ISSN 1330-3651(Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20250308002449
Original scientific paper

Gannet Optimization Algorithm with Attention Enhanced Deep Learning for Intrusions Detecting in IoT

V. RAJAKANI, K. VINOTH KUMAR*, A. SRIDEVI, N. PRATHAP

Abstract: As a new paradigm, the Internet of Things (IoT) incorporates the Internet and physical objects belonging to many different areas including human health, home automation, environmental monitoring, and industrial processes. In our daily activities, it deepens the presence of Internet-connected devices bringing, along with various challenges, and benefits related to security problems. Over the years, Intrusion Detection Systems (IDS) have been instrumental in the security of information systems and networks. However, applying classical IDS approaches to IoT is challenging owing to its specific features such as specific protocol stacks, standards, and constrained-resource devices. Deep learning (DL), specifically recurrent methods, is successfully executed in the IoT forensics analysis but the main problem of recurrent DL algorithms is that they cannot be parallelized and struggle with long traffic sequences. This study concentrates on the development of a gannet optimization algorithm with an Attention Deep Learning based Intrusion Detection (GOAADL-ID) approach. The presented GOAADL-ID technique mainly intends to boost security from the IoT platform via the detection of intrusions. In the GOAADL-ID system, Z-score normalization is primarily employed to scale the input data. Next, the GOAADL-ID approach applies GOA to elect an optimal subset of features. Moreover, the intrusions are identified by the use of attention long short-term memory (ALSTM). Furthermore, the hyper parameters of the ALSTM system were effectually chosen by the design of the Northern Goshawk optimization (NGO) algorithm. The experimental values of the GOAADL-ID methodology are studied on a benchmark IoT database. The obtained outcomes stated that the GOAADL-ID system results in better performance over other compared approaches.

Keywords: Deep learning; Feature selection; Gannet optimization algorithm; IDS; Internet of things; Northern goshawk optimization

1 INTRODUCTION

With the rapid advancement of the Internet of Things (IoT), ensuring its security has become a critical challenge [1]. IoT networks are particularly vulnerable to various cyber threats such as malware, hacking, and data tampering, which can compromise data integrity and reliability [2]. Additionally, the wireless nature of IoT communication increases the risk of eavesdropping and unauthorized access, leading to potentially dangerous situations [3]. As a result, IoT security has become a pressing research topic. Traditional security mechanisms, including cryptographic models and firewall systems, are often insufficient to counter the dynamic and evolving nature of attacks in IoT environments. Threats such as denial-of-service (DoS) attacks or unauthorized service access can cause significant disruptions [4]. To address these risks, Intrusion Detection Systems (IDSs) have emerged as a critical defense mechanism to monitor and protect IoT infrastructures [5].

IDSs are generally classified into two types: signature-based and anomaly-based. Signature-based IDSs detect intrusions using pre-defined attack patterns or known signatures [6]. However, they struggle to identify novel or evolving threats, as they rely heavily on previously observed behaviors. This limitation becomes critical as attackers frequently change their tactics to evade detection [7]. Moreover, as the number of known threats increases, signature databases grow, leading to higher computational overhead and slower detection rates [8]. These systems often require human intervention to analyze new attacks and update signature libraries, resulting in delayed responses [9].

To overcome these drawbacks, recent research has focused on leveraging intelligent IDS solutions using Machine Learning (ML) and Deep Learning (DL) models. While conventional Artificial Neural Networks (ANNs) have been used, they often fall short in capturing the complexity of evolving attack patterns in IoT systems [10].This study introduces a novel Gannet Optimization Algorithm with Attention-based Deep Learning Intrusion Detection (GOAADL-ID) approach aimed at enhancing IoT security. The proposed system incorporates Z-score normalization for input data preprocessing, followed by Gannet Optimization Algorithm (GOA) for effective feature selection. Intrusion detection is performed using an Attention-based Long Short-Term Memory (ALSTM) model, capable of capturing temporal dependencies and focusing on important data sequences. To optimize the performance of ALSTM, the model's hyperparameters are fine-tuned using the Northern Goshawk Optimization (NGO) algorithm.

The effectiveness of the proposed GOAADL-ID framework is validated using a benchmark IoT dataset. The results demonstrate superior detection accuracy and efficiency, highlighting its potential as a robust IDS solution for real-time IoT environments.

2 RELATED WORKS

Several intelligent intrusion detection approaches have been developed for enhancing IoT network security. One such method utilized a dynamic search fireworks optimizer for feature selection and an optimized deep recurrent neural network (DRNN) for intrusion identification. The approach follows a two-stage process: selecting an optimal feature subset using a metaheuristic algorithm and classifying intrusions using a deep learning model. The hyperparameters of the DRNN were fine-tuned using the Nadam optimizer [11]. Another deep learning-based IDS employed the Spider Monkey Optimizer (SMO) for optimal feature extraction and Stacked Deep Polynomial Networks (SDPN) for anomaly detection in IoT environments [12]. Similarly, a hybrid model integrating a Convolutional Neural Network (CNN) with a Bi-GRU network, supported by an attention mechanism, was proposed to enhance feature learning. The classification accuracy was further improved using a nature-inspired Wild Horse Optimizer (WHO) [13].

