ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 12 (2022) No. 4, pp. 383-397
DOI:10.33168/JSMS.2022.0423

Hybrid Pigeon Inspired Optimizer-Gray Wolf Optimization for Network Intrusion Detection

Sasikumar Gurumurthy[1], Hemalatha K. L.[2], D. Pamela[3], Upendra Roy[4], Vishwanath P.[5]

[1]Department of Computer Science and Engineering, Jerusalem College of Engineering, Chennai - 600100, Tamil Nadu, India

[2]Department of ISE, Sri Krishna Institute of Technology, Bengaluru 560090, India

[3]Department of Biomedical Engineering Karunya Institute of Technology and Sciences, Coimbatore - 641114, Tamil Nadu, India

[4]Department of Electrical and Electronics Engineering, Channabasaveshwara Institute of Technology, Tumkur, Karnataka 572216, India

[5]Department of Electronics and Communication Engineering, H.K.E.S’s S.L.N. College Of Engineering, Raichur, India

sasichief@gmail.com (Corresponding author)

Abstract. The physical objects like smart home appliances many more are present in the Internet of Things (IoT). The network has an assigned Internet Address (IP) uniquely that communicates through the external entities of user from a smart home in a network for exchange in data via internet. The IoT devices face an issue that are increased rapidly due to intruders or attackers such as Distributed Denial-of-Service (DDoS) attacks occurring at IoT environment. It has occurred due to the strong and security monitoring protection techniques. Thus, it is important for providing security during IoT attack detection. The hybrid optimization approach was used that is a combination of Pigeon Inspired Optimizer (PIO) and Gray Wolf Optimization (GWO) that is developed for detecting intrusion attacks. The Cosine-Similarity fitness function selects an optimal value during feature selection and the features are fed for the Multi-Support Vector Machine (M-SVM) for the attacks classification. Finally, results showed that the proposed hybrid PIO-GWO obtained better accuracy of 96.94 % better than the existing ensemble learning model of 96 %.

Keywords: attacks, cosine-similarity fitness, internet of things, Pigeon Inspired Optimizer (PIO), Gray wolf optimization, security issues.

1. Introduction

Recently, the cyber-attacks occurred against the infrastructure of the cloud that resulted with the massive data due to breaches cost billion dollars which were exposed with various sensitive documents. The most of the attacks were due to the customer misconfigured cloud resources such as publicly exposed databases, over-privileged users, lacked in audit logging etc., thus it is required for Cloud Security Alliance (CSA)'s that identified data breaches. It is because of misconfiguration and changes in the control that gave rise to severe cloud security threats. There are several attacks present for the cloud computing platform that gave rise to DDoS was the typical attack affected services (Zhang et al., 2019; li et al., 2020; Balakrishnan 2019). The DDoS attack is referred as an attack which considered vulnerable hosts of thousands that carried out it as a vulnerable host that carried out the attacks in the devices (Otoum et al., 2019). The main reason for rise in the security issue is due to the increased DDoS attacks with respect to the cloud platform for significant extortion of security. The hack information diverted the users by diverting the data traffic from an attacker. The business Intrusion Detection System (IDS) has exploited a rule based database known as the signature based IDS that showed a challenge in discovering the intrusions in the network on the basis of host based system (Aljawarneh et al., 2018). Thus, the detection scheme is clear and required to clear cut to provide cloud security and showed challenges to side step to protect for proficient users as it is discrepancy to recognize the attacks. Thus, these were the motives to aid a technique for ascertain without losing anyone for early model attacks detection.

The IDS should detect the competence for the detection of all the newly perceived with ordinary attacks without any failure. There is machine learning model has provided a careful consideration that has been placed with two categories on the basis of detection method. The classification process is defined with the procedure for finding DDoS attack that detected attack differentiated the multiple objects (Elmasry et al., 2020). The distinct classifiers such as Naïve Bayes, K-Nearest Neighbor, Least Square Support Vector Machine (LS-SVM), and Multi-Layer Perceptron were used that performed the process of attacks or threat classification. The contribution of the research is as follows:

- To present a research that introduced PIO feature selection which aimed for number of feature reduction that build a IDS robustly when maintaining the detection rate showed low false alarm and accuracy.
- To develop GWO as an IDS to classify the data efficiently with various number of intrusions.
- To hybrid PIO-GWO algorithm selected an optimal value for selecting the features based on the Cosine –similarity fitness function. The PSO algorithm showed faster speed during computation that was extensively used for training, estimating, and detection with wide range of disciplines. Additionally, the

GWO developed IDS to classify the data efficiently for detection of various intrusions. The GWO developed an intrusion detection approach that classified the data efficiently based on various intrusions.

