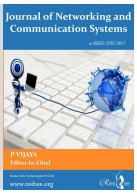
Vol.4 No.2 April 2021

Journal of Networking and Communication Systems

Received 16 December, Revised 19 February, Accepted 14 March



Cloud Intrusion Detection using Modified Crow Search Optimized based Neural Network

Vaibhav Ankush Thorat
Griffith College, Dublin, Ireland
vaibhavthorat77@gmail.com

Abstract: For computing services, cloud computing is represented as the internet-based method whereas cloud users use the resources. In the cloud service, intrusion or attacks is considered as one of the main problems in the cloud environment because it corrupts the performance. The service is affected because of the various attacks, and it provides deceptive information also maximizes the false rate. A novel Modified CSA-based Levenberg-Marquardt Neural Network (MCS-LM NN) is proposed in this paper to recognize the intrusion behavior. At first, the cloud network experiences producing the clusters by exploiting the WLI fuzzy clustering model. This model attains the diverse count of clusters in that the data objects are clustered together. Subsequently, the clustered data is subjected to the MCS-LM NN, which is the integration of the Levenberg-Marquardt method of NN and Modified CSA. The CSA is exploited to update the weight, as well as it also exploits to ascertain the optimal weight to identify the malicious activity via training procedure. Hence, the diverse clustered data is subjected to the developed optimization technique. After training the data, the data requires to be aggregated. Then that data is subjected to the MCS-LMNN model, whereas the intrusion behavior is recognized. At last, the experimentation outcomes of the developed technique and the performance analysis are carried out using the False Positive Rate (FPR), accuracy, and True Positive Rate (TPR). Therefore, the developed model obtains superior accuracy and it assures improved detection performance.

Keywords*:* Attacks, Cloud Computing, Clustering, Intrusion, Neural Network.

Nomenclature

Abbreviations	Descriptions
SaaS	Software-as-a-Service
IT	Information Technology
CPs	Cloud Providers
IDS	Intrusion Detection System
ANN	Artificial neural network
EaaS	Expert-as-a-Service
ABC	Artificial Bee Colony
PaaS	Platform-as a-Service
IACC	Interference-Aware Congestion Control

1. Introduction

Cloud computing act as a new model, which delivers IT based on the internet-based infrastructure and it offers the computing resources like storage services, operating systems, network infrastructure, hardware equipment, and even complete software applications to users in a minimum-cost manner. The Internet technologies, as well as the cloud metaphor, reference the ever-present accessibility as well as the availability of computing resources. To user programs the computing resources are assigned as on-demand services and that are provided by the cloud. Actually, users disburse for the resource and it utilizes in a manner which existing services namely electricity, water as well as natural gas. The significant services namely IaaS, SaaS, EaaS, and PaaS and it is provided by cloud computing services [1].The IDs recognize the computer attacks by verifying several data records seen in the network. Misuse signature, as well as anomaly-based detection, is classified. The anomaly detection tries to identify variations from the normal patterns, which might be stated as intrusions [2].

Conversely, misuse detection exploits patterns associated with the known attacks, or system vulnerabilities to recognize intrusions [3].

https://doi.org/10.46253/jnacs.v4i2.a2

For cloud computing systems, the complex model creates vulnerability to numerous types of attacks. Currently,potential outcomes are exhibited that the exploit of cooperative ID to enhance the detection precision while comparing with the conventional single IDS [10]. It is because of the reality becoming mainly issue for single IDS to recognize all conventional attacks and it restricted the knowledge of attack implications as well as patterns. The collaboration between IDs which be owned by diverse CPs can be attained by permitting them to swap their intrusion analysis feedback as well as it exploits each other expertise hence, it attains mutual advantages [9].

In cloud computing, ID is an NP-Hard issue. Hence, this issue can be resolved by numerous techniques based on the meta-heuristic methods as well as evolutionary computing. A novel technology has appeared on the basis of the integrations of ABC, and ANNs, and fuzzy clustering techniques. In IDs, ANN can function alone, but the integration of ANN, ABC, and fuzzy clustering creates IDS highly efficient [11].

