zero and one. *#SF* refers to the count of FSs and *#All_F* denotes the entire count of elements from the original database. α is utilized for controlling the impact of classifier quality and subset length.

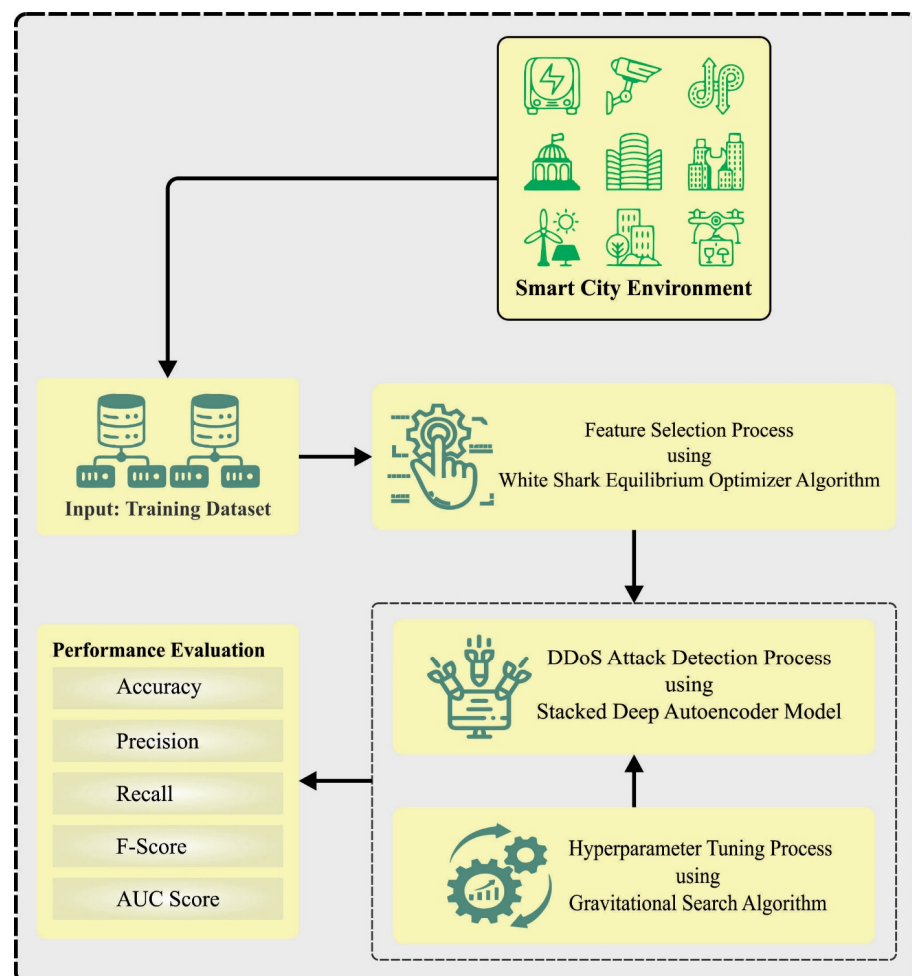


Figure 1. Overall flow of WSEO-HDLCS system.

3.2. Design of SDAE Classifier

For the identification of DDoS attacks, the SADE model is applied. In DAE, any trained parameters can be employed and written as the input vector $x_i(1, 2, \dots, N)$ and as the hidden state h_i [19]. An input vector calculates x_i and a joint probability distribution function of h_i . It can be employed as the matrix weighted on the primary phase. Figure 2 portrays the infrastructure of SDAE. The estimate of the probability distribution function is provided as:

$$p(h_i = 1|x) = \sigma\left(b_i + \sum_j w_{ij}x_i\right) \quad (3)$$

whereas σ denotes the sigmoid function. The sigmoid function was determined as:

$$\sigma = \frac{1}{1 + e^{-z}} \quad (4)$$

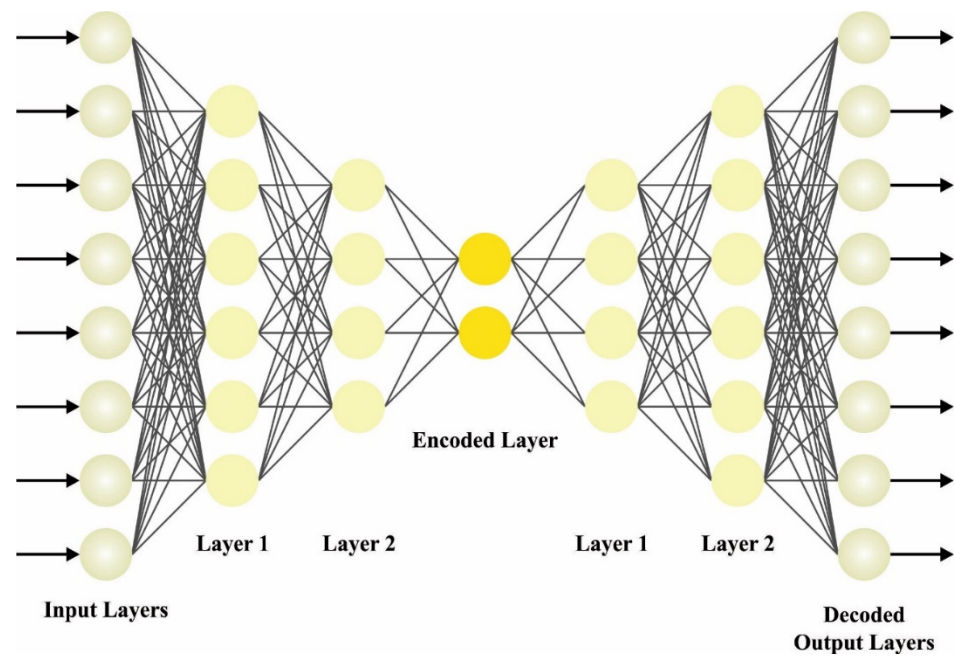


Figure 2. Architecture of SDAE.

