Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.036735
Article

Machine Learning Based Cybersecurity Threat Detection for Secure IoT Assisted Cloud Environment

Z. Faizal Khan[1], Saeed M. Alshahrani[2,*], Abdulrahman Alghamdi[2], Someah Alangari[3], Nouf Ibrahim Altamami[4], Khalid A. Alissa[5], Sana Alazwari[6], Mesfer Al Duhayyim[7] and Fahd N. Al-Wesabi[8]

[1]Department of Computer Engineering, College of Computing and Information Technology, Shaqra University, Shaqra, Saudi Arabia
[2]Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra, Saudi Arabia
[3]Department of Computer Science, College of Science and Humanities Dawadmi, Shaqra University, Shaqra, Saudi Arabia
[4]Department of Mathematics, College of Education, Shaqra University, Shaqra, Saudi Arabia
[5]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
[6]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif P.O. Box 11099, Taif, 21944, Saudi Arabia
[7]Department of Computer Science, College of Sciences and Humanities-Aflaj, Prince Sattam bin Abdulaziz University, Alaflaj, 16828, Saudi Arabia
[8]Department of Computer Science, College of Science & Art at Mahayil, King Khalid University, Saudi Arabia
*Corresponding Author: Saeed M. Alshahrani. Email: salshahrani@su.edu.sa
Received: 10 October 2022; Accepted: 21 December 2022; Published: 26 May 2023

Abstract: The Internet of Things (IoT) is determine enormous economic openings for industries and allow stimulating innovation which obtain between domains in childcare for eldercare, in health service to energy, and in developed to transport. Cybersecurity develops a difficult problem in IoT platform whereas the presence of cyber-attack requires that solved. The progress of automatic devices for cyber-attack classifier and detection employing Artificial Intelligence (AI) and Machine Learning (ML) devices are crucial fact to realize security in IoT platform. It can be required for minimizing the issues of security based on IoT devices efficiently. Thus, this research proposal establishes novel mayfly optimized with Regularized Extreme Learning Machine technique called as MFO-RELM model for Cybersecurity Threat classification and detection from the cloud and IoT environments. The proposed MFO-RELM model provides the effective detection of cybersecurity threat which occur in the cloud and IoT platforms. To accomplish this, the MFO-RELM technique pre-processed the actual cloud and IoT data as to meaningful format. Besides, the proposed models will receive the pre-processing data and carry out the classifier method. For boosting the efficiency of the proposed models, the MFO technique was utilized to it. The experiential outcome of the proposed technique was tested utilizing the standard CICIDS 2017 dataset, and the outcomes are examined under distinct aspects.

Keywords: Mayfly optimization; machine learning; artificial intelligence; cybersecurity; threat detection

1 Introduction

The Internet of Things (IoT) is central to digital transformation in several industrial sectors [1]. Owing to the pervasive nature of such gadgets and due to the simplicity of observing and controlling gadgets from distant places, there occurs a fast advancement in framing various new applications in numerous fields like connected industrial and manufacturing sensors and equipment, smart home devices, health monitoring gadgets, energy management gadgets, wearable devices, etc. [2,3]. The main concern in the IoT network was managing the device's security and data protection from assaults. Cyber-attacks were unauthorized access or intentional exploitation of infrastructures or information of other organizations or individuals [4]. Protection of IoT gadgets from assaults becomes a problem because of the heterogeneity of protocols and gadgets, direct exposure of gadgets to the internet, and resource limits on devices. The mitigation method presented for IT networks does not suit the IoT atmosphere, and some Machine Learning (ML) techniques were advanced for detecting assaults based on IoT traffic paradigms [5,6]. ML techniques will be appropriate since they can be implemented in several applications like anomaly detection (AD), data classification, and clustering [7].

Several research works are focused on solving the security problems and difficulties of cloud computing (CC) and IoT by utilizing a lightweight authentication procedure, the data security searching and sharing of cloud-related IoT [8]. They could operate the consistency and accuracy of IoT data for its complete lifetime [9]. Thus, these cyber-attacks should be solved for safe IoT usage [10]. Subsequently, massive efforts to manage the security problems in the IoT method were made recently. Another cyber threat was malware. Malware or malicious software has software which can be fixed on a computer for disrupting their function and damage electrical data. Trojan horses, viruses, spyware, ransomware, malvertising, worms, and adware are important malware forms [11]. Malign intrusions on the computer network and gadgets were other cyber-attack to cyberspace. Such intrusions were utilized for identifying and scanning the susceptibilities of a computer system or network [12]. An intrusion detection system (IDS) can be utilized for protecting beside such intrusion [13]. ML has become the most effective and basic technique for competing with cyber-attacks and solving the limits of predictable security mechanisms. Disdain has all its charms, and ML methods have their limitations and constraints. ML is a subclass of AI [14]. The captivating superiority of ML methods was that ML methods did not program explicitly since they could mechanically learn from their experience for generating the outcomes.

This paper designs a novel mayfly optimized with Regularized Extreme Learning Machine approach called as MFO-RELM model, for cybersecurity threat classifier and detection in the cloud and IoT environments. The proposed MFO-RELM model primarily pre-processes the actual cloud and IoT data as to meaningful format. Besides, the proposed methodology will receive the pre-processing data and carry out the classifier system using the RELM model. For boosting the efficiency of the proposed models, the MFO algorithms are utilized to it. High-accurate simulations and several scenarios of experiments will be performed. The experimental validation of the presented systems will be tested utilizing standard databases in several features.

2 Related Works

Kumar et al. [15] introduced an intellectual cyber-attack detection mechanism for IoT systems with the use of a new hybrid feature minimized technique. This method initially executes feature ranking utilizing correlation co-efficient, RF, mean diminishing accuracy, and gaining ratio for gaining 3 distinct feature sets. After, features were integrated through the usage of a suitable devised system (AND operations), for gaining a single optimizer feature set. At last, the gained diminish feature sets were given to 3 renowned ML techniques like RF, K-NN, and XGBoost, for detecting cyberattacks. In [16], the cognitive ML-enabled attack detection structure was devised for sharing medical data securely. The healthcare CPS is efficient in dispersing the accumulated data to cloud storage. ML approaches forecast cyber-attack behaviour in the healthcare decision support system. In [17], the authors sightsee an assault and AD method based on ML approaches like KNN, LR, RF, SVM, ANN, and DT for defending against and mitigating IoT cybersecurity menaces in smart cities. Or otherwise, prevailing studies that concentrate on one classifier, the authors even sightsee ensemble approaches such as stacking, bagging and boosting for enhancing the activity of the detection mechanism.

