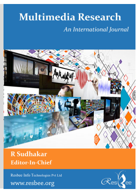
Vol.4 No.4 Oct 2021

Multimedia Research

Received 5 September, Revised 6 October, Accepted 31 October



Hybrid Grasshopper Optimization and Bat Algorithm based DBN for Intrusion Detection in Cloud

Rama Krishna Meher

University of Leicester, United Kingdom

Abstract: Cloud computing is vulnerable to accessible Information Technology (IT) attacks, as it expands as well as exploits conventional OS, IT infrastructure as well as applications. Nevertheless, the cloud computing environment occurs several security problems in recognizing the anomalous network behaviors with respect to the existing threats. An effectual Intrusion Detection System (IDS) called a hybrid Grasshopper Optimization (GSO) algorithm with Bat Algorithm (BA)-based DBN is developed to identify suspicious intrusions in cloud environments in order to solve security problems. By exploiting the fitness function the optimal solution to detect the intrusion is shown that recognizes the minimum error value as the optimal solution. Moreover, using adopted optimization approach is used to tune the weights optimally to produce an effective and best solution to detect the intruders. Nevertheless, the adopted optimization model-based Deep Belief Network (DBN) attained superior performance regarding the accuracy, sensitivity, as well as specificity by exploiting the BoT-IoT dataset.

Keywords: Cloud computing, DBN, Fitness Function, IT, OS, IDS.

Nomenclature

Abbreviations	Descriptions
BA	Bat Algorithm
DBN	Deep Belief Network
IT	Information Technology
GSO	Grasshopper Optimization
OSs	Operating System
GL	Genetic Algorithm
VM	Virtual Machine
IDS	Intrusion Detection System
PSO	Particle Swarm Optimization
CI	Computational Intelligence
SMOA	Spider-Monkey Optimization Algorithm
NN	Neural Network
RC-NN	Recurrent Convolutional Neural Network
ALO	Ant Lion Optimization
SC	Smart Controller
CNN	Convolutional Neural Network
NFV	Network Function Virtualization
DC	Domain Controllers
LSTM	Long Short Term Memory
ABC	Artificial Bee Colony
ML-IDP	Multilayered Intrusion Detection and Prevention
SDN	Software Defined Networking
HS	Harmony Search
CC	Cloud Computing
AI	Artificial Intelligence
MCC	Mobile Cloud Computing
IDPS	Intrusion Detection and Prevention System
FL	Fuzzy Logic
ANN	Artificial Neural network

https://doi.org/10.46253/j.mr.v4i4.a5

1. Introduction

In conventional IT attacks, cloud computing is vulnerable due to its employs as well as expands the conventional OSs, IT infrastructure as well as applications. Cloud computing environments countenance novel security problems since they engage numerous novel technologies which might cause new forms of exploitation with respect to the conventional threats. Cloud computing is considered as the shared resource environment which develops unpredicted novel kinds of threats like covert channel attacks as well as side channels. In addition, if a malicious user deploys a hacking tool in a VM additional VMs, as well as hypervisors, can be attacked as well as turn out to be victims. In addition, the cloud presents large numbers of computational resources that might be leveraged using a malicious user to carry out attacks outside or else within the cloud. Moreover, the constant configuration, and cloud elasticity as well as cloud resources migration increase novel, confronts for intrusion detection. Even though it is presently probable for cloud consumers to use virtual instances as well as tenant networks the shelf IDS, these systems are restricted in their focal point as well as cannot identify definite changes in the cloud hosting environment [1].

The network attacks are a serious issue that challenges the cloud providers as well as numerous amount of mobile users who has the right to use distance clouds in routine activities, presenting the security for user authentication with digital certificates or passwords as well as privacy information transmission. To surmount aforesaid problems some techniques were presented so far. To identify the cyber attacks in mobile cloud circumstances, a model which exploits uses a deep learning model [2].