The input data to a network can be provided as z , and the resultant data of the network are provided as $h_{w,b}(z)$, and $w_{ij}(i, j = 1, 2, \dots, N)$ signifies the primary weighted data. An input data point z can be stimulated using the mapping function to offer m_f as:

$$mf = \text{sigm}(w_i z + b_i) \quad (5)$$

in which *sigm* refers to the activation function, recognized as a sigmoid function:

$$\text{sigm} = \frac{1}{1 + e^{-z}} \quad (6)$$

The reconstructed signal in the decoded phase is expressed as:

$$\hat{x}_i = h_{w,d}(z) = g(w_i^t m_f + b_{i+1}) \quad (7)$$

The abovementioned formula, the weighted matrix and bias amongst the states (hidden and output) are defined as w and b .

The resultant features X attained later, and the decoded and the input data x attained before the encoded features, are the most important conditions of AE, and where the error appeared, reconstruction is provided by probability function:

$$l(x, \hat{x}) = \frac{1}{2} |x_i - \hat{x}_i|^2 \quad (8)$$

SDAE contains several layers of encoded and decoded features, generating a deeper network. All layers of the encoded features decrease the data size, and all the layers of decoded features gradually reform the data back to its original size. The intermediate layer procedure is the compressed representations, and it develops gradually towards abstraction as it keeps moving deeper into a network.

The training of a SDAE is normally performed in a layer-by-layer method. It contains all the layers trained separately as AEs first. If the lower layers can be trained, they can be integrated as a single network and more fine-tuned as an end-to-end method.

3.3. Process Involved in GSA-Based Hyperparameter Tuning

Finally, the hyperparameters of the GSA model can be chosen by the use of GSAs. The GSA is inspired by the optimization strategy improved by the law of gravity [20]. In this technique, particles represent the object, while masses are used for the performance measurement. The particles communicated by using the laws of action and Newton's law of gravity. Consider a solution that contains N particles (masses).

$$x_i = (x_i^1, \dots, x_i^d, \dots, x_i^D) \text{ for } i = 1, 2, 3, \dots, n \quad (9)$$

In Equation (9), x_i^d indicates the position of particle i at d dimension, and D denotes the overall amount of dimensions. All the performances of the particles are defined by the mass and measured by a vigor process. The gravity and inertial masses of each particle were modernized and equalized with all the iterations:

$$M_{ai} = M_{pi} = M_{ii} = M_i \quad (10)$$

$$m_i = \frac{fit_i - worst}{best - worst} \quad (11)$$

$$M_i = \frac{m_i}{\sum_{j=1}^N m_j} \quad (12)$$

where fit_i shows the i^{th} particle FV, and $best$ and $worst$ denotes the particles' highest and lowest fitness scores.

Maximization challenges are characterized as follows:

$$best = \max_{j \in \{1, \dots, N\}} fit_j \quad (13)$$

$$worst = \min_{j \in \{1, \dots, N\}} fit_j \quad (14)$$

Considering the reducing issues, which are different and are evaluated as follows:

$$best = \min_{j \in \{1, \dots, N\}} fit_j \quad (15)$$

$$worst = \max_{j \in \{1, \dots, N\}} fit_j \quad (16)$$

The gravity F_{ij}^d exerted on i^{th} particles from j^{th} particles is computed using Equation (17):

$$F_{ij}^d = G \frac{M_{pi} \times M_{aj}}{R_{ij} + \varepsilon} \times (x_j^d - x_i^d) \quad (17)$$

where M_{aj} shows the kinetic gravity energy of j^{th} particles and M_{pi} is the sedentary gravity potential of i^{th} particles. ε denotes the teeny invariant. G is designated the gravity acceleration. R_{ij} shows the Euclidean space within two particles,

$$G = G_0 e^{-\alpha \frac{t}{T}} \quad (18)$$

In Equation (18), G_0 and α are adjusted initially and gradually decreased to control the search accuracy, T shows the max iteration. The force used on i^{th} particles in d size is a random weight matrix of other gravitational forces of the particles.

$$F_i^d = \sum_{j \in Kbest, j \neq i} rrand_j F_{ij}^d \quad (19)$$

where $rrand_j$ shows the constant random parameter within $[0, 1]$. During the search process, keeping equilibrium is crucial to avoid becoming trapped in the local optimal and to strike the symmetry within exploitation and exploration. Solely, particles $Kbest$ with the most important fitness weights are used to have a gravitational attraction on another particle.

$$Kbest = N \times \frac{per + (1 - \frac{t}{T}) \times (100 - per)}{100} \quad (20)$$

where per represents the particles' proportion that efficiently contributes towards different particles in the final analysis. The rate of i^{th} particles in d size at t iteration can be defined as follows:

$$a_i^d = \frac{F_i^d}{M_{ii}} \quad (21)$$

Now, M_{ii} shows inertial mass of the i^{th} particles. The velocity of the particle at d dimension is the proportion of current speed and velocity.

$$v_i^d = rand_i \times v_i^d + a_i^d \quad (22)$$

Now, $rand_i$ denotes the invariant arbitrary variable within $[0, 1]$ and provides the search for the random characteristic. In addition, the following equations evaluate the next location of the particles in dimension d .

$$x_i^d = x_i^d + v_i^d \quad (23)$$

Fitness choice is a key aspect of the GSA system. Solution encoding can be utilized to assess a better solution for candidate performances. In this work, maximum accuracy can be considered as the fitness function, as given below.

$$Fitness = \max(P) \quad (24)$$

$$P = \frac{TP}{TP + FP} \quad (25)$$

in which FP and TP imply the false and true positive values.

