ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20230414000533
Original scientific paper

Barnacles Mating Optimizer with Hopfield Neural Network Based Intrusion Detection in Internet of Things Environment

Rajakani VELUMANI, Vinoth Kumar KALIMUTHU*

Abstract: Owing to the development and expansion of energy-aware sensing devices and autonomous and intelligent systems, the Internet of Things (IoT) has gained remarkable growth and found uses in several day-to-day applications. Currently, the Internet of Things (IoT) network is gradually developing ubiquitous connectivity amongst distinct new applications namely smart homes, smart grids, smart cities, and several others. The developing network of smart devices and objects allows people to make smart decisions with machine to machine (M2M) communications. One of the real-world security and IoT-related challenges was vulnerable to distinct attacks which poses several security and privacy challenges. Thus, an IoT provides effective and efficient solutions. An Intrusion Detection System (IDS) is a solution for addressing security and privacy challenges with identifying distinct IoT attacks. This study develops a new Barnacles Mating Optimizer with Hopfield Neural Network based Intrusion Detection (BMOHNN-ID) in IoT environment. The presented BMOHNN-ID technique majorly concentrates on the detection and classification of intrusions from IoT environments. In order to attain this, the BMOHNN-ID technique primarily pre-processes the input data for transforming it into a compatible format. Next, the HNN model was employed for the effectual recognition and classification of intrusions from IoT environments. Moreover, the BMO technique was exploited to optimally modify the parameters related to the HNN model. When a list of possible susceptibilities of every device is ordered, every device is profiled utilizing data related to every device. It comprises routing data, the reported hostname, network flow, and topology. This data was offered to the external modules for digesting the data via REST API model. The experimental values assured that the BMOHNN-ID model has gained effectual intrusion classification performance over the other models.

Keywords: barnacles mating optimizer; Hopfield neural network; internet of things; intrusion detection; REST API; security

1 INTRODUCTION

Recently, more than 25 billion gadgets have been linked to the Internet globally. The Internet of Things (IoT) depends on interlinked smart gadgets, and various services employed for integrating them into one network [1, 2]. This lets the smart gadgets for collecting delicate information and important operations taking place, and such gadgets communicate and connect with one another at maximum velocity and make choices in accordance with indicators data. The IoT network employs cloud service as a back-end to procedure information and retains remote controls [3]. Users utilize web services or mobile applications to make data accessibility by adjusting their gadgets. The IoT structure employs many sensors to eliminate essential data, and it can be scrutinized by artificial intelligence (AI) methods [4]. An intrusion detection system (IDS) is an administrative methodological, and regulatory means employed to prevent unofficial use, misuse, and retrieval of electronic data and transmission mechanisms and the data they contain, focused on assuring the continuity and accessibility of works of the information method and fostering the privacy, protection, and secrecy of private data by some initiatives [5].

Cyber security means the practice of protecting electronic methods, computers, mobile devices, servers, networks, and data from malicious assaults. It is otherwise called information technology security [6]. Such intrusions include domain of research control mechanism by monitoring a change of the document mechanism, accessing sensitive records, making unapproved logins, using malware, and heightening advantages that can change the network conditions. Network intrusions happen because of approaching packets in the network for performing conducts, like denial of service (DoS) assaults or tries that separate as the mechanism [7]. DoS assaults were tried to make PC properties distant by its planned users, for instance, flood attacks, land assaults, and ping of death (POD). Intrusion indications include abnormal results at executing various client charges illustrated by moderate mechanism implementation, and sudden mechanism smashes and variations in fragments of data structure were bizarrely, moderate mechanism implementation (i.e., accessing sites or opening records).

AI is a type of data-driven technique where the initial level was to comprehend the data [8-10]. Several kinds of data indicate particular attack conducts which include network activities and host behaviours. Network traffic indicates network behaviours and server logs reflect host behaviour. There were numerous kinds of assaults, with each containing a specific paradigm [11]. Thus, it becomes significant for selecting appropriate data sources for detecting several assaults according to the threat features. One vital feature of a DoS assault, for instance, was to transmit numerous packets in a very limited period; therefore, flow data were ideal for DoS attack identification [12]. A hidden channel has a data leaking function amongst 2 distinct IP addresses and is optimally suitable for session data recognition. Thus, the development of DL methods is helpful in detecting such network behaviours [13].

Several research works have devised the progression of network security systems, and AI serves the main part in cyber security areas related to IoT to design an intellectual mechanism for security in the IoT network. Existing research notes that deep learning (DL) approaches can detect IoT assaults more efficiently compared to conventional ML techniques However, only the cloud layer has the resources for running such techniques. Moreover, such approaches are not continuously active in certain situations, such as remote live functioning, as the mechanism is supposed to constitute realistic decisions quickly.

2 RELATED WORKS

Malibari et al. [14] present a new meta-heuristic (MH) with DL-assisted intrusion detection (ID) mechanism for secured smart atmosphere, termed MDLIDS-SSE approach. The main aim of the MDLIDS-SSE algorithm

was to detect the presence of intrusion in the secured smart settings. Moreover, for electing an optimum feature subset, the MDLIDS-SSE method allows improved arithmetic optimization algorithm related FS (IAOA-FS) approach. Further, quantum behaved PSO (QPSO) together with deep wavelet NN (DWNN) method can be useful in the classification and detection of intrusion in the secured smart setting. Dahou et al. [15] introduce a new structure for improvising IDS performance related to the data gathered from the IoT networks. The formulated structure depends upon DL and MH optimization techniques for executing FS and feature extraction. A simpler one but potential CNN can be applied as the core feature extractors of this structure with a view to studying better and highly appropriate representation of input in a low-dimension space. A new FS system can be formulated related to lately projected MH technique; termed Reptile Search Algorithm (RSA) is enthused by the crocodiles' hunting activities.