Nevertheless, developing these recognition methods tends to raise the number of events within the cloud therefore recognition procedure turns out to be encumbered by soft computing aids. These involve ANN, GL, FL, and such to improve the effectiveness and detection rate accuracy of anomalies. Amid these ANN is extensively exploited owing to the ability to pact with data that is not absolute. Additionally, the mining rule association model is the present proposed model for intrusive data detection. ANN can be exploited in numerous manners in intrusion detection.

In IDS, the main disadvantage is that needs a suitable number of time as well as a raised number of training sets for effectual simulation. In the cloud, ANN integrated recognition system is a sturdy secured approach as well as this can add on GA for furthermore effectuality. ABC, HS, and PSO are a few among them exploited besides ANN-based IDS systems. Additionally, there are a few techniques that integrate 2 or more such for optimization as well as enlarged resource utilization in CC. Using search approaches the IDs' effectiveness can be enhanced that carry out to decide the optimum network parameters kinds exploited by these heuristic techniques. For example, to recognize VM attacks hybrid techniques are capable that integrating classification as well as feature selection. A security system with GA integration with the PSO examined on NSS-based Knowledge Discovery in Database data can be established in conventional research [3].

The major contribution of this paper is to achieve an intrusion detection model by exploiting the Hybrid GSO and BA model-based DBN classifier. The adopted model is mainly interested in recognizing the intruders by exploiting the features selection by exploiting the fuzzy score. At first, from the database input data is obtained as well as this data is permitted to feature the selection phase. From the fuzzy score, the features are chosen so that the fuzzy score is computed via fuzzy entropy-based metrics such as holoentropy, entropy, as well as Renyi entropy. The fuzzy score is taken into consideration as a threshold value as well as features are efficiently chosen from the fuzzy score that maximizes the detection accuracy. On the basis of the weight as well as bias related to the neurons, the DBN classifier recognizes the intruder so that the weights are trained by exploiting the optimization Hybrid GSO-BA approach.

2. Related Works

In 2020, Abdulaziz Aldribi et al [1], developed a new hypervisor-based cloud IDS to identify anomalous network behaviors that use online multivariate statistical change analysis. The reality that a hypervisor comprises a compilation of instances was leveraged as a departure from the existing monolithic network IDS feature approach, to initiate an instance-oriented feature approach that uses individual and correlated behaviors of occurrences to enhance recognition ability. The developed model was estimated by gathering and by exploiting a novel cloud intrusion dataset that involves an extensive diversity of attack vectors.

In 2020, Jitendra Kumar Samriya and Narander Kumar [2], worked on a novel hybridization model for the IDS to enhance the general security of cloud-based computing environments. Additionally, this method aids to handle different kinds of security hurdles on the cloud for instance detection of Data leakage, fake identity, as well as Phishing attacks, and so on to preserve security over the cloud. The technique exploits fuzzy on the basis of Artificial Neural Network for effectual anomalies clustering wherein fuzzy-based clustering was furthermore optimized by exploiting the SMOA. This hybrid method may overwhelm the iterative classification as well as the selection procedure of the fuzzy clustering model. Moreover, the SMO model may consequence of dimensionality as well as the minimized dataset was transmitted into NN. The developed model consequences minimized computational time and improved accuracy while evaluated with conventional hybridization models.

In 2020, T. Thilagam R. Aruna [3], worked on the IDS which was subjected on the basis of a new optimized custom RC-NN that was developed for IDS beside the ALO approach. Using this method, CNN was done hybrid with LSTM. Therefore, all attacks recognized with the network layer of the cloud were classified effectually. The investigational outcomes exhibited explain the arrangement of the IDS classification technique with maximum accuracy, therefore enhancing the error rate or detection rate.

In 2020, Shahab Shamshirband et al [4], presented a complete survey of IDS that exploit CI techniques in a cloud environment. At first, a general idea of CC a\nd MCC paradigms as well as service models was presented, in addition to this security threats were reviewed in this paper. Subsequently, taxonomy for IDS was defined as well as CI-based approaches were classified into single as well as hybrid techniques. At last, open problems, and future research for investigating this topic, were enlighted.

