sustainability

MDPI

Article

Modelling of Metaheuristics with Machine Learning-Enabled Cybersecurity in Unmanned Aerial Vehicles

Mohammed Rizwanullah [1,*], Hanan Abdullah Mengash [2], Mohammad Alamgeer [3], Khaled Tarmissi [4], Amira Sayed A. Aziz [5], Amgad Atta Abdelmageed [1], Mohamed Ibrahim Alsaid [1] and Mohamed I. Eldesouki [6]

1 Department of Computer and Self Development, Prince Sattam bin Abdulaziz University, AlKharj, 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 Science & Art at Mahayil, King Khalid University, Abha, Saudi Arabia
4 Department of Computer Science, College of Computing and Information System, Umm Al-Qura University, Mecca, Saudi Arabia
5 Department of Digital Media, Faculty of Computers and Information Technology, Future University in Egypt, New Cairo 11835, Egypt
6 Department of Information System, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia
* Correspondence: r.mohammed@psau.edu.sa

Abstract: The adoption and recent development of Unmanned Aerial Vehicles (UAVs) are because of their widespread applications in the private and public sectors, from logistics to environment monitoring. The incorporation of 5G technologies, satellites, and UAVs has provoked telecommunication networks to advance to provide more stable and high-quality services to remote areas. However, UAVs are vulnerable to cyberattacks because of the rapidly expanding volume and poor inbuilt security. Cyber security and the detection of cyber threats might considerably benefit from the development of artificial intelligence. A machine learning algorithm can be trained to search for attacks that may be similar to other types of attacks. This study proposes a new approach: metaheuristics with machine learning-enabled cybersecurity in unmanned aerial vehicles (MMLCS-UAVs). The presented MMLCS-UAV technique mainly focuses on the recognition and classification of intrusions in the UAV network. To obtain this, the presented MMLCS-UAV technique designed a quantum invasive weed optimization-based feature selection (QIWO-FS) method to select the optimal feature subsets. For intrusion detection, the MMLCS-UAV technique applied a weighted regularized extreme learning machine (WRELM) algorithm with swallow swarm optimization (SSO) as a parameter tuning model. The experimental validation of the MMLCS-UAV method was tested using benchmark datasets. This widespread comparison study reports the superiority of the MMLCS-UAV technique over other existing approaches.

Keywords: metaheuristics; machine learning; cybersecurity; intrusion detection system; unmanned aerial vehicles

Citation: Rizwanullah, M.; Mengash, H.A.; Alamgeer, M.; Tarmissi, K.; Aziz, A.S.A.; Abdelmageed, A.A.; Alsaid, M.I.; Eldesouki, M.I. Modelling of Metaheuristics with Machine Learning-Enabled Cybersecurity in Unmanned Aerial Vehicles. *Sustainability* **2022**, *14*, 16741. https://doi.org/10.3390/su142416741

Academic Editors: Ming Hour Yang, Vijayalakshmi Murugesan and Mercy Shalinie Selvaraj

Received: 11 October 2022
Accepted: 1 December 2022
Published: 14 December 2022

1. Introduction

Nowadays, unmanned aerial vehicles (UAVs), also called drones, are gaining in popularity. They can be used for various purposes with regard to everyday flying objects interconnected with the internet, and can find themselves connected to other devices by sharing data through smart gadgets such as tablets and smartphones [1,2]. Put simply, drones are flying objects that either fly with the help of human pilots or autonomously. UAVs can be used for rescue operations, aerial photography, agriculture, package deliveries, environmental management, monitoring, and other perilous applications [3–5]. The

reliability of a UAV and its wireless communications are significant for crucial applications. Intrusion detection (ID) methods and security schemes have been employed for ensuring critical safety features. Drones may interact with terrestrial networks [6]. Due to the high probability of drones using ground-based line of sight (LoS) networks as well as the mobility, high elevation of the drones, and service quality needs, UAV-based wireless communication and cellular-connected UAV transmissions may vary from their terrestrial counterparts [7–9].

It is essential to frame data connection channels among UAVs to form a mobile self-organizing network if a greater number of drones cooperate to perform a task [10]. The drones in the network can realize real-time data sharing over this mobile network, which need not be sent by a ground station, and this could effectively enhance the combat ability and survivability of the drone group [11–14]. As the drone network is a subdivision of mobile ad hoc networks (MANETs), frequent attacks on the MANET can threaten the drone network. Due to the multiplicity of network access techniques and the openness of networks, drone networks have been covered by many security threats [15–17]. The defense function of conventional network security systems is generally passive, and it can be difficult to fight network attacks with changing technologies. An intrusion detection system (IDS) constitutes the inadequacies of conventional security technologies as an active defensive network security system. IDSs have acquired much interest from users, but certain issues exist that must be enhanced in real-time applications [18]. A classical IDS is inefficient and has an insufficient outcome, particularly in modern computer networks, including large traffic and a high bandwidth. Conventional IDSs cannot fulfill the demand of the present network security, which is very complex, distributed, and automated. Therefore, numerous authors have presented machine learning (ML) methods in the ID field and have made great achievements to diminish the false alarm rate and enhance the detection efficiency level of IDSs [19–21].

One of the main aspects of the design of a ML-based detection technique is the selection of a proper set of features to build the model. Provided with a dataset with a large number of features, the identification of proper features can considerably improve the classification performance. Generally, not all features are beneficial to the classification process and several features can be either treated as noisy, reducing the process performance, or highly correlated to one another and eliminated. Feature selection (FS) is a promising technique used to decrease the feature space and choose the most significant features. As an important pre-processing step in ML, FS has gained significance in network management, particularly in network intrusion detection. The inclusion of the FS process in the ML-based classification model reduces the computation complexity and increases the classification performance.

This study proposes a new metaheuristics with machine learning-enabled cybersecurity in unmanned aerial vehicles (MMLCS-UAVs) method. The presented MMLCS-UAV technique initially designed a quantum invasive weed optimization-based feature selection (QIWO-FS) method to improve the ID results. Next, a weighted regularized extreme learning machine (WRELM) model was applied to detect and categorize the intrusions. Finally, swallow swarm optimization (SSO) was used as a parameter tuning model for the WRELM model. The analysis of the results of the MMLCS-UAV technique was tested using benchmark datasets. Briefly, the contributions of this paper are given below.

- An intelligent MMLCS-UAV technique encompassing QIWO-FS, a WRELM classification, and SSO-based parameter tuning is introduced to detect intrusions in a UAV network.
- A QIWO-FS technique is developed using a standard IWO algorithm and quantum computing, which helps to select the useful features from the dataset.
- SSO-based parameter tuning for the WRELM model is designed to eliminate the tedious trial and error parameter tuning process. This also helps to enhance the predictive outcomes of the proposed model for unseen data.

The remaining sections of the paper are as follows. Section 2 elaborates on a detailed survey of existing works and Section 3 provides the proposed MMLCS-UAV technique. Section 4 provides the experimental validation of the proposed approach and Section 5 provides the concluding remarks.

2. Literature Review

Shrestha et al. [21] developed a drone- and satellite-oriented 5G network security system that could harness ML to efficiently discover cyberattacks and vulnerabilities. The solution could be classified into two parts: one was the application of a ML-oriented algorithm into satellite or terrestrial gateways and the other was the creation of a model for ID with the help of numerous ML techniques. Using a real-time CSE-CIC IDS-2018 network database, the system could identify different forms of attacks. To categorize the malicious or benign packets and enhance the security in drone networks, this study illustrated that ML techniques were employed. In [22], an effective technique of an IDS was formulated to identify anomalies in a vehicular system. An in-vehicle network (IVN) transmission system that was a control area network (CAN) was used in this work. The method could classify various attacks, including fuzzing attacks, on vehicles into reconnaissance and denial-of-service (DoS).

