drones

MDPI

Article

Crystal Structure Optimization with Deep-Autoencoder-Based Intrusion Detection for Secure Internet of Drones Environment

Khalid A. Alissa [1], Saud S. Alotaibi [2], Fatma S. Alrayes [3], Mohammed Aljebreen [4], Sana Alazwari [5], Hussain Alshahrani [6], Mohamed Ahmed Elfaki [6], Mahmoud Othman [7] and Abdelwahed Motwakel [8,*]

[1] Saudi Aramco Cybersecurity Chair, Networks and Communications Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia
[2] Department of Information Systems, College of Computing and Information System, Umm Al-Qura University, Mecca 24382, Saudi Arabia
[3] Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[4] Department of Computer Science, Community College, King Saud University, P.O. Box 28095, Riyadh 11437, Saudi Arabia
[5] Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia
[6] Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra 17472, Saudi Arabia
[7] Department of Computer Science, Faculty of Computers and Information Technology, Future University in Egypt, New Cairo 11835, Egypt
[8] Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia
* Correspondence: a.ismaeil@psau.edu.sa

Abstract: Drone developments, especially small-sized drones, usher in novel trends and possibilities in various domains. Drones offer navigational inter-location services with the involvement of the Internet of Things (IoT). On the other hand, drone networks are highly prone to privacy and security risks owing to their strategy flaws. In order to achieve the desired efficiency, it is essential to create a secure network. The purpose of the current study is to have an overview of the privacy and security problems that recently impacted the Internet of Drones (IoD). An Intrusion Detection System (IDS) is an effective approach to determine the presence of intrusions in the IoD environment. The current study focuses on the design of Crystal Structure Optimization with Deep-Autoencoder-based Intrusion Detection (CSODAE-ID) for a secure IoD environment. The aim of the presented CSODAE-ID model is to identify the occurrences of intrusions in IoD environment. In the proposed CSODAE-ID model, a new Modified Deer Hunting Optimization-based Feature Selection (MDHO-FS) technique is applied to choose the feature subsets. At the same time, the Autoencoder (AE) method is employed for the classification of intrusions in the IoD environment. The CSO algorithm, inspired by the formation of crystal structures based on the lattice points, is employed at last for the hyperparameter-tuning process. To validate the enhanced performance of the proposed CSODAE-ID model, multiple simulation analyses were performed and the outcomes were assessed under distinct aspects. The comparative study outcomes demonstrate the superiority of the proposed CSODAE-ID model over the existing techniques.

Keywords: internet of drones; security; intrusion detection; machine learning; feature selection

Citation: Alissa, K.A.; Alotaibi, S.S.; Alrayes, F.S.; Aljebreen, M.; Alazwari, S.; Alshahrani, H.; Ahmed Elfaki, M.; Othman, M.; Motwakel, A. Crystal Structure Optimization with Deep-Autoencoder-Based Intrusion Detection for Secure Internet of Drones Environment. *Drones* **2022**, *6*, 297. https://doi.org/10.3390/drones6100297

Academic Editors: Mohammed H. Alsharif and Muhammad Asghar Khan

Received: 6 August 2022
Accepted: 2 September 2022
Published: 10 October 2022

1. Introduction

The Internet of Drones (IoD) was developed from the concept of IoT by replacing 'Things' with 'Drones' while the former possesses unmatched characteristics [1]. IoD is a 'layered network control architecture' that serves a vital part in the growth of drones

or Unmanned Aerial Vehicles (UAVs) [2,3]. In the IoD networking concept, numerous UAVs are linked with one another and a network is constituted in which the data are received and forwarded in a seamless manner [4,5]. At present, network security is one of the highly critical research domains, especially after the advancements made in internet and transmission methods [6]. In this scenario, various tools such as Network Intrusion Detection Systems (NIDSs) and firewalls are used to save the assets from cyber-attacks and provide network security. NIDSs are utilized to observe for any suspicious and bad behavior in the network traffic permanently [7,8]. Although the initial ideology of IDS was conceived in 1980, numerous Intrusion Detection Systems (IDS) have been proposed and implemented in recent years to fulfil the network security requirements [9]. There has been a tremendous increase observed in the past few years in network and communication technologies. This scenario has increased the size of the networks, the number of applications, and the volume of data produced and shared over networks [10]. In parallel, the number of novel types of cyber-attacks has also increased drastically. It is challenging to identify and recognize the types of attacks. For instance, data are critical at some nodes for an association to exist while any contact to the node might seriously affect the association [11].

The term Intrusion Detection System refers to a system that monitors the network traffic and is utilized for the detection of abnormal or suspicious acts, while it also executes protective initiatives against the intrusion risks. Thus, IDSs are of two types: Host IDS (HIDS) and Network IDS (NIDS). The NIDS is commonly deployed at perilous network points in order to ensure that the vulnerable locations and risk-prone areas are safeguarded from the attacks [12]. In terms of a HIDS system, it functions on devices that have internet access. In order to identify the intrusions, two key methods are followed, IDS related to the signatures and IDS related to the anomalies. A signature-related IDS (Knowledge-related Detection or Misuse Detection) focuses on the detection of a 'signature', a paradigm of intrusion events, and it is effective when upgrading the databases at a particular point in time [13].

Recently, various authors have suggested the application of Machine Learning (ML) and Deep Learning (DL) models for effective NIDS to identify the malicious attacks. However, the progressive rise in security threats coupled with network traffic brought various difficulties for the proposed NIDS methods in the proficient detection of assaults. In general, the aim of the IDSs is to identify the intruders. In the IoT domain, such intruders camouflage as hosts and try to access other nodes without a license. A NIDS has three fundamental features: a response module, an agent, and an analysis engine. The key objective of the agent is to collect the data from the network through event observations. Conversely, the response module and the analysis engine are accountable for outlining the signs of intrusions, producing alerts, and reacting to the outcomes attained from the analysis engine. NIDSs are highly helpful in the detection of attacks and their efficiency has evolved throughout these years. However, the attackers, too, have developed advanced attack techniques to overcome such detection technologies. This is attributed to the fact that the conventional NIDSs cannot be applied in the complex network layers of UAVs [14]. The number of ongoing studies in the field of cyber-attacks, especially upon drones, is expanding very quickly. So, there is a need to detect drone-related cyber-attacks and measure the kinds of threats imposed upon a smart city's airspace and the impact of a drone-related assault upon the economy of a city.

The current research article focuses on the design of Crystal Structure Optimization with Deep-Autoencoder-based Intrusion Detection (CSODAE-ID) for a secure IoD environment. The aim of the presented CSODAE-ID model is to identify the occurrences of intrusions in the IoD environment. In the proposed CSODAE-ID model, a new Modified Deer Hunting Optimization-related Feature Selection (MDHO-FS) technique is applied to choose the feature subsets. At the same time, the CSO algorithm with Autoencoder (AE) technique is leveraged for the classification of intrusions in the IoD environment. To validate the enhanced performance of the proposed CSODAE-ID model, different simulation

analyses were performed and the outcomes were assessed under distinct prospects. In short, the contributions of the paper are summarized herewith.

- The development of a new CSODAE-ID model for intrusion detection in the IoD environment.
- The presentation of a new MDHO-FS technique for feature subset selection process and enhancement of the classification accuracy.
- Implementation of the CSO algorithm for a DAE classification model to boost the overall classification performance.
- To the best of the authors' knowledge, the presented CSODAE-ID model is the first of its kind in the literature. The design of the CSO algorithm and MDHO-FS technique demonstrates the novelty of the current study.

The rest of the paper is organized as follows. Section 2 discusses the works related to the topic and Section 3 introduces the proposed model. Next, Section 4 offers the experimental validation and Section 5 concludes the paper with major findings.

2. Related Works

This section provides a brief survey of the existing IDS techniques in the IoD environment. In Perumalla et al.'s study [15], a novel technique was proposed for secure communication in an IoD network with the help of a robust Blockchain (BC)-aided access control. This IDS was developed based on the recently developed Deep Neuro-Fuzzy Network model. In general, the BC-based access control technique comprises of four stages, registration, pre-deployment, access control, and authentication, to transmit the relevant data in the IoD platform. In addition, the presented algorithm was able to detect the intrusions in the IoD environment. In the literature [16], the authors presented a novel hybrid IDS to resolve these issues. This method was proposed on the basis of spectral traffic analysis. Furthermore, a strong observer or controller was also included to determine the anomalies inside the UAV network. In the primary stage of the suggested hybrid model, the statistical sign of the traffic interchange, in a network, is considered. The difference among the resultant signatures was inspected and utilized for the selection of a precise method for accurate evaluation of the abnormal traffic. Basan et al. [17] detected the anomalies in UAV groups and also determined the type of attacks. To perform these tasks, the researchers designed an experimental stand emulating traffic communication in a UAV group. The presented algorithm functions on the basis of analyzing the changes in traffic communication patterns.

