



# Dynamic distributed generative adversarial network for intrusion detection system over internet of things

S. Balaji<sup>1</sup> · S. Sankara Narayanan<sup>1</sup>

Accepted: 24 October 2022 / Published online: 23 November 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

## Abstract

The Internet of Things (IoT) intelligently facilitates individuals interacting with the real-world applications which forms smart environment through internet connectivity at anywhere anytime (dynamic in nature), the devices in an IoT environment encounters several security threats. To overcome these security challenges numerous state of art approaches have been implemented to ensure the security of IoT appliances, but still innovative methods are desirable. The traditional Machine learning (ML) integrates with deep learning algorithm exhibits a potential of detecting abnormal intrusion patterns by formulating a seamless option for anomaly-based detection. This work proposed a Dynamic Distributed—Generative Adversarial Network (DD-GAN) with Improved Firefly Optimization- Hybrid Deep Learning based Convolutional Neural Network -Adaptive Neuro-Fuzzy Inference System (IFFO-HDLCNN + ANFIS) that takes gain of IoT's power, offers enhanced behavior for efficiently examining the entire traffic which traverses in the IoT. Initially, Synthetic Minority Over-sampling Technique (SMOTE) is engaged for pre-processing of data and then Modified Principal Component Analysis (MPCA) is being applied for feature reduction. The optimal features are selected through the Improve Firefly Optimization (IFFO) for optimum fitness value to enhance the classification accuracy of HDLCNN. Finally the intrusion detection is carried out by HDLCNN + ANFIS model, which is competent in detecting threats. The experimental results have proven that model demonstrates ability to perceive any kind of probable intrusion and anomalous behavior. In comparison to existing methods, the suggested IFFO-HDLCNN + ANFIS algorithm delivers improved intrusion detection performance regarding higher accuracy, precision, recall, f-measure, reduced False Positive Rate (FPR).

**Keywords** Internet of things · Machine learning · Deep learning · Anomaly-based detection · Intrusion detection · Dynamic distributed—generative adversarial network · Improved firefly optimization · Deep learning based convolutional neural network · Adaptive neuro-fuzzy inference system · Synthetic minority over-sampling technique and feature selection

## 1 Introduction

The foremost aspiration of smart environments is to enhance the excellence of human life with respect to providing sophisticated environment with comfort and competence. The substantial growth of advancement achieved

in the proficient utilization of electronic services and applications facilitates to immense developments in telecommunications networks and the appearance of an idea of the Internet of Things (IoT) that is a universally agreed technology in intelligent networks. The IoT is a promising infrastructure model in which devices serves as objects or “things” that have the talent to gather information through sensing their environment, forms mutual communication with each other, and shares data over the Internet. It is predicted that by 2023, more than one trillion dynamic IP addresses or things will be facilitated to form a smart environment through internet connection [1]. In recent time's appearance of IoT paradigm is extensively adapted in forming smart environments, such as smart healthcare, smart cities and smart industries, with diverse

---

✉ S. Balaji  
balajinithin19@gmail.com

S. Sankara Narayanan  
ssankaranarayanan@veltech.edu.in

<sup>1</sup> 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

application fields and associated services. The ambition of developing such well-designed environments is to formulate the human life more fruitful and peaceful by triumph over the challenges related to the living environment, energy utilization, and industrial desires [2].

However, IoT systems are jeopardize to a variety of known security attacks, namely denial-of-service (DoS) attacks and distributed denial-of-service (DDoS) attacks. These attacks can cause significant harm to the facilities and intelligent environment applications in an IoT networks. For that reason, securing IoT environment becomes the major task and focus of attention otherwise it will led to huge damage. The major security breach was happened on Friday, October 21, 2016 in US; the intruders launched clusters of DDoS attacks that demoralized the security breaches in IoT systems and affected millions of websites, IoT devices and social media applications such as Twitter, Netflix, and PayPal [3].

For this reasons, in smart IoT networks, the application of IDS solutions is principally researched [4]. The works in [5], for example, used signature-based methodologies wherein network activity is matched to a database of attack signatures. Furthermore, anomaly-based IDSs compare a network's activities to the system's regular behavior, and an alarm is raised when divergence from actual state reaches a threshold. In addition, [6] employs novel ways to compare the condition of system to established criteria like connection maximum capacity, packet size, or conceptual rules depending on IoT traffic.

Traditional IDSs, like those used in [7], may not be effective because of much exclusive uniqueness of IoT systems, like their coverage range, large number devices and secure sharing of sensitive information. The IDS is typically deployed on economically powerful networks, data centers, cloud environments in which the data need to be analyzed which are gathered from large IoT networks and from the cluster of adjacent devices. Still, due to the IoT's massive extent of nodes, we cannot assure guarantee for the security by deploying IDS solutions on centralized nodes which may exposes those nodes to malicious attacks, and the rest of the network surely exposed as a consequence if the centralized IDS is hacked [8]. Furthermore, many IDSs necessitate the accessibility of significant data point's quantity pertaining to network's actual condition and failure events. In IoT systems, on the other hand, every IoT device may only have a dataset that represents a small percentage of network's state. Furthermore, the end user not required to share his or her existing information with system administrator in several applications, like health or financial activity monitoring, rendering data-centered IDS solutions worthless.

GANs are generative models that are built on differentiable generative networks. Basic thought behind GANs is

to pit a generator network not in favor of a discriminator network in a game theory-like environment. The discriminator network's purpose is to discriminate among samples from original and generated data, while the generator network's goal is to learn best approximation of training data. In [9], GANs were used to begin a considered adversarial perturbation in network data for threaten IDS efficiency, subsequently a GAN model has been added to the IDS based Machine Learning (ML) model to assure robustness. The findings demonstrate that adversarial perturbation created by GANs can successfully avoid ML/Deep Learning (DL)-based IDSs [10, 11]. Remarkably, GAN technology may be used not just to attack IDSs, but also to empower them. The findings reveal that IDSs is made robust against already seen with unknown adversarial perturbations by employing a GAN-based defense. For efficient IDS dataset analysis, ML/DL techniques are suggested for classification challenges. The IOT network data has enormous features hence the building of ML model consumes more time which degrades the detection performance of IDS. In these circumstances, an efficient feature selection algorithm must be employed for ML based IDS that builds the models in least time and accomplishes superior results in intrusion detection [12]. With this motivation DL can deliver accurate findings and analysis by constructing quick and efficient techniques and data-driven models for real-time processing of IoT dataset streams [13]. Classification algorithms that are efficient and effective are utilized to enhance the accuracy of the training and testing datasets. Most important aspect of addressing the issues is to seek for those useful features which include much information about output class.

The main focus of this study is on intrusion detection in IoT. The current existing models and algorithms have several constraints and limitations in terms of high computational overhead and inaccuracy in IDS classification findings. To address the aforementioned concerns, IFFO-HDLCNN + ANFIS model is suggested here to enhance overall performance of the DD-GAN with IoT system. The building of the DD-GAN model, preprocessing, feature extraction, feature selection, and detection method are the primary contributions of this study. The suggested approach uses valuable eminent algorithms which show efficiency of predicting and formulates more accurate IDS findings for the specified dataset. The primary responsibility of the work is illustrated in detail given below:

- At first, Human Activity Recognition (HAR) dataset is given as input and further SMOTE is utilized for preprocessing, and it is designed to handle the imbalanced dataset effectively that result of balanced data is then used to extract features.

- Second, MPCA is being employed to extort more informative features throughout the feature extraction process.
- Third, Feature selection process is performed using IFFO method, which selects the best features from the dataset. Through the optimum fitness value, IFFO enhances classification accuracy.
- The intrusion detection is then carried out using the HDLCNN + ANFIS method, which is employed to efficiently detect threats.

This investigation research study is structured into four core chapters. Section 2 elaborates the major reason and inspiration for the research work along with the inference. Section 3 summarizes the methods and techniques in detail. Section 4 shows the proven evidence of the experimental results on two standard datasets. The final Sect. 5 concludes this research with future work.

## 2 Related work

Liu et al. focused on detecting the security threat in the IoT by using artificial immune system methods to IoT setting in [14]. Technique of applying immunity theory to IoT context is built to establish an intrusion detection system in Internet of Things. The self device and non-self device networks are all simulated in Internet of Things. To monitor malicious behavior and identify attacks in the IoT, three types of detectors have been defined: immature, mature, and memory detector. Detectors evolve dynamically to identify modified, even new IoT threats in order to become accustomed to difficult and changing setting of IoT. The library of attack information has been defined. The attack information library is merged with threats identified by IoT detectors to alert Internet of Things management. On the other hand, such IDSs encounter constraints in performance with respect to high false positive rate and computational complexity.

Ferdowsi et al. presented a unique watermarking technique for dynamic authentication of Internet of Things signals in order to identify cyber-attacks in [8]. Watermarking allows IoT nodes (IoTDs) to mine a collection of distinguished characteristics from the signal generated and employs a deep learning framework for continuously watermark imperative relevant features mapping in to signal. This approach can be used by the IoT gateway that gathers signals from IoTDs to ensure authentication of the signals' consistency. In addition, because the gateway cannot verify all IoTDs at the same time due to computing constraints in large-scale IoT scenarios, a game-theoretic approach was applied in order to enhance the gateway's

supervisory prediction ability for identifying susceptible IoTDs. For this game, MSNE (mixed-strategy Nash equilibrium) is calculated, and the anticipated utility at the equilibrium is shown to be unique. There are high numbers of viable actions for the gateway, the MSNE has exposed to be critically tough to infer in the vast IoT system, and hence a learning technique that incorporated with the MSNE is applied. In addition, when the gateway is unable to find out the status of illegal IoTDs, which gets the help of deep reinforcement learning model for rapidly anticipating the current status of unauthorized IoTDs, and allowing the intermediate gateway for selecting the correct IoTDs in order to authorize. The results of simulations show that messages may be sent reliably from IoTDs with an attack detection time of less than one second. However, implementing this methodology in different provinces of an IoT network is a critical task due to the allied management concerns.

Thanigaivelan et al. [15] proposed a distributed interior abnormality discovery method employed in Internet of Things in their paper. Each node in detection system monitors the neighbors, and when an anomalous behavior is revealed, to monitoring node immediately suspend the packets from malicious behavior node in data link layer will send notification to the parent node. Until it reaches root, the reporting propagates from child to parent nodes. Distress propagation object (DPO), a new control message, is created to testimony the abnormality to successive parents then finally, the edge-router. The message is part of the Routing Protocol for Lossy and Low-Power Networks which includes user-configurable profile settings which can learn and distinguish between typical and questionable node behaviors without prior knowledge. At the data link and network layers, it has different subsystems and operation phases that distribute a common repository in a node. Without the help of a positioning system, the system employs network fingerprinting to detect changes in network structure and node locations. The minor quantity resource necessities make it most suitable for the perception layer of IoT. The method has several merits with respect to dynamic self-adaptation, low false alarm rate, reduced communication overhead with the major constraint of could not be able to detect all anomalies.

