Hybrid Deep Neural Network Model for Detection of Security Attacks in IoT Enabled Environment

Amit Sagu, Nasib Singh Gill, Preeti Gulia
Department of Computer Science and Applications
Maharshi Dayanand University
Rohtak, Haryana, India

***Abstract*—The extensive use of Internet of Things (IoT) appliances has greatly contributed in the growth of smart cities. Moreover, the smart city deploys IoT-enabled applications, communications, and technologies to improve the quality of life, people's wellbeing, quality of services for the service providers and increase the operational efficiency. Nevertheless, the expansion of smart city network has become the utmost hazard due to increased cyber security attacks and threats. Consequently, it is more significant to develop the system models for preventing the attacks and also to protect the IoT devices from hazards. This paper aims to present a novel deep hybrid attack detection method. The input data is subjected for preprocessing phase. Here, data normalization process is carried out. From the preprocessed data, the statistical and higher order statistical features are extracted. Finally, the extracted features are subjected to hybrid deep learning model for detecting the presence of attack. The proposed hybrid classifier combines the models like Convolution Neural Network (CNN) and Deep Belief Network (DBN). To make the detection more precise and accurate, the training of CNN and DBN is carried out by using Seagull Adopted Elephant Herding optimization (SAEHO) model by tuning the optimal weights.**

Keywords*—Internet of things; deep learning; optimization; convolutional neural network; security attack detection

I. Introduction

IoT is an integration of services, people, interconnected entities, and physical infrastructure that process the information [1]. Moreover, the IoT systems are dynamically distribute, edge based computational resources and allocations of information. IoT devices communicate with one another by wireless communication systems and transfer the information to a centralized model [2][3]. IoT is one of the interrelated models that supports seamless information among the devices (e.g.), automotive sensors, environmental sensor, industrial robots, road-side sensors, surveillance devices, medical devices and smart home sensors. The sum figure of the linked IoT devices has touched the usage of 27 billion in 2017. IoT devices used various technologies, service types, and protocols [4]. Consequently, it seems more complex to maintain the upcoming IoT framework as it leads to unwanted vulnerability in the environment. The cyber-attack could access the details in an illegal manner regarding each activity of citizens without the user's knowledge or can reconfigure the devices with the unsecured settings [5][6].

The risk rendering through these attacks may affect the protection of IoT networks and the entire eco-system such as applications, web-sites, servers and social networks, through malicious smart device known as botnet (i.e.), robot networks. Also, a communication channels or single component in IoT-based systems can be compromised by paralyzing the complete or part of Internet network [7][8][9]. Hence, the standard attack detection model is required, which could analyze the behavior of attacks in network. The rising of deep learning (DL) has alleviated the limitations of the conventional machine learning (ML) schemes due to the combined implementation of classifier and feature extraction, and its strong representative ability [10] [11][12] Further, DL model is used for avoiding the overhead of manual selection of features, and that is an essential section for traditional classification systems [13][14].

Several researchers have used the DL tools for solving the problems related to the communication which is progressively being carried out [15] [16]. Particularly, DBN is implemented based on the AMC scheme through SCF feature; however, it attains the restricted classification outcomes due to inadequate ability. Furthermore, an unsorted DNN is used for identifying the signal modulation systems with less computational complication [17] [18] [19] [20][21]. Still, the deficiencies of the convolutional operation make it more complex for extracting the high-dimensional features. The IoT devices creates large amount of data. Moreover, the ML [22][23] pipelines has performed the process of data collection, feature extraction, and binary classification in many systems or models for the detection of IoT traffic. Several ML algorithms [24][25] [26][27] including NNs[28][29][30], BNs, EL, clustering, FS, SVMs, and DTs are used for IoT attack detection with great impact. Recently, DL model is used for detecting the anomalous behavior in the IoT field [31][32][33].

The key contributions of the proposed model are given below:

- Introduces the Hybrid model for detection of attack in IoT.
- Proposed the Seagull Adopted Elephant Herding Optimization (SAEHO) algorithm for training the hybrid system through tuning the optimal weights.

In this paper, the literature review on attack detection in IoT is given in Section II. Overall description of the adopted attack detection model is determined in Section III. Pre-processing and feature extraction phase are described in

Section IV. Section V describes attack detection by proposed hybrid deep learning model. Section VI depicts the proposed seagull adopted elephant herding optimization algorithm for optimal training of hybrid model via tuning the weights. Section VII specifies the result and discussion. At the end, the conclusion of this paper is depicted in Section VIII.

II. Literature Review

A. Related Works

In [34] Li, et al., (2019) has introduced the information security approach of block chain on the basis of intrusion detection technique in the IoT. Moreover, the intrusion detection technology was used for analyzing the recognition technology on the basics of dissimilar systems, and the security of block chain information. From hacker attack, the intrusion detection model was one of the security technologies for protecting the network resources. IDS were more beneficial enhancement to the firewall that would assist the network approach for enhancing the integrity of the information security framework and detecting the attacks quickly. Finally, the proposed intrusion detection technique was used for the block chain information security system, and the experimental outcomes have shown better fault tolerance and higher detection efficiency.

In [35] Boubeta, et al., (2020) has proposed an intelligent architecture which combined ML paradigm and the CEP technology for detecting various categories of security attacks in real time IoT. Additionally, the proposed architecture was accomplished for managing the event patterns easily and the conditions depend on values attained via ML models. Moreover, an automatic code generation and a model-driven graphical device were provided for pattern definition in security attack and it hides all the complication attained from execution information of domain experts. The simulation outcome of the adopted model has demonstrated better performance than other schemes.