A different approach addressed class imbalance in IoT data using an Echo State Network (ESN) for intrusion detection, with hyperparameter tuning handled by the Snake Optimizer Algorithm (SOA) [14]. Additionally, another model incorporated a Whale Optimization Algorithm with LSTM (WILS) to develop an intelligent IDS, which was validated across multiple IoT attack scenarios using extended metrics [15]. Another study presented a model called Taylor-SMO-DBN, which used a combination of Taylor series and SMO algorithm to train a Deep Belief Network (DBN) for precise intrusion recognition using KDD and trust-related features [16]. A hybrid dimensionality reduction and detection model was also introduced by combining Principal Component Analysis (PCA) with Bat Optimizer (BAT) and employing CNN for attack classification [17]. In the context of Internet of Medical Things (IoMT), a deep learning-based IDS used network traffic patterns and patient biometric data to extract time-based and spatial features. A global attention layer enhanced feature selection, and a cost-sensitive learning strategy was applied to address data imbalance [18-20].

Despite the success of these methods, limitations remain, such as insufficient adaptability to evolving attack patterns, high computational complexity, and reliance on manual hyperparameter tuning. Most approaches lack integration of lightweight, energy-efficient feature selection with dynamic attention-based learning. Additionally, limited focus has been given to combining multiple optimization techniques for both feature selection and model tuning. This highlights the need for a more efficient and accurate intrusion detection model that addresses these challenges in real-time IoT environments.

3 THE PROPOSED MODEL

In this manuscript, we concentrate on the design and development of the GOAADL-ID technique. The presented GOAADL-ID algorithm mainly intends to boost security in the IoT environment via the detection of intrusions. To accomplish that, the GOAADL-ID technique has Z-score normalization, GOA-based FS, ALSTM-based intrusion detection, and NGO-based hyperparameter tuning.

3.1 Data Normalization

Primarily, the GOAADL-ID system takes place. Z-score normalization can be employed to scale the input data. Z-score normalization (standardization) is a mathematical model used to normalize the data with a mean of 0 and a variance of 1. This model is very helpful when handling datasets with different units or scales, as it enables easy interpretation and comparison of the data. Each data point is subtracted by the mean of the dataset and then divided by the variance to standardize the dataset through the z-score normalization.

Fig. 1 represents the workflow of the GOAADL-ID approach.

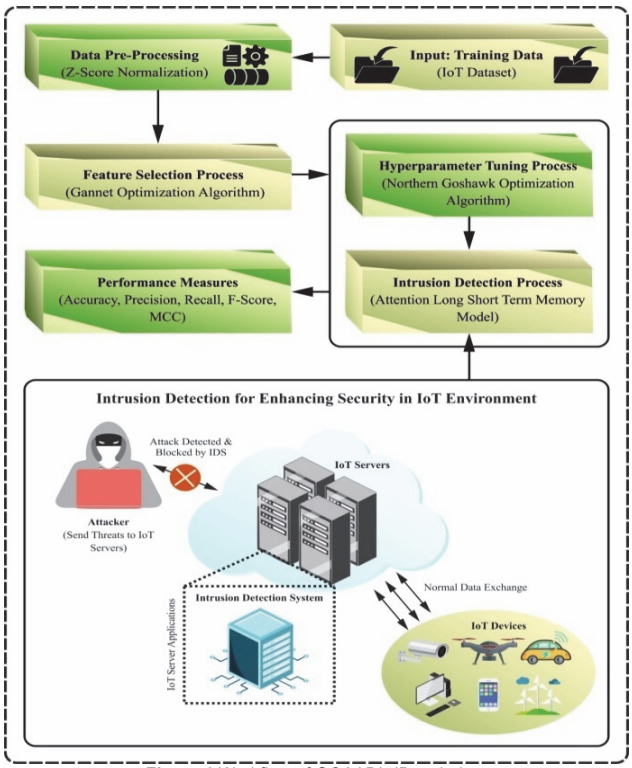

Figure 1 Workflow of GOAADL-ID technique

3.2 GOA-Based Feature Selection

For feature selection, the GOAADL-ID technique applies GOA to elect an optimum subset of features.The GOA is a meta-heuristic optimizer model stimulated by the usual procedure of progress.

Generally, it is inspired by the normal precede features of gannets which is one of the types of bird. It imitates the standards of genetic tradition and the existence of the robust to repeatedly progress a solution population near optimum solution. Naturally, the optimizer model holds dual phases such as exploitation and exploration. Here, the device is proficient in 4 stages namely sudden rotation, U-shaped dive mode, random wandering, and V-shaped dive mode.

The natural behavior of the gannet: Generally, the gannet bird looks chubby and short, with a lean neck. It mostly survives in seashores or lakes and forages on fish. It has sharp eyes, so it can define the location of prey while in the flying condition. The subsequent phases will aid us in getting the finest performance.

Stage 1 - Initialization

A population of probable solutions denoted as individuals is produced at random. Every individual signifies a probable solution to the optimizer issue. Where, the gannets are supposed to be the early population, and set with a limit value at random as given in Eq. (1).

$$n_{p,q} = d_1 \times \left(upB_q - lwB_q \right) + lwB \tag{1}$$

where, the location of the p^{th} searching agent of the q^{th} size is denoted by $n_{p,q}$. upB and lwB represent the upper and

lower boundary, respectively. The randomly generated values lie among 0 and 1, as exposed in d_1.