The research work structure is as follows: section 2 is the literature review on the existing models that were involved for attack detection. The section 3 is the proposed method section that explains about the steps involved in the research. The section 4 discusses about the results and discussions for the proposed research. At last, the section 5 is the conclusion and future work of the research.

2. Literature Review

The existing researches based on NIDS using Machine learning models are as follows:

KA Torkura et al (2021) performed Continuous Auditing and Threat Detection in Multi-Cloud Infrastructure. The developed Cloud Storage Broker (CSB) using Cloud RAID which is a security system in cloud which monitors its infrastructure to detect malicious attacks that changes with respect to the unauthorized users. The developed CSBAuditor evaluated using certain strategies that employ Infrastructure as Software (IaS), however the reversibility strategy needed better guidance and handle systematically for practitioners in IaS.

S. Krishnaveni et al (2021) developed an Ensemble approach for threat detection occurring in the network and also classify the attacks on cloud computing. The developed model classified the known and unknown malicious network streams. The developed Ensemble approach classified the network attacks by segregating into 4 classes such as Remote to local (R2L), denial of services (DoS), User to root (U2R), and probe to meet the goal overcame the end in building the IDS model effectively. However, the model failed to select and implement the model thereby the performance of the system was lowered as the best features were not selected in the model.

S. Velliangiri et al (2021) developed a model that detected the DDoS attacks in cloud computing environment using the Taylor-Elephant Herd Optimization-Deep Belief Network (TEHO-DBN). The developed TEHO-DBN model was the modified version of Elephant Herd Optimization (EHO) technique is done by updating the Taylor series in the algorithm and the data obtained were adopted for training DBN for detection of attacks. However, due to low training the network was sophisticated from the attack detection in the cloud computing network.

Hadeel Alazzam et al (2020) developed Pigeon Inspired Optimization (PIO) algorithm for threat detection and intrusion detection which acted as a feature selection process. The developed PIO showed the convergence speed faster as the discretization process and the sigmoid function was used in the developed model. However, the developed model which used optimization algorithm for intrusion detection used excessive CPU usage and also the I/O components for various instances that negotiated the positive effects that lead to challenges.

Sasha Mahdavi Hezavehi et al (2020) developed an anomaly based framework for various attacks mitigations such as DDoS using the TPA for cloud computing environment. The developed Anomaly based attack detection framework for cloud environment using the TPA. The model made various assumptions and configurations in cloud environment for performing simulations tests in evaluating the results. However, distinct effects caused in different CSPs deployment for attack detection was not much effective using the developed model.

3. Proposed Model

The proposed method block diagram is shown in the figure 1 which consists of the following steps such as dataset, pre-processing, feature extraction, feature selection, and classification. The classifier classified the attacks into DoS, R2L, Probe, U2R.

3.1. Dataset

The NSL-KDD is a type of dataset which has been used in IoT environment. There are distinct parts present that are having KDD cup 99 dataset for performing redundancies and duplications (2009). There are mainly 4 types of attacks like DoS, R2L, U2R, and probe attack.

Probe attack:

The network is scanned that is misused by the collection of the information in the network weaknesses. The attacks presented in probe are as follows: Satan, Portsweep, Mscan, Ipsweep, Saint, and Nmap are the types of attacks which are present in probe attack.

R2L: The transmission of packets to the machine for detecting the weakness with respect to the user account in a network. There are various attacks present in R2L that includes Snmpget attack, Send mail, Warez client, Phf, Snmpguess, Ftp-write, Guess-Password, Imap, Xsnoop, Spy, Httptunnel, Multihop, Warezmaster, and Xlock.

U2R: The U2R has the accesses the root. The U2R attacks are having load module, rootkit, buffer overflow, sqlattacks, and Ps.