Schlegl et al. proposed an innovative idea using deep convolutional generative adversarial network to gain knowledge of a diverse of normal and abnormal unpredictability, as well as a new anomaly scoring method founded to correlate mapping of image into latent space in [16]. Models are usually built using vast data and annotated examples of recognized markers with the goal of automating detection. The power of such systems is limited by the high trivial effort and use of a limited terminology of known markers. It uses unsupervised learning to find

difference in imaging data that could be used as markers. Anomalies are labeled, and image patches are scored based on how well they fit into the learnt distribution. The method properly recognizes anomalous images, like images consist of retinal fluid and hyper reflective foci, based on results from optical coherence tomography scans of retina. In addition, the attacker is competent to damage all nodes of the network by knowing the network topology. The limitation of the method is it only concentrates on extenuating impacts of specific intrusions.

Vasan et al. investigated the performance of Principal Component Analysis algorithm in intrusion detection, determining the Reduction Ratio (RR), the optimal quantity of key features required in abnormality detection along with the causes of noisy data in PCA in [17]. They used the two standard datasets, KDD CUP and UNB ISCX, it conducted PCA test employing several classifier techniques. Experiments have shown that the top ten major components are efficient in classification. Conversely, the model does not suitable for real-time IDS and it has timing overhead, also it requires serious implementation overheads.

Intrator et al. [18] demonstrated how GANs are utilized to produce additional training samples for classifiers, hence increasing their accuracy and robustness. GANs, on the other hand, are exclusively employed to reconstruct existing data instead of producing new ones in anomaly detection. In most domains, this is due to the modest number and be deficient in of assortment of anomalous data. GAN proposed a unique GAN architecture for enhancing anomaly detection by generating more samples in this work. In this they deployed two types of discriminators: first one consist of dense network to determine to check that the generated samples exhibits adequate quality, and second part consists of an auto-encoder to detect anomalies. GAN facilitates us to accomplish major competing objectives: in first it provides superior quality samples that deceive the first discriminator, then it produce samples which that second discriminator is capable of successfully reconstruct, hence improving the efficiency. The approach's strengths are demonstrated via empirical examination on a wide collection of datasets. But, the model consumes high energy and it could be only employed to detect a restricted number of attacks.

Seo et al. focused on reducing the dataset's class imbalance in [19]. The goal was to use the Synthetic Minority Oversampling Technique (SMOTE) for maximizing SMOTE ratios for U2R, R2L, and Probe unusual classes. In subsequent to the constructing of random number of SMOTE ratio tuples, build an essential mathematical model using the tuples in order to improve the SMOTE quotients of unusual classes. Then the Model was built using support vector regression and allocated to each

occurrence in the test dataset, and the best SMOTE ratios were chosen. The optimum ratios were used in the studies using machine-learning algorithms. The approach produced much better outcomes than the previous approach and other comparable work. Due it the complexity in building, the whole model building process takes practically an extended duration.

Najeeb et al. discussed how to implement IDS for effective attack detection in [20]. The Firefly Algorithm (FA), a new binary feature selection method, is employed and executed as a result of this. The FA chooses the most appropriate amount of features from the NSL dataset. Furthermore, FA is used with multi-objectives based on accuracy of classification and quantity of features being used at related time. It is proved that it is a valuable approach to detecting threats and reducing false alarms. The categorization and feature selection techniques improved the IDS's performance in detecting attacks. The method have several limitations with respect to energy usage, packet overhead, and memory utilizations along with the high false positive rate, focused to detect only one specific type of attack with low accuracy.

Rahman et al. suggested an innovative attack detection model for IoT networks employing the Artificial Neuro-Fuzzy Interface System (ANFIS) in [21]. ANFIS changes the rules and membership parameters depending on input-output profile using a hybrid back propagation and learning approach. Sugeno type ANFIS has been discussed in this study. The ANFIS model may accept dynamic information like nature of packet traffic stream, liveliness of devices, energy level, size of the data packet, travel rate etc., IP address of source and IP address of destination, source-destination ports address, consider to be an input profiles and output profiles to construct the current network security state. The effectiveness of ANFIS attack detection model is compared to attack detection models based on fuzzy logic implementation with the help DNN, which applies pattern matching algorithm. The model outperforms previous methods depending on confusion matrix, MSE, MAE errors along with detection accuracy in terms of trustworthiness. Even though the model exhibits competency in detecting intrusions, it is proven that capable of detecting limited number of attacks and not proficient in real-time applications. And also, the approach strongly depends on the knowledge of the network administrator, similar to specification-based methods in which specifications will increase the false positives and false negatives rate.

Yao et al. [22] designed an innovative IDS structure using Hybrid Multi-Level Data Mining (HMLD), assessed on the KDDCUP99 dataset. The classification phase deals with filtering each attack with an explicit classifier trained to detect the attack. They preferred SVM-linear classifier

for detecting DOS attacks. ANN-*logistic* for Probe, here ANN-*can* recognize for U2L and ANN-*relu* for R2L. The overall model precision in the KDDCUP99 dataset was 96.70%. In this work they create a special class for unknown intrusions, achieved a lower temporal complexity than ANN and SVM, Although it has been proved higher accuracy, they did not address multiclass classification precision for distributed environments.

Toupas et al. [23] proposed a new local–global computation paradigm, FEDFOREST, a novel learning-based NIDS by combining the interpretable Gradient Boosting Decision Tree (GBDT) and Federated Learning (FL) framework. Specifically, FEDFOREST is composed of multiple clients that extract local cyber attack data features for the server to educate models and detect intrusions. A privacy-enhanced strategy is also planned in FEDFOREST to further conquer the privacy of the Federated Learning models. Widespread experiments on 4 cyber attack datasets of diverse tasks expresses that FEDFOREST is valuable, competent, interpretable, and further implementable. Although the model is proven to be efficient in local cyber attacks, it has not addressed the concern of network related unknown attacks.

Tian Dong et al. [24] proposed an efficient Federated Learning -based Network Intrusion Detection system. In particular, they influence the attribute of network traffic data, by modification of small change without affecting the natural feature, and apply data binning to extract feature data on clients. These feature data are applied for training the classifier at the server end [. Although the proposed algorithm efficiently detects internal intrusions attacks, it does not address the external and unknown attacks and it is has limitation on client device performance.

From above literature reviews, we found that in recent time’s integration of ML/DL-based approaches have been widely employed for intrusion detection in IoT. The Existing IDSs have been developed by assuming that IoT devices have the same feature pattern and packet types. But in reality, IoT devices heterogeneous in features such as hardware features and operations, computational ability. The features become meager when nodes are aggregated to create data and the inappropriate features or attributes are set to either nulls or zeros which major disadvantage have impact on detection accuracy and efficiency of data modeling.

Hence the Feature selection, is a significant part of a ML/DL-based solution, plays a key role in improving the detection accuracy and reduces the duration of the training phase. It has been observed that, IDSs in the IoT

environment still needs enhancements with respect to detection accuracy, increasing true positive rate, and reducing energy consumption. Even though above-mentioned deep learning techniques in the IoT network intrusion detection have achieved adequate results.

However, still it is very difficult in achieving zero attack efficiency in the problem of insufficient data for training and complex high dimensional data collected from IoT network., Hence The main challenge of this research work is to detect intrusion over the complex and time-varying dynamic IoT networks, here the intrusion samples are cohesive with normal samples hence the leads to insufficient model training samples and also detection results will might consists of high false detection rate.

To overcome above challenges a lot of exploration and techniques are popularized but the existing Distributed Generative Adversarial Network based IDS does not accomplish detection accuracy greatly. The current trendy is that generally the NIDSs are designed through anomaly detection to examine network traffic are non-interpretable for further improvement and robustness. conversely; an anomaly detection-based NIDS has several challenges such as accuracy is depends on training data quality, it is still difficult recognizes the attack category automatic without human intervention, lack scalability, hence the significant enhancement on the ML models is mandatory for training a new model in privacy sensitive scenarios.

In the existing deep learning models a Centralized deployment of IDS is usually done for the small networks with low scalability Decentralized and Distributed architectures deploy multiple IDS for active detection of attacks and also some research work describes about Federated Learning provides a server-client architecture that involves computation at the server end (i.e., model aggregation) as well as the client end (i.e., model training). This style of work division prevents the server from becoming the bottleneck while taking advantage of edge computation. But still, majority of the existing methods have constraints’ on computational complexity and imprecise IDS classification outcome. In order to crack the challenges is IFFA-HDLCNN + ANFIS proposed to improve detection performance which is not depends on centralized server or federated learning models. In this proposed a novel intrusion detection model which employs dynamic distributed model DD-GAN Model which is constructed with an enhanced deep neural network model to classify the network traffic which has blended integration of centralized distributed model approaches.

