Received: February 8, 2020. Revised: April 5, 2021. 66

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Hybrid Particle Swarm and Gray Wolf Optimization Algorithm for IoT Intrusion Detection System

Ediga Sathyanarayana Phalguna Krishna[1]* **Thangavelu Arunkumar[1]**

[1]*School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology, Vellore, India*
* Corresponding author's Email: phalgunakrishna@gmail.com

Abstract: Internet of Things (IoT) is a network that provides security for physical objects such as smart home appliance, smart machines and many more. The physical objects are assigned to a unique Internet address known as Internet Protocol (IP) that is used for data communication with the external entities of the network through the internet. The IoT devices are facing security issues due to the rapid increase in attacks that are launched by the intruders during data sharing through the internet. The detection of attacks is essential to provide a strong security mechanism for such threatening attacks. The proposed hybrid optimization algorithm utilizes the combination of Particle Swarm Optimization (PSO) and Gray Wolf Optimization (GWO) in this research. The PSO is known for its fast computation speed and has found extensive utility in data training as well as data estimation. The GWO is developed as an intrusion detection approach to classify data and to efficiently detect several of intrusions. The proposed hybrid GWO-PSO uses NSL-KDD data set with binary and multi class problem respectively for showing the effectiveness of the present work. The results obtained better accuracy value of 99.97 % when compared to the existing LSTM-RNN that achieved 97.72% of accuracy, whereas the multi class SVM obtained 98 % and modified rank-based information gain feature selection method showed 99.8 % of accuracy.

Keywords: Distributed denial-of-service, Gray wolf optimization, Internet address, Internet of things, Particle swarm optimization.

1. Introduction

IoT is referred to as the network of physical objects that are embedded with software and are connected through the internet for providing security during exchange of a big volume of data. However, the purpose of connecting to the IoT devices for exchanging the data through internet faces security challenges for industries [1]. As a result, variety of malware variants and threats are newly emerging at a faster pace. [2-4] Attacks against IoT include theft of sensitive data or disrupting the functions of the network which include, Brute Force, Port Scanning, Denial of Service (DoS), Remote to Local (R2L), Probing (Probe), User to Root (U2R) attacks, etc., These attacks are affect the real-time applications such as transport and network protocols such as HTTP, TCP, SMTP, UDP, FTP, ICMP, etc [5-7]. In contrast, anomaly-based detection is used to detect either known or unknown attacks [8, 9]. Moreover, NIDSs rely on the concept of "traffic identification", used for extracting the useful features from the captured traffic flow, and then classifies the traffic record as either "normal" or "attack" using machine learning algorithm [10]. Artificial intelligence (AI) can stop IoT-based DDoS attacks in their tracks. Advanced technologies of machine learning, particularly deep learning are used in providing security against attacks [11, 12] since it has better accuracy and robustness in the detection of attacks. The AI techniques are used for attack detection automatically which does not require expert knowledge for classification. The objectives and contributions of the present research are given as follows to utilize metaheuristic features and hyper parameters by employing a hybrid GWO-PSO based algorithm. The proposed hybrid GWO-PSO extensively trained the data and was used for data

estimation. The GWO classified efficiently the data based on several intrusions and improved the system and classification performance. The proposed hybrid GWO-PSO showed 99.97 % better when compared to the existing LSTM-RNN that achieved 97.72%, multi class SVM obtained 98 % and modified rank-based information gain feature selection method showed 99.8 %.

The structure of the research paper is given as follows: Section 2 describes the literature review of existing algorithms, which are used to provide security in IoT. Section 3 describes the proposed GWO-PSO model. Section 4 explains the results that include the quantitative and comparative analysis. The conclusion and future work of this proposed research is given in Section 5.

2. Literature review

The existing works have been intensively researched using AI techniques for network intrusion detection. Most previous works have explored network intrusion detection on the full feature set of the dataset and are discussed as follows:

McDermott [13] developed a model to evaluate perception and awareness of Botnet Activity within Consumer Internet of Things (IoT). While analyzing the requirements of the user from the IoT devices [14], particular importance was placed on the privacy and security. The developed model explored the relationship between technical knowledge and the detection of threats for IoT devices using additional data for their detection. However, the developed model limited the self-report data usage.

Ansam Khraisat [15] developed a novel Hybrid Intrusion detection system for IoT attacks. In order to protect IOT devices, the developed ensemble Hybrid Intrusion Detection System (HIDS) was used by combining the Signature Intrusion Detection System (SIDS) for Anomaly Base Intrusion Detection System (AIDS). The results of the developed model showed that the hybrid IDS was showing superior performance. However, the developed model failed to detect other distinct types of attacks in the IoT system.

Philokypros [16] developed Routing Protocol for Low-Power and Lossy Networks (RPL) which was based on IoT, to detect DoS Attacks and Counter measures. The developed model detected the attacks that exploited IPv6 RPL during routing of packets at low-power IoT networks. The results obtained from the developed model showed that the RPL-based characteristics in IoT worked for normal operation and measured the countermeasures against the malicious intruder activities in the networks environment.