Whelan et al. [18] developed a novel IDS approach for UAVs through one-class classification. This one-class classifier requires the presence of non-anomalous information in the training subset. The said condition enables the utilization of flight logs, generated by UAVs, as the training dataset. Principal Component Analysis (PCA) can be implemented to sensor the logs so as to reduce the dimensions, while a one-class classification model can be produced for each sensor. Global Positioning System (GPS) spoofing is used as an example for external sensor-related attacks. Ouiazzane et al. [19] suggested the application of model-based Machine Learning techniques and multi-agent systems to identify the DoS cyber-attacks that target the network of drones. Being an autonomous method, the presented method is highly accurate and allows the recognition of both unknown as well as known DoS attacks in UAV networks with low false-positive and negative rates and high performance. This methodology was proposed to overcome the security issues faced in drone-related infrastructure and to demonstrate the significance of security, so the researchers paid more attention to the security aspects of the drones.

Digulescu et al. [20] introduced an innovative method for the characterization of drone movements and detection of attacks on the basis of advanced signal-processing methods and Ultra-Wide-Band (UWB) sensing systems. This technique symbolized the drone movement using traditional approaches, namely, recurrence plot analysis, correlation, envelope detection, and time-scale analysis. Moustafa and Jolfaei [21] developed an autonomous IDS to determine the sophisticated and advanced cyber-attacks that take

full advantage of the drone networks. A testbed was designed in this study to launch malicious activities towards the drone networks. This was performed so as to collect malicious and legitimate observations and estimate the performance of ML methods on a real-time basis.

Shrestha et al. [22] devised a UAV- and satellite-related 5G network security method to harness the benefits of ML for the effectual detection of cyber-attacks and vulnerabilities in the network. The proposed solution had two major parts, the creation of an intrusion detection method utilizing several ML techniques and the application of an ML-related method in satellite or terrestrial gateways. Ouiazzane et al. [23] presented an innovative IDS method for a fleet of drones that was organized with ad hoc transmission architecture. The scientific community has rarely addressed the security issues in drone fleets while most of the studies have concentrated on battery autonomy and routing protocols only. The multi-agent paradigm is considered as the most adequate and appropriate solution to model a potential IDS that can detect the intrusions directing a drone fleet. This mechanism can perfectly address the security issue of a drone fleet in the presence of cooperation, mobility, autonomy, and distribution features in the network connecting various nodes of the fleet.

Khan et al. [24] proposed a decentralized ML structure related to BC for performance improvement of the drones. The presented structure can pointedly improve the storage aspect and integrity of the data for intellectual decision making among multiple drones. The authors applied BC technology to perform decentralized prediction analytics and provided a structure that can apply ML techniques and share it successfully in a decentralized way. Abu Al-Haija and Al Badawi [25] modelled an autonomous IDS using Deep Convolutional Neural Networks (UAV-IDS-ConvNet) that can proficiently identify the malicious threats which invade the UAV network. The presented system considered the encoded Wi-Fi traffic data records collected from three different kinds of usually utilized UAVs: DJI Spark UAVs, Parrot Bebop UAVs, and DBPower UAVs. In order to evaluate the developed system, the author used UAV-IDS-2020 data which encompass numerous assaults on UAV networks in bidirectional and unidirectional transmission flow modes. Furthermore, the author also emulated the context of heterogeneous and homogeneous networking drones.

Conventional IDSs fail to meet the current dynamic network security requirements. In order to improve the detection efficacy and reduce the false-alarm rate of the IDSs, various studies have presented ML techniques in this domain which have made good progression as well. However, the existing models lack a hyperparameter selection process that mainly influences the performance of the classification model. Particularly, the hyperparameters such as epoch count, batch size, and learning rate selection are essential to attain an effectual outcome. Since the trial-and-error method for hyperparameter tuning is not only tedious but also an erroneous process, metaheuristic algorithms can be applied. Therefore, in this work, the CSO algorithm is employed for parameter selection of the DAE model.

3. The Proposed Model

In this article, a new CSODAE-ID algorithm is introduced for intrusion detection in the IoD environment. Initially, the proposed CSODAE-ID technique pre-processes the data. Following this, the MDHO-FS technique is applied to select the feature subsets. Moreover, the AE model is employed for the classification of intrusions in the IoD environment. Finally, the CSO algorithm, inspired by the formation of crystal structures based on lattice points, is employed for the hyperparameter-tuning process. Figure 1 portrays the overall processes involved in the proposed CSODAE-ID algorithm.

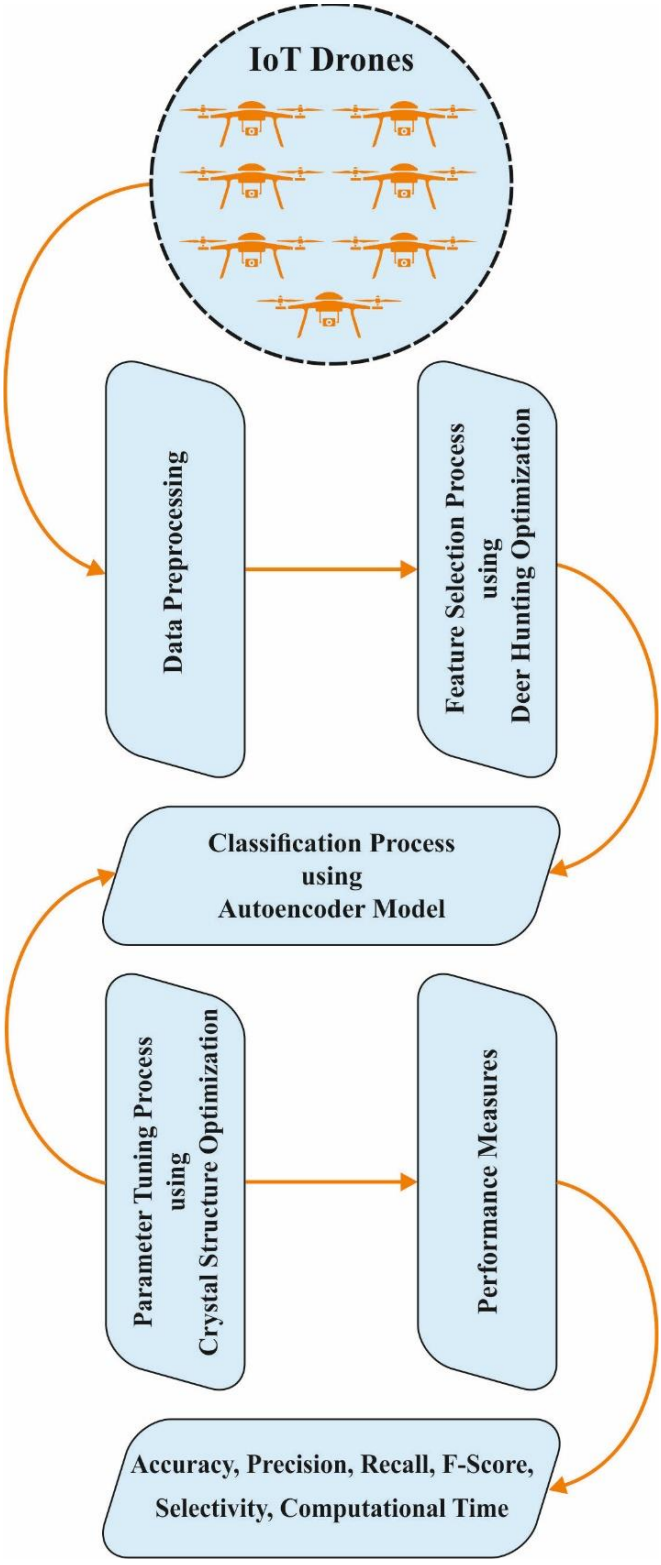

Figure 1. Overall process of CSODAE-ID algorithm.