4. Results Analysis

In this study, the DDoS attack detection performance can be validated using the CICIDS-2017 dataset [21]. It holds 113,270 samples with two classes, as represented in Table 1.

Table 1. Description of database.

Class	No. of Samples
BENIGN	67,343
DDoS	45,927
Total Samples	113,270

Figure 3 reveals the classifier outcome of the WSEO-HDLCS algorithm on the test dataset. Figure 3a portrays the confusion matrix attained by the WSEO-HDLCS system on 80% of the TR set. The outcome inferred that the WSEO-HDLCS system has recognized 53,244 instances under the benign class and 35,420 instances under the DDoS class. Moreover, Figure 3b exemplifies the confusion matrix attained by the WSEO-HDLCS system on 20% of the TS set. The results signified that the WSEO-HDLCS methodology has recognized 13,282 instances under the benign class and 8927 instances under the DDoS class. Following this, Figure 3c represents the PR curve of the WSEO-HDLCS system. The outcome inferred that the WSEO-HDLCS system has achieved greater PR outcomes in two classes. But Figure 3d displays the ROC curve of the WSEO-HDLCS system. The result outperformed that the WSEO-HDLCS approach has led to capable performances with enhanced ROC values on two class labels.

Table 2 represents the DDoS attack detection results of the WSEO-HDLCS technique. Figure 4 inspects the overall results of the WSEO-HDLCS technique with 80% of the TR set. The outcomes inferred that the WSEO-HDLCS technique reaches enhanced identification of attacks. With the benign class, the WSEO-HDLCS technique offers $accu_y$, $prec_n$, $reca_l$, F_{score} , and AUC_{score} values of 97.85%, 97.66%, 98.74%, 98.20%, and 97.64%, respectively. Additionally, with the DDoS class, the WSEO-HDLCS approach attains $accu_y$, $prec_n$, $reca_l$, F_{score} , and AUC_{score} values of 97.85%, 98.12%, 96.53%, 97.32%, and 97.64%, respectively.

Figure 5 examines the overall outcomes of the WSEO-HDLCS methodology with 20% of the TS set. The outcome inferred that the WSEO-HDLCS algorithm gains improved recognition of attacks. With the benign class, the WSEO-HDLCS methodology provides $accu_y$, $prec_n$, $reca_l$, F_{score} , and AUC_{score} values of 98.04%, 97.75%, 98.96%, 98.35%, and 97.83%, respectively. Moreover, with the DDoS class, the WSEO-HDLCS methodology achieves $accu_y$, $prec_n$, $reca_l$, F_{score} , and AUC_{score} values of 98.04%, 98.47%, 96.69%, 97.57%, and 97.83%, respectively.

Table 2. DDoS attack detection outcome of WSEO-HDLCS approach on 80% of TR set/20% of TS set.

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	AUC_{Score}
Training Phase (80%)					
Benign	97.85	97.66	98.74	98.20	97.64
DDoS	97.85	98.12	96.53	97.32	97.64
Average	97.85	97.89	97.64	97.76	97.64
Testing Phase (20%)					
Benign	98.04	97.75	98.96	98.35	97.83
DDoS	98.04	98.47	96.69	97.57	97.83
Average	98.04	98.11	97.83	97.96	97.83