Spathoulas [17] developed a Collaborative BlockChain-Based Detection of DDoS Attacks Based on IoT Botnets. The existing methods included the solutions and approaches that were insufficient to protect the systems. Therefore, the aforementioned problem from the existing methods were overcome by the developed model by installing lightweight agents at distinct multiple IoT installations. The results obtained from the developed model showed that the operation evaluated the efficiency of detection against malicious agents. However, the developed model failed to obtain the proof of the applicability for the solution and stressed out limitations that may emerge.

Gassais [18] developed Multi-level host-based intrusion detection system for Internet of things. The developed techniques automatically traced the behaviour of devices and processed the data into numeric arrays. Whenever an intrusion was found, an alert was raised in the model which was an added advantage of the developed model. However, to select different models according to the targeted device, combining more than one algorithm would help further in obtaining better accuracy.

Elmasry [19] developed deep learning architectures for network intrusion detection using a double PSO metaheuristic. The developed model consisted of two levels such as the upper level where the optimal feature subset is selected for the given dataset and the vector of optimized hyper parameters was determined automatically maximized accuracy over the reduced dataset. However, only few types of attacks were included in the test set rather than in the training set to examine the ability that failed to classify them properly.

Bambang Setiawan [20] developed Increasing Accuracy and Completeness of Intrusion Detection Model using Fusion of Normalization, Feature Selection Method and Support Vector Machine (SVM). The developed model combined modified rank-based information gain feature selection method, log normalization, and SVM that trained unbalanced training data. However, the developed model showed parameter optimization due to usage of more parameters for feature selection.

Bukka Narendra Kumar [21] developed an Intrusion Detection System using the Multi Linear Dimensionality Reduction (ML-DR) with Multi-Class SVM. The combined dimensionality reduction technique with the Multi-class SVM reduced the dimension as well as sshorten the training time. However, the rank limitation problem was showed in

discriminant vectors that hindered the information obtained classification results poor.

In order to overcome the problems occurred in the existing models, the proposed hybrid GWO-PSO is explained that shows effective classifications of attacks into binary as well as multi classes based on the NSL-KDD dataset.

3. Proposed methodology

The major steps of the proposed method hybrid optimization model include GWO-PSO which is presented in Fig. 1. The block diagram consists of data collection taken from NSL-KDD and N-BaIoT datasets. Fig. 2 shows the Pictorial Representation of IoT towards attackers. The steps followed in the proposed Hybrid GWO-PSO is as follows.

The Pre-processing of data is undergone to overcome the problem of unstructured data thereby makes the classification easier.

3.1 Collection of dataset

The NSL-KDD dataset is the most common datasets used in IoT environment. The NSL-KDD dataset is formed from the different parts of the original KDD Cup 99 dataset, without the redundancies and duplication. The NSL-KDD dataset includes 41 attributes, which are labeled normal connections or attack types. NSL-KDD is a data set that suggested to solve some of the inherent problems of the KDD'99 data set which are mentioned. The number of records in the NSL-KDD train and test sets are reasonable. The advantage makes it affordable to run the experiments on the complete set without the need to randomly select a small portion. Consequently, evaluation results of different research work will be consistent and comparable. The NSL-KDD contain four attacks such as DoS, U2R, R2L, and probe Attack, which are detailed as follows:

Probe attack: The probe attack is occurred during the network scanning that will misuse the data after collecting the information of network. The probe attacks include Portsweep, Satan, Ipsweep, Mscan, Saint, and Nmap that steal the data through the internet.

R2L: The user account is obtained by transmitting the packets to machine and then detect the weakness in the network. R2L attacks include several attacks such as Snmpget attack, send mail, Phf, Snmpguess, Warez client, Guess-Password, Ftp-write, Multihop, Xsnoop, Httptunnel, Spy, Xlock, Imap, and Warezmaster that steal the data through the internet.

U2R: U2R gets access to the root account once the ordinary account is achieved. Some of the attacks

