Acta Montanistica Slovaca
ISSN 1335-1788
actamont.tuke.sk

Oppositional Coyote Optimization based Feature Selection with Deep Learning Model for Intrusion Detection in Fog-Assisted Wireless Sensor Network

Vinoth Kumar KALIMUTHU[1] *and* ***Thiruppathi MUTHU***[2]

Authors'affiliations and addresses:
[1]Department of Electronics and Communication Engineering, SSM Institute of Engineering and Technology, Dindigul, India.
e-mail: vinodkumaran87@gmail.com

[2]Department of Electronics and Communication Engineering, Vivekanandha College of Engineering for Women, Tiruchengode, India.
e-mail: mailtothiruppathi@gmail.com

***Correspondence:**
Vinoth Kumar Kalimuthu, Department of Electronics and Communication Engineering, SSM Institute of Engineering and Technology, Dindigul, India.
tel.: +91-9787367067
e-mail: vinodkumaran87@gmail.com

How to cite this article:
Kalimuthu, V.K. and Muthu, T. (2023). Oppositional Coyote Optimization based Feature Selection with Deep Learning Model for Intrusion Detection in Fog-Assisted Wireless Sensor Network. *Acta Montanistica Slovaca*, Volume 28 (2), 496-508

DOI:
https://doi.org/10.46544/AMS.v28i2.18

Abstract
Recently, Wireless Sensor Networks (WSN) and the Internet of Things (IoT) become widespread in several real-time applications. Since IoT devices have generated a huge amount of data, the processing of data at the cloud server leads to high delay. To reduce the delay, fog-assisted WSN can be developed where the Fog Nodes are kept at the edge of the network nearer to the client. Besides, security becomes a challenging issue in fog-assisted WSN and can be accomplished by using Intrusion Detection System (IDS). This paper presents an Oppositional Coyote Optimization based feature selection with Cat Swarm Optimization based Bidirectional Gated Recurrent Unit (OCOA-CSBiGRU) for intrusion detection in fog-assisted WSN. The intention of the OCOA-CSBiGRU technique is to identify the occurrence of intrusions in the fog-assisted WSN by the use of feature selection and classification models. The proposed OCOA-CSBiGRU technique initially designs a novel OCOA-based feature selection technique for the optimal selection of features. Besides, the BiGRU model is utilized for the detection and classification of intrusions. In order to improve the detection efficiency of the BiGRU model, the Cat Swarm Optimization (CSO) algorithm has been utilized. A comprehensive experimental analysis is carried out on benchmark datasets, and the results indicatebetter outcomes of the OCOA-CSBiGRU technique over the recent methods interms of different metrics.

Keywords
Computing, Wireless Sensor Networks, Deep learning, Metaheuristics, Intrusion detection, Security.

Introduction

The Wireless Sensor Network (WSN) is commonly employed in environment monitoring, vehicular communication, and military surveillance systems [Ahmed et al, 2020]. Owing to the limitation of storage and computational ability, processing a considerable amount of sensory data in WSN is a serious problem [Bangui & Buhnova, 2021; Butun et al, 2020]. Cloud Computing (CC) technique has made significant development, which has inserted new vitality to WSN. CC could offer data storage and processing for conventional WSN, bringing many new applications and solutions [Chen et al, 2016; De Souza et al, 2020]. With the ever-growing popularity of the CC technique, an increasing number of user outsources their dataset to the cloud to prevent the overhead of storage and management [Diro & Chilamkurti, 2018]. In cloud storage, information is encrypted beforehand outsourcing. Hence data privacy is assured and thus becomes increasingly prominent in various aspects. Sensor-cloud is a scheme that incorporates CC and WSN. In contrast with CC, fog computing is an effective approach for WSN that expands CC to the network edge, consequently enabling new services and applications. Like the Cloud, the Fog could offer storage, data, application, and computational services to end users [Diro & Chilamkurti, 2018; Djenouri et al, 2019]. The fog layers connect WSN to the Cloud. Usually, the Fog node consists of robust nodes with great processing and storage ability when compared to normal sensors, namely mobile sinks, mobile nodes, and mobile collectors. The major differences between fog computing and CC are that fog computing could offer mobility and local storage for end users. Fig. 1 illustrates the structure of WSN. Given the security problems in the virtual world and the new technologies of the WSN, and owing to the challenge of infiltrating this system [Kaur & Sood, 2019], it is important to offer an optimum method to maintain security and detect intrusion in this system. Thus, to handle attackers and intruders on computer networks and systems, various methodologies were introduced named intrusion detection method, which takes the responsibility to monitor the event that occurs in a computer network or system. The Intrution Detection Systems (IDS) is applied to detectan illegal access to any system or network [Kaushik & Sinha, 202; Kumar et al, 2021].

It is extensively deployed in two manners; initially, atthe Host level on a node for monitoring the operating system running on the node or activity on its system application files. In this phase, a node could be a computer device or system in IoT [Kumar et al, 202; Lawal et al, 2021]. Next, at the Network level on a border router or gateway, where it can monitor network traffic flow. The NIDS is classified based on the technique of deployment and detection framework. Based on the deployment framework, the NIDS could use a distributed, hybrid, or centralized deployment approach.