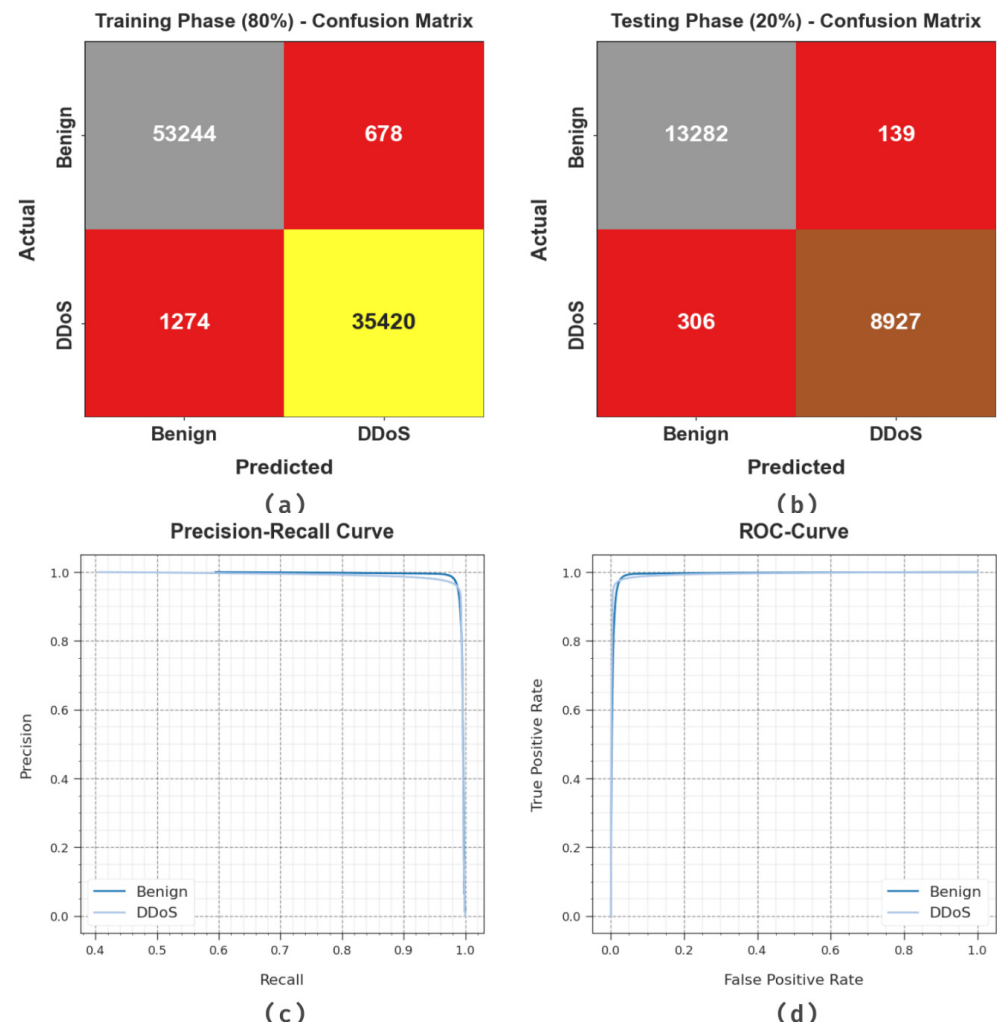


Figure 3. Performance of (a,b) 80% of TR set/20% of TS set, (c) PR_curve, and (d) ROC_curve.

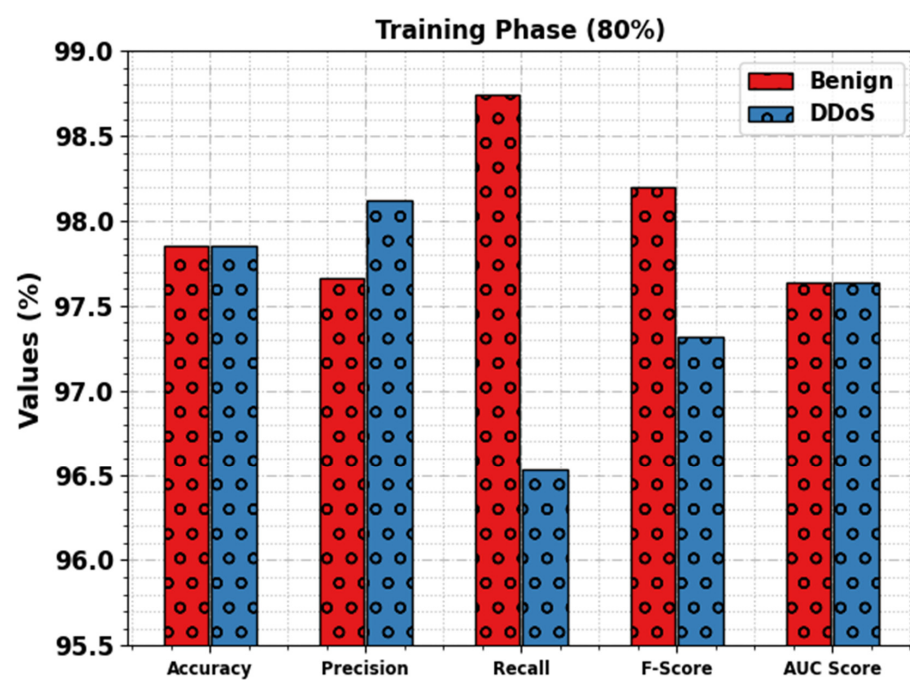


Figure 4. DDoS attack detection outcomes of WSEO-HDLCS approach on 80% of TR set.

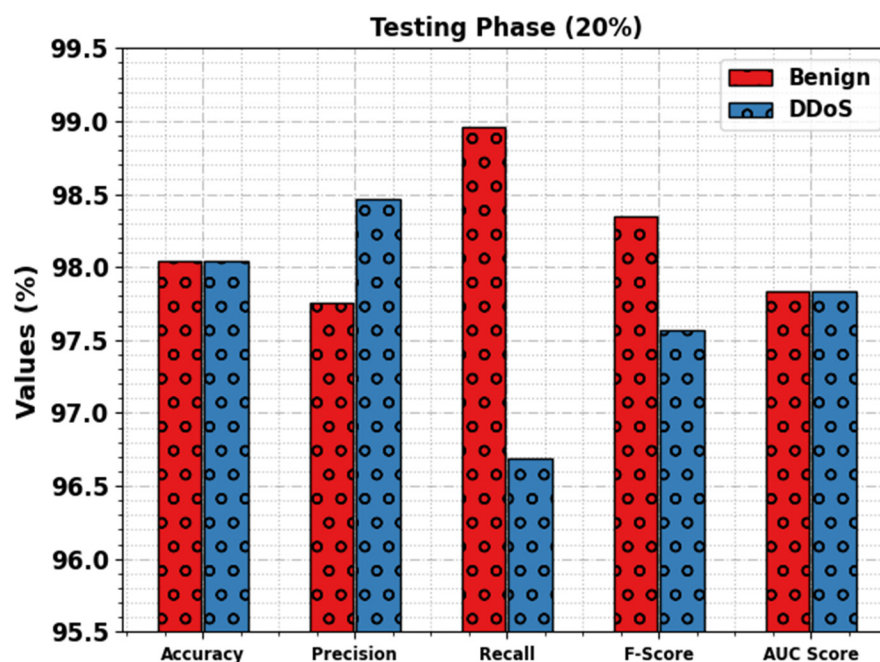


Figure 5. DDoS attack detection outcomes of WSEO-HDLCS approach on 20% of TS set.

