FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 4 | Pages 948-953 | e-ISSN: 2347-470X

Hybrid Deep-Generative Adversarial Network Based Intrusion Detection Model for Internet of Things Using Binary Particle Swarm Optimization

Balaji S[1], Dr. S. Sankaranarayanan[2]

[1]*Research Scholar, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, India,balajinithin19@gmail.com*
[2]*Associate Professor, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, India, sankarme2007@gmail.com*

***Correspondence:** Balaji S; balajinithin19@gmail.com

░ **ABSTRACT-** The applications of internet of things networks extensively increasing which provide ease of data communication among interconnected smart devices. IoT connected with smart devices diverse in a range of fields associated with smart cities, smart-transportation, smart- industrial, healthcare, hospitality etc. The smart devices lack with computational power, energy and inconsistent topology. Due to these factors these are most vulnerable to security attacks which affect the transmission reliability of data between nodes. An IoT network connects heterogeneous devices together and generates high volume of data. To provide security against intrusion attacks, deep neural network (DNN) techniques are adopted to detect malicious attacks. We have proposed on an anomaly Hybrid based deep learning-based approach which is Generative Adversarial Network in accordance with detecting malicious intruders. We designed a distributed IDS controller validated over dataset of NSL-KDD and proven with higher performance in detecting the DDOS Distributed- Denial- of service- attacks. Thus, Experimental Results are calculated with predefined threshold values to detect DDoS-attacks and the resultant proves that HD-GAN model offers better intrusion detection with respect to higher accuracy, recall, precision, f-measure, and lower FPR (False-Positive-Rate).

General Terms: Intrusion detection, Security, Machine Learning, Smart devices.
Keywords: Distributed Deep Neural Network, Distributed Denial of Service (DDoS), Generative Adversarial Network (GAN).

ARTICLE INFORMATION
Author(s): Balaji S, Dr. S. Sankaranarayanan;
Received: 07/07/2022; **Accepted:** 05/10/2022; **Published:** 10/11/2022;
E- ISSN: 2347-470X;
Paper Id: IJEER220714;
Citation: 10.37391/IJEER.100432
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100432.html

Publisher's Note: FOREX Publication stays neutral with regard to jurisdictional claims in Published maps and institutional affiliations.

░ 1. INTRODUCTION

The IoT- Internet of Things which is either network or grouping smart computing entities which enables to communicate with each and outside world for creating the better living standard. IoT devices connected together and limited in computing power, processing, storage resources, protocol capabilities and size. It is a challenging task to protect the heterogeneous networks against intrusion attacks. The Distributed-Denial- of Service (DDoS) attack considered to be serious threat. The IDS is the major contribution for providing defense and for identifying threats along with spotting and keep in track of intruders. Hence, we proposed an intrusion detection methodology based on deep learning approach to DDoS attacks in heterogeneous network environment. The neural network uses vital features as input and final findings were confirmed in comparison. They demonstrated 99% class accuracy, 90% sensitivity and 100% clarity. This was done on training and testing on given dataset. The generated data from the IOT environment is collected and it is examined by Deep Learning algorithms to find out the presence of attacks.

The remainder of this paper is structured as follows. *Section 2* discusses the study of related work in intrusion detection. The *Section 3* introduces significant background examination about different deep learning techniques and *Section 4* elaborates proposed HDGAN Model. *Section 5* describes the experimental results and performance analysis. Finally, *Section 6* presents some conclusions and future work.

░ 2. RELATED WORK

Internet of Things has a massive probable towards all kinds of applications that ranges from healthcare to military and the security challenges are the major issues due to its restricted computational proficiency [1]. Saikiran, et al., elaborated a novel intrusion detection methodology on machine learning basis to spot sniffing and poisoning intrudes in IoT networks. They constructed an adversarial scheme with the use of laptop system to detect the malicious data is identified and marked as attacked data. They employed machine learning such as SVM, decision tree, Naïve Bayes classifiers for sorting out data between regular and attacked class. Although they achieved higher accuracy, the supervised model requires large no of samples labels and more time for learning and training [2].Athira Remesh, et al., introduced an efficient intrusion detecting scheme for IoT network intended to spot DoS, DDoS-attacks by applying Wi-Fi Detector scheme, the DDoS-attack is carried out through SYN flooding over ESP8266 and botnet scheme using the malware called Mirai. This model lacks in scalability and not suited for real time environments [3]. Y.-W. Chen, J. -P. Sheu, et al, designed a machine learning based multilayer DDoS attack detection scheme to spot most vulnerable attacks. It supports multilayer classification, but still algorithm requires much training data and produces inconsistent results in large networks [4].