The ABC aids the ANN to ascertain the ideal values for connection weights and biases more rapidly. Nevertheless, the augmentation of two methods to the ANN is highly expensive. The current study has exhibited that mutual detection can improve the detection rate up to 60%.

The most important contribution of this paper is to develop a present a Modified CS-LMNN which is the integration of a modified Crow Search algorithm with the LM NN. This optimization algorithm is exploited to determine the optimal weight of the network; the optimal weight is used to determine to recognize the intruder. To produce multiple counts of clusters for intrusion detection system WLI fuzzy clustering model is exploited.

2.Literature Review

In 2020, AbdulazizAldribi et al [1], introduced a novel hypervisor-based cloud IDS to recognize anomalous network behaviors, which exploits the online multivariate statistical change analysis. Since an exit from the existing monolithic network IDS feature technique was modeled. Also, a hypervisor comprises of an instance collection was developed. In 2019, Adel Abusitta et al [2], developed an ML-based cooperative IDS that effectively uses the historical feedback data to present the capability of proactive decision making. Particularly, the developed technique was on the basis of a DA that was exploited to model a deep NN. The DA power relies on its capability to learn to model the IDS feedback. In 2018, Mohamed Idhammad et al [3], developed a distributed ML-based IDS for Cloud environments. The developed technique was modeled to be inserted in the Cloud side by side with the edge network modules of the Cloud provider. This permits to interruption of inward network traffic to the edge network routers of the physical layer. To preprocess the captured network traffic a time-based sliding window method was exploited on each Cloud router. In 2017, Mingming Chen et al [4], addressed a competent fuzz yclustering-based technique for ID of a mobile node or MANETs experimentation in a cloud storage environment. This work developed a technique and investigational validations to enhance the effectiveness. In 2018, Bahram Hajimirzaei and Nima Jafari Navimipour [5], adopted a new IDS on the basis of the amalgamation of an MLP network, and ABC as well as fuzzy clustering techniques. Abnormal and normal network traffic packets were recognized using MLP when MLP training was performed using the ABC method via optimizing the values of connection weights as well as biases.

3. System Model

The malicious behavior of the cloud environment is detected by exploiting the hypervisor detection system. In Virtual Machines (VM), the hypervisor is created and executed, and it is stated as firmware and software. In a hardware platform, the VM runs which can be saved on several positions as well as it monitors the cloud network traffic. Hence, the clustering model is exploited by the hypervisor detector, and the malicious, as well as intrusion node detection, is exploited by the optimization approach.

Fig 1 demonstrates the architecture model of the proposed approach.