Figure 6 inspects the overall average result of the WSEO-HDLCS algorithm with 80% of the TR set and 20% of the TS set. The simulation outcome denoted that the WSEO-HDLCS system gains greater detection of attacks. On 80% of the TR set, the WSEO-HDLCS method achieves average $accu_y$, $prec_n$, $recal$, F_{score} , and AUC_{score} values of 97.85%, 97.89%, 97.64%, 97.76%, and 97.64%, respectively. On 20% of TS set, the WSEO-HDLCS algorithm reaches average $accu_y$, $prec_n$, $recal$, F_{score} , and AUC_{score} values of 98.04%, 98.11%, 97.83%, 97.96%, and 97.83%, respectively.

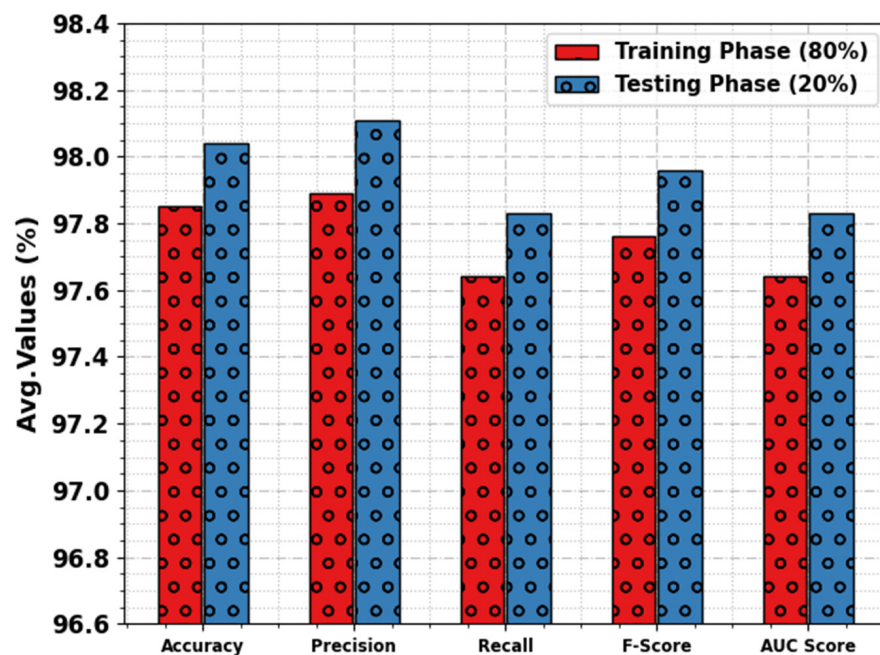


Figure 6. Average outcome of WSEO-HDLCS approach on 80% of TR set/20% of TS set.

Figure 7 illustrates the training accuracy TR_{accu_y} and VL_{accu_y} of the WSEO-HDLCS approach. The TR_{accu_y} is defined by the assessment of the WSEO-HDLCS system on the TR dataset, whereas the VL_{accu_y} is calculated by estimating the solution on a separate

testing dataset. The outcomes display that TR_accu_y and VL_accu_y enhance with an increase in epochs. Thus, the outcome the WSEO-HDLCS system obtains is greater on the TR and TS dataset with a rise in the count of epochs.

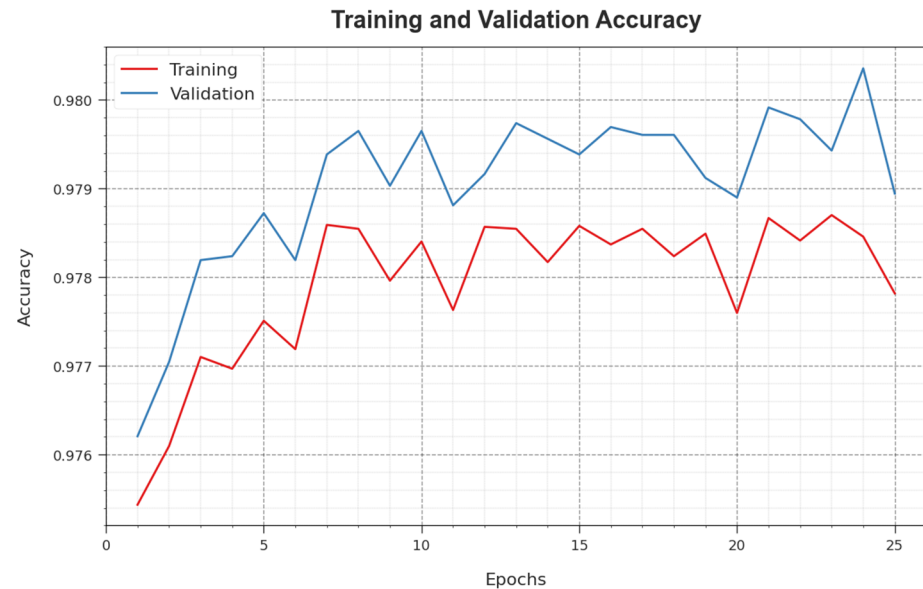


Figure 7. $Accu_y$ curve of the WSEO-HDLCS approach.

In Figure 8, the TR_loss and VR_loss curves of the WSEO-HDLCS system are exposed. The TR_loss demonstrates the error among the predictive solution and original values on the TR data. The VR_loss signifies the evaluation of the performance of the WSEO-HDLCS technique on individual validation data. The outcomes point out that the TR_loss and VR_loss tend to be less with increasing epochs. It represented the improved solution of the WSEO-HDLCS technique and its ability to produce an accurate classification. The minimal value of TR_loss and VR_loss reveals the improved outcome of the WSEO-HDLCS method on capturing patterns and relationships.



Figure 8. Loss curve of the WSEO-HDLCS approach.