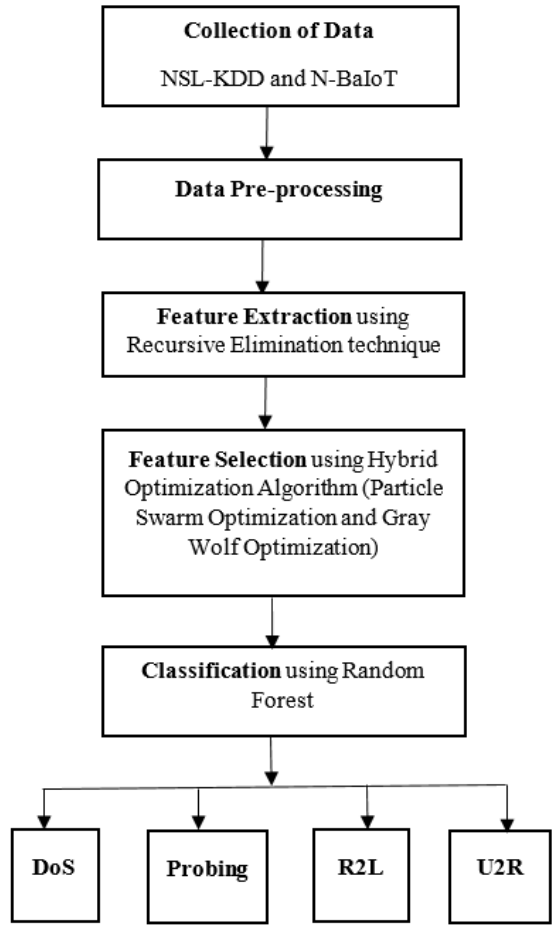

Figure 1. Block diagram of the proposed hybrid GWO-PSO algorithm

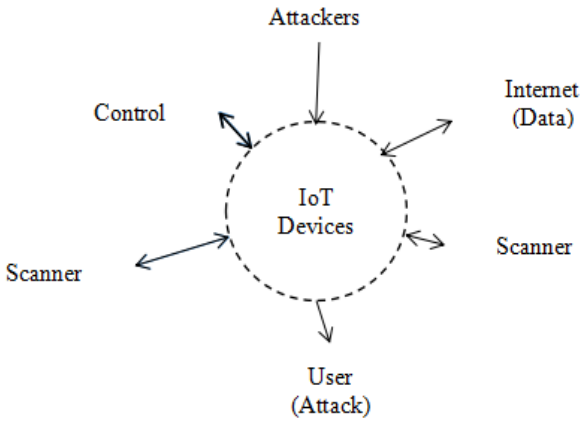

Figure 2. Pictorial Representation of IoT towards attackers

in U2R are Buffer-overflow, Load module, Perl, Sqlattack, Xterm, Rootkit, and Ps.

DoS: Due to increase in network traffic usage, a service cannot be provided by the system that results in DoS attack. The types of DoS attack in DoS are Neptune, Apache2, Udp storm, Back, Land, Smurf, Teardrop, Worm, and Pod that steals the data through internet.

Table 1. Statistical information about the NSL-KDD dataset

	Abnormal				Normal	Total
Dataset	**DoS**	**Probing**	**R2L**	**U2R**		
KDD Train +	45927	11656	995	52	67343	125973
KDD Test+	7458	2754	2421	200	9711	22544

The KDD Train+ consists of training subset, which contains 53,873 normal records, while validation and test subset both contain 6,735 normal records and 6,735 anomaly records respectively. The N-BaIoT dataset is a sequential and multivariate dataset, which includes 7062606 instances.

The N-BaIoT dataset includes 115 real numbers of attributes attacks, where the tasks are associated with clustering and classification. The original network traffic records in NSL-KDD dataset are stored as 41-dimensional vectors that contain both numerical values and categorical values. The data values present in the dataset for each of the subsets are fed to the pre-processing stage to normalize the data. The table 1 shows the statistical information about the NSL-KDD dataset.

3.2 Pre-processing

Initially, the input data is taken for experimental analysis from the given two datasets. Then the input data is prepossessed to remove the noises and the missing data. In the research, several data Pre-processing methods are utilized such as Data Cleaning, Normalization, Transformation, Integration of data and an explanation for each step for the proposed Hybrid GWO-PSO is given as follows:

3.2.1. Data cleaning

Data cleaning is the process where the data preparation is done that modified the data which were incomplete, incorrect, irrelevant, duplicated or improperly framed. The data is not necessary when it comes to data, analyzing as it would hinder the process of generating inaccurate results. The cleaning of data is not simply erased the accuracy but also for information deleting. The data cleaning includes removal of data, modifying data which are incorrect, erasing the unwanted information without deleting important information. The main objective was to clean the data in the datasets that standardized the data analysis which accessed easily for finding the right data for the query.

3.2.2. Normalization

As the incomplete or uncertain data were present, the missing data were needed to be modified by deleting unwanted data to improve quality. The Min-Max normalization process plays an important role for integration and as well as data normalization. Each and every feature value that is having a minimum value gets transformed into 0 and the maximum value is transformed into 1. All the values will be converted from decimals ranging from 0 and 1. Eq. (1) expresses the normalization process.

$$X_{norm} = \frac{X_i - X_{min}}{X_{max} - X_{min}} \tag{1}$$

Where, X_i is the data point, X_{min} is the minimum value of the data point, X_{max} is the maximum value of the data point or the batch instances. These variables calculate normalized value that fills the missing data using structured data. Once the min max normalization is performed for the unstructured data still more the uncertainty in the data will be present due to contaminated traffic data. Thus, extraction of such features from the various complex structures helps to determine predication of disease.

3.2.3. Discretization

The decentralization process is performed for continuous function expressed in terms of variable, equation for discrete counter parts. The discretization process is known to perform variable modification to category granularity when the multiple discrete variables were summed up. The main aim of the developed model is to reduce the level of the amount considered for modelling uses.