Zhang et al. [23] introduced an advanced technology termed an unmanned aerial system multifractal analysis IDS (AMDES) to recognize spoofing attacks. In an earlier study, an IDS related to a multifractal (MF) spectral analysis was employed to render precise MF spectrum predictions of network traffic. Tan et al. [24] modelled an ID technique related to deep belief networks (DBNs), boosted by a particle swarm optimization (PSO) algorithm. First, to gain an optimum DBN structure, a classifier method that relied upon the DBN was framed, the PSO method was employed to augment the hidden layer nodes of the DBN. Praveena et al. [25] introduced a deep reinforcement learning (DRL) method, optimized by the Black Widow Optimization technique for a drone network (DRL-BWO). Moreover, the DRL included an enhanced reinforcement learning-oriented DBN for ID. The BWO method was enforced for the parameter optimization of the DRL methodology. It aids the optimization of the ID performance of drone networks.

Masadeh et al. [26] applied a reinforcement learning (RL)-oriented method to solve the issue by allowing a drone to independently study the dynamics of a target or intruder. To be specific, numerous design variants of the RL-oriented method were applied that varied in the employed temporal difference approaches (state-action-reward-state-action or Q-learning) and in the exploration approaches (greedy or convergence-related ϵ-). Kumar et al. [27] introduced a new secure data sharing structure for software drone environments that combined deep learning and a blockchain (BC).

3. The Proposed Model

In this article, a new MMLCS-UAV technique was developed to accomplish cybersecurity in UAV networks. The presented MMLCS-UAV technique mainly focused on the recognition and classification of intrusions in the UAV network. In the presented MMLCS-UAV technique, a series of processes were carried out; namely, a feature subset selection using the QIWO-FS technique, a WRELM-based classification, and SSO-based parameter tuning. Figure 1 shows the workflow of MMLCS-UAV approach.

3.1. Algorithmic Design of the QIWO-FS Technique

The presented MMLCS-UAV technique introduced a new QIWO-FS technique to select the optimal feature subsets. As a population-based optimization technique, invasive weed optimization (IWO) can fulfill the remarkable outcome of the mathematical formula of randomization and adaptation of the weed colonies. The IWO technique is a powerful and new optimization algorithm that finds the global optimal solution of a mathematical function by mimicking the randomness and compatibility of a weed colony. This algorithm is utilized as an underlying structure for optimization approaches. It is a simple process

with a significant convergence speed, a lower computational encumbrance, independence to the problem, and near-global solutions; its gradient-free nature makes it useful for the resolution of FS problems.

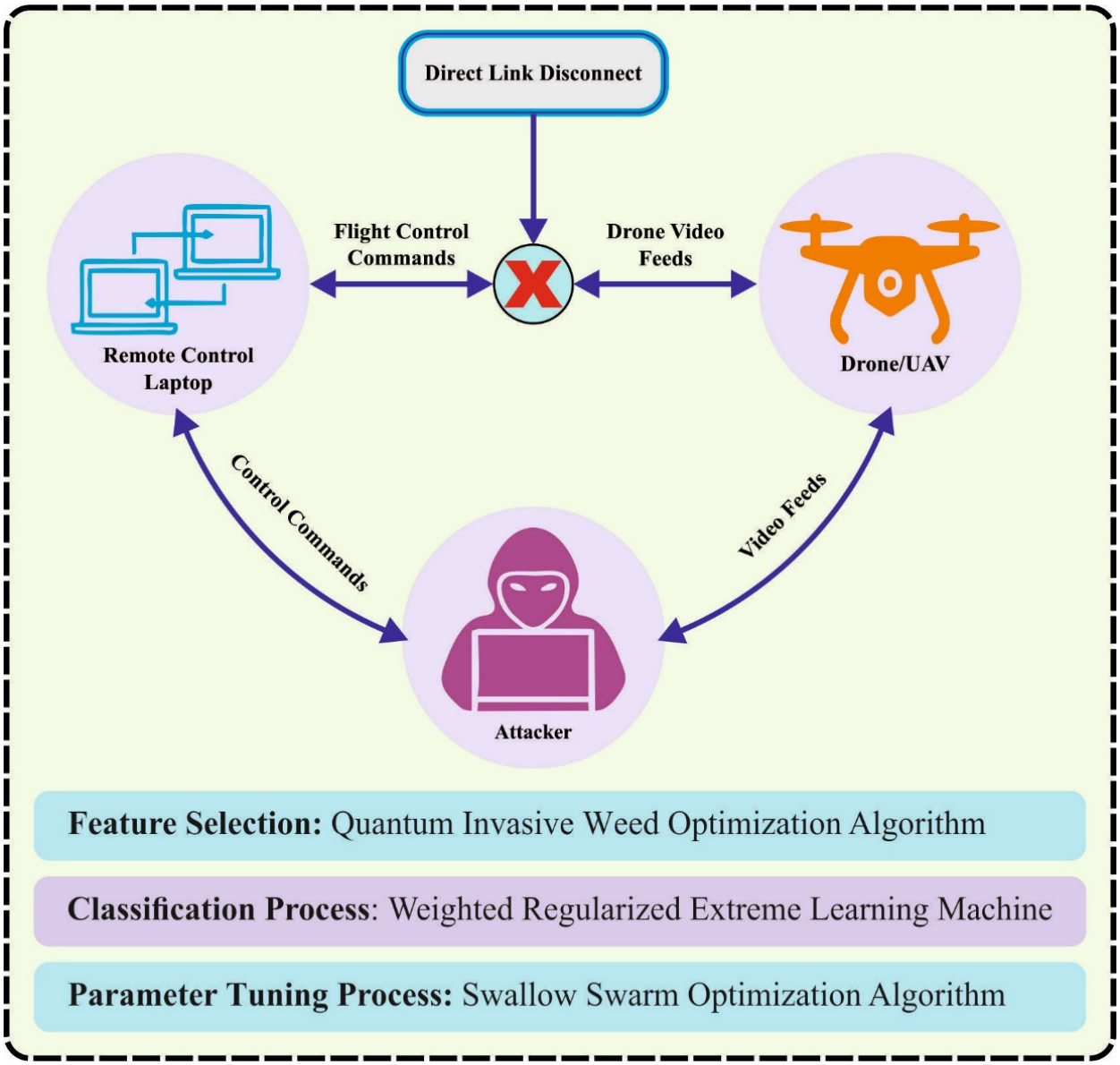

Figure 1. Workflow of MMLCS-UAV model.

The significant rise of weeds (strong herbs) is presumed to be a serious risk to plant products. Weeds have a high resistance level against environmental and climate changes. Thus, a strong optimization technique is obtained based on its features. In the presented method, the weed community and its resistance, compatibility, and randomness attempted to overcome the challenges. IWO was developed according to the phenomenon of agriculture; viz., motivated by an invasive weed colony. As previously mentioned, weeds (as a plant) are able to grow accidentally. There are various benefits to the existence of weeds in urban spaces. However, the accidental growth of these plants can encompass severe harm to human or planet activities; thus, it is regarded as a "weed". Although IWO is the simplest technique based on the concept, implementation, and structure, it is an efficient optimization technique to solve optimization problems [28]. The subsequent stages are essential to better understand the habitat behaviors and their weeds:

(1) Initializing Population: several seeds are partially spread in the searching space.
(2) Reproduction is initiated by pouring every individual plant into the flowering plant; then, the procedure can generate seeds that are worth their proportion. Later, the quantity of the plant seeds linearly decreases from $S_{\max}$ to $S_{\min}$:

$$n(w_i) = \frac{S_{\max}(\max fit - fit(w_i)) + S_{\min}(fit(w_i) - \min fit)}{\max fit - \min fit} \quad (1)$$

(3) This stage is related to determining a novel location of the seed in the search space. Here, the child seed is positioned near to the parents.
(4) Competitive removal is related to generating the optimum seeds. This happens whilst the amount of seeds obtains a certain range $(p_{\max})$.
(5) Finally, once the criteria are fulfilled, to finish the process, the second phase is repeated; otherwise, the procedure stops.