DoS: The network traffic usage is increased that has provided the service that was not provided with a system resulted with the DoS attacks. There are different types of DoS attacks such as Apache2, Neptune, Land, Udp storm, Back, Teardrop, Worm, Smurf, and Pod.

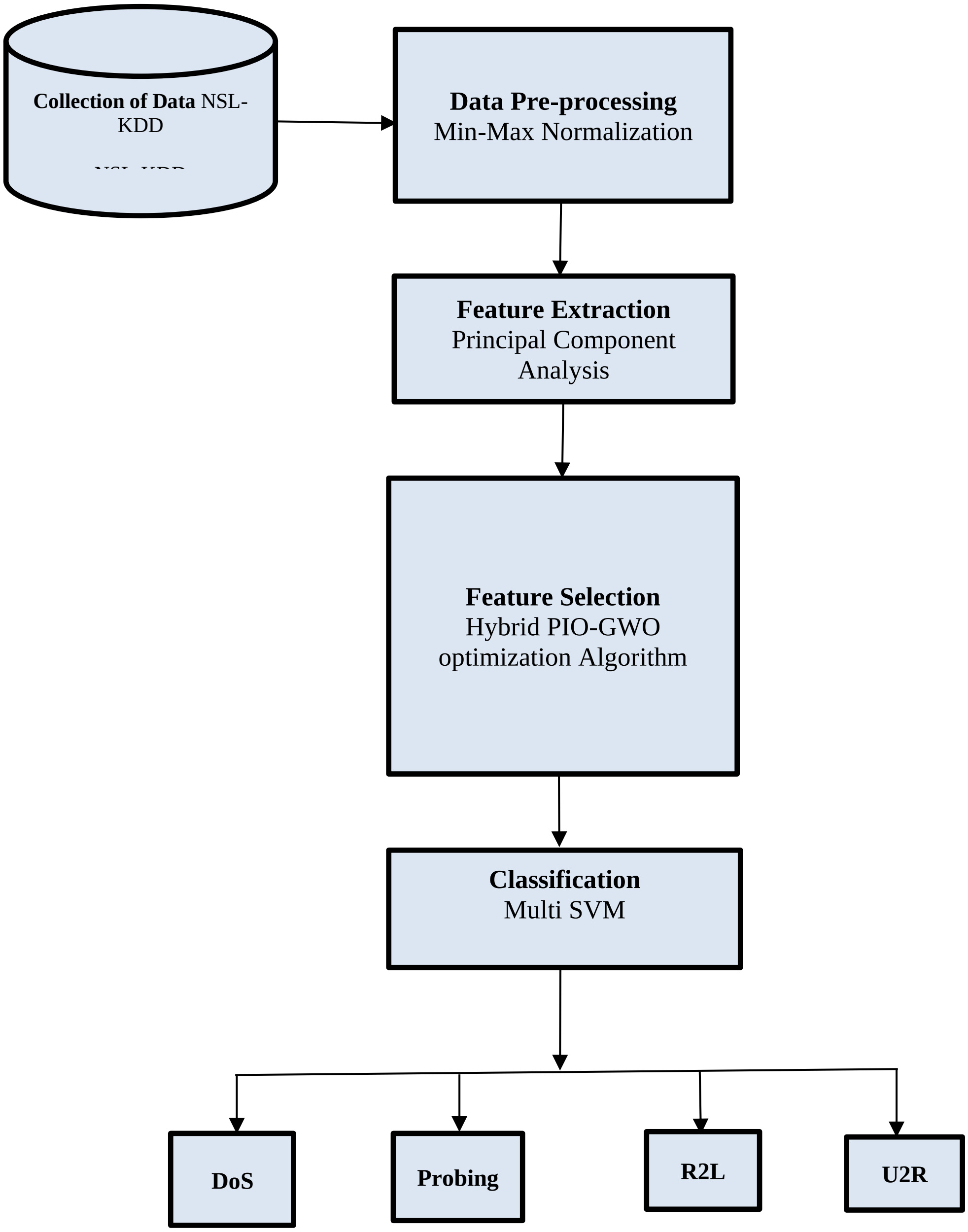

Fig. 1: Block diagram of the proposed method.

3.2. Pre-processing

Initially, the data is taken in the experiment that is provided with the two datasets. The data which is taken as an input is pre-processed to remove the noise. Thus, in the research, various data is pre-processed by utilizing the normalization technique.