A decentralized system of security was offered in [18] utilizing a SDN compiled with blockchain (BC) for IoT in fog and mobile edge computing. The SDN incessantly analyses and observes the traffic of a system to offer an assault recognition approach. The BC was leveraged for overcoming the failure problems faced in the current techniques by distributing a decentralized attack recognition technique that identifies assaults in fog and minimizes it in edge nodes. In [19], the authors rendered the complete advancement of novel intellectual and autonomous DL-related classification and detection mechanism for cyber threats in IoT transmission network which uses the power of CNN is named IoT-IDCS-CNN (IoT related intrusion detection and classifier mechanism utilizing CNN). The presented IoT-IDCS-CNN uses higher efficiency computing which uses the powerful Compute Unified Device Architecture (CUDA) related parallel processing and Nvidia GPUs that uses high-speed I9-core-related Intel CPUs.

Elsisi et al. [20] present a compiled IoT structure for managing the issue of cyber-attacks related to an advanced DNN having a rectified linear unit for providing secure and reliable online observation for automated guided vehicle (AGV). The advanced IoT structure related to a DNN introduced a novel technique for network monitoring of AGVs towards cyberattacks with an easy and cheap application as an alternative to conventional cyberattack detection techniques. This DNN can be well-trained related to new AGV data that indicate the AGV's real state and various kinds of cyber-attacks involving a sinusoidal attack, random assault, pulse assault, and ramp assault that can be inserted by attacker as to internet network. In [21], the authors devise a technique utilizing advanced DL for recognizing cyberattacks in IoT systems. To be Specific, this technique compiles an LSTM set modules into a collective of detectors. Such elements were compiled utilizing a DT for arriving at a combined output at the last phase.

3 The Proposed Model

In this work, a novel MFO-RELM model was introduced for cyber-attack detection and classification in the cloud-enabled IoT platform. The proposed MFO-RELM model provides the effective identification of cybersecurity attacks which occur from the cloud and IoT platforms. Fig. 1 represents the overall workflow of the MFO-RELM system.

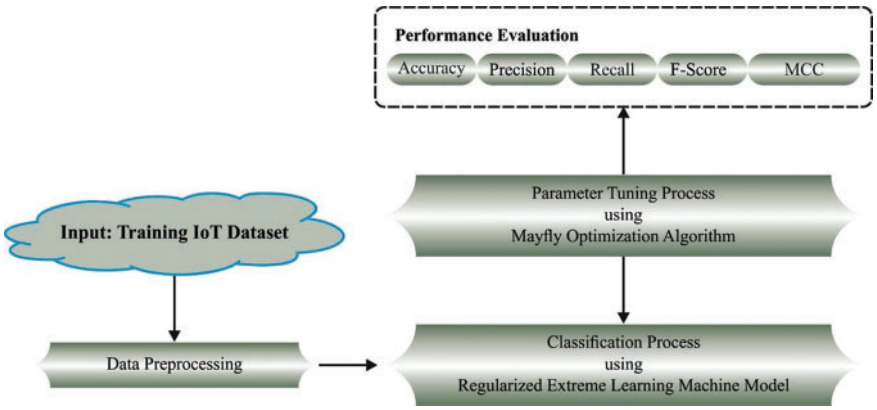

Figure 1: Workflow of MFO-RELM system

3.1 Data Normalization

Firstly, the MFO-RELM approach pre-processed the actual cloud and IoT data into a meaningful format. Raw information for the analysis can sometimes be unsuitable for a set of statistical tests, and to be capable of using those statistical tests and to raise the performance of the analysis, and we should make some modifications to the raw information. Such modifications are named data conversion, which is mathematical modelling used to change parameters that don't follow the statistical assumption of uniform linearity, scattering, and normality, or have a pattern with unusual outliers.

Amongst them, data normalized has higher efficacy. Normalization has distinct statistical meaning, the simple usage is to normalize variables or data, and is a technique that puts information in a similar field once they are not. In other words, a data miner may encounter conditions whereby the property of the information involves viz., various domains or ranges. The larger-value features could have a larger impact on the cost function than the lowest feature values. These problems can be overcome by normalizing the properties so that the values are in the same range. While creating a Meta model from the information, beforehand model training initiates, the information is divided into large values to be normalized to values amongst [0, 1] to minimalize the impact of the full scale and have nearly every input in a similar range.

The min-max technique is the simplest and most popular normalization approach in medicinal imaging [22]. In the study, the unifying data scale, data changing edges would be distributed within [0, 1]. By assuming attribute X, mapping from the dataset among X_{min} and X_{max}, the min-max normalization (X_{norm}) can be accomplished as follows:

$$X_{norm} = \frac{X - X_{\min}}{X_{\max} - X_{\min}}. \tag{1}$$

3.2 RELM-Based Cyber Threat Detection

At this stage, the proposed model will receive the pre-processing data and carry out the classifier procedure using the RELM model. For achieving a robust solution to the network resultant weight W_{out} in terms of perturbations to data representation from the ELM space, it can resolve the subsequent optimized problems [23]:

$$\mathcal{J} = \arg_{W_{out}} \min \| W_{out}^T \phi - T \|_F^2, \tag{2}$$

$$subject\ to: \ W_{out}^T \varphi_i = W_{out}^T \widetilde{\varphi}_{i,m}, i = 1, \ldots, N, m = 1, \ldots, M, \tag{3}$$

whereas $\widetilde{\varphi}_{i,m} \in \mathbb{R}^L$ refers to the perturbed copy of φ_i. Specifically, it will be similar to learned network resultant weight, which generates network outcomes of perturbed instances $\widetilde{\varphi}$ that is as nearby as feasible to the network outcomes to the original instances φ_i, that is, $W_{out}^T \widetilde{\varphi}_{i,m} = \widetilde{o}_{i,m} \simeq 0_i = W_{out}^T \varphi_i$, but (simultaneously) the network trained error is as lower as feasible.

An identical technique was exploited in AEs, controlling to suppose that De-noising AEs. In recent times, it can also be demonstrated that an identical manner is used to train FFNNs. In any case, it can be demonstrated that the implementation of perturbed instances is a result of the regularization of the attained network parameters that improve the generalized capability of trained networks and controls to optimum generalized performances. For incorporating such a regularization manner in Backpropagation (BP) based network training, the training set has generally developed by creating arbitrary perturbations of trained data as the network resultant weights are attained dependent upon closed procedure solution. Fig. 2 showcases the framework of ELM.