Elmasry et al. [16] modelled a double PSO related technique in order to choose feature subsets as well as hyperparameters in a single procedure. The above-mentioned mechanism can be used in the pretraining stage to choose the model's hyperparameters and optimize features automatically. Kareem et al. [17] propose a novel FS technique via fostering the act of Gorilla Troops Optimizer (GTO) related to the method for bird swarms (BSA). The BSA is helpful in fostering GTO performance exploitations in the recently advanced GTO-BSA since it has a strong capability in finding possible regions having optimum solutions. Fatani et al. [18] project an effectual AI-oriented system for IDS in IoT systems. The author makes use of the advances of DL and MHs methods that approved its potentiality in resolving complicated engineering complexities. The author presents a feature extracting algorithm utilizing the CNNs for the purpose of extraction of appropriate features. Likewise, the author formulates an innovative FS algorithm utilizing a novel different of transient search optimization (TSO) technique, termed TSODE, employing the operator of differential evolution (DE) method.

Kumar [19] devises a Hybrid Meta heuristic Optimization related Feature Subset Selection (HMOFS) having an Optimal Wavelet KELM (OWKELM) related Classifier methodology termed HMOFS-OWKELM algorithm for IDS in big data atmosphere. The presented HMOFS-OWKELM method includes pre-processing for removing the unnecessary noise that occurs in it. Additionally, the HMOFS involves the Hybridizing hill Climbing (HC) related FS procedure and moth flame optimization (MFO). The HC idea was to incorporate the MFO technique for enhancing the convergence rates. In [20], an MH association scale can be devised for extracting threshold values for the transaction and ensemble classifications can be employed for analyzing the transaction as attack or normal. In the presented mechanism Ensemble classifier was utilized depending on drift identification having the capability for examining the requests at stream levels. The presented methodology extracts the features from the stream level and employs drift detection for scrutinizing the stream features.

This study develops a new Barnacles Mating Optimizer with Hopfield Neural Network based Intrusion Detection (BMOHNN-ID) in IoT environment. The presented BMOHNN-ID technique primarily pre-processes the input data to change it as a compatible format. Next, the HNN model was leveraged for the effectual recognition and classification of intrusions from the IoT environment.

3 THE PROPOSED MODEL

In this study, an automated BMOHNN-ID system was developed for the detection and classification of intrusions from IoT environments. At the initial level, the BMOHNN-ID technique primarily pre-processes the input data for transforming it into a compatible format. Next, the HNN model can be utilized for the effectual recognition and classification of intrusions from IoT environments. Moreover, the BMO approach was exploited to optimally modify the parameters related to the HNN model.

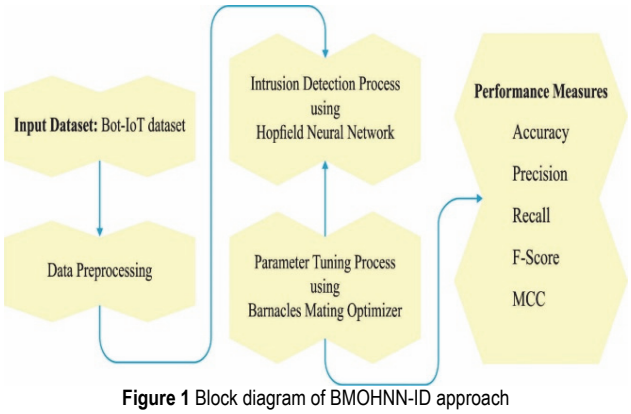

Figure 1 Block diagram of BMOHNN-ID approach

Fig. 1 demonstrates the block diagram of BMOHNN-ID approach.

3.1 Network Profiling

The performance of the Network Profiling (NP) module can be classified into two main characteristics, first is the utility to mechanically scan linked gadgets on the locally accessible networks for currently running services and potential common vulnerabilities. The data which is vulnerable is sourced mainly in a regularly upgraded listing in the open-source CVE Mitre databases [21]. Those vulnerabilities were mapped to accessible network services that are discovered sequentially via network port scanning systems like those given by Nmap. When the lists of potential vulnerabilities of every gadget was compiled, all the devices are profiled utilizing data related to the device and it takes account of the reported hostname, routing information, topology, and network flow; then these data are delivered to external component for digesting those data via a REST API.

The next is NP service which is able to compute bound Npconducts; this can be computed by continuous monitoring of network traffic flow from every gadget over the networks. It utilizes rate informed heuristic profiling to construct an anticipated throughput paradigm for all the devices on the LAN which it is interconnected to. Then, this profile was compared with 3 distinct predetermined profiles. One is Weekly Profile (W) - A NP can be informed by a packet capture viz., refreshed weekly. Another one is Hourly Profile (H) - A NP can be intimated by a packet capture viz. refreshed hourly. Lastly, Daily Profile (D) - A NP can be intimated by a packet capture

viz., refreshed daily. The aim of utilizing distinct profiles detached and refreshed by period was to offer a precise map of the network condition that a device would undergo over time. It rises accurateness of the profile and makes the system adapt better to varied device usage and variable network conditions.

3.2 Data Pre-Processing

At this stage, the BMOHNN-ID technique primarily pre-processes the input data to transform it into a compatible format. A huge gap amongst distinct dimensional feature data in the dataset is accomplished and there are issues like slow model trained and insignificant accuracy enhancement; so, to challenge this problem, the Min Max Scaler is implemented for mapping the data as range of zero and one as follows:

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{1}$$

whereas $x_{\max}$ represents the maximal value, and $x_{\min}$ signifies the minimal value.