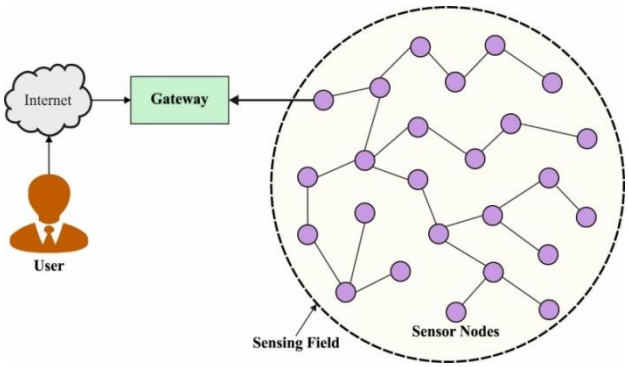

Fig. 1. WSN structure

In centralized deployment, the NIDS is placed on a router or a devoted host. It monitors network traffic flows and transactions among the internet and the inside of its network. In the distributed deployment framework, the NIDS is positioned on the network node, where the node monitors each network transaction. Hybrid deployment uses distributed and centralized frameworks to reduce shortcomings and leverage the deployment strategy's benefits [Li et al, 2018; Lynn, 2019]. The NIDS is usually categorized into hybrid-based, signature-based, and anomaly-based models based on the detection method. The signature-based IDS detects attacks or threats via rules with network traffic flow features or matching stored attack signatures. The anomaly-based system employs protocol-specific, statistical, or machine data to construct a legitimate network traffic flow method as a benchmark for its process [Maheswari & Karthika, 2021; Malik & Khamparia, 2020]. This paper presents an oppositional coyote optimization-based feature selection with cat swarm optimization-based bidirectional gated recurrent unit (OCOA-CSBiGRU) for intrusion detection in fog-assisted WSN. The intention of the OCOA-CSBiGRU technique is to identify the occurrence of intrusions in the fog-assisted WSN by the use of feature selection and classification models. The proposed OCOA-CSBiGRU technique initially designs a novel OCOA-based feature selection technique for the optimal selection of features. Besides, BiGRU model is utilized forthe detection and classification of intrusions. In order to improve the detection efficiency of the BiGRU model, the cat swarm optimization (CSO)

algorithm has been utilized. A comprehensive simulation assessment takes place on datasets and assessesthe results under varying aspects.

Theoretical MOSPO-CMR Model

In this study, a novel OCOA-CSBiGRU technique has been developed for the identification of intrusions in the fog-assisted WSN. The proposed OCOA-CSBiGRU technique comprises OCOA-based feature selection, BiGRU-based classification, and CSO-based hyperparameter optimization. Using OCOA and CSO algorithms helps accomplish maximum intrusion detection outcomes in the fog-assisted WSN. Fig. 2 demonstrates the overall process of the OCOA-CSBiGRU technique.

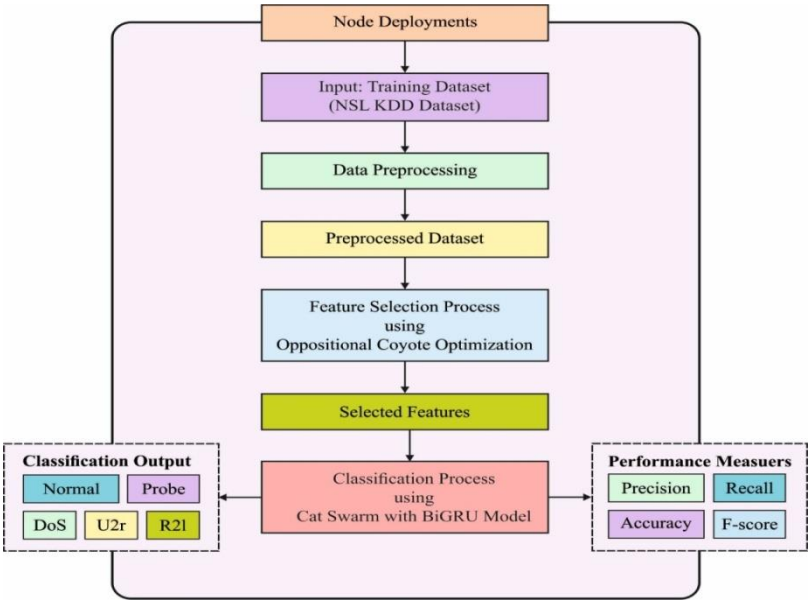

Fig. 2. Overall process of the OCOA-CSBiGRU technique

Design of the OCOA-FS Technique

Primarily, the networking data is fed into the OCOA-FS technique for the election of optimum feature subsets. The COA is a meta-heuristic optimization approach as the evolutionary and swarm models [Omar et al, 2021]. It is inspired bythe *Canis latrans* species. The social behavior of coyote c in a group p at time t is taken into account as a set of design parameters:

$$soc_c^{p,t} = x = (x_1, x_2, \ldots\ldots, x_D) \tag{1}$$

The coyote'sadaptation tothe environment is taken into account the fitness cost function. Initially, the agents or coyotes are randomly generated with the searching space:

$$soc_{c,j}^{p,t} = LB_j + r_j(UB_j - LB_j) \tag{2}$$

Whereas LB_j and UB_j represent the lower and upper limits of the parameter j and r_j denotes an arbitrary value within [0,1].

$$fit_c^{p,t} = f(soc_c^{p,t}) \tag{3}$$

Initially, the coyote is arbitrarily included in the group, but they occasionally move from its group to another. This coyote leave is related to a probability P_L, as follows:

$$P_L = 0.005.N_c^2 \tag{4}$$

The presented method assists in replacing the coyote's culture among the groups. The leader of the coyote or the alpha coyote is taken into account as the optimally adopted coyote with the environment:

$$alpha^{p,t} = soc_c^{p,t} \text{ for } min\ fi_c^{p,t} \tag{5}$$

The COA collects data amongst the coyote through the groups. Regarding this, there areculture transfers among the coyotes within the group:

$$cul_j^{p,t} = \begin{cases} O^{p,t}_{\frac{N_c+1}{2},j}, N_c\ is\ odd\ number \\ \dfrac{\left(0^{p,t}_{\frac{N_c}{2}_i} + O^{p,t}\left(\frac{N_c}{2}+1\right), j\right)}{2}, otherwise \end{cases} \tag{6}$$

Whereas $O^{p,t}$ represent the ranked social condition of the coyote of the group p at time t of the parameter j. The COA considered the life cycle of coyotes, such as birth and death:

$$Pup_i^{p,t} = \begin{cases} soc_{r1,j}^{p,t}, rand_j < P_s or j = j_1 \\ soc_{r2,j}^{p,t}, rand_j \geq P_s + P_a or j = j_2 \\ R_i, otherwise \end{cases} \tag{7}$$

Whereas r_1 and r_2 represent arbitrary coyotes with the groups $p, j_1\ and\ j_2$ denotes arbitrary parameters, P_s and P_a denotes the scatter and association likelihoods. This probability indicates the culturaldiversity of coyotes from the group, and the value is defined as follows:

$$P_s = 1/D \tag{8}$$

$$P_o = (1 - P_s)/2 \tag{9}$$

Whereas D represent the dimension of parameters. When the social behavior is superior to the previous one, as follows.

$$\delta_1 = alpha^{p,t} - soc_{cr1}^{p,t} \tag{10}$$

$$\delta_2 = cul^{p,f} - soc_{cr2}^{p,f} \tag{11}$$

The social behavior of coyotes is upgraded by the group influence and the alpha coyote:

$$nsoc_c^{p,t} = soc_c^{p,t} + r_1\delta_1 + r_2\delta_2 \tag{12}$$

Whereas r_1 and r_2 represent arbitrary values within [0,1] expressed in the group influence and the weight of alpha. The fitness value of a coyote is estimated by the following:

$$nfit_C^{p,t} = f(nsoc_c^{p,t}) \tag{13}$$

$$soc_c^{p,f+1} = \begin{cases} nsoc_c^{p,t}, nfif_c^{p,t} < fit_c^{p,t} \\ soc_c^{p,t}, otherwise \end{cases} \tag{14}$$

Finally, the social behavior of optimal adaptation to theenvironment is selected as an optimal solution.

