Date of publication DEC-30, 2022, date of current version JUL-28, 2022.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.21.4.2781

Hybrid Deep-GAN Model for Intrusion Detection in IoT Through Enhanced Whale Optimization

BALAJI S., S. SANKARA NARAYANAN
Department of Computer Science and Engineering, School of Computing,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India

Corresponding author: Balaji S. (e-mail: balajinithin19@gmail.com).

ABSTRACT IoT networks emerging as a significant growth in modern communication technological applications. The network formed with sensor nodes with resource restrictions in complexity, open wireless transmission features lead them prone to security threats. An efficient Intrusion Detection System aids in detecting attacks and performs crucial counter act to promise secure and reliable function. However, for the reason of the widespread nature of IoT, the intrusion detection system is supposed to carry out in discrete form with fewer fascination on common manager. In order to conquer these issues, Distributed – Generative Adversarial Network (D-GAN) with Enhanced Whale Optimization – Distributed deep learning based on Artificial Neural Network (EWO-HDL+ANN) is proposed. Here the GAN can detect internal attacks and the D-GAN is capable of detecting both internal and external attacks effectively. Transfer By Subspace Similarity is engaged to carry out. After that the preprocessed data is fed into feature extraction stage. Modified Principal Component Analysis (MPCA) is applied to feature extraction, which is used to extract new features that are enlightened. Then, feature selection is executed by Enhanced Whale Optimization Algorithm, which is used to choose significant and superfluous features from the dataset. It gets better the classification accuracy through the greatest fitness value. Then the intrusion detection is evaluated by applying HDL+ANN algorithm used to detect the attacks powerfully. The experimental conclusion proves that the introduced EWO-DDL+ANN method provides enhanced intrusion detection system in the view of greater accuracy, precision, recall, f-measure and low False Positive Rate.

KEYWORDS Intrusion Detection; Distributed-GAN; Generative Adversarial Network; Improved Whale Optimization (IWO); Hybrid Deep Learning; Artificial Neural Network; MPCA; Feature selection; Redundant features; K-mean clustering.

I. INTRODUCTION

IoT is a crucial field to ensure security for the both device and applications that offers an extensive technical progress at superior grade in the surveillance of enormous data. It has stepped into newer applications and devices along with electronics, sensors, actuators, protocols, software, to enhance association, compilation, and data communication [1]. IoT network lacks robust security implementation end to end. The intruders can gain the control of devices. Almost 85% of IoT devices are bare to diversity of cyber intrusions. Also, they are subjected to numerous threats such as DoS, DDoS, sinkhole, wormhole, data/identity stealing, device detain and other advanced intelligent attacks. In order to protect security based important systems from attackers well-built safety accomplishment is well thought-out to identify all forms of known and strange threats [2].

In present days it has been proved that Neural networks have the capability to reconstruct their own code to progress, shield and heal against the intrusions. The Intrusion Detection System with neural network with the aim of investigating network traffic and system information from hurtful actions and given warning is the major healing mechanism. To analyze and generate responses for the attacks from the different layers we adapt an Intrusion Prevention System with integrated with IDS to evade intruder from performing harmful action to the model [3].

It has been proven that conventional IDS is not appropriate since a lot of exclusive characters of IoT with respect to size, low processing capability, privacy defending type, the direct method of applying intrusion detection will not result in success because in the conventional algorithms, system can implement Intrusion Detection System only on data centers/

nodes which are dealing with the information from the absolute IoT model. But it is been observed that the majority of IoT networks, which depend on centralized system for mount intrusion detection solution are vulnerable for security breaches. And there is a possibility that these central intrusion detection systems can be compromised or influenced [4]. In contrast, within Intrusion detection, every device should contain a database which has low part of state of network. In addition, applications such as health care, smart home, smart cities, industrial automations in which model, client may not disclose vital exclusive information with system controllers, in such case it is proved that data-centered intrusion system is incompetent [5]

Hence in this paper, we focus more on GAN (Generative Adversarial Networks) scheme to construct a distributed model along with Deep Learning methods, we propose an unsupervisory learning model named as the generative modeling for performing automatic discovery of gathering data, analyzing and examining input data to use the model for creating/outputting innovative sampling which potentially will be acquired from real database [6]. Generative Adversarial Networks is a smart way of training the inventive model via structuring the problem as supervised learning apprehension with two sub-models namely generator model which trains to create new samples, discriminator model which endeavors to discriminate the sample as unique or reproduction. These models are trained concurrently in zero-sum adversarial game till the model is deception on semi-period, i.e., generator model is creating prospective samples [7]. Fig. 1 demonstrates the common organization of GAN.

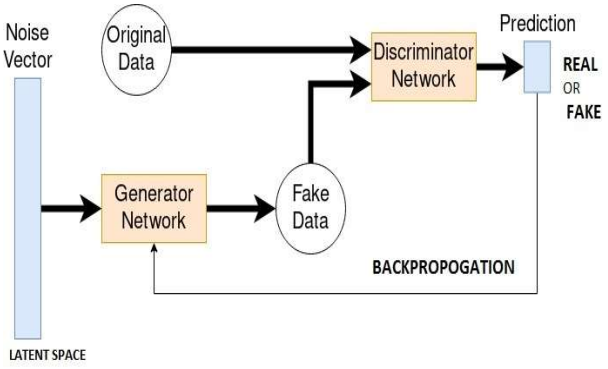

Figure 1. The Generative Adversarial Network Architecture.

The GAN exercises the idea of adversarial learning to train the model to handle the complexity of high-dimensional data generated in the IoT network. GAN has generator G along with the discriminator D networks. The generator G learns to generate bogus samples by renovating noise variables z into generator sample G (z) to betray the discriminator, while the discriminator D is trained to take advantage of the likelihood of predicting whether its inputs are training examples or generator samples G (z).

A generator transforms malicious edition of the input and sends it to the Detection system for sorting and to the discriminator. The objective of the generator is to betray IDS, and the aim of the discriminator is to emulate the IDS on classifying inputs whether it is truthful or erroneous and provide response to the generator.

Intrusion detection in network intrusion identifier is therefore a data collector that collects real-time network information by congregation of packets in the network. These packets are handled earlier to inflowing the dataset. Packet capture function is executed within the data collector to acquire the packets and extract the features. Feature reduction/extraction reconstructs the multi-spatial space to less space; thus, the renovation will be linear/non-linear. This also allows throwing away the superfluous values to make the system to a large extent simpler. During training, feature selection or extraction is investigated for feasible feature set from input sample and they are in a job of classifier training [8].

Feature extraction method strives to reposition of input features with new feature set, but Feature Selection scheme seems to be superior enlightening features from actual input data. FS is of significant eminence in intrusion detection which is persuasive in increasing learning usefulness, increasing generalization result, and accomplishing data visualization. In the episode of FS, feature with linear correlations, non-linear correlations are measured to determine relevance among the class label in the data associated with a category which is calculated and redundant features for output class. An approximate-Markov-blanket search strategy is adapted to discover a fitting feature which holds information associated to output class at the greatest [9].

The scheme of identifying the absolute labels is expressed as classification. This is executed to sort out the data depending on training and characteristic values. It is also called as class categorization/prediction/supervised learning. The model is engaged to foresee the class labels and test the fabricated model with test samples; accordingly, accuracy of classification policy is anticipated. ML techniques are employed to scrutinize and inspect huge network data as abnormal/accurate data [10]. Since data generated from diverse sources, traffic in the network is enormous. The ML methods similar to clustering, classification is engaged to create IDS powerfully as well as Deep Learning (DL) based techniques used to advance the large quantity of IDS dataset successfully over the IoT [11].

The main idea of this research work is to develop a model for intrusion detection over the IoT network. Due to the composite and time-varying vibrant nature of the IoT network, the network intrusion specimens are pooled into a large number of normal samples; due to this model training samples are inadequate in intrusion detection system and the detection results go ahead with a high false detection rate.