3.3 Intrusion Detection using HNN Model

In this study, the HNN method was utilized for the effectual recognition and classification of intrusions in the IoT environment. The model infrastructure of HNN has connected neurons and powerful features of content addressable memory which is vital from resolving several optimization and combinatorial tasks [22]. The HNN approach structure includes organized neurons, each one of which is demonstrated by variable recognized as Using variable. In bipolar detection, the neurons from discrete HNN are utilized; 1 is implemented for representing the true state, and their falsification is defined by 1. The basic analysis of neuron state activation from HNN is represented in Eq. (2).

$$S_i = \begin{cases} 1, & \text{if} \quad \sum_j W_{ij} S_i > \psi, \\ -1, & \text{Otherwise} \end{cases} \tag{2}$$

whereas W_{ij} refers the synaptic weighted vector of HNN-RANkSAT deriving from neuron j to neuron i. S_i is demonstrated as the state of neurons i from HNN, and ψ is the existing values. The value $\psi = 0$ is to verify that the network's energy reduces to 0. The synaptic weighted connection from discrete HNN has no link with itself, and the synaptic linked in one neuron to other neurons is 0 that is, $W_{iii} = W_{jjj} = W_{kkk}$ and $W_{ii} = W_{jj} = W_{kk}$. Accordingly, HNN has symmetrical features with respect to structure. The HNN technique has the same intricate facts as that used in the method of magnetism. In bipolar expression, as the neuron state is named as spin points execute the magnetic field trajectory. All the neurons are compelled to flip still it obtains a stable equilibrium state according to Eq. (3).

$$S_i \to \text{sgn}\,[h_i(t)] \tag{3}$$

The local field vector which links every neuron from HNN is determined as h_i. The sum of fields is caused by all the neuron states as follows:

$$h_i = \sum_k^N \sum_j^N W_{ijk} S_j S_k + \sum_j^N W_{ij} S_j + W_i \tag{4}$$

The task of local fields is for evaluating the last state of neurons and creates every feasible 3SAT induced logic achieved in the last state of neurons. The most prominent feature of HNN networks is the detail that it continuously converges. The generalized fitness function, $E_{F_{\text{RANkSAT}}}$, **controls** the integration of neurons from HNN. $E_{F_{\text{RANkSAT}}}$ is offered as follows:

$$E_{F_{\text{RANkSAT}}} = \sum_{i=1}^{NN} \prod_{j=1}^{V} T_{ijk} \tag{5}$$

In which V and NN imply the number of variables and neurons created from F_{RANkSAT} correspondingly. The inconsistency of F_{RANkSAT} demonstration as:

$$T_{ij} = \begin{cases} \frac{1}{2}(1 - S_\rho)\,, if \neg\rho \\ \frac{1}{2}(1 + S_\rho)\,, \text{otherwise} \end{cases} \tag{6}$$

The value F_{RANkSAT} is proportional to value of inconsistencies in the logical clauses. The rule for upgrading the neural condition is

$$S_i(t+1) = \begin{cases} 1, & h_i = \sum_K^N \sum_J^N W_{ijk} S_j S_k + \sum_J^N W_{ij} S_j + W_i \geq 0 \\ -1, & h_i = \sum_K^N \sum_J^N W_{ijk} S_j S_k + \sum_J^N W_{ij} S_j + W_i < 0 \end{cases} \tag{7}$$

Eq. (8) defines the Lyapunov energy function from the HNN.

$$H_{\text{FRINNAT}} = -\frac{1}{3} \sum_{i=1, i\neq j, j\neq kj=1}^{N} , \sum_{i\neq j, j\neq ik=1}^{N} , \sum_{i\neq j, k\neq i}^{N} W_{ijk} S_i S_j S_k - \frac{1}{2} \sum_{i=1, i\neq jj=1 i\neq j}^{N} \sum^{N} W_{ij} S_i S_j - \sum_{i=1}^{N} W_i S_i \tag{8}$$

Eq. (9) has utilized for classifying if the solution obtains global/local minimal energy. HNN creates the optimum allocation if the induced neuron state obtains global minimal energy. Restricted analyses are integrated HNN and ACO as a single computational network. Therefore, the robustness of ACO enhances the trained procedure from HNN. Accordingly, the quality of last neuronal condition is retained in Eq. (9).

$$\left| H_{F_{\text{RANkSAT}}} - H^{\min}_{F_{\text{RANkSAT}}} \right| \leq \xi \tag{9}$$

whereas ξ represents a certain tolerance value. The value ξ = 0.001. If the F_{RANkSAT} logical representation embedding from HNN does not fulfill the conditions in Eq. (9), after that the neurons are surrounded in the wrong pattern from the last state.

3.4 Parameter Tuning using BMO Algorithm

To optimally modify the parameters related to the HNN model, the BMO algorithm is exploited in this study. Sulaiman et al. [23] proposed a BMO technique which is a novel evolutionary algorithm that is stimulated from the property of barnacles called micro-organisms that have female and male reproduction. They symbolize the solution in BMO that resembles a chromosome in GA and a particle in PSO. Barnacles are reproduced by sperm mating and natural intercourse. Through random movement, they search for a partner and later release the sperm into cavity of the partner mantle. In contrast, once the sperm is released into the seawater where fertilizing the barnacle eggs, sperm mating is taking place. The BMA optimization method has 3 major phases.