As a consequence of the IWO feature as well as the local and global potency for exploration and exploitation, and in addition to the prosperous results in vast quantities of applications, several effective ideas of the quantum concept have been applied to develop the performance of IWO. The fundamental method for QIWO is similar to IWO; certain advantageous variations are implemented to increase the exploration stage in a quantum searching space [29]. To optimize the stochastic module for initializing the seed (population), every seed can be determined by the one Q-bit, which is termed the Q-seed.

The state of the Q-bit (Ψ) is defined by:

$$\Psi = \bigcup_{j=1}^{n} |\psi_j(t)\} = [\alpha_j \ \beta_j]^T \quad j = 1, 2, \cdots, n \quad (2)$$

In Equation (2), α and β characterize the arbitrary integers that characterize the state possibility. $|\alpha|^2$ and $|\beta|^2$ correspondingly show the possibility that the Q-bit $|\psi\}$ depends on "0" and "1" states. Afterward, they fulfil the relationship $|\alpha|^2 + |\beta|^2 = 1$. Initially, the mediocrity of range $[0,\ 1]$ is selected as the first population.

$$\psi_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \end{bmatrix} \quad (3)$$

After initialization, the arbitrarily generated seed is normalized within zero and one:

$$|\psi\rangle_{[0,1]} = \frac{|\psi\rangle - \min(|\psi\rangle)}{Max(|\psi\rangle) - \min(|\psi\rangle)} \quad (4)$$

The max $(|\psi\rangle)$ and min $(|\psi\}$ correspondingly signify the maximal and minimal limits. In the presented technique, to produce the Q-seed, every individual was accomplished:

$$\left\{ \begin{array}{c} \alpha_j(t) = rand \\ |\alpha_j(t)|^2 + |\beta_j(t)|^2 = 1 \end{array} \right\} \Rightarrow$$
$$\left\{ \begin{array}{l} |\beta_j(t)| = \sqrt{1 - |\alpha_j(t)|^2} \Rightarrow \\ \beta_j(t) > 0 \& \alpha_j(t) > 0 \end{array} \right. \quad (5)$$
$$\therefore \beta_j(t) = \sqrt{1 - \alpha_j(t)^2}$$

In the FS mechanism, once the size of the feature vector refers to N, the sum of the combination of dissimilar features is likely to become 2^N, which is an enormous space for a comprehensive search. The presented hybrid technique was employed to dynamically search the feature space and produce an accurate combination of features. The FS fell

within the multi-objective problems because it fulfilled more than one objective to obtain a better solution, which decreased the group of selected features and concurrently decreased the performance of the output for the given classifier.

As aforesaid, the fitness function determines solutions in these scenarios to accomplish a balance amongst those objectives.

$$itness = \alpha\Delta_R(D) + \beta\frac{|Y|}{|T|} \tag{6}$$

In Equation (6), $\Delta_R(D)$ characterizes the classification error rate. $|Y|$ represents the size of the subset that the process chooses and $|T|$ is the total quantity of the features encompassed in the current dataset. α correspondingly shows the parameter $\in [0, 1]$ regarding the weight of the classification error rate and $\beta = 1 - \alpha$ indicates the significance of the reduction.

3.2. Intrusion Detection Process

For the intrusion detection, the MMLCS-UAV technique applied SSO to the WRELM model. The WRELM was introduced to enhance the standard extreme learning machine (ELM) and determine the optimum weight for all the instances [30]. We assumed that N was a hidden node from the ELM and sample pairs $\{X_i, P_i\}$; the resulting ELM was formulated by Equation (7):

$$f(X_i) = \sum_{n=1}^{N} \alpha_n H(\varphi_n, X_i, b_n), i = 1, 2, \ldots, N, \tag{7}$$

where $H(\cdot)$ symbolizes the activation functions, φ_n indicates the input weight vector, α_n implies the n^{th} resulting in weight, and b_n denotes the equivalent bias.

$$\widetilde{P} = H\alpha = \begin{bmatrix} H(\varphi_1, X_1, b_1) & H(\varphi_2, X_1, b_2) & \cdots & H(\varphi_N, X_1, b_N) \\ H(\varphi_1, X_2, b_1) & H(\varphi_2, X_2, b_2) & \cdots & H(\varphi_N, X_2, b_N) \\ \vdots & \vdots & \vdots & \vdots \\ H(\varphi_1, X_N, b_1) & H(\varphi_2, X_N, b_2) & \cdots & H(\varphi_N, X_N, b_N) \end{bmatrix} \cdot \alpha, \tag{8}$$

Here, $\widetilde{P}$ refers to the resulting vector.

To obtain the assessment of the α parameter, the major function was exploited by:

$$\text{argmin } \|\widetilde{P} - P\|_2^2 = \text{argmin } \|H\alpha - P\|_2^2, \tag{9}$$

In Equation (9), P denotes the observation data. The weight-regularized ELM is formulated by [31,32]:

$$\arg\min C\|\sigma\varepsilon\|_2^2 + \|\alpha\|_2^2 \tag{10}$$

Dependent on the state:

$$P = H\alpha + \varepsilon \tag{11}$$

In Equation (10), σ refers to the diagonal matrix, ε signifies the vector of regression error, and C epitomizes the regularized term. The Lagrange multiplier was introduced to resolve the abovementioned problem, and the corresponding solution to α is shown below:

$$\alpha = (H'\sigma^2 H + \frac{I}{C})^{-1} H'\sigma^2 P \tag{12}$$

The SSO approach was utilized to adjust the parameters related to the WRELM model. A major role of the SSO approach was energized by swallow swarm optimization [21]. There exists three diversities of particles; namely:

- An aimless particle (o_i);

- A leader particle (l_i);
- An explorer particle (e_i).

Every particle from the colony (each colony had a subcolony) was accountable for the whole performance; they guided the colony nearer to the optimal condition. The explorer particles included the population of the colony. First, it was responsible to explore the search space [33]. By properly achieving an extreme point, a varying sound guided the group near the location; when the location was led one from problem space, then these particles played as the head leader (HL_i). When the particles were at a favorable location similar to the adjacent particles, it was selected as the local leader (LL_i); otherwise, every particle e_i with respect to V_{LLi} (velocity vector of the particles near to the LL), V_{HLi} (velocity vector of the particle near to the HL), and the ability of backlash of these two bearings produced indiscriminative changes.

An aimless particle then started from the search condition, which did not have an optimal location, and the count of $f(o_i)$ was poor; they had arbitrary and exploratory searches. It began to arbitrarily move and did not have anything implemented with the location of HL_i and LL_i. In addition, there existed a particle from the SSO approach that was named the leader. The optimal leader, termed LH, was realized as a common leader in the colony. There also existed another particle, termed the LL [34,35].

$$V_{HLi+1} = V_{HLi} + \alpha_{HL}\, rand()(e_{best} - e_i) + \beta_{HL} rand()(HL_i - e_i) \quad (13)$$

$$V_{LLi+1} = V_{LLi} + \alpha_{LL} rand()(e_{best} - e_i) + \beta_{LL} rand()(LL_i - e_i) \quad (14)$$

where V_{HL} = Velocity of the HL, V_{LL} = velocity of the LL, e_{best} = better location of the explorer particle, and $e_i \rightarrow$ presents the location of the explorer particle:

$$V_{i+1} = V_{HLi+1} + V_{LLi+1} \quad (15)$$

The particle values were upgraded by:

$$e_{i+1} = e_i + V_{i+1} \quad (16)$$

In order to attain improvised classifier results, the SSO algorithm derived a fitness function as given below.

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

4. Performance Validation

In this section, the performance validation of the MMLCS-UAV technique is briefly investigated. Figure 2 depicts the confusion matrices of the MMLCS-UAV method. The results indicated that the MMLCS-UAV approach properly recognized all the attacks that existed in the dataset.