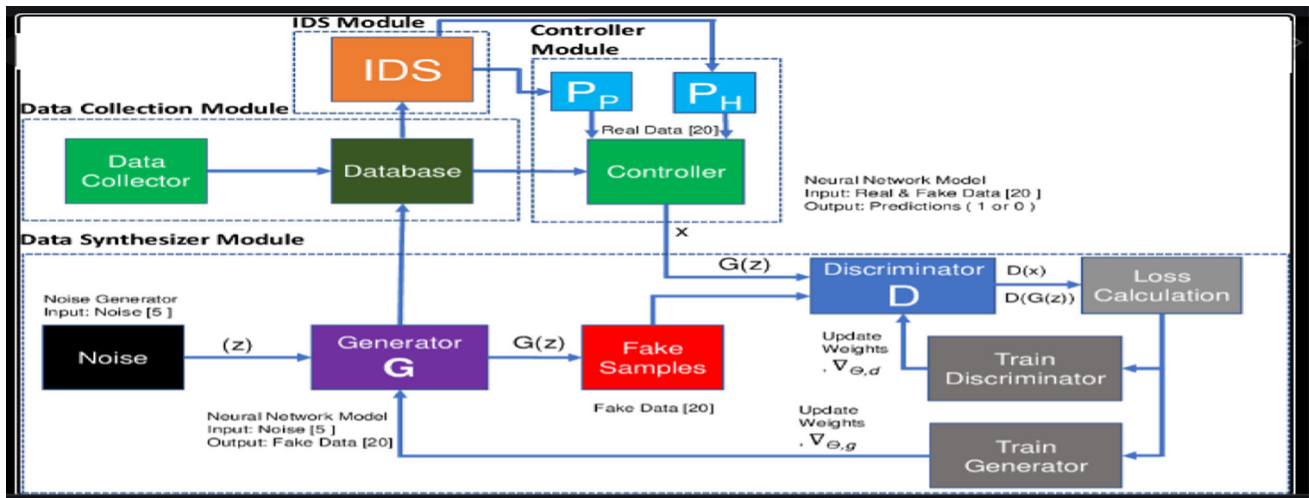
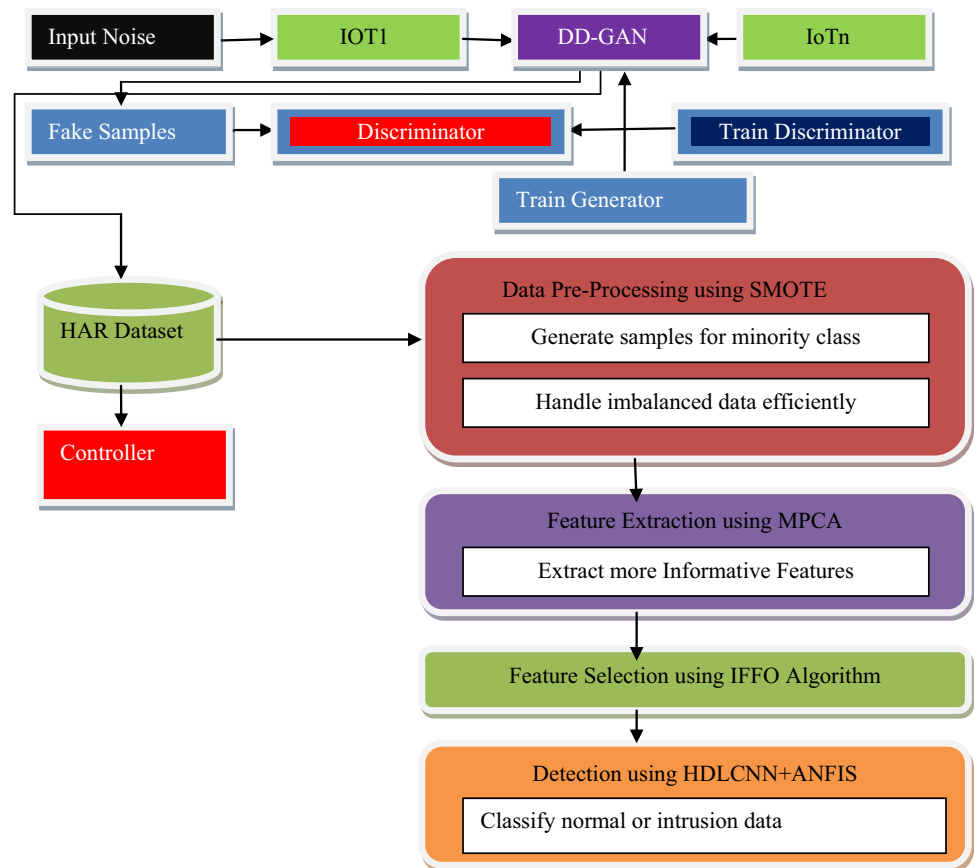


Fig. 1 GAN with IDS Framework

Fig. 2 Overall framework of the proposed DD-GAN with IFFO-HDLCNN + ANFIS system



### 3 Proposed methodology

To detect the heterogeneous intrusion attacks in distributed IoT networks, a Dynamic Distributed—Generative Adversarial Network (DD-GAN) with IFFA-HDLCNN +

ANFIS is suggested in this study. The suggested technique entails the creation of a DD-GAN structure, performing pre-processing, feature extraction, feature selection, classification, and performance evaluation. Figure 2 illustrates the suggested method’s overall block diagram.

### 3.1 Construct dynamic distributed (DD)–GAN model based on IoT system for IDS

DD-GAN is built in this work to identify intrusions more efficiently in the distributed IoT networks. GAN is one of deep learning's most powerful and promising tools which use an adversarial technique to estimate a generative model which consists of twin models: the generator (G) along with discriminator (D). Over real data space  $x$ , the generative model G calculates the data distribution  $p(g)$ . G intends to produce fresh adversarial samples  $G(z)$  from the identical allocation of  $x$  given an input noise variable  $p(z)$ .

In the suggested DD-GAN based IDS, a number of machines are found to be linked to a single server,  $N$  systems are associated with a single server in the same way and every system has the own distinct address. A single server may monitor entire systems in real time, while the user can watch each client system separately. The goal is to discover the best generator and discriminator algorithms for a standalone IoT. Hence the DD-GAN based IDS also employed to effectively identify both known internal and unknown external attacks. The performance of the system may be improved and information can be transferred more simply when employing DD-GAN based IDS [25].

The discriminator unit D, conversely, provides the probability  $D(x)$  which provided sample  $x$  originated from an actual data set instead of being created by G. G's ultimate purpose is to increase likelihood that D will mistake created data for genuine data, while D's goal is to do the exact reverse [26]. As a result, G and D act as two-players to play a minmax game until they find a unique solution. The following is the definition of the value function  $V(G; D)$ :

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

Assume an IoT system with  $N$  of  $n$  IoTDS, each of which  $i$  hold a collection of earlier sent data points,  $D_i$ , which follow a distribution  $p_{data}^i(x)$ , wherein  $x$  can represent time series, statistical data records, health monitoring data, according to the IoT application. It is assumed to be  $D_i$  have data points from IoTDS's standard position, where there is no IoT intrusion. It also allows  $D_1 \cup D_2 \cup \dots \cup D_n = D$ , where  $D$  the total accessible data and  $p_{data}$  is the distribution. Each IoTDS  $i$  in this system try to train a generator with distribution  $p_{g_i}$  through the accessible dataset  $D_i$  hence  $p_{g_i} = p_{data}$  and uses the distribution for identifying malicious actions.

Any behavior by an attacker which affects an IoTDS to communicate data points which is not belongs to their respective data distribution  $p_{d_i}$  is considered a system intrusion, Actually, if an IoTDS knows the about its specific normal state distribution, it can quickly distinguish a data point varies with the usual state distribution. It defined a previous input noise  $z$  contains distribution  $p_{z_i}(z)$  along with mapping  $G_i(z, \theta_{g_i})$  with the random variable  $z$  to data space, in this where  $G_i$  considered as ANFIS contains parameters  $\theta_{g_i}$ , which is used for learning the distribution  $p_{g_i}$  at every IoTDS  $i$ . the structure of ANFIS is made up of fuzzy, product, normalized, defuzzify layers that plots an input to an output layer. For each IoTDS  $i$  it creates a discriminator  $D_i(x, \theta_{d_i})$  that collects a data point  $x$ , compute and output value in between 0 and 1. Whenever the discriminator's result value is nearer to 1, then the established data point is in a normal state, and otherwise the result is nearer to 0, the received data represents irregularity at IoTDS  $i$ .

The discriminator aims to maximize the value function defined in (1), but each IoTDS's generator would endeavor to decrease it. Hence, we apply minmax problem is used to obtain best discriminator and generator solutions.

$$\{D_i^*, G_i^* = \arg \min_{G_i} \arg \max_{D_i} V_i(D_i, G_i) \quad (2)$$

Distributed GAN-based IDS is given here, which is formed on architecture described in [27]. The dynamic distributed GAN designed with the intension to discover a discriminator at each IoTDS which does not of require them to share their datasets, so that each IoTDS's discriminator be able to dynamically classify when a novel data point follows overall data distribution,  $p_{data}$ . Primary distinction between distributed and individual IDS learns to distinguish the new data point to the own data distribution,  $p_{data_i}$ , hence the proposed DD-IDS, each IoTDS can evaluate a new data point to overall data distribution,  $p_{data}$ . As a result, because each IoTDS's discriminator understands the distribution of total data in distributed IDS, each IoTDS might capable of detecting abnormalities, intrusions in the other neighbor IoTDSs.

Only during the training phase of the DD-GAN does it utilize a central unit with generator  $G_\varphi$ , here  $\varphi$  represents the weights of generator's ANFIS, Additionally, each IoTDS contains one discriminator,  $D_{\theta_i}$  wherein  $\theta_i$  is weights of each discriminator's ANFIS. Every IoTDS in a dynamic network is linked to at least one other IoTDS in the architecture, which helps the IoTDS's connection graph to structure a cycle. Furthermore, every IoTDS is associated

with central node in the entire training phase.  $T$  denotes the number of epochs during which IoT devices correspond to centre, and  $E$  denotes the number of epochs while that IoT devices attached with all. In The training session epoch the ANFIS weights are updated using all of the data points.

### 3.2 Data pre-processing is performed via synthetic minority oversampling technique (SMOTE) technique

Pre-processing is done in this study via SMOTE technique to efficiently improve the imbalanced dataset. It takes care of minority sampling, which is utilized to enhance intrusion detection accuracy for the Human Activity Recognition (HAR) dataset. The basic goal of balancing classes is to increase the frequency of minority classes whilst decreasing frequency of majority classes in which both classes might get roughly the same number of instances by doing these behaviors. The SMOTE techniques is used in this model to balance the classes where the minority class would be over-sampled through selecting each sample and interleaves artificial instances through line segments combining random of  $k$  minority group adjacent neighbors. To calculate amount of over-sampling required according to this select the neighbors from the  $k$  nearest neighbors at random for this SMOTE employs  $K$ -nearest neighbors to generate the artificial data [28]. In the SMOTE approach, the following procedures are carried out for the minority class.

Step 1: compute difference among feature vector (sample) in concern and the nearest neighbor.

Step 2: The difference is multiplied by an arbitrary value between 0 and 1.

Step 3: The results are incorporated into the feature vector in concern.

Step 4: Select a random point along the line segment any between two particular features.

Step 5: Give the new synthetic minority class sample a value.

Step 6: Repeat the procedure for all feature vectors that have been identified.

In order to synthesize samples (for minority class) among these neighbors, it must determine the nearest neighbors of a point in the  $d$ -dimensional space. Here the random distribution of data to various nodes in a dispersed cluster may allow points that are closest to one another to be disseminated to various nodes, rendering individual nodes unaware of these closest neighbors. As a result, SMOTE vital to group the nearest points together and then distribute them to the other nodes in a way that they're always analyzed on same node which proves that the SMOTE method effectively tackles the issue of data imbalance.