1) Initialization: Similar to other optimization techniques, the initialization processes characterize the initial step in BMO, whereby the early population can be generated in a random manner. The early population is denoted as a matrix of decision parameters as follows.

$$X = \begin{bmatrix} x_1^1 & x_1^2 & \cdots & x_1^N \\ x_2^1 & x_2^2 & \cdots & x_2^N \\ \vdots & \vdots & \ddots & \vdots \\ x_n^1 & x_n^2 & \cdots & x_n^N \end{bmatrix} \tag{10}$$

In Eq. (10), n signifies the population count and N describes the amount of decision variables. Such parameters must be integrated with lower and upper limits of the issue to be resolved in the following:

$$lb = [lb_1, lb_2, lb_3, ..., lb_i] \tag{11}$$

$$ub = [ub_1, ub_2, ub_3, ..., ub_i] \tag{12}$$

From the equation, lb and ub denote the lower and upper bounds of i^{th} parameter. Here, every barnacle in the early population is calculated by objective function and later sorting method can take place for setting the optimal solution at top of solution matrix [24].

2) Choice process: According to the length of barnacle penises, p_1, the selection method of two barnacles can be executed in a random fashion and it is based on the succeeding features:

The selection was a random procedure constrained to the distance of barnacle penis.

Every individual provides or receives its sperm to or from other barnacles. But every individual barnacle would be fertilized once by only one individual.

Once a similar barnacle can be chosen at a particular point (self-mating), this won't be considered in this work, and won't release new offspring generation.

In a specific iteration, once the choice can be greater than determined p_1, the sperm casting would take place. The abovementioned factor explains that BMO technique includes exploration and exploitation stages. The offspring generation is continuous over the procedure of sperm cast being a term for exploration and the mathematical expression is given below that shows that the choice was randomly made, and later the initial assumption was accomplished.

$$b_{\text{D}} = \text{rand}(n) \tag{13}$$

$$b_{\text{M}} = \text{rand}(n) \tag{14}$$

Now b_{D} and b_{M} describes the mated parent.

3) Reproduction process: Simultaneously, no analytical method was introduced for the reproduction of barnacles, the BMO approach focuses on paying attention towards the features of genotype or the inheritance frequencies of parent in producing off-spring based on the concept of Hardy-Weinberg and every new off-spring is attained as follows:

$$X_i^{N\text{New}} = pX_{b_{\text{D}}}^N + qX_{b_{\text{M}}}^N \tag{15}$$

In Eq. (15), P represents a pseudo-random usually distributed with [0, 1], $q = (1-p)$, and $X_{b_{\text{D}}}^N$ and $X_{b_{\text{M}}}^N$ denotes the parameter of individual Dad and Mum correspondingly.

Sperm casting takes place once choice of barnacles being mated exceeds the value of p_1, that is firstly set as follows.

$$X_i^{N\text{New}} = \text{rand} * X_{b_{\text{M}}}^n \tag{16}$$

In Eq. (16), rand denotes a random integer within [0, 1]. The new off-spring for the exploration process is produced through the individual Mum. Fig. 2 depicts the flowchart of BMO technique.

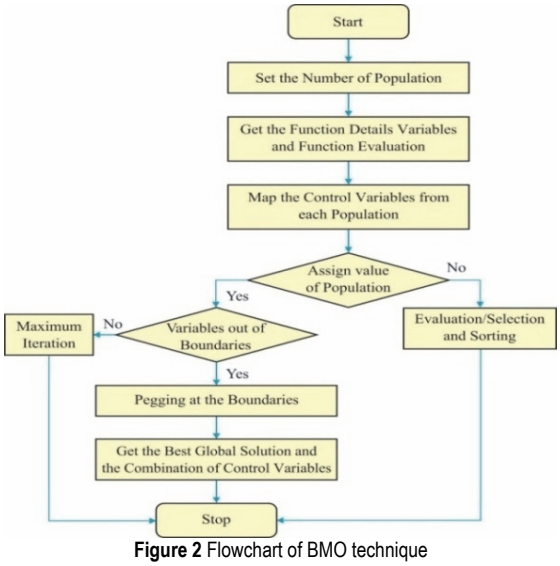

Figure 2 Flowchart of BMO technique

The offspring was estimated and merged with parent to handle solution matrix expansion from the single dimension. As a result, the arranging procedure is done to choose the fifty percent top solution that fits the population size and the undesirable outcomes get removed. Algorithm 1 determines the pseudo code of BMO technique.

Algorithm l: Pseudo code of BMO approach
Input: Max Iter, N, pl, 1, u, i: counter
Output: The optimal barnacles (solution).
Produce an early population, X.
Evaluate every barnacle fitness through the fitness function.
Sort barnacle fitness and set the optimal one in the top (P).
While t < MaxIter do
Carry out the choice method based on Eqs. (13) and (14).
If the designated Dad and Mum $\leq p_1$ then
For every parameter do
Produce the offspring based on Eq. (15)
End for
Else
For every parameter do
Produce the offspring based on Eq. (16)
End for
End if
Restore the barnacle once it violated the limit.
Evaluate the fitness of every barnacle individual
Sort barnacle fitness and upgrade P if is better.
$i = i + 1$
End while
Return P

In this study, the BMO algorithm computes a fitness function with the minimization of classification error rate. The fitness function derived by the BMO algorithm is determined as follows:

$$fitness\ function = classification\ error\ rate = \frac{number\ of\ misclassified\ samples}{Total\ number\ of\ samples} * 100 \quad (17)$$

4 RESULTS AND DISCUSSION

This section inspects the intrusion detection outcomes of the BMOHNN-ID model using the BoT-IoT dataset [25]. It includes 10000 samples with distinct class labels as depicted in Tab. 1. The results are inspected in terms of binary classification and multi-class classification.