3.1. Algorithmic Steps of MDHO-FS Technique

In this step, the MDHO-FS technique is applied to choose an optimal subset of features. A novel metaheuristic DHO method, inspired by the hunting behavior of deer with a set of hunters, was proposed earlier [26]. At the time of hunting a herd of deer, the hunter surrounds and travels nearby the deer based on a set of strategies. These strategies contain

distinct variables such as the position of the deer and the wind angle. The co-operation among the hunters is a crucial condition to make the hunting process an effective one. Finally, it influences the target based on the locations of the leader and its successor. In Equation (1), the main function of the presented algorithm is given.

$$f(x) = \max(accuracy) \tag{1}$$

Here, accuracy is calculated by dividing the number of correct predictions by the total number of predictions. The steps for weight optimization using the DHO algorithm are listed herewith.

The technique begins with the random generation of the population, called hunters, as given below.

$$X = \{X_1, X_2, \ldots, X_m\} 1 < j \leq m \tag{2}$$

In Equation (2), m characterizes the number of the hunters' population (weight) and X represents the total quantity of the weight as defined below.

$$\theta_j = 2\pi a \tag{3}$$

In Equation (3), a indicates an arbitrary number that lies in the range of [0, 1] and J denotes the existing iteration. Furthermore, θ denotes the wind angle. Next, the propagated positions with (X_l) leader position and (X_s) successor position for optimization are determined. The leader position defines the optimal position of a hunter. However, the successor position describes the position of a subsequent weight.

After the initialization of the optimal position, each weight in the population takes efforts to create an impact on the optimal position. Next, the 'position upgrade method' gets initiated by modeling the surrounding performance as defined herewith.

$$X_{j+1} = X_l - Y \cdot p \cdot \left| L \times X_l - X_j \right| \tag{4}$$

In Equation (4), X_j denotes the position at the existing and succeeding iterations as illustrated by X_{j+1}. Both Z and K coefficient vectors exist in the algorithm. The arbitrary number can be determined by taking the wind speed as denoted by p, and it encompasses the values in the range of (0–2). The equation to evaluate the coefficient vectors such as Z and K is demonstrated below.

$$Z = \frac{1}{4} \log\left(j + \frac{1}{j_{\max}}\right) b \tag{5}$$

$$K = 2 \cdot c \tag{6}$$

Here, $j_{\max}$ indicates the maximal iteration and $(X,\ Y)$ denotes the primary position of the hunter who attains the updated position based on the position of the prey. The two coefficient vectors such as Z and K depend on the optimal position, i.e., $(X_b,\ Y_b)$. If $p < 1$, then the position is upgraded, which in turn infers that the hunter is arbitrarily moving in various directions without considering the angle position.

The upgradation of the angle position is considered to increase the searching space. In order to create the hunting effect, it is essential to define the angle position of the hunter. Based on the position angle, the position upgrade is implemented as follows.

$$X_{j+1} = X_l - p \cdot \left| \cos(\mathrm{v}) \times X_l - X_j \right| \tag{7}$$

Here, $B = \varphi_{j+1}$ denotes the optimal location whereas X_{b_j} and p denote the arbitrary numbers.

A separate position is determined with various capabilities to the angle position so that the prey remains unaware of the hunter. Figure 2 defines the flowchart of the DHO technique.

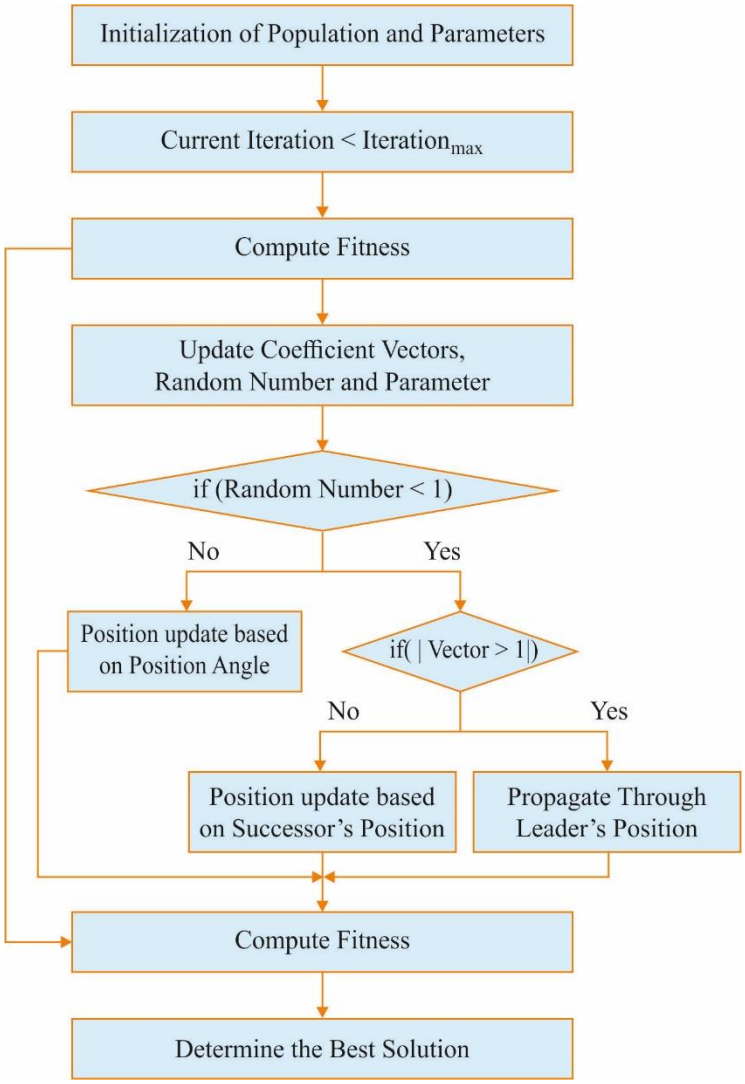

Figure 2. Flowchart of DHO algorithm.

During the exploration phase, the K vector is determined based on the surrounding performance. In the first position, an arbitrary searching method is implemented, concerning the value of K being less than 1. Ultimately, the position upgrade method takes place related to the successor place rather than the optimal position. Then, the global search is implemented as follows.

$$X_{j+1} = X_s - Z \cdot p \cdot \left| K \times X_s - X_j \right| \tag{8}$$

The position upgrade methodology is applied to recognize the optimal position (ending criteria).

The MDHO approach is derived by incorporating the concept of Nelder Mead (NM) upon the DHO algorithm. In NM, simplex search is a portion of a common class of direct search techniques. It is a popular approach to resolve the un-constrained non-linear optimization issues without applying the derivatives [27]. Commonly, it is employed for local optimization issues. The NM approach tends to diminish the non-linear scalar function of n parameters by approximating the objective function. At first, the NM method performs an initial simplex, Δ_1, of $n + 1$ vertices from the starting point x_0, whereby the vertex denotes the parameter set x of n variable.

The Fitness Function (FF) assumes the accuracy of the classifier and the count of selective features. It optimizes the classifier's accuracy and minimizes the fixed size of the

selective features. Hence, the subsequent FF is employed to assess the individual solutions as shown in Equation (9).

$$Fitness = \alpha \times ErrorRate + (1 - \alpha) \times \frac{\#SF}{\#All\_F} \tag{9}$$

Here, *ErrorRate* implies the classifier's error rate when employing the selective features. Furthermore, $\#SF$ denotes the count of selective features and $\#All\_F$ defines the entire count of attributes from the original dataset. In this equation, α is employed to control the significance of the classifier's quality and the length of the subset.

3.2. Intrusion Detection Using AE Model

For the purpose of intrusion detection and its classification, the AE model is exploited in this study. This is a form of multi-layer Feed Forward Neural Network (FFNN) that reconstructs and compresses the dataset [28]. Both input and the output units have n number of neurons in which n denotes the dimensionality of the dataset. For every j dimension, the input x_j is recreated as r_j at the output. In such case, the number of the neurons in the middle hidden layer is denoted by $h(h \ll n)$, while the first and third hidden states have a size of 2 h each. By enforcing the 'bottleneck' structure, the AE technique enables the compression of (encoding) the input dataset to a low dimension and reconstructs it at the output state.

Here, the rectified linear activation function (ReLU) is applied for the hidden layer, whereas the output layer takes the form of a sigmoid activation function. The aim of the training method is to mitigate the aggregated reconstruction errors which are summed up over each data point.

$$E = \sum_{i}^{N} \sum_{j=1}^{n} (x_{ij} - r_{ij})^2, \tag{10}$$

Post training, the data demonstration captures the principle of the input dataset to enable the data reconstruction process at the output layer with low error. This section described the 'encoder' portion of the trainable AE model.