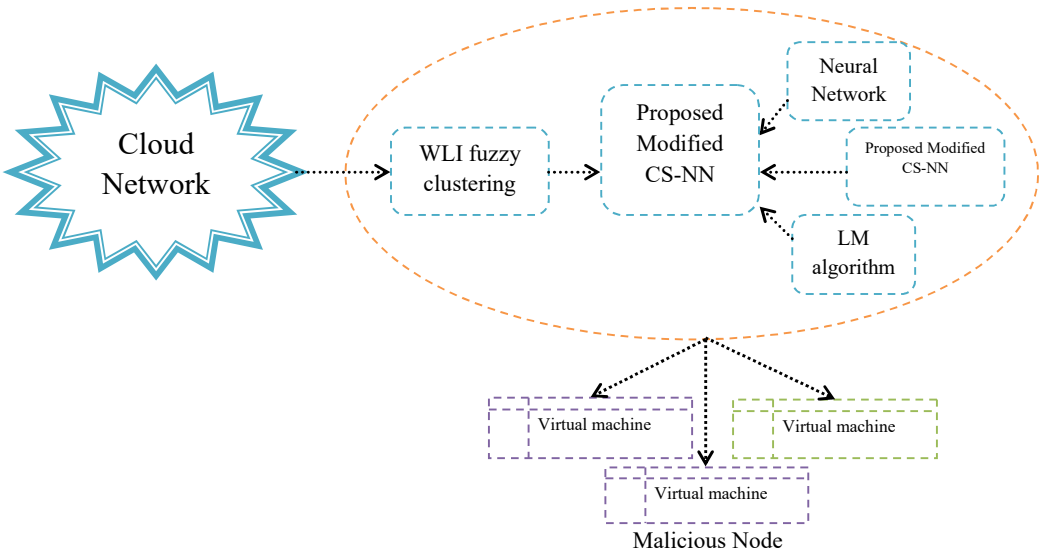


Fig. 1*Architecture model of the proposed method*

4. Cloud intrusion using an Optimized Algorithm

The main contribution of this work is to model and propose a system by exploiting the WLI fuzzy clustering and Modified CS-NN model for the cloud ID. At the hypervisor layer, the ID system is modeled known as Hypervisor detector which uses the adopted technique to detect the behavior of the intrusion of the cloud network. Initially, to the cloud network, the WLI fuzzy clustering model is used to produce a diverse count of clusters. Subsequently, to the training approach, the ensuing clustered outcome is subjected as the input for the learning procedure. The new Modified CS-NN model is developed for the effectually ID. The developed method is recently devised by integrating the LM model-based NN and CS technique. Using the LM model and CS method, the weight update is performed. Therefore, the proposed model is applied to the NN, which acts as a training approach. At last, the developed technique uses the NN, to train with the proposed model to recognize the intrusion behavior that acts as an ID of the cloud network.

i) An optimized algorithm with LM-NN

In this work, the novel Modified CS-NN is developed, the intrusions in the cloud environment are detected by a hypervisor detector. The NN, LMNN [7],and CS [6] aid the developed and adopted model. The important contribution of the adopted model is to ascertain the malicious activities of the cloud environment using the proposed model. Moreover, the modified-CSNN techniques are used to train the datasets by exploiting the CS method as well as the LM NN model the weights amid the layers are newly produced. The developed Modified CSNN formulation is stated as follows:

a) Initially, the NN is stated as a 3 layered structure that comprises an input layer, an output layer, and a hidden layer. Moreover, it consists of a huge number of neuron which is exploited to extremely be linked the network. The NN formulation is stated as:

$$b_y = \sum_{z=1}^{x} w_z a_z \tag{1}$$

whereas, a_z and b_y indicates the input, as well as output neurons of NN and, w_z indicates the weight neurons amid input as well as output layer.

b) In the NN, because of large computational resources, the LM [7] is used to present superior effectiveness as well as better convergence property. Initially, LMNN is used to calculate the Jacobian matrix it is mostly exploited to alleviate the training error. Hence, the LM method is stated as,

$$W_{new}^{LM} = W_{old} + \Delta W \tag{2}$$

whereas, W_{old} signifies the weight attained using NN, W_{new}^{LM} signifies the new weighting function of by exploiting LM method, ΔW adjusts weights amid neurons that are expressed as:

$$\Delta W = \left(J^T J + \lambda I \right) J^T e \tag{3}$$

whereas, e indicates the learning error and J indicates the Jacobian matrix.

c) The LM method restriction is sensitive to the first network weights of the learning method. In order to solve this issue, the crow search method is integrated with the LM technique on the basis of the NN.