Mayur Rahul et al proposed a hybrid deep learning approach which combines RNN and CNN to retrieve relevant features dataset from EMOTIC for efficiently recognize emotion. The experimental result shows that the proposed method achieves 94% accuracy in emotion recognition. Even though this hybrid method achieves higher accuracy, it has undesirable time complexities [5].Tanzila saba, et al., elaborated CNN methodology for spotting intrudes attacks present over IoT networks detecting real time attacks which utilizes the IoT's power, for monitoring entire network, shows the detection accuracy with 92.85%. But still they do not address the issues related hidden nodes and learning rate [6].

Stefanos Tsemindis, et al, designed a deep learning data driven approach which posses an ability to spot unfamiliar attack using approaches on the basis of anomaly over IoT with accuracy rate of 97.4%. The experimental result exhibits that the model results less than 2% errors in detection [7]. Ziadoon K. Maseer, et al, presented a novel hybrid weighted deep belief network (HW-DBN) algorithm building an efficient and reliable IDS (DeepIoT.IDS) intrusion detection system classifier with accuracy rate 95% [8].A Modified Density Peak Clustering Algorithm (MDPCA) and Deep Belief Networks (DBNs) for fuzzy aggregation model is employed. Al though it produces a higher accuracy and high detection rate the training set looks complex and need to be divided [9].The hybrid convolutional neural network with Intrusion detection system is introduced to detect the various types of attack which are established on IoT networks [10]. The Intrusion Detection System with Routing Protocol identifies the wormhole attacks which are very severe in routing nodes and detecting using Contiki OS and Cooja Simulator and the success rate for identifying reaches 90% accuracy [11]. The Sybil attack senses the domain in IoT and acts a legitimate node. The Sybil node distributes multiple identities of devices which act as the authorized device based on the observation of the environment [12].Anil Kumar Yaramala, et al, investigates an application of AI in IoT based unmanned aerial vehicle network for integrating drone network intelligently with the capability of the drone for automatic take-off, habitual landing and monitors the movement from the IoT devices for detecting malicious behavior[13].A novel Intrusion Detection Algorithm based on neighbor information against sink hole attack (IDASA) is proposed to detect the sinkhole attack using sensor nodes in Wireless sensor Networks. The method has several merits with respect to dynamic self-adaptation, low false alarm rate, reduced communication overhead with the major limitation that it could not able to detect all anomalies [14].The sink hole attacks are more vulnerable and they consumes the resources such as memory and processing leading to slaying of resources. The behavior of router nodes is monitored and dynamic clustering is accepted by the INTI in the forwarding task. In addition, the attacker is competent to damage all nodes of the network by knowing the network topology. The restriction of the method is it only deliberates on extenuating impacts of definite intrusions [15]. The Distress Propagation Object is incorporated with Low – Power and Lossy Networks (RPL) for routing protocol is allotted to detect the anomaly to the nearest neighbors or parents and to the edge router. The edge router conducts timely checks, the information is correlated and decision is taken to give an alarm to users conversely, the model does not appropriate for real-time IDS and it has timing overhead, also it requires severe implementation overheads. [16]. Ulya Sabeel et al proposed an efficient defensive AI engine joint with a twofold feature selection technique and the defensive AI engine significantly increases the True Positive Rate (TPR) on multiple a typical attacks for intrusion [17].The [18] proposed a feature reduction technique using information gain and correlation tested over NSL-KDD dataset for computing an optimal subset of features Information Gain to identify relevant features and eliminates redundant features.