To improve the effectiveness of the COA, population initiation using OBL is derived for designing the OCOA [Pacheco et al, 2020]. OBL demonstrates an optimized approach utilized by several analyses to improve the quality of its introduced population solution by diversifying it. The OBL method works by searching both directions from the search space. These 2 directions comprise one novel solution, but the other direction is signified by their opposite solutions. At last, the OBL approach gets the fittest solution in every solution.

Opposite number: z has been determined as a real number on the interval $z \in [lb, ub]$. The opposite number of z is represented as $\tilde{z}$, and for determining their value Eq. (15) is utilized:

$$\tilde{z} = lb + ub - z \tag{15}$$

Eq. (15) is a generalization for applying it in a search space with multi-dimensional. So, for generalizing it, all search agent's place and their opposite place are signified as the subsequent Eqs. (16) & (17):

$$z = [z_1, z_2, z_3, \dots z_D] \tag{16}$$

$$\tilde{z} = [\tilde{z}_1, \tilde{z}_2, \tilde{z}_3, \dots, \tilde{z}_D] \tag{17}$$

The values of each element from $\tilde{z}$ is defined utilizing Eq. (18):

$$\tilde{z}_j = lb_j + ub_j - z_j where j = 1,2,3, \dots, D \tag{18}$$

Optimization Based on Opposite population: during this approach, the FF is $f(.)$. Hence, once the fitness value $f(\tilde{z})$ of the opposite solution was higher than $f(z)$ of their novel solution z, next $z = \tilde{z}$; else $z = z$.

The OCOA-FS technique has been mathematically formulated as follows. Generally, the classification of data includes a size $N_S \times N_F$ where N_S and N_F denotes the number of samples and features, respectively. The major intention of the FS problem is the choice of feature subsets S from available features (N_F) where the size of $S < N_F$. It can be accomplished byminimizing the objective function, as given below.

$$Fit = \lambda \times \gamma_S + (1 - \lambda) \times \left(\frac{|S|}{N_F}\right) \tag{19}$$

where γ_S denotes classifier error rate by the use of S and $|S|$ represents chosen feature count. λ can be used for
for balancing $\left(\frac{|S|}{N_P}\right)$ and γ_S.

BiGRU-based Intrusion Detection Model

During intrusion detection and classification models, the chosen feature subsets are passed into the BiGRU model. Because of the complex structure of the LSTM unit, there was a problem withthe long training time. The GRU memory unit integrates the input gate i and the forgetting gate f in the LSTM to an update gate z that resolves the long dependence problem and retains significant features, while the structure is simple when compared to the LSTM [Pierezan & Coelho, 2018]. In time t, for an input X_t, the hidden layers of the GRU output h_t, in the following:

$$z_t = \sigma(W_Z \cdot [h_{t-1}, x_t]) \tag{20}$$

$$r_t = \sigma(W_r \cdot [h_{t-1}, x_t]) \tag{21}$$

$$\tilde{h}_t = tanh\,(W \cdot [r_t * h_{t-1}, x_t]) \tag{22}$$

$$h_t = (1 - z_t) * h_{t-1} + z_t * \tilde{h}_t \tag{23}$$

Whereas σ and $tanh$ denote the activation function, W represents the weight matrix connecting the two layers. $z\&r$ indicate the update and the reset gates correspondingly. Compared to the sequence problem, the typical RNN employs the preceding data based on the forward input sequence. Based on this problem, the Bi-RNN system was presented when memorizing the abovementioned dataand subsequent data. The fundamental concept is to utilize two RNNs for processing the forward and reverse sequences correspondingly. Then, the output is interconnected to a similar output layer. Thus, bi-directional contextual data for the feature sequence could be recorded. According to the BRNN, the BiGRU system is attained by substituting the hidden layers in the BRNN with the GRU memory unit.For a d-dimension input $(\chi_1, \chi_2 \chi_n)$. At time t, the hidden neuron of the BiGRU output h_t.

$$\overrightarrow{h_t} = \sigma(W_{x\vec{h}} x_t + W_{\vec{h}\vec{h}} \overrightarrow{h_{t-1}} + b_{\vec{h}}) \tag{24}$$

$$\overleftarrow{h_t} = \sigma\left(W_{x\overleftarrow{h}} x_t + W_{\overleftarrow{h}\overleftarrow{h}} \overleftarrow{h_{t-1}} + b_{\overleftarrow{h}}\right) \tag{25}$$

$$h_t = \overrightarrow{h_t} \oplus \overleftarrow{h_t} \tag{26}$$

Whereas W represent the weight matrix connecting the two layers, b denotes the bias vector, σ shows the activation function, $\overrightarrow{h_t}$ and $\overleftarrow{h_t}$ indicates the output of positive and negative GRU correspondingly. $\oplus$ represent element-wise sum.

Design of CSO-based Hyperparameter Tuning

For optimally modifying the hyperparameters involved in the BiGRU model, the CSO algorithm has been employed to it [Prabavathy et al, 2018]. CSO is a novel optimized technique from the domain of SI [Rahman et al, 2020]. The CSO technique processes the performance of cats into 2 processes: the 'Seeking method'and the 'Tracing method'. The swarm was produced of the primary population collected of particles for searching from the solution spaces. i.e., it could simulate bird, ant, and bee and generate PSO, ACO, and BCO correspondingly. At this point, in CSO, it can be utilized cats as particles to resolve the problem. In CSO, all cats have their individual place collected of D dimensional, velocity to all dimensions, fitness value that signifies the accommodation of cat to FF, and flag for identifying when the cat is in seek/trace systems. The last solutions are the optimum place for most cats. The CSO keeps the optimum solutions and attains the last iterations [Rath & Misra, 2018]. The CSO technique involves 2 procedures for solving the issues that are explained under:

It can utilize the seeking method to model the performance of cats from resting time and being alert. This process is a time to think and decide on the next moves. This method contains 4 important parameters that are declared as follows: self-position consideration (SPC), seeking memory pool (SMP), counts of dimension to change (CDC), and seeking a range of selected dimensional (SRD).