Table 1 offers the overall cybersecurity performance of the MMLCS-UAV technique on 80% of the training (TR) data and 20% of the testing (TS) data. Figure 3 reports an average classification outcome of the MMLCS-UAV methodology on 80% of the TR data. The results exhibited that the MMLCS-UAV method showed the maximum performance in each class. It was noticed that the MMLCS-UAV system attained an average $accu_y$ of 99.37%, $prec_n$ of 98.11%, $reca_l$ of 98.11%, F_{score} of 98.11%, and a Matthew's correlation coefficient (MCC) of 97.73%.

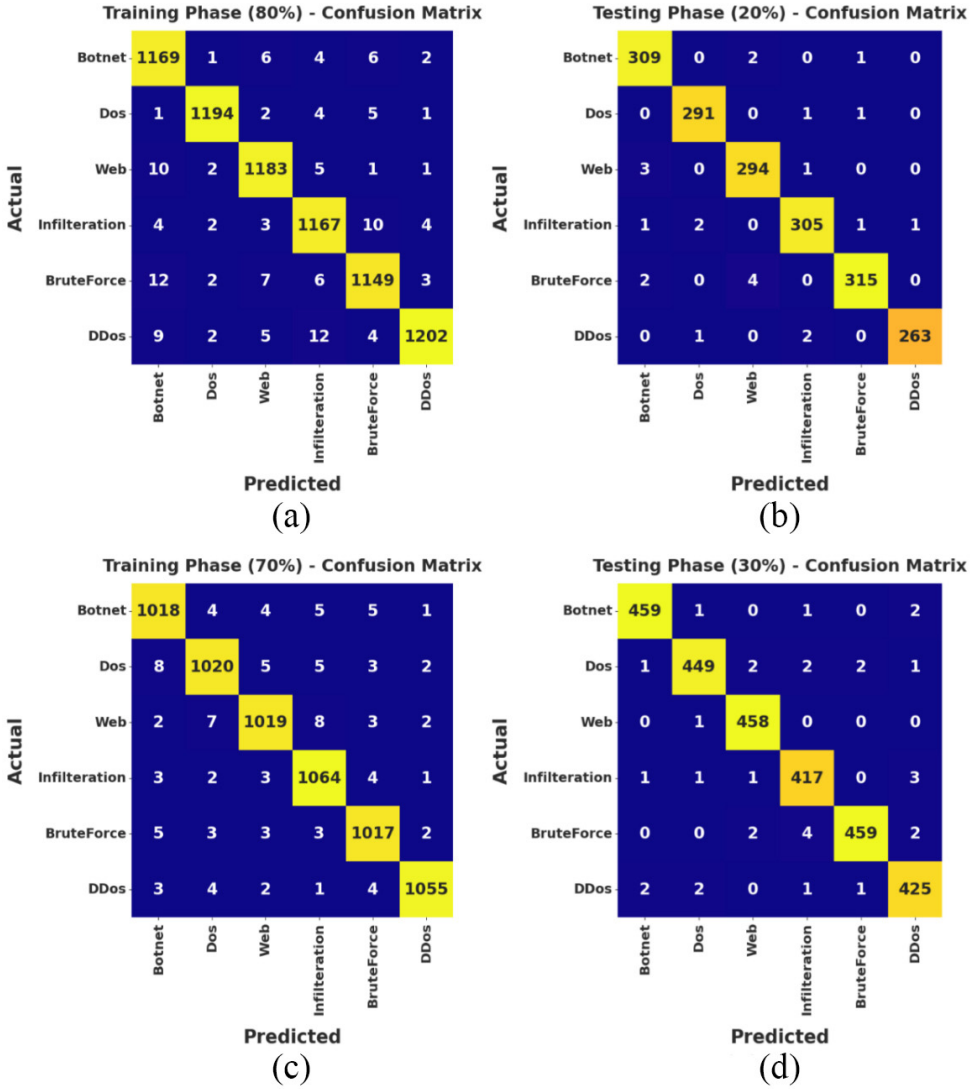

Figure 2. Confusion matrices of MMLCS-UAV model.

Table 1. Overall results of MMLCS-UAV model on 80:20 of TR/TS data.

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	MCC
			Training Phase (80%)		
Botnet	99.24	97.01	98.40	97.70	97.25
Dos	99.69	99.25	98.92	99.09	98.90
Web	99.42	98.09	98.42	98.26	97.91
Infilteration	99.25	97.41	98.07	97.74	97.29
BruteForce	99.22	97.79	97.46	97.62	97.16
DDos	99.40	99.09	97.41	98.24	97.89
Average	99.37	98.11	98.11	98.11	97.73
			Testing Phase (20%)		
Botnet	99.50	98.10	99.04	98.56	98.26
Dos	99.72	98.98	99.32	99.15	98.98
Web	99.44	98.00	98.66	98.33	98.00
Infilteration	99.50	98.71	98.39	98.55	98.24
BruteForce	99.50	99.06	98.13	98.59	98.29
DDos	99.78	99.62	98.87	99.25	99.12
Average	99.57	98.74	98.73	98.74	98.48

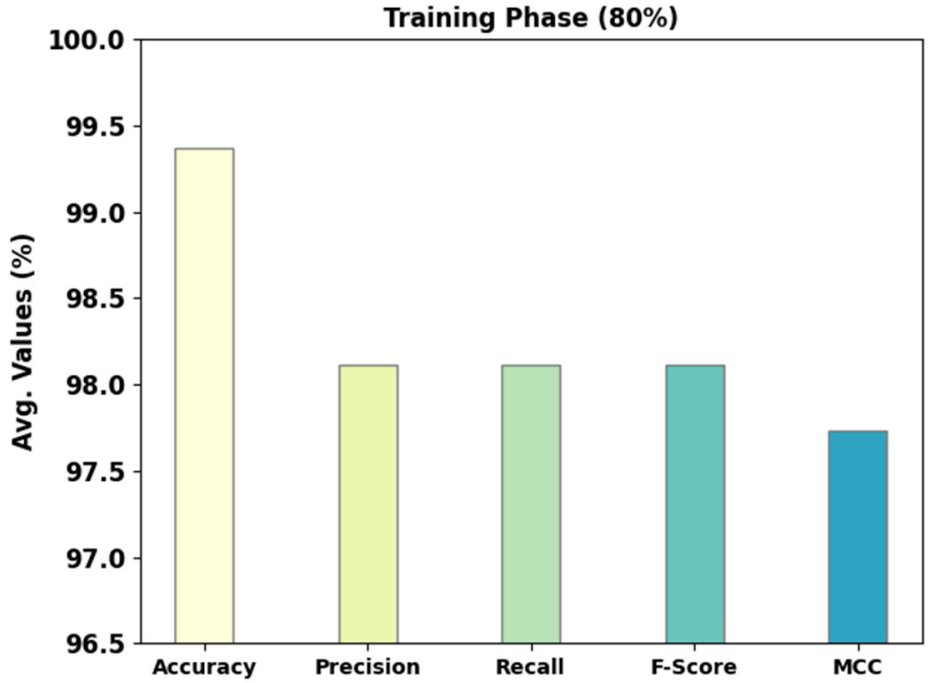

Figure 3. Classification results of MMLCS-UAV technique on 80% of TR data.

Figure 4 portrays the average classification outcomes of the MMLCS-UAV technique on 20% of the TS data. The results exhibited that the MMLCS-UAV method displayed the maximum performance in each class. Note that the MMLCS-UAV methodology gained an average $accu_y$ of 99.57%, $prec_n$ of 98.74%, $reca_l$ of 98.73%, F_{score} of 98.74%, and MCC of 98.48%.