### 3.3 Feature extraction using modified principal component analysis (MPCA)

Here, MPCA method for feature extraction is suggested, with the goal of reducing the amount of features. In this PCA reduces the enormous dimensionality of observed variables to less significant essential dimensionality of feature independent variable, for economically enlighten the data. When there is a substantial association between observed variables, then the PCA fruitfully diminishes the number of features by eradicating minor components and demonstrates the data set in a low-dimensional subspace [29, 30]. We here used the multivariate data analysis technique called a PCA is employed to extort linear features in which coefficients are employed as feature vectors to effectively represent the IDS dataset, when extracting features from a tiny dataset the standard PCA approach will miss significant feature information. The information linked to the relevant classes cannot be efficiently compressed using the PCA approach. Modified PCA is provided to prevent the aforementioned concerns.

To decrease the eigenvectors influence associated to huge eigenvectors in MPCA method by normalizing the  $i$ th feature vector  $y$ 's  $j$ th constituent  $y_{ij}$  with regard to the standard deviation,  $\sqrt{\lambda_j}$ . As a result, the new feature vector  $y'_i$  has been rewritten as

$$y'_i = \left[ \frac{y_{i0}}{\lambda_0}, \frac{y_{i1}}{\lambda_1}, \dots, \frac{y_{i(r-1)}}{\lambda_{r-1}} \right] \quad (3)$$

A new feature subspace is built using these normalized feature vectors. In this method, the feature vectors are first normalized by square root of respective eigenvalues, and then distance among training and testing features is calculated.

Linearly transform (PCA) is represented as the subsequent equation in general:

$$Y = TX \quad (4)$$

$T$  stands for transform matrix,  $X$  for original vectors, and  $Y$  for transformed vectors. The following equation can be used to solve the transform matrix  $T$ :

$$(\lambda I - S)U = 0 \quad (5)$$

Is computed,  $I, S, U$  and  $\lambda$  are square matrix contain unity in the diagonal, which are the covariance matrix of real images, the eigenvectors and the eigenvalues.  $U_j$  and  $\lambda_j (j = 1, 2, \dots, m)$  are calculated by Eq. (2), along with the eigenvalues ordered as  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_m$ . Eigenvectors  $U$  can be indicated as  $U = [U_1, U_2, \dots, U_m]$ .

The MPCA selects training samples from an IDS dataset that are relevant for a given application, and the transformed matrix  $T'$  is derived from these training examples. The following equation can be used to express it:



$$Y = T'X \quad (6)$$

$$V_N = b_1u_1 + b_2u_2 + \dots + b_Nu_N \quad (7)$$

$$S = \sum_{i=0}^1 b_1u_1 1N \quad (8)$$

In which  $N$  denotes the amount of data. When comparing Eqs. (7) and (8), the difference is in transform matrix, and more specifically, in the samples used to calculate covariance matrix; one is based on training samples, while the other is based on entire hate speech dataset.

MPCA is a mathematical process that maps data gathered from a multi-dimensional observed variable space to a low-dimensional space which contains essential features with the help of linear transformations. In linear transformation we can use Eigen vectors of the covariance matrix to identify the essential feature (low-dimensional space). The error-minimizing and de-correlating properties are used in this work to identify valuable important intrusion features for a human activity identification dataset. As a result, MPCA is able to successfully decrease the enormous dimension of datasets by concentrate on coordinates with high variance values rather than low variance data. The normal and intrusion data input data have properties such as mean and standard deviation.

(i) Mean = sum of no of data /total number of data (9)

(ii) Standard deviation : denoted as root – mean square

*deviation*– for finding the square root of means of squared deviation from arithmetic mean.

$$\sigma = \sqrt{(\sum(x - \bar{x})^2)/N}$$

#### Algorithm 1: MPCA

1. Start
2. Determine the mean value  $S'$  of the IDS dataset  $S$ .
3. Subtract  $S$  from mean value.
4. Obtain the newly created matrix.  $A$
5. The matrix,  $C = AAT$ , is used to calculate covariance. The covariance matrices  $V_1V_2V_3V_4\dots V_N$  are used to calculate Eigen values.
6. Lastly, Eigen vectors for the covariance matrix  $C$  are computed.
7. Using the formula (7), any vector  $S$  could be articulated as a linear combination of Eigen vectors
8. To construct a reduced dimension data collection, only the largest Eigen values are maintained.
9. Match the feature combinations in the given IDS dataset (8)
10. Using the mean and standard deviation, compute the feature (9) & (10)
11. Extract the more useful features (intrusion features)
12. End

The MPCA algorithm is utilized to extract important features from a dataset as well as to reduce feature dimension effectively.

### 3.4 Feature selection using improved firefly optimization (IFFO) algorithm

The IFFO method is used to choose features in this study. As a biologically stochastic global optimization strategy, the Firefly algorithm (FA) was created [31]. Here Firefly Algorithm simulates a population-based meta-heuristic that considers every firefly in the population as a possible search space solution. Hence the Firefly algorithm imitates the behavior of fireflies mating for exchanging information using flash lighting. They also employ flash lighting to attract potential prey and serve as a warning system.

The FA has three principles that describe firefly behavior:

- (i) All the fireflies capacity of attracted to each other, they are unisex;
- (ii) Attractiveness is relative to brightness, so any pair of fireflies, which has the low brightness, will be attracted to the brighter firefly. Hence the attraction, on the other hand, will be decreased while the distance among the two fireflies rises
- (iii) The fitness function is linked to the brightness of the firefly; if there is no firefly brighter than the present one, it will attract at random

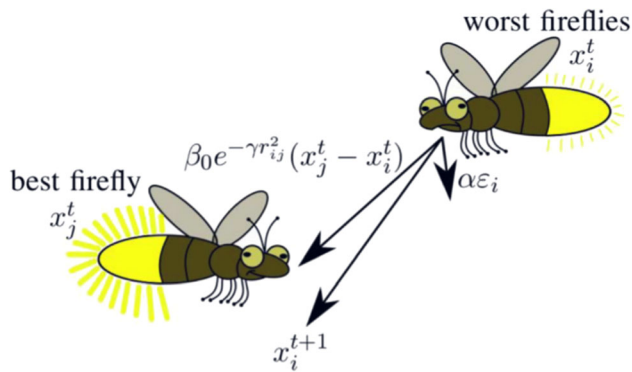
There are two key points in the traditional firefly approach. One is the change in attractiveness, while the other is the formulation of light intensity. To begin with, the encoded objective function landscape can always be assumed to determine the brightness of firefly. Second, it must specify variations in light intensity as well as changes in attractiveness. Since light intensity  $I$  changes exponentially and monotonically along the distance  $r$ , light absorption parameter and intensity [32] in nature, assume that light intensity  $I$  differ exponentially and monotonically for the distance  $r$  and light absorption parameter  $\gamma$ . specifically

$$I = I_0e^{-\gamma r^2} \quad (11)$$

Here  $I_0$  is initial light intensity at source ( $r = 0$ ),  $\gamma$  is light absorption coefficient. This is derived from idealized principles that the attraction of a firefly in simulation is related to light intensity  $I$ . With effect of this consequence, it can describe the firefly's light attractive coefficient  $\beta$  and also the light intensity coefficient  $I$ .specifically

$$\beta = \beta_0e^{-\gamma r^2} \quad (12)$$

Here  $\beta_0$  is actual light attractiveness at  $r = 0$ .



**Fig. 3** Basic mechanism of the Firefly Algorithm

Cartesian distance formula will be employed to determine distance between any two fireflies  $i$  and  $j$  at  $x_i$  and  $x_j$

$$\text{Cartesian distance } r_{i,j} = \sqrt{\sum_{k=1}^d (x_{i,k} - x_{j,k})^2} \quad (13)$$

Here  $d$  is number of dimensions. Distance of movement of firefly  $i$  to a different more attractive (brighter) firefly  $j$  is defined by

$$x_i = x_i + \beta_0 e^{-\gamma r^2} (x_j - x_i) + \alpha \left( \text{rand} - \frac{1}{2} \right) \quad (14)$$

Here the first term represents present location of firefly,  $i$  represents movement of attraction between two fireflies. The second element is related to attraction, and  $\beta_0$  is the starting attractiveness, which is always set to 1, as well as the absorption coefficient  $\gamma$ , which governs the speed at which fireflies converge. The third term is randomization, which is represented as a vector of random variables marked by the random number for the new member chosen  $i$ .  $\alpha$  is a scaling parameter which regulates step size and has to be related to the problems' interests.

The objective function calculates the firefly's brightness in statistical form. Figure 3 depicts the key idea of the firefly method.

The Firefly algorithm was chosen for the ability to provide most favorable optimal results to the multi-objective situations. The maximization of brightness is proportional to corresponding objective function. To provide simple solution, it is assumed that a firefly's attractiveness is illustrated by the brightness or light intensity, which is associated to the encoded objective function.

An adaptive firefly method (IFFO) is created by introducing an adaptation parameter for both the absorption and random parameters. By altering the parameter linearly during iterations period, these modifications improve the global and local search capabilities [33].

Compute  $\alpha$  as:

$$\alpha(t+1) = \left( 1 - \frac{t}{\text{MaxG}} \right) \alpha(t) \quad (15)$$

$\alpha$  adapts the value to optimization's distance deviation degree for the purpose of improving the solution precision and convergence speed. Simultaneously, with the aim of improving population flexibility, it is reformulated as follows:

$$\alpha = \alpha_{\min} + (\alpha_{\max} - \alpha_{\min}) \times \|x_i - x_{\text{best}}\| / L_{\max} \quad (16)$$

$$\text{Where } L_{\max} = (x_{\text{worst}} - x_{\text{best}}) \quad (17)$$

The features  $\alpha_{\max}$  and  $\alpha_{\min}$  are the maximum and minimum, correspondingly. In Eq. (17),  $x_{\text{worst}}$  worst denotes worst individual's location at generation  $t$  firefly, and  $L_{\max}$  is distance among worst individual  $x_{\text{worst}}$  and the global optimal individual  $x_{\text{best}}$ . The firefly individuals are dispersed throughout the space in the early stages of the procedure, and the majority of them are far away from the globally optimum individuals. The value of  $\|x_i - x_{\text{best}}\|$  is bigger at this stage, and  $L_{\max}$  and  $(\alpha_{\max} - \alpha_{\min})$  are fixed values. As a result of Eq. (16), the value of  $\alpha$  is bigger in the early stages, resulting in a better global optimization impact. Individual  $i$  is fascinated by brighter fireflies than itself, and is near to global optimal features, as algorithm implementation. In the future, firefly individuals  $i$  will cluster near the global ideal individuals; value of  $\|x_i - x_{\text{best}}\|$  will be reduced at this point, which will make it easier to increase the cloud search for optimal features. The  $\alpha$  is modified with the position of the optimum in each iteration, that enhances algorithm's convergence speed [34]. The ability of algorithm creation and search, as per the aforementioned study, the step size factor varies adaptively and dynamically depending on distance among individuals of firefly.