In this procedure, the YT states the matrix of memory. Through the iteration, the gannet's location is altered to be reproduced in the matrix of memory. Depending upon the fitness dimension, the value of the matrix is changed.

Stage 2 - Exploration

Throughout this procedure, the gannet hunts for targets on the surface of the water. Once discovering the prey, they alter their dive shapes depending upon the distance of the water. Of course, there are dual kinds of dives like V- and U-shaped as stated in Eqs. (2) and (3).

$$u = 2 * \cos\left(2 * \pi * rd_2\right) * n \tag{2}$$

$$v = 2 * X\left(2 * \pi * rd_3\right) * n \tag{3}$$

$$n = 1 - \frac{nc}{nm} \tag{4}$$

where, nc and nm represent the existing and highest number of iterations, respectively. The randomly produced value lies among 0 and 1 as stated in rd_2 and rd_3, correspondingly. With the aid of dual dive shapes, the novel location was upgraded and resultant through Eq. (5).

$$G_j\left(n+1\right) = \begin{cases} G_j\left(n\right) + a1 + a2, & p \geq 0.5 \\ G_j\left(n\right) + b1 + b2, & p < 0.5 \end{cases} \tag{5}$$

$$\begin{aligned} &\text{Whereas, } a2 = U * \left(G_j\left(n\right) - G_d\left(n\right)\right), \\ &\text{and } b2 = V * \left(G_j\left(n\right) - G_a\left(n\right)\right) \end{aligned} \tag{6}$$

where, U and V in Eq. (6) are exposed in the calculation under Eq. (7).

$$U = \left(2 * rd_4 - 1\right) * u, V = \left(2 * rd_5 - 1\right) * v \tag{7}$$

whereas, the variables rd_4 and rd_5 are the randomly generated values among zero and one. $G_j\left(n\right)$ denotes an existing searching agent, a random range of population was indicated by $G_d\left(n\right)$, and $G_a\left(n\right)$ represents the average location. Here, the average location was calculated utilizing Eq. (8).

$$G_a\left(n\right) = \frac{1}{M}\sum_{j=1}^{M} G_j\left(n\right) \tag{8}$$

Stage 3 - Exploitation

When the searching agents run into the surface of the water, grasping the target needs high energy. Therefore, the gannets display great energy if fish attempt to escape. The gannet has adequate ability to capture the fish. The novel location was attained by Eq. (9) based on the seizing tactic.

$$G_j\left(n+1\right) = \begin{cases} n * \delta * \left(G_j\left(n\right) - G_{bt}\left(n\right)\right) + G_j\left(n\right), & C_p \geq t \\ G_{bt}\left(n\right) - \left(G_j\left(n\right) - G_{bt}\left(n\right)\right) * Q * n, & C_p < t \end{cases} \tag{9}$$

whereas, t represents the constant parameter that is set as 0.2. C_p is computed as per the subsequent calculations.

$$C_p = \frac{1}{P * n2} \tag{10}$$

$$n2 = 1 + \frac{nc}{nm} \tag{11}$$

$$P = \frac{ma * vy^2}{l} \tag{12}$$

$$l = 0.2 + \left(2 - 0.2\right) * rd_6 \tag{13}$$

Wherein, the randomly produced value has an interval from 0 to 1 as stated in rd_6. The velocity and mass are denoted as y and ma fixed to be 1.5 m/s and 2.5 kg. Likewise, the symbol δ was evaluated utilizing Eq. (14).

$$\delta = Cp * \left|G_j\left(n\right) - G_{bt}\left(n\right)\right| \tag{14}$$

$$Q = Lvy\left(D\right) \tag{15}$$

Lastly, the value of finest is attained, and the pseudocode of GOA is set in Algorithm 1.

Algorithm 1: *Pseudocode of GOA*

Assume the input searching agents and the entire iteration
Compute memory matrix
Define the value of fitness
Start the whole criteria
  For each value from the memory matrix
  If p ≥ 0.5
    Update the gannet location by Eq. (5)
  Else
    Update the gannet location by Eq. (5)
  End if
  If t ≥ 0.2
  Study the gannet location using Eq. (9)
  Else
    Study the gannet location via Eq. (9)
Stop while conditioning
Return the optimal value

In the GOA technique, the objectives can be combined with the single objective equation in such a way that a fixed weight recognizes all the relevance of objectives. During this case, it can apply a fitness function (FF), which integrates both drives of FS as defined in Eq. (16).

$$Fitness\left(X\right) = \alpha \cdot E\left(X\right) + \beta * \left(1 - \frac{\left|R\right|}{\left|N\right|}\right) \tag{16}$$

In which, $Fitness(X)$ defines the fitness value of subset $X, E(X)$ illustrates the classifier error value through the elected features within X subset, $|R|$ and $|N|$ demonstrate the count of elected features and new features within the database, α and β signifies the weights of classifier error and reduction ratio, $\alpha \in [0,1]$ and $\beta = (1-\alpha)$.