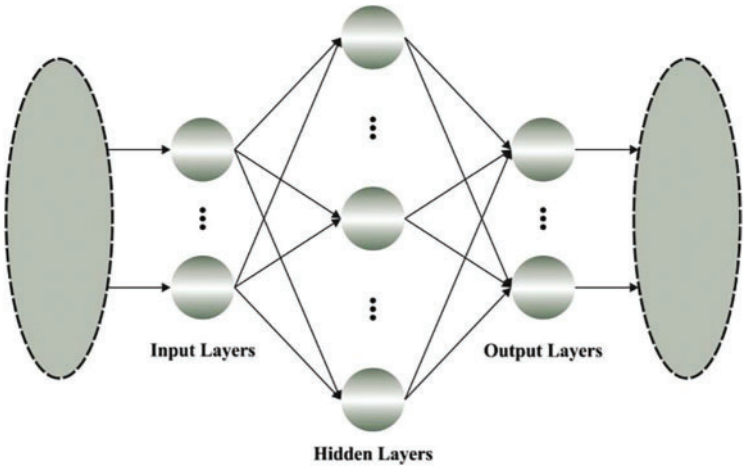

Figure 2: Architecture of ELM

The perturbed instance $\widetilde{\varphi}_{i,m}$ was attained by copying the j^{th} element of φ_i with probability equivalent to p, or by setting the equivalent element corresponding to 0 with probability identical to $(1 - p)$. This procedure is formulated as $\widetilde{\varphi}_{i,m} = b_{i,m} \circ \varphi_i$, whereas $b_{i,m} \in \mathbb{R}^L$, taking their elements equivalent to one with probability p, or zero with probability $(1 - p)$ and $\circ$ refers to the element-wise product of 2 vectors. With setting $\varphi_{i,m} = \varphi_i - \widetilde{\varphi}_{i,m}$, the constraint Eq. (3) is interchanged with the succeeding one:

$$W_{out}^T \varphi_{i,m} = 0, \ i = 1, \ \ldots, \ N, \ m = 1, \ \ldots, \ M. \tag{4}$$

By replacing Eqs. (4) with (2) and taking the corresponding dual problem, it can be attained:

$$\mathcal{J}_D = \arg_{W_{out}} \min \| W_{out}^T \Phi - T \|_F^2 + \frac{c}{M} \sum\nolimits_{m=1}^{M} \| W_{out}^T \Phi_m \|_F^2, \tag{5}$$

whereas $\Phi_m = [\varphi_{1,m}, \ldots, \varphi_{N,m}]$. In Eq. (5), the network resultant weighted were achieved as:

$$W_{out} = \left(\Phi\Phi^T + c\sum_{m=1}^{M}\Phi_m\Phi_m^T\right)^{-1}\Phi T^T. \tag{6}$$

Therefore, for calculating the network resultant weighted by utilizing the presented regularized technique, it can enrich our dataset with the addition of M arbitrary perturbations of all the samples (once demonstrated from the ELM space). But this technique is simply executed from the small- and medium-scale problems, it can be applied to large-scale, complex problems. But, it can be assumed that the count of utilized perturbations is higher $(M \to \infty)$, dependent upon the weak law of huge numbers the regularized term $R = \frac{1}{M}\sum_{m=1}^{m}\Phi_m\Phi_m^T$ in Eq. (6) converges to their estimated value:

$$R \to E\left[\frac{1}{M}\sum_{m=1}^{M}\Phi_m\Phi_m^T\right]_{M\to\infty} = \left(\Phi\Phi^T\right)\circ P, \tag{7}$$

In which $P = (1-p)^2 1 + (1-p)^2 I$ and $1 \in \mathbb{R}^{L\times L}$ is a matrix of ones. Utilizing Eqs. (7), (6) are formulated as:

$$W_{out} = (\Phi\Phi^T + c\left[\Phi\Phi^T\right]\circ P)^{-1}\Phi T^T = (\left[\Phi\Phi^T\right]\circ[1 + cP])^{-1}\Phi T^T. \tag{8}$$

So, it is detected that either the time or memory complexity of presented regularization ELM is similar to ELM and RELM.

3.3 MFO-Based Parameter Optimization

For boosting the efficiency of the proposed models, the MFO technique is utilized to it. The mayflies in a swarm for the MFO approach are classified into male and female individuals [24]. Also, male mayflies are often the strongest ones, and therefore, they are well performed in optimization. Based on individual swarming in the PSO approach, the individuals in the MFO method upgrade the location based on the current location $p_i(t)$ and velocity $v_i(t)$ at the existing iteration:

$$p_i(t+1) = p_i(t) + v_i(t+1) \tag{9}$$

Every female and male mayfly upgrades its position based on the above equation. However, the velocity gets upgraded in different ways.

Movement of male mayfly

Male mayfly in swarming executes exploration or exploitation processes in iteration. The velocity is upgraded according to the existing fitness value $f(x_i)$ and the past optimum fitness value in trajectories $f\left(x_{h_i}\right)$. When $f(x_i) > f\left(x_{h_i}\right)$, then the male mayfly upgrades the velocity based on the present velocity, as well as the distance between them and the optimum global locations, the past optimum trajectories:

$$\mathrm{v_i}(\mathrm{t}+1) = \mathrm{g}\cdot\mathrm{v_i}(\mathrm{t}) + \mathrm{a_1 e^{-\beta r_p^2}}\left[\mathrm{x_{h_i}} - \mathrm{x_i}(\mathrm{t})\right] + \mathrm{a_2 e^{-\beta r_q^2}},\ \left[\mathrm{x_g} - \mathrm{x_i}(\mathrm{t})\right] \tag{10}$$

In Eq. (10), g indicates a variable that linearly declined from the highest value to the lowest one. a_1, a_2, and β symbolize 2 constants to balance the value. RP and r_g specify 2 variables applied for Cartesian distance betwixt the individuals and past and global optimum position in the swarm:

$$\left|\left|\mathrm{x_i} - \mathrm{x_j}\right|\right| = \sqrt{\sum_{\mathrm{k=1}}^{\mathrm{n}}\left(\mathrm{x_{ik}} - \mathrm{x_{jk}}\right)^2} \tag{11}$$

On the other hand, if $f(x_i) < f(x_{h_i})$, the male mayfly upgrades the velocity from the present one using a random dance co-efficient d:

$$v_i(t+1) = g \cdot v_i(t) + d \cdot r_1 \tag{12}$$

In Eq. (12), r_1 symbolizes the random number in uniform distribution and selected from the range -1 and 1.

Movement of female mayfly

The female will upgrade the velocity based on different styles. Generally, the female mayfly with wings lives for 1 to 7 days at the most. Therefore the female mayfly would be onrush to find the male mayfly to mate and reproduce itself. In the MFO method, the optimum male and female mayflies are treated as the 1st mate, and 2nd optimum female male mayfly is processed as 2nd mate, etc. therefore, for *i-th* females, when $f(y_i) < f(x_i)$:

$$v_i(t+1) = g \cdot v_i(t) + a_3 e^{-\beta r_{mf}^2} [x_i(t) - y_i(t)] \tag{13}$$

In Eq. (13), a_3 indicates an additional constant and is exploited to balance the velocity. r_m shows the Cartesian distance amongst themselves. At the same time, when $(y_i) < f(x_i)$, the female mayfly upgrades the velocity from the present one using random dance fl:

$$v_i(t) = g \cdot v_i(t) + fl \cdot r_2 \tag{14}$$

Consider r_2 indicates a uniformly distributed random number within $[-1, 1]$.