Many examinations and schemes are in trend although the D-GAN based IDS accuracy is not greatly proficient. A large amount of the existing techniques comprises restrictions like computational cost and imprecise IDS classification outcome. To resolve the above pointed out evils, now, IWO-DDL+ANN are presented to enhance the complete D-GAN IoT system performance. The most important involvement of this research is building of D-GAN model, preprocessing, feature extraction, feature selection and method of identification. The pioneer approach is used to offer extremely correct IDS result by providing work for competent approach for given database. In this anticipated HDGAN intrusion detection algorithm we firstly execute preprocessing of collected data from IoT devices system to diminish the noise samples and then amplify the minority samples by TBSS algorithm, here, the GAN model entirely learns the features of minority samples and deeply reduces the model training time and feature Extraction in combination with Modified Principal Component Analysis by applying wrapper feature selection using Improved Whale Optimization (IEWO) techniques. Lastly, we engaged

distributed GAN network which provides better detection accuracy and classification of the intrusion.

The rest of this paper is prepared as follows. Chapter 2 introduces the research of deep learning based intrusion detection in IoT network and associated research to solve the problem of complex inadequate high dimensional data. Chapter 3 introduces applicable background knowledge and proposes HDGAN Model and also describes preprocessing feature extraction and feature selection models in detail. Chapter 4 describes the experimental results and performance analysis. Finally, Chapter 5 presents a few conclusions and further work.

II. RELATED WORK

In [12], the author concentrated much on identifying the security threats in the Internet of Things, a technique of adversarial sample is used for IoT environment. An application method of intrusion detection system has been built. Intrusion detection system is launched in IoT, the generator of the network has been trained with data distribution of normal samples from Internet of Things. Finally adversarial sample detection has been built to reconstruct the data for calculating reconstruction error, the discriminator matching error of samples and detectors are illustrated to identify risks in Internet of Things. To regulate complex and dynamic surroundings of Internet of Things, detectors change robustly for identifying mutated and fresh threats of IoT. Hazard information compilation is portrayed. Threats identified by the detector in IoT are clustered in threat information collection to notify the manager of Internet of Things.

In [13], security threats of different kinds were considered to evade IoT network from DDoS risk. An Endeavor of DOS is to force network resources hard for authorized users. While numerous DoS threats are in the network then it is classified as DDoS attack. The approach is to prevent DDoS in networks of IoT through idea of LSVM and neural networks. At this point, Mirai Architecture is permitted to perform as a model for Internet of Things to find and discriminate limitations in IoT devices that can be beaten through its IP address, thus performing as middleware. DDoS prevention policy focuses on Mirai depending on IoT architecture. The conclusion of simulation pointed out that Mirai is competent in evading DDoS threats in Networks of IoT.

In [14], it was recommended fresh IDS by utilizing Transfer by Subspace Similarity classification algorithm that improves the gathered data quality by computing the relevance correlations between variable and filling the missing values in the dataset. Assessment conducted on NSL-KDD database demonstrated that the method is highly successful compared with that which is reliant on Transfer by Subspace Similarity technique. Furthermore, the technique has higher rate of identification and reduces false positive rate of detection. In [15], it was concentrated on PCA proficiency for detection of intrusion and confirmed RR (Reduction Ratio), perfect number of PCA required for identification of intrusion and consequence of noisy data in PCA. Countless assessments were executed on PCA by exploiting lots of classifiers for two typical databases such as UNB ISCX, KDD CUP. Effect of assessment indicated that preliminary 10 principal components are proficient for classification.

In [16], the authors considered reducing the cost of computation in management IDS raw data using feature extraction. The development of feature extraction is to translate features to low dimension to speed up the process of learning and improving the accuracy. Here, they focus on automatic feature extraction by adapting simple auto-encoder and SVM to classify IDS attacks. It makes use of various activation functions and loss to scrutinize the degree of feature extraction in improving the accuracy. The competence of the detecting practice after feature extraction is estimated by through KDD Cup` 99 NSL-KDD dataset. At this time, activation function as parameter activation and cross-entropy loss function endows through better accuracy when contrasting with other functions.

In [17], Li et al (2019) focused on the IoT system that was built steadily, beginning with broad industrial base that contains electronic components, integrated chips, integrated systems, and software devices, services of IoT and telecom networks. With respect to choosy rerouting assaults, virus destruction, spiteful malware intrusion and so on, victims formed due to security issues are extremely passionate in predictable networks that contain network data and physical things. Resource deficiency in IoT network intricacy and open wireless transmission features enable them prone to threats. Intrusion detection aids in identifying network variation and making apt countermeasures for protected and truthful IoT applications' functions. At this juncture, an IoT feature extraction with intrusion identification for smart city focuses on deep migration learning method that incorporates DL with ID method employed.

In [18], WOA (Whale Optimization Algorithm) was launched which enhanced labeling and dimensionality reduction for surplus feature reduction on intrusion identification network. Typically, WOA converge steadily in the course of penetrating and rapidly falls to local optima in revising method that confines the classification and dimensionality reduction. Consequently, here they have applied nonlinear convergence factor strategy in search process and adapted PSO for updating practice. IBWOA (An Improved Binary Whale Optimization Algorithm) is created to attain good dimension reduction in the initiative of assurance accuracy for choosing features for ID. For appraisal, several datasets from UCI are engaged for proof by contrasting with other methods of feature selection. Finally, KDD CUP 99 database is utilized for feature selection verification in Intrusion Detection. Experimental proof indicates that distinguishing with GA, WOA and PSO enhances the classification accuracy in addition to reducing the dimensionality when selecting features for ID.

In [19], a fresh approach for intrusion detection in IoT systems was recommended resulting from DL using CNN. IoT log data like address, duration, location, functions, service and so on are extracted for actual feature set. Then, this is improved and encoded as digital matrix which is supplied in to CNN for training and identification. Combining with various devices, atmosphere and transmission protocols IoT is at high risk of insecurity and vulnerability. Therefore, an efficient ID model which is fit for IoT system is mandatory. In [20], Hanif et al (2019) recommended ANN based IoT intrusion identification to determine authentication process. It spends supervised learning process to classify risks and also controller discards the instructions when it is identified as attack. ANN consists of input, output and hidden layers in which input sends data as signal to hidden layer. The hidden layer calculates the signals along with weights allocated and activation function is engaged to convert them to output signal. The technique can identify attacks capably and appropriate evaluations are made to deal with the threats. ANN method accomplishes 84% of average

accuracy and average false positive rate of less than 8% for monotonous 10 fold cross substantiation. It proves the precision, accuracy and power of method for enormous diverse database and drastically increases IDS utilization.

In [21], a GAN based IDS (G-IDS) was presented. In this GAN synthetic examples are generated and utilized for training IDS as well as original data. G-IDS identifies the intricacy in unstable or absent value concern. It represents a network security database for forthcoming CPS by utilizing NSL KDD-99 database and evaluates the performance of the system using diverse measures and ascertains that G-IDS model makes progress in identifying attacks and alleviates the model in the entire training process in contrast to separate IDS.

The deep learning techniques in the IoT network intrusion detection have attained reasonable results. We cannot give guarantee for the competence of detecting all the attacks since the data scarcity for training and multifarious high dimensional data. Deep learning model is not prominent in detecting the strange attacks. In order to overcome above issues and complexity, we have proposed the Distributed Generative Adversarial Network with deep learning for detecting the unknown interior and outside attacks on IoT networks.

III. METHODOLOGY

In this endeavor, DD-GAN with IWO-DDL+ANN is proposed for intrusion detection over IoT. This work involves the construction of D-GAN model, data pre-processing, extraction and choice of feature, classification and result appraisal. The overall design of introduced method is depicted in Fig 2.