The procedure of seeking system was explained as follows:

Step_1: Generate j copy of the existing place of cat_k, whereas $j =$ SMP. When the value of SPC is true, assume $j =$(SMP -1), afterward retain the existing place as most candidates.

Step_2: To all copies, based on CDC, arbitrarily plus or minus SRD percent the existing value and exchange the old ones.

Step_3: Calculate the fitness values (FS) of every candidate point.

Step_4: Once every FS isn't exactly equivalent, compute the choosing probabilities of all candidates point by (1);else, set every choosing probability of all candidate points to be 1.

Step5: Arbitrarily pick the point for moving to the candidate point, and exchange the place of cat_k.

$$P_i = \frac{|SSE_i - SSE_{max}|}{SSE_{max} - SSE_{min}} \tag{27}$$

When the aim of FF is to find the minimal solution, $FS_b = FS_{max}$, else $FS_b = FS_{min}$

The tracing system is the 2nd process of technique. During this method, the cat needsto tracethe target as well as the food. The procedure of the tracing system is explained as follows:

Step_1: Upgrade the velocity to all dimensional based on Eq. (28).

Step_2: Verified the velocity from the range of maximal velocities. During this case, a novel velocity is over-range;it can be set equivalent to limits.

$$V_{k,d} = V_{k,d} + r_1 c_1 \left(X_{best,d} - X_{k,d}\right) \tag{29}$$

Step_3: Upgrade the place of cat_k based on Eq. (30).

$$x_{k,d} = x_{k,d} + V_{k,d} \tag{30}$$

X_{bestd} refers to the place of the cat as an optimum fitness value, $X_{k,d}$ signifies the place of cat_k, c_1 is an acceleration co-efficient to extend the velocity of the cat for moving from the solution spaces and generally is equivalent to 2.05 and r_1 stands for the arbitrary value uniformly created from the range of zero and one. The CSO algorithm computes a FF to attain higher classification performance. It defines the positive integer for representing the optimum performance of the candidate solution. During this case, the minimized classification error rate was assumed as FF in Eq. (31). A better solution is a minimal error rate, and the least solution gains an improved error rate.

$$fitness(x_i) = Classifier\ Error\ Rate(x_i)$$

$$= \frac{number\ of\ misclassified\ instances}{Total\ number\ of\ instances} * 100 \tag{31}$$

The GRU memory unit integrates the input gate i and the forgetting gate f in the LSTM to an update gate z that resolves the long dependence problem and retains significant features, while the structure is simple when compared to the LSTM . In time t, for an input X_t, the hidden layers of the GRU output h_t, in the following:

$$z_t = \sigma(W_Z \cdot [h_{t-1}, x_t]) \tag{20}$$

Performance Evaluation

This section verifies the accuracy and reliability of the proposed scheme through simulation and comparison of the performance with several well-known schemes.

Simulation Environment

This section inspects the result analysis of the MOSPO-CMR techniques with recent approaches, under several aspects are discussed here. Table 1 inspects the result analysis of the MOSPO-CMR technique in terms of energy consumption (ECM), network lifetime (NLFT), and throughput (THRP).

The experimental result analysis of theOCOA-CSBiGRU technique takes place using the KDDCup99 dataset [source], which holds 125973 instances with 41 features and 2 classes. Fig. 3 shows the FS results of the OCOA-FS technique with other techniques. From the figure, it is evident that the GA-FS and BGOA-V techniques have resulted in poor performance with the higher number of chosen features. Besides, the TLBO-FS, BGOA-S, and BGOA techniques have accomplished a moderately reduced number of selected features. However, the OCOA-FS technique has attained improved performance with fewer features.

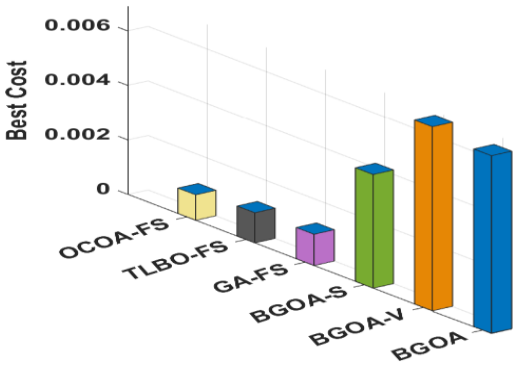

Fig. 3. FS analysis of OCOA-FS technique

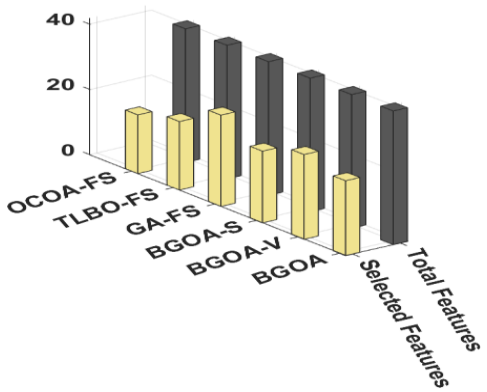

Fig. 4. BC analysis of OCOA-FS technique

Fig. 4 demonstrates the BC examination of the OCOA-FS and existing techniques. The results indicated that the OCOA-FS technique hadobtained effectual outcomes with the least BC of 0.000936, whereas the TLBO-FS, GA-FS, BGOA-S, BGOA-V, and BGOA techniques have attained slightly increased BC of 0.001108, 0.001150, 0.004176, 0.006763, and 0.006530 respectively.