Mating of mayfly

Every male and female mayfly was mated and provided a pair of childrens. The offspring is established randomly from the parent:

$$offspring1 = L * male + (1 - L) * female \tag{15}$$

$$offspring2 = L * female + (1 - L) * male \tag{16}$$

Now, L indicates the random value in the Gauss distribution. The MFO approach initiates with the initialization of female and male mayfly populations. Next, the velocity and solution of the mayfly are upgraded. Then, the ranking procedure of mayfly is performed, and the worst solution will be replaced with the optimal solution. The MFO approach makes extraction of a Fitness Function (FF) for achieving enriched classifier result. It ascertains positive values for denoting enhanced outcomes of the candidate result. During this work, the decrease of the classifier rate of errors were regarded as the FF is given in Eq. (17).

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

4 Results and Discussion

The presented method was simulated utilizing Python 3.6.5 tool on GeForce 1050Ti 4 GB, PC i5-8600k, 250 GB SSD, 1TB HDD, and 16 GB RAM. The parameter setting are provided as follows: epoch count: 50, rate of learning: 0.01, batch size: 5, activation: ReLU, and dropout: 0.5. The simulation outcome of the MFO-RELM approach was tested using CICIDS 2017 dataset under

two aspects: binary classification and multi-classification. Table 1 depicts the details of the binary classification dataset. The presented technique was simulated utilizing the Python tool.

Table 1: Details on binary classification dataset

Class	No. of samples
Normal	80000
Abnormal	219451
Total number of samples	**299451**

Fig. 3 represents the confusion matrix generated by the MFO-RELM algorithm on the binary classifier of the CICIDS 2017 database. With the entire database, the MFO-RELM model has recognized 79254 instances into the normal class and 217611 instances into the abnormal class. Also, with 70% of TRS, the MFO-RELM approach has recognized 55520 instances into the normal class and 152308 instances into the abnormal class. Meanwhile, with 30% of TSS, the MFO-RELM system has recognized 23734 instances into the normal class and 65303 instances into the abnormal class.

Table 2 and Fig. 4 report the binary classifier result of the MFO-RELM model. On the entire database, the MFO-RELM approach has obtainable average $accu_{racy}$ of 99.14%, $Prec_n$ of 98.69%, $reca_l$ of 99.11%, F_{score} of 98.90%, and MCC of 97.81%. Additionally, on 70% of TRS, the MFO-RELM approach has a reachable average $accu_{racy}$ of 99.15%, $Prec_n$ of 98.71%, $reca_l$ of 99.13%, F_{score} of 98.92%, and MCC of 97.84%. Similarly, on 30% of TSS, the MFO-RELM algorithm has an accessible average $accu_{racy}$ of 99.11%, $Prec_n$ of 98.66%, $reca_l$ of 99.09%, F_{score} of 98.87%, and MCC of 97.74%.

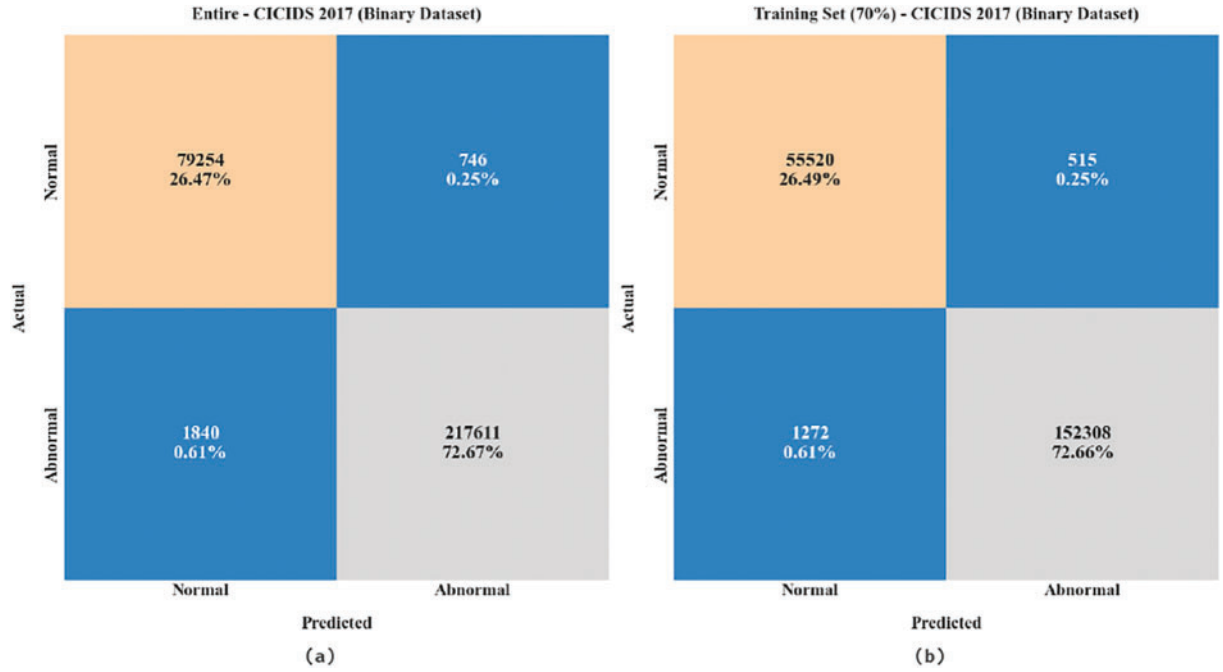

Figure 3: (Continued)

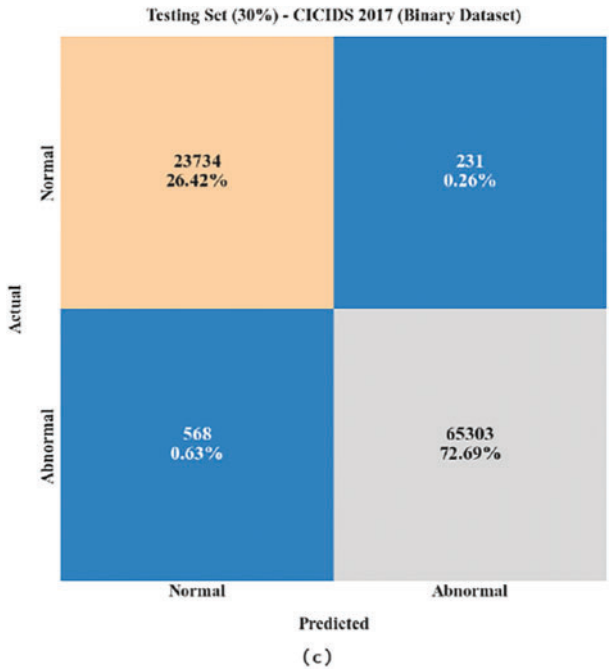

Figure 3: Confusion matrices of MFO-RELM system under binary database (a) entire database, (b) 70% of TRS, and (c) 30% of TSS

Table 2: Classifier outcome of MFO-RELM system with various measures under binary database