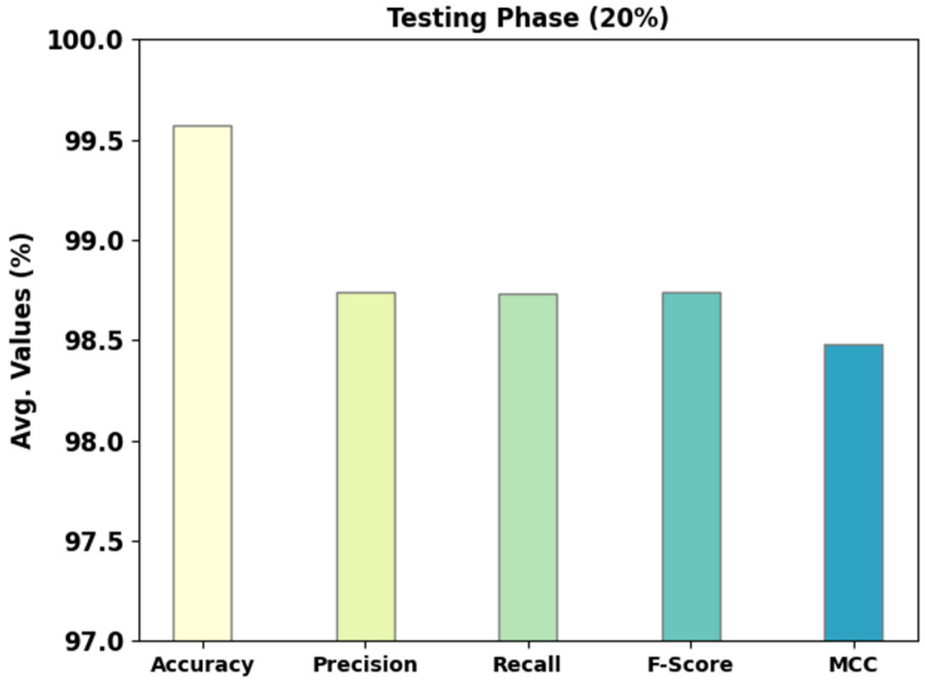

Figure 4. Classification results of MMLCS-UAV model on 20% of TS data.

Table 2 presents the overall cybersecurity performance of the MMLCS-UAV technique on 70% of the TR data and 30% of the TS data. Figure 5 shows the average classification outcomes of the MMLCS-UAV approach on 70% of the TR data. The outcomes displayed that the MMLCS-UAV approach exposed the maximum performance for each class. It was

noted that the MMLCS-UAV method achieved an average $accu_y$ of 99.43%, $prec_n$ of 98.30%, $reca_l$ of 98.30%, F_{score} of 98.30%, and MCC of 97.96%.

Table 2. Overall results of MMLCS-UAV model on 70:30 of TR/TS data.

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	MCC
Training Phase (70%)					
Botnet	99.37	97.98	98.17	98.07	97.69
Dos	99.32	98.08	97.79	97.94	97.53
Web	99.38	98.36	97.89	98.12	97.75
Infilteration	99.44	97.97	98.79	98.38	98.05
BruteForce	99.44	98.17	98.45	98.31	97.98
DDos	99.65	99.25	98.69	98.97	98.76
Average	99.43	98.30	98.30	98.30	97.96
Testing Phase (30%)					
Botnet	99.70	99.14	99.14	99.14	98.96
Dos	99.52	98.90	98.25	98.57	98.28
Web	99.78	98.92	99.78	99.35	99.22
Infilteration	99.48	98.12	98.58	98.35	98.04
BruteForce	99.59	99.35	98.29	98.82	98.57
DDos	99.48	98.15	98.61	98.38	98.07
Average	99.59	98.76	98.77	98.77	98.52

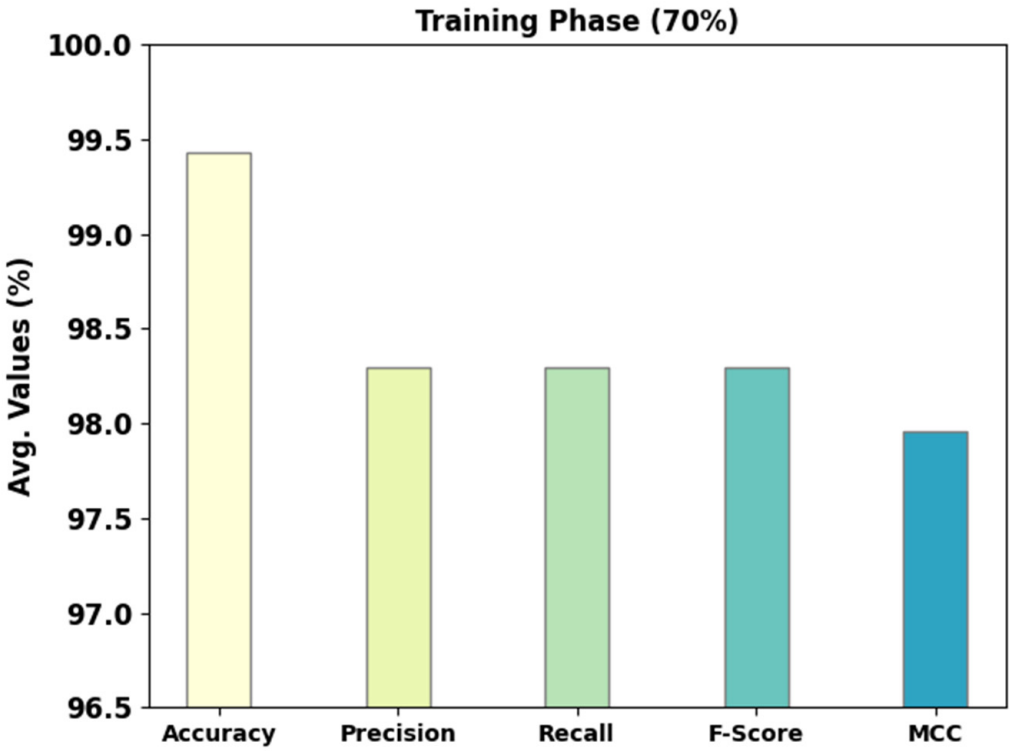

Figure 5. Classification results of MMLCS-UAV model on 70% of TR data.

Figure 6 exhibits the average classification outcome of the MMLCS-UAV model on 30% of the TS data. The outcome exhibited that the MMLCS-UAV technique showed the maximum performance in each class. It was noticed that the MMLCS-UAV method achieved an average $accu_y$ of 99.59%, $prec_n$ of 98.76%, $reca_l$ of 98.77%, F_{score} of 98.77%, and MCC of 98.52%.