In [36] Marcos, et al., (2020) have adopted a near real-time SDN security model in which it secures the basis of SDN controller besides the traffic destruction and avoids the DDoS attacks in the source-end network. Further, the CNN for DDoS detection was tested and applied, and determined the system alleviate the identified attacks. A GT based technique was used to mitigate the attack in which it optimized the packet discard rate and concern within the SDN's central controller. At the end, the experimental results of the presented SDN security scheme have shown better outcomes against next-generation DDoS attacks.

In [37] Mabodi, et al., (2020) have determined a hybrid system based on the cryptographic authentication. In addition, the adopted model includes four stages like gray hole attack discovery, testing the routes, the malicious attack removal procedure in MTISS-IoT, and the IoT identifying node trust. The adopted system was assessed via extensive simulations that were done in the NS-3 tool. At the end, the experimental results of four circumstances have determined that the MTISS-IoT model has shown better FPR, FNR, and detection rate than other models.

In [38] Chunsheng, et al., (2020) have implemented a MMFN for identifying the signal modulations via a new feature known as PCCs. Furthermore, a PCCP was implemented for converting the raw modulated signals into PCCs, and it was the inputs given to MMFN. The multi-module fusion model was proposed in MMFN for acquiring the higher representation capability. Moreover, the characterization module was implemented for balancing the tradeoff among the dimensions of the extracted features and the number of parameters. At the end, the experimental results of the presented MMFN approach have achieved 90% accuracy at 1 dB SNR and superior classification performance.

In [39] Mohammed, et al., (2020) has discussed the IoT-ED possibility with implanted HT which provides serious privacy, security, and available issues to the IoT based HAN. Moreover, the traditional network attack detection models have worked the network protocol layers, while the IoT-ED with HT leads to the demonstration of attack at the firmware or/and physical level. The adopted model was used for identifying the multiple attacks and differentiated the various attack types. Further, the IoT-ED behaviors have been studied for 5 various random attacks that includes the DoS, impersonation attacks, power depletion, ARQ, and covert channel. The adopted method could distinguish with 92% accuracy for all the attacks simultaneously.

In [40] Sahay, et al., (2020) have determined a layered scheme of IoT routing security for analyzing the susceptibility linked with every phase of the routing method. The adopted system has explored the leverage of inherent features in blockchain for enhancing the security in IoT-LLNs. Moreover, the blockchain network operated as a protected data link among the attack detection mechanism and the IoT-LLN to enhance the outcomes of XGBoost algorithm. Finally, the blockchain-based model was implemented with elegant contract to generate the real-time alerts for identifying the sensor nodes.

In [41] Alabady, et al., (2020) have introduced a novel security system in the IoT era for cooperative virtual networks. The proposed model has determined the attacks and risks in switches, network security vulnerabilities, threats, routers and firewalls, along with a policy for mitigating those risks. The adopted method has offered the basics of secure networking scheme that includes router, firewall, VLAN technology and AAA server. At last, the simulation results of the adopted approach have demonstrated an effective security execution with excellent network services and speed.

B. Review

Table I shows the review on attack detection system in IoT. Originally, the Mapping UML model was determined in [41] that presents higher detection efficiency, fault tolerance and better accuracy; however, the data selection sensor technique was not incorporated into the computer environment. Moreover, the CEP and ML models were deployed in [24] that provide better precision, higher recall, and maximum F1 score. Nevertheless, more event patterns were not defined in the proposed model for detecting other types of attacks. CNN model was exploited in [42] that offer

higher accuracy, improved precision rate, and maximum recall, but need to maximize the host count in the simulated SDN environment. Likewise, MTISS-IoT model was exploited in [23], which offers better FPR, low FNR and maximum detection rate. However, the firefly optimization was not used in the proposed work to lower consumption energy and malicious attacks on the IoT. MMFN method was exploited in [29] that have robustness, higher classification accuracy, and strong characterization ability; however, the small-scale data-driven DL- AMC model with less training time was needed for training the neural network (NN). In addition, an IoT-based HAN model was determined in [28], which offers better accuracy, reduced false positives, and high precision. However, the proposed work needs to suggest the moving data process nearer to the network edge. XGBoost Classifier was suggested in [33] that offers secured network, maximum accuracy, higher recall and improved operational efficiency. However, need to investigate an efficient mechanism to address and analyze the challenges. Finally, the VLAN was introduced in [35], that offers effective security execution, best network speed and services, but the VLAN technology were not utilized in the LAN environment. Thus, the challenges have to be taken into account based on attack detection method in IoT in the present work efficiently.

III. System Model of Intrusion Detection on IoT Framework

The IoT plays significant role in the information age, and it is a significant component of the novel information technology. Moreover, the IoT server is the functional core of the entire IoT business scheme. The essential functions of terminal sensor processing, data collection and return the processing outcomes are all designed through the server. Further, the security vital in cyber life as it relies with great advancement of IoT techniques. In addition, the IDS are the protector for the Internet servers. Fig. 1 indicates the circumstances in which the IDS are concerned in the IoT network. Many of the IoT devices and IoT servers are exposed directly to the public Internet due to the feature of remote control. In addition, the attackers would capture the vulnerabilities for intruding the IoT servers. However, the IDS are extremely needed for protecting and detecting the IoT servers from the attackers. The IDS usage would protect the terminal users and also protect the service providers from the hazards on the Internet. The security protections are not fully achieved in the IoT application as it reduces the attack plane. The lowering of the attack plane is limited extremely, and intruders may find the path to crack the assured node in the network. This work seeks the strategy of deep learning concept in the intrusion detection system. Fig. 1 illustrates the IoT framework.