Algorithm 2: IFFO for feature selection

**Input:** Let us define the Population size ( $n$ ), Maximum of iteration ( $\text{maxIter}$ ), Absorption coefficient ( $\gamma$ ), Randomization parameter ( $\alpha$ ), prettiness or attractiveness value ( $\beta_0 = 1$ ).

1. Consider that  $n$  be the swarm size of firefly, input  $X_i = \{x_1, x_2, \dots, x_n\}$ , mission data
2. Objective function ( $f(x)$ ,  $x = (x_1, \dots, x_n)^T$ ) consider higher accuracy of classifier as objective function
3. Produce initial population of fireflies  $x_i$  (where  $i = 1, 2, \dots, n$ )
4. Light intensity  $I_i$  on  $x_i$  is determined via  $f(x_i)$
5. Describe light absorption coefficient  $\gamma$
6. Verify the condition while ( $t < \text{MaxIter}$ )
7. For  $i = 1:n$  every  $n$  fireflies
8. For  $j = 1:i$  every  $n$  fireflies
9. if  $(I_j > I_i)$  is satisfied, progress firefly  $i$  towards  $j$  in  $d$ -dimension;
10. End if

11. Attractiveness changes along with distance  $r$  via  $\exp[-\gamma r]$
12. Determine fitness function using (14)
13. Evaluate objective model using (13)
14. Estimate latest solutions using this update light intensity using (11)
15. Update the optimal features using (16)
16. End for  $j$
17. End for  $i$
18. grade the fireflies to discover the greatest firefly
19. End while
20. A firefly  $i$  shifts to a more attractive

The IFFO technique is utilized in this scenario to generate optimal solutions by increasing the energy and interruption measures. Then the fireflies can be sorted in the IFFO method, and the best fitness values are used to select the best firefly. Crossover and mutation are used by the chosen fireflies to reproduce among them. The best new solutions are inserted to the firefly pool, and then the firefly iteration process continues. Every firefly in the searching space moves in a specific direction with the goal to find most excellent feature subset according to the correctness of classifier model by using the essential subset of features chosen. The precision of the evaluator is depends on supplied feature, brightness of firefly as an objective function. When Eq. (13) and the distance between the two fireflies are taken into account, the firefly with lower accuracy/brightness would fly toward firefly with higher accuracy/brightness (16).

### 3.5 Hybrid deep learning based convolutional neural network with artificial neural network (HDLCNN + ANFIS) for intrusion detection

The Hybrid Deep Learning method integrated to Convolutional Neural Network architecture and blended with Artificial Neural Network (HDLCNN + ANFIS) approach is used to detect intrusions in this study. The method initiates by gathering data from sensors that cover the entire record in a dataset. The fuzzy integration system Adaptive Network Based Fuzzy Inference System (ANFIS) is made up of two primary mechanisms: 1) logic rules-if-else and 2) input–output data integrated with fuzzy logic is trained on neural networks. ANFIS is a nonlinear (complex) problem-solving model. Using the ANFIS training procedure [35], the ANFIS manages the membership function and related parameters. The back-propagation learning algorithms together with least squares approach are combined in the ANFIS learning algorithm. This ANFIS structure is effective in resolving complex noisy problems.

By using method, an early fuzzy model and the input variables are created using rules taken from the system's

input output data. The Neural Network will be employed to refrain the initial fuzzy model rules, resulting in system's ultimate ANFIS model and utilized to develop adaptability, rapid convergence, and high accuracy for a database. The ANFIS algorithm flowchart is shown in Fig. 4.

ANFIS' internal structure can be separated into two parts: antecedent and consequent. These two sides are linked together by rules in the form of a network [36]. ANFIS discovers fuzzy rules using the given set of input–output data in first phase, and then refines those rules with a neural network in the second phase. By means of the inputs  $x$ ,  $y$ , and output  $Z$ , then the typical Takagi–Sugeno rule set can be described as:

$$\text{if } x \text{ is } A_1 \text{ and } y \text{ is } B_1 \text{ then } f_1 = \alpha_1 x + \beta_1 y + r_1 \quad (18)$$

$$\text{if } x \text{ is } A_2 \text{ and } y \text{ is } B_2 \text{ then } f_2 = \alpha_2 x + \beta_2 y + r_2 \quad (19)$$

here  $\alpha$ ,  $\beta$  and  $r$  indicates linear output parameters. It comprises five layers and two types of nodes, which are represented by circles and squares, respectively. The adaptable node, which receives parameters, is known as the square node. The fixed node is the circle node, which does not accept any parameters. The ANFIS algorithm's uniqueness significantly improves the convergence speed for larger image datasets. As a result, it delivers improved prediction results for the supplied dataset in terms of intrusion or normal feature.

#### 3.5.1 Training of the discriminators

The generator generates  $2n$  batches  $\{B_{a1}, \dots, B_{an}, B_{g1}, \dots, B_{gn}\}$  of  $b$  abnormal points, i.e. forged points which were not obtained from the genuine datasets,  $T$  epochs, for a fixed  $\phi$ . Furthermore, at every IoTD  $i$  the discriminator selects a bunch  $B_{ri}$  of  $b$  points from the existing dataset  $D_i$ . Every created batch  $B_{ai}$  is sent to all IoTD  $i$  then computes the loss value as follows:

$$L_i(\theta_i) = \frac{1}{b} \left[ \sum_{x \in B_{ri}} \log D_{\theta_i}(x) + \sum_{x \in B_{ai}} \log(1 - D_{\theta_i}(x)) \right] \quad (20)$$

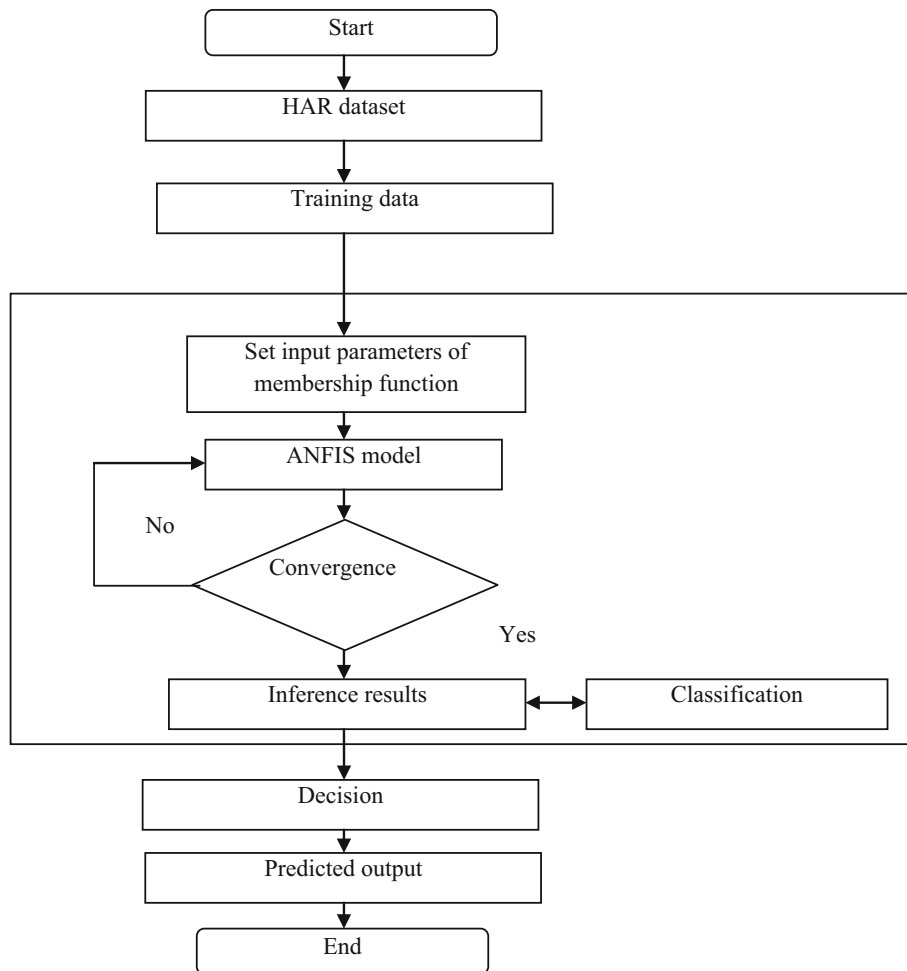
The value function for every IoTD's discriminator in  $L_i(\theta_i)$  is a rough estimation of the value function (1). The IoTD then adjusts the own weights  $\theta_i$  by applying the gradient descent algorithm like the Adam optimizer [31].

#### 3.5.2 Training the central generator

Each  $T$  epochs, each IoTD  $i$  employ  $B_{gi}$  for computing the subsequent loss:

$$L_i^g = \frac{1}{b} \left[ \sum_{x \in B_{gi}} \log(1 - D_{\theta_i}(x)) \right] \quad (21)$$

**Fig. 4** ANFIS algorithm flowchart



This would be an approximation of every IoT's generator's value function in (21).

For more accurate intrusion detection with less calculation time, DLCNN is paired with ANFIS. The structure of DLCNN contains an input and output layer, several hidden layers. In the hidden layers enclosed with DLCNN, convolutional layers, pooling layers, along with fully connected layers are frequent. Before transferring the output to next layer, convolutional layers takes input perform a convolution on that. The convolution models the response of a single neuron to represent as visual motivation. In convolutional networks, local and global pooling layers joining the outputs of neuron clusters in one layer into a distinct neuron in the next layer. The average value derived from every cluster of neurons used for mean pooling. We take all the neuron in one layer can be combined to neurons exist in different layer in fully connected layers. In theory, DLCNN is similar to the standard multi-layer perceptron NN [37]. In the Suggested HDLCNN have three layers: input, convolutional, and classification. For assessing high-dimensional data, the suggested methodology has apparent advantages. For

reducing the parameters in convolutional layers we employ a parameter sharing technique.