3.2.4. Data transformation

Data transformed into appropriate forms of mining is involved using following discussions:

1. In Normalization, where the attribute data are scaled to fall within a small specified range, such as -1.0 to 1.0, or 0 to 1.0.
2. Smoothing works to remove the noise from the data.
3. In Aggregation, summary or aggregation operations are applied to the data.
4. In Generalization of the Data, low level or primitive or raw data are replaced by higher level concepts through the use of concept hierarchies.

3.2.5. Integration of data

The data integration focus on an exclusive theoretical work for solving the various open problems which were unsolved. The collaboration among the internal as well as external users were done by using the data integration. The data received data were integrated with the heterogeneous database that stored the coherent data for accessing the files of clients.

The Recursive Feature Elimination (RFE) is the feature selection technique that is used to reduce the feature numbers. The RFE specified the feature numbers was not known in advance about the validity and therefore RFE helped to choose and to select the features.

3.3 Feature selection

Once the data are chosen from RFE process, the feature values are automatically contributed to the feature selection process which helps improving the accuracy. The unselected feature values that would be unneeded, redundant or irrelevant, will be no more useful for classification of attacks. Therefore, feature selection techniques are employed for selecting prominent features in order to determine the accuracy in the search space. In order to improve the robustness of the researches, the optimization approaches hybrid exploration algorithms. The optimization algorithms include GWO and PSO that are hybridised together for improving the accuracy.

3.3.1. Particle swarm optimization

The fundamental judgment was inspired primarily by the social behavior of animals such as fish schooling and bird flocking. The birds search for the food thereby moves from one place to another and the bird is able to smell the food wherever is available. The bird is aware of its position and used for finding, managing the food resources. The learning approach from the animal's behavior is calculated using the global optimization approaches where the swarm or crowd will be known as a particle. The PSO technique determines each partner's position in the crowd for searching the space globally is updated using the following Eq. (2) and (3).

$$v_i^{k+1} = v_i^k + c_1 r_1 \left(p_i^k - x_i^k\right) + c_2 r_2 \left(g_{best} - x_i^k\right) \quad (2)$$

v_i^k is the velocity vector of particle
x_i^k is particle's vector position
p_i^k is personal best position of particle
g_{best} is the global best position of particle
t is the time of initialization
c_1, c_2 are positive acceleration constants
$r_1 r_2$ are random numbers

The next position x_i^{k+1} of the particle is calculated based on the previous particle position x_i^k and its velocity v_i^{k+1} is as shown in the Eq. (3).

$$x_i^{k+1} = x_i^k + v_i^{k+1} \quad (3)$$

3.3.2. Grey wolf optimizer (GWO)

The wolves in the groups are ranked as the alpha, beta, omega and remaining subordinate wolves are classified as delta. In GWO, the crowd is split into four different groups such as alpha, beta, delta, and omega which are employed for simulating the leadership hierarchy.

Alpha wolves are the decision makers of the group and controlling all the living activities of the group including the hunt.

Beta wolves are the subordinate to the alpha wolves, they are support the decision made by the alpha wolves

Omega are present in the next rank in the group and they maintain the group dominance hierarchical structure.

Delta are the rest of the wolves' members who are sub-ordinance to the Omega.

GWO solution are divided into the three level based on the fitness and optimal of the solution. Probably the alpha decision is the fittest solution for the optimizing problem. Furthermore, the swarm intelligent methods are used to solve the optimization problem which doesn't have the leader to monitor the entire proceeding period. This limitation is resolved in GWO method; the grey wolves have individual leadership capacity. During implementation, the research study combines the effective optimization algorithm for finding the attacks in IoT.

The swam intelligence improvisations were done using GWO that were inspired by grey wolves and had the capability for solving the real life and standard applications. The GWO variant performed the hunting mechanism thereby maintained the quality of leadership of grey wolves for the nature.

If a wolf is not an alpha (α) or beta (β) or omega (γ) then subordinate δ has to submit for alpha to (α, β,γ). The major steps present in the GWO are the hunting, prey searching, prey attacking and prey encircling that are used for performing optimization. The encircling behavior of each agent of the crowd is as shown in the mathematical Eq. (4) ands (5).

$$d = \left| c \cdot x_{p(t)} - x(t) \right| \quad (4)$$

$$x(t+1) = x_{p(t)} - a \cdot d \quad (5)$$

where d is the encircling behavior of each agent, t is the current iteration, a and c are the coefficient vectors, x_p(t) is the prey's position vector, x is the position of the grey wolf in vector, l is the agent.

The vectors a and c are formulated mathematically as shown in the Eq. (6) and (7)

$$a = 2l.r_1 \quad (6)$$

$$c = 2.r_2 \quad (7)$$

- **Hunting**

In order to mathematically simulate the hunting behavior, an alpha (α), beta (β), and delta (δ) values are computed which gives knowledge for locating the prey's position.

- **Searching for prey and attacking prey.**

The random values lie between $[-2a, 2a]$ and the selected value are compared with the gap. If the random value $|A| < 1$ then the attacks are forced towards prey. If searching the prey is explored, then the attacking ability of the prey will be explored and the values are utilized in order to move against the prey. The population members are enforced away from the prey divergence.