TABLE I. Review on Traditional Attack Detection Model in IoT: Features and Challenge

Author [citation]	**Adopted scheme**	**Features**	**Challenges**
Li *et al.* [34]	Mapping UML model	✓ Higher detection efficiency ✓ Fault tolerance ✓ Better accuracy	➢ The data selection sensor technique was not incorporated into the computer environment.
Boubeta, et al. [35]	CEP and ML models	✓ Better precision ✓ Higher recall ✓ Maximum F1 score	➢ More event patterns were not defined in the proposed model for detecting other types of attacks.
Marcos *et al.* [36]	CNN model	✓ Higher accuracy ✓ Improved precision rate ✓ Maximum recall	➢ Need to maximize the host count in the simulated SDN environment.
Mabodi *et al.* [37]	MTISS-IoT model	✓ Better FPR ✓ Low FNR ✓ Maximum detection rate	➢ The firefly optimization was not used in the proposed work to lower consumption energy and malicious attacks on the IoT.
Sai *et al.* [38]	MMFN method	✓ Robustness, ✓ Higher classification accuracy ✓ Strong characterization ability.	➢ The small-scale data-driven DL- AMC model with less training time was needed for training the NN.
Mohammed *et al.* [39]	IoT-based HAN model	✓ Better accuracy ✓ Reduced false positives ✓ High precision	➢ The proposed work needs to suggest the moving data process close to the network edge
Sahay *et al.* [40]	XGBoost Classifier	✓ Secured network ✓ Maximum accuracy ✓ Higher recall ✓ Improved operational efficiency	➢ Need to investigate an efficient mechanism to address and analyze the challenges.
Alabady *et al.* [41]	VLAN	✓ Effective security execution ✓ Best network speed and services	➢ The VLAN technology were not utilized in the LAN environment.

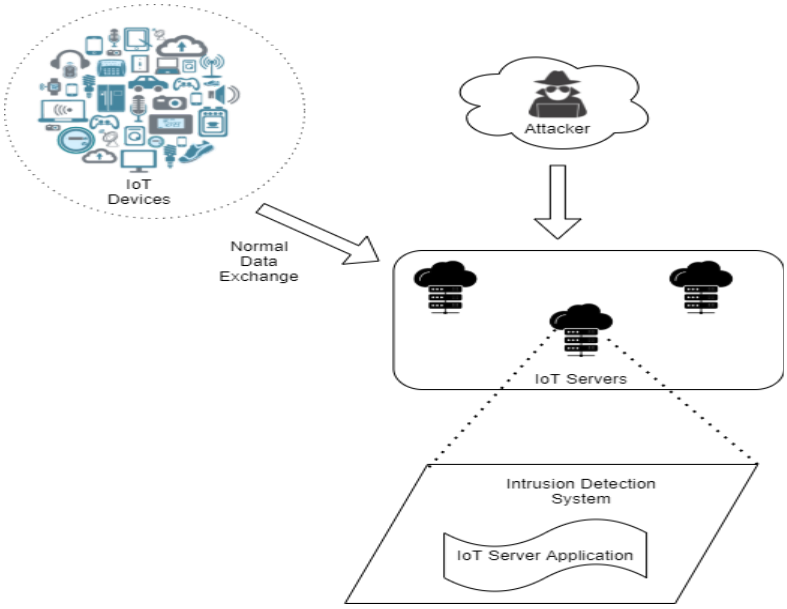

Fig. 1. IoT Framework.

IV. Overall Description of the Adopted Attack Detection Model in IoT

This proposal intends to introduce a novel deep hybrid attack detection system that consists of three phases: "(i) preprocessing (ii) Feature extraction (iii) Classification". Originally, the input data is preprocessed under data normalization process. Subsequently, the preprocessed data is subjected to the feature extraction stage, where the higher order statistical features and statistical features are extracted. Moreover, the statistical features include mean, median, SD, mode, HM, RMS, peak amplitude and pitch angle; and the higher order statistical features include kurtosis, skewness, energy, entropy, mean frequency, and percentile are extracted. Moreover, the extracted features are provided as the input to the detection phase with hybrid model that combines the models like CNN and DBN. It is obvious that the detection model must be trained in a proper manner, such that the detection accuracy increases in this way. To make this possible, this work adhere the utilization of optimization logic that could make the training process more optimal. Thereby, the weights of both the CNN and DBN are optimally tuned by a new SAEHO algorithm. This is the proposed hybrid algorithm, which combine the logic of both the EHO and SOA algorithm. Fig. 2 illustrates the architecture of proposed detection system.