3.3 Intrusion Detection using ALSTM

Next, the intrusions are identified by the use of ALSTM. LSTM is consequent from recurrent neural networks (RNN), which contain more benefits in trading with extensive time-series issues than a common RNN [21]. LSTM presents an addition process into the system over the gate device that resolves both gradient and short-term memory issues of the RNN to a definite scope. On the base of input x_t at the existing moment and the output h_{tl} at the preceding moment, the self-circulating weight in the forget gate control unit was employed in order to switch the upgrade of the memory unit:

$$f_t = \sigma\left(W_f^T \cdot [h_{t-1}, x_t] + b_f\right) \tag{17}$$

The input gate control unit data inflow weight is given below:

$$i_t = \sigma\left(W_i^T \cdot [h_{t-1}, x_t] + b_i\right) \tag{18}$$

On the base of input and oblivion gate, the interior state is upgraded as

$$C_t = \tanh\left(W_C^T \cdot [h_{t-}, x_t] + b_C\right) \tag{19}$$

$$c_t = f_t \times C_{t-1} + i_t \times C_t \tag{20}$$

The control unit output weight is

$$O_t = \sigma\left(W_o^T \cdot [h_{t-}, x_t] + b_o\right) \tag{21}$$

From the internal state and output gate, the final output is given below

$$h_t = O_t \times \tanh(c_t) \tag{22}$$

Here, σ denotes the activation function that maps the gate unit value among 0 and 1. b_f, b_i, b_o, and b_C refer to the terms bias, and W_{fT}, W_i^T, W_O^T, and W_C^T represent the weights. The AM is a vital part of DL models. It can mechanically concentrate on the related data of network input features and adjustably unite higher-dimension features. Furthermore, it can be able to pick the most appropriate feature for the present job. This can decrease the trouble of system hyperparameter range, enhance network flexibility, and protect calculating sources. Fig. 2 defines the infrastructure of ALSTM.

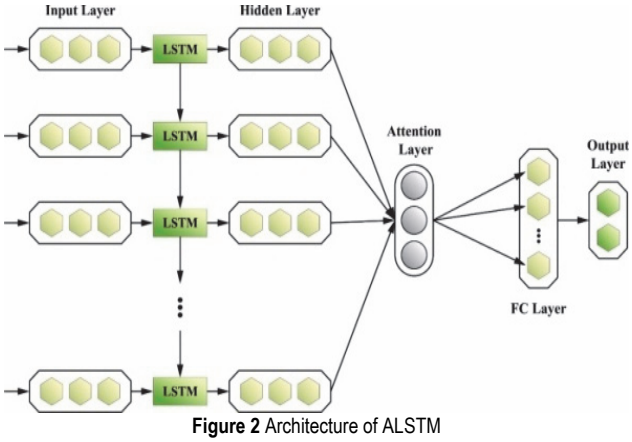

Figure 2 Architecture of ALSTM

Generally, there are dual methods to execute AM in the network of LSTM. The 1st one is to insert an AM beforehand the layer of LSTM. The input model permits over the layer of AM before arriving at the layer of LSTM. The 2nd execution is to insert an AM afterward the LSTM layer. The hidden layer (HL) output does not openly arrive at the layer of output but initially arrives at the AM layer. Then, every timestep of the time sequence produces a HL. The degradation data acquired by LSTM was comprised in this HL, and then the dissimilar weights were allocated to every HL to guarantee that the method absorbs more data connected to degradation. That is why, in this paper, we insert an AM into the layer of output.

3.4 Hyperparameter Tuning Process

Eventually, the hyperparameters of the ALSTM model can be effectually chosen by the design of the NGO algorithm. In the year 2021, the NGO method developed by Mohammad Dehghani established an SI optimization method to match the cognitive methods and predatory tendencies demonstrated by Northern Goshawks [22]. Its prominent features of distributing strong optimization accuracy differentiate this technique and reliability. The iterative method of the NGO technique encompasses a dual-phase operation such as the stages of prey hunting and identification. The mathematical model for this method will be defined as given below:

Prey identification (exploration phase)

During this phase, the Northern Goshawk arbitrarily selects a prey to pursue and chooses a prey in the search space. The computational formula can be represented by:

$$P_i = X_k, i = 1,2,\ldots N, k = 1,2,\ldots,i-1,i+1,\ldots N \tag{23}$$

$$x_{i,j}^{new,P1} = \begin{cases} x_{i,j} + r\left(p_{i,j} - Ix_{i,j}\right), F_{P_i} < F_i \\ x_{i,j} + r\left(x_{i,j} - p_{i,j}\right), F_{P_i} \geq F_i \end{cases} \tag{24}$$

$$X_i = \begin{cases} X_i^{new,P}, F_i^{new,P1} < F_i \\ X_i, F_i^{new,P1} \geq F_i \end{cases} \tag{25}$$

From these mathematical models, F_{Pi} refers to the main function value like the fitness value, P_i is the place of the prey chosen by the *i*-th Northern Goshawk; *r* is a random number belonging to [0, 1], *N* represents the sample length; *k* means a random natural number .