In this the input layer collects intrusion features from training samples which unifies the data so that it may be sent correctly to the following layer. This layer may establish the essential metrics, namely scale of local receptive fields and the variety of filters.

Convolution layer (Cx) uses a convolution method to process the input data and creates numerous layers called feature maps, which are built through the convolution computation outcome from previous layers. It is mainly employed to extract critical features and to reduce network's computational overhead.

And then for each convolutional layer, an activation function may be utilized. Activation function is employed for mapping an output to the collection of inputs, resulting in a non-linear network structure. Initially we set the connection weights to complete set of feature values. After then, a newly generated input pattern is used, result is calculated as

$$y(n) = f\left(\sum_{i=1}^{i=N} w_i(n)x_i(n)\right) \quad (22)$$

$$\text{here } f(x) = \begin{cases} +1 & \text{if } x \geq 0 \\ -1 & \text{if } x < 0 \end{cases} \quad (23)$$

here  $n$  is iteration index.

We update Connection weights as per

$$w_i(n+1) = w_i(n) + \eta(d(n) - y(n))x_i(n), \quad (24)$$

*where*  $i = 1, 2, \dots, N$

Here  $\eta$  is gain factor.

Then determine and employ standard deviation

$$\sigma = \sqrt{\frac{1}{n} \sum f_i(x_i - \bar{x})^2} \quad (25)$$

These weighted intrusion features were sent to the suggested ANFIS network, which resulted in enhance accuracy in classification. The foremost finding of the study evaluated on the same set of data is established by the polynomial distribution function.

**Layer of Classification:** The data passes through several convolution layers, output feature maps size reduces. Each feature map in classification layer is made up of single neuron and produces a feature vector. A classifier is completely correlated to the vector.

**Algorithm 3: Steps in HDLCNN + ANFIS**

1. IDS dataset Procedure
2. For every input feature, define intrusion feature  $\in$  IDS dataset do
3. For each neurons, input features do
4. Conduct Training to the ANFIS model through Fuzzify and defuzzify process using (18) and (19)
5. Hybrid DLCNN with ANFIS in DD-GAN
6. Transform the input into convolution and classification layers
7. identify intrusion features by applying (22)
8. Choose more useful and appropriate features
9. Conduct training and testing procedure for specified database through (24) and (25)
10. Replicate predefined intrusion feature label for every feature according to the input dataset
11. Distinguish extremely precise intrusion outcome.

There will be no need for the central unit when the DD-GAN federated in which every discriminator at IoTDs in a position to identify the intrusion encountered. Hence, each IoTD process it is observed real-time data via both the own and one of the neighbors' discriminators. In a given normal state data point, the best discriminator will output 1/2. As a result, discriminator output is contrasted with 1/2 to detect a system intrusion, and when output is near to 1/2, the IoTD assumed to be in the normal state. When output

is close to 0 or 1, however, there is a possibility that IoTD is attacked. Because each IoTD examine the neighbor's data, this approach permits IoT system to identify an intruder independently without the using the central unit. By developing a technique wherein each IoTD observes neighboring IoTDs, the suggested DD-GAN architecture delivers effective IDS. The HDLCNN + ANFIS framework is shown in Fig. 5.

## 4 Experimental result

In this experimentation the daily activity recognition database [38] is utilized, which was acquired via a smart phone from 30 people of various genders, ages, heights, and weights. This dataset was selected since it is a superior example of health datasets gathered with the help of wearable IoTDS. To preserve privacy on this sensitive the health datasets are kept personal and they don't wish to share the data. We have taken human actions such as Walking forward, walking left, walking right, walking staircase, leisurely moving forward, fitness values, heart beat samples, blood pressure values, walking downstairs, running, skipping, running forward, sitting, footing, resting, idle, breathing, elevator up, and elevator downward for which data were gathered. The dataset comprises a collection of 2,365 recordings, each of which has 565 frequency and time domain variables. It divides the dataset as 75% for training and 25% as test datasets. Existing techniques like centralized GAN, D-GAN with ANN, and D-GAN with EWO-HDLCNN + ANN are compared to the new DD-GAN with IFFO-HDLCNN + ANFIS method in this study. The accuracy, precision, recall, f-measure, FPR, and computational complexity of traditional centralized GAN [39], D-GAN with ANN [40], D-GAN with EWO-HDLCNN + ANN, and DD-GAN with IFFO-HDLCNN + ANFIS methodologies were compared using performance measures-accuracy, precision, recall, f-measure, FPR, computational complexity. The experimentation and evaluation is conducted in IOT simulation environment and implemented using python language. The proposed model has been designed with major objective of detecting intrusions with higher accuracy in IoT network. The dynamic Deep-GAN model enhances the detecting performance by reducing the false positive Rate to ensure efficient intrusion detection and robust in any real time IoT environment. The experimental results shows the proof higher detection rate by Deep GAN model compared with the existing machine learning models the higher performance is achieved by an ability to detecting abnormal data. Although there are certain limitation have been encountered in training the GAN network, since it has been

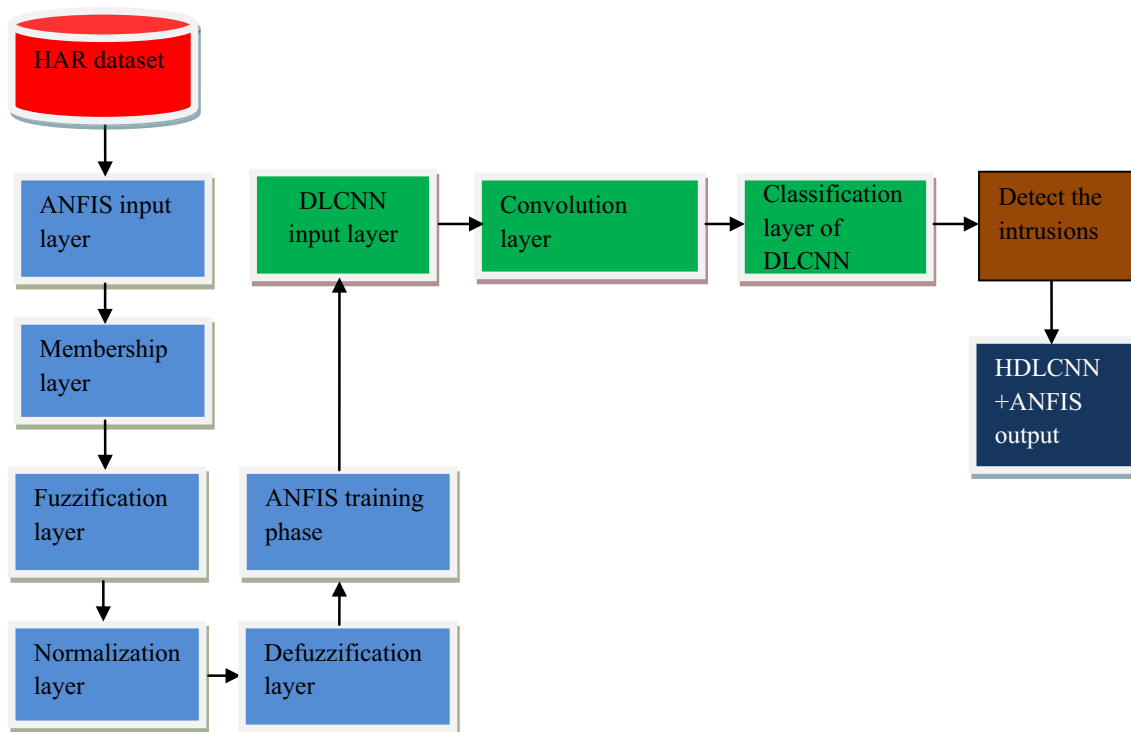


Fig. 5 HDLCNN + ANFIS framework

combined two different portions Generator and discriminator model must be trained in parallel, which requires more training time. But still the proposed model provides provide guarantee for higher detection accuracy.

**4.1 Accuracy**

Accuracy is measured in terms of complete accuracy of the model which is computed as total actual classification parameters ( $T_p + T_n$ ) that is segregated by entire classification parameters ( $T_p + T_n + F_p + F_n$ ). calculated as follows:

$$Accuracy = \frac{T_p + T_n}{(T_p + T_n + F_p + F_n)} \tag{26}$$

here  $T_p$ - true positive,  $T_n$ -true negative,  $F_p$ -false positive,  $F_n$ -false negative.

In terms of accuracy, the comparison metric is evaluated using both present and suggested techniques, as depicted in Fig. 6. The techniques are indicated on the x-axis, where the accuracy can be indicated on the y-axis. For IDS database, conventional approaches attain lower accuracy values 76%, 86% and 91% for centralized GAN, D-GAN with ANN, and D-GAN with EWO-HDLCNN + ANN methods respectively, however the suggested DD-GAN with IFFO-HDLCNN + ANFIS method provides higher

accuracy value of 94%. As a consequence, the suggested DD-GAN with IFFO-HDLCNN + ANFIS improves the final detection rate for various attacks, while GAN improves the training process stability of IDS. The proposed methods are relatively resistant to noise in training data, allowing for higher accuracy while eliminating the local optima issue. Moreover, in comparison to other algorithms, DD-GAN with IFFO-HDLCNN + ANFIS has a faster convergence capability while eliminating premature convergence, which increases recognition rate.

**4.2 Precision**

Precision can be formulated as:

$$Precision = \frac{True\ positive}{True\ positive + False\ positive} \tag{27}$$

Precision is defined as a measure for completeness or quantity, whilst precision is defined as calculation for accuracy or quality. In general, increased precision is that a method produced far more relevant findings than irrelevant ones. Total true positives divided by total components classified in to the positive class is the precision for a class in a classification problem.