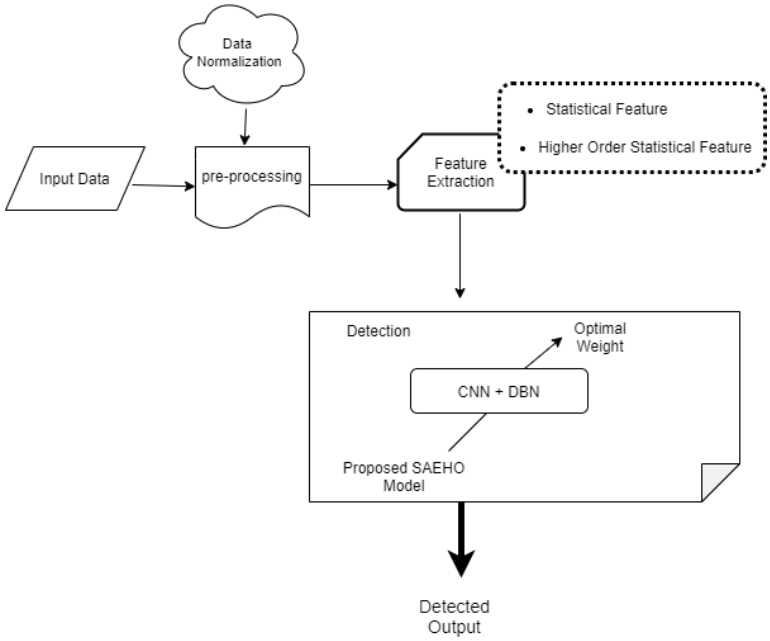

Fig. 2. Overall Framework of the Proposed Model.

V. Attack Detection by Proposed Hybrid Deep Learning Model

The proposed hybrid model follows the parallel execution of both the models with the extracted feature set, and finally averages the outcomes obtained from each model, which is considered as the final detection results.

A. Optimized CNN Model

The extracted features FE are provided as input to optimized CNN [43]. Convolutional Networks are the trainable multistage framework that includes numerous stages. The input and output of every stage are group of arrays recognized as feature maps. In addition, the well-recognized classifier is CNN that consists of 3 layers like "fully connected layer, pooling layer, and convolution layers". Furthermore, the convolution layer contains of several convolution kernels. The entire feature map was determined by the numerous kernels. Moreover, the s^{th}layers matched to x^{th}feature map and feature values in the place(e, g) is denoted as$H^s_{e,g,x}$, and it is given in Eq. (1). Similarly, thex^{th} filter value is provided in thes^{th}layer. Consequently, the optimal tuning of the weight is performed using the adopted SAEHO scheme. The linked input patches in the x^{th}layer at location(e, g) are determined using$L^s_{e,g}$. The non-linearity is attained through the activation function which predicts the nonlinear features of multi-layer networks. Moreover, $\left(A^s_{e,g,x}\right)$ and $A(\bullet)$ are defined in Eq. (2). Even though, the shift-variance in the pooling layer is deployed through minimizing the resolution of feature maps as given in Eq. (3). $pool(\ \ )$and Local neighbourhood for every feature map$\left(A^s_{e,g,x}\right)$at (e, g) is portrayed as$I_{e,g}$.

$$H^s_{e,g,x} = W_l^{sT} L^s_{e,g} + B^s_l \tag{1}$$

$$A^s_{e,g,x} = A\left(H^s_{e,g,x}\right) \tag{2}$$

$$O^s_{e,g,x} = pool\left(A^s_{e,g,x}\right), \forall(\hat{c}, \hat{r}) \in I_{e,g} \tag{3}$$

Eq. (4) determines the loss function in CNN. The constraints $(\varsigma)$of CNN are associated to the required IOinput-output relation, and it is given as$\left\{\left(V^{(t)}, U^{(t)}\right); t \in \left[1, \cdots, I\hat{O}\right]\right\}$.

$$Loss = \frac{1}{Num} \sum_{t=1}^{ms} \hat{P}\left(\varsigma; U^{(t)}, OUT^{(t)}\right) \tag{4}$$

Pooling layer: "In CNN, the pooling layer has performed the processes of down sampling with the resultant attained from the convolutional layers. Further, the 2 renowned pooling types such as max pooling and average pooling are used. The max pooling has attained the higher value; but the average value is observed in the average pooling".

Fully connected layer: It works within the flattened inputs. In general, the results attained from the pooling layer are given as the input of fully connected layer and thus the inputs are connected to all layers. In the CNN structure, the fully connected layer occurs at its edges. The output of CNN is denoted asCL_{CNN}.

B. DBN based Attack Detection

In 1986, Smolensky implemented DBN [44] with multiple layers, and there is a visible and hidden neuron in each of the layer. The visible neurons are fully interconnected with the hidden neurons. Naturally, the stochastic neuron's outcome is probabilistic in the Boltzmann networks. The DBN is fully trained to distinguish the occurrence of attackers within the network grounded on the extracted features. DBN framework is an intellectual model that includes of hidden neurons, visible neurons and layers form output layer. Furthermore, there found connotation exists via hidden and input neurons; yet, no relation in visible neurons, the association rule is not existing among hidden neurons. The link existing among visible and hidden neurons is symmetric and exclusive.