3.3.3. Proposed hybrid optimization algorithm

The hybridization of GWO-PSO algorithm generates a mixed low-level co-evolutionary functionality. The hybrid optimization process lowers the performance as both variants that possessed low functionalities were merged. Based on these modifications, the exploration towards PSO is done in GWO to produce variants strength which will be an added advantage for the mode. The proposed Hybrid GWO-PSO utilized first three agents' position at the search space which is calculated using mathematical equation. The exploration and exploitation of the grey wolf are controlled in the search space by inertia constant w. The modified set of governing equations are (8), (9) and (10).

$$\vec{d}_\alpha = |\vec{c}_1 \cdot \vec{x}_\alpha - w \times \vec{x}| \quad (8)$$

$$\vec{d}_\beta = \left|\vec{c}_2 \cdot \vec{x}_\beta - w \times \vec{x}\right| \quad (9)$$

$$\vec{d}_\delta = |\vec{c}_3 \cdot \vec{x}_\delta - w \times \vec{x}| \quad (10)$$

where, c_3 is the positive acceleration constant, d ⃗_α d ⃗_β,(d) ⃗_δ are the three agents positions, x ⃗ is the vector position.

In order to combine PSO and GWO variants, the velocity and updated equation are proposed as following in the Eq. (11) and (12)

$$v_i^{k+1} = w \times (v_i^k + c_1 r_1 (x_1 - x_i^k) + c_2 r_2 (x_2 - x_i^k) + c_3 r_3 (x_3 - x_i^k)) \quad (11)$$

$$x_i^{k+1} = x_i^k + v_i^{k+1} \quad (12)$$

The fitness function is used to select the best optimum value. In the proposed hybrid optimization algorithm, the Rosen Brock function and the objective function are used for the calculation of the fitness function. Rosen Brock function is efficiently optimized using an adapting appropriate coordinate system without using any gradient information and without building local approximation models f(x) using the following Eq. (13).

$$f(x) = \sum_{i=1}^{N-1} [100(x_{i+1} - x_i^2)^2 + (1 - x_i)^2] \quad (13)$$

where $x = (x_{1,\ldots,} x_N) \in \mathbb{R}^N$ is a rational function

The objective function indicates how much each variable contributes to the value to be optimized in order to overcome the problem. The objective function Z takes the following general form which is expressed as shown in the Eq. (14).

$$Z = \sum_{i=1}^{N} c_i X_i \quad (14)$$

c_i is the objective function coefficient corresponding to the i^{th} variable varies from 1 to N, and X_i is the i^{th} decision variable.

Pseudo code hybrid GWO-PSO

Initialization

Initialize l, a, w and c //w=0.5+$rand()/2$

The fitness of agents is evaluated using the Eq. (11) and (12).

While (t<maximum Number of iterations)

For each search agent

The velocity and position is updated using Eq. (8), (9) and (10)

End for

Update $l, a, w \; and \; c$

The fitness values for all of the search agents are evaluated using Eqs. (13) and (14)

The positions of the first three agents are updated using $t = t + 1$

End while

Return // first best search agent position

By selecting the best set of features from the subset, the uncertainty for information gain is determined.

3.4 Classification using random forest

Once the best optimum values are found, these values are fed into the Random forest classifier for the classification of attacks. The Random forest classifier is having decision trees and therefore lower classification error is present when compared with the existing classification algorithms. An advantage of Random Forest classifier to use in the research work is because an important feature of the developed model is that the RF accuracy will be generated automatically which is crucial for classifying the attacks.

The tree's decision is performed for each of the class object that represents as a vote. The forest selects the class which has received a number of votes for the objects. Therefore, RF utilizes both boosting and bagging as the successful approach select the random variable for building the tree. The features present in the random forest are explained as follows:

Using the Random forest, the generalization error is bound to be dependent mainly on the tree strength that achieves correlation among them. Based on the maximum voting approach, the elements such as i and j are voted in the RF model thereby classifies the attacks using the following Eq. (15).

$$prox(i,j) = \frac{\sum_{t=1}^{ntree} \mathrm{I}\,(h_t(i) = h_t(j))}{ntree} \qquad (15)$$

where $I(\cdot)$ represents the indicator function,

h_t represents the tree of the forest

$h_t(i)$is the value which is predicted for all the values of i

If $prox(i,j)$ = 1 then the classes i and j of the same classes are classified

Therefore, RF provides the important rank which will be variable and that is used to select the important features.

4. Results and discussion

The of proposed hybrid optimization method is simulated using Anaconda navigator and python 3.6 software with the system requirements; operating system: windows 10, RAM: 128 GB, processor: Intel core i9 with 3GHz, and hard disk: 4 TB. In this work, the proposed hybrid optimization model performance is compared with a benchmark model to validate the performance of hybrid optimization model. In this research study, NSL-KDD and N-BaIoT datasets are undertaken for testing.

The proposed method evaluates the results using the following parameters:

- **Accuracy:**

Accuracy is defined as the ratio of correctly predicted to the total number of observations. The accuracy is calculated using the Eq. (16).