3. DEEP LEARNING TECHNIQUES

In general an IoT device network is designed to perform specific exact functions. We focus on applying deep learning techniques to develop various network monitoring tools for detecting intrusion in the IoT network intrusion detection (NIDS) using GAN (Generative Adversarial Network) for intrusion classification. The GAN network learns the legal networking behavior profile and detects any variation from it.
DL methods can be applied on datasets with high volumes and real time data in complex vector space as input to a neural network to discover the mainly valuable features from the low-level features and achieves reasonable inference and sequence classification to find illegal devices in IoT and employed on complex computational structure that integrate with multiple processing layers to gain knowledge of diverse data representations.

The above-mentioned deep learning techniques have achieved reasonable results with higher accuracy. But still it is very hard in achieving zero attack competence and also not precise in detecting the unknown attacks and also it has been observed that, IDSs in the IoT environment still needs enrichment with respect to detection accuracy, to increase true positive rate, and to reduce the energy consumption. Hence, we have proposed to design a Hybrid distributed Generative Adversarial Network which is proficient in detecting the both internal and external attacks in distributed IoT networks.

Table 1. Comparison of Various IDS Methods Performance

Ref	Algorithm	Year	Accuracy	Demerits
[2]	SVM	2020	94.6%	Not suited for multiple classification
[3]	Bot-Net	2020	90%	Not suited for real time environments

[4]	DL Method	2020	95 %	Inconsistent Results
[5]	Hybrid RNN & CNN	2022	94 %	Undesirable time complexities
[6]	CNN	2022	92.85 %	Learning rate is time consuming
[7]	Deep Learning	2022	97.4 %	Not suitable for large networks
[8]	HW-DBN	2021	95%	Complex Training
[17]	Defensive AI Engine	2021	96.7%	Not suitable for unknown attacks
	HD-GAN	2022	99%	**Merits**: Detecting unknown attacks in distributed IoT Real time environments.

Experimentation carried over network traffic data formed from smart FANET network demonstrates such that our proposed methodology resultant with great performances as shown the FANET architecture IoT network in *figure 1*.

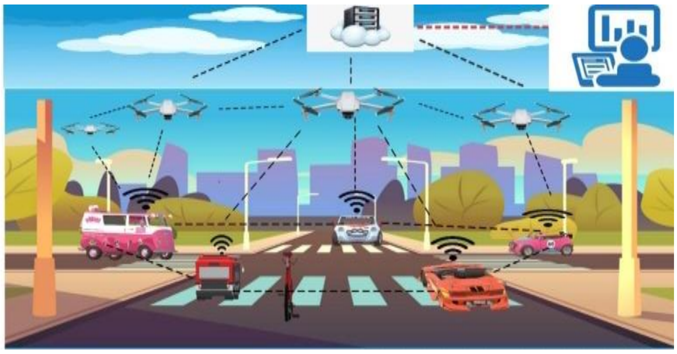

Figure 1. Architecture of FANET IoT Network

The FANET networks devices will have to interact with the base station at ground level and also, they shift from point to another, according to the application domain. UAV (unmanned vehicles) IDS operates on either batch or stream, as per the applied technology. Deep learning-based intrusion detection ensures the secure exchange of data and its communication from drones to base station and as well between the drones themselves [19].

4. HYBRID DEEP LEARNING-BASED INTRUSION DETECTION SYSTEM (HD-GAN) USING GENERATIVE ADVERSARIAL NETWORK

GAN is an innovative framework to design and assess generative model with use of adversarial process, through that we trained two models simultaneously such that the generative model 'G' will collect the data distribution while the discriminative model 'D' will estimate the probability that more samples are collected through trained data to G [20]. GAN schemes are widely used to creating non-real images which appears to be similar with real ones. The main approach is Generative Adversarial Network (GANs) that consecutively trains these two models namely generative as well discriminative models and it is listed in Figure 2.The generator model generates data samples and discriminator methodology determines originality of the sample data given through binary classification that represents the sigmoid functions which predicts whether the data is real or fake. This also helps in finding out the attacks in the environment.