3.2.1. Normalization

The examination of a large data is important for accurate attacks determination. If the data is missing in the dataset, the human error has been occurred that give rise to database failure in the system. To overcome the problem, the missing data is defined with a structured data showed uncertain and incomplete data. It should be modified with missing data by unwanted data removal and improving the quality. The process of Min-max normalization is performed which played an important role for data normalization. Each of the value of the features are having a value with minimum is transferred to either maximum value of 1 or minimum value of 0. These values converted 0 to 1. The process of normalization is expressed as shown in the below Eq. (1)

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

Where, $X_i$is the data point, $X_{min}$is known as the data point with minimum value, $X_{max}$is the maximum value of the data point or the batch instances. These variables calculate normalized value known as missing data performed uncertainty in unstructured data because of the traffic data contamination. Therefore, the extraction of features with complex structure has helped for disease predication.

3.3. Feature extraction using principal component analysis

The process of removing irrelevant and redundant features using dimensionality reduction techniques plays an important role. It is an important step to apply learning algorithm and the attribute space reduction has lead the model different with higher classification accuracy. The dimensionality reduction is the most popular technique for removing the features and is the prior step to apply it for learning model. The attribute space reduction has lead a model better with highest accuracy in classification showed less time. The linear transformation technique used is PCA that transforms the data such that the data with first co-ordinate is representing the data with the highest variance, co-ordinate represents data with second variance etc., Thus, PCA reduced the large dimensions in the dataset that considered the co-ordinates with high variance value and ignored the data with a lower variance. The PCA model can be represented by using the below equation (2)

$$u_{mx1} = W_{mxd} x_{dx1} \tag{2}$$

Where u is an m-dimensional vector which is the projection of x having the original dimensional data vector d where ($m \ll d$)

From the equation m is known as the projection vectors which maximizes the variance u which is given by using the equations Eigen Vectors $e_1, e_2, \ldots., e_m$ of the dataset's covariance matrix S that will corresponds to m largest non-zero Eigen values that are represented as $\lambda_1, \lambda_2, .. \lambda_m$. The covariance matrix S for the dataset is represented by using the equation (3)

$$S = \frac{1}{n-1} \sum_{i=1}^{n} (x-\mu)(x-\mu)^T \tag{3}$$

where μ is the mean vector of x.

The eigenvectors e_i are calculated by solving the following equation (4)

$$(S - \lambda_i I) e_i = 0 \tag{4}$$

Where $i = 1,2, \dots, d$

From the equation λ_i is the Eigen values belonging to th Covariance matrix S. Based on the magnitude values of Eigen vectors they are sorted out. The largest Eigen values from the m vectors are chosen and the PCA matrix is calculated using the below equation (5)

$$W = E^T \tag{5}$$

Where E has the m eigenvectors which are in columns and W is a $m \times d$ matrix.

Pseudo code for PCA algorithm

Step 1: Use NSL-KDD dataset and acquire data

Step 2: The mean is subtracted by using Eq. (6)

$$\bar{X} = \frac{\sum_{i=1}^{n} X_i}{n} \tag{6}$$

Step 3: The evaluation of covariance matrix is evaluated.

Step 4: The Eigen vectors and values of the covariance matrix are evaluated.

Step 5: The feature vectors are generated and are chose the components that are having signal values and the generated features are the principal components.

Step 6: The data generated are later obtained by multiplication of old data with received components obtained in step 5.

3.4. Feature selection

The data chosen through the process of PCA is now automatically processed to improve the selected accuracy. The feature values were unselected that would be unneeded, irrelevant, or redundant attributes which is not useful to classify the attacks. The robustness of researches is improved by the process of optimization algorithm by using a hybrid exploration algorithm.

3.4.1. Pigeon inspired optimizer

The pigeons use the reception senses of magnetic field in the earth that has the ability in the magnetic field beside the pigeons that perceive the altitude. It compasses for adjusting in their direction. It has the ability for sensing earth that increase in the pigeons that can do. The pigeons have become closer with the destination and are dependent on the map for compassing operator. It is followed for finding the pigeon’s best position. The positions of all the pigeon are evaluated by using the fitness function. The best pigeon will be the black pigeon that will be followed by other pigeon which is as illustrated by using the below equations. The equation at its first part is represented with the current direction of the pigeon and the second part is the best pigeon direction.