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \times 100 \qquad (16)$$

- **Recall**

The ratio of correctly predicted fault-modules is defined as recall. The proportion of actual positives is correctly predicted using recall, which is shown in Eq. (18).

$$Recall = \frac{TP}{TP + FN} \times 100 \qquad (17)$$

- **F 1-measure**

The harmonic mean of recall and precision is defined as F1-Measure, which is shown in Eq. (19).

$$F1 - measure = \frac{2 \times Precision \times Recall}{Precision + Recall} \times 100 \qquad (18)$$

- **Area under the curve**

Area Under the Curve (AUC) provides an aggregate measure of possible classification thresholds, which calculated using the Eq. (20).

$$AUC = \int_a^b f(x)\,dx \times 100 \qquad (19)$$

The AUC is determined by using the curve equation y=f(x) that ranges among x=a and x=b. The

Table 1. The multi classification results of NSL-KDD Experiment

Classifiers	Attacks	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)	AUC (%)
Gradient Boosting Classifier	DoS	97.19	99.66	95.42	97.47	99.35
	Probe	83.43	90.77	66.25	69.54	78.68
	R2L	98.53	98.95	97.41	98.14	97.76
	U2R	99.87	99.87	99.87	99.86	98.56
AdaBoost Classifier	DoS	97.50	98.93	96.63	97.77	99.10
	Probe	85.20	87.56	85.20	82.66	79.60
	R2L	98.42	98.44	98.42	98.41	97.96
	U2R	99.65	99.00	81.30	87.20	97.56
Proposed Method	DoS	99.47	99.89	99.18	99.53	99.77
	Probe	85.44	87.88	85.44	82.99	79.75
	R2L	98.81	99.18	97.88	98.50	98.66
	U2R	99.96	99.27	98.57	98.89	99.99

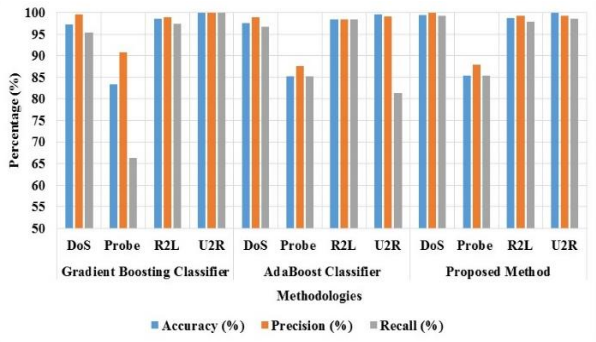

Figure 3. Comparison of the performance measure with respect to the existing and proposed method for multi classification

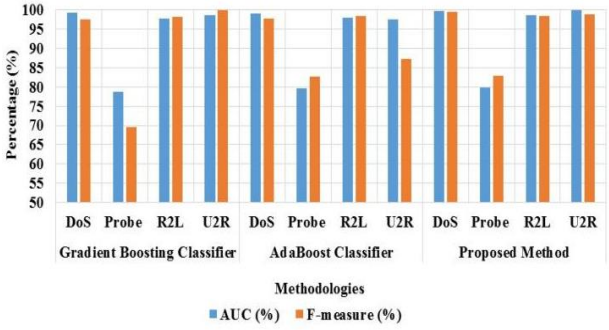

Figure 4. Comparison of the AUC and F-measure with respect to the existing and proposed method

integration of the function operating among the limit x=a and x=b. Areas under the x-axis will be a negative area and x-axis above the axis will be positive.

FN, FP, TP, & TP denoted as number of False Negatives, False Positive, True Positive and True Negative respectively.

4.1 Quantitative Analysis for NSL-KDD dataset

Table 2. classification results of N-BaIoT-experiment

Metric (%)	Gradient Boosting Classifier	AdaBoost Classifier	Proposed Method
Accuracy	99.54	99.30	99.86
Precision	99.91	99.91	99.94
Recall	99.91	99.91	99.94
F1 Measure	99.55	99.91	99.86

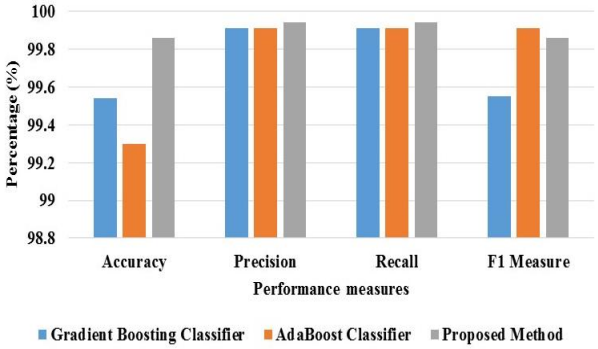

Figure 5. Comparison of performance measures with respect to the existing and proposed method

The results obtained for the proposed Hybrid optimization model in terms of the performance obtained for binary classification to NSL-KDD dataset, the experimental outcomes are evaluated.