In 2020, Ihsan H Abdulqadder et al [5], developed a new technique which was indicated as ML-IDP in an SDN. The developed model defends against security attacks by exploiting AI. Here, five layers were utilized data acquisition layer, SC layer, DC layer, switches layer, and virtualization layer (NFV infrastructure). By exploiting the Four-Q-Curve approach, the User authentication was detained in the initial layer. The game theory model that was simulated in the IDP agent was developed. By exploiting a deep reinforcement learning approach of IDPS agent participation was to totally evade a flow table overloading attack.

3. Cloud Model

In order to pact with the problems related to the data analytical process in the cloud, the IDS is designed. It is mainly important that the studies should be authenticated, and legally admissible as well as it is described. IDS are exploited to raise the security metrics via the systematic monitoring of network traffic, log file as well as configurations. In a cloud environment, conventional IDS are not effectual as network-based IDS, because the network-based IDS is unsuccessful to recognize encrypted node communication. Therefore, to recognize attacks the IDS at the cloud middle layer is adopted. Nevertheless, the IDS model comprises storage, service, storage, and node as well as event auditor. Moreover, via the middleware, the services are made easy regarding communication. To ensure and aid the big-sized file with maximum availability the IDS exploits the distributed meta-data structure. Nevertheless, in the cloud environment, the heterogeneous data started effectively controlling as well as analyzing the data without the bottleneck.

4. Intrusion Detection in the Cloud using Hybrid GSO-BA Model

Here, to recognize the intruder pretenses an immense confrontation in the cloud environment. In the cloud, the conventional IDS undergo maximum running time as well as minimum accuracy. Therefore, an effectual IDS method is developed in this paper to carry out the IDS model. The developed IDS model by exploiting the optimization model includes three++ diverse phases such as input data fetching, feature selection as well as ID stage. At first, the input data is gathered from the database as well as this input data is fed to the feature selection phase, wherein important as well as helpful features are efficiently chosen on the basis of a fuzzy score therefore fuzzy score is computed by exploiting the fuzzy entropy-based metrics such as entropy, holoentropy as well as Renyi entropy [6]. To the DBN classifier fuzzy score is subjected as input that effectually recognizes the intruder as well as the trusted user regarding the data. In the intrusion detection stage, the ID model procedure is performed by exploiting the DBN classifier that is trained by exploiting the optimization Hybrid GSO-BA model. Fig 1demonstrates the architectural model of the adopted optimization algorithm for intrusion detection in the cloud.

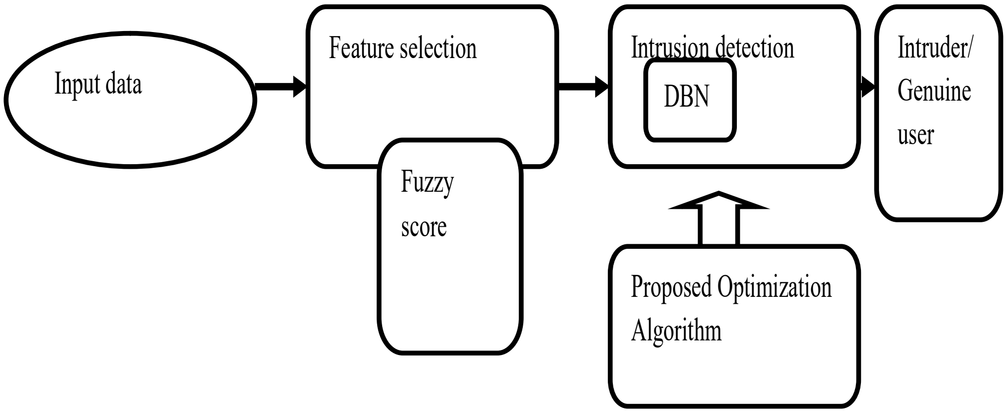


Fig.1. *Architectural model of the adopted optimization algorithm for intrusion detection in cloud*