A. HYBRID DISTRIBUTED–GAN MODEL

Here, D-GAN is built for competent detecting the intrusions in the IoT. GAN is a highly influential and proficient method in Deep learning. Here GAN approximates a generative model using adversarial process. Typically, GAN has two autonomous models such as G – generator and D – discriminator. The Generative structure assesses data distribution $p(g)$ upon actual data space x. The intend of G is to create fresh adversarial sample G (z) that is attained from similar distribution of x.

Here, D discriminator model consequences the probability $D(x)$, with respect to the given example x is a real data set formed by G. The major goal of G is to boost the possibility which D inaccurately anticipates created data as real and the objective of D is to perform opposite [22]. Consequently, D and G will achieve minmax equivalent and at last attain an elite result. Value function $V\ (G;D)$ is described as following:

$$\min_G \max_D V(D,G) = \mathbb{E}_{x\sim p_{data}}(x)[log\ D(x)] + \mathbb{E}_{z\sim p_z(z)}[\log(1 - D(G(z)))]. \quad (1)$$

Prefer an IoT which contains set $N\ of\ n$ IoTDs where every IoTD i has a set of prior broadcasted data points, Di, which outcome in distribution $p_{data}i\ (x)$, here x *possibly* time series, military data, economic reports, or health observation database. It imagines that D_i consists of data points from genuine IoTD state when there are no attacks in IoT. It as well permit let $D_1 \cup D_2 \cup \ldots \cup D_n = D$ here D represents entire reachable data with a distributionp_{data}. Here, each IoTD i endeavors to learn *generator* distribution pg_iahead its accessible database D_i so as to $pg_i = p_{data}$ and employs the distribution to identify an attack in the system.

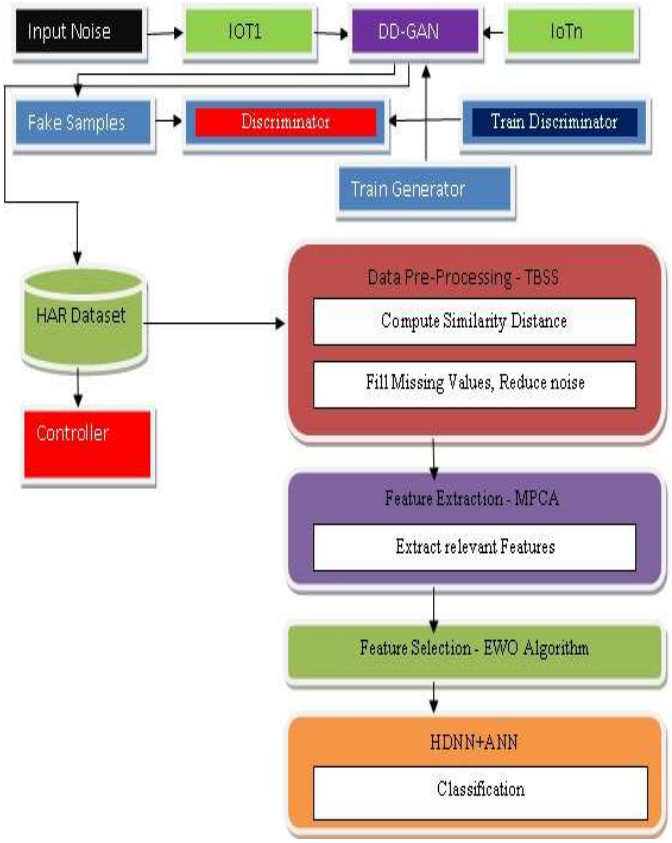

Figure 2. Hybrid Distributed Deep Learning based Intrusion Detection in IOT

Attack in the system is any act by intruder those origins IoTD to correspond data points with the aim not to approach subsequent to data distributionp_{d_i}. In fact, when IoTD realizes allocation of its own actual state, it effortlessly disfavors data point which is distinct to normal state distribution. In general, ANN consists of artificial neurons and activation function that map input and output. A supplementary ANN called discriminator $Di(x, \theta_{di})$ is defined for all IoTD i which gets data point x and produces a value between 0 and 1. If the discriminator outcome is closer to 1, acquired data point is in usual state otherwise it is an attack at IoTD i.

While all IoTD's generator would intend to reduce value function mentioned in (1), discriminator tries to enlarge the value. Hence, viable result for discriminator and generator might be attained from subsequent minmax problem.

$$\{D_i^*, G_i^*\} = argmin_{G_i} \arg\max D_i V_i(D_i, G_i). \quad (2)$$

Here, distributed GAN-based IDS develops structural design from [31]. Endeavor of distributed GAN is to establish a discriminator at each IoTD further than distribution databases mutually in an effort to each IoTD's discriminator can discriminate when a new data point extends total data distribution, p_{data}.

In D-GAN, during the training phase, it provides work for a central unit which includes generator G_φ here φ is the ANN generator's weight. In addition, each IoTD contains discriminator specified as $D_{\theta i}$ here θi is the each ANN

discriminator's weight. In this model, all IoTDs are allied with not less than one IoTD in internet of things network so that connection graph of the IoTDs must outline a $cycle$. Moreover, during training phase, all IoTDs are connected with the central unit.

The GAN is competent in classifying the consequences from trained sample, but still due to unsupervised learning and unsteady Training it grows to be very complicated to train and engender output.

B. DATA PRE-PROCESSING USING TRANSFER BY SUBSPACE SIMILARITY (TBSS)

Here, improved TBSS algorithm is adapted for performing data preprocessing significantly improves the precision of Intrusion Detection for exclusive Human Activity Recognition (HAR) database. TBSS is flexible for detecting real time activity. The major goal is to design an algorithm to deal with these sequence data in order to improve the data mining quality by including missing data, fine-tune noise, and modify volatility for given database greatly. In this it is required to transfer data

$$D \text{ to the } D\hat{}, \hat{}d = (x\ n\ e, cn), \hat{}d \in D\hat{}. \tag{3}$$

Hence the Improved TBSS is a proficient clustering strategy operates to divide the identical data in the dataset into some group according to different labels which produces collection τ based on different class [23].

$$\tau = \{T_0^{C_m}\}_{m=1}^{n}. \tag{4}$$

The sampling methods randomly select data and we could construct sub-datasets, finally we can determine the vital information between them as new features using TBSS function (transfer by subspace similarity). Fig. 3 shows the outline of the improved TBSS algorithm.

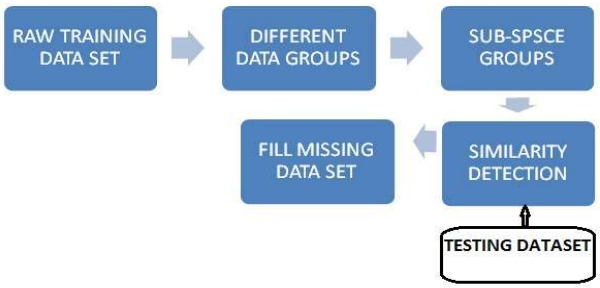

Figure 3. The General working model of TBSS Algorithm

The power of TBSS is to compute the probability between each subspace similarity and straightforward implementation.

We determine the Time-consumption based on the time spent on constructing the subspace and time taken to perform distribution of the original space. If the original space is large, the sampling times might be high since it is required to ensure the coverage rate for the original space. If the original space is less, the sampling times and cost time will be low.

Thus, preprocessing method is used to improve the intrusion detection accuracy successfully by using TBSS algorithm.

C. FEATURE EXTRACTION USING MODIFIED PRINCIPAL COMPONENT ANALYSIS (MPCA)

In this work, MPCA algorithm is projected for extraction of features which pay attention to diminish the number of attributes. PCA endeavors to decrease high dimension data space, i.e., experimental variables to low inherent feature space dimensionality, i.e., autonomous variables, which are essential to define data convincingly. This is applicable to in the case once there is a high relationship among tentative variables. During removal of minor components, PCA can decrease the feature quantity and place the dataset in little dimensional subspace [22-25]. PCA is a typical multivariate data examination method which is adapted in linear extraction of features. So, we select the PCA feature extraction process. Aspects of these methods are exploits as feature vectors that are well utilized to symbolize IDS dataset. The standard PCA algorithm can be applied for extracting features from undersized dataset and will ignore essential feature information. The PCA technique does not give guarantee for the data related to the associated classes is proficiently compressed. To prevent the above cited issues, modified PCA is planned.