Table 1 Dataset details

Class	Sub-Category	No. of Records
Normal		2000
Attack	Reconnaissance	2000
	DoS	2000
	DDoS	2000
	Information theft	2000
Total Number of Attacks		10000

With entire dataset, the BMOHNN-ID model has identified 1901 samples into normal and 7953 samples into attack. In addition, with 70% of TR data, the BMOHNN-ID technique has identified 1323 samples into normal and 5572 samples into attack. Besides, with 30% of TS data, the BMOHNN-ID algorithm has identified 578 samples into normal and 2381 samples into attack.

Tab. 2 and Fig. 3 portray the classification outcomes of the BMOHNN-ID model on binary classification. The results implied that the BMOHNN-ID model has offered improved results under each aspect. For instance, on entire dataset, the BMOHNN-ID model has obtained average $accu_y$, $prec_n$, $reca_l$, F_{score}, and MCC of 98.54%, 98.18%, 97.23%, 97.70%, and 95.41% respectively. Meanwhile, on 70% of TR data, the BMOHNN-ID approach has gained average $accu_y$, $prec_n$, $reca_l$, F_{score}, and MCC of 98.50%, 98.12%, 97153%, 97.62%, and 95.26% correspondingly. Eventually, on 30% of TS data, the BMOHNN-ID methodology has achieved average $accu_y$, $prec_n$, $reca_l$, F_{score}, and MCC of 98.63%, 98.32%, 97.42%, 97.86%, and 95.73% correspondingly.

Table 2 Result analysis of BMOHNN-ID approach with distinct measures under binary class

Binary Class					
Labels	***Accuracy***	***Precision***	***Recall***	***F-Score***	***MCC***
Entire Dataset					
Normal	98.54	97.59	95.05	96.30	95.41
Attack	98.54	98.77	99.41	99.09	95.41
Average	98.54	98.18	97.23	97.70	95.41
Training Phase (70%)					
Normal	98.50	97.49	94.91	96.18	95.26
Attack	98.50	98.74	99.39	99.07	95.26
Average	98.50	98.12	97.15	97.62	95.26
Testing Phase (30%)					
Normal	98.63	97.80	95.38	96.57	95.73
Attack	98.63	98.84	99.46	99.15	95.73
Average	98.63	98.32	97.42	97.86	95.73

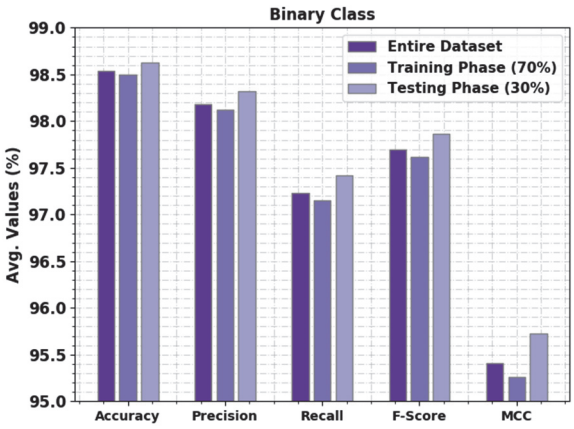

Figure 3 Average analysis of BMOHNN-ID approach under binary class

Figure 4 TRA and VLA analysis of BMOHNN-ID approach under binary class

The training accuracy (TRA) and validation accuracy (VLA) acquired by the BMOHNN-ID algorithm on binary class is shown in Fig. 4. The experimental outcome denoted the BMOHNN-ID technique has attained maximal values of TRA and VLA. Seemingly the VLA is greater than TRA.

The training loss (TRL) and validation loss (VLL) obtained by the BMOHNN-ID methodology on binary class are displayed in Fig. 5. The experimental outcome indicates that the BMOHNN-ID approach has exhibited minimal values of TRL and VLL. Evidently, the VLL is lesser than TRL.

Figure 5 TRL and VLL analysis of BMOHNN-ID approach under binary class

With entire dataset, the BMOHNN-ID technique has identified 1909 samples into normal, 1972 samples into reconnaissance, 1966 samples into DoS, 1972 samples into normal, and 1953 samples into attack. Moreover, with 70% of TR data, the BMOHNN-ID technique has identified 1348 samples into normal, 1399 samples into reconnaissance, 1358 samples into DoS, 1379 samples into normal, and 1361 samples into attack. Further, with 30% of TS data, the BMOHNN-ID approach has identified 561 samples into normal, 573 samples into reconnaissance, 608 samples into DoS, 593 samples into normal, and 592 samples into attack.