The output of the neurons is probabilistic in the Boltzmann network. The output $\hat{o}$ is grounded on the probability function$S(\psi)$in Eq. (5). The probability function has used the sigmoid-shaped function.

$$\hat{o} = \begin{cases} 1 & with S(\psi) \\ 0 & with 1 - S(\psi) \end{cases} \tag{5}$$

$$S(\psi) = \frac{1}{1 + e^{\frac{-\psi}{p}}} \tag{6}$$

Eq. (7) define the DBN model, where,$p$signifies the pseudo-temperature.

$$\lim_{p \to 0^+} S(\psi) = \lim_{p \to 0^+} \frac{1}{1 + e^{\frac{-\psi}{p}}} = \begin{cases} 0 & for \quad \psi < 0 \\ \frac{1}{2} & for \quad \psi = 0 \\ 1 & for \quad \psi > 0 \end{cases} \tag{7}$$

In DBN architecture, the path of the feature processing is shown by a collection of RBM layers, and the classification procedure shown by MLP. The mathematical model depict Boltzmann machine energy in the method of neuron or binary state$b$as portrayed in Eq. (8) and Eq. (9). Where, $w_{c,r}$ indicates the weights amid neurons, which is optimally adjusted or tuned by a new proposed SAEHO model and $\gamma_c$specifies the biases.

$$F\left(\hat{b}\right) = -\sum_{c<r} \hat{b}_c \, w_{c,r} - \sum_c \gamma_c \, \hat{b}_c \tag{8}$$

$$\Delta F\left(\hat{b}_c\right) = \sum_r \hat{b}_c \, w_{c,r} + \gamma_c \tag{9}$$

The growth of energy grounded on combined conformation in visible or hidden neurons $(a, f)$is described in Eq. (10), Eq. (11) and Eq. (12), where,$f_c$and$a_c$portrays the binary state of hidden unit r and c visible unit. X_c and Y_r indicates the biases and $w_{c,r}$signifies the weight among them.

$$F\left(\vec{a}, \vec{f}\right) = -\sum_{(c,r)} w_{c,r} \, a_c f_r - \sum_c X_c \, a_c - \sum_r Y_r \, f_c \tag{10}$$

$$\Delta F\left(a_c, \vec{f}\right) = \sum_r w_{c,r} \, f_r + X_c \tag{11}$$

$$\Delta F(\vec{a}, f_r) = \sum_c w_{c,r} \, a_c + Y_r \tag{12}$$

RBM training achieves the resultant weight allocation and the distributed probabilities are stated as in Eq. (13). The probability distribution in RBM method for the visible and hidden vectors pair$\left(\vec{a}, \overrightarrow{f}\right)$is given in Eq. (14). The partition function$Z$ is specified in Eq. (15).

$$\widehat{w}_{(C)} = \max_{\widehat{w}} \prod_{\vec{a} \in \hat{I}} D(\vec{a}) \tag{13}$$

$$D\left(\vec{a}, \overrightarrow{f}\right) = \frac{1}{Z} e^{-F(\vec{a}, \vec{f})} \tag{14}$$

$$Z = \sum_{\vec{a},\vec{f}} e^{-F(\vec{a},\vec{f})} \quad (15)$$

DBN scheme utilize the CD learning approach and the output of DBN is denoted asCL_{DBN}.The final classification output is denoted as CL, and it is expressed in Eq. (16).

$$CL = \frac{CL_{CNN}+CL_{DBN}}{2} \quad (16)$$

VI. Proposed Seagull Adopted Elephant Herding Optimization Algorithm for Optimal Training of Hybrid Model Via Tuning the Weights

A. Solution Encoding and Fitness Evaluation

The weight of both DBN and CNN are optimally adjusted or tuned via the adopted SAEHO. The input solution subjected to the adopted SAEHO scheme is demonstrated in Fig. 3, where, W_1,W_2,….$W_N$shows the weights of CNN,w_1,w_2,….w_{mn} shows the weights of DBN,N indicates the total counts of weight in CNN, andmn denotes the total number of weights in DBN. The fitnessobjective of adopted detection model is stated in Eq. (17). Here, $Loss$ indicates the detection error.

$$Obj = Min(Loss) \quad (17)$$

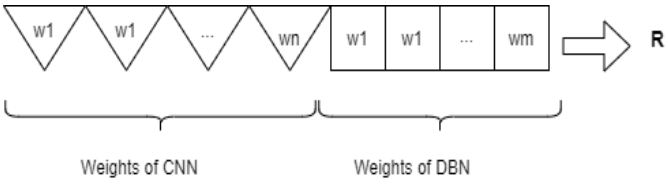

Fig. 3. Solution Encoding.

B. Proposed SAEHO Model

This paper implements a new hybrid SAEHO scheme which combines the logic of EHO [45] and SOA[46], respectively. While the traditional EHO gives better performance; the disadvantage is that it will not use the required data to identify the present and future searches. The existing SOA model has solved the challenging large-scale constrained issues and hence solve 7 constrained real-life industrial applications; still, the constraints are very tedious and computational complexity. This becomes the issue while solving optimization problems. This makes us to combine the logics of both the algorithm since the Hybrid models are reported to be promising for certain search problems with better convergence speed [23]. Here, the logic of SOA is integrated with EHO, and thereby named as SAEHO.

Naturally, the elephants live in social groups called clans and each clan stay with Matriarch, the female elephant leader. The grown male elephant lives separately from their groups. The elephant population is produced randomly and it splits into a number of clans according to their fitness value.EHO algorithm having three major rules to follows.

- The elephant population consists of number of clans with fixed number of female and male elephants in every clan.
- Some of male elephants live far from the clans individually.
- The elephant lives together with the leader of all clans, matriarch (i.e.,) female elephant in each clan.