The MPCA method will decrease the eigenvectors influence subsequent to massive Eigen values through standardizing the j-th element y_{ij}, of i-th feature of vector y concerning its standard deviation, $\sqrt{\lambda_j}$. As a result, new feature vector y_i' is modified as

$$y_i' = [\frac{y_{i0}}{\lambda_0}, \frac{y_{i1}}{\lambda_1}, \ldots . \frac{y_{i(r-1)}}{\lambda_{r-1}}]. \tag{5}$$

Homogeneous feature vectors are employed to build new feature subspace. In this process, it first normalizes the feature vectors by the square root of subsequent eigen values, and consequently calculates the distance between the training and testing features.

Normally, the linearly transform (PCA) might be stated as following equation:

$$Y = TX. \tag{6}$$

Here T is transform matrix, X is an original vector and Y is a transformed vector to determine the transform matrix T, the next equation:

$$(\lambda I - S)U = 0, \tag{7}$$

is applied, here matrices I, S, U and λ are square matrix with unity on its diagonal, original image covariance matrix, eigenvectors and eigen values. U_j And $\lambda_j (j = 1,2, \ldots m)$might be calculated by equation (2), with the eigen values ordered as $\lambda_1 \geq \lambda_2 \geq \cdots . \geq \lambda_m$. Eigen vectors U may be stated as $U = [U_1, U_2, \ldots \ldots, U_m]$.

In the MPCA, the training samples that are associated with a given application are chosen from an IDS dataset, and the transformed matrix T' was obtained from these training samples. It could be described as successive equation:

$$Y = T'X, \tag{8}$$

$$V_N = b_1 u_1 + b_2 u_2 + \cdots . + b_N u_N, \tag{9}$$

$$S = \sum_{i=0}^{1} b_1 u_1; 1 < N. \quad (10)$$

By contrasting equations (7) and (8), the variation is presented in the transform matrix, and principally presented in the samples for calculating the covariance matrix, here we take a unit from training samples; next one is from the whole detestation speech dataset.

The major objective of MPCA is to compute three similarity matrices using the similarity measurements based on three parameters namely mutual information, angle information and Gaussian kernel. The MPCA merges the wrapper method and the forward selection method has a dominant discriminative competence to classify samples. We can adapt MPCA to the functions in which the number of the training samples is less than the data dimensionality. MPCA offers superior classification accuracy and clustering outcome compared with PCA.

MPCA is a mathematical algorithm that makes use of linear adjustment to connect data from vast dimensional space to low dimensional space. Low dimensional space focuses on Eigen vectors of covariance matrix. In this work, we adapted MPCA to extort valuable significant intrusion features for human activity recognition dataset by decrease ng error and de-correlating features. As a result, MPCA fruitfully reduces the high dataset dimension through including high variance value coordinates and evading low variance data acquiring input data of normal and intrusion data that comprises features such as mean and standard deviation.

(i) Mean= sum of no of data /total no of data. (11)

(ii) Standard deviation: also termed as root-mean square deviation since it is the square root of means of squared deviation from arithmetic mean.

$$\sigma = \sqrt{(\sum(x - \ddot{x})/n)}. \quad (12)$$

The MPCA practice is employed to extort enlightening features from given dataset and also it is used for valuable feature dimension reduction.

It has been proved that MPCA takes less time for extracting the features from the nonlinear combination of variables such as, IoT network data and takes minimal features compared to PCA algorithm in contrast with auto encoder algorithm which takes longer time for feature extraction.

And also, it has been observed that modified PCA has been tested with IoT data sets in which it doesn't eradicate the prominent features which are measured as a major feature to compute the prediction in an accurate way.

D. FEATURE SELECTION USING ENHANCED WHALE OPTIMIZATION (EWO) ALGORITHM

In this work, EWO is presented for efficient selection of features over IDS dataset. The aim of feature selection is to detect relevant features from the given data to identify the occurrence and absence of intrusion and non-intrusion features. The Whale Optimization Algorithm (WOA) is used for numerous optimization problems to find the optimal solution and select significant features. WOA algorithm is vital to select relevant features and precise to determine what WOA performance can be improved more to produce higher results, and is applied for feature selection in IDS datasets for precise detection.

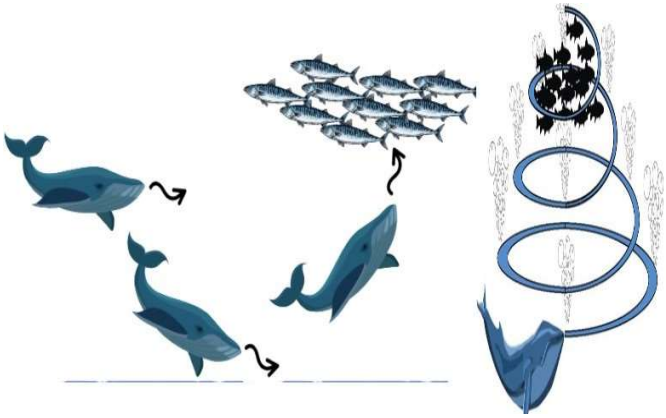

Figure 4 (a). Environment of Whale Optimization Algorithm

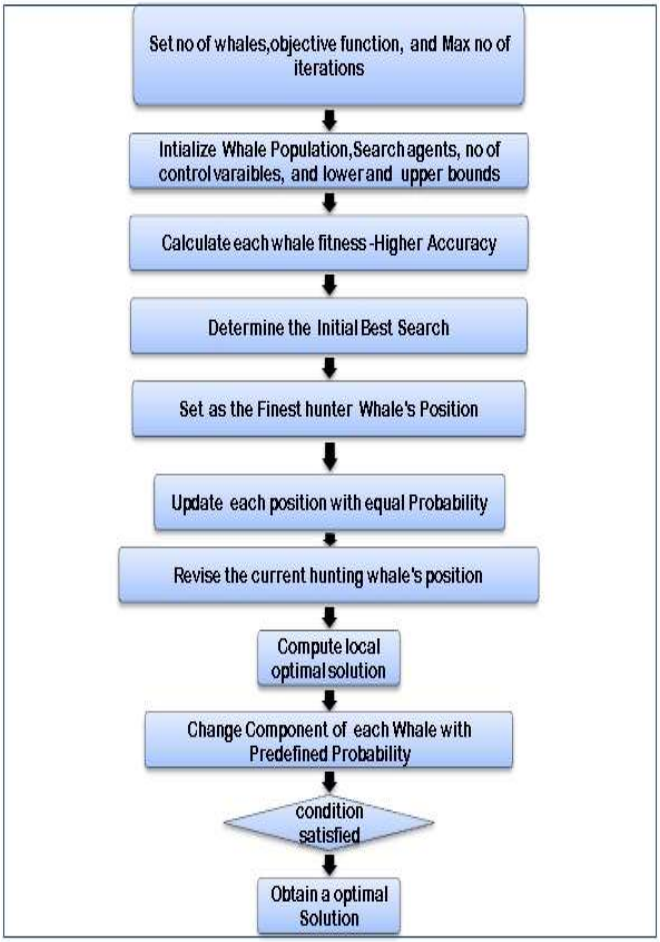

Figure 4 (b). Flowchart of Enhanced Whale Optimization

The idea of WOA is inspired based on the hunting strategy of humpback whales and obtains an algebraic model for the hunting scheme. The hunting approach uses a bubble-net method according to which the whales circle around the prey, typically small fish and eat it. Whales travel deep below the fishes and begin moving to the surface, constructs a big circle of bubbles. The bubbles act as an ambush and induce the fish to move to the surface. The whales persecute the fish moving to the surface [26]. In principle the hunting practice involves three stages, to be precise circling, exploitation and exploration. The excellence of exploitation and exploration determines the worth of the fish eaten. Encircling stage: During

this stage whales identify the location of the fish and encircle them. At the start the point of the optimum location is not defined and initiated at arbitrary. Based on the random initiation other agent revises their position and the updated position happens to be the optimum location to the target.