From the above mentioned steps, the summation of the vectors present is in the direction of flying pigeon. The pigeons adjust their position in accordance with the new direction and are ranked as per the fitness value. The pigeons number are updated and half number pigeons were considered to calculate the position of wanted ones from the centered pigeon. The other pigeons are adjusted with their positions by calculating with other pigeons are updated towards their position. The destination position with desirable range is represented with the help of black pigeon that is represented in the half number of pigeon circled calculated using equation (7)

$$N_p(t+1) = \frac{N_p(t)}{2} \tag{7}$$

Where N_p is the total number of pigeons for the t^{th} iteration

$$X_c(t+1) = \frac{\sum X_i(t+1) \cdot Fitness(X_i(t+1))}{N_p \sum Fitness\ (X_i(t+1)} \tag{8}$$

Where X_c is centered position of the desired pigeons

X_i is the current positions for all the pigeons calculated using Eq. (9)

$$X_i(t+1) = X_i(t) + rand\ (X_c(t+1) - X_i(t)) \tag{9}$$

3.4.2. Grey wolf optimizer (GWO)

The groups of wolves were ranked as Alpha, Beta, omega, and the other were remained as a subordinate wolf that were known as delta. The crowd splits to distinct groups like beta, omega, alpha, delta were employed for performing simulation.

- The Alpha wolves makes the decision for the group to control the activities of living for a group that included the hunt. The Alpha wolves are known as the dominator male or female wolf, head in a group.
- The Beta wolves have alpha wolves which are the subordinates which are supported with the decision made by the wolves. The Beta Wolves are the potential candidate mainly to support the cause of the alpha. The role of the Beta is to support the alpha as supporter and lead the team as in the decision is taken by alpha.
- The Omega wolves rank next in a group that has been maintained with group dominance of hierarchical structure.
- The Delta wolves that are remaining in a groups which are classified as the delta wolves and are the sub-ordinance with the omega wolves.

The alpha (α) wolves are liable generally to make the decision for time to wake, sleep, hunting, etc., The second top level is the grey wolves (β) present in the hierarchy. The sub-ordinates with the wolves helped for finding the levels to make a decision or with the pack actions. The wolf (β) is at the second level reinforces (α) as the first level which orders thoroughly the pack and shows a feedback for the alpha. The next level ranking grey wolf is known as the omega where the wolf is playing the scapegoat role. The grey level wolves are submitting the dominant wolves that are having the third level wolves showed significance. It showed significance in personality but it is also observed with the entire pack faces. The entire pack struggle the troubles for losing which is because of frustration and violence with all wolves with the value of omega (γ). The value is fulfilled with the whole pack to maintain the dominance structure. The encircling behavior of each agent within the crowd evaluates based on the mathematical equations (10) and (11)

$$d = \left|c \cdot x_{p(t)} - x(t)\right| \tag{10}$$

$$x(t+1) = x_{p(t)} - a \cdot d \tag{11}$$

From the above Eq. (10 and 11), the current iteration t, the coefficient vector a and c, the prey's position is represented as $x_{p(t)}$, x represents the grey wolf position in vector. Mathematically, vectors, a and c are represented as shown in the below Eq. (12) and (13)

$$a = 2l.r_1 \tag{12}$$

$$c = 2.r_2 \tag{13}$$

3.5. Classification using multi SVM

The volume of data is necessary to train that varies according to the attack type used. The training results for the attack type is affected with the volume of data that is owed to unbalance the size of training data. Additionally, the current training data represented the whole class due to the new type of attack that is included in the attack class. It is emerged and increasing thus, the binary classifier is subjected for misclassification. It is created and the binary classifier known as SVM is subjected for misclassification that is created with the decision boundary that included the unobserved area. Therefore, it is important to select the decision boundary using the one-class SVM [8] which has expressed the corresponding class. The present research work uses a multi class SVM that classified the attacks into different types. There are k-dataset having the patterns with d-dimensional input space as N_k, present in the d-dimensional input space with $D_k = \{x_i^k \in R^d | i = 1, \ldots, N_k\}$; $k = 1, \ldots, K$. The multi class SVM classified the class as a problem for obtaining a sphere which minimized the volume that includes the training data. It is formalized through the problem of optimization which has evaluated using the Eq. (14)

$$\min L_0\left(R_k^2, a_k, \xi_k\right) = R_k^2 + C \sum_{i=1}^{N_k} \xi_i^k \; \left|x_i^k - a_k\right| \tag{14}$$

$$\left||x_i^k - a_k|\right|^2 \leq R_k^2 + \xi_i^k, \xi_i^k \geq 0, \forall_i \tag{15}$$