Table 1 Classification results of the OCOA-CSBiGRU Technique under distinct epochs

Class	$Prec_n$	$Reca_l$	$F_{measure}$	$Accu_y$	Kappa
Epoch-100					
DoS	99.996	99.993	99.790	99.996	99.991
R2l	99.994	99.996	99.893	99.994	99.990
Probe	99.912	99.994	99.890	99.996	99.992
U2r	99.996	99.992	99.876	99.992	99.691
Normal	99.975	99.995	99.684	99.991	99.796
Average	**99.975**	**99.994**	**99.827**	**99.994**	**99.892**
Epoch-200					
DoS	99.996	99.985	99.608	99.963	99.426
R2l	99.997	99.988	99.589	99.949	99.534
Probe	99.962	99.984	99.614	99.953	99.592
U2r	99.997	99.990	99.613	99.958	99.557
Normal	99.994	99.986	99.654	99.956	99.597
Average	**99.989**	**99.987**	**99.616**	**99.956**	**99.541**
Epoch-300					
DoS	99.931	99.983	99.865	99.957	99.628
R2l	99.946	99.982	99.839	99.955	99.671
Probe	99.921	99.972	99.872	99.950	99.635
U2r	99.945	99.981	99.806	99.962	99.600
Normal	99.955	99.976	99.873	99.980	99.596
Average	**99.940**	**99.979**	**99.851**	**99.961**	**99.626**
Epoch-400					
DoS	99.838	99.946	99.892	99.930	99.605
R2l	99.851	99.964	99.801	99.930	99.630
Probe	99.844	99.951	99.858	99.937	99.611
U2r	99.852	99.963	99.833	99.939	99.639
Normal	99.848	99.949	99.800	99.931	99.697
Average	**99.847**	**99.955**	**99.837**	**99.933**	**99.636**
Epoch-500					
DoS	99.962	99.992	99.578	99.993	99.592
R2l	99.973	99.990	99.541	99.994	99.644
Probe	99.969	99.994	99.506	99.994	99.620
U2r	99.963	99.991	99.534	99.994	99.666
Normal	99.979	99.990	99.541	99.990	99.567
Average	**99.969**	**99.991**	**99.540**	**99.993**	**99.618**

Table 1 and Fig. 5 offer a detailed result analysis of the OCOA-CSBiGRU technique under distinct epochs and classes. The results demonstrated that the OCOA-CSBiGRU technique hadaccomplished enhanced classifier results interms of different measures. Under 100 epochs, the OCOA-CSBiGRU technique has obtained average $prec_n$ of 99.975%, $reca_l$, 99.993%, $F_{measure}$ of 99.790, $accu_y$ of 99.996%, and $kappa$ of 99.991%. Moreover, under 200 epochs, the OCOA-CSBiGRU approach has gained average $prec_n$ of 99.989%, $reca_l$, 99.987%, $F_{measure}$of 99.616, $accu_y$ of 99.956%, and $kappa$ of 99.541%. Furthermore, under 300 epochs, the OCOA-CSBiGRU system has reached average $prec_n$ of 99.940%, $reca_l$, 99.979%, $F_{measure}$ of 99.851, $accu_y$ of 99.961%, and $kappa$ of 99.626%. Simultaneously, under 400 epochs, the OCOA-CSBiGRU approach has obtained average $prec_n$ of 99.847%, $reca_l$, 99.955%, $F_{measure}$ of 99.837, $accu_y$ of 99.933%, and $kappa$ of 99.636%.

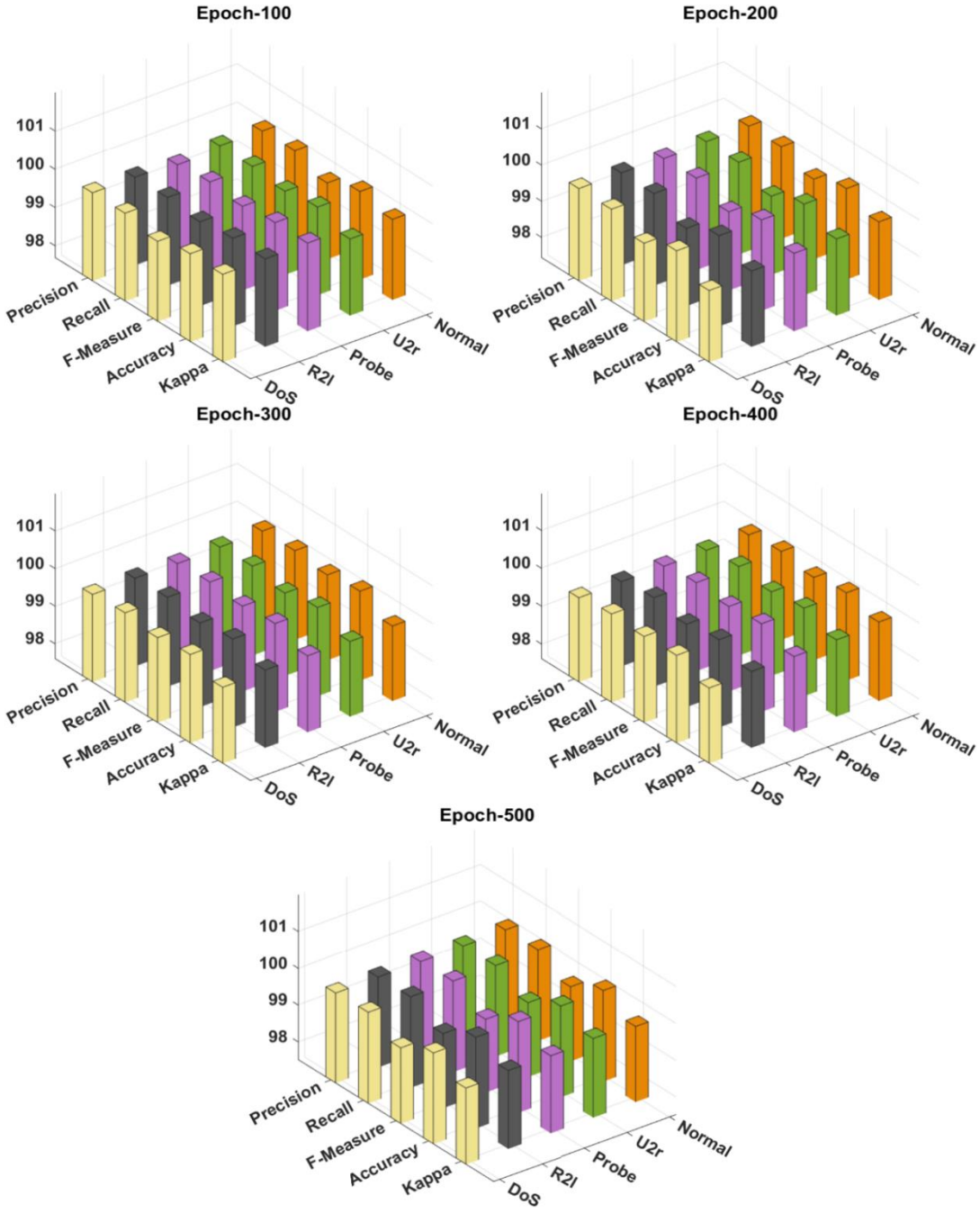

Fig. 5. Results of Different Runs on the Proposed Model

*C*oncurrently, under 500 epochs, the OCOA-CSBiGRU methodology has gained average $prec_n$ of 99.969%, $reca_l$, 99.991%, $F_{measure}$ of 99.540, $accu_y$ of 99.993%, and $kappa$ of 99.618%.