1) Clan updating: In this operator, each clan updating is done individually. Conventionally, the subsequent position is influenced by matriarch h and for each elephant in clan h for the clan updating operators. However, as per the proposed SAEHO method, the SOA updation function is used for clan updation as given in Eq. (18).

$$R_b(\tilde{t}) = \hat{B} \times \left(R_{best}(\tilde{t}) - R_{\hat{l}}(\tilde{t})\right) + Levy(\zeta) \quad (18)$$

In Eq. (18), R_b indicates the locations of seagull search agent $R_{\hat{l}}$towards the best fit search agent PR_{best} (i.e., fittest seagull), $R_{\hat{l}}$denotes the search agent's current position, $\tilde{t}$refers to the current iteration, and the behavior $\hat{B}$is randomized used for proper balancing among exploitation and exploration.

Moreover, for the best fit elephant, the updation is achieved by Eq. (19).

$$R_{n,h,k} = \eta \times R_{cen,h} \quad (19)$$

In Eq. (19), η[0,1] is the center of clan h. The new individual $R_{n,h,k}$is expressed from the information obtained by all elephants in clan$h$. $R_{cen,h}$ represent the centre of clan h, and it is given in Eq. (20).

$$R_{cen,h} = \frac{1}{G_h} \times \sum_{k-1}^{G_h} R_{h,k,\tilde{d}} \quad (20)$$

In Eq. (21), $1 \le \hat{D} \le \tilde{d}$ denotes the $\hat{D}^{th}$ dimension and $\tilde{d}$ indicates the total dimensions. G_h specify the number of elephants in clan$h$.$R_{h,k,\tilde{d}}$ refers to the $\tilde{d}$ dimensions of the elephant individual $R_{h,k}$.

2) Separating operator: The grown male elephants in clan starts live separately. The separating operator is determined after the separating process while solving the optimization problem. As per the proposed SAEHO logic, for enhancing the search ability, the worst fitness of elephant at each generation in the separating operator is defined as per the proposed evaluation given in Eq. (21).

$$R_{worst,h} = R(R_{best} - R_{worst})_{min} \quad (21)$$

Here,R_{min}indicates the minimum bounds in the positions of single elephant. $R_{worst,h}$indicates the worst elephant individuals of clan ci and $rand$ value is calculated using Chebyshev chaotic map. The value ranges from 0 to 1.

$$R_{\tilde{q}+1} = cos\left(\tilde{q}\, cos^{-1}\left(R_{\tilde{q}}\right)\right) \quad (22)$$

The pseudo code of adopted approach is given in Algorithm 1.

Algorithm 1: Pseudo code of proposed SAEHO method
Initialization
Compute the elephant fitness
Repeat
Arrange all the elephants based on its fitness
Clan updating
For $h = 1$ to $nclan$ do
For $k = 1$ to nci do
If $R_{h,k} = R_{best,ci}$ then
Clan updation is done by the elephant position using Eq. (20).
Else
Proposed clan updation is done by the seagull position using Eq. (19)
End if
End for k
End h
Separating operator
For $h = 1$ to $nclan$ do
Replace the worst elephant as per the proposed Eq. (22)
End for h
Evaluate population by the new update positions
Until

VI. Conclusion

This paper has introduced a novel deep hybrid attack detection method. The input data subjected for preprocessing phase and data normalization process was carried out. From the preprocessed data, the statistical and higher order statistical features were extracted. Finally, the extracted features were given to hybrid deep learning model for detecting the presence of attack. The proposed hybrid classifier combines the models like DBN and CNN. To make the detection more precise and accurate algorithm named SAEHO proposed which used for tuning the optimal weights. SAEHO combines the logic of EHO and SOA. In the algorithm, two kinds of operator used i.e., clan updating and separating. Clan updating is done by EHO providing it able to find the best position else SOA is used to find the solution. As our next task, the performance of the proposed model will be computed over the present methods in terms of various metrics like FNR, MCC, Rand index, sensitivity, FPR, specificity, FDR, precision, NPV, accuracy, and FMS, correspondingly.

References

[1] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," IEEE Communications Surveys and Tutorials, vol. 21, no. 3, pp. 2671–2701, Jul. 2019, doi: 10.1109/COMST.2019.2896380.

[2] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," Applied Soft Computing Journal, vol. 72, pp. 79–89, Nov. 2018, doi: 10.1016/j.asoc.2018.05.049.

[3] M. Hossain and J. Xie, "Third Eye: Context-Aware Detection for Hidden Terminal Emulation Attacks in Cognitive Radio-Enabled IoT Networks," IEEE Transactions on Cognitive Communications and Networking, vol. 6, no. 1, pp. 214–228, Mar. 2020, doi: 10.1109/TCCN.2020.2968324.

[4] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," Journal of Network and Computer Applications, vol. 161, Jul. 2020, doi: 10.1016/j.jnca.2020.102630.

[5] A. Kore and S. Patil, "IC-MADS: IoT Enabled Cross Layer Man-in-Middle Attack Detection System for Smart Healthcare Application," Wireless Personal Communications, vol. 113, no. 2, pp. 727–746, Jul. 2020, doi: 10.1007/s11277-020-07250-0.

[6] D. Yin, L. Zhang, and K. Yang, "A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework," IEEE Access, vol. 6, pp. 24694–24705, Apr. 2018, doi: 10.1109/ACCESS.2018.2831284.