3.3. Hyperparameter Tuning

For optimal modification of the hyperparameters related to AE method, the CSO technique is utilized which also enriches the classification performance. In the current study, the mathematical modelling of CryStAl is proposed in which the key concept of a crystal is utilized with essential modifications [29]. In this model, every solution candidate of the optimization technique is regarded as a single crystal in the space. For the purpose of iteration, the number of crystals is determined randomly for initialization.

$$Cr = \begin{bmatrix} Cr_1 \\ Cr_2 \\ \vdots \\ Cr_i \\ \vdots \\ Cr_n \end{bmatrix}$$

$$= \begin{bmatrix} x_1^1 & x_1^2 & \dots & x_1^j & \dots & x_1^d \\ x_2^1 & x_2^2 & \dots & x_2^j & \dots & x_2^d \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_i^1 & x_i^2 & \dots & x_i^j & \dots & x_i^d \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_n^1 & x_n^2 & \dots & x_n^j & \dots & x_n^d \end{bmatrix}$$

$$\begin{cases} i = 1, 2, \ldots, n \\ j = 1, 2, \ldots, d \end{cases} \tag{11}$$

In Equation (11), n refers to the number of crystals (solution candidate) and d indicates the dimensions of the problem. The initial position of the crystal is randomly determined in the searching space to solve the problem.

$$x_i^j(0) = x_{i,\,\min}^j + \xi\left(x_{i,\,\max}^j - x_{i,m\dot{m}}^j\right), \begin{cases} i = 1, 2, \ldots, n \\ j = 1, 2, \ldots, d \end{cases} \tag{12}$$

In Equation (12), $x_i^j(0)$ denotes the initial location of the crystal, $x_{i,\,\min}^j$ and $x_{i,\,\max}^j$ correspondingly refer to the minimal and maximal allowable values for the jth decision parameter of the ith solution candidate and ξ denotes a random value between [0, 1].

According to the idea of 'basis' in crystallography, each crystal is regarded as a major crystal at the corner, whereas Cr_{main} is randomly determined based on the first-made crystal (i.e., solution candidate). It is important to note that the random selection technique, for all the steps, is defined by neglecting the existing Cr. The crystals with the optimal formation are defined by Cr_b while the mean value of the randomly chosen crystals is represented by F_c.

In order to update the position of the solution candidate in the searching space, the fundamental principles are deliberated in which four different kinds of upgrading procedures are listed herewith.

(i) Simple cubicle:

$$Cr_{new} = Cr_{old} + rCr_{main}, \tag{13}$$

(ii) Cubicle with the best crystals:

$$Cr_{new} = Cr_{old} + r_1 Cr_{main} + r_2 Crb, \tag{14}$$

(iii) Cubicle with mean crystals:

$$Cr_{new} = Cr_{old} + r_1 Cr_{main} + r_2 F_c, \tag{15}$$

(iv) Cubicle with the best and mean crystals:

$$Cr_{new} = Cr_{old} + r_1 Cr_{main} + r_2 Crb + r_3 F_c, \tag{16}$$

From the four abovementioned equations, the new position is represented by Cr_{new} whereas the old position is denoted by c_{rold}, and r, r_1, r_2 and r_3 denote the random numbers.

It is noteworthy to mention that the exploitation and exploration phases are the two key characteristics of meta-heuristics and the global and local search models are simultaneously carried out in this model. To manage the solution variable x_i^j that violates the boundary condition of the variable, a mathematical flag is determined for x_i^j outside the variable range. Then, a boundary change is ordered for violating the variable. The end condition is determined on the basis of maximal iteration count, whereas the optimized algorithm is ended after a fixed iteration count.

The CSO system comes with a Fitness Function (FF) to accomplish the maximum classification results. It sets a positive value to represent the superior act of a candidate solution. The minimal classifier error rate is assumed to be the FF as given in Equation (17).

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{number\ of\ misclassified\ samples}{Total\ number\ of\ samples} * 100 \tag{17}$$

4. Results and Discussion

The current section examines the intrusion detection performance of the proposed CSODAE-ID technique. The dataset [10] holds a total of 8000 samples under four class labels as illustrated in Table 1. The proposed model was simulated using the Python 3.6.5 tool.

Table 1. Dataset details.

Class	No. of Sample Instances
DOS	2000
R2L	2000
U2R	2000
Probe	2000
Total Number of Samples	8000

Figure 3 exhibits the confusion matrices produced by the proposed CSODAE-ID technique. On the entire dataset, the proposed CSODAE-ID technique recognized 1954, 1954, 1979, and 1969 samples under DOS, R2L, U2R, and Probe classes, respectively. At the same time, on 70% of the training (TR) data, the presented CSODAE-ID method classified 1370, 1381, 1384, and 1363 samples under DOS, R2L, U2R, and Probe classes, respectively. On 30% of the testing (TS) data, the proposed CSODAE-ID algorithm categorized 584, 573, 595, and 606 samples under DOS, R2L, U2R, and Probe classes, respectively.

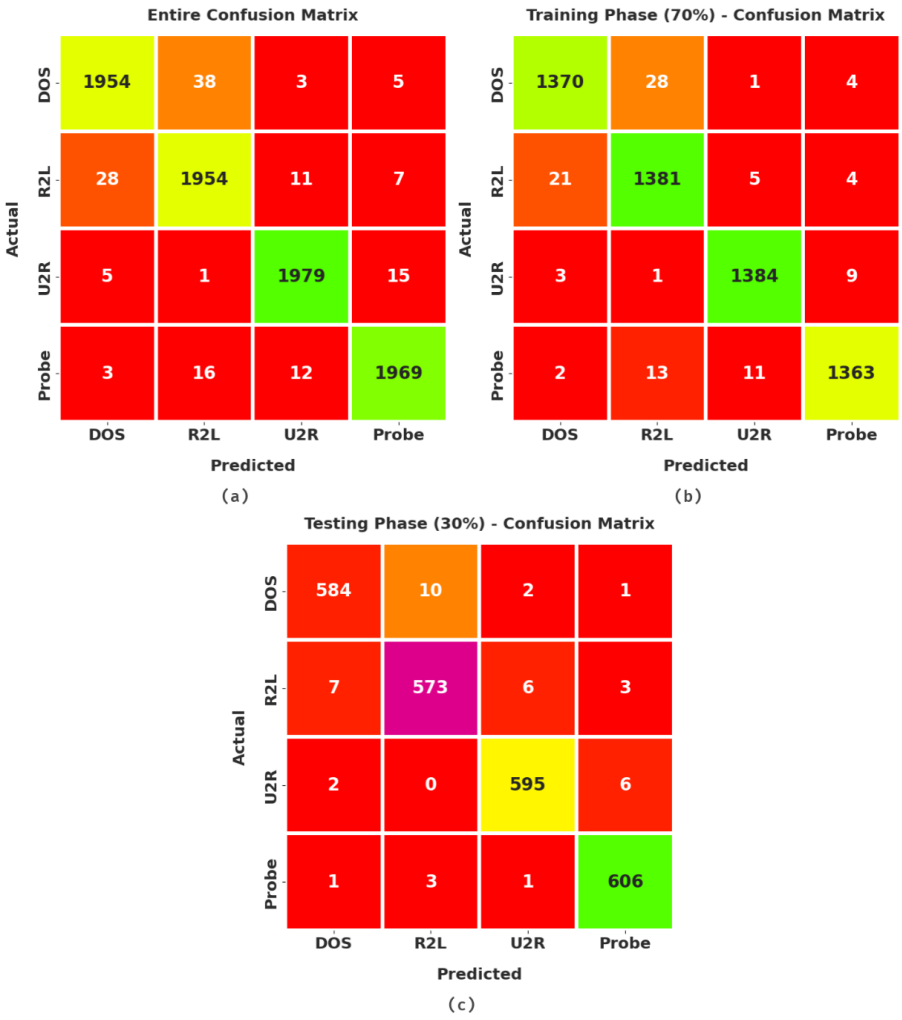

Figure 3. Confusion matrices of CSODAE-ID approach. (**a**) Entire dataset, (**b**) 70% of TR data, and (**c**) 30% of TS data.

Table 2 provides the overall IDS outcomes achieved by the proposed CSODAE-ID model. Figure 4 provides a brief overview of the intrusion detection performance of the proposed CSODAE-ID method on the entire dataset. The figure implies that the CSODAE-ID model achieved enhanced results under all the classes. For instance, on the DOS class, the proposed CSODAE-ID model offered $accu_y$, $prec_n$, $reca_l$, $sele_y$, and F_{score} values such as 98.98%, 98.19%, 97.70%, 99.40%, and 97.94%, respectively. Furthermore, on the R2L class, the presented CSODAE-ID approach attained $accu_y$, $prec_n$, $reca_l$, $sele_y$, and F_{score} values such as 98.74%, 97.26%, 97.70%, 99.08%, and 97.48%, respectively. Moreover, on the U2R class, the proposed CSODAE-ID methodology provided $accu_y$, $prec_n$, $reca_l$, $sele_y$, and F_{score} values such as 99.41%, 98.70%, 98.95%, 99.57%, and 98.83%, respectively.