Table 1 is for the multi classification of attacks are evaluated for NSL-KDD dataset and the results are validated for the attacks such as DoS, Probe, R2D and U2R. The results are evaluated for all the attacks in terms of accuracy, precision, recall and F-measure. Fig. 3 shows that the proposed method achieves better results when compared with the existing methods Gradient Boosting Classifier and AdaBoost Classifier. Fig. 4 presented the comparison result to existing method in terms of multi classification, AUC & F-measure.

Table 3. Comparative analysis for the existing methods and the proposed hybrid GWO-PSO method for both Binary (B) and Multi (M) classification results using NSL-KDD-experiment

Metric (%)	DNN (Wisam Elmasry) [19]	LSTM-RNN (Wisam Elmasry) [19]	DBN (Wisam Elmasry) [19]	Proposed Method
Accuracy (B)	97.72	98.8	99.79	**99.98**
Accuracy (M)	96.25	97.44	98.77	**99.97**
Precision (B)	99.6	99.7	99.83	**99.87**
Precision(M)	93.86	95.85	98.1	**99.95**
Recall (B)	96.38	98.18	99.81	**100**
Recall(M)	80.61	86.19	92.29	**99.97**
F1 Measure (B)	97.96	98.94	99.82	**99.73**
F1 Measure(M)	86.73	90.76	95.11	**99.96**

4.2 Quantitative analysis for N-BaIoT dataset

The results for the proposed hybrid GWO-PSO method are evaluated in terms of Accuracy, Recall, Precision, F-measure and Error Rate using the N-BaIoT datasets. The values obtained for the proposed method are evaluated and tabulated in the table 2 and shown in Fig. 5.

4.3 Comparative analysis

The Table 3 shows the results obtained in the existing methods DNN, LSTM-RNN, RNN [19] are compared with the proposed hybrid optimization algorithm using NSL-KDD dataset. The proposed hybrid GWO-PSO obtained better accuracy of 99.98% when compared to existing methods DNN, LSTM-RNN, and DBN that obtained accuracy of 97.72 %, 98.8 % and 99.79% of accuracy respectively.

Table 4 shows the Comparative analysis for the existing method and Multi classification of attacks using NSL-KDD dataset.

The proposed hybrid GWO-PSO has obtained better accuracy of 99.98 % of average accuracy for Multi-class which showed better when compared with the existing LSTM-RNN, Modified rank-based information gain feature with SVM and ML-DR with SVM obtained accuracy of 98.8 %, 99.8 %, and 98 %.

Wisam Elmasry [19] classified only few types of attacks for the testing set rather than in the training set examined but the ability to classify the attacks were failed. Bambang Setiawan [20] developed a modified rank-based information gain feature selection method that used log normalization, and SVM showed optimization problems for the trained parameters. Bukka Narendra Lastly, Kumar [21] developed ML-DR with multi class SVM showed classification results lowered due to non-consideration of discriminant vectored feature. Whereas, the proposed hybrid GWO-PSO extensively trained the data that utilized the data for training and also for data estimation. The GWO classified efficiently the data based on several intrusions and improved the system and classification performance. Fig. 6 presented the comparison result of proposed method to existing method NSL-KDD for multi classification of attacks.

Table 4. Comparative analysis for the existing method and Multi classification results of NSL-KDD-experimentt

Authors	Methodology	Accuracy (%)
Wisam Elmasry [19]	LSTM-RNN	98.8
Bambang Setiawan[20]	Modified rank-based information gain feature and SVM	99.8
Bukka Narendra Kumar [21]	ML-DR with multi SVM	98
Proposed	**Hybrid GWO-PSO**	**99.98**

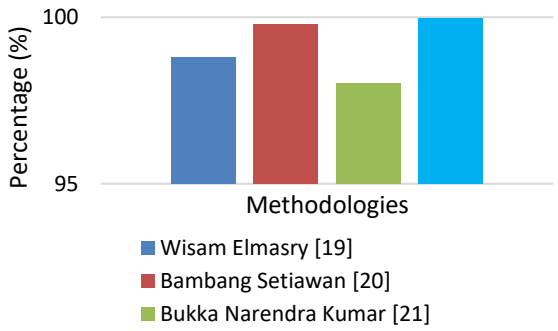

Figure. 6 Comparison of the performance measures with respect to the existing and proposed method

5. Conclusion

IoT have a uniquely assigned IP address through which they can communicate to the external entities (i.e., user of a smart home) of the network. The IoT environment ranges from high-end computing systems to the basic microprocessors with low memory and computational capacity. The security issues in the IoT devices are of big concern because the number of attacks being launched in the IoT

environment are increasing rapidly. The attackers through the internet intrude the attacks and preventing these attacks at an early stage will make the data secure. The capabilities of devices at different levels of IoT varies, hence, implementing security mechanisms at the different level will have different dimensions and properties. But, the existing mechanisms are not sufficient for the IoT malware detection and analysis. The DDoS attacks in IoT environments occur because of the lack of strong security monitoring and protection techniques. In this research proposal, a hybrid GWO-PSO optimization algorithm is used to detect the attacks such as DoS, Probe, R2L and U2R Random forest which gives better results in terms of accuracy when compared to the existing methods. The proposed hybrid GWO-PSO extensively trained the data and was used for data estimation. The GWO classify efficiently the data based on several intrusions and improved the system and classification performance. The results obtained better accuracy value of 99.97 % when compared to the existing LSTM-RNN that achieved 97.72% of accuracy, multi class SVM obtained 98 % and modified rank-based information gain feature selection method showed 99.8%. In future, the complexity of the system can be improved for better performance and results.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper background work, conceptualization, methodology, dataset collection, implementation, result analysis and comparison, preparing and editing draft, visualization have been done by first author.