Binary dataset					
Labels	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	MCC
Entire dataset					
Normal	99.14	97.73	99.07	98.39	97.81
Abnormal	99.14	99.66	99.16	99.41	97.81
Average	**99.14**	**98.69**	**99.11**	**98.90**	**97.81**
Training phase (70%)					
Normal	99.15	97.76	99.08	98.42	97.84
Abnormal	99.15	99.66	99.17	99.42	97.84
Average	**99.15**	**98.71**	**99.13**	**98.92**	**97.84**
Testing phase (30%)					
Normal	99.11	97.66	99.04	98.34	97.74
Abnormal	99.11	99.65	99.14	99.39	97.74
Average	**99.11**	**98.66**	**99.09**	**98.87**	**97.74**

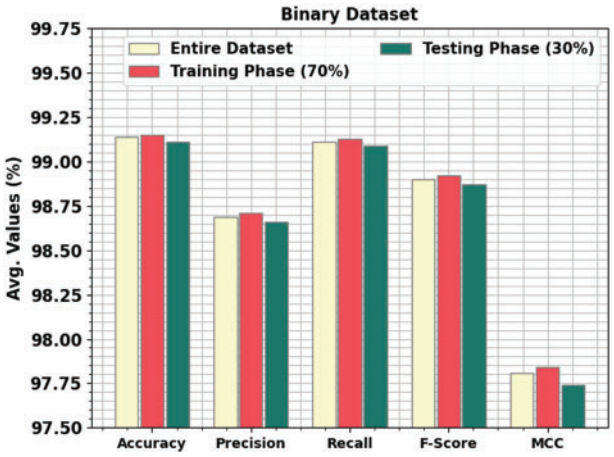

Figure 4: Average outcome of the MFO-RELM system under binary database

The TACC and VACC acquired by the MFO-RELM system on binary dataset are displayed in Fig. 5. The performance outcome stated that the MFO-RELM algorithm had obtained enhanced values of TACC and VACC. In specific, the VACC considered that higher than TACC.

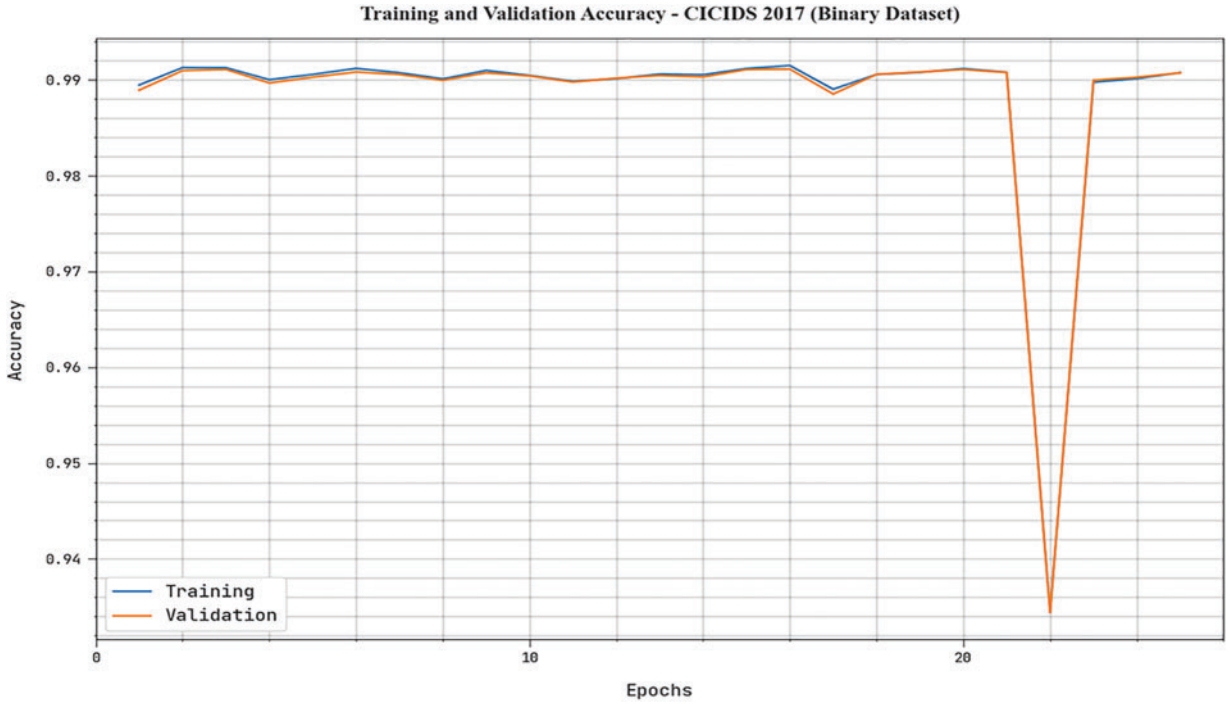

Figure 5: TACC and VACC outcome of MFO-RELM system under binary dataset

The TLS and VLS attained by the MFO-RELM methodology on binary dataset are depicted in Fig. 6. The performance outcome pointed out that the MFO-RELM method has achieved minimal values of TLS and VLS. In certain, the VLS is lower than TLS.