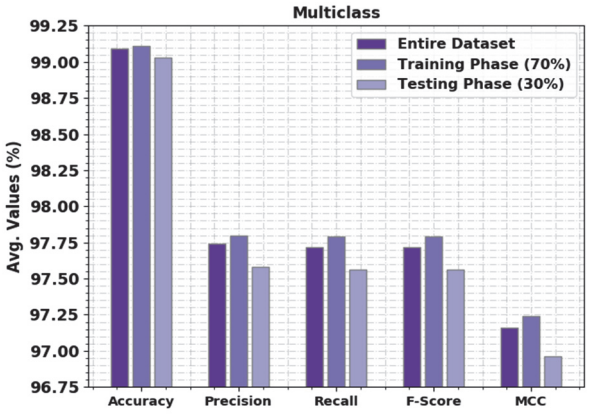

Figure 7 Average analysis of BMOHNN-ID approach under multiclass

Tab. 3 and Fig. 7 describe the classification outcomes of the BMOHNN-ID methodology on Multiclass. The results represented the BMOHNN-ID approach has rendered enhanced results under each aspect. For example, on entire dataset, the BMOHNN-ID algorithm has acquired average $accu_y$, $prec_n$, $reca_1$, F_{score}, and *MCC* of 99.09%, 97.74%, 97.72%, 97.72%, and 97.16% correspondingly. In the meantime, on 70% of TR data, the BMOHNN-ID technique has reached average $accu_y$, $prec_n$, $reca_1$, F_{score}, and *MCC* of 99.11%, 97.80%, 97.79%, 97.79%, and 97.24% correspondingly. Similarly, on 30% of TS data, the BMOHNN-ID technique has reached average $accu_y$, $prec_n$, $reca_1$, F_{score}, and *MCC* of 99.03%, 97.58%, 97.56%, 97.56%, and 96.96% correspondingly.

Table 3 Result analysis of BMOHNN-ID approach with distinct measures under multiclass

Multiclass					
Labels	***Accuracy***	***Precision***	***Recall***	***F-Score***	***MCC***
Entire Dataset					
Normal	98.74	98.20	95.45	96.81	96.04
Reconnaissance	99.23	97.58	98.60	98.09	97.61
DoS	99.42	98.79	98.30	98.55	98.18
DDoS	99.49	98.85	98.60	98.72	98.40
Information theft	98.56	95.27	97.65	96.44	95.55
Average	99.09	97.74	97.72	97.72	97.16
Training Phase (70%)					
Normal	98.76	98.11	95.67	96.87	96.11
Reconnaissance	99.33	97.90	98.80	98.35	97.93
DoS	99.41	98.84	98.19	98.51	98.15
DDoS	99.50	99.07	98.43	98.75	98.44
Information theft	98.57	95.11	97.84	96.46	95.58
Average	99.11	97.80	97.79	97.79	97.24
Testing Phase (30%)					
Normal	98.70	98.42	94.92	96.64	95.86
Reconnaissance	99.00	96.79	98.12	97.45	96.83
DoS	99.43	98.70	98.54	98.62	98.26
DDoS	99.47	98.34	99.00	98.67	98.34
Information theft	98.53	95.64	97.21	96.42	95.50
Average	99.03	97.58	97.56	97.56	96.96

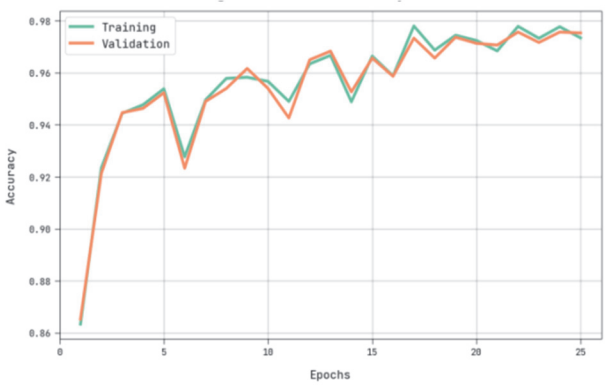

Figure 8 TRA and VLA analysis of BMOHNN-ID approach under multiclass dataset

The TRA and VLA reached by the BMOHNN-ID methodology on multiclass dataset are shown in Fig. 8. The experimental outcome denoted that the BMOHNN-ID approach has gained maximal values of TRA and VLA. In Particular, the VLA is greater than TRA.

The TRL and VLL gained by the BMOHNN-ID algorithm on multiclass dataset are exhibited in Fig. 10. The experimental outcome indicated that the BMOHNN-ID technique has exhibited least values of TRL and VLL. Specifically, the VLL is lesser than TRL.

A wide range of comparison study of the BMOHNN-ID model with recent models is provided in Tab. 4 and Fig. 10 [26]. The experimental values inferred the enhanced performance of the BMOHNN-ID model over other recent models. Based on $accu_y$, the BMOHNN-ID model has

offered higher $accu_y$ of 99.03% whereas the RNN, LSTM, ensemble, deep DCA, TCNN, and FNN models have obtained lower $accu_y$ of 94.21%, 95.86%, 95.95%, 97.02%, 98.79%, and 94.74% respectively. Meanwhile, based on $prec_n$, the BMOHNN-ID algorithm has rendered higher $prec_n$ of 97.58% whereas the RNN, LSTM, ensemble, deepDCA, TCNN, and FNN techniques have reached lower $prec_n$ of 95.66%, 96.49%, 95.59%, 95.2%, 96.93%, and 96.59% correspondingly.

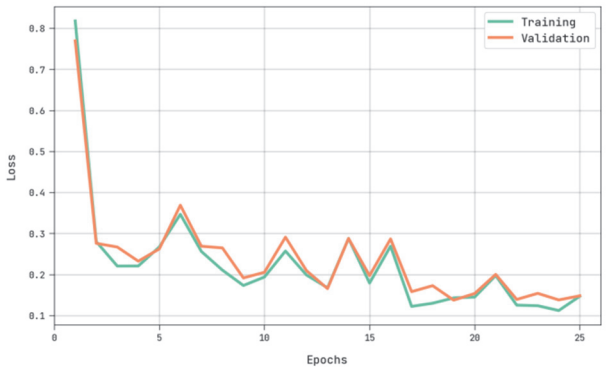

Figure 10 TRL and VLL analysis of BMOHNN-ID approach under multiclass dataset

Table 4 Comparative analysis of BMOHNN-ID approach with existing methodologies

Methods	*Accuracy*	*Precision*	*Recall*	*F-Score*
BMOHNN-ID	99.03	97.58	97.56	97.56
RNN	94.21	95.66	95.82	95.89
LSTM	95.86	96.49	94.47	95.57
Ensemble Model	95.95	95.59	94.93	95.64
DeepDCA	97.02	95.2	96.89	96.53
TCNN	98.79	96.93	97.03	97.18
FNN	94.74	96.59	96.83	96.91

Eventually, based on $reca_l$, the BMOHNN-ID approach has granted higher $reca_l$ of 97.56% whereas the RNN, LSTM, ensemble, deep DCA, TCNN, and FNN methodologies have reached lower $reca_l$ of 95.82%, 94.47%, 94.93%, 96.89%, 97.03%, and 96.83% correspondingly. Therefore, the experimental values assured that the BMOHNN-ID model has gained effectual intrusion classification performance over other models.