WOA operation phase learns using transfer learning techniques and imitates the present best solution behaviour which decreases the population diversity. In WOA investigation phase, the procedure of learning from random individual has a little loss of sight and be short of efficient data transformation between groups, which affect the rate of convergence of the procedure. Hence the regular WOA has problems with slow convergence speed. To conquer the above mentioned problem, EWO is presented to improve the convergence speed by eliminating local optima vale and focus on global optima.

The environment which is simulated with animal swarm optimization takes features from best and other associates; this will systematically boost the individual's quality. Dynamic social discovering method is to organize the individual's neighbourhood by computing the individual's social ranking and social power, and building a social network [27]. To enhance the communication between groups, this method is engaged to build the dynamic neighbourhood of whales, and an innovative idea created on neighbourhood update is formed to enhance the population diversity and estimated accuracy.

The position of the whale and the encircling given in the equations is as follows:

$$\vec{H} = |\vec{C}x\vec{X} * (t) - \vec{X}(t)|. \quad (13)$$

$$\vec{X}(t+1) = \vec{X}(t) - \vec{A} \times \vec{H}. \quad (14)$$

The terms $\vec{A}$ and $\overrightarrow{C}$ furnish vector coefficients, t stands for the present iterations, term $\vec{X}$ provides the position vector and $\vec{X} *$ assumed to be the best solution (position) started at random. The vector $\vec{A}$ and $\overrightarrow{C}$ coefficients are computed via equations (14) and (15).

$$\vec{A} = 2\vec{a} \times \vec{r} - \vec{a}. \quad (15)$$

$$\vec{C} = 2x\vec{r}. \quad (16)$$

The components of $\vec{a}$ are reduced from 2 to 0 during each iteration linearly and symbolize the arbitrary value between 0 and 1.

Humpback whale exploits bubble-net process to circle around the prey and hunt it [28, 29]. Whales encircle the prey, resembling fish, and might revise their location to locate the realistic end result. Numerical WOA element is pointed out in the equations.

$$X(t+1) = X^*(t) - A.|C.X^*(t) - X(t)| \; if \; p < 0.5, \quad (17)$$

$$X(t+1)|C.X^*(t) - X(t)|.e^{bl} \cos(2\pi t) + X^*(t) \; if \; p \geq 0.5, \quad (18)$$

where X is a vector of entire whales' locations; t is the time and index for iteration; X* is the optimum solution produced so as yet; A=2a. (r-a);C=2.r; a is coefficient vector which are condensed linearly starting from 2 to 0 through iterations; r is a random vector with values contained by 0 and 1; b is a steady value which expresses logarithmic spiral shape according to the particular path and at this point the value is assigned as 1; l is a random number among – 1 and 1; p is a random number among 0 and 1 and is applied to modify among (14) and (15) in changes the location of whales; in equations (16) and (17), the possibilities are 50% – 50%; it entails in the time of optimization course, whales prefer any path randomly with equal probability. During the bubble-net phase, the random value for A is among – 1 and 1, though in the searching phase, the random value of vector A possibly will be > 1 or < 1. Searching method is represented in Equation (18).

$$X(t+1) = X_{rand} - A.|C.X_{rand} - X(t)|. \quad (19)$$

Random search with value of |A| >1 enlightens the searching operation and maintains the WOA algorithm to perform a global search. Random solutions are created at the early stage of WOA searching process. Then these results are modified for every iteration.

Searching process is repeated until the maximum iterations are reached.

Operation Phase: This phase consists of two steps i) encircling and ii) revising the position spirally. Encircling actions can be invented by diminishing $\vec{a}$ linearly from 2 to 0 for every iteration.

Revise Spiral position: In this spot of the whale to the fish, the helical shaped movement of the whales is specified by

$$\overrightarrow{X}(t+1) = \vec{D}xe^{b1}xcos(2\pi l) + \vec{X} * (t), \quad (20)$$

where $\overrightarrow{D'} = |\vec{X} * (t)\_\vec{X}(t)|$ is the recent position between the fish and the whale, b static factor or constant that represents the spiral movement of the whales and b also a random vector of $[-1, 1]$. As well as, there exist a probability of option: either diving deep through circling and shapes spiral is specified accurately by equation 6 or the random vector of value is p[0,1].

Investigation Phase: Detection of fish is described as global search with whales searching for the fish that move to the surface. The preference of switching between exploitation and exploration is based on $\vec{A}$, a vector with values of [0,1] where 0 entails exploration and 1 exploitation.

$$\vec{H} = |\vec{C}x\vec{X}_{rand} - \vec{X}|, \quad (21)$$

$$\overrightarrow{X}(t+1) = \vec{X}_{rand} - \vec{A}x\vec{H}, \quad (22)$$

where $\vec{X}_{rand}$ gives the latest position of the whale which is selected at arbitrarily from the other whales.

By applying the social learning theory to construct neighbourhood membership association for every whale, it can transform the behaviour of simulation of the current finest result, improve the data sharing among the groups, and improve the ability of process pop off the local optimal outcome. For the present population:

$$G(t) = \{x_1(t), x_2(t), \ldots, x_N(t)\}. \quad (23)$$

Here N is the size of population. All individual's fitness is calculated and regimented from small to large to achieve the ordered population

$$G_1(t) = \{x_{(1)}(t), x_{(2)}(t), \ldots., x_{(N)}(t)\}. \quad (24)$$

And social position of $x_{(i)}(t)$ is

$$I_{(i)}(t) = \frac{R_{(i)}(t)}{N}, \; i = 1,2, \ldots, N, \quad (25)$$

where $R_{(i)}$ is random number and $I_{(i)}(t)$ with the aim of a creature has improved the association with other creature, therefore, the exploitation stage of the process is principally importunate on the finest search result solution, and the exploration potential is refined by the relationship among groups, a new whale search method is formed on dynamic societal neighbourhood strategy.

$$\text{Fitness value (X)} = \sum_{i=1}^{k} yi - y'i, \quad (26)$$

where X is a model parameter; yi represents actual network traffic value, where k denotes number of iterations.

The minimum fitness value can be represented as

$$\min \text{fitness value (X)} s.t. \; LB \leq X < UB, \quad (27)$$

where X is denoted as D dimensional variable, D is no of parameters, UB-Upper Boundary, LB-Lower Boundary.

The algorithm performance is enhanced by ignoring local optima and concentrates more on global optima to increase the convergence rate and avoid huge fluctuations at the end of every iteration.

Algorithm 1: Enhanced Whale Optimization

```
Begin
Set whale population position (intrusion) X
Calculate each whale fitness (higher accuracy)
Initialize the whale population, no of iterations
Set a and r, compute A and C
Calculate each whale fitness
Set X* as the finest hunter whale's position
Set t = 1
While t ≤ max iterations do
For each hunting whale do
If p < 0.5
If |A| < 1
Alter the current hunting whale's position by (16)
Else if |A| ≥ 1
Randomly select another search agent (feature)
Update the current hunting whale's position by (17)
End if
Else if p ≥ 0.5
Update the current hunting whale's position by (18)
End if
Determine the local optimal solution using (22) &
(23)
End for
Revise X* if there is a better result
t = t + 1
Analyze the offspring Ui
If Ui is superior than Xi then
Revise individual i, Xi = Ui
If Ui is superior than X* then
Revise best individual, X* = Ui
End if
End if
 t = t + 1;
End while
Produce  X* obtain best solution as higher accuracy
End
```

Output the best Search Agent.