4.1 Obtain Input Data

The input data is exploited to carry out an ID model that is gathered from the dataset. Using several phases the input data is processed as well as carries out the ID model on the basis of the DBN classifier. Assume the database as G with n count of data is stated in eq. (1). Here, X_i signifies the data located at i^{th} element, X signifies input data, as well as X_n signifies the total count of data present in the database, as well as G signifies database, correspondingly.

$$G = \{X_1, X_2, \ldots X_i, \ldots X_n\} \tag{1}$$

4.2 Feature Selections using Fuzzy Entropy

To carry out the ID procedure, the input data is X_i is chosen from the database. The input data X_i is subjected to the feature selection phase, wherein the necessary, as well as helpful features, are efficiently chosen. Feature selection is stated as the procedure of choosing the appropriate as well as helpful features that are put in towards precise recognition consequence. The main important cause of exploiting the feature selection procedure is to minimize overfitting, minimize training time as well as improve detection accuracy.

On the basis of the fuzzy score, s features are chosen so that the s is computed by exploiting the entropy α, holoentropy β, as well as Renyi entropy γ. Nevertheless, the entropy factor is calculated by exploiting eq. (2), wherein, $\alpha(X_i)$ signifies data entropy X_i, p_i signifies probability, and $u(X_i)$ signifies a number of exclusive values in input data X_i. On basis of the entropy factor, holoentropy β is computed as eq. (3), wherein, $\beta(X_i)$ signifies holoentropy of data X_i, B signifies attribute weight, as well as attribute weight, B is computed as eq. (4).

$$\alpha(X_i) = -\sum_{i=1}^{u(X_i)} p_i \log p_i \tag{2}$$

$$\beta(X_i) = B.\alpha(X_i) \tag{3}$$

$$B = 2\left[1 - \frac{1}{1+\exp(-\alpha(X_i))}\right] \tag{4}$$

The Renyi entropy is a simplification form of entropy on basis of a parameter such as Tsallis. Nevertheless, Renyi entropy is stated in eq. (5), wherein, $\gamma(X_i)$ specifies input data Renyi entropy X_i, μ specifies entropy order. At last, entropy α, holoentropy β, and the Renyi entropy γ are subjected to the fuzzy system to produce a fuzzy score s. Moreover, the fuzzy score s is represented as a threshold value as well as appropriate features are efficiently chosen from the fuzzy score. On the basis of the features selected, the intrusion detection process can be improved by exploiting the DBN classifier.

$$\gamma(X_i) = \frac{1}{1-\mu}\log\left[\sum_{i=1}^{b} p(X_i)\right] \tag{5}$$

4.3 Intrusion Detection in Cloud

In order to carry out the ID model fuzzy score s is subjected as input to DBN. To carry out the intrusion detection process, the DBN is considered an important classifier while compared with the other deep learning classifiers. The DBN needs minimum training time as well as a small labeled dataset. The DBN produces precise detection outcomes while compared with the conventional classifier. Hence, in this paper, the DBN classifier is exploited to carry out the Intrusion Detection model in the cloud [9].

4.3.1 DBN Architecture

The architecture model of the DBN classifier comprises 2 RBBM layers as well as a single MLP layer. There is no link amid visible neurons as well as hidden neurons so an interlink is present among the visible as well as hidden neurons in the DBN classifier. In RBM layer-1 visible layer fuzzy score s is subjected as input. The outcome attained from RBM layer-1 is subjected as input to RBM layer-2 as well as an outcome from RBM layer-2 is transmitted as input to the MLP layer correspondingly [10].