Table 2. Results of the analysis of CSODAE-ID approach under distinct class labels.

Labels	Accuracy (%)	Precision (%)	Recall (%)	Selectivity (%)	F_{score} (%)
Entire Dataset					
DOS	98.98	98.19	97.70	99.40	97.94
R2L	98.74	97.26	97.70	99.08	97.48
U2R	99.41	98.70	98.95	99.57	98.83
Probe	99.28	98.65	98.45	99.55	98.55
Average	99.10	98.20	98.20	99.40	98.20
Training Phase (70%)					
DOS	98.95	98.14	97.65	99.38	97.89
R2L	98.71	97.05	97.87	99.00	97.46
U2R	99.46	98.79	99.07	99.60	98.93
Probe	99.23	98.77	98.13	99.60	98.45
Average	99.09	98.19	98.18	99.39	98.18
Testing Phase (30%)					
DOS	99.04	98.32	97.82	99.45	98.07
R2L	98.79	97.78	97.28	99.28	97.53
U2R	99.29	98.51	98.67	99.50	98.59
Probe	99.38	98.38	99.18	99.44	98.78
Average	99.12	98.25	98.24	99.42	98.24

Figure 5 is a detailed demonstration of the intrusion detection results achieved using the CSODAE-ID technique on 70% of the TR data. The figure denotes that the proposed CSODAE-ID approach demonstrated enhanced results under all the classes. For example, on the DOS class, the proposed CSODAE-ID method attained $accu_y$, $prec_n$, $reca_l$, $sele_y$, and F_{score} values such as 98.95%, 98.14%, 97.65%, 99.38%, and 97.89%, respectively. Similarly, on the R2L class, the proposed CSODAE-ID model offered $accu_y$, $prec_n$, $reca_l$, $sele_y$, and F_{score} values such as 98.71%, 97.05%, 97.87%, 99.00%, and 97.46%, respectively. Additionally, on the U2R class, the presented CSODAE-ID approach accomplished $accu_y$, $prec_n$, $reca_l$, $sele_y$, and F_{score} values such as 99.46%, 98.79%, 99.07%, 99.60%, and 98.93%, respectively.

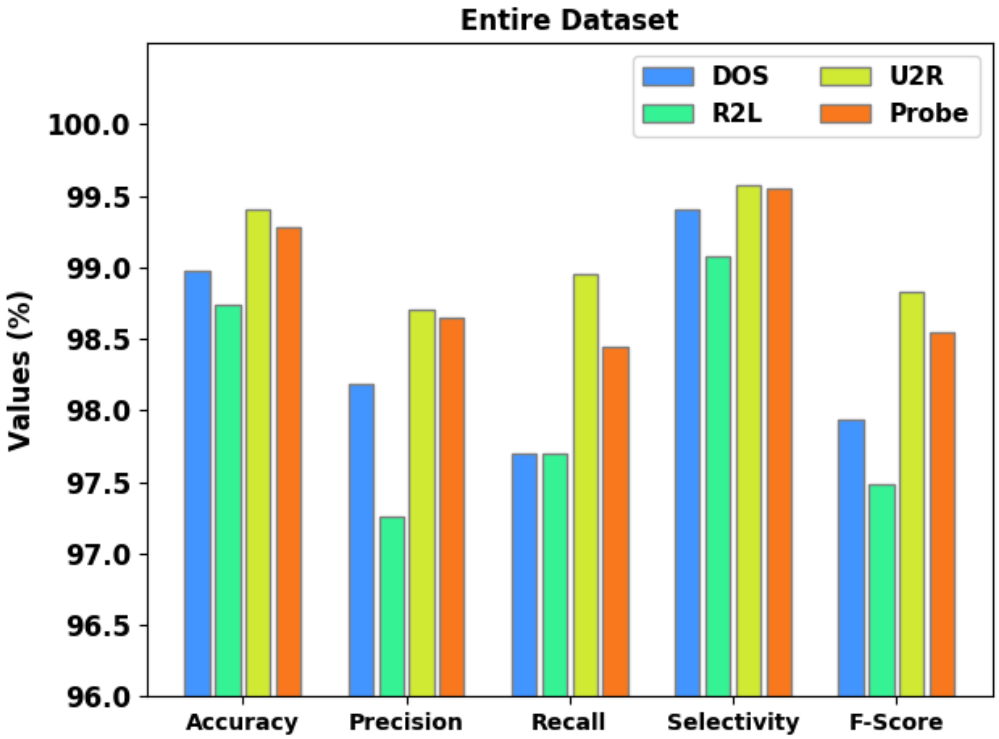

Figure 4. Results of the analysis of CSODAE-ID approach on entire dataset.

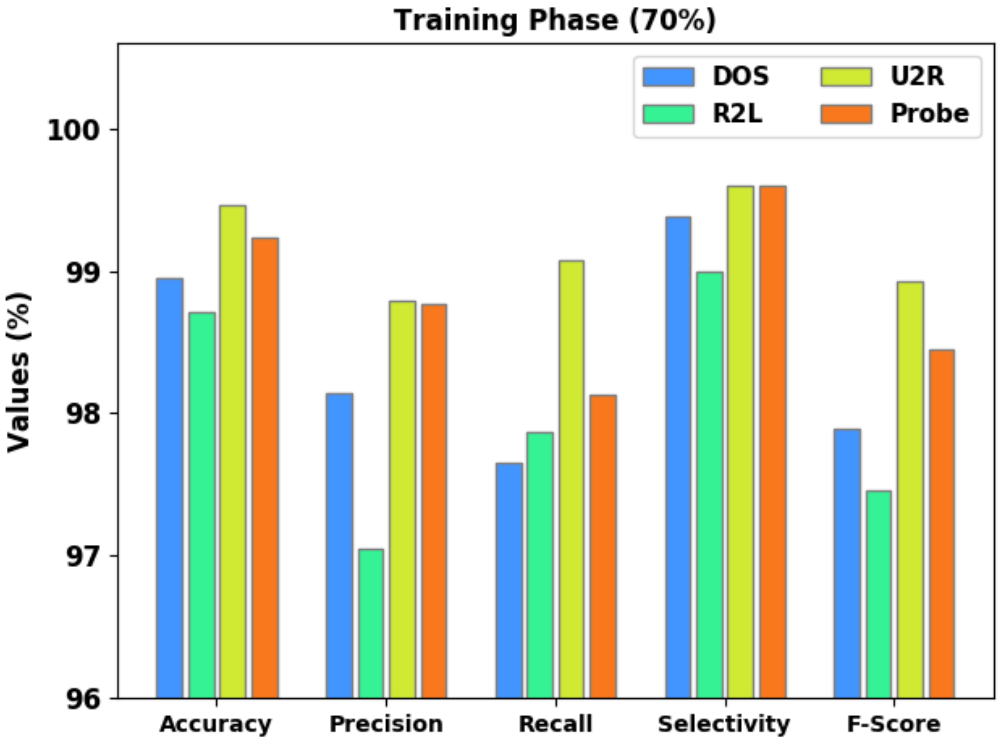

Figure 5. Results of the analysis of CSODAE-ID approach on 70% of TR data.

Figure 6 represents the comparative intrusion detection results yielded by the proposed CSODAE-ID method on 30% of the TS data. The figure implies that the proposed CSODAE-ID approach accomplished enhanced results under all the classes. For example, on the DOS class, the proposed CSODAE-ID methodology rendered $accu_y$, $prec_n$, $reca_l$, $sele_y$, and F_{score} values such as 99.04%, 98.32%, 97.82%, 99.45%, and 98.07%, respectively. In addition, on the R2L class, the proposed CSODAE-ID technique achieved $accu_y$, $prec_n$, $reca_l$, $sele_y$, and

F_{score} values such as 98.79%, 97.78%, 97.28%, 99.28%, and 97.53%, respectively. Along with the U2R class, the proposed CSODAE-ID methodology attained $accu_y$, $prec_n$, $reca_l$, $sele_y$, and F_{score} values such as 99.29%, 98.51%, 98.67%, 99.50%, and 98.59%, respectively.