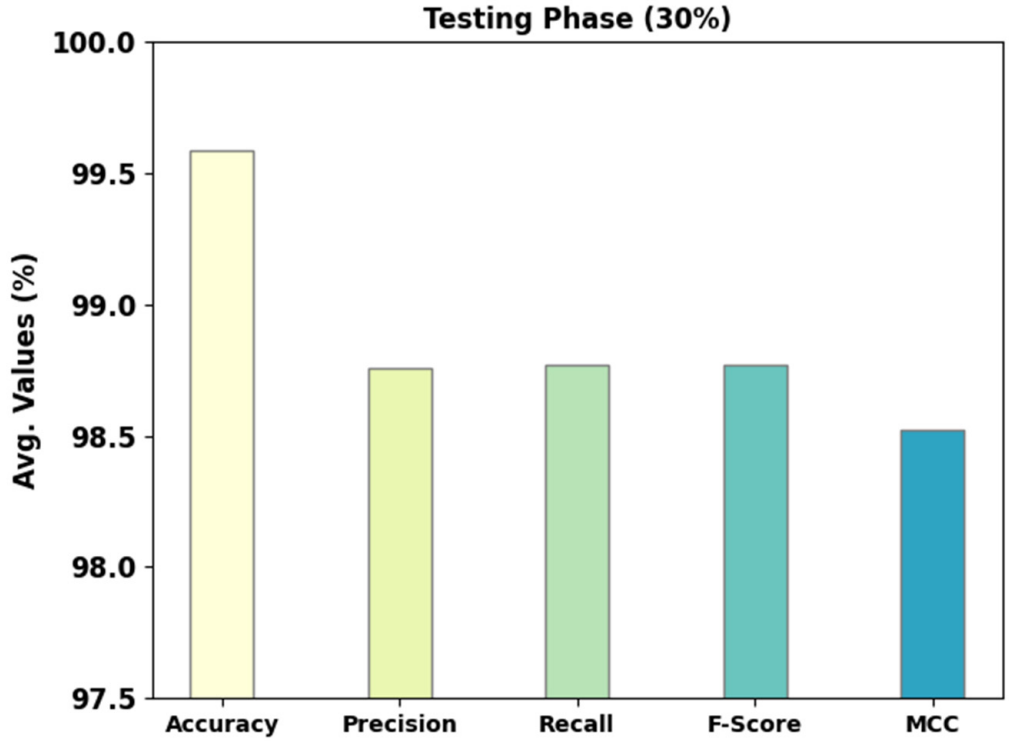

Figure 6. Classification outcomes of MMLCS-UAV technique on 30% of TS data.

In Table 3, a comparison study of the MMLCS-UAV technique with existing approaches [21,24] such as a genetic algorithm with DBN (GA-DBN), a butterfly optimization algorithm with DBN (BOA-DBN), k-nearest neighbor (KNN), logistic regression (LR), a linear discriminant analysis (LDA), Gaussian Naive Bayes (GNB), and decision tree (DT) is provided. Figure 7 examines the comparative $accu_y$ examination of the MMLCS-UAV model with other existing models. The results signified that the GA-DBN, BOA-DBN, LR, and LDA models reached a minimal $accu_y$ of 91.76%, 91.13%, 91.65%, and 92%, respectively.

Table 3. Comparison study of MMLCS-UAV model with recent models [21,24].

Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
MMLCS-UAV	99.59	98.76	98.77	98.77
GA-DBN	91.76	90.28	98.14	98.02
BOA-DBN	91.13	89.70	98.47	97.86
LR Model	91.65	90.51	98.63	96.33
LDA Model	92.00	90.89	98.41	97.19
KNN Model	97.80	97.85	95.34	95.39
DT Model	95.70	95.60	97.34	96.77
GNB Model	96.50	96.56	98.15	96.40

Meanwhile, the DT and GNB models gained closer $accu_y$ values of 95.70% and 96.50%, respectively. Although the KNN model attained a reasonable $accu_y$ of 97.80%, the MMLCS-UAV model ensured a maximum $accu_y$ of 99.59%.

Figure 8 inspects the comparative $accu_y$ examination of the MMLCS-UAV model with the other existing techniques. The results signified that the KNN, DT, GA-DBN, and GNB models reached a minimal $accu_y$ of 89.7, 90.28, 90.51, and 90.89%, respectively. Meanwhile, the LDA and BOA-DBN methods obtained closer $accu_y$ values of 95.6 and 96.56%, respectively. Although the LR approach attained a reasonable $accu_y$ of 97.85%, the MMLCS-UAV method ensured a maximum $accu_y$ of 98.76%.

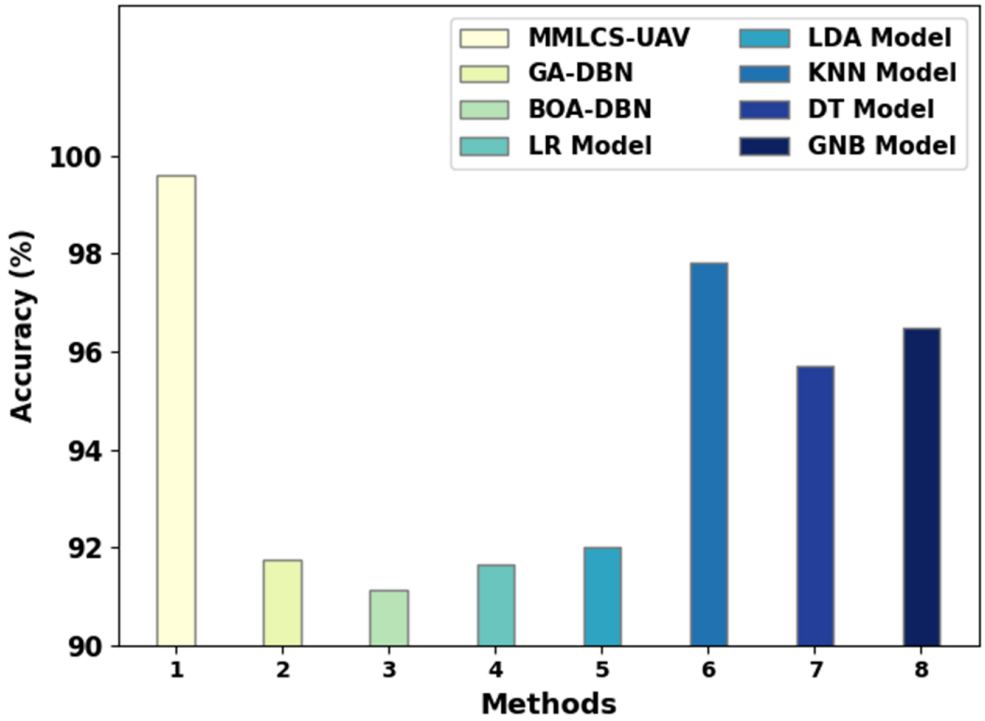

Figure 7. Comparative $accu_y$ assessment of MMLCS-UAV model.

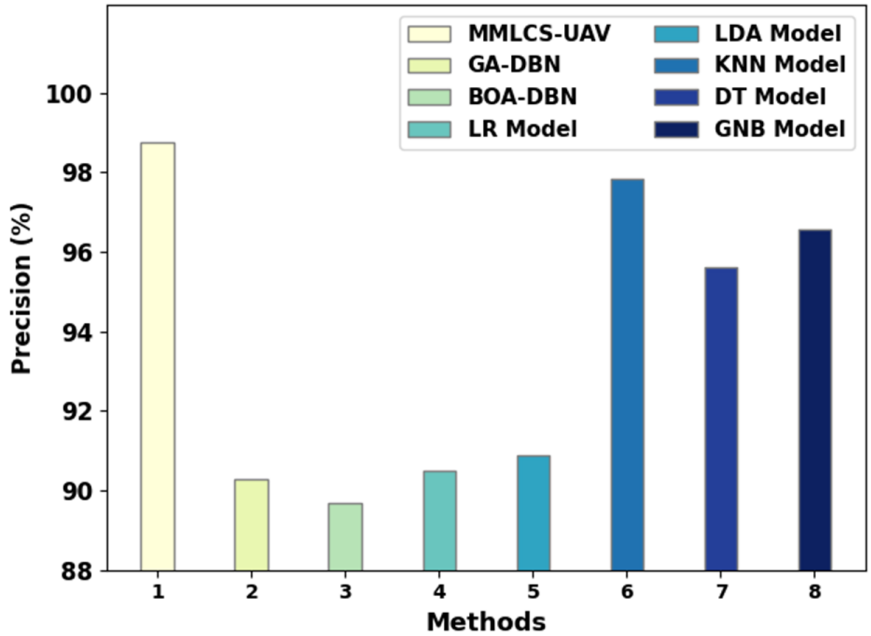

Figure 8. Comparative $prec_n$ assessment of MMLCS-UAV model.