With respect to precision, the comparison measure is estimated applying the present and suggested approaches,

Fig. 6 Accuracy

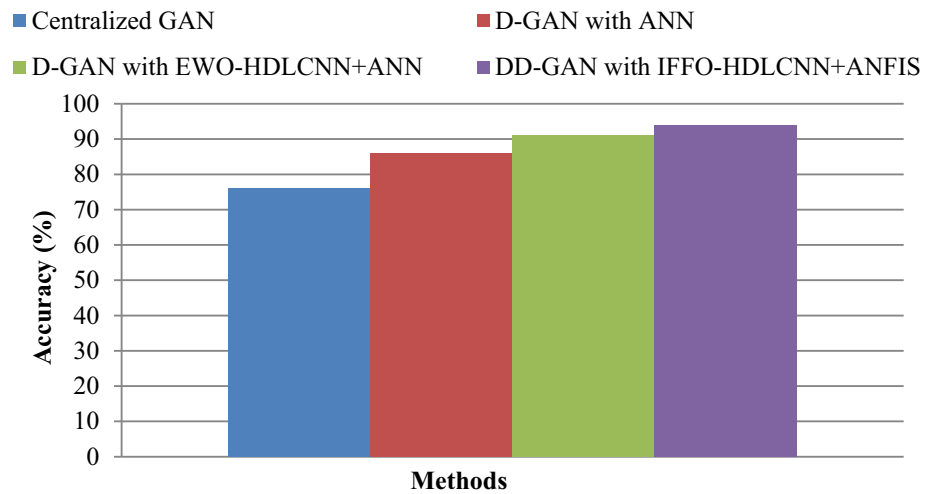
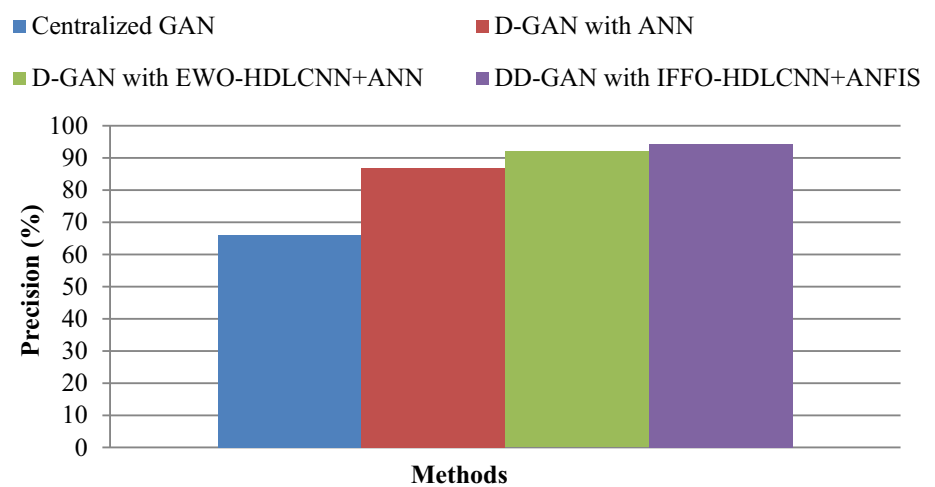


Fig. 7 Precision



as depicted in the above Fig. 7. The techniques were indicated on the x-axis, also the precision value is shown on the y-axis. For IDS database, conventional approaches attain lower precision values 66%, 87% and 92% for centralized GAN, D-GAN with ANN, and D-GAN with EWO-HDLCNN + ANN methods respectively, however the suggested DD-GAN with IFFO-HDLCNN + ANFIS method provides higher precision value of 94.45%. As a result of the suggested DD-GAN with IFFO-HDLCNN + ANFIS system’s optimal feature selection, the intrusion detection precision is increased.

**4.3 Recall**

$$\text{Recall} = \frac{\text{True positive}}{\text{True positive} + \text{False negative}} \tag{28}$$

The comparison graph is given below:  
 Total relevant documents retrieved by a search divided by total obtainable relevant documents is known as recall,

whereas total significant documents retrieved by a search divided by the entire documents retrieved by the search is known as precision.

With respect to recall, the comparison measure is estimated using the existing present and suggested techniques, as indicated in the Fig. 8. The techniques are indicated on the x-axis, while the recall is displayed on the y-axis. For IDS database, conventional approaches attain lower accuracy values 76%, 86% and 91% for centralized GAN, D-GAN with ANN, and D-GAN with EWO-HDLCNN + ANN methods respectively, however the suggested DD-GAN with IFFO-HDLCNN + ANFIS method provides higher accuracy value of 93.6%. As a result, the IDS training process is substantially more stable. Since the GAN-generated samples substituted in the gaps as in data distribution, IDS can easily learn the dispersion of training data to settle down. As a result, by balancing an imbalanced dataset, G-IDS improve performance. The justification for this is that the DD-GAN with IFFO-HDLCNN + ANFIS is typically significantly faster to

Fig. 8 Recall

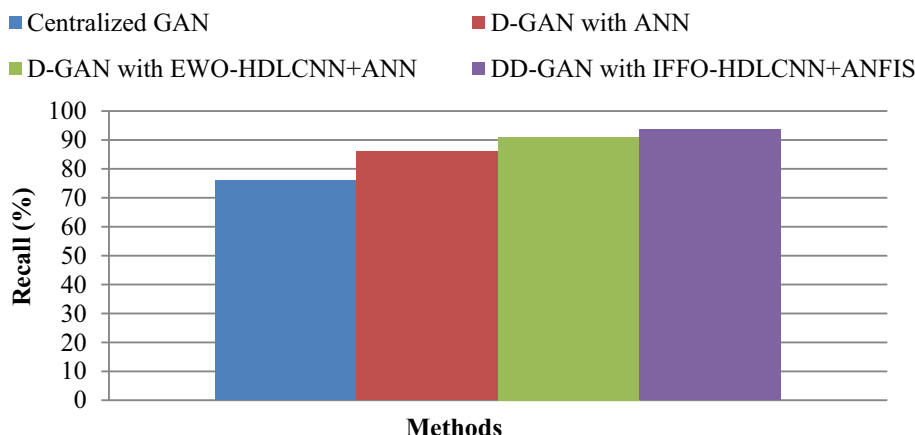
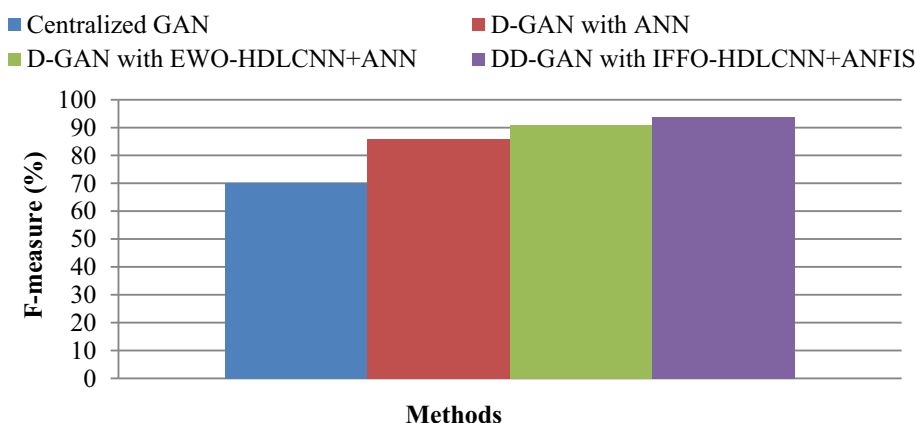


Fig. 9 F-measure



train than the existing methods, and it also has effective preprocessing stages, which increases the recall value.

4.4 F-measure

F-measure can be determined with the mixture of recall R and precision P,

$$F = 2 \cdot \frac{PR}{P + R} \tag{29}$$

The F-measure is used to evaluate classification algorithms which can be applied as regular measure for combining precision P and recall R.

With respect to F-measure, the comparison measure is assessed through the present and suggested techniques, as indicated in the Fig. 9. The techniques are indicated on the x-axis, along with F-measure value is shown on the y-axis. For IDS database, conventional approaches attain lower accuracy values 76%, 86% and 91% for centralized GAN, D-GAN with ANN, and D-GAN with EWO-HDLCNN + ANN methods respectively, however the suggested DD-GAN with IFFO-HDLCNN + ANFIS method provides higher f-measure value of 93.6%. Therefore, the suggested

DD-GAN with IFFO-HDLCNN + ANFIS method enhances intrusion detection performance by the optimal choice of features, according to the results.

4.5 FPR

FPR (False Positive Rate) of IDS is computed as

$$\frac{FP}{FP + TN} \tag{30}$$

FPR of IDS is ratio of total normal state data points incorrectly classified as incursion (FP) to total actual normal state data points (FP + TN).

With respect to FPR, it can be shown in Fig. 10 that comparison measure is analyzed with respect to the present and proposed methods. The methods are represented on x-axis, the FPR value displayed on y-axis. For the provided IDS dataset, conventional approaches like centralized GAN, D-GAN with ANN, and D-GAN with EWO-HDLCNN + ANN provide higher FPR, however the suggested DD-GAN with IFFO-HDLCNN + ANFIS method delivers lower FPR. For IDS database, conventional approaches attain lower FPR values 4.67%, 2.73% and



Fig. 10 FPR

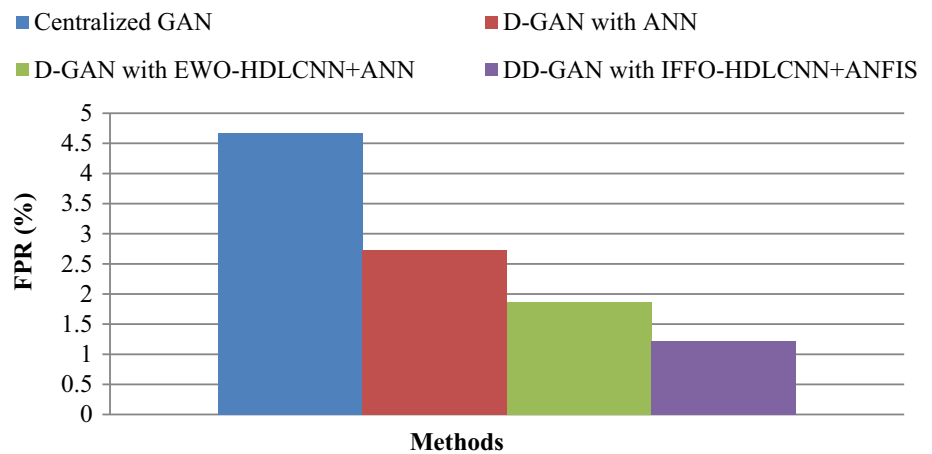


Table 1 Comparison Results for IDS Dataset

Methods/Metrics	Centralized GAN	D-GAN with ANN	D-GAN with EWO-HDLCNN + ANN	Proposed DD-GAN with IFFO-HDLCNN + ANFIS
Accuracy (%)	76	86	91	94
Weighted Precision (%)	66	87	92	94.45
Weighted Recall (%)	76	86	91	93.6
Weighted F-score (%)	70	86	91	93.84
FPR (%)	4.670	2.730	1.870	1.22

1.87% for centralized GAN, D-GAN with ANN, and D-GAN with EWO-HDLCNN + ANN methods respectively, however the suggested DD-GAN with IFFO-HDLCNN + ANFIS method provides lower accuracy value of 1.22%. Therefore, the suggested method enhances intrusion recognition performance by the optimal assortment of features, according to the results. Table 1 compares the results of existing and suggested approaches for the IDS dataset.