Table 2 offers thorough comparative results of the OCOA-CSBiGRU technique with existing techniques. Fig. 6 investigates the performance of the OCOA-CSBiGRU technique with existing ones interms of $prec_n$ and $reca_l$. The figure reported that the Deep Learning, DPCDBN, and AKNN techniques hadreached poor results with minimal values of $prec_n$ and $reca_l$. In line with this, the C4.5, AdaBoost, and T-SID techniques have accomplished moderately closer values of $prec_n$ and $reca_l$. Though the DBN model has resulted in near-optimal outcomes with the $prec_n$ and $reca_l$ of 0.9994 and 0.9997, the presented OCOA-CSBiGRU technique has accomplished better outcomes with the higher $prec_n$ and $reca_l$ of 0.9998 and 0.9999.

Table 2 Comparative classifier results of the OCOA-CSBiGRU Technique

Methods	$Prec_n$	$Reca_l$	$F_{measure}$	$Accu_y$
OCOA-CSBiGRU	*0.9998*	*0.9999*	*0.9983*	*0.9999*
DBN Technique	*0.9994*	*0.9997*	*0.9995*	*0.9996*
T-SID Algorithm	*0.9750*	*0.9520*	*0.9730*	*0.9400*
Deep Learning	*0.9350*	*0.9490*	*0.9410*	*0.9280*
DPCDBN	*0.9510*	*0.9500*	*0.9510*	*0.9500*
AKNN	*0.9220*	*0.9380*	*0.9290*	*0.9200*
C4.5 Algorithm	*0.9660*	*0.9280*	*0.9540*	*0.9370*
Adaboost	*0.9740*	*0.9320*	*0.9570*	*0.9590*

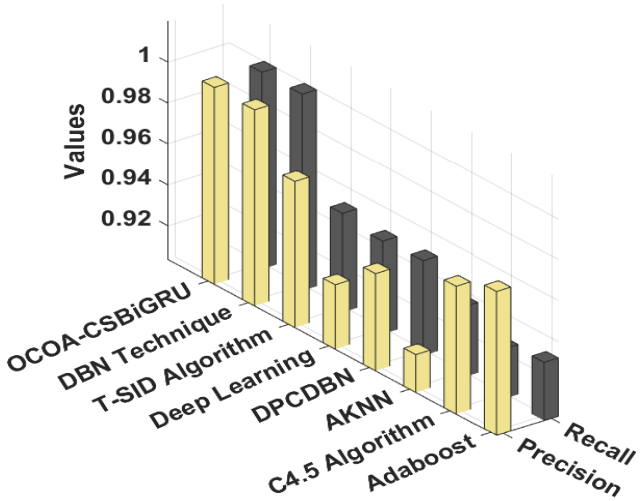

Fig. 6. Precision and recall analysis of the OCOA-CSBiGRU technique

Fig. 7 examines the performance of the OCOA-CSBiGRU system with other ones based on $F_{measure}$ and acc_y. The results depicted that the Deep Learning, DPCDBN, and AKNN approaches have gained worse outcomes with minimal values of $prF_{measure}$ and acc_y. In line with this, the C4.5, AdaBoost, and T-SID techniques have accomplished reasonably closer values of $F_{measure}$ and acc_y. Eventually, the DBN system has resulted in near-optimal outcomes with $F_{measure}$ and acc_y of 0.9995 and 0.9996, the presented OCOA-CSBiGRU algorithm has accomplished optimum outcomes with the superior $F_{measure}$ and $acc_y$of 0.9983 and 0.9999.

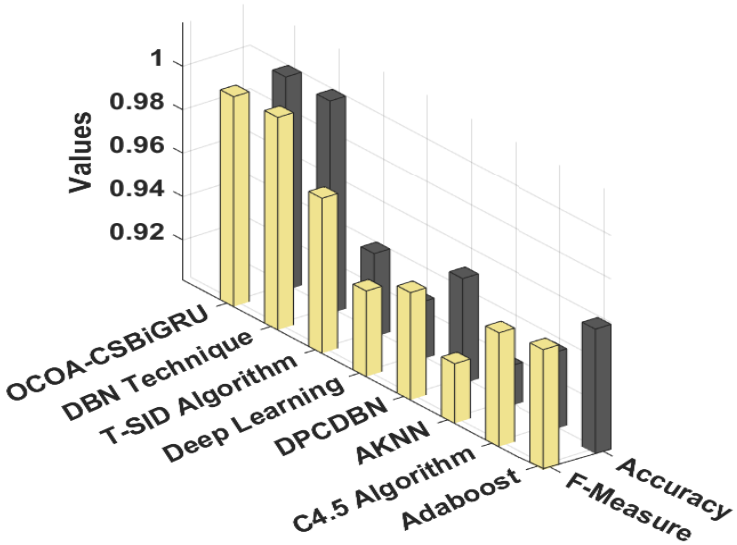

Fig. 7. Accuracy and F-measure analysis of OCOA-CSBiGRU technique

The accuracy outcome analysis of the OCOA-CSBiGRU approach on the test data is demonstrated in Fig. 8. The results portrayed that the OCOA-CSBiGRU system has accomplished higher validation accuracy related to training accuracy. It is also noticeable that the accuracy values get saturated with the count of epochs.