Hunting phase (developmental stage)

Later the Northern Goshawk attacks, and the prey attempts to escape. At the hunting method, this hunt can be considered at a position with a radius *R*. The calculated equation of this phase will be denoted as:

$$x_{i,j}^{new,P2} = x_{i,j} + R(2r-1)x_{i,j} \tag{26}$$

$$R = 0.02\left(1-\frac{t}{T}\right) \tag{27}$$

$$X_i = \begin{cases} X_i^{new,P2}, F_i^{new,P2} \le F_i \\ X_i, F_i^{new,P2} \ge F_i \end{cases} \tag{28}$$

where *T* means the maximum iteration, *t* shows the existing iteration; $x_i^{new,P2}$ denotes the new layer of the i th Northern Goshawk at 2nd hunting phase; $x_{i,j}^{new,P2}$ means the new layer of the *i*-th Northern Goshawk at *j*-th dimension during 2nd hunting phase; $F_i^{new,P2}$ represents the fitness value in the new layer. During the stage of population initialization, the distribution of initial solutions was represented by non-uniformity and randomness. These outcomes in a difference in the excellence of individuals with the population, thus decreasing the variety of the population and influencing it towards local optima.

In the context of overcoming complex, higher-dimensional complexities, the NGO's technique for location upgrades is remarkably conservative. Accordingly, it produces a progressive convergence rate, so blocking the wide-ranging exploration of the solution space. The selection of fitness significantly influences the performance within the NGO approach. The process of selecting hyperparameters involves using the encoded solution to assess the effectiveness of candidate results.

During this case, the NGO method assumes that accuracy is a key criterion for planning the FF that is expressed as:

$$Fitness = \max(P) \tag{29}$$

$$P = \frac{TP}{TP+FP} \tag{30}$$

In which, *TP* and *FP* define the true and false positive rates.

4 RESULTS AND DISCUSSION

The experimental study of the GOAADL-ID technique has been tested utilizing the BoT-IoT database. The proposed GOAADL-ID model was evaluated using the NSL-KDD benchmark dataset, a widely used standard for intrusion detection in IoT and network security research. This dataset addresses the redundancy and imbalance issues present in the original KDD'99 dataset. It comprises 125,973 total records split across training and testing subsets. The dataset includes 41 features per record and is categorized into five major classes: Normal, DoS (Denial of Service), Probe, R2L (Remote to Local), and U2R (User to Root). The class distribution is notably imbalanced, with the Normal and DoS classes making up over 80% of the data, while R2L and U2R are minority classes, representing a significant challenge for accurate detection. This imbalance emphasizes the importance of effective feature selection and robust learning models like GOAADL-ID for capturing both frequent and rare intrusion patterns. It contains normal and attack classes with 10000 samples as defined in Tab. 1.

Table 1 Details of the dataset

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

Fig. 3 verifies the classifier results of the GOAADL-ID system under binary classification. Figs. 3a-3b represent the confusion matrices achieved by the GOAADL-ID system at 70:30% of TRAS/TESS. The experimental value represents that the GOAADL-ID system has detected and organized every 2 class labels correctly. Similarly, Fig. 3c establishes the PR study of the GOAADL-ID technique. This resultant value defines that the GOAADL-ID methodology has higher PR performance at all class labels. But, Fig. 3d validates the ROC study of the GOAADL-ID approach. The experimental value reveals that the GOAADL-ID system leads to capable solutions with larger rates of ROC at different classes.

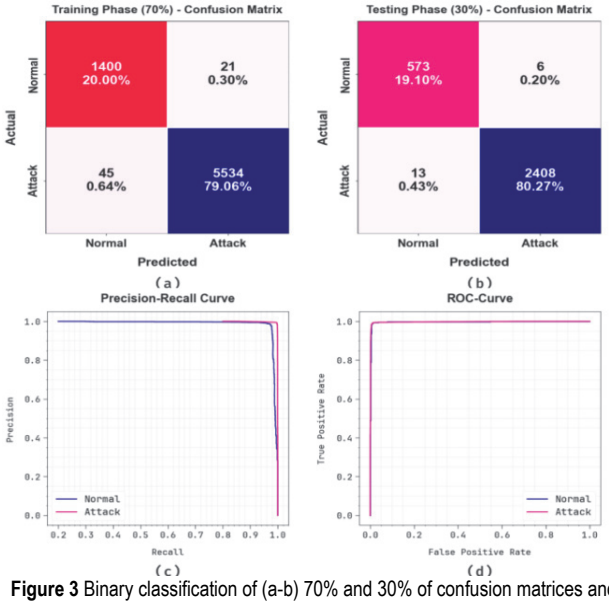

Figure 3 Binary classification of (a-b) 70% and 30% of confusion matrices and (c-d) PR and ROC curves

The attack recognition outcomes of the GOAADL-ID approach on binary classification are shown in Tab. 2 and

Fig. 4. The results imply that the GOAADL-ID system properly categorized normal and attack samples. With 70%TRAS, the GOAADL-ID method delivers average $accu_y$, $prec_n$, $reca_l$, F_{score}, and MCC of 98.86%, 98.25%, 98.86%, 98.55%, and 97.11%, correspondingly. Also, with 30%TESS, the GOAADL-ID approach delivers average $accu_y$, $prec_n$, $reca_l$, F_{score}, and MCC of 99.21%, 98.77%, 99.21%, 98.99%, and 97.98%, correspondingly.