## 5 Conclusion

In the proposed model for more effective intrusion detection, the Dynamic Distributed—Generative Adversarial Network (DD-GAN) with Improved Firefly Optimization—Hybrid Deep Learning based CNN with Adaptive Neuro-Fuzzy Inference System (IFFO-HDLCNN + ANFIS) is constructed. It has been proven that employing IDS as an important agent in the deep learning field, and also demonstrated that DD-GAN is a fashionable tool in this field. Hence in this paper, a dynamic distributed DD-GAN model is built to identify both internal and external threats in the distributed IoT networks which contain huge heterogeneous data from devices. In order to handle the

imbalanced dataset more effectively, the data pre-processing is performed through SMOTE method. And then the MPCA algorithm along with IFFO is employed for vital crucial features selection. The solution indicates that dynamic distributed model offer better performance by means on superior accuracy, precision, recall, f-measure and lower false positive rate, computational complexity comparing with the existing algorithms in detecting malicious attacks in IoT networks. In future work, we consider for constructing an exciting, dexterous, and lightweight distributed method to execute it in the end devices of Internet of Things Networks.

**Funding** The authors did not receive support from any organization for the submitted work.

**Data availability** The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

## Declarations

**Conflict of interests** The authors have no relevant financial or non-financial interests to disclose.

## References

- Gendreau, A. A., & Moorman, M. (2016, August). Survey of intrusion detection systems towards an end to end secure internet of things. In: *2016 IEEE 4th International conference on future internet of things and cloud (FiCloud)* pp. 84–90. IEEE.
- Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless personal communications*, 58(1), 49–69.
- IoT Bots Cause Massive Internet Outage. <https://www.beyondtrust.com/blog/iot-bots-cause-october-21st-2016-massive-internet-outage/>. Accessed 22 Oct 2016.
- Hodo, Elike, et al. 2016 Threat analysis of IoT networks using artificial neural network intrusion detection system. In: *2016 International symposium on networks, computers and communications (ISNCC)*. IEEE
- Li, W., et al. (2019). Designing collaborative blockchained signature-based intrusion detection in IoT environments. *Future Generation Computer Systems*, 96, 481–489.
- Ge, Mengmeng, et al. 2019 Deep learning-based intrusion detection for IoT networks. In: *2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC)*. IEEE
- Ding, Yalei, and Yuqing Zhai. 2018 Intrusion detection system for NSL-KDD dataset using convolutional neural networks. In: *Proceedings of the 2018 2nd International conference on computer science and artificial intelligence*.
- Ferdowsi, A., & Saad, W. (2018). Deep learning for signal authentication and security in massive internet-of-things systems. *IEEE Transactions on Communications*, 67(2), 1371–1387.
- Miyato, Takeru, Toshiaki Kataoka, Masanori Koyama, and Yuichi Yoshida. (2018) Spectral normalization for generative adversarial networks. *arXiv preprint arXiv:1802.05957*.
- Verma, A., & Ranga, V. (2020). Machine learning based intrusion detection systems for IoT applications. *Wireless Personal Communications*, 111(4), 2287–2310.
- Yilmaz, Ibrahim, Rahat Masum, and Ambareen Siraj. 2020 Addressing imbalanced data problem with generative adversarial network for intrusion detection. In: *2020 IEEE 21st International conference on information reuse and integration for data science (IRI)*. IEEE
- Ambusaidi, Mohammed A., et al. 2014 A novel feature selection approach for intrusion detection data classification. In: *2014 IEEE 13th International conference on trust, security and privacy in computing and communications*. IEEE
- Shu, Dule, et al. 2020 Generative adversarial attacks against intrusion detection systems using active learning. In: *Proceedings of the 2nd ACM workshop on wireless security and machine learning*
- Liu, Caiming, et al. 2011 Research on immunity-based intrusion detection technology for the Internet of Things. In: *2011 Seventh International conference on natural computation*. Vol. 1. IEEE
- Thanigaivelan, Nanda Kumar, et al. “Distributed internal anomaly detection system for Internet-of-Things.” *2016 13th IEEE annual consumer communications & networking conference (CCNC)*. IEEE, 2016.
- Schlegl, Thomas, et al. Unsupervised anomaly detection with generative adversarial networks to guide marker discovery. In: *International conference on information processing in medical imaging*. Springer, Cham, 2017.
- Vasan, K. K., & Surendiran, B. (2016). Dimensionality reduction using principal component analysis for network intrusion detection. *Perspectives in Science*, 8, 510–512.
- Intrator, Yotam, Gilad Katz, and Asaf Shabtai. Mdgan (2018) Boosting anomaly detection using multi-discriminator generative adversarial networks. *arXiv preprint arXiv:1810.05221*
- Seo, Jae-Hyun, and Yong-Hyuk Kim. (2018) Machine-learning approach to optimize smote ratio in class imbalance dataset for intrusion detection. *Computational intelligence and neuroscience* 2018.
- Najeeb, R. F., & Dhannoon, B. N. (2018). A feature selection approach using binary firefly algorithm for network intrusion detection system. *ARPJ Journal of Engineering and Applied Sciences*, 13(6), 2347–2352.
- Rahman, Saoreen, et al. 2016 PHY/MAC layer attack detection system using neuro-fuzzy algorithm for IoT network. In: *2016 International conference on electrical, electronics, and optimization techniques (ICEEOT)*. IEEE
- Yao, H., Wang, Q., Wang, L., Zhang, P., Li, M., & Liu, Y. (2019). An Intrusion Detection framework Based on Hybrid Multi-Level Data Mining. *International Journal of Parallel Programming*, 47(4), 740–758.
- P. Toupas, D. Chamou, K. M. Giannoutakis, A. Drosou and D. Tzovaras, 2019 An Intrusion Detection System for Multi-class Classification Based on Deep Neural Networks, In: *2019 18th IEEE International conference on machine learning and applications (ICMLA)* pp. 1253–1258, doi: <https://doi.org/10.1109/ICMLA.2019.00206>.
- Tian Dong, Song Li, Han Qiu, Jialiang Lu., 2022, An Interpretable Federated learning based network intrusion Detection framework, cryptography and network security.
- Xiong, Wei, et al. 2018 Learning to generate time-lapse videos using multi-stage dynamic generative adversarial networks. In: *Proceedings of the IEEE conference on computer vision and pattern recognition*.
- Yin, Chuanlong, et al. 2018 An enhancing framework for botnet detection using generative adversarial networks. In: *2018 International conference on artificial intelligence and big data (ICAIBD)*. IEEE
- Upasani, N., & Om, H. (2019). A modified neuro-fuzzy classifier and its parallel implementation on modern GPUs for real time intrusion detection. *Applied Soft Computing*, 82, 105595.
- Zhang, H., et al. (2020). An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset. *Computer Networks*, 177, 107315.
- Taguchi, Y. H., and Yoshiki Murakami. “Principal component analysis based feature extraction approach to identify circulating microRNA biomarkers.” *PLoS one* 8.6 (2013): e66714.
- Pal, A. (2018). Principal Component Analysis of TF-IDF In Click Through Rate Prediction. *International Journal of New Technology and Research IJNTR*, ISSN: 2454-4116, 4(12), 24–26.
- Yang, X.-S. (2010). *Firefly algorithm, Levy flights and global optimization* (pp. 209–218). Research and development in intelligent systems XXVI. Springer.
- Kaur, A., Pal, S. K., & Singh, A. P. (2018). Hybridization of K-Means and Firefly Algorithm for intrusion detection system. *International Journal of System Assurance Engineering and Management*, 9.4, 901–910.
- Zhang, L., Shan, L., & Wang, J. (2017). Optimal feature selection using distance-based discrete firefly algorithm with mutual information criterion. *Neural Computing and Applications*, 28(9), 2795–2808.
- Cheung, N. J., Ding, X. M., & Shen, H. B. (2014). Adaptive firefly algorithm: Parameter analysis and its application. *PLoS ONE*, 9(11), e112634.
- Turabieh, H., Mafarja, M., & Mirjalili, S. (2019). Dynamic adaptive network-based fuzzy inference system (D-ANFIS) for the imputation of missing data for Internet of medical Things applications. *IEEE Internet of Things Journal*, 6(6), 9316–9325.
- Shahriar, Md Hasan, et al. 2020 G-ids: Generative adversarial networks assisted intrusion detection system. In: *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE

37. Aslam, P. M., & Abulaish, M. (2019). Multi-label classification of microblogging texts using convolution neural network. *IEEE Access*, 7, 68678–68691.
38. Reyes-Ortiz, J.-L., et al. (2016). Transition-aware human activity recognition using smartphones. *Neurocomputing*, 171, 754–767.
39. Ferdowsi, A., & Saad, W. (2019). Generative adversarial networks for distributed intrusion detection in the internet of things. In: *2019 IEEE Global Communications Conference (GLOBECOM)* pp. 1–6. IEEE.
40. Xie, G., Yang, L. T., Yang, Y., Luo, H., Li, R., & Alazab, M. (2021). Threat analysis for automotive CAN networks: A GAN model-based intrusion detection technique. *IEEE Transactions on Intelligent Transportation Systems*, 22(7), 4467–4477.

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.



**S. Balaji** Received his B.Tech Information Technology from Madras University in 2002. Master of Engineering 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 in Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, India. He has more than 19 years of teaching experience and Research experience.

His research interests include Wireless Sensor Networks, Cyber

Physical Systems, Network Security, Internet of Things (IoT) and Machine Learning. He has published many research articles in reputed international journals.



**S. Sankara Narayanan** received the B.E Degree in Computer Science and Engineering from Madurai Kamaraj University, in 2001, M.E degree in Computer Science and Engineering from Anna University, Chennai in 2007 and Ph.D. in Computer Science and Engineering from Kalasalingam Academy of Research and Education in 2019. He has more than 20 publications in international journal and international conference proceedings. He has

published 2 Indian patents. He has 17 years of teaching experience. His areas of interest include Mobile Ad hoc Networks, Network Security, image processing and IOT. He is currently working as an Associate Professor in the Department of Computer Science and Engineering at Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Tamil Nadu, India. He is life member of ISTE and IET.