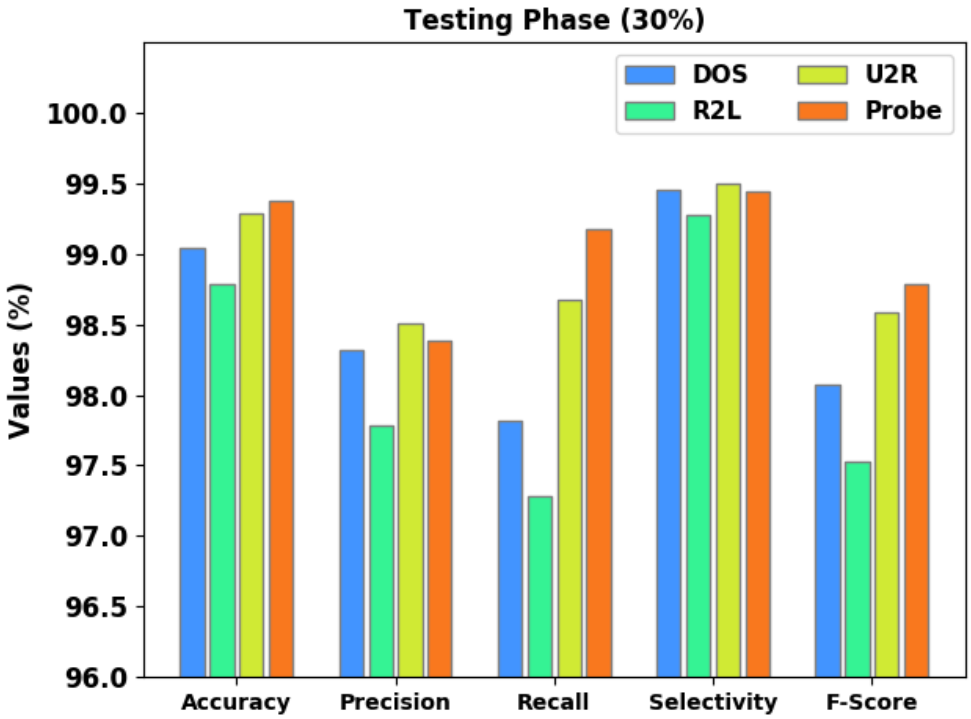

Figure 6. Results of the analysis of CSODAE-ID approach on 30% of TS data.

Both Training Accuracy (TRA) and Validation Accuracy (VLA) values, acquired by the proposed CSODAE-ID algorithm on the test dataset, are shown in Figure 7. The experimental results denote that the proposed CSODAE-ID approach achieved the maximum TRA and VLA values whereas the VLA values were higher than the TRA values.

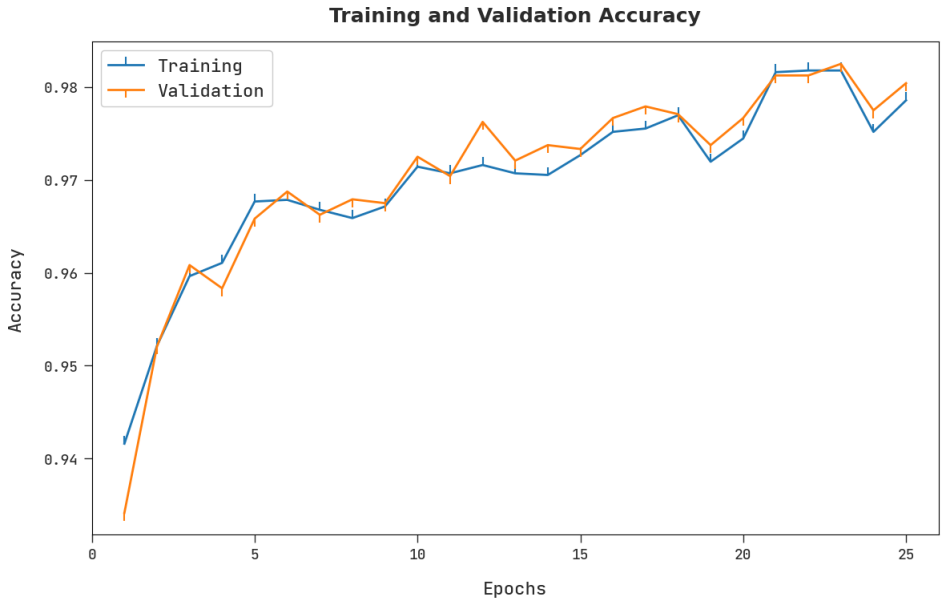

Figure 7. TRA and VLA analyses results of CSODAE-ID methodology.

Both Training Loss (TRL) and Validation Loss (VLL) values, reached by the proposed CSODAE-ID approach on the test dataset, are exhibited in Figure 8. The experimental

outcomes imply that the proposed CSODAE-ID method exhibited the lowest TRL and VLL values whereas the VLL values were lower than the TRL values.

Figure 8. TRL and VLL analyses results of CSODAE-ID methodology.

A clear precision–recall analysis was conducted upon the proposed CSODAE-ID approach using the test dataset, and the results are shown in Figure 9. The figure shows that the proposed CSODAE-ID methodology yielded high precision–recall values under all the classes.

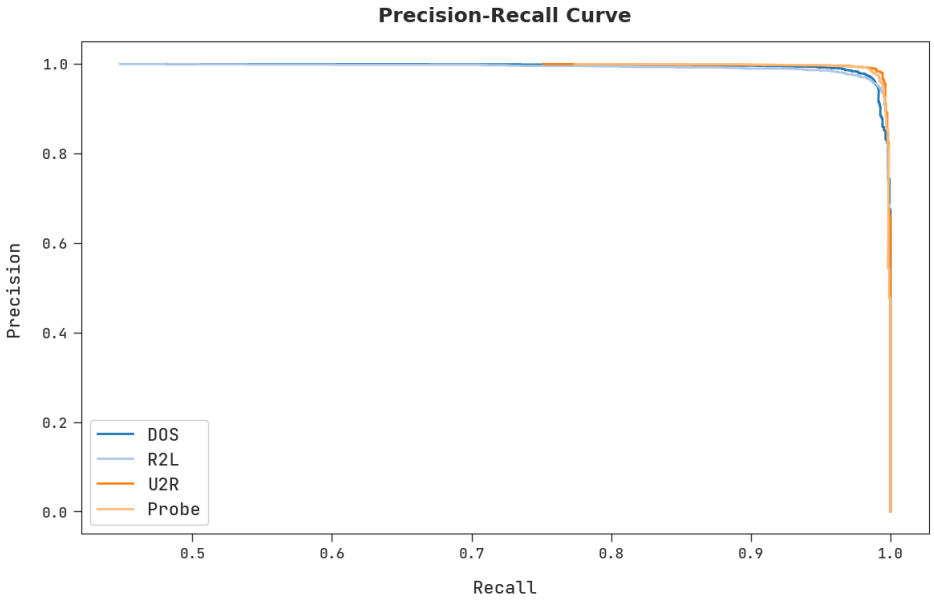

Figure 9. Precision–recall analysis results of CSODAE-ID methodology.

A detailed ROC analysis was conducted upon the proposed CSODAE-ID algorithm using the test dataset, and the results are portrayed in Figure 10. The results denote that the proposed CSODAE-ID technique established its ability to categorize the test dataset under distinct classes.

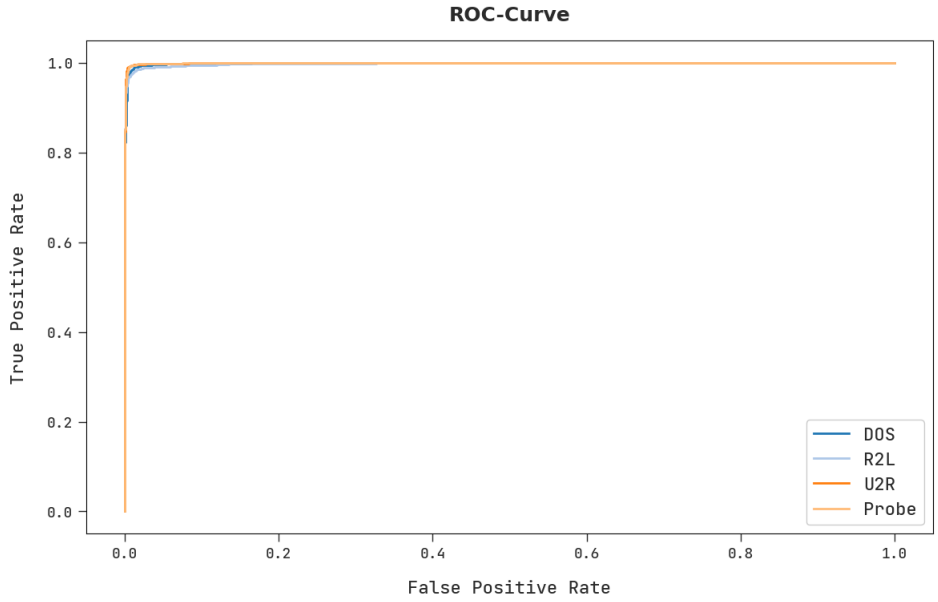

Figure 10. ROC analysis results of CSODAE-ID methodology.