IV. INTRUSION DETECTION USING HYBRID DEEP LEARNING BASED CONVOLUTIONAL NEURAL NETWORK WITH ARTIFICIAL NEURAL NETWORK (HDLCNN+ANN) METHOD

In this proposed work, HDNN+ANN method is introduced for enhanced accurate intrusion detection for the given dataset. The anticipated deep learning process accomplishes higher accuracy. Fig. 5 illustrates the role of HDNN+ANN algorithm.

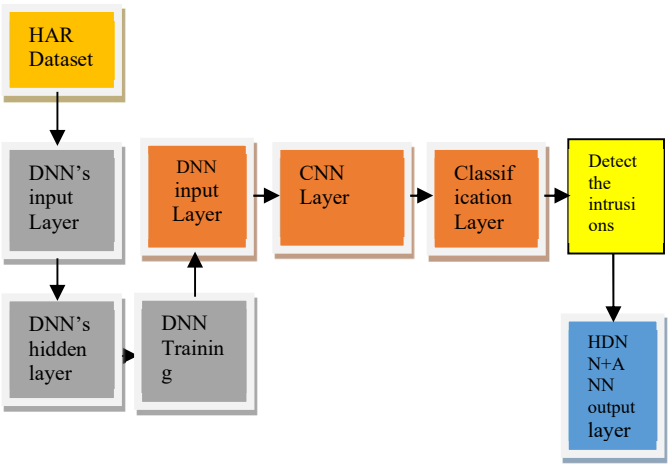

Figure 5. Working model of HDNN+ANN

A. TRAINING THE MODEL

The DNN is exploiting for gathering the information through discovering. DNN has three layers such as, input, hidden and output. The Input layer collects input values and analyses and produces 'n' inputs. This process has been determined with respect to weights. Weights assist data to resolve problems in NN [30]. Hidden information is extracted by hidden layer from input layer and moves towards output layer as soon as hidden vital information is extracted. DNN is adapted for identifying invasion features. IDS dataset training provided on DNN and in testing phase features are classified and identify the intrusions.

Introduced HDLCNN contains input, convolutional and classification layers. Introduced approach has obvious advantages for analyzing data with higher dimension. It uses a parameter sharing method that is utilized in convolutional layers to manage and decrease the number of factors. Fig. 6 shows the basic DLCNN architecture.

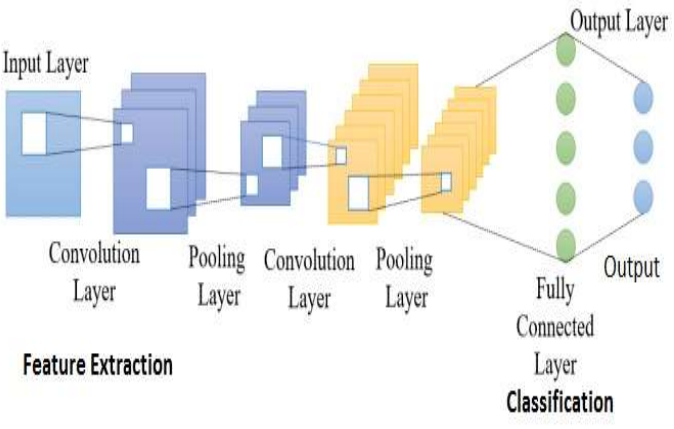

Figure 6. Fundamental DLCNN Architecture

Input layer accepts intrusion features from training examples and converts the data to combined form to deliver the data to subsequent layers properly. Here initial parameters are defined as the scale of the local receptive fields and dissimilar filters.

Convolution layer is generally utilized to extort important features and diminish the computational network complexity.

Algorithm 2: Intrusion Detection Algorithm-HDNN+ANN

```
1.  Input the IDS dataset
2.  For all input features, describe intrusion
    feature ∈ IDS dataset do
3.  For neurons, input features do
4.  Train ANN for the given dataset
5.  Hybrid DLCNN with ANN in D-GAN
6.  Transform input to convolution and
    classification layers
7.  Identify intrusion features
8.  Select more informative and relevant features
9.  Do training and testing procedure for
    specified database
10. Copy predefined intrusion feature label for
    every feature as indicated by the input
    database
11. Detect supplementary accurate intrusions
```

B. TESTING THE MODEL

The Hybrid D-GAN does not require any central unit since entire discriminators at each IoTDs will be able to identify the attack in the system. D-GAN is converged with deep learning GAN model, hence each IoTD executes its actual real-time data by its individual discriminator and any of the neighbor's discriminator. Viable discriminator will produce 0.5 for a standard state data point. Hence, to identify an intrusion in the system, output of the discriminator can be contrasted to 0.5 and when the output is near to 0.5, the IoTD remains in no intrusion state. Even so, when output is near to 0/1 the IoTD is under threat. The method assists the IoT system to identify the threat in the system without dependence on a central unit as each IoTD can verify its neighbor's data.

V. EXPERIMENTAL RESULT

In this work, daily activity recognition dataset is employed which is collected from 100 subjects under various genders, ages, heights, weights using a smartphone. This might be a better illustration of medical database which is gathered thorough wearable IoTDs. Similar databases are elite for its corresponding holder will not like to share out. Gathered data is about 12 tasks like walking forward, walking left, walking right, walking upstairs, walking downstairs, move forward, idle position, running forward, jumping, sitting, standing, sleeping, going up the elevator, and going down the elevator. Database consists of 5,368 copies totally and each copy in the database contains 561 frequency and time domain attributes. It divides the database as training and test database in 4: 1. The Python language program is used for experimentation and for determining the results.

In this work, existing algorithms are such as centralized GAN and D-GAN with ANN evaluated with proposed D-GAN with EWO-HDNN+ANN algorithm. Performance measures are determined as following ones: accuracy, precision, recall, f-measure, FPR and computational complexity.

Accuracy is determined as follows:

$$\text{Accuracy} = \frac{T_p+T_n}{(T_p+T_n+F_p+F_n)}, \tag{28}$$

where Tp is true positive, Tn is true negative, Fp is false positive and Fn is false negative.

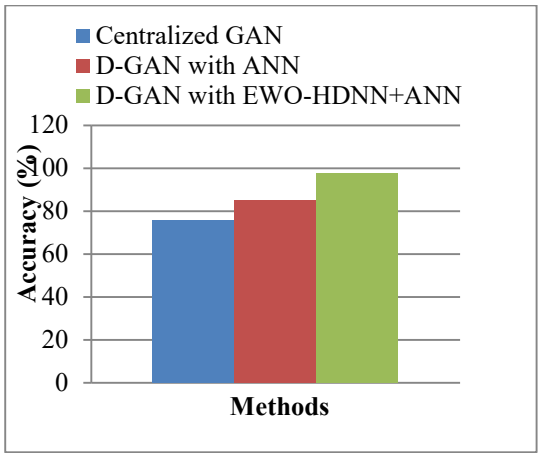

Figure 7. Accuracy

Precision

Precision is computed as

$$\text{Precision} = \frac{\text{True positive}}{\text{True positive+Fal positive}}. \tag{29}$$

Precision is viewed as computation of accuracy or quality.

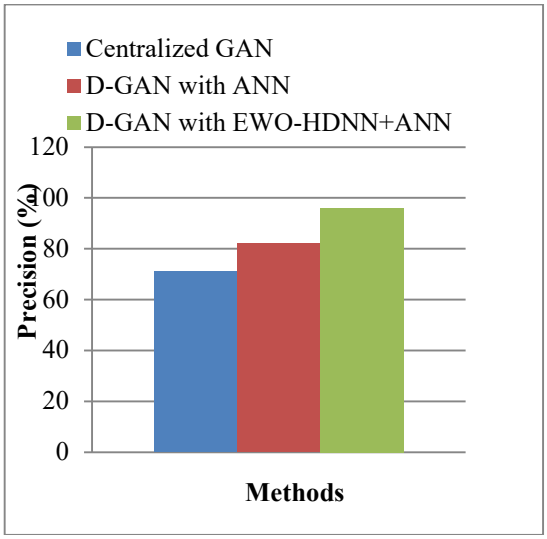

Figure 8. Precision

Recall

Recall is computed as:

$$\text{Recall} = \frac{\text{True positive}}{\text{True positive+Fal negative}}. \tag{30}$$

Recall is ratio of amount of appropriate content found in search by total current related documents.