A comprehensive PR analysis of the WSEO-HDLCS algorithm is depicted on the test database in Figure 9. The simulation outcome inferred that the WSEO-HDLCS system

outcomes enhanced the values of PR. Furthermore, it could be noticed that the WSEO-HDLCS algorithm attains greater PR values on two classes.

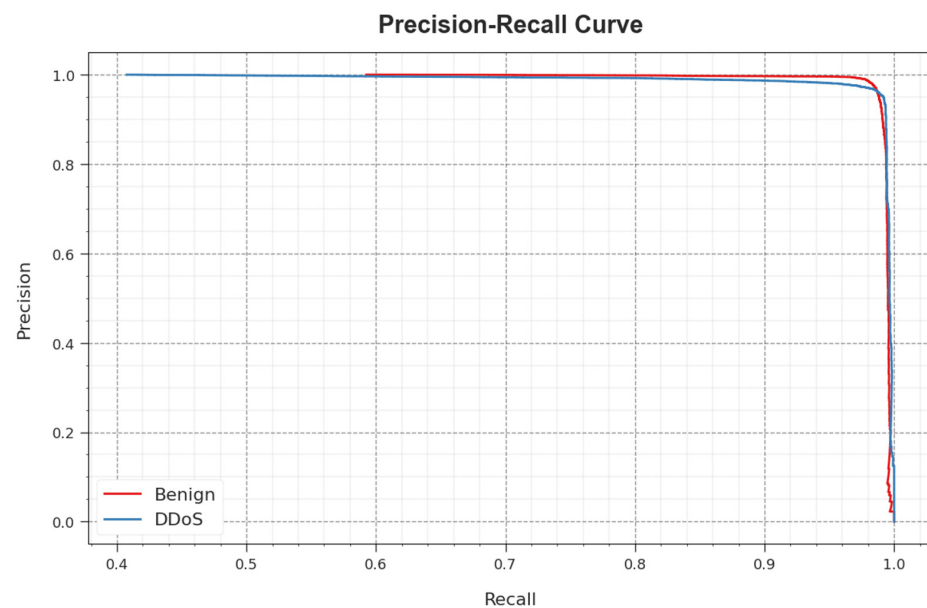


Figure 9. PR curve of the WSEO-HDLCS approach.

In Figure 10, a ROC curve for the WSEO-HDLCS methodology on the test database is shown. The simulation value explained that the WSEO-HDLCS system gives rise to increased ROC values. Also, it can be observed that the WSEO-HDLCS algorithm extends greater ROC values on two classes.

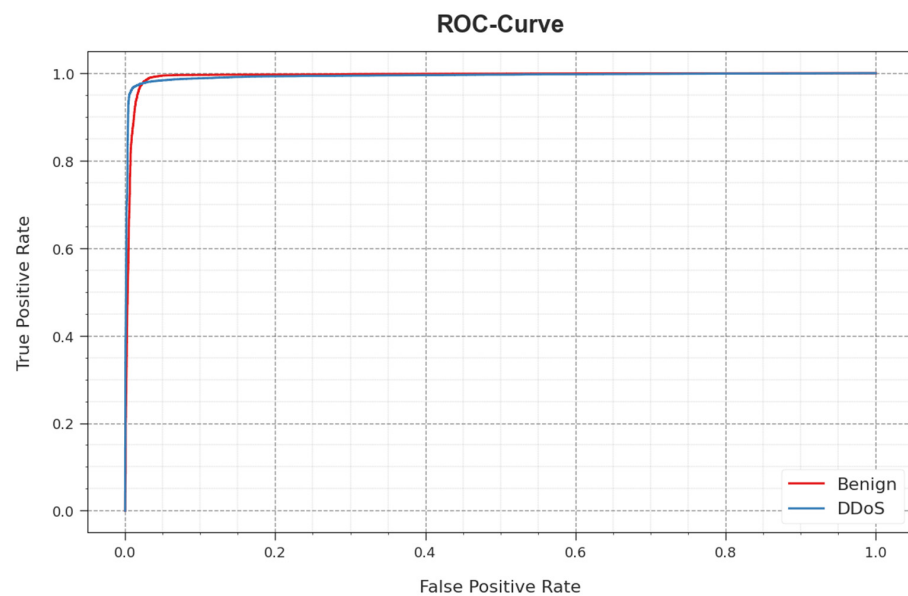
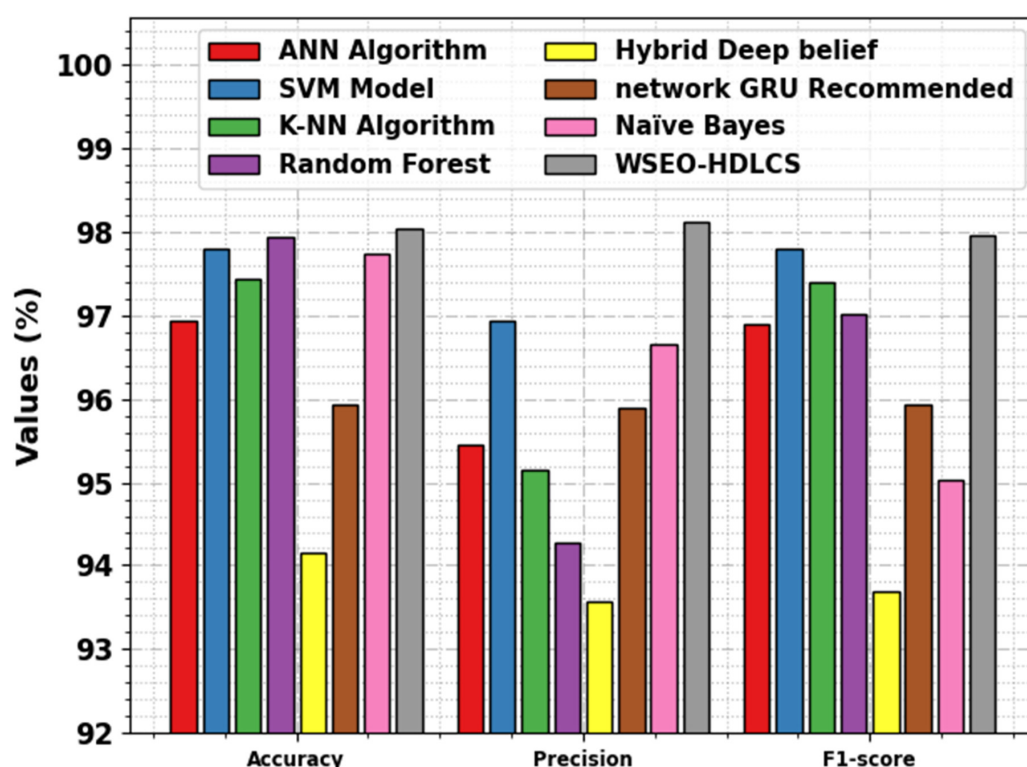