The fuzzy score is considered as input to DBN as well as the eq. (6) and (7) represents a hidden layer of RBM layer-1, wherein, g_r^1 signifies r^{th} hidden neuron, s_q^1 signifies q^{th} visible neuron of RBM layer-1, as well as z signifies the sum of hidden neurons. Every neuron available in hidden as well as visible layer comprises of bias. Consider g as well as h represents a bias of visible as well as the hidden layer. Nevertheless, 2 bias which stands for neurons of the hidden as well as a visible layer of RBM layer-1 which is stated in eq. (8) and (9). g_q^1 signifies the bias which stands for q^{th} visible neuron and h_r^1 stands for bias stand for the r^{th} hidden neuron. Nevertheless, eq. (10) represents the weights linked to RBM layer-1, wherein, Y_{qr}^1 indicates weight linked among q^{th} visible and r^{th} hidden neurons so that weight dimension is $w \times z$. Therefore, eq. (11) represents the outcome of the hidden layer at RBM layer-1 is computed on basis of weight as well as bias linked to visible neuron, λ specifies activation function. Hence, eq. (12) indicates the outcome attained from RBM layer-1.

$$s^1 = \left\{s_1^1, s_2^1, \ldots, s_q^1, \ldots, s_w^1\right\}; 1 \le q \le w \tag{6}$$

$$g^1 = \left\{g_1^1, g_2^1, \ldots, g_r^1, \ldots, g_z^1\right\}; 1 \le r \le z \tag{7}$$

$$g^1 = \left\{g_1^1, g_2^1, \ldots, g_q^1, \ldots, g_w^1\right\} \tag{8}$$

$$h^1 = \left\{h_1^1, h_2^1, \ldots, h_r^1, \ldots, h_z^1\right\} \tag{9}$$

$$Y^1 = \left\{Y_{qr}^1\right\}; 1 \le q \le w; 1 \le r \le z \tag{10}$$

$$g_r^1 = \lambda\left[h_r^1 + \sum_q s_q^1 Y_{qr}^1\right] \tag{11}$$

$$g^1 = \left\{g_r^1\right\}; 1 \le r \le z \tag{12}$$

The RBM layer-2 learning process is developed by exploiting the outcome acquired from a hidden layer of RBM layer-1. The RBM layer-1 output is stated in Eq. (12) that creates input to RBM layer-2. In addition, eq. (13) represents the count of visible neurons in RBM layer-2 is equal to the count of hidden neurons of RBM layer-1. $\left\{g_r^1\right\}$ represents the outcome vector of RBM layer-1. Hence, eq. (14) represents the hidden layer indication of RBM layer-2 [11].

$$s^2 = \left\{s_1^2, s_2^2, \ldots, s_z^2\right\} = \left\{g_r^1\right\}; 1 \le r \le z \tag{13}$$

$$g^2 = \left\{g_1^2, g_2^2, \ldots, g_r^2, \ldots, g_z^2\right\}; 1 \le r \le z \tag{14}$$

As stated in Eq. (8) and (9) bias of hidden as well as visible layers possesses related indication but are stated as g^2 as well as h^2, correspondingly. The RBM layer-2 weight vector is stated in eq. (15), wherein, Y_{rr}^2 signifies weight amid r^{th} visible neuron as well as r^{th} hidden neuron so that the weight vector dimension is stated in $z \times z$. Nevertheless, eq. (16) represents the outcome of r^{th} hidden neuron, wherein, h_r^2 signifies bias linked to r^{th} hidden neuron. Hence, eq. (17) represents the output attained from the hidden layer [12].

$$Y^2 = \left\{Y_{rr}^2\right\}; 1 \le r \le z \tag{15}$$

$$g_r^2 = \lambda\left[h_r^2 + \sum_q s_q^2 Y_{rr}^2\right] \forall s_q^2 = g_r^1 \tag{16}$$

$$g^2 = \left\{g_r^2\right\};1 \le r \le z \tag{17}$$

The aforesaid formulation is subjected as input to the MLP layer, wherein z indicates the count of neurons. Nevertheless, eq. (18) indicates the MLP layer input, wherein, z available in the input layer and is attained from the outcome of the RBM layer-2 hidden layer $\left\{g_r^2\right\}$. Nevertheless, the hidden layer of MLP is stated as eq. (19). wherein, A specifies the total numeral of hidden neurons. Assume that Z_D as the bias of D^{th} hidden neuron, wherein $D = 1,2,\ldots,A$. The outcome attained from the MLP layer is stated in eq. (20), wherein, k represents the count of neurons in the outcome layer. MLP comprises of 2 weight vectors, wherein, 1 is indicated amid input as well as a hidden layer, while the other is indicated amid a hidden as well as output layer.