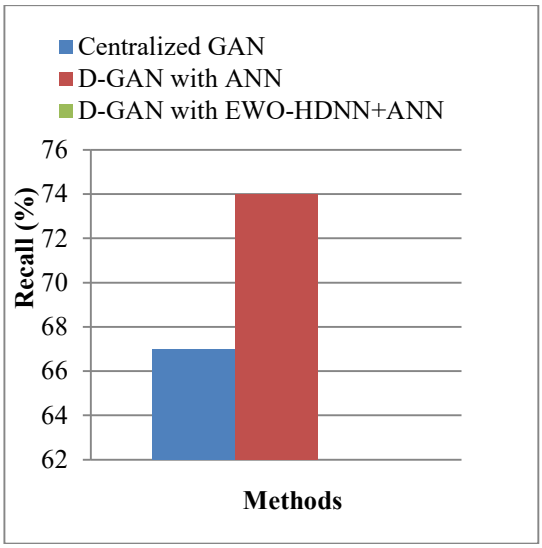

Figure 9. Recall

F-measure

F-measure is a mixture of precision and recall:

$$F = 2.\frac{PR}{P+R}. \quad (31)$$

To evaluate classification procedures, rely on F-measure as it is a typical measure of encapsulating precision P in addition to recall R.

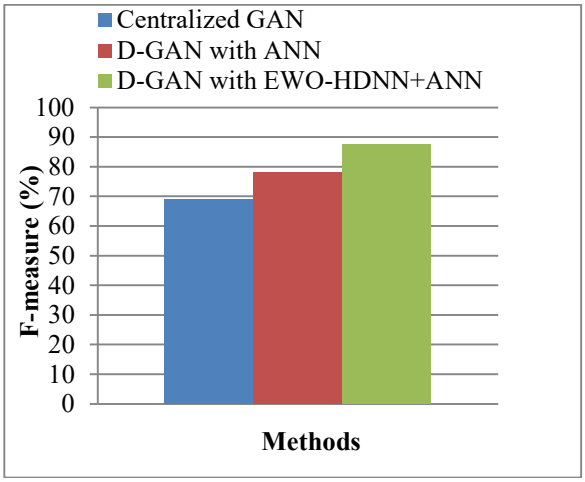

Figure 10. F-Measure

FPR

The False positive Rate of IDS is computed as

$$\frac{FP}{FP+T} \quad (32)$$

For IDS, FPR is proportion among amount of standard state data points wrongly classified as intrusion (*FP*) and the amount of real standard state data points (*FP* + *TN*).

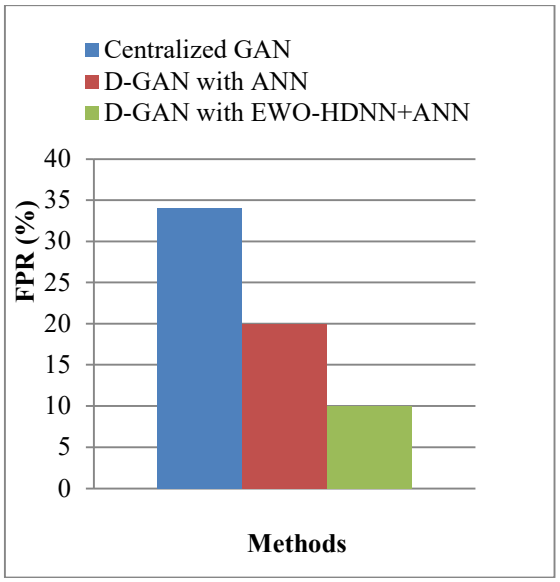

Figure 11. False Positive Rate

Computational Complexity

System is superior while proposed method offers less computational complexity when the gathered data preprocessed with EWO which reduces the complexity.

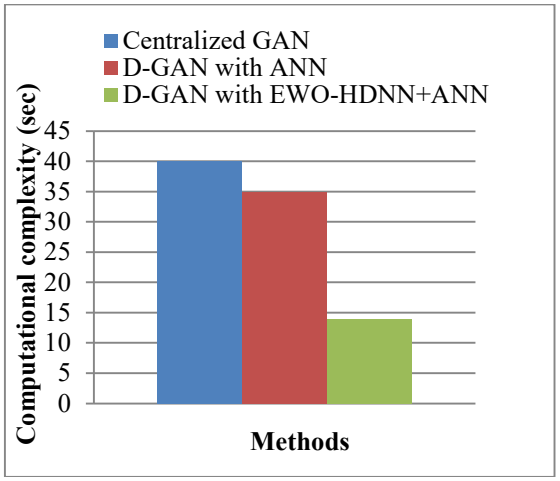

Figure 12. Computational Complexity

Table 1 shows the comparison values for IDS dataset using existing and proposed methods.

Table 1. Comparison values for IDS Dataset

Methods/Metrics	Centralized GAN	D-GAN with ANN	Proposed D-GAN with EWO-HDNN+ANN
Accuracy (%)	76	85	97.4
Precision (%)	71	82	96
Recall (%)	67	74	88.5
F-measure (%)	69	78	87.4
FPR (%)	34	20	10
Time Complexity (sec)	40	35	14

VI. CONCLUSION

In this paper, a proposed technique Hybrid Deep-GAN can efficiently detect the intrusions encounters due to the dynamic nature of IoT networks. It has been proved that the proposed GAN is prominent in Deep Learning field and major concern of this area is designing an intrusion detection system which provides solutions for the security breaches. In this proposal we constructed the Deep-GAN model for detecting all the unknown attacks significantly. Due to huge heterogeneous data generated from the network, it is mandatory to pre-process here by TBSS algorithm which is efficient in filling the missing data. And then MPCA method is adapted for feature selection to extract the significant features. And also Enhanced Whale Optimization algorithm is employed with the aim of selecting the finest fitness features. Finally, HDNN+ANN method is applied to classify intrusions accurately on the given dataset. The final outcome specifies that innovative EWO-HDNN+ANN method provides superior performance with respect to accuracy, precision, recall, f-measure and offers lower false positive rate, reduces computational complexity in comparison with other machine learning algorithms. And also in our future work, we will focus on creation of a dynamic, capable, and lightweight distributed technique to implement it in the end devices of Internet of Things Networks.

References

[1] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) Security," *IEEE Communications Surveys Tutorials*, vol. 22, issue 3, pp. 1646–1685, 2020. https://doi.org/10.1109/COMST.2020.2988293.

[2] M A. Rahman, Md H. Shahriar and R. Masum, "False data injection attacks against contingency analysis in power grids: poster," *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 343–344. https://doi.org/10.1145/3317549.3326323.

[3] S. Smys, A. Basar, and H. Wang, "Hybrid intrusion detection system for Internet of Things (IoT)," *Journal of ISMAC*, vol. 2, issue 4, pp. 190-199, 2020. https://doi.org/10.36548/jismac.2020.4.002.

[4] B. A. Tama, M. Comuzzi, K.-H. Rhee, "TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system," *IEEE Access*, vol. 7, pp. 94497, 2019. https://doi.org/10.1109/ACCESS.2019.2928048.

[5] A. Ferdowsi, W. Saad, "Deep learning for signal authentication and security in massive internet-of-things systems," *IEEE Transactions on Communications*, vol. 67, issue 2, pp. 1371-1387, 2018. https://doi.org/10.1109/TCOMM.2018.2878025.