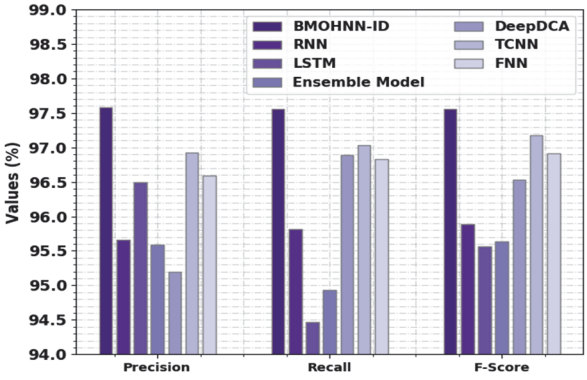

Figure 10 Comparative analysis of BMOHNN-ID approach with existing methodologies

5 CONCLUSION

In this research, an automated BMOHNN-ID algorithm is developed for the detection and classification of intrusions in the IoT environment. At the initial level, the BMOHNN-ID technique primarily pre-processes the input data to transform it into a compatible format. Next, the HNN model is utilized for the effectual recognition and classification of intrusions in the IoT environment. Moreover, the BMO approach is exploited to optimally modify the parameters related to the HNN model. When a list of possible susceptibilities of every device is ordered, every device is profiled utilizing data related to every device. It comprises routing data, the reported host name, network flow, and topology; this information is offered to the external elements for digesting the data via REST API model. To verify the effectual outcomes of the BMOHNN-ID model, a wide-ranging experimental analysis is performed on BoT-IoT dataset. A brief set of comparative studies reported the enhanced performance of the BMOHNN-ID model over other approaches. In future, feature selection process can be integrated to the BMOHNN-ID model to enhance classifier results.

6 REFERENCES

[1] Fatani, A., Abd Elaziz, M., Dahou, A., Al-Qaness, M. A., & Lu, S. (2021). IoT intrusion detection system using deep learning and enhanced transient search optimization. *IEEE Access*, *9*, 123448-123464. https://doi.org/10.1109/access.2021.3109081

[2] Acko, B., Weber, H., Hutzschenreuter, D., & Smith, I. (2020). Communication and validation of metrological smart data in IoT-networks. *Advances in Production Engineering & Management*, *15*(1), 107-117. https://doi.org/10.14743/apem2020.1.353

[3] Moizuddin, M. D. & Jose, M. V. (2022). A bio-inspired hybrid deep learning model for network intrusion detection. *Knowledge-Based Systems*, *238*, 107894. https://doi.org/10.1016/j.knosys.2021.107894

[4] Fatani, A., Dahou, A., Al-Qaness, M. A., Lu, S., & Elaziz, M. A. (2022). Advanced feature extraction and selection approach using deep learning and Aquila optimizer for IoT intrusion detection system. *Sensors*, *22*(1), 140. https://doi.org/10.3390/s22010140

[5] Pandey, J. K., Kumar, S., Lamin, M., Gupta, S., Dubey, R. K., & Sammy, F. (2022). A Metaheuristic Autoencoder Deep Learning Model for Intrusion Detector System. *Mathematical Problems in Engineering*, 1-11. https://doi.org/10.1155/2022/3859155

[6] Rm, B., Mewada, H. K., & Br., R. (2022). Hybrid machine learning approach based intrusion detection in cloud: A metaheuristic assisted model. *Multiagent and Grid Systems*, *18*(1), 21-43. https://doi.org/10.3233/MGS-220360

[7] Sahu, A. & Davis, K. (2022). Inter-Domain Fusion for Enhanced Intrusion Detection in Power Systems: An Evidence Theoretic and Meta-Heuristic Approach. *Sensors*, *22*(6), 2100. https://doi.org/10.3390/s22062100

[8] Balogun, B. F., Gbolagade, K. A., Arowolo, M. O., & Saheed, Y. K. (2021). A Hybrid Metaheuristic Algorithm for Features Dimensionality Reduction in Network Intrusion Detection System. *International Conference on Computational Science and Its Applications, Springer, Cham*, 101-114. https://doi.org/10.1007/978-3-030-87013-3_8

[9] Kavitha, S., Uma Maheswari, N., & Venkatesh, R. (2023). Intelligent Intrusion Detection System using Enhanced Arithmetic Optimization Algorithm with Deep Learning Model. *Tehnicki vjesnik-Technical Gazette*, *30*(4), 1217-1224. https://doi.org/10.17559/TV-20221128071759

[10] Premkumar, M., Sundararajan, T. V. P., & Mohanbabu, G. (2022). Dynamic Defense Mechanism for DoS Attacks in

Wireless Environments Using Hybrid Intrusion Detection System and Statistical Approaches. *Tehnicki vjesnik-Technical Gazette*, *29*(3), 965-970. https://doi.org/10.17559/TV-20210604113859