From the above Equations, a_k is known as the sphere's center with k^{th} class, R_k^2 represents the square value having the radius of sphere, ξ_i^k is known as the penalty term that showed the training data of i^{th} term, x_i^k is pertained with the k^{th}class which is deviated with the sphere having the tradeoff constant as C.

4. Results and Discussion

The system specifications required for the proposed hybrid PIO-GWO optimization algorithm for attacks and threat detection is as shown in the table 1. The proposed hybrid optimization is simulated by using the Anaconda navigator and python 3.6 software which is working with windows 10 that has 128 GB RAM, 1 TB memory that operated with i9 processor having 3 GHz. The benchmark model is validated to analyse the performance that undergoes for testing using NSL-KDD. The dataset has mainly 53873 normal records for training and validation subset consisted of 6735 of normal records and 6735 of anomaly records.

4.1. Performance evaluation

The results evaluated for the proposed method are in terms of the following. The equations represented are as follows (16-19) :

$$Accuracy = \frac{(TP+TN)}{(TP+TN+FP+FN)} \quad (16)$$

$$F1 - measure = \frac{2 \times TP}{2 \times TP+FP+FN} \quad (17)$$

$$Sensitivity = \frac{TP}{TP+FN} \quad (18)$$

$$False\ Alarm = \frac{FP}{TN+FP} \quad (19)$$

True Positive (TP)

True Negative (TN)

False Positive (FP)

False Negative (FN)

4.2. Quantitative analysis

The proposed hybrid PIO-GWO is used for threat detection and attacks detection evaluated in terms of Sensitivity, False Alarm, Accuracy, and F-score that obtained results as 91.7 %, 9.4%, 96.09 %, 96.4 % which is shown in table 2. There were many features consisting of low samples or features that ratio introduce noise to the dataset. That is the reason the classification algorithm overfit the model showed lower performances. The number of feature reduced the running time and enabled the algorithm having higher complexity for more hyper parameters for evaluations. The feature numbers are reduced that in turn reduces the running time having the later stages. This in turn enabled the use of algorithm showed complexity at higher rate and the more hyper parameters were used for more evaluations. The present research work without using feature selection algorithm obtained the Sensitivity of 85.7 %, False Alarm of 15.4%, Accuracy of 90.94 %, and F-score of 91.4 %. The table 2 shows results evaluation in terms of performance measures evaluated in terms of Sensitivity, False alarm, Accuracy, and F-score without feature selection algorithm.

Table 2: The results evaluation for the performance measures in terms of sensitivity, false alarm, accuracy, and f-score without feature selection algorithm.

Performance measure	Percentage (%)
Sensitivity	85.7
False Alarm	15.4
Accuracy	90.94
F-score	91.4

Similarly, with the PIO-GWO hybrid feature selection algorithm showed an effective way to overcome the problem eliminated the irrelevant and redundant data. The irrelevant data has showed improvement in terms of accuracy, reduced the computation and facilitated the model by enhancing the learning rate of the model. The present research work without using feature selection algorithm obtained the Sensitivity of 91.7 %, False Alarm of 9.4%, Accuracy of 96.94 %, and F-score of 96.4 %.

Table 3: Quantitative analysis in terms of sensitivity, false alarm, accuracy, and f-score obtained during classification using PIO-GWO.