In general, the crow searches approach, which is enthused by the crow's behavior, is exploited to ascertain the optimal solution. On the basis of an inherent behavior, crows pursue birds to discover food position. The crows' memory [6] the value of AP is represented as follows:

$$AP^{j.itr} = Z^{itr} \times \left(\frac{f_m^{j.itr}}{f_m^{jmax}} \right) \alpha \tag{4}$$

whereas, $AP^{j.itr}$ indicates the awareness crow probability, $f_m^{j.itr}$ indicates the objective model of memory solution and f_m^{jmax} indicates the maximum value of the objective function, α indicates the constant coefficients, which ascertains memory in order to tune the AP.

d) **Modified CS LMNN:** In the cloud environment, to detect an intruder or malicious node modified CS LMNN is the newly developed training method. The developed technique is modeled using the aforesaid LM NN and CS approach. In the optimization algorithm, the LM is extensively exploited whereas the optimal solution is attained considerably. In the CS approach, the weights (solution) are updated using eq. (4). Hence, to detect the intrusion the new weighting function is exploited that is calculated as follows,

$$W_{new}^{crow} = W_{new}^{LM} + [c_1 r_2 - 0.05] \cdot \left(W_{old} - r_1 W_{new}^{LM} \right) \tag{5}$$

where,

$$c_1 = [X_{max} - X_{min}] * \left(\frac{X_{curr}}{X_{min}} \right) + X_{min} \tag{6}$$

whereas, W_{new}^{LM} indicates the weight attained using the LM approach as well as r_1 and r_2 indicates the random variables. Additionally, the optimal weights are attained iteratively when exploiting the Crow Search optimization method. Therefore, in aforesaid formulation, X_{curr} indicates the current iteration as well as X_{max} , X_{min} indicates the maximum and minimum iteration.

e) At last, using the LM method as well as the CS method, the error is calculated. On the basis of the error value, to detect an abnormal (malicious) node, the optimal weight is ascertained. If the error of Crow search weight is lesser than LM method error, subsequently optimal weight is stated as W_{new}^{Crow}. Else, the novel weight is stated as W_{new}^{LM}. Therefore, the error is computed amid the actual input and output data object of the NN. The data is subjected to train beside the weight W_{new}^{LM} and W_{new}^{Crow} . The error formulation is stated as follows.

$$E\left(W_{new}^{(L)} \right) = \sum_{i=1}^{s} \left(d_i - d_i^* \right) \tag{7}$$

whereas, d_i^* signifies the actual output data object, d_i signifies the input data object, and CS indicates the Crow search method. Hence, the optimal weight exploited in the modified CS-NN model is used to detect the intrusion behavior. The novel weight is attained based upon the error value condition and it is indicated as

$$\begin{aligned} W_{new} &= W_{new}^{LM} \\ W_{new} &= W_{new}^{crow} \end{aligned} ; \quad \text{if} \begin{cases} E\left(W_{new}^{LM} \right) < E\left(W_{new}^{crow} \right) \\ \text{Otherwise} \end{cases} \tag{8}$$

ii)Modelling a hypervisor detector

In a cloud environment, ID is an extensively exploited detector. In this work, the three stages are exploited for the intrusion detection system WLI fuzzy clustering, developed Modified CSNN as well as Data aggregation components.

In WLI fuzzy clustering model [8], input data is subjected, whereas the data are cluster jointly to carry out the hypervisor detector. The CVI is exploited in WLI fuzzy model for the clustering model. Therefore, the Euclidean distance is measured amid data objects. In addition, it uses the fuzzy membership function besides the cluster centroid as well as the data object.

a) *Initialization:* From input data is C_l, $1 \le l \le N$, N number of clusters is arbitrarily produced from the input data.

b) *Distance and membership matrix:* In WLI fuzzy clustering model, median distance is indicated as the most important feature. Hence, fuzzy compactness is ascertained help by the fuzzy cardinality of clusters and fuzzy weighting distances [8].

$$\mu_{ij}^{\mathbf{2}}\left\|\mathrm{d_i}-\mathrm{c_j}\right\| \tag{9}$$

whereas, μ_{ij} signifies the membership function as well as $\mathrm{d_i}$ signifies the $\mathrm{i^{th}}$ data object and $\mathrm{c_j}$ signifies the $\mathrm{j^{th}}$ cluster. Subsequently, the fuzzy cardinality of the cluster is stated as $\sum_{\mathrm{i}=\mathbf{1}}^{\mathrm{K}}\mu_{ij}$.