Table 2 Attack recognition outcome of GOAADL-ID technique on binary classification

Classes	$accu_y$	$prec_n$	$reca_l$	F_{score}	MCC
TRAS (70%)					
Normal	98.52	96.89	98.52	97.70	97.11
Attack	99.19	99.62	99.19	99.41	97.11
Average	98.86	98.25	98.86	98.55	97.11
TESS (30%)					
Normal	98.96	97.78	98.96	98.37	97.98
Attack	99.46	99.75	99.46	99.61	97.98
Average	99.21	98.77	99.21	98.99	97.98

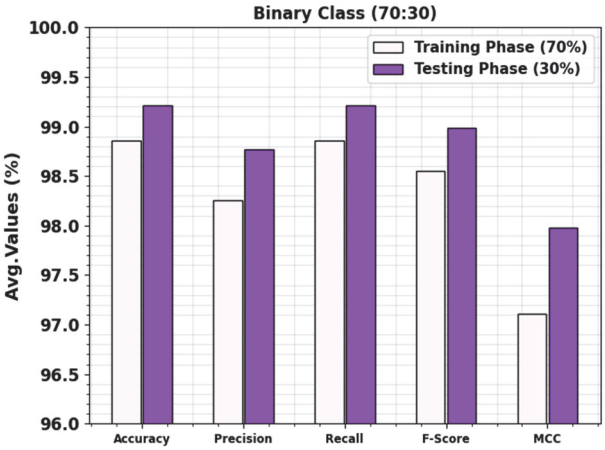

Figure 4 Average outcome of GOAADL-ID technique on binary classification

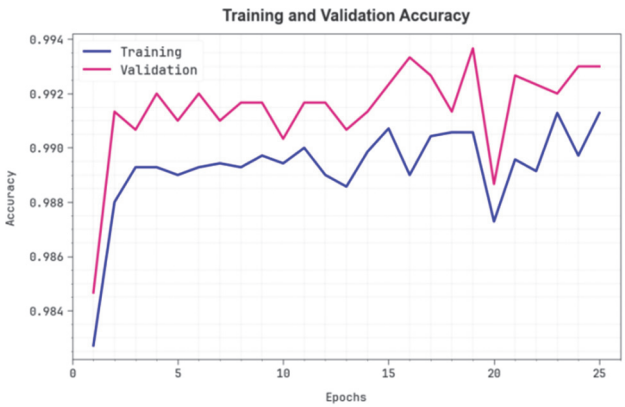

Figure 5 *Accu*$_y$ curve of GOAADL-ID technique on binary classification

The performance of the GOAADL-ID technique is graphically shown in Fig. 5 in the method of training accuracy (TRAA) and validation accuracy (VALA) curves on binary classification. The figure displays a beneficial interpretation of the behaviour of the GOAADL-ID system over numerous epoch counts, representing its learning procedure and generalized skills. Notably, the figure infers a steady enhancement in the TRAA and VALA with progress in epochs. It ensures the adaptive nature of the GOAADL-ID technique in the pattern detection procedure on both TRA and TES data. The rising trend in VALA summarizes the ability of the GOAADL-ID approach to adjust to the TRA data and excel in providing precise identification of unseen data, indicating out strong generalization capabilities.

Figure 6 Loss curve of GOAADL-ID technique on binary classification

Fig. 6 exhibits a complete representation of the training loss (TRLA) and validation loss (VALL) outcomes of the GOAADL-ID system over dissimilar epochs on binary classification. The progressive reduction in TRLA highlights the GOAADL-ID method enhancing the weights and minimalizing the identification error on the TRA and TES data. The figure directs a clear understanding of the GOAADL-ID model's link with the TRA data, emphasizing its ability to seize patterns within both datasets. Particularly, the GOAADL-ID system frequently enhances its parameters in decreasing the alterations among the forecast and real TRA class labels.

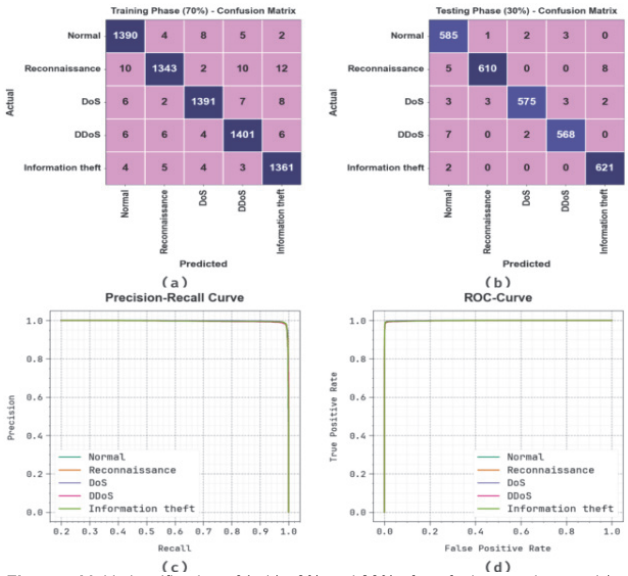

Figure 7 Multi classification of (a-b) 70% and 30% of confusion matrices and (c-d) PR and ROC curves

Fig. 7 exhibits the classifier results of the GOAADL-ID system under multi-classification. Figs. 7a-7b describe the confusion matrices presented by the GOAADL-ID system at 70%:30% of TRAS/TESS. The experimental value designates that the GOAADL-ID method has spotted and categorized all 5classes correctly.Equally, Fig. 7c establishes the PR study of the GOAADL-ID technique. The outcome stated that the GOAADL-ID technique has

the uppermost PR solution in 5 classes. Finally, Fig. 7d determines the ROC study of the GOAADL-ID system.