Table 3 provides the comprehensive comparison analysis outcomes achieved by the proposed CSODAE-ID model and other recent models [10]. Figure 11 shows the $accu_y$ and $F1_{score}$ values achieved by the CSODAE-ID and other recent methods. The figure infers that the proposed CSODAE-ID model achieved a high performance with maximum $accu_y$ and $F1_{score}$ values.

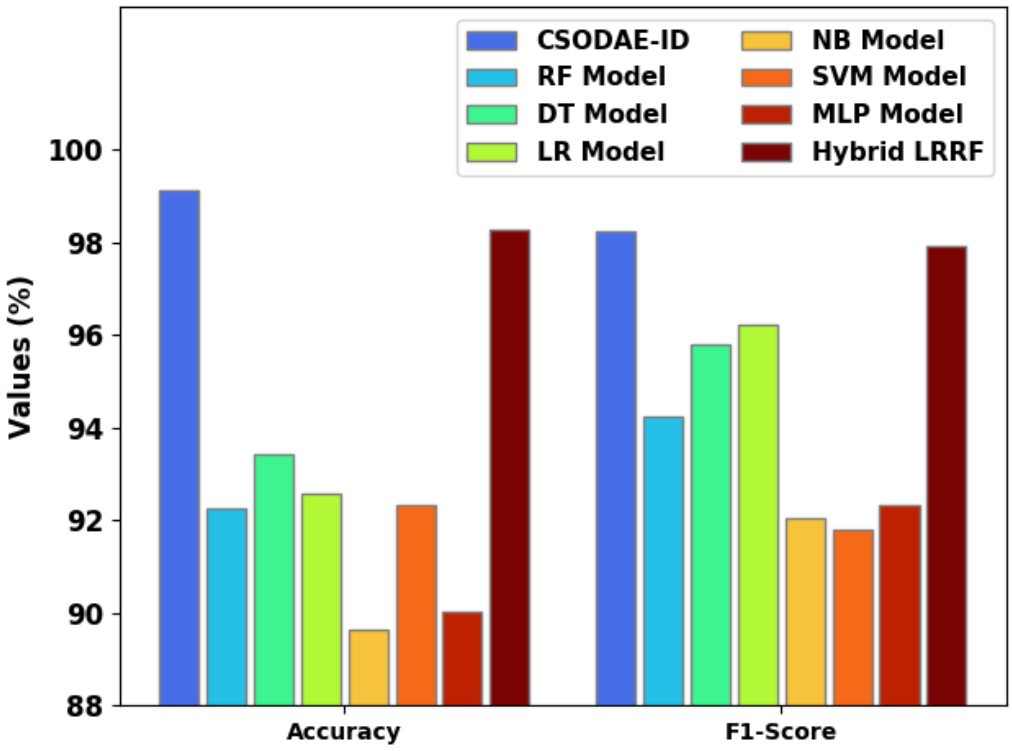

Figure 11. $Accu_y$ and $F1_{score}$ analyses results of CSODAE-ID approach and other existing methodologies.

Table 3. Comparative analysis results of CSODAE-ID approach and other existing methodologies.

Models	Accuracy (%)	Precision (%)	Recall (%)	$F1_{score}$ (%)
CSODAE-ID	99.12	98.25	98.24	98.24
RF Model	92.26	92.16	92.93	94.23
DT Model	93.43	91.14	92.75	95.78
LR Model	92.56	95.96	94.20	96.22
NB Model	89.63	90.49	91.52	92.05
SVM Model	92.32	94.20	92.78	91.80
MLP Model	90.03	88.19	89.19	92.31
Hybrid LRRF	98.28	97.48	98.10	97.92

For instance, with respect to $accu_y$, the proposed CSODAE-ID approach achieved a maximum $accu_y$ of 99.12%, whereas RF, DT, LR, NB, SVM, MLP, and hybrid LRRF techniques obtained the lowest $accu_y$ values such as 92.26%, 93.43%, 92.56%, 89.63%, 92.32%, 90.03%, and 98.28%, respectively. Conversely, with respect to $F1_{score}$, the proposed CSODAE-ID technique achieved a maximum $F1_{score}$ of 98.24%, whereas RF, DT, LR, NB, SVM, MLP, and hybrid LRRF approaches gained the lowest $F1_{score}$ values such as 94.23%, 95.78%, 96.22%, 92.05%, 91.80%, 92.31%, and 97.92%, respectively.

Figure 12 denotes the $prec_n$ and $reca_l$ values achieved by the proposed CSODAE-ID approach and other recent models. The figure implies that the proposed CSODAE-ID algorithm exhibited an excellent performance with maximal values of $prec_n$ and $reca_l$. For example, with respect to $prec_n$, the proposed CSODAE-ID technique offered a maximum $prec_n$ of 98.25%, whereas RF, DT, LR, NB, SVM, MLP, and hybrid LRRF techniques reached the lowest $prec_n$ values such as 92.16%, 91.14%, 95.96%, 90.49%, 94.20%, 88.19%, and 97.48%, respectively.

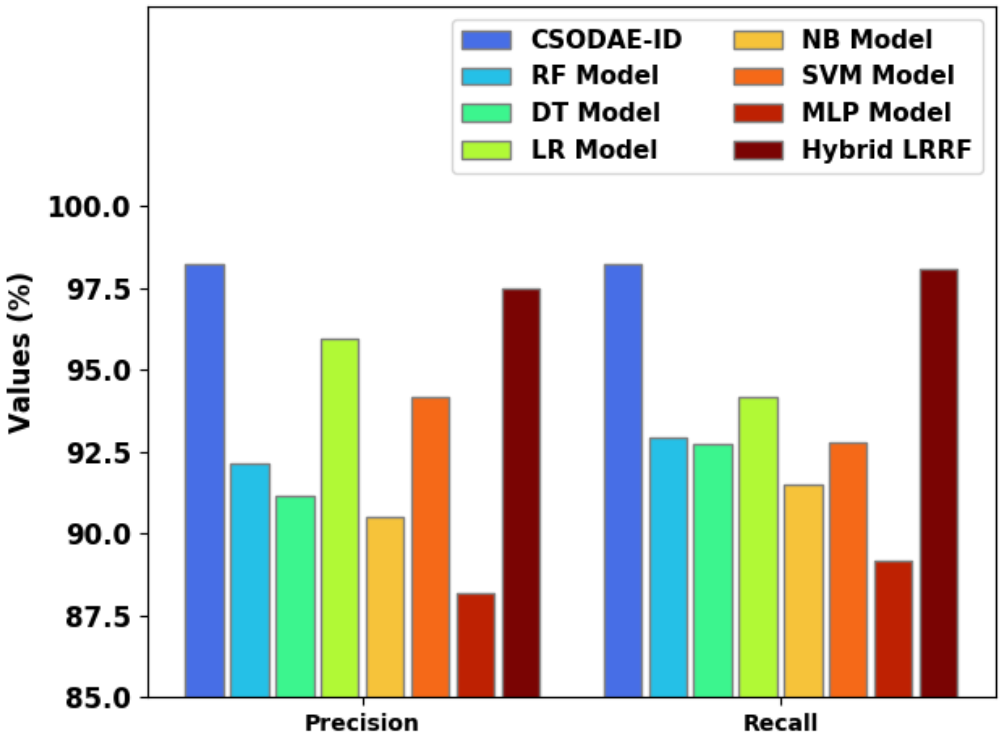

Figure 12. $Prec_n$ and $Reca_l$ analyses results of CSODAE-ID approach and other existing methodologies.