c) *Fuzzy compactness*: For all clusters, the total fuzzy compactness ranges from 1 *to* N, and it is stated as follows:

$$\mathrm{WL_f}=\sum_{\mathrm{j}=\mathbf{1}}^{\mathrm{N}}\left[\frac{\sum_{\mathrm{i}=\mathbf{1}}^{\mathrm{K}}\mu_{ij}\left\|\mathrm{d_i}-\mathrm{c_j}\right\|^{\mathbf{2}}}{\sum_{\mathrm{i}=\mathbf{1}}^{\mathrm{K}}\mu_{ij}}\right] \tag{10}$$

d) *Cluster separation:* The median as well as minimum distance is measured amid centroids pair to separate the clusters. $N(N-1)/2$ is used to evaluate the distance amid N centroids. The least distance of all $N(N-1)/2$ distance is called 'min'. Subsequently, $\frac{\mathrm{N}(\mathrm{N}-\mathbf{1})/\mathbf{2}}{\mathbf{2}}$ is used to determine the median distance for all clusters. Hence, the cluster separation measure is calculated as:

$$\mathrm{WL_d}=\frac{\mathbf{1}}{\mathbf{2}}\left(\min_{\mathrm{i}\neq\mathrm{j}}\left\{\left\|\mathrm{c_i}-\mathrm{c_k}\right\|^{\mathbf{2}}\right\}+\operatorname*{median}_{\mathrm{i}\neq\mathrm{j}}\left\{\left\|\mathrm{c_i}-\mathrm{c_k}\right\|^{\mathbf{2}}\right\}\right) \tag{11}$$

e) *Cluster Validity Index:* At last, the N number of clusters is catered by the WLI fuzzy clustering whereas input data are clustered correspondingly. Using the ratio of cluster separation as well as fuzzy compactness the WLI is calculated. The cluster validity index is calculated as,

$$\mathrm{WLI(N)}=\frac{\mathrm{WL_f}}{\mathbf{2}\times\mathrm{WL_d}} \tag{12}$$

The WLI fuzzy clustering model presents the P count of clusters that is subsequently subjected to the developed technique. The centroid is chosen by the least value of WLI value in each cluster and it is devised as

$$\mathrm{C}=\min_{\mathrm{N}\in\mathrm{d_i}}\left\{\mathrm{WLI(N)}\right\} \tag{13}$$

For ID, to train the data, the crow is exploited to weight in the network. Hence, the crow method is used to update the weights. In the cloud environment, the proposed technique employs the NN trained with the help of the LM method to recognize the intrusion. The benefits of the developed model against the conventional model possess maximum tolerance, which tends to classify the abnormal i.e., malicious node and normal node.

In each cluster, data are aggregated in size $\mathrm{mp}\times\mathrm{n}$, whereas P indicates the total count of clusters. To Q count clusters clustered data is subjected as input. Hence, the clustered output is stated as,

$$\mathrm{C_j}=\left\{\mathrm{c_{j\mathbf{1}}},\mathrm{c_{j\mathbf{2}}},.....,\mathrm{c_{jk}}\right\} \tag{14}$$

whereas, $\mathrm{c_{jk}}$ signifies the output of $\mathrm{k^{th}}$ cluster and j signifies the number of output attained using the WLI fuzzy clustering model. The proposed technique is devised as:

$$\mathrm{a_y(q)}=\sum_{\mathrm{x}=\mathbf{1}}^{\mathrm{h}}\mathrm{w_{new}c_x(p)};\quad\begin{cases}\mathbf{1}\le\mathrm{p}\le\mathrm{P}\\ \mathbf{1}\le\mathrm{q}\le\mathrm{Q}\end{cases} \tag{15}$$

whereas, c_x indicates the clustered input, P as well as Q indicates the total count of clusters and developed technique, as well as a_y indicates the modified CS-NN output. Subsequently, the significant problem in the training method is the weight w_{new} which is optimal weight attained using the LM method of NN and the modified CS method. Hence, the clustered data size of $\mathrm{mp}\times\mathrm{n}$ is trained using the proposed model that presents the $\mathrm{mp}\times\mathbf{1}$ size of trained data.