[11] Saha, A., Chowdhury, C., Jana, M., & Biswas, S. (2021). IoT sensor data analysis and fusion applying machine learning and meta-heuristic approaches. *Enabling AI applications in data science*, 441-469. https://doi.org/10.1007/978-3-030-52067-0_20

[12] Forestiero, A. (2021). Metaheuristic algorithm for anomaly detection in Internet of Things leveraging on a neural-driven multiagent system. *Knowledge-Based Systems*, 228, 107241. https://doi.org/10.1016/j.knosys.2021.10724

[13] Vinoth Kumar, K. & Balaganesh, D. (2022). Efficient Privacy-Preserving Red Deer Optimization Algorithm with Blockchain Technology for Clustered VANET. *Technical Gazette*, *29*(3), 813-817. https://doi.org/10.17559/TV-202112161156350

[14] Malibari, A. A., Alotaibi, S. S., Alshahrani, R., Dhahbi, S., Alabdan, R., Al-wesabi, F. N., & Hilal, A. M. (2022). A novel metaheuristics with deep learning enabled intrusion detection system for secured smart environment. *Sustainable Energy Technologies and Assessments*, *52*, 102312. https://doi.org/10.1016/j.seta.2022.102312

[15] Dahou, A., Abd Elaziz, M., Chelloug, S. A., Awadallah, M. A., Al-Betar, M. A., Al-qaness, M. A., & Forestiero, A. (2022). Intrusion Detection System for IoT Based on Deep Learning and Modified Reptile Search Algorithm. *Computational Intelligence and Neuroscience*, *4*, 1-15. https://doi.org/10.1155/2022/6473507

[16] Elmasry, W., Akbulut, A., & Zaim, A. H. (2020). Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic. *Computer Networks*, *168*, 107042. https://doi.org/10.1016/j.comnet.2019.107042

[17] Kareem, S. S., Mostafa, R. R., Hashim, F. A., & El-Bakry, H. M. (2022). An effective feature selection model using hybrid metaheuristic algorithms for IoT intrusion detection. *Sensors*, *22*(4), 1396. https://doi.org/10.3390/s22041396

[18] Li, Y. & Zhanyong, W. (2022). A Cloud Based Network Intrusion Detection System. *Tehnički vjesnik*, *29*(3), 987-992. https://doi.org/10.17559/TV-20211130024245

[19] Gopinath, S., Vinoth Kumar, K., Elayaraja, P., Parameswari, A., Balakrishnan, S., & Thiruppathi, M. (2021). SCEER: Secure cluster based efficient energy routing scheme for wireless sensor networks. *Materials Today: Proceedings (Elsevier)*, *45*(2), 3579-3584. https://doi.org/10.1016/j.matpr.2020.12.1096

[20] Dasari, D. B., Edamadaka, G., Chowdary, C., & Sobhana, M. (2021). Anomaly-based network intrusion detection with ensemble classifiers and meta-heuristic scale (ECMHS) in traffic flow streams. *Journal of Ambient Intelligence and Humanized Computing*, *12*(10), 9241-9268. https://doi.org/10.1007/s12652-020-02628-1

[21] Vinoth Kumar, K., Jayasankar, T., Eswaramoorthy, V., & Nivedhitha, V. (2020). SDARP: Security based Data Aware Routing Protocol for Ad hoc Sensor Networks. *International Journal of Intelligent Networks (Elsevier-KeAi)*, *1*, 36-42. https://doi.org/10.1016/j.ijin.2020.05.005

[22] Abubakar, H., Muhammad, A., & Bello, S. (2022). Ants colony optimization algorithm in the Hopfield neural network for agricultural soil fertility reverse analysis. *Iraqi Journal for Computer Science and Mathematics*, *3*(1), 32-42. https://doi.org/10.52866/ijcsm.2022.01.01.004

[23] Sulaiman, M. H., Mustaffa, Z., Saari, M. M., & Daniyal, H. (2020). Barnacles mating optimizer: a new bio-inspired algorithm for solving engineering optimization problems. *Engineering Applications of Artificial Intelligence*, *87*, 103330. https://doi.org/10.1016/j.engappai.2019.103330

[24] Selim, A., Kamel, S., Zawbaa, H. M., Khan, B., & Jurado, F. (2022). Optimal allocation of distributed generation with the presence of photovoltaic and battery energy storage system using improved barnacles mating optimizer. *Energy Science & Engineering*, 2970-3000. https://doi.org/10.1002/ese3.1182

[25] Cigdem, B. & Veli, H. (2020). Classifying Database Users for Intrusion Prediction and Detection in Data Security. *Tehnički vjesnik*, *27*(6), 1857-1862. https://doi.org/10.17559/TV-20190710100638

[26] Derhab, A., Aldweesh, A., Emam, A. Z., & Khan, F.A. (2020). Intrusion detection system for internet of things based on temporal convolution neural network and efficient feature engineering. *Wireless Communications and Mobile Computing*, 2020. https://doi.org/10.1155/2020/6689134

Contact information:

Mr. Rajakani VELUMANI, Assistant Professor
Department of Electronics and Communication Engineering,
Anjalai Ammal Mahalingam Engineering College,
Kovilvenni, Tiruvarur-Dist., Tamilnadu, India-614 403
E-mail: rajakani.v@gmail.com

Dr. Vinoth Kumar KALIMUTHU, Professor
(Corresponding author)
Department of Electronics and Communication Engineering,
SSM Institute of Engineering & Technology,
Dindigul, Tamilnadu, India-624 002
E-mail: vinodkumaran87@gmail.com