$$v = \left\{v_1, v_2, \ldots, v_r, \ldots, v_z\right\} = \left\{g_r^2\right\};1 \le r \le z \tag{18}$$

$$a = \left\{a_1, a_2, \ldots, a_D, \ldots, a_A\right\};1 \le D \le A \tag{19}$$

$$M = \left\{M_1, M_2, \ldots, M_d, \ldots, M_k\right\};1 \le d \le k \tag{20}$$

Consider Y^C specifies weight among input as well as a hidden layer that is indicated in eq. (21), wherein, Y_{rD}^C represents weight among r^{th} input neurons as well as D^{th} hidden neurons so that weight dimension Y^C is stated as $z \times A$. On the basis of the weight as well as bias related to neurons, hidden layer output is computed as eq. (22), wherein, Z_D indicates hidden neuron bias and $v_r = g_r^2$, as the RBM layer-2 outcome creates input to MLP layer. The weights related among hidden as well as outcome layer is indicated as Y^R as well as stated in eq. (24).

$$Y^C = \left\{Y_{rD}^C\right\};1 \le r \le z;1 \le D \le A \tag{21}$$

$$a_D = \left[\sum_{r=1}^{z} Y_{rD}^C * v_r\right] Z_D \forall v_r = g_r^2 \tag{22}$$

$$Y^R = \left\{Y_{Dd}^R\right\};1 \le D \le A;1 \le d \le k \tag{23}$$

With weight Y^R as well as hidden layer output, the eq. (24) signifies output vector is calculated wherein, Y_{Dd}^R specifies weight linked among D^{th} hidden neuron as well as d^{th} output neuron, as well as a_D represents the output of hidden layer.

$$M_d = \sum_{D=1}^{A} Y_{Dd}^R * a_D \tag{24}$$

4.3.2 Adopted Hybrid GSO-BA Model

Using the adopted optimization method training procedure of the DBN classifier is performed. The adopted optimization is exploited to carry out the ID model on basis of fitness measures.

Fitness function: To calculate the optimal solution the fitness function with optimal value is presented as the optimal solution. Nevertheless, the function exploited to calculate fitness measures is indicated as eq. (25).

$$F = \frac{1}{t}\sum_{\upsilon=1}^{t}\left(M_d^{\upsilon} - \tau^{\upsilon}\right) \tag{25}$$

wherein, M_d indicates a yield of DBN classifier, t indicates the total count of samples, F states fitness function, and τ^{υ} signifies estimated output.

In the conventional GOA, initially, a levy flight by means of a variable coefficient is exploited to improve the exploration ability. Subsequently, in order to balance the exploitation as well as exploration, the GOA is integrated with the BA algorithm. In addition, an arbitrary scheme is performed on the maximum quality population to enhance the exploitation ability.

In order to encourage the optimization approach performance, the levy flight has the ability to search the space with an arbitrary walk that is extensively exploited.