[7] A. Y. Khan, R. Latif, S. Latif, S. Tahir, G. Batool, and T. Saba, "Malicious Insider Attack Detection in IoTs Using Data Analytics," IEEE Access, vol. 8, pp. 11743–11753, 2020, doi: 10.1109/ACCESS.2019.2959047.

[8] K. Mandal, M. Rajkumar, P. Ezhumalai, D. Jayakumar, and R. Yuvarani, "Improved security using machine learning for IoT intrusion detection system," Materials Today: Proceedings, Dec. 2020, doi: 10.1016/j.matpr.2020.10.187.

[9] D. C. Wang, I. R. Chen, and H. Al-Hamadi, "Reliability of Autonomous Internet of Things Systems with Intrusion Detection Attack-Defense Game Design," IEEE Transactions on Reliability, vol. 70, no. 1, pp. 188–199, Mar. 2021, doi: 10.1109/TR.2020.2983610.

[10] S. Rani and N. Singh Gill, "HYBRID MODEL FOR TWITTER DATA SENTIMENT ANALYSIS BASED ON ENSEMBLE OF DICTIONARY BASED CLASSIFIER AND STACKED MACHINE LEARNING CLASSIFIERS-SVM, KNN AND C5.0," Journal of Theoretical and Applied Information Technology, vol. 29, p. 4, 2020, Accessed: Jan. 19, 2022. [Online]. Available: www.jatit.org

[11] N. S. G. Sangeeta Rani, "Hybrid Model using Stack-Based Ensemble Classifier and Dictionary Classifier to Improve Classification Accuracy of Twitter Sentiment Analysis," International Journal of Emerging Trends in Engineering Research, vol. 8, no. 7, 2020.

[12] P. Gulia and N. Singh Gill, "Comprehensive Analysis of Flow Incorporated Neural Network based Lightweight Video Compression Architecture," IJACSA) International Journal of Advanced Computer Science and Applications, vol. 12, no. 3, 2021, Accessed: Jan. 19, 2022. [Online]. Available: www.ijacsa.thesai.org

[13] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism against IoT DDoS Attacks," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9552–9562, Oct. 2020, doi: 10.1109/JIOT.2020.2993782.

[14] T. Zhi, Y. Liu, and J. Wu, "A Reputation Value-Based Early Detection Mechanism against the Consumer-Provider Collusive Attack in Information-Centric IoT," IEEE Access, vol. 8, pp. 38262–38275, 2020, doi: 10.1109/ACCESS.2020.2976141.

[15] H. Al-Hamadi, I. R. Chen, D. C. Wang, and M. Almashan, "Attack and defense strategies for intrusion detection in autonomous distributed IoT systems," IEEE Access, vol. 8, pp. 168994–169009, 2020, doi: 10.1109/ACCESS.2020.3023616.

[16] S. Patranabis et al., "Lightweight Design-for-Security Strategies for Combined Countermeasures Against Side Channel and Fault Analysis in IoT Applications," Journal of Hardware and Systems Security, vol. 3, no. 2, pp. 103–131, Jun. 2019, doi: 10.1007/s41635-018-0049-y.

[17] A. Sagu, N. Singh, G., and P. Gulia, "Artificial Neural Network for the Internet of Things Security," International Journal of Engineering Trends and Technology, vol. 68, pp. 137–144, 2020, doi: 10.14445/22315381/IJETT-V68I11P218.

[18] N. S. G. Sagu Amit, "Machine Learning Decision Tree Classifier and Logistics Regression Model," International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, no. 1.4, pp. 163–166, Sep. 2020, doi: 10.30534/ijatcse/2020/2491.42020.

[19] N. S. G. Sangeeta, "Framework for Tweet Sentiment Classification Using Boostingbased Ensemble Approach," CIENCIA E TECNICA.VITIVINICOLAA SCIENCE AND TECHNOLOGY JOURNAL (ISSN: 2416-3953), pp. 1–13, 2017.

[20] S. Rani, N. S. Gill, and P. Gulia, "Analyzing impact of number of features on efficiency of hybrid model of lexicon and stack based ensemble classifier for twitter sentiment analysis using WEKA tool," Indonesian Journal of Electrical Engineering and Computer Science, vol. 22, no. 2, pp. 1041–1051, May 2021, doi: 10.11591/IJEECS.V22.I2.PP1041-1051.

[21] P. Gulia, "Performance Analysis of Advancements in Video Compression with Deep Learning," International Journal of Electrical Engineering and Technology, vol. 11, no. 5, pp. 137–143, 2020, doi: 10.34218/IJEET.11.5.2020.016.

[22] M. Zaminkar and R. Fotohi, "SoS-RPL: Securing Internet of Things Against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism," Wireless Personal Communications, vol. 114, no. 2, pp. 1287–1312, Sep. 2020, doi: 10.1007/s11277-020-07421-z.

[23] M. M. Beno, V. I. R, S. S. M, and B. R. Rajakumar, "Threshold prediction for segmenting tumour from brain MRI scans," International Journal of Imaging Systems and Technology, vol. 24, no. 2, pp. 129–137, 2014, doi: 10.1002/ima.22087.

[24] R. Marimuthu and B. Chakraborty, "An Approach for Speech Enhancement Using Deep Convolutional Neural Network," 2019.

[25] A. Sarkar, "Optimization Assisted Convolutional Neural Network for Facial Emotion Recognition."