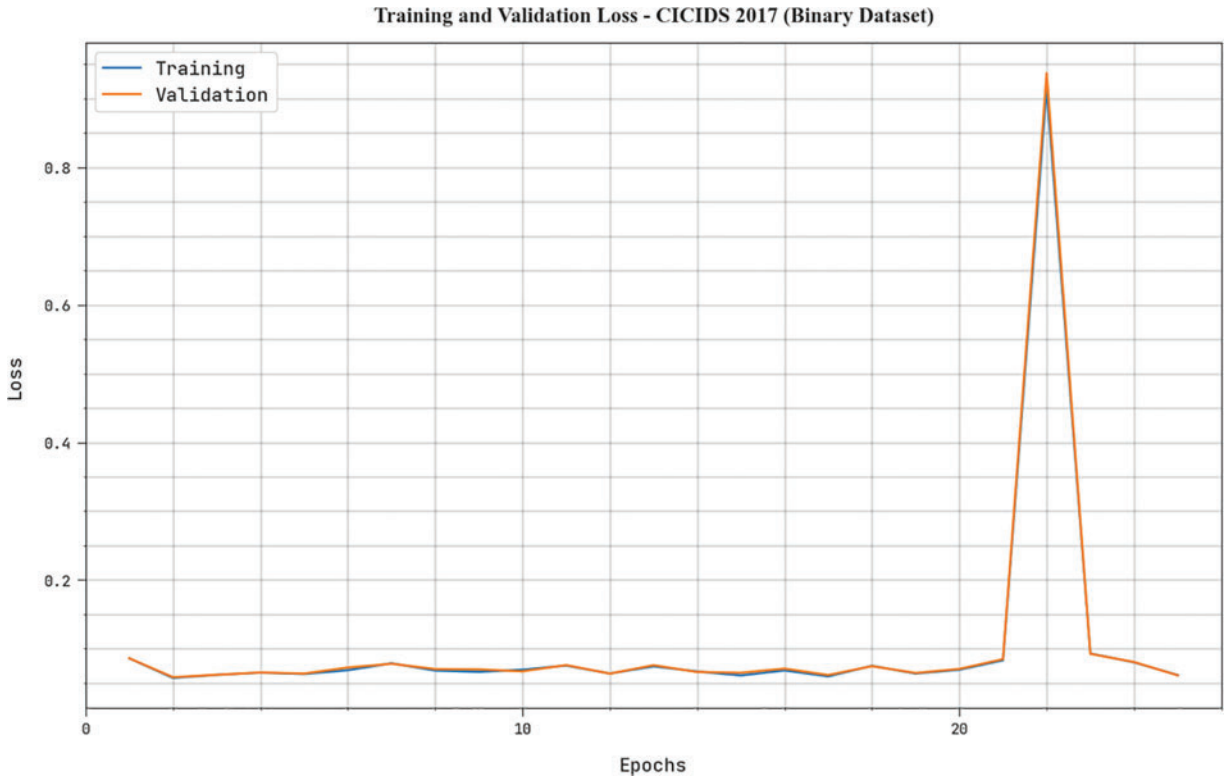

Figure 6: TLS and VLS outcome of MFO-RELM system under binary database

Table 3 demonstrates a detailed description of the multi-classification dataset. Fig. 7 demonstrates the confusion matrix generated by the MFO-RELM method under the multi-classification of the CICIDS 2017 dataset. With the entire database, the MFO-RELM system has detection 78227 samples in the N class, 3 samples in the A1 class, 1894 samples in the A2 class, 21395 samples in the A3 class, 25248 samples in the A4 class, 19029 samples in A5 class, 8134 samples into A6 class, 7181 samples into A7 class, 36981 samples into A8 class, 39105 samples into A9 class, and 38833 samples into A10 class.

Table 3: Details on the multi-classification dataset

Label	Class	No. of samples
N	Normal	80000
A1	Botnet	1974
A2	DoSSlowhttptest	7851
A3	FTP-Pastor	22147
A4	SSH-Patatpr	27215
A5	DoSGoldenEye	21235
A6	DoSslowloris	9519
A7	Hearbleed	9510
A8	PortScan	40000

(Continued)

Table 3: Continued

Label	Class	No. of samples
A9	DDoS	40000
A10	DosHulk	40000
Total Number of Samples		**299451**

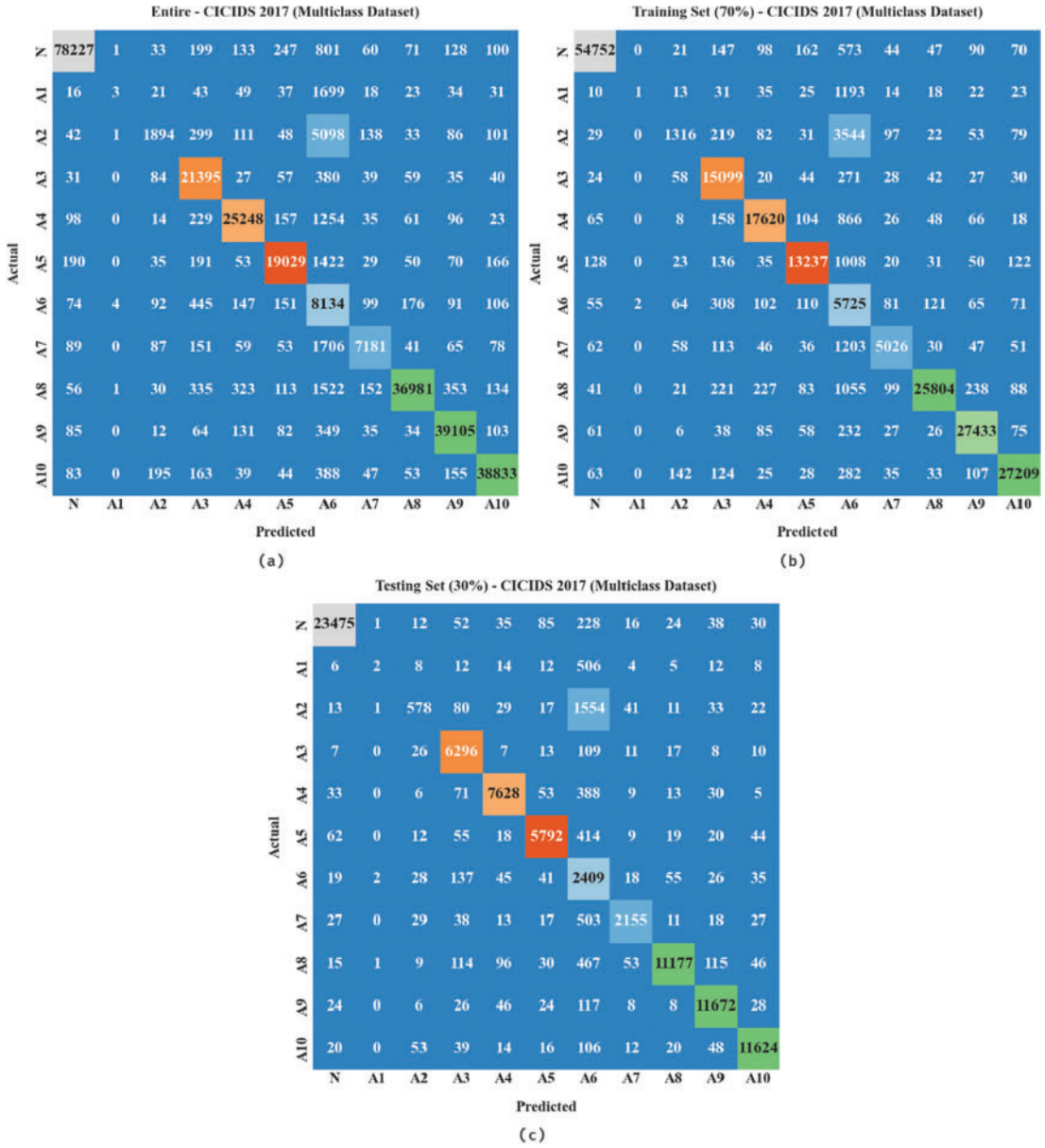

Figure 7: Confusion matrices of MFO-RELM system on multiclass database (a) entire database, (b) 70% of TRS, and (c) 30% of TSS

Table 4 and Fig. 8 report the multi-classification outcome of the MFO-RELM technique. On the entire database, the MFO-RELM approach has obtainable average $accu_{racy}$ of 98.58%, $Prec_n$ of 82.52%, $reca_l$ of 77.21%, F_{score} of 76.28%, and MCC of 76.86%. Moreover, on 70% of TRS, the MFO-RELM system has offered average $accu_{racy}$ of 98.58%, $Prec_n$ of 82.83%, $reca_l$ of 77.17%, F_{score} of 76.25%, and MCC of 76.80%. Lastly, on 30% of TSS, the MFO-RELM system has an existing average $accu_{racy}$ of 98.58%, $Prec_n$ of 82.52%, $reca_l$ of 77.21%, F_{score} of 76.28%, and MCC of 76.86%.