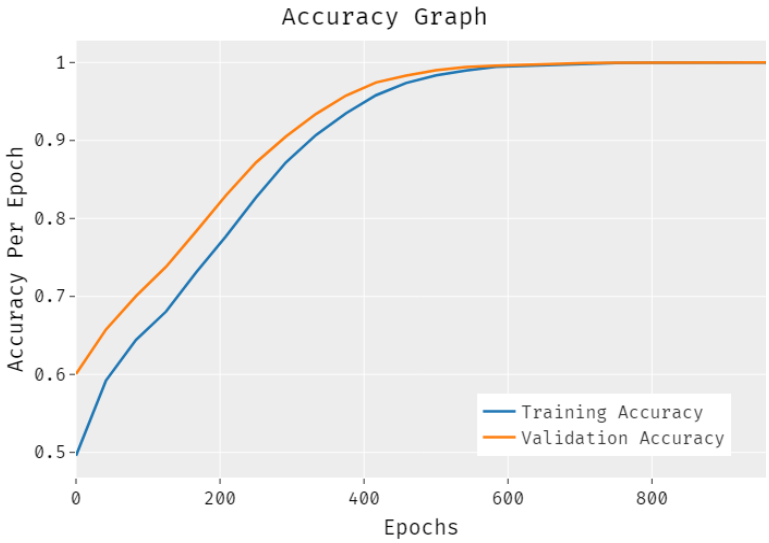

Fig. 8. Accuracy graph analysis of OCOA-CSBiGRU technique

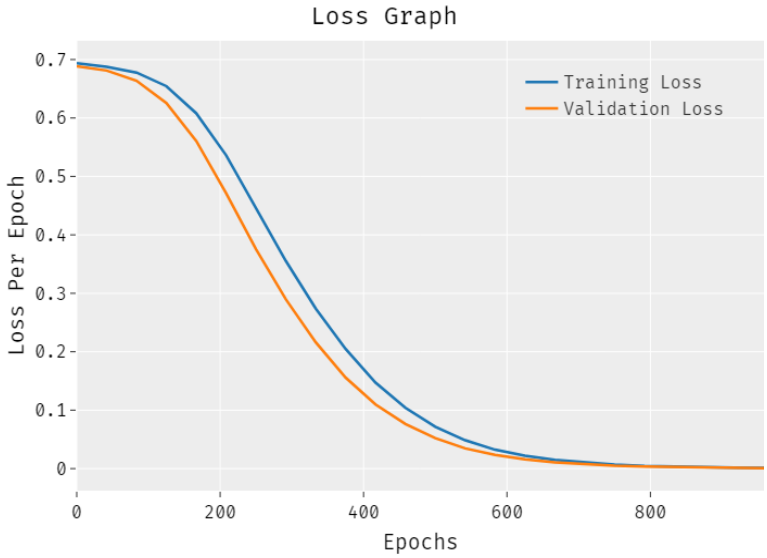

Fig. 9. Loss graph analysis of the OCOA-CSBiGRU technique

The loss outcome analysis of the OCOA-CSBiGRU algorithm on the test data is demonstrated in Fig. 9. The results revealed that the OCOA-CSBiGRU method represented the lower validation loss over the training loss. It can be additionally observed that the loss values get saturated with the count of epochs. In order to demonstrate the enhanced outcomes of the OCOA-CSBiGRU with other techniques, a detailed accuracy analysis is made in Fig. 10 [Shafi et al, 2018; Vinoth Kumar et al, 2020; Vikram & Sinha, 2021; Yang et al, 2019]. The results depicted that the CS-PSO algorithm has resulted in reduced $accu_y$ of 0.7551. In addition, the COA-IDS and DNN-SVM techniques have attained slightly improved $accu_y$ values of 0.9688 and 0.9203, respectively.

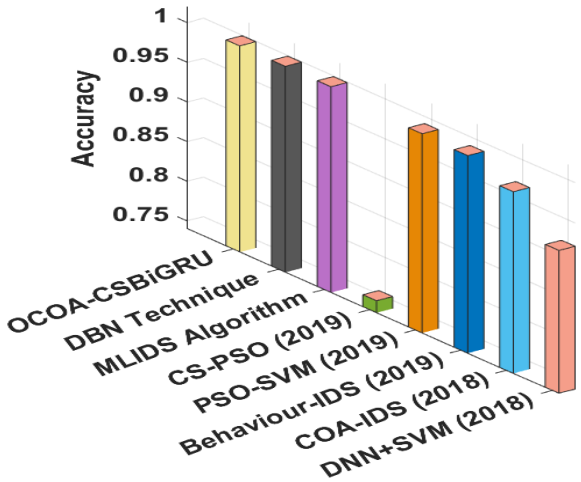

Fig. 10. Accuracy analysis of OCOA-CSBiGRU technique with existing methods

Along with that, the DBN, MLIDS, PSO-SVM, and Behaviour-IDS techniques have obtained moderately improved $accu_y$ values of 0.9996, 0.9993, 0.9910, and 0.9889, respectively. However, the OCOA-CSBiGRU technique has accomplished superior results with the maximum $accu_y$ of 0.9999. By looking into the abovementioned results, it is evident that the OCOA-CSBiGRU technique has outdone the recent methods inseveral aspects.

Conclusions

In this study, a novel OCOA-CSBiGRU technique has been developed to identify intrusions in the fog-assisted WSN. The proposed OCOA-CSBiGRU technique comprises OCOA for choice of features, BiGRU classifier, and CSO hyperparameter optimizer. Using OCOA and CSO algorithms helps accomplish maximum intrusion detection outcomes in the fog-assisted WSN. A comprehensive result analysis is done on benchmark datasets and assessesthe results under varying aspects. The comparative result analysis indicated the better outcomes of the OCOA-CSBiGRU technique over the recent methods interms of different metrics. In the future, outlier removal approaches can be integrated with Metaheuristics to improvise security and reduce complexity.