A Levy flight scheme with variable coefficient and integration to the GOA is proposed in this paper. The formulation of levy flight is stated as below:

$$levy \sim u = t^{-\lambda}, 1 < \lambda \le 3 \tag{26}$$

On the basis of the Mantegna Levy random step is stated as below

$$s = \frac{\mu}{|v|^{1/\beta}} \tag{27}$$

σ_μ can be computed as below:

$$\sigma_\mu = \left[\frac{\Gamma(1+\beta)\times\sin\left(\pi\times{}^{\beta}/_{2}\right)}{\Gamma[(1+\beta)/2]\times\beta\times2^{(\beta-1/2)}}\right] \tag{28}$$

In the adopted model [14], β represents the variable coefficient before the constant that is stated below:

$$\beta = \chi + \eta rand \tag{29}$$

Hence, the enhanced mathematical formulation of GOA is stated as below:

$$X_d^i = levy * c\left(\sum_{\substack{j=i\\j\neq i}}^{N} c\frac{ub_d - lb_d}{2} s\left(|x_j^d - x_i^d|\right)\frac{x_j - x_i}{d_{ij}}\right) + \hat{T}_d \tag{30}$$

The local search operation is an important segment of BA and plays a significant role in balancing exploration as well as exploitation. Based on this, it is used to enhance GOA performance.

A novel random scheme to additional promotes the searching ability of GOA. The grasshoppers are arranged on the basis of their objective function values in the random strategy. Subsequently, k grasshoppers are chosen from the top-ranked population.

New grasshoppers are produced as below:

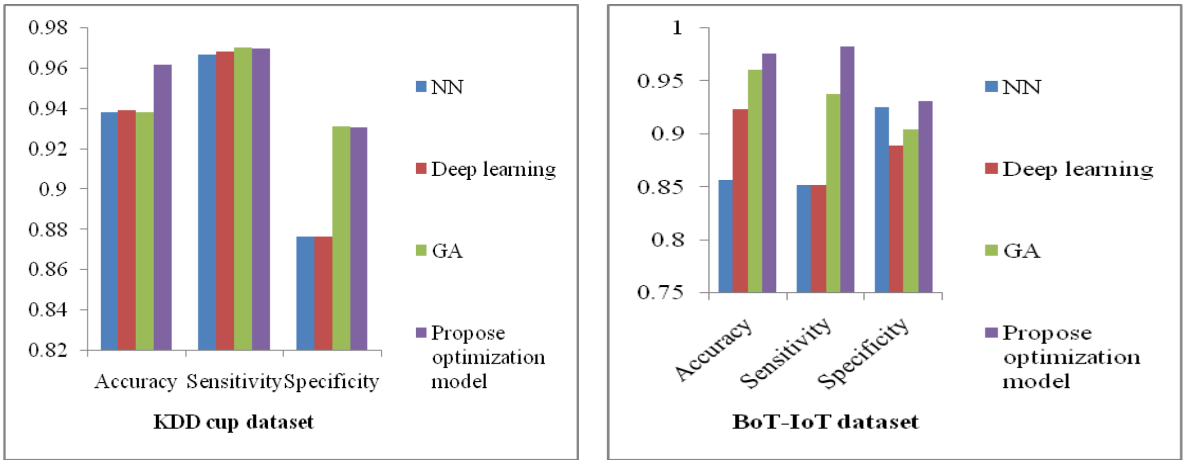
$$X_{new} = \sum_{i=1}^{k} c_i X_i \tag{31}$$

5. Result and Discussion

The simulation analysis of the developed hybrid GSA-BA-based DBN for intrusion detection was performed by exploiting the "KDD cup dataset [7], and BoT-IoT dataset [8]" [15]. The BoT-IoT dataset was developed to model the network environment to perform an intrusion detection method. The KDD cup dataset comprises a few standard set of data that involves a diversity of intrusions that were experimented within a network environment. It combines botnet, as well as normal traffic as well as source files of the dataset, which were presented in several formats, like CSV files, argus files, and pcap files, correspondingly.

The adopted model performance was shown by exploiting the evaluation measures, such as accuracy, sensitivity, as well as specificity. Here, the proposed model was compared with the conventional models such as NN, deep learning, and GA.

Fig 2 demonstrates the analysis of the adopted Hybrid GSA-BA-based DBN. It is evidently shown that the adopted Hybrid GSA-BA-based DBN attained superior performance regarding the accuracy, sensitivity, and specificity for both the KDD cup dataset as well as the BoT-IoT dataset, correspondingly.