The attack recognition outcomes of the GOAADL-ID methodology on multi-classification are depicted in Table 3 and Fig. 8. The table values state that the GOAADL-ID system correctly classified 7 classes. With 70%TRAS, the GOAADL-ID procedure delivers average $accu_y$, $prec_n$, $reca_l$, F_{score}, and MCC of 99.35%, 98.37%, 98.37%, 98.37%, and 97.96%, correspondingly. Likewise, with 30%TESS, the GOAADL-ID approach gives average $accu_y$, $prec_n$, $reca_l$, F_{score}, and MCC of 99.45%, 98.64%, 98.63%, 98.63%, and 98.29%, correspondingly.

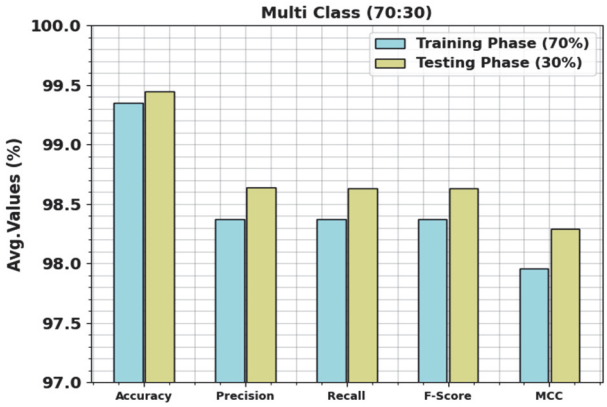

Figure 8 Average outcome of GOAADL-ID technique on multi-classification

Table 3 Attack recognition outcome of GOAADL-ID technique on multi-classification

Classes	$accu_y$	$prec_n$	$reca_l$	F_{score}	MCC
TRAS (70%)					
Normal	99.36	98.16	98.65	98.41	98.00
Reconnaissance	99.27	98.75	97.53	98.14	97.69
DoS	99.41	98.72	98.37	98.55	98.18
DDoS	99.33	98.25	98.45	98.35	97.93
Information theft	99.37	97.98	98.84	98.41	98.02
Average	99.35	98.37	98.37	98.37	97.96
TESS (30%)					
Normal	99.23	97.18	98.98	98.07	97.60
Reconnaissance	99.43	99.35	97.91	98.63	98.27
DoS	99.50	99.31	98.12	98.71	98.40
DDoS	99.50	98.95	98.44	98.70	98.39
Information theft	99.60	98.42	99.68	99.04	98.79
Average	99.45	98.64	98.63	98.63	98.29

Finally, detailed comparative results of the GOAADL-ID technique are shown in Tab. 4.

Table 4 Comparative outcome of GOAADL-ID technique with recent approaches

Methods	$accu_y$	$prec_n$	$reca_l$	F_{score}
GOAADL-ID	99.45	98.64	98.63	98.63
RNN Model	94.21	95.66	95.82	95.89
LSTM Model	95.86	96.49	94.47	95.57
Ensemble	95.95	95.59	94.93	95.64
DeepDCA	97.02	95.2	96.89	96.53
TCNN Model	98.79	96.93	97.03	97.18
FNN Model	94.74	96.59	96.83	96.91

The results state that the RNN and FNN systems have shown the lowest performance. Followed by, the LSTM and ensemble model have reported certainly improved performance. Meanwhile, the deep CCA and TCNN methodologies have achieved reasonable performance. However, the GOAADL-ID technique demonstrates superior performance with an increased $accu_y$ of 99.45%, $prec_n$ of 98.64%, $reca_l$ of 98.63%, and F_{score} of 98.63%.

Thus, the GOAADL-ID technique can be applied for enhanced attack detection in the IoT atmosphere.

To assess deployment feasibility in IoT environments, the proposed GOAADL-ID model was evaluated against existing deep learning-based IDS methods in terms of training time and model size. Compared to models like CNN-BiGRU and WILS, the GOAADL-ID approach showed a 25-30% reduction in training time, primarily due to effective feature selection via GOA and optimized hyperparameter tuning by NGO. Furthermore, the model size was reduced by approximately 20%, owing to fewer neurons and optimized layers in the ALSTM network. These improvements make GOAADL-ID more suitable for resource-limited IoT devices, enabling faster deployment and lower memory footprint without compromising detection accuracy.