References

Ahmed, A.M., Rashid, T.A., & Saeed, S.A.M. (2020). Cat swarm optimization algorithm: a survey and performance evaluation. Computational intelligence and neuroscience, 2020, pp.1-20, https://dx.doi.org/10.1155/2020/4854895

Bangui, H., Ge, M., & Buhnova, B. (1). A hybrid machine learning model for intrusion detection in VANET. Computing, 104(3), pp.503-531, https://dx.doi.org/10.30486/mjee.2022.696508

Butun, I., Sari, A., & Österberg, P. (2020). Hardware Security of Fog End-Devices for the Internet of Things. Sensors, 20(20), p.5729, https://dx.doi.org/10.3390/s20205729

Chen, X., Yu, K., Du, W., Zhao, W., & Liu, G. (2016). Parameters identification of solar cell models using generalized oppositional teaching learning based optimization. Energy, 99, pp.170-180. https://dx.doi.org/10.1016/j.energy.2016.01.052

De Souza, C.A., Westphall, C.B., Machado, R.B., Sobral, J.B.M., & Vieira, G. (2020). Hybrid approach to intrusion detection in fog-based IoT environments. Computer Networks, 180, p.107417, https://dx.doi.org/10.1016/j.comnet.2020.107417

Diro, A., & Chilamkurti, N. (2018). Leveraging LSTM networks for attack detection in fog-to-things communications. IEEE Communications Magazine, 56(9), pp.124-130, https://dx.doi.org/10.1109/MCOM.2018.1701270

Diro A., & Chilamkurti, N. (2018) Distributed attack detection scheme using deep learning approach for internet of things. Future Generation Computer Systems, 82, pp.761–768 43 https://dx.doi.org/10.1016/j.future.2017.08.043

Djenouri, Y., Belhadi, A., Lin, J.C.W., & Cano, A. (2019) Adapted k-nearest neighbors for detecting anomalies on spatio–temporal traffic flow. IEEE Access, 7, pp.10015–10027, https://dx.doi.org/10.1109/ACCESS.2019.2891933

Kaur, H. & Sood, S.K. (2019). Fog-assisted IoT-enabled scalable network infrastructure for wildfire surveillance. Journal of Network and Computer Applications, 144(11), pp.171-183, https://dx.doi.org/10.1016/j.jnca.2019.07.005

Kaushik, S., & Sinha, A. (2021). Fog-Assisted Data Security and Privacy in Healthcare. In Fog Computing for Healthcare 4.0 Environments, pp. 315-336, https://dx.doi.org/10.1007/978-3-030-46197-3_13

Kumar, G., Mohan, S. & Nagesh, A. (2021). An ensemble of feature subset selection with deep belief network based secure intrusion detection in big data environment. Indian Journal of Computer Science and Engineering, 12(2), pp.409-420, https://dx.doi.org/10.21817/indjcse/2021/v12i2/211202101

Kumar, P., Gupta, G.P. & Tripathi, R. (2021). TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. Journal of Systems Architecture, 115(5), p.101954. https://dx.doi.org/10.1016/j.sysarc.2020.101954

Lawal, M.A., Shaikh, R.A., & Hassan, S.R. (2021). A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing. Procedia Computer Science, 182(8), pp.13-20. https://dx.doi.org/ 10.1016/j.procs.2021.02.003

Li, J., Zhao, Z., Li, R., & Zhang, H. (2018) AI-based two-stage intrusion detection for software defined IoT networks. IEEE Internet Things, 6(2), pp.2093–2102, https://dx.doi.org/10.1109/JIOT.2018.2883344

Lynn, H.M., Pan, S.B., & Kim, P. (2019). A deep bidirectional GRU network model for biometric electrocardiogram classification based on recurrent neural networks. IEEE Access, 7, pp.145395-145405. https://dx.doi.org/ 10.1109/ACCESS.2019.2939947

Maheswari, M., & Karthika, R.A. (2021). A Novel QoS Based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks. Wireless Personal Communications, 118(4), pp.1-23. https://dx.doi.org/ 10.1007/s11277-021-08101-2

Malik, A., & Khamparia, A. (2020). An Overview to Design an Efficient and Secure Fog assisted Data Collection Method in the Internet of Things. Fog, Edge, and Pervasive Computing in Intelligent IoT Driven Applications, pp.193-208, https://dx.doi.org/10.1002/9781119670087.ch11

Omar, H.O.M., Goyal, S.B., & Varadarajan, V. (2021). Application of Sliding Window Deep Learning for Intrusion Detection in Fog Computing. Emerging Trends in Industry 4.0 (ETI 4.0), pp. 1-6. IEEE. https://dx.doi.org/10.1109/ETI4.051663.2021.9619421

Pacheco, J., Benitez, V.H., Felix-Herran, L.C., & Satam, P. (2020). Artificial neural networks-based intrusion detection system for internet of things fog nodes. IEEE Access, 8, pp.73907-73918. https://dx.doi.org/10.1109/ACCESS.2020.2988055

Pierezan, J., & Coelho, L.D.S. (2018). Coyote optimization algorithm: a new metaheuristic for global optimization problems. IEEE congress on evolutionary computation (CEC), 242(7-8), pp. 1-8. IEEE. https://dx.doi.org/10.1016/j.compstruc.2020.106353

Prabavathy, S., Sundarakantham, K., & Shalinie, S.M. (2018). Design of cognitive fog computing for intrusion detection in Internet of Things. Journal of Communications and Networks, 20(3), pp.291-298. https://dx.doi.org/ 10.1109/JCN.2018.000041

Rahman, M.A., Asyhari, A.T., Leong, L.S., Satrya, G.B., Tao, M.H., & Zolkipli, M.F. (2020). Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. Sustainable Cities and Society, 61(1), p.102324. https://dx.doi.org/10.1016/j.scs.2020.102324

Rath, M., & Misra, R. (2018). An exhaustive study and analysis of assorted application and challenges in fog computing and emerging ubiquitous computing technology. International Journal of Applied Evolutionary Computation (IJAEC), 9(2), pp.17-32. https://dx.doi.org/10.4018/IJAEC.2018040102

Source: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

Shafi, Q., Basit, A., Qaisar, S., Koay, A., & Welch, I. (2018). Fog-assisted SDN controlled framework for enduring anomaly detection in an IoT network. IEEE Access, 6, pp.73713-73723. https://dx.doi.org/10.1109/ACCESS.2018.2884293

Vinoth Kumar, K., Jayasankar., Eswaramoorthy., & Nivedhitha, V. (2020). SDARP: Security based Data Aware Routing Protocol for Ad hoc Sensor Networks. International Journal of Intelligent Networks, 2020(1) , pp36-42, httpss://doi.org/10.1016/j.ijin.2020.05.005

Vikram, R., & Sinha, D. (2021). FogFire: fog assisted IoT enabled forest fire management. Evolutionary Intelligence, 16(1145/2896387), pp.1-22. https://dx.doi.org/ 10.1007/s12065-021-00666-y

Yang, Y., Zheng, K., Wu, C., Niu, X., & Yang, Y. (2019). Building an effective intrusion detection system using the modified density peak clustering algorithm and deep belief networks. Applied Sciences 9(2), p.238. https://dx.doi.org/ 10.3390/app9020238