Table 4: Classifier outcome of the MFO-RELM system with various measures under the Multiclass database

Multiclass dataset					
Labels	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	MCC
Entire dataset					
N	99.15	99.03	97.78	98.40	97.83
A1	99.34	30.00	00.15	00.30	02.10
A2	97.81	75.85	24.12	36.61	42.03
A3	99.04	90.99	96.60	93.71	93.24
A4	98.99	95.93	92.77	94.32	93.78
A5	98.93	95.06	89.61	92.26	91.73
A6	94.66	35.75	85.45	50.41	53.24
A7	99.00	91.68	75.51	82.81	82.71
A8	98.79	98.40	92.45	95.33	94.70
A9	99.33	97.23	97.76	97.50	97.11
A10	99.32	97.78	97.08	97.43	97.04
Average	**98.58**	**82.52**	**77.21**	**76.28**	**76.86**
Training phase (70%)					
N	99.15	99.03	97.76	98.39	97.81
A1	99.34	33.33	00.07	00.14	01.53
A2	97.82	76.07	24.05	36.55	42.03
A3	99.03	90.99	96.52	93.67	93.20
A4	98.99	95.89	92.84	94.34	93.80
A5	98.93	95.11	89.50	92.22	91.70
A6	94.65	35.89	85.40	50.54	53.32
A7	98.99	91.43	75.33	82.60	82.50
A8	98.81	98.41	92.56	95.40	94.77
A9	99.34	97.29	97.83	97.56	97.18
A10	99.30	97.75	97.01	97.38	96.97
Average	**98.58**	**82.83**	**77.17**	**76.25**	**76.80**
Testing phase (30%)					
N	99.15	99.03	97.78	98.40	97.83
A1	99.34	30.00	00.15	00.30	02.10
A2	97.81	75.85	24.12	36.61	42.03
A3	99.04	90.99	96.60	93.71	93.24
A4	98.99	95.93	92.77	94.32	93.78

(Continued)

Table 4: Continued

Multiclass dataset					
Labels	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	MCC
A5	98.93	95.06	89.61	92.26	91.73
A6	94.66	35.75	85.45	50.41	53.24
A7	99.00	91.68	75.51	82.81	82.71
A8	98.79	98.40	92.45	95.33	94.70
A9	99.33	97.23	97.76	97.50	97.11
A10	99.32	97.78	97.08	97.43	97.04
Average	**98.58**	**82.52**	**77.21**	**76.28**	**76.86**

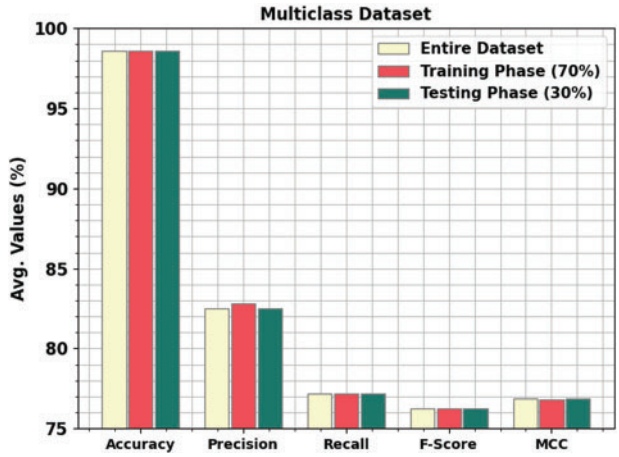

Figure 8: Average analysis of the MFO-RELM approach under a multiclass database

Table 5 and Fig. 9 showcase the MFO-RELM approach with existing methods on binary classification. The simulation values inferred that the MFO-RELM algorithm had shown enhanced performance over other models. The XGB model has shown ineffectual performance with minimal $accu_{racy}$ of 94.56%. In addition, the RF and ANN models have obtained certainly improved $accu_{racy}$ values of 97.92% and 97.86%, respectively. Moreover, the Rearguard, NB-SVM, and DBN models have reached reasonable $accu_{racy}$ of 98.95%, 98.48% and 98.73%, respectively. But the MFO-RELM model has shown superior performance with increased $accu_{racy}$ of 99.15%.

Fig. 10 demonstrates the MFO-RELM approach with existing techniques on multiclass classification. The experimental values inferred that the MFO-RELM system had demonstrated higher performance over other techniques. The RF approach has exhibited ineffectual performance with minimal $accu_{racy}$ of 96.39%. Besides, the Support Vector Classifier (SVC) and ANN systems have obtained higher $accu_{racy}$ values of 96.91% and 97.37%, respectively. Furthermore, the Rearguard, multilayer perceptron (MLP), and XGB models have obtained reasonable $accu_{racy}$ of 98.16%, 97.69% and 97.87%, correspondingly. Finally, the MFO-RELM technique has portrayed superior performance with enhanced $accu_{racy}$ of 98.58%.

Table 5: Comparative outcome of MFO-RELM system with existing algorithms on binary database

Binary dataset	
Methods	Accuracy (%)
MFO-RELM	99.15
Rearguard	98.95
NB-SVM	98.48
RF Model	97.92
DBN Model	98.73
XGB Model	94.56
ANN Model	97.86