[6] Y. Dai, H. Li, Y. Qian,Y. Guo, M. Zheng, "Anticoncept drift method for malware detector based on generative adversarial network," *Security and Communication Networks*, vol. 10, no. 1155, pp.1-12, 2021. https://doi.org/10.1155/2021/6644107.

[7] M. Ahmad, Q. Riaz, M. Zeeshan *et al.*, "Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set," *J Wireless Com Network*, vol. 10, issue 2021, 2021. https://doi.org/10.1186/s13638-021-01893-8.

[8] D. Li, et al., "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning," *International Journal of Information Management*, vol. 49, pp. 533-545, 2019. https://doi.org/10.1016/j.ijinfomgt.2019.04.006.

[9] G. Sun, J. Li, J. Dai, Z. Song, F. Lang, Fei, "MIC-based feature selection method for IoT data processing," *Future Generation Computer Systems*, vol. 89, 2018. https://doi.org/10.1016/j.future.2018.05.060.

[10] A. Abubakar, B. Pranggono, "Machine learning based intrusion detection system for software defined networks," *Proceedings of the IEEE International Conference on Emerging Security Technologies (EST)*, 2017. https://doi.org/10.1109/EST.2017.8090413.

[11] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, A. Robles-Kelly, "Deep learning-based intrusion detection for IoT networks," *International Symposium on Dependable Computing (PRDC)*, 2019. https://doi.org/10.1109/PRDC47002.2019.00056.

[12] Y. Peng, G. Fu, Y. Luo, J. Hu, B. Li and Q. Yan, "Detecting adversarial examples for network intrusion detection system with GAN," *Proceedings of the 2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS)*, 2020, pp. 6-10. https://doi.org/10.1109/ICSESS49938.2020.9237728.

[13] M. H. Aysa, A. A. Ibrahim and A. H. Mohammed, "IoT Ddos attack detection using machine learning," *Proceedings of the 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, 2020, pp. 1-7. https://doi.org/10.1109/ISMSIT50672.2020.9254703.

[14] Y. Zhong, S. Fong, S. Hu, R. Wong, W. Lin, "A novel sensor data pre-processing methodology for the Internet of Things using anomaly detection and transfer-by-subspace-similarity transformation," *Sensors*, vol. 19, issue 20, 4536, 2019. https://doi.org/10.3390/s19204536. PMID: 31635371; PMCID: PMC6832605.

[15] K. K. Vasan, and B. Surendiran, "Dimensionality reduction using principal component analysis for network intrusion detection," *Perspectives in Science*, vol. 8, pp. 510-512, 2016. https://doi.org/10.1016/j.pisc.2016.05.010.

[16] Y. N. Kunang, et al., "Automatic features extraction using autoencoder in intrusion detection system," *Proceedings of the International Conference on Electrical Engineering and Computer Science (ICECOS)*, 2018, pp. 219-224. https://doi.org/10.1109/ICECOS.2018.8605181.

[17] D. Li, L. Deng, M. Lee, H. Wang, "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning," *International Journal of Information Management*, vol. 49, pp. 533-545, 2019. https://doi.org/10.1016/j.ijinfomgt.2019.04.006.

[18] H. Xu, et al., "An improved binary whale optimization algorithm for feature selection of network intrusion detection," *Proceedings of the 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, 2018, pp. 10-15. https://doi.org/10.1109/IDAACS-SWS.2018.8525539.

[19] P. V. Huong, L. D. Thuan, L. T. Hong Van and D. V. Hung, "Intrusion detection in IoT systems based on deep learning using convolutional neural network," *Proceedings of the 2019 6th NAFOSTED Conference on Information and Computer Science (NICS)*, 2019, pp. 448-453. https://doi.org/10.1109/NICS48868.2019.9023871.

[20] S. Hanif, T. Ilyas, and M. Zeeshan, "Intrusion detection in IoT using artificial neural networks on UNSW-15 dataset," *Proceedings of the IEEE* International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT), 2019, pp. 152-156. https://doi.org/10.1109/HONET.2019.8908122.

[21] Md H. Shahriar, et al., "G-ids: Generative adversarial networks assisted intrusion detection system," *Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2020. arXiv:2006.00676v1. https://doi.org/10.1109/COMPSAC48688.2020.0-218.

[22] C. Yin, et al., "An enhancing framework for botnet detection using generative adversarial networks," *Proceedings of the International Conference on Artificial Intelligence and Big Data (ICAIBD)*, 2018, pp. 228-234. https://doi.org/10.1109/ICAIBD.2018.8396200.

[23] Y. Zhong, S. Fong, S. Hu, R. Wong, W. Lin, "A novel sensor data pre-processing methodology for the Internet of Things using anomaly detection and transfer-by-subspace-similarity transformation," *Sensors*, vol. 19, 4536, 2019. https://doi.org/10.3390/s19204536.

[24] Y. H. Taguchi, and Y. Murakami, "Principal component analysis based feature extraction approach to identify circulating microRNA biomarkers," *PloS one*, vol. 8, issue 6, e66714, 2013. https://doi.org/10.1371/journal.pone.0066714.

[25] G. J. Xiong, J. Zhang, D. Y. Shi, Y. He, "Parameter extraction of solar photovoltaic models using an improved whale optimization algorithm," *Energy Convers. Manage*, vol. 174, pp. 388–405, 2018. https://doi.org/10.1016/j.enconman.2018.08.053.

[26] Q. Jin, Z. Xu, and W. Cai, "An improved whale optimization algorithm with random evolution and special reinforcement dual-operation strategy collaboration," Symmetry, vol. 13, issue 2, pp. 1-25, 2021. https://doi.org/10.3390/sym13020238.

[27] Q. Fan, Z. Chen, W. Zhang, X. Fang, "ESSAWOA: Enhanced whale optimization algorithm integrated with salp swarm algorithm for global optimization", *Engineering with Computers*, 2020, pp. 1–18. https://doi.org/10.1007/s00366-020-01189-3.

[28] G. I. Sayed, A. Darwish, A. E. Hassanien, "A new chaotic whale optimization algorithm for features selection," *Journal of Classification*, vol. 35, issue 2, pp. 300–344, 2018. https://doi.org/10.1007/s00357-018-9261-2.

[29] A. Singh, "Laplacian whale optimization algorithm," *International Journal of System Assurance Engineering and Management*, vol. 10, pp. 713–730, 2019. https://doi.org/10.1007/s13198-019-00801-0.

[30] N. El-Khamisy Mohamed, and A. S. M. El-Bhrawy, "Artificial neural networks in data mining," *IOSR Journal of Computer Engineering*, vol. 18, pp. 55-59, 2016.
[31] Md A. Parwez, and M. Abulaish, "Multi-label classification of microblogging texts using convolution neural network," *IEEE Access*, vol. 7, issue 4, pp. 68678-68691, 2019. https://doi.org/10.1109/ACCESS.2019.2919494.
[32] J.-L. Reyes-Ortiz, et al., "Transition-aware human activity recognition using smart phones," *Neurocomputing*, vol. 171, pp. 754-767, 2016. https://doi.org/10.1016/j.neucom.2015.07.085.

S. BALAJI, *Received his B. Tech Information Technology from Madras University in 2002, ME degree in Computer Science and Engineering from Anna University, India in 2006. He is enrolled and currently pursuing Ph.D. in Computer science and Engineering at the Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, India. He has 17 years of teaching experience.*

His research interests include Wireless Sensor Networks, Cyber Physical Systems, Network Security, Internet of Things (IoT) and Machine Learning.

Dr. S. SANKARA NARAYANAN, *received the Undergraduate Degree in Computer Science and Engineering from Madurai Kamaraj University, in 2001, the PG degree in CSE from Anna University, Chennai in 2007 and Ph. D degree in Computer Science and Engineering from Kalasalingam Academy of Research and Education in 2019. He has 16 years of teaching experience. His areas of interest Mobile Ad hoc Networks, Network Security.*

He is currently working as an Associate Professor in the Department of CSE at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, India.