Figure 9 portrays the comparative $accu_y$ examination of the MMLCS-UAV approach with the other existing techniques. The results signified that the KNN, DT, GA-DBN, and GNB models reached a minimal $accu_y$ of 95.34, 97.34, 98.14, and 98.15%, respectively. Simultaneously, the LDA and BOA-DBN methods achieved closer $accu_y$ values of 98.41 and 98.47%, respectively. Although the LR method attained a reasonable $accu_y$ of 98.63%, the MMLCS-UAV algorithm ensured a maximum $accu_y$ of 98.77%.

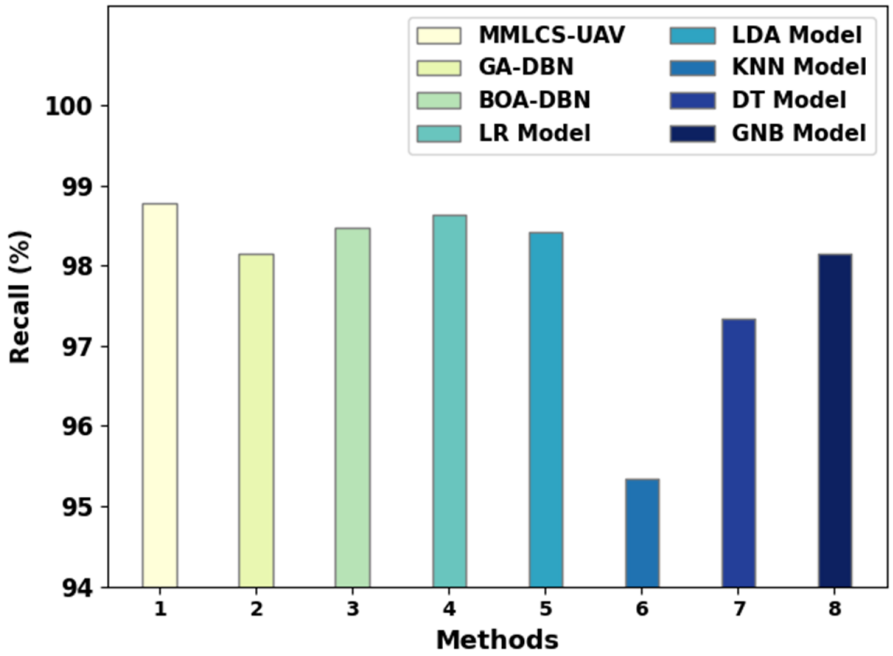

Figure 9. Comparative $reca_l$ assessment of MMLCS-UAV model.

Figure 10 displays the comparative $accu_y$ inspection of the MMLCS-UAV method with the other existing approaches. The results exhibited that the KNN, DT, GA-DBN, and GNB approaches reached a minimal $accu_y$ of 95.39, 96.33, 96.4, and 96.77%, respectively.

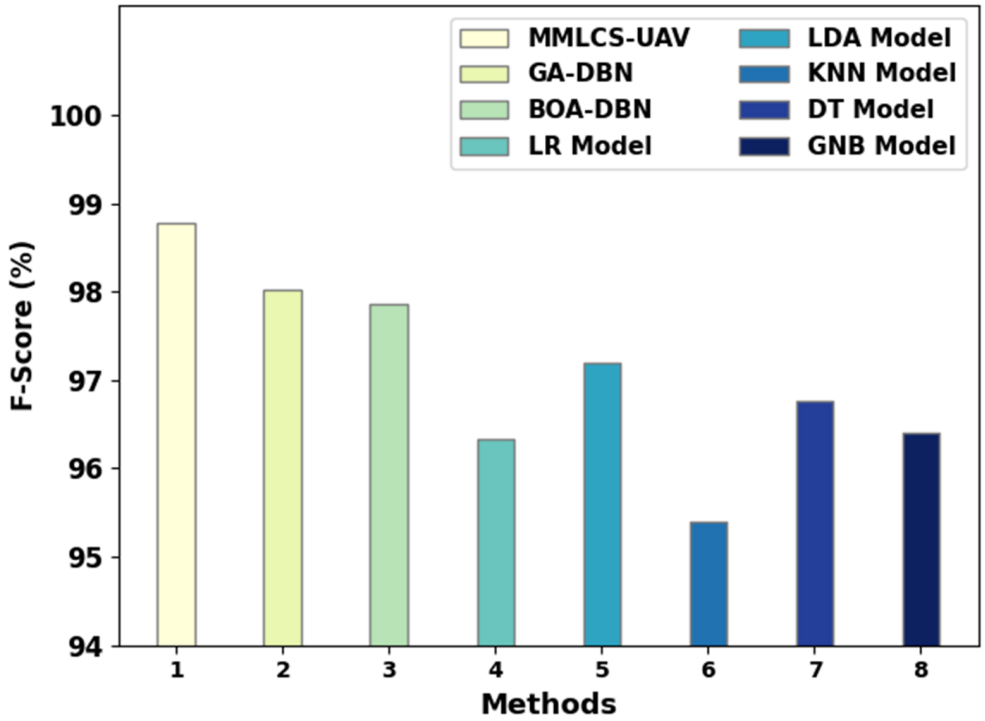

Figure 10. Comparative F_{score} assessment of MMLCS-UAV model.

In the meantime, the LDA and BOA-DBN techniques reached closer $accu_y$ values of 97.19 and 97.86%, respectively. Although the LR technique reached a reasonable $accu_y$ of 98.02%, the MMLCS-UAV method ensured a maximum $accu_y$ of 98.77%. These results highlighted the supreme performance of the MMLCS-UAV model.

5. Conclusions

In this article, a new MMLCS-UAV technique was developed to accomplish cybersecurity in UAV networks. The presented MMLCS-UAV technique mainly focused on the recognition and classification of intrusions in a UAV network. To obtain this, the presented MMLCS-UAV technique introduced a new QIWO-FS technique to select the optimal feature subsets. For intrusion detection, the MMLCS-UAV technique applied SSO to the WRELM model. The design of the QIWO algorithm and SSO algorithm helped to accomplish an enhanced classification performance. A widespread comparison study reported the superiority of the MMLCS-UAV technique over other existing approaches, with a highest accuracy of 99.59%, precision of 98.76%, recall of 98.77%, and F-score of 98.77%. Thus, the presented MMLCS-UAV technique could be employed for maximum cybersecurity in UAV networks. In the future, deep learning-based classifiers can be introduced to improve secure UAV communications. Moreover, the proposed algorithm could be tested on a large-scale real-time dataset. Additionally, data clustering techniques could be involved to improve the classification performance and security of UAV networks.

Author Contributions: Conceptualization, K.T.; Methodology, A.S.A.A.; Software, A.A.A. and M.I.A.; Validation, M.R., H.A.M., M.A., A.S.A.A., A.A.A. and M.I.E.; Formal analysis, M.I.A.; Investigation, M.I.E.; Resources, A.S.A.A.; Data curation, K.T. and A.A.A.; Writing—original draft, M.R., H.A.M., M.A. and K.T.; Writing—review & editing, A.S.A.A., M.I.A. and M.I.E.; Visualization, A.A.A.; Supervision, M.A.; Project administration, M.R. 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 the Large Groups Project under grant number (180/43). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R114), 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: (22UQU4331004DSR07).

Institutional Review Board Statement: This article does not contain any studies with human participants performed by any of the authors.

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 that they have no conflict of interest. The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript.