[26] Ganeshan R, "Skin Cancer Detection with Optimized Neural Network via Hybrid Algorithm."

[27] Vinolin V and Vinusha S, "Resbee Publishers Journal of Computational Mechanics, Power System and Control Enhancement in Biodiesel Blend with the Aid of Neural Network and SAPSO," 2018.

[28] J. Bhasha Shaik, "Resbee Publishers Journal of Computational Mechanics, Power System and Control Deep Neural Network and Social Ski-Driver Optimization Algorithm for Power System Restoration with VSC-HVDC Technology."

[29] Bhagyalakshmi V, DrRamchandra, and DrGeeta D, "Resbee Publishers Journal of Networking and Communication Systems Arrhythmia Classification Using Cat Swarm Optimization Based Support Vector Neural Network."

[30] S. B. Chandanapalli, S. Reddy, and R. Lakshmi, "Resbee Publishers Journal of Networking and Communication Systems Convolutional Neural Network for Water Quality Prediction in WSN," 2019.

[31] N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3559–3570, Apr. 2020, doi: 10.1109/JIOT.2020.2973176.

[32] J. Yoon, "Deep-learning approach to attack handling of IoT devices using IoT-enabled network services," Internet of Things (Netherlands), vol. 11, Sep. 2020, doi: 10.1016/j.iot.2020.100241.

[33] J. Bhayo, S. Hameed, and S. A. Shah, "An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)," IEEE Access, 2020, doi: 10.1109/ACCESS.2020.3043082.

[34] D. Li, Z. Cai, L. Deng, X. Yao, and H. H. Wang, "Information security model of block chain based on intrusion sensing in the IoT environment," Cluster Computing, vol. 22, pp. 451–468, Jan. 2019, doi: 10.1007/s10586-018-2516-1.

[35] J. Roldán, J. Boubeta-Puig, J. Luis Martínez, and G. Ortiz, "Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks," Expert Systems with Applications, vol. 149, Jul. 2020, doi: 10.1016/j.eswa.2020.113251.

[36] M. V. O. de Assis, L. F. Carvalho, J. J. P. C. Rodrigues, J. Lloret, and M. L. Proença, "Near real-time security system applied to SDN environments in IoT networks using convolutional neural network," Computers and Electrical Engineering, vol. 86, Sep. 2020, doi: 10.1016/j.compeleceng.2020.106738.

[37] K. Mabodi, M. Yusefi, S. Zandiyan, L. Irankhah, and R. Fotohi, "Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication," Journal of Supercomputing, vol. 76, no. 9, pp. 7081–7106, Sep. 2020, doi: 10.1007/s11227-019-03137-5.

[38] S. Huang, C. Lin, K. Zhou, Y. Yao, H. Lu, and F. Zhu, "Identifying physical-layer attacks for IoT security: An automatic modulation classification approach using multi-module fusion neural network," Physical Communication, vol. 43, Dec. 2020, doi: 10.1016/j.phycom.2020.101180.

[39] H. Mohammed, S. R. Hasan, and F. Awwad, "Fusion-on-field security and privacy preservation for IoT edge devices: Concurrent defense against multiple types of hardware trojan attacks," IEEE Access, vol. 8, pp. 36847–36862, 2020, doi: 10.1109/ACCESS.2020.2975016.

[40] R. Sahay, G. Geethakumari, and B. Mitra, "A novel blockchain based framework to secure IoT-LLNs against routing attacks," Computing, vol. 102, no. 11, pp. 2445–2470, Nov. 2020, doi: 10.1007/s00607-020-00823-8.

[41] S. A. Alabady, F. Al-Turjman, and S. Din, "A Novel Security Model for Cooperative Virtual Networks in the IoT Era," International Journal of Parallel Programming, vol. 48, no. 2, pp. 280–295, Apr. 2020, doi: 10.1007/s10766-018-0580-z.

[42] E. Avci, "A new intelligent diagnosis system for the heart valve diseases by using genetic-SVM classifier," Expert Systems with Applications, vol. 36, no. 7, pp. 10618–10626, Sep. 2009, doi: 10.1016/j.eswa.2009.02.053.

[43] Y. LeCun, K. Kavukcuoglu, and C. Farabet, "Convolutional networks and applications in vision," in ISCAS 2010 - 2010 IEEE International Symposium on Circuits and Systems: Nano-Bio Circuit Fabrics and Systems, 2010, pp. 253–256. doi: 10.1109/ISCAS.2010.5537907.

[44] H. Z. Wang, G. B. Wang, G. Q. Li, J. C. Peng, and Y. T. Liu, "Deep belief network based deterministic and probabilistic wind speed forecasting approach," Applied Energy, vol. 182, pp. 80–93, Nov. 2016, doi: 10.1016/j.apenergy.2016.08.108.

[45] M. A. Elhosseini, R. A. el Sehiemy, Y. I. Rashwan, and X. Z. Gao, "On the performance improvement of elephant herding optimization algorithm," Knowledge-Based Systems, vol. 166, pp. 58–70, Feb. 2019, doi: 10.1016/j.knosys.2018.12.012.

[46] G. Dhiman and V. Kumar, "Seagull optimization algorithm: Theory and its applications for large-scale industrial engineering problems," Knowledge-Based Systems, vol. 165, pp. 169–196, Feb. 2019, doi: 10.1016/j.knosys.2018.11.024.