Figure 10. ROC curve of the WSEO-HDLCS algorithm.

Finally, the improved performance of the WSEO-HDLCS technique can be ensured by studying the comparisons in Table 3 and Figure 11 [12,22–24]. The simulation values portrayed that the hybrid deep belief and network GRU-recommended models have shown poor performance. Along with that, the ANN, SVM, KNN, RF, and NB approaches have reported moderate solutions.

Table 3. Comparative outcome of WSEO-HDLCS approach with other methods.

Algorithms	$Accu_y$	$Prec_n$	$F1_{score}$
ANN Algorithm [22]	96.94	95.45	96.90
SVM Model [22]	97.80	96.93	97.80
K-NN Algorithm [22]	97.44	95.16	97.40
Random Forest [22]	97.94	94.28	97.01
Hybrid Deep belief [23]	94.14	93.57	93.68
Network GRU Recommended [12]	95.93	95.89	95.94
Naïve Bayes [24]	97.74	96.65	95.04
WSEO-HDLCS	98.04	98.11	97.96

**Figure 11.** Comparative outcomes of WSEO-HDLCS approach with other methods.

Nevertheless, the WSEO-HDLCS algorithm exhibited superior performance, with a maximum $accu_y$ of 98.04%, $prec_n$ of 98.11%, and F_{score} of 97.96%. These results confirmed that the WSEO-HDLCS technique can identify the DDoS attacks in the SG effectually.

5. Conclusions

In this manuscript, we have designed and established a WSEO-HDLCS algorithm for cybersecurity in the SG environment. The major purpose of the WSEO-HDLCS technique is to recognize the presence of DDoS attacks, in order to ensure cybersecurity. In the proposed WSEO-HDLCS system, the three main sub-processes contained are the WSEO-FS technique, SDAE-based classification, and GSA-based hyperparameter selection. The GSA is utilized for the optimal selection of the hyperparameters related to the SDAE model. The simulation value of the WSEO-HDLCS system was validated on the CICIDS-2017 database. The widespread simulation outcome highlighted the promising solution of the WSEO-HDLCS approach, compared to other methods. The proposed model offers various benefits in real-time applications, such as enhanced network resilience, reduced downtime, less service disruptions, reduced economic loss, effective resource utilization, and resilience

against evolving threats. In future, the adaptability of the proposed model can be improved on evolving attacks using ensemble models. Additionally, real-time monitoring can be developed for the detection of DDoS attacks promptly. In addition, automated systems can trigger alarms or mitigation actions when suspicious traffic patterns are detected. Finally, flow-based monitoring and analysis approaches can be developed to gain insights into traffic flows, recognize suspicious activity, and isolate the sources of DDoS attacks.

Author Contributions: Conceptualization, L.A. and H.A.; methodology, S.S.A. (Sumayh S. Aljameel), H.A. and M.A.H.; software, A.S.S.; validation, L.A., M.A.H. and H.A.; formal analysis, A.S.S.; investigation, L.A.; resources, M.A.H.; data curation, S.S.A. (Sumayh S. Aljameel); writing—original draft preparation, L.A., S.S.A. (Sumayh S. Aljameel), H.A., S.S.A. (Saud S. Alotaibi) and M.A.H. writing—review and editing, S.S.A. (Saud S. Alotaibi), A.S.S., S.S.A. (Sumayh S. Aljameel) and H.A.; visualization, M.A.H.; supervision, L.A.; project administration, M.A.H.; funding acquisition, L.A., S.S.A. (Sumayh S. Aljameel) and H.A. All authors have read and agreed to the published version of the manuscript.

Funding: 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 (PNURSP2023R349), 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).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing is not applicable to this article, as no datasets were generated during the current study.

Conflicts of Interest: The authors declare that they have no conflict of interest. The manuscript was written with contributions by all authors. All authors have given their approval to the final version of the manuscript.