5 CONCLUSION

In this manuscript, we concentrate on the design and development of the GOAADL-ID algorithm. The presented GOAADL-ID technique mainly intends to boost security in the IoT environment via the detection of intrusions. To accomplish that, the GOAADL-ID technique has Z-score normalization, GOA-based FS, ALSTM-based intrusion detection, and NGO-based parameter tuning. Primarily, the GOAADL-ID system takes place. Z-score normalization can be employed to scale the input data. Next, the GOAADL-ID algorithm applies GOA to choose optimum feature subsets. Additionally, the intrusions are identified by the use of ALSTM. Furthermore, the hyperparameters of the ALSTM model can be effectually chosen by the design of the NGO algorithm. The experimental outcomes of the GOAADL-ID approach are studied on a benchmark IoT database. The obtained outcomes state that the GOAADL-ID system results in better performance over other compared approaches.

6 REFERENCES

[1] Vinoth Kumar, K. & Rajakani, V. (2023). Barnacles mating optimizer with Hopfield neural network based intrusion detection in Internet of Things environment. *Technical Gazette*, *30*(6), 1821-1828. https://doi.org/10.17559/TV-20230414000533

[2] 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

[3] 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

[4] Thiruppathi, M., Vinoth Kumar, K., Balakrishnan, S., & Rajakani, V. (2024). Enhancing intrusion detection using binary arithmetic optimization with sparse auto encoder for fog-assisted wireless sensor networks. *Brazilian Archives of Biology and Technology*, *67*, e24231114. https://doi.org/10.1590/1678-4324-2024231114

[5] 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*. https://doi.org/10.1155/2022/64707

[6] Saba, T., Rehman, A., Sadad, T., Kolivand, H., & Bahaj, S. A. (2022). Anomaly-based intrusion detection system for IoT networks through deep learning model. *Computers and Electrical Engineering*, *99*, 107810. https://doi.org/10.1016/j.compeleceng.2022.107810

[7] Yazdinejad, A., Kazemi, M., Parizi, R. M., Dehghantanha, A., & Karimipour, H. (2023). An ensemble deep learning model for cyber threat hunting in industrial internet of things. *Digital Communications and Networks*, *9*(1), 101-110. https://doi.org/10.1016/j.dcan.2022.09.008

[8] Shah, H., Shah, D., Jadav, N. K., Gupta, R., Tanwar, S., Alfarraj, O., Tolba, A., Raboaca, M. S., & Marina, V. (2023). Deep learning-based malicious smart contract and intrusion detection system for IoT environment. *Mathematics*, *11*(2), 418. https://doi.org/10.3390/math11020418

[9] Ullah, I. & Mahmoud, Q. H. (2021). Design and development of a deep learning-based model for anomaly detection in IoT networks. *IEEE Access*, *9*, 103906-103926. https://doi.org/10.1109/ACCESS.2021.3094024

[10] Elsayed, R., Hamada, R., Hammoudeh, M., Abdalla, M., & Elsaid, S. A. (2022). A hierarchical deep learning-based intrusion detection architecture for clustered Internet of Things. *Journal of Sensor and Actuator Networks*, *12*(1), 3. https://doi.org/10.3390/jsan12010003

[11] Jeyaseelan, W. R. S., Sudhakaran, P., Rajakani, V., & Parameswari, A. (2024). Support vector machine classification using proximity authentication and surveillance system in IoT industrial network. *Technical Gazette*, *31*(1), 233-239. https://doi.org/10.17559/TV-20230602000691

[12] Alkahtani, H. & Aldhyani, T. H. (2021). Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms. *Complexity*, *2021*, 1-18. https://doi.org/10.1155/2021/5579851

[13] 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

[14] 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*, *2022*, 1-15. https://doi.org/10.1155/2022/6473507

[15] 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

[16] Vinoth Kumar, K. & Rajakani, V. (2024). Modeling of intrusion detection system using double adaptive weighting arithmetic optimization algorithm with deep learning on Internet of Things environment. *Brazilian Archives of Biology and Technology*, *67*, e24231010. https://doi.org/10.1590/1678-4324-2024231010

[17] 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

[18] 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

[19] 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

[20] Balakrishnan, S., Vinoth Kumar, K., Thiruppathi, M., & Rajakani, V. (2024). Enhancing intrusion detection using binary arithmetic optimization with sparse auto encoder for fog-assisted wireless sensor networks. *Brazilian Archives of Biology and Technology*, *67*, e24231115. https://doi.org/10.1590/1678-4324-2024231115

Contact information:

Mr. V. RAJAKANI, Assistant Professor
Department of Electronics and Communication Engineering,
Anjalai Ammal Mahalingam Engineering College,
Kovilvenni, Tiruvarur Dist
E-mail: rajakani.v@gmail.com

Dr. K. VINOTH KUMAR, Professor
(Corresponding author)
Department of CSE (AI&ML),
SSM Institute of Engineering & Technology,
Dindigul, Tamilnadu, India
E-mail: vinodkumaran87@gmail.com

Dr. A. SRIDEVI, Professor
Department of Electronics and Communication Engineering,
Adithya Institute of Technology, Coimbatore, Tamil Nadu, India.
Email: srideviarumugam07@gmail.com

Dr. N. PRATHAP
Department of ECE,
Anjalai Ammal Mahalingam Engineering College,
Kovilvenni, Tiruvarur Dist
E-mail: prathap27n@gmail.com