Hence, the aggregated data is subjected to the novel optimization model. The optimization method input is indicated as below:

$$t = \{f_1, f_2, ..., f_q\} \quad (16)$$

whereas t indicates the input of the new aggregated model comprises of trained data from Q number of the proposed model. At last, the data size of $m \times 1$ is obtained using the aggregation technique to carry out the ID.

5. Experimentation Procedure

The experimentation outcomes and the evaluations of the developed model were presented in this section. The analysis was estimated by considering various measures such as TPR, accuracy, and FPR. Here, the proposed method was compared with the conventional models such as Particle Swarm Optimization (PSO), Genetic Algorithm (GA), and Artificial Bee Colony (ABC).

Fig 2, 3, and 4 demonstrates the graphical representation of the proposed models over the conventional modes. In Fig 2, the proposed method is compared with the conventional models for the cluster size. Here, the proposed method is 22% better than the PSO, 20% better than the GA, 19% better than the ABC for the accuracy. In Fig 3, the proposed method is compared with the conventional models for the training data. Here, the proposed method is 30% better than the PSO, 28% better than the GA, 23% better than the ABC for the accuracy. The proposed method is compared with the conventional models for the features. Here, the proposed method is 27% better than the PSO, 24% better than the GA, 21% better than the ABC for the accuracy in Fig 4.The overall analysis shows that the proposed method over the conventional method, the proposed model revealed higher performance.