References

1. Habib, A.A.; Hasan, M.K.; Hassan, R.; Islam, S.; Thakkar, R.; Vo, N. Distributed denial-of-service attack detection for smart grid wide area measurement system: A hybrid machine learning technique. *Energy Rep.* **2023**, *9*, 638–646. [\[CrossRef\]](#)
2. Khoei, T.T.; Kaabouch, N. Densely Connected Neural Networks for Detecting Denial of Service Attacks on Smart Grid Network. In Proceedings of the 2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 26–29 October 2022; pp. 207–211.
3. Radoglou Grammatikis, P.; Sarigiannidis, P.; Efstathiopoulos, G.; Panaousis, E. ARIES: A novel multivariate intrusion detection system for smart grid. *Sensors* **2020**, *20*, 5305. [\[CrossRef\]](#) [\[PubMed\]](#)
4. Ortega-Fernandez, I.; Liberati, F. A Review of Denial of Service Attack and Mitigation in the Smart Grid Using Reinforcement Learning. *Energies* **2023**, *16*, 635. [\[CrossRef\]](#)
5. Raja, D.J.S.; Sriranjani, R.; Parvathy, A.; Hemavathi, N. A review on distributed denial of service attack in smart grid. In Proceedings of the 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 22–24 June 2022; pp. 812–819.
6. Hasan, M.K.; Habib, A.A.; Islam, S.; Safie, N.; Abdullah, S.N.H.S.; Pandey, B. DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. *Energy Rep.* **2023**, *9*, 1318–1326. [\[CrossRef\]](#)
7. Meriaux, E.; Koehler, D.; Islam, M.Z.; Vokkarane, V.; Lin, Y. Performance Comparison of Machine Learning Methods in DDoS Attack Detection in Smart Grids. In Proceedings of the 2022 IEEE MIT Undergraduate Research Technology Conference (URTC), Cambridge, MA, USA, 30 September–2 October 2022; pp. 1–5.
8. Huseinović, A.; Mrdović, S.; Bicaćki, K.; Uludag, S. A survey of denial-of-service attacks and solutions in the smart grid. *IEEE Access* **2020**, *8*, 177447–177470. [\[CrossRef\]](#)
9. Aribisala, A.; Khan, M.S.; Husari, G. Machine learning algorithms and their applications in classifying cyber-attacks on a smart grid network. In Proceedings of the 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 27–30 October 2021; pp. 63–69.
10. Ali, S.; Li, Y. Learning multilevel auto-encoders for DDoS attack detection in smart grid network. *IEEE Access* **2019**, *7*, 108647–108659. [\[CrossRef\]](#)

11. Monday, H.N.; Li, J.P.; Nneji, G.U.; Yutra, A.Z.; Lemessa, B.D.; Nahar, S.; James, E.C.; Haq, A.U. The Capability of Wavelet Convolutional Neural Network for Detecting Cyber Attack of Distributed Denial of Service in Smart Grid. In Proceedings of the 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 17–19 December 2021; pp. 413–418.
12. Diaba, S.Y.; Elmusrati, M. Proposed algorithm for smart grid DDoS detection based on deep learning. *Neural Netw.* **2023**, *159*, 175–184. [[CrossRef](#)] [[PubMed](#)]
13. Nagaraj, K.; Starke, A.; McNair, J. Glass: A graph learning approach for software defined network based smart grid ddos security. In Proceedings of the ICC 2021-IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
14. Ebojoh, C.; Yeboah-Ofori, A. Agent Based Simulation of Botnet Volumetric and Amplification Attack Scenarios Applied to Smart Grid Systems. In Proceedings of the 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, UK, 9–11 May 2023; pp. 1–6.
15. Zhe, W.; Wei, C.; Chunlin, L. DoS attack detection model of smart grid based on machine learning method. In Proceedings of the 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS), Shenyang, China, 28–30 July 2020; pp. 735–738.
16. Ma, Z.; Ma, H.; Gao, X.; Gai, J.; Zhang, X.; He, F.; Zhao, J. An Improved DDoS Attack Detection Model Based on Unsupervised Learning in Smart Grid. In *International Conference on Mobile Multimedia Communications*; Springer International Publishing: Cham, Germany, 2021; pp. 550–562.
17. Khoei, T.T.; Hu, W.C.; Kaabouch, N. Residual Convolutional Network for Detecting Attacks on Intrusion Detection Systems in Smart Grid. In Proceedings of the 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, 19–21 May 2022; pp. 231–237.
18. Makhadmeh, S.N.; Al-Betar, M.A.; Assaleh, K.; Kassaymeh, S. A Hybrid White Shark Equilibrium Optimizer for Power Scheduling Problem Based IoT. *IEEE Access* **2022**, *10*, 132212–132231. [[CrossRef](#)]
19. Das, H.S.; Roy, P. Bottleneck feature-based hybrid deep autoencoder approach for Indian language identification. *Arab. J. Sci. Eng.* **2020**, *45*, 3425–3436. [[CrossRef](#)]
20. Ahmad, Z.; Mahmood, T.; Rehman, A.; Saba, T.; Alamri, F.S. Enhancing Time State Networks. *IEEE Access* **2023**, *11*, 79466–79479. [[CrossRef](#)]
21. Available online: <https://www.unb.ca/cic/datasets/ids-2017.html> (accessed on 12 February 2023).
22. Subasi, A.; Al-Marwani, K.; Alghamdi, R.; Kwairanga, A.; Qaisar, S.M.; Al-Nory, M.; Rambo, K.A. Intrusion Detection in Smart Grid Using Data Mining Techniques. In Proceedings of the 2018 21st Saudi Computer Society National Computer Conference, Riyadh, Saudi Arabia, 25–26 April 2018; pp. 1–6.
23. Aldossary, L.A.; Ali, M.; Alasaadi, A. Securing SCADA Systems against Cyber-Attacks using Artificial Intelligence. In Proceedings of the 2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Zallaq, Bahrain, 29–30 September 2021; pp. 739–745.
24. Alhaidari, F.A.; AL-Dahasi, E.M. New Approach to Determine DDoS Attack Patterns on SCADA System Using Machine Learning. In Proceedings of the 2019 International Conference on Computer and Information Sciences, Sakaka, Saudi Arabia, 3–4 April 2019; pp. 1–6.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.