The supervision, review of work and project administration, have been done by second author.

References

[1] J. Alzubi, J. Selvakumar, O. Alzubi, and R. Manikandan, "Decentralized Internet of Things", *Indian Journal of Public Health Research and Development*, Vol. 10, No. 2, 2019.

[2] C. Luo, Z. Tan, G. Min, J. Gan, W. Shi, and Z. Tian, "A Novel Web Attack Detection System for Internet of Things via Ensemble Classification", *IEEE Transactions on Industrial Informatics*, 2020.

[3] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network", *IEEE Access*, Vol. 8, pp. 77396-77404, 2020.

[4] S. Deshmukh-Bhosale and S. S. Sonavane, "Design of Intrusion Detection System for Wormhole Attack Detection in Internet of Things", *Advanced Computing and Intelligent Engineering*, pp. 513-523, 2020.

[5] A. Amouri, V. T. Alaparthy, and S. D. Morgera, "A Machine Learning Based Intrusion Detection System for Mobile Internet of Things", *Sensors*, Vol. 20, No. 2, pp. 461, 2020.

[6] B. Mbarek, M. Ge, and T. Pitner, "Enhanced network intrusion detection system protocol for internet of things", In: *Proc. of the 35th Annual ACM Symposium on Applied Computing*, pp. 1156-1163, 2020.

[7] M. Roopak, G. Y. Tian, and J. Chambers, "Multi-objective-based feature selection for DDoS attack detection in IoT networks", *IET Networks*, Vol. 9, No. 3, pp. 120-127, 2020.

[8] A. Kore and S. Patil, "IC-MADS: IoT Enabled Cross Layer Man-in-Middle Attack Detection System for Smart Healthcare Application", Wireless Personal Communications, pp. 1-20, 2020.

[9] M. H. Shahriar, N. I. Haque, M. A. Rahman, and M. Alonso Jr, "G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System", *arXiv preprint arXiv:2006.00676*, 2020.

[10] Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system", *Simulation Modelling Practice and Theory*, Vol. 101, pp. 102031, 2020.1

[11] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System", *IEEE Access*, Vol. 8, pp. 83965-83973, 2020.

[12] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city", *Future Generation Computer Systems*, Vol. 107, pp. 433-442, 2020

[13] D. McDermott, J. P. Isaacs, and A. V. Petrovski, "Evaluating awareness and perception of botnet activity within consumer internet-of-things (IoT) networks", In*: Proc. of Informatics Multidisciplinary Digital Publishing Institute*, Vol. 6, No. 1, pp. 8, 2019.

[14] J. A. Alzubi, R. Manikandan, O. A. Alzubi, N. Gayathri, and R. Patan, "A Survey of Specific IoT Applications", *International Journal on*

Emerging Technologies, Vol. 10, No. 1, pp. 47-53, 2019

[15] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks", *Electronics*, Vol. 8, No. 11, pp. 1210, 2019.

[16] P. P. Ioulianou and V. G. Vassilakis, "Denial-of-Service Attacks and Countermeasures in the RPL-Based Internet of Things", *Computer Security*, pp. 374-390, 2019.

[17] G. Spathoulas, N. Giachoudis, G. P. Damiris, and G. Theodoridis, "Collaborative Blockchain-Based Detection of Distributed Denial of Service Attacks Based on Internet of Things Botnets", *Future Internet*, Vol. 11, No. 11, pp. 226, 2019.

[18] R. Gassais, N. Ezzati-Jivan, J. M. Fernandez, D. Aloise, and M. R. Dagenais, "Multi-level host-based intrusion detection system for Internet of things", *Journal of Cloud Computing*, Vol. 9, No. 1, pp. 1-16, 2020.

[19] W. Elmasry, A. Akbulut, and A. H. Zaim, "Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic", *Computer Networks*, Vol. 168, pp. 107042, 2020.

[20] B. Setiawan, S. Djanali, and T. Ahmad, "Increasing accuracy and completeness of intrusion detection model using fusion of normalization, feature selection method and support vector machine", *International Journal of Intelligent Engineering and Systems*, Vol. 12, No. 4, pp. 378-389, 2019.

[21] B. N. Kumar, M. S. V. S. B. Raju, and B.V. Vardhan, "Enhancing the performance of an intrusion detection system through multi-linear dimensionality reduction and Multi-class SVM", *International Journal of Intelligent Engineering and Systems*, Vol. 11, No. 1, pp. 181-192, 2018.