(a) (b)

Fig. 2. *Performance analysis of the proposed and conventional model for (a) KDD cup dataset and (b) BoT-IoT dataset*

6. Conclusion

The major purpose of this work was to develop a capable intrusion detection approach to recognize the intruder in a cloud environment. At first, from the database, the input data was gathered as well as the input data was processed by exploiting the DBN classifier on the basis of the fuzzy score. This was exploited for the helpful as well as appropriate features were effectually chosen so that the fuzzy score was computed by exploiting the fuzzy entropy-based metrics such as entropy, holoentropy as well as Renyi entropy. To the DBN classifier, the fuzzy score was transmitted as the input that effectually recognizes the intruder as well as an authentic user by exploiting the fitness metrics. On the basis of the error value, the fitness measure was estimated so that function with a minimum error value was established as the optimal solution. By exploiting the optimization Hybrid GSO-BA model the DBN classifier was trained. Nevertheless, the adopted optimization Hybrid GSO-BA model attained superior performance regarding the accuracy, sensitivity, as well as specificity obtained by exploiting the BoT-IoT dataset.

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.

Reference

[1] Abdulaziz AldribiIssa TraoréOnyekachi Nwamuo,"Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking", Computers & Security10 October 2019.

[2] Jitendra Kumar SamriyaNarander Kumar," A novel intrusion detection system using hybrid clustering-optimization approach in cloud computing", Materials Today: ProceedingsAvailable online 28 October 2020.

[3] T. ThilagamR. Aruna,"Intrusion detection for network based cloud computing by custom RC-NN and optimization", ICT ExpressAvailable online 5 May 2021.

[4] Shahab ShamshirbandMahdis FathiAntonio Pescapè,"Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues", Journal of Information Security and Applications15 September 2020.

[5] Ihsan H AbdulqadderShijie ZhouSyed Muhammad Abrar Akber,"Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms", Computer Networks10 June 2020.

[6] Zheng, Y., Qin, Z., Shao, L. and Hou, X., "A novel objective image quality metric for image fusion based on Renyi entropy," Inf. Technol. J, vol.7, no.6, pp.930-935, 2008.

[7] KDD Cup 1999 Data, "http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html," Accessed on February 2020.

[8] The BoT-IoT Dataset, "https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/bot_iot.php," Accessed on February 2020.

[9] Abusitta, A., Bellaiche, M., Dagenais, M. and Halabi, T., "A deep learning approach for proactive multi-cloud cooperative intrusion detection system," Future Generation Computer Systems, vol.98, pp.308-318, 2019.

[10] Chiba, Z., Abghour, N., Moussaid, K., El Omri, A. and Rida, M., "Smart Approach to Build A Deep Neural Network Based IDS for Cloud Environment Using an Optimized Genetic Algorithm," In Networking, Information Systems & Security, ACM, pp.60, 2019.

[11] Mayuranathan, M., Murugan, M. and Dhanakoti, V., "Best features based intrusion detection system by RBM model for detecting DDoS in cloud environment," Journal of Ambient Intelligence and Humanized Computing, pp.1-11, 2019.

[12] Dey, S., Ye, Q. and Sampalli, S., "A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks," Information Fusion, vol.49, pp.205-215, 2019.

[13] Shone, N., Ngoc, T.N., Phai, V.D. and Shi, Q., "A deep learning approach to network intrusion detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol.2, no.1, pp.41-50, 2018.

[14] Yue, S., Zhang, H. A hybrid grasshopper optimization algorithm with bat algorithm for global optimization. Multimed Tools Appl 80, 3863–3884,2021.

[15] R. Cristin,Dr.V.Cyril Raj and Ramalatha Marimuthu, "Face Image Forgery Detection by Weight Optimized Neural Network Model", Multimedia Research, vol. 2, no. 2, April 2019.