References

1. Shrestha, R.; Bajracharya, R.; Kim, S. 6G Enabled Unmanned Aerial Vehicle Traffic Management: A Perspective. *IEEE Access* **2021**, *9*, 91119–91136. [CrossRef]
2. Chien, W.C.; Lai, C.F.; Hossain, M.S.; Muhammad, G. Heterogeneous Space and Terrestrial Integrated Networks for IoT: Architecture and Challenges. *IEEE Netw.* **2018**, *33*, 15–21. [CrossRef]
3. Karatas, G.; Demir, O.; Sahingoz, O.K. Increasing the Performance of Machine Learning-Based IDSs on an Imbalanced and Up-to-Date Dataset. *IEEE Access* **2020**, *8*, 32150–32162. [CrossRef]
4. Shrestha, R.; Nam, S.Y.; Bajracharya, R.; Kim, S. Evolution of V2X Communication and Integration of Blockchain for Security Enhancements. *Electronics* **2020**, *9*, 1338. [CrossRef]
5. Leevy, J.L.; Khoshgoftaar, T.M. A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data. *J. Big Data* **2020**, *7*, 104. [CrossRef]
6. Ferrag, M.A.; Maglaras, L. DeliveryCoin: An IDS and Blockchain-Based Delivery Framework for Drone-Delivered Services. *Computers* **2019**, *8*, 58. [CrossRef]
7. D'hooge, L.; Wauters, T.; Volckaert, B.; De Turck, F. Inter-dataset generalization strength of supervised machine learning methods for intrusion detection. *J. Inf. Secur. Appl.* **2020**, *54*, 102564. [CrossRef]
8. Kim, J.; Kim, J.; Kim, H.; Shim, M.; Choi, E. CNN-Based Network Intrusion Detection against Denial-of-Service Attacks. *Electronics* **2020**, *9*, 916. [CrossRef]

9. Gamage, S.; Samarabandu, J. Deep learning methods in network intrusion detection: A survey and an objective comparison. *J. Netw. Comput. Appl.* **2020**, *169*, 102767. [CrossRef]
10. Zhang, H.; Li, J.L.; Liu, X.M.; Dong, C. Multi-dimensional feature fusion and stacking ensemble mechanism for network intrusion detection. *Future Gener. Comput. Syst.* **2021**, *122*, 130–143. [CrossRef]
11. Fotohi, R.; Abdan, M.; Ghasemi, S. A Self-Adaptive Intrusion Detection System for Securing UAV-to-UAV Communications Based on the Human Immune System in UAV Networks. *J. Grid Comput.* **2022**, *20*, 22. [CrossRef]
12. 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]
13. 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]
14. Basan, E.; Lapina, M.; Mudruk, N.; Abramov, E. Intelligent intrusion detection system for a group of UAVs. In *International Conference on Swarm Intelligence*; Springer: Cham, Switzerland, 2021; pp. 230–240.
15. Whelan, J.; Almehmadi, A.; El-Khatib, K. Artificial intelligence for intrusion detection systems in unmanned aerial vehicles. *Comput. Electr. Eng.* **2022**, *99*, 107784. [CrossRef]
16. Wang, C.N.; Yang, F.C.; Nguyen, V.T.T.; Nguyen, Q.M.; Huynh, N.T.; Huynh, T.T. Optimal Design for Compliant Mechanism Flexure Hinges: Bridge-Type. *Micromachines* **2021**, *12*, 1304. [CrossRef]
17. Radanliev, P.; De Roure, D.; Maple, C.; Ani, U. Super-forecasting the 'technological singularity'risks from artificial intelligence. *Evol. Syst.* **2022**, *13*, 747–757. [CrossRef]
18. Radanliev, P.; De Roure, D.; Maple, C.; Santos, O. Forecasts on Future Evolution of Artificial Intelligence and Intelligent Systems. *IEEE Access* **2022**, *10*, 45280–45288. [CrossRef]
19. Wang, C.N.; Yang, F.C.; Nguyen, V.T.T.; Vo, N.T. CFD analysis and optimum design for a centrifugal pump using an effectively artificial intelligent algorithm. *Micromachines* **2022**, *13*, 1208. [CrossRef]
20. Nguyen, T.V.; Huynh, N.T.; Vu, N.C.; Kieu, V.N.; Huang, S.C. Optimizing compliant gripper mechanism design by employing an effective bi-Algorithm: Fuzzy logic and ANFIS. *Microsyst. Technol.* **2021**, *27*, 3389–3412. [CrossRef]
21. Shrestha, R.; Omidkar, A.; Roudi, S.A.; Abbas, R.; Kim, S. Machine-learning-enabled intrusion detection system for cellular connected UAV networks. *Electronics* **2021**, *10*, 1549. [CrossRef]
22. Basavaraj, D.; Tayeb, S. Towards a Lightweight Intrusion Detection Framework for In-Vehicle Networks. *J. Sens. Actuator Netw.* **2022**, *11*, 6. [CrossRef]
23. Zhang, R.; Condomines, J.P.; Lochin, E. A Multifractal Analysis and Machine Learning Based Intrusion Detection System with an Application in a UAS/RADAR System. *Drones* **2022**, *6*, 21. [CrossRef]
24. Tan, X.; Su, S.; Zuo, Z.; Guo, X.; Sun, X. Intrusion detection of UAVs based on the deep belief network optimized by PSO. *Sensors* **2019**, *19*, 5529. [CrossRef]
25. Praveena, V.; Vijayaraj, A.; Chinnasamy, P.; Ali, I.; Alroobaea, R.; Alyahyan, S.Y.; Raza, M.A. Optimal deep reinforcement learning for intrusion detection in UAVs. *CMC-Comput. Mater. Contin.* **2022**, *70*, 2639–2653. [CrossRef]
26. Masadeh, A.E.; Alhafnawi, M.; Salameh, H.A.B.; Musa, A.; Jararweh, Y. Reinforcement Learning-Based Security/Safety UAV System for Intrusion Detection Under Dynamic and Uncertain Target Movement. *IEEE Trans. Eng. Manag.* **2022**, 1–11. [CrossRef]
27. Kumar, P.; Kumar, R.; Kumar, A.; Franklin, A.A.; Jolfaei, A. Blockchain and deep learning empowered secure data sharing framework for softwarized uavs. In Proceedings of the 2022 IEEE International Conference on Communications Workshops (ICC Workshops), Seoul, Republic of Korea, 16–20 May 2022; pp. 770–775.
28. Misaghi, M.; Yaghoobi, M. Improved invasive weed optimization algorithm (IWO) based on chaos theory for optimal design of PID controller. *J. Comput. Des. Eng.* **2019**, *6*, 284–295. [CrossRef]
29. Razmjooy, N.; Razmjooy, S. Skin melanoma segmentation using neural networks optimized by quantum invasive weed optimization algorithm. In *Metaheuristics and Optimization in Computer and Electrical Engineering*; Springer: Cham, Switzerland, 2021; pp. 233–250.
30. Alizadeh, A.; Rajabi, A.; Shabanlou, S.; Yaghoubi, B.; Yosefvand, F. Modeling long-term rainfall-runoff time series through wavelet-weighted regularization extreme learning machine. *Earth Sci. Inform.* **2021**, *14*, 1047–1063. [CrossRef]
31. Wang, Y.; Zhou, G. The Novel Successive Variational Mode Decomposition and Weighted Regularized Extreme Learning Machine for Fault Diagnosis of Automobile Gearbox. *Shock. Vib.* **2021**, *2021*, 5544031. [CrossRef]
32. Maimaitiyiming, M.; Sagan, V.; Sidike, P.; Kwasniewski, M.T. Dual activation function-based Extreme Learning Machine (ELM) for estimating grapevine berry yield and quality. *Remote Sens.* **2019**, *11*, 740. [CrossRef]
33. Poongodi, K.; Kumar, D. Mining serial positioning episode rules by natural exponent inertia weight based swallow swarm optimization algorithm with constraint based event sequences. *J. Intell. Fuzzy Syst.* **2021**, *40*, 4599–4615. [CrossRef]
34. Neshat, M.; Sepidnam, G.; Sargolzaei, M. Swallow swarm optimization algorithm: A new method to optimization. *Neural Comput. Appl.* **2013**, *23*, 429–454. [CrossRef]
35. Hodashinsky, I.; Sarin, K.; Shelupanov, A.; Slezkin, A. Feature selection based on swallow swarm optimization for fuzzy classification. *Symmetry* **2019**, *11*, 1423. [CrossRef]