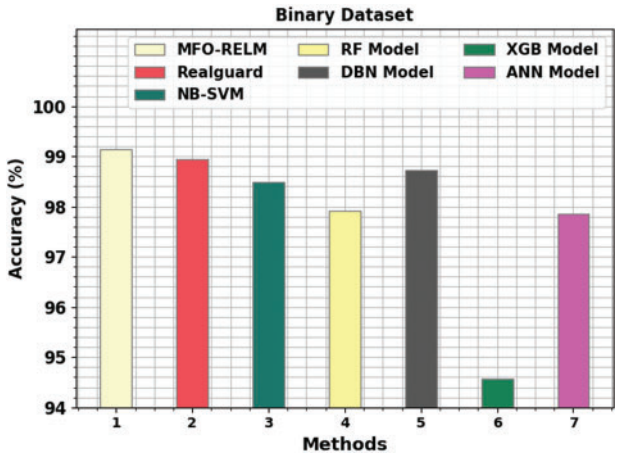

Figure 9: Comparative outcome of MFO-RELM system under binary database

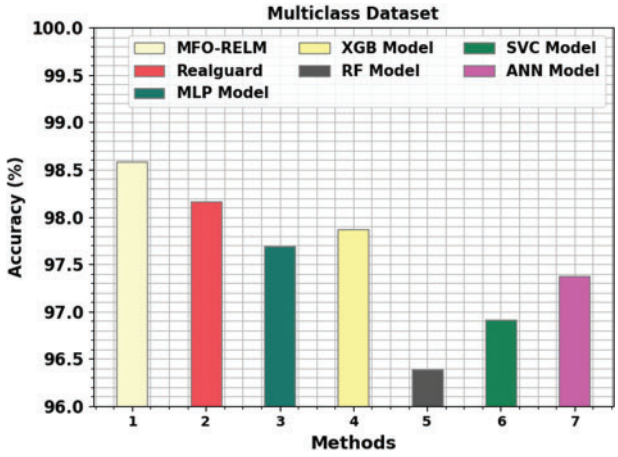

Figure 10: Comparative outcome of the MFO-RELM system on multiclass database

5 Conclusion

In this work, a novel MFO-RELM model was introduced for cyber-attack detection and classification in the cloud-enabled IoT platform. The proposed MFO-RELM model provides the effective identification of cybersecurity attacks which occur from the cloud and IoT platforms. In order to realize this, the MFO-RELM approach pre-processed the actual cloud and IoT data as to meaningful format. Also, the proposed approach will receive the pre-processing data and carry out the classifier system using the RELM model. For boosting the efficiency of the proposed models, the MFO technique will be utilized to it. A series of simulations were carried out on CICIDS 2017 dataset and the outcomes are inspected with respect to various measures. A widespread comparison study portrayed the enhanced performance of the proposed model. Thus, the presented MFO-RELM model accomplishes maximum detection efficiency over other existing models. In future, advanced DL approaches are combined as to the MFO-RELM system for improved classifier efficacy. Besides, the computation complexity of the MFO-RELM approach was investigated in future.

Funding Statement: The authors extend their appreciation to the deanship of scientific research at Shaqra University for funding this research work through the project number (SU-NN-202210).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] V. Dutta, M. Choraś, M. Pawlicki and R. Kozik, "A deep learning ensemble for network anomaly and cyber-attack detection," *Sensors*, vol. 20, no. 16, pp. 4583, 2020.

[2] S. Lysenko, K. Bobrovnikova, V. Kharchenko and O. Savenko, "IoT Multi-vector cyberattack detection based on machine learning algorithms: Traffic features analysis, experiments, and efficiency," *Algorithms*, vol. 15, no. 7, pp. 239, 2022.

[3] M. A. Alohali, F. N. Al-Wasabi, A. M. Hilal, S. Goel, D. Gupta *et al.,* "Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment," *Cognitive Neurodynamics*, vol. 16, no. 5, pp. 1045–1057, 2022.

[4] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto and K. Sakurai, "Rule generation for signature-based detection systems of cyber attacks in IoT environments," *Bulletin of Networking, Computing, Systems, and Software*, vol. 8, no. 2, pp. 93–97, 2019.

[5] A. Abdulrahman Albraikan, S. Ben Haj Hassine, S. Mohamed Fati, F. N. Al-Wasabi, A. Mustafa Hilal *et al.,* "Optimal deep learning-based cyberattack detection and classification technique on social networks," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 907–923, 2022.

[6] M. Shafiq, Z. Tian, A. K. Bashir, X. Du and M. Guizani, "orrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3242–3254, 2020.

[7] H. Hameed, F. Yang, S. U. Bazai, M. I. Ghafoor, A. Alshehri *et al.,* "Urbanization detection using LiDAR-based remote sensing images of Azad Kashmir using novel 3D CNNs," *Journal of Sensors*, 2022. https://doi.org/10.1155/2022/6430120

[8] M. I. Ghafoor, M. S. Roomi, M. Aqeel, U. Sadiq and S. U. Bazai, "Multi-features classification of SMD screen in smart cities using randomised machine learning algorithms," in *2021 2nd Int. Informatics and Software Engineering Conf. (IISEC)*, Ankara, Turkey, pp. 1–5, 2021.

[9] A. Al-Qarafi, F. Alrowais, S. Alotaibi, N. Nemri, F. N. Al-Wasabi *et al.,* "Optimal machine learning based privacy-preserving blockchain assisted internet of things with smart cities environment," *Applied Sciences*, vol. 12, no. 12, pp. 1–17, 2022.

[10] W. Wang, F. Harrow, B. Bouyeddou, S. M. Senouci and Y. Sun, "A stacked deep learning approach to cyber-attacks detection in industrial systems: Application to power system and gas pipeline systems," *Cluster Computing*, vol. 25, no. 1, pp. 561–578, 2022.

[11] E. Bout, V. Loscri and A. Gallais, "How machine learning changes the nature of cyberattacks on IoT networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 248–279, 2021.

[12] C. Iwendi, S. U. Rehman, A. R. Javed, S. Khan and G. Srivastava, "Sustainable security for the internet of things using artificial intelligence architectures," *ACM Transactions on Internet Technology*, vol. 21, no. 3, pp. 1–22, 2021.

[13] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto and K. Sakurai, "Towards a lightweight detection system for cyber attacks in the IoT environment using corresponding features," *Electronics*, vol. 9, no. 1, pp. 144, 2020.

[14] A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M. A. Ferran *et al.,* "Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security," *Sensors*, vol. 19, no. 14, pp. 3119, 2019.

[15] P. Kumar, G. P. Gupta and R. Tripathi, "Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for IoT networks," *Arabian Journal for Science and Engineering*, vol. 46, no. 4, pp. 3749–3778, 2021.

[16] A. A. AlZubi, M. Al-Mariah and A. Alarifi, "Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques," *Soft Computing*, vol. 25, no. 18, pp. 12319–12332, 2021.

[17] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam and S. Gordon, "Cyberattacks detection in IoT-based smart city applications using machine learning techniques," *International Journal of Environmental Research and Public Health*, vol. 17, no. 24, pp. 9347, 2020.

[18] D. G. Roy and S. N. Srirama, "A blockchain-based cyber attack detection scheme for decentralized internet of things using software-defined network," *Software: Practice and Experience*, vol. 51, no. 7, pp. 1540–1556, 2021.

[19] Q. A. A. Haija and S. Z. Sabato, "An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks," *Electronics*, vol. 9, no. 12, pp. 2152, 2020.

[20] M. Elsisi and M. Q. Tran, "Development of an IoT architecture based on a deep neural network against cyber-attacks for automated guided vehicles," *Sensors*, vol. 21, no. 24, pp. 8467, 2021.

[21] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K. K. R. Choo and R. M. Parizi, "An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8852–8859, 2020.

[22] A. Pandey and A. Jain, "Comparative analysis of KNN algorithm using various normalization techniques," *International Journal of Computer Network and Information Security*, vol. 9, no. 11, pp. 36, 2017.

[23] D. Gupta, B. B. Hazarika and M. Berlin, "Robust regularized extreme learning machine with asymmetric Huber loss function," *Neural Computing and Applications*, vol. 32, no. 16, pp. 12971–12998, 2020.

[24] R. M. Adnan, O. Kisi, R. R. Mostafa, A. N. Ahmed and A. El-Shafie, "The potential of a novel support vector machine trained with modified mayfly optimization algorithm for streamflow prediction," *Hydrological Sciences Journal*, vol. 67, no. 2, pp. 161–174, 2022.