Performance measure	Percentage (%)
Sensitivity	91.7
False Alarm	9.4
Accuracy	96.94
F-score	96.4

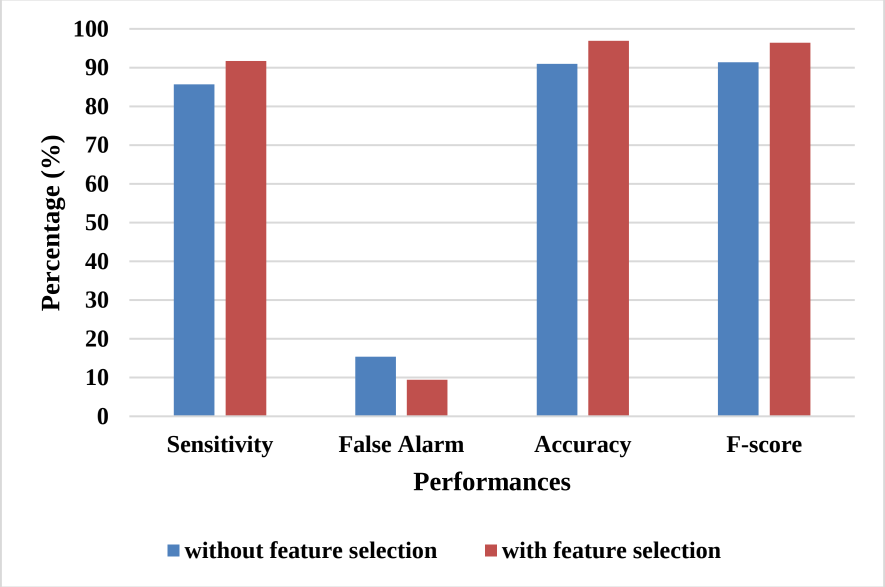

Fig. 2: Analysis of performances with and without PIO-GWO feature selection algorithm.

4.3. Comparative analysis

The proposed research and the existing researches is compared in terms of accuracy shown in table 3. The proposed Hybrid PIO-GWO obtained accuracy of 96.94 % whereas the exisitng models such as Ensemble Learning method achieved accuracy of 96.062%, TEHO-DBN obtained accuracy of 83 %, PIO obtained accuracy of 86.9%. The results showed that present research obtained better attack detection rate when compared with the existing models. The existing models showed lower performances due to more presence of features that gave rise to complexity in the system. However, the redundant features were removed by the proposed PIO-GWO with the help of Cosine Similarity function improved the level of accuracy compared to the existing models. The figure 4 shows the comparison graph for the exisitng and the proposed hybrid PIO-GWO.

Table 3: Comparative analysis.

Methodology	Accuracy (%)	FAR (%)	F-score (%)	Sensitivity (%)
Ensemble Learning method [12]	96.062	0.076	NA	93
TEHO-DBN [13]	83	NA	NA	89
Pigeon Inspired Optimizer [14]	86.9	NA	86.4	81.7
Proposed Hybrid PIO-GWO	96.94	9.4	96.4	91.7