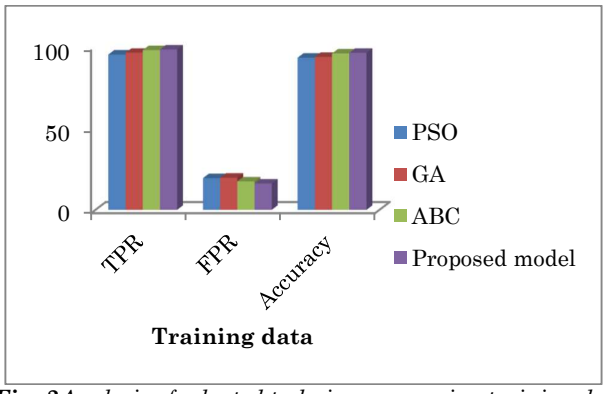


Fig. 2*Analysis of adopted techniqueconcerning training data*

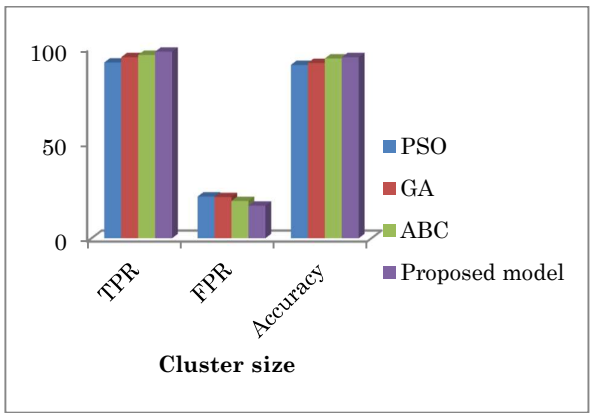


Fig. 3*Analysis of adopted technique concerning cluster size*

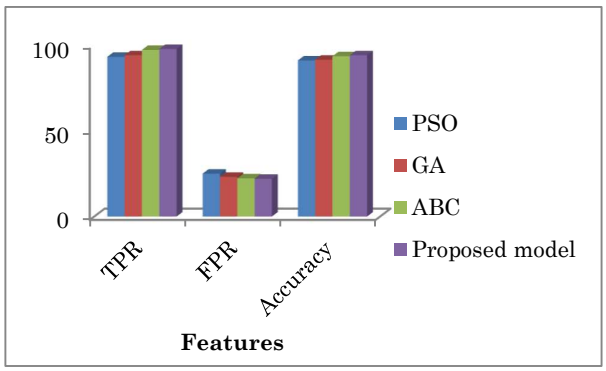


Fig. 4*Analysis of adopted technique concerning features*

6. Conclusion

In this research, a new optimization algorithm named modified CS-based LM NN algorithm as well as WLI clustering model for the cloud ID. The main intention of the developed model was exploited to update weights for the learning model. At first, to create the multiple numbers of clusters, WLI fuzzy clustering model was developed for the cloud network in that the data objected were aggregated. As a result, the proposed optimization technique was exploited to assist the NN. In each cluster, the data object was subjected to its proposed model. In this technique, the data were trained that was subsequently gathered using the data aggregation component. At last, in the proposed optimization technique, the aggregated data was subjected whereas the labels were allocated as either malicious or normal nodes. Therefore, the experimentation outcomes and the performance were evaluated with the conventional models.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] Abdulaziz AldribiIssa TraoréOnyekachi Nwamuo,"Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking", Computers & Security, vol. 88, 10 October 2019.

[2] Adel AbusittaMartine BellaicheTalal Halabi,"A deep learning approach for proactive multi-cloud cooperative intrusion detection system", Future Generation Computer Systems, vol. 98, pp. 308-318, 29 March 2019.

[3] Mohamed IdhammadKarim AfdelMustapha Belouch,"Distributed Intrusion Detection System for Cloud Environments based on Data Mining techniques", Procedia Computer Science, vol. 127, pp.35-41, 12 March 2018.

[4] Mingming ChenNing WangYuzhi Chen,"FCM technique for efficient intrusion detection system for wireless networks in cloud environment",Computers & Electrical Engineering24 October 2017.

[5] Bahram HajimirzaeiNima Jafari Navimipour,"Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm", ICT Express, vol.5, no. 1, pp. 56-59, 16 May 2018.

[6] Sina MakhdoomiAlireza Askarzadeh,"Optimizing operation of a photovoltaic/diesel generator hybrid energy system with pumped hydro storage by a modified crow search algorithm", Journal of Energy Storage, vol.27, 6 November 2019.

[7] Sotiris Konstantinidis, Pythagoras Karampiperis and Miguel-Angel Sicilia, "Enhancing the Levenberg-Marquardt Method in Neural Network training using the direct computation of the Error Cost Function Hessian", In proceedings of ACM International Conference on Engineering Applications of Neural Network, pp. 1-5, 2015.

[8] Chih-Hung Wu, Chen-Sen Ouyang, Li-Wen Chen, and Li-Wei Lu, "A New Fuzzy Clustering Validity Index with a Median Factor for Centroid-based Clustering", IEEE Transactions on Fuzzy Systems, vol. 23, no. 3, pp. 701 - 718, June 2015.

[9] Amol V Dhumane,"Examining User Experience of eLearning Systems using EKhool Learners", Journal of Networking and Communication Systems, vol. 3, no. 4, October 2020.

[10] Amit Sarkar,Senthil Murugan T," Adaptive Cuckoo Search and Squirrel Search Algorithm for Optimal Cluster Head Selection in WSN", Journal of Networking and Communication Systems, vol. 2, no. 3, July 2019.

[11] Suresh Babu Chandanapalli,Sreenivasa Reddy E,Rajya Lakshmi D,"Convolutional Neural Network for Water Quality Prediction in WSN",, Journal of Networking and Communication Systems, vol. 2, no. 3, July 2019.