Additionally, with respect to $reca_l$, the proposed CSODAE-ID approach achieved a high $reca_l$ of 98.24%, whereas RF, DT, LR, NB, SVM, MLP, and hybrid LRRF methods obtained low $reca_l$ values such as 92.93%, 92.75%, 94.20%, 91.52%, 92.78%, 89.19%, and

98.10%, respectively. These results assured the enhanced performance of the proposed CSODAE-ID method over other models in intrusion detection.

5. Conclusions

In the current study, a new CSODAE-ID algorithm has been introduced, developed, and validated for intrusion detection in the IoD environment. At the initial stage, the proposed CSODAE-ID technique pre-processes the data. Following this, the MDHO-FS technique is applied to choose the feature subsets. Then, the AE approach is leveraged for the classification of intrusions in the IoD environment. Finally, the CSO algorithm, inspired by the formation of crystal structures based on lattice points, is employed for the hyperparameter-tuning process. To validate the enhanced performance of the proposed CSODAE-ID model, a wide range of simulations were conducted and the outcomes were assessed under distinct aspects. The comparative study outcomes demonstrate the superiority of the proposed CSODAE-ID model over recent approaches with a high accuracy of 99.12%. Thus, the proposed CSODAE-ID technique can be applied in the future for the effectual detection of intrusions in the IoD environment. In upcoming years, the classification performance of the proposed CSODAE-ID approach can be enhanced using hybrid ensemble fusion methods. Moreover, the proposed model can also be tested on a real-time large-scale dataset in the future.

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

Funding: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R319), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (22UQU4210118DSR32). Research Supporting Project number (RSP2022R459), King Saud University, Riyadh, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zhang, Z.; Zhang, Y.; Niu, J.; Guo, D. Unknown network attack detection based on open-set recognition and active learning in drone network. *Trans. Emerg. Telecommun. Technol.* **2021**, e4212. [CrossRef]
2. Ramadan, R.A.; Emara, A.-H.; Al-Sarem, M.; Elhamahmy, M. Internet of Drones Intrusion Detection Using Deep Learning. *Electronics* **2021**, *10*, 2633. [CrossRef]
3. Ferrag, M.A.; Maglaras, L. DeliveryCoin: An IDS and Blockchain-Based Delivery Framework for Drone-Delivered Services. *Computers* **2019**, *8*, 58. [CrossRef]
4. Hamza, M.A.; Hassine, S.B.H.; Abunadi, I.; Al-Wesabi, F.N.; Alsolai, H.; Hilal, A.M.; Yaseen, I.; Motwakel, A. Feature Selection with Optimal Stacked Sparse Autoencoder for Data Mining. *Comput. Mater. Contin.* **2022**, *72*, 2581–2596. [CrossRef]
5. Ferrag, M.; Shu, L.; Djallel, H.; Choo, K.-K. Deep Learning-Based Intrusion Detection for Distributed Denial of Service Attack in Agriculture 4.0. *Electronics* **2021**, *10*, 1257. [CrossRef]
6. Alohali, M.A.; Al-Wesabi, F.N.; Hilal, A.M.; Goel, S.; Gupta, D.; Khanna, A. Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment. *Cogn. Neurodyn.* **2022**. [CrossRef]
7. Wazid, M.; Das, A.K.; Shetty, S.; Gope, P.; Rodrigues, J.J.P.C. Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap. *IEEE Access* **2020**, *9*, 4466–4489. [CrossRef]

8. Rout, G.P.; Mohanty, S.N. A hybrid approach for network intrusion detection. In Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 4–6 April 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 614–617.
9. Abdelmaboud, A. The Internet of Drones: Requirements, Taxonomy, Recent Advances, and Challenges of Research Trends. *Sensors* **2021**, *21*, 5718. [CrossRef] [PubMed]
10. Hilal, A.M.; Alohali, M.A.; Al-Wesabi, F.N.; Nemri, N.; Alyamani, H.J.; Gupta, D. Enhancing quality of experience in mobile edge computing using deep learning based data offloading and cyberattack detection technique. *Clust. Comput.* **2021**. [CrossRef]
11. Sharma, M.K.; Singal, G.; Gupta, S.K.; Chandraneil, B.; Agarwal, S.; Garg, D.; Mukhopadhyay, D. INTERVENOR: Intelligent Border Surveillance using Sensors and Drones. In Proceedings of the 2021 6th International Conference for Convergence in Technology (I2CT), Maharashtra, India, 2–4 April 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–7.
12. Olawale, O.P.; Dimililer, K.; Al-Turjman, F. AI simulations and programming environments for drones: An overview. In *Drones in Smart-Cities*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 93–106.
13. Pu, C.; Zhu, P. Defending against flooding attacks in the internet of drones environment. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
14. Aldaej, A.; Ahanger, T.A.; Atiquzzaman, M.; Ullah, I.; Yousufudin, M. Smart Cybersecurity Framework for IoT-Empowered Drones: Machine Learning Perspective. *Sensors* **2022**, *22*, 2630. [CrossRef] [PubMed]
15. Perumalla, S.; Chatterjee, S.; Kumar, A.S. Block Chain-based access control and intrusion detection system in IoD. In Proceedings of the 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 8–10 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 511–518.
16. Condomines, J.-P.; Zhang, R.; Larrieu, N. Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation. *Ad Hoc Netw.* **2019**, *90*, 101759. [CrossRef]
17. Basan, E.; Lapina, M.; Mudruk, N.; Abramov, E. Intelligent intrusion detection system for a group of UAVs. In Proceedings of the International Conference on Swarm Intelligence, Qingdao, China, 17–21 July 2021; Springer: Cham, Switzerland, 2021; pp. 230–240.
18. Whelan, J.; Sangarapillai, T.; Minawi, O.; Almehmadi, A.; El-Khatib, K. Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles. In Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Alicante, Spain, 16–20 November 2020; pp. 23–28.
19. Ouiazzane, S.; Addou, M.; Barramou, F. A Multiagent and Machine Learning Based Denial of Service Intrusion Detection System for Drone Networks. In *Geospatial Intelligence*; Springer: Cham, Switzerland, 2022; pp. 51–65.
20. Digulescu, A.; Despina-Stoian, C.; Stănescu, D.; Popescu, F.; Enache, F.; Ioana, C.; Rădoi, E.; Rîncu, I.; Șerbănescu, A. New Approach of UAV Movement Detection and Characterization Using Advanced Signal Processing Methods Based on UWB Sensing. *Sensors* **2020**, *20*, 5904. [CrossRef] [PubMed]
21. Moustafa, N.; Jolfaei, A. Autonomous detection of malicious events using machine learning models in drone networks. In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and beyond, London, UK, 25 September 2020; pp. 61–66.
22. Shrestha, R.; Omidkar, A.; Roudi, S.; Abbas, R.; Kim, S. Machine-Learning-Enabled Intrusion Detection System for Cellular Connected UAV Networks. *Electronics* **2021**, *10*, 1549. [CrossRef]
23. Ouiazzane, S.; Barramou, F.; Addou, M. Towards a Multi-Agent based Network Intrusion Detection System for a Fleet of Drones. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*. [CrossRef]
24. Khan, A.A.; Khan, M.M.; Khan, K.M.; Arshad, J.; Ahmad, F. A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs. *Comput. Netw.* **2021**, *196*, 108217. [CrossRef]
25. Abu Al-Haija, Q.; Al Badawi, A. High-performance intrusion detection system for networked UAVs via deep learning. *Neural Comput. Appl.* **2022**, *34*, 10885–10900. [CrossRef]
26. Tian, M.-W.; Yan, S.-R.; Han, S.-Z.; Nojavan, S.; Jermsittiparsert, K.; Razmjooy, N. New optimal design for a hybrid solar chimney, solid oxide electrolysis and fuel cell based on improved deer hunting optimization algorithm. *J. Clean. Prod.* **2020**, *249*, 119414. [CrossRef]
27. Audet, C.; Tribes, C. Mesh-based Nelder–Mead algorithm for inequality constrained optimization. *Comput. Optim. Appl.* **2018**, *71*, 331–352. [CrossRef]
28. Gong, D.; Liu, L.; Le, V.; Saha, B.; Mansour, M.R.; Venkatesh, S.; Hengel, A.V.D. Memorizing normality to detect anomaly: Memory-augmented deep autoencoder for unsupervised anomaly detection. In Proceedings of the IEEE/CVF International Conference on Computer Vision, Seoul, Korea, 27 October–2 November 2019; pp. 1705–1714.
29. Hussein, R.; Schmidt, J.; Barros, T.; Marques, M.A.; Botti, S. Machine-learning correction to density-functional crystal structure optimization. *MRS Bull.* **2022**, 1–7. [CrossRef]