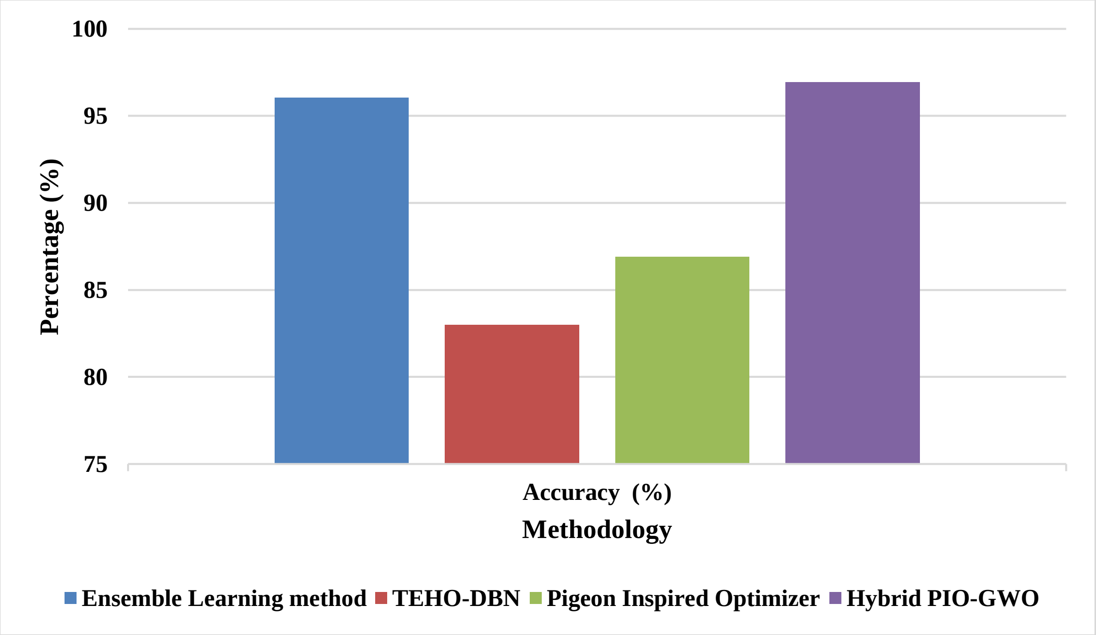

Fig. 4: Graphical representation for comparing exisitng models with the proposed hybrid PIO-GWO algorithm.

5. Conclusion

The IoT has assigned a uniquely assigned IP address which is used for communicating the external entities. The IoT networks were ranging from higher end of computing systems based on the structure that is having low memory and showed complexity in capacity. The issues of security were occurred in IoT devices that were rapidly increasing rapidly that would launch so much of attacks in the environment as days goes on. The attacks are intruded by the attackers through the internet and prevented the attacks at an early stage made the data safe. There are various devices present with different levels with variations in IoT that implemented the security mechanism. It is having different level with different properties and dimensions. The existing mechanisms showed insufficiency with respect to the detection of malware when analyzing. The attacks in the IoT environment are detected but lacked in security monitoring and protection techniques. The hybrid optimization algorithm is used for detecting the attacks which classified to mainly DoS, R2L, U2R, and probe obtained better results compared with existing methods. However, the soft computing of the hybrid optimization process showed complexity in the system. In future, the system complexity should be taken care off.

References

Alazzam, H., Sharieh, A., & Sabri, K. E. (2020). A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer. *Expert systems with applications*, *148*, 113249.

Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science*, 25, 152-160.

Balakrishnan, N., Rajendran, A., Pelusi, D., & Ponnusamy, V. (2019). Deep belief network enhanced intrusion detection system to prevent security breach in the Internet of Things *Internet of Things*, 100112.

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.

Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., & Alazab, A. (2019). A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. *Electronics*, 8(11), 1210.

Krishnaveni, S., Sivamohan, S., Sridhar, S. S., & Prabakaran, S. (2021). Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing. *Cluster Computing*, *24*(3), 1761-1779.

Liu, L., Xu, B., Zhang, X., & Wu, X. (2018). An intrusion detection method for internet of things based on suppressed fuzzy clustering. *EURASIP Journal on Wireless Communications and Networking*, (1), 1-7.

Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., Zhao, Y., & Cui, L. (2020). Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. *Measurement*, 154, 107450.

Mahdavi Hezavehi, S. & Rahmani, R. (2020). An anomaly-based framework for mitigating effects of DDoS attacks using a third party auditor in cloud computing environments. *Cluster Computing*, *23*(4), 2609-2627.

Otoum, Y., Liu, D., & Nayak, A. (2019). DL-IDS: A deep learning based intrusion detection framework for securing IoT. *Transactions on Emerging Telecommunications Technologies*, e3803.

Smys, S., Basar, A., & Wang, H. (2020). Hybrid intrusion detection system for internet of Things (IoT). *Journal of ISMAC*, 2(4), 190-199.

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. (2009). A detailed analysis of the KDD CUP 99 data set. *Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*.

Torkura, K. A., Sukmana, M. I., Cheng, F., & Meinel, C., (2021). Continuous auditing and threat detection in multi-cloud infrastructure. *Computers & Security*, 102, 102124.

Vijayanand, R., Devaraj, D., & Kannapiran, B. (2018). Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection. *Computers & Security*, 77, 304-314.

Velliangiri, S., Karthikeyan, P., & Vinoth Kumar, V. (2021). Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. *Journal of Experimental & Theoretical Artificial Intelligence*, 33(3), 405-424.

Zhang, Y., Li, P., & Wang, X. (2019). Intrusion detection for IoT based on improved genetic algorithm and deep belief network *IEEE Access*, 7, 31711-31722.