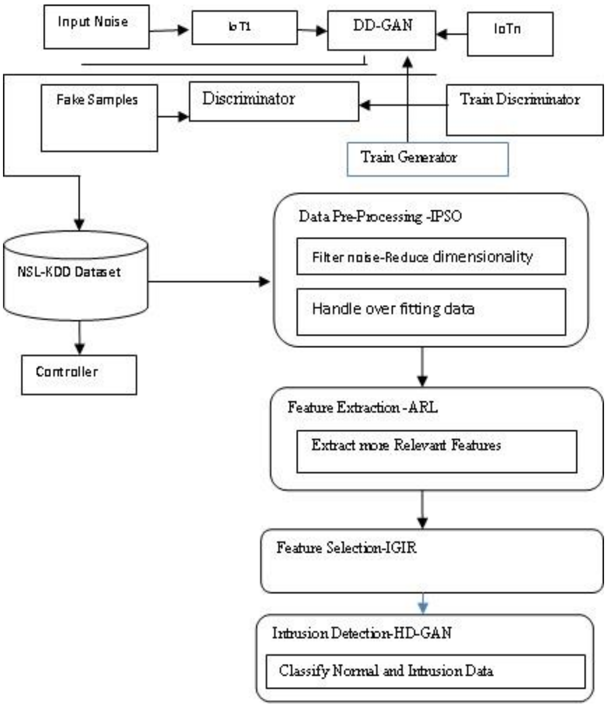

Figure 2. The Hybrid Distributed GAN Intrusion Detection System

4.1 Pre-Processing by Improved binary Particle Swarm optimization Technique

The pre-processing is considered necessary for better outcome of intrusion detection. In this paper, pre-processing is done by using improved binary particle swarm (B-PSO) optimization for improving the imbalanced dataset efficiently. A swarm is a collection of cooperating agents to achieve intended behavior and mission Partial swarm optimization depends on the position of particles in D-dimensional space. The particles altered based on three conditions lies on its inactivity, idealist position and Swarm's optimist position. An enhanced strategy for particles' position value in PSO is described as follows.

Step 1: Determine the number of path nodes, based on real environment and calculates the values for the swarm size (m), the maximum generation (Magen), the maximum fitness value (maxFit),
Step 2: Initialize the parameters of the particle evenly and set values for the particle position along with the particle population and velocity.
Step 3: For each iterations, generate of random number R (value from 0 to 1) for each dimension.
Step 4: compute the fitness value of the particle and update the velocity and position of the particle.
Step 5: In every generation, the particle's position value in each dimension will be held in reserve and also updated by its local

optimal value Pbest otherwise by global optima Gbest value and changed with new random value.
Step 6: Repeat the above process until to get the optimal path or the termination condition is met.

In this a feature weighting directed initialization is adapted to improve the quality of the initial swarm where the bits (features) with higher weights are given higher probabilities to be initialized as 1 and then the dynamic bit masking technique iteratively places a mask on the features each definite number of generations to significantly narrow the search space throughout the evolutionary process, which is favorable for IPSO to find enhanced solutions in a smaller exploration [21]. Through this preprocessing process gradually reduces the search space which will lead to a feasible solution and handling imbalanced data issues well.

4.2 Feature Construction using Associative Rule Learning (ARL)

For the purpose of feature construction associative rule learning method is employed, which are needed to describe the data precisely. The association rule learning can define as given below Consider that I= $\{i_1, i_2, i_3 \ldots i_n\}$ be a set of n features selected from the inspected data. Also, D = $\{r_1, r_2 \ldots r_m\}$ be a set of records in obtained data set. Each record r_i contains a subset of features in *I*. The rule is defined as per the implication: $X \Rightarrow Y$, where, and X, $Y \subseteq I$, $X \cap Y=0$.There are certain challenges and limitations in the proposed binary particle swarm optimization (BPSO), the determined acceleration coefficients values of each particle stay on the same in iteration. But some enhancement might be implemented on the least fit particles to move rapid and best fit consequently, in order to accelerate the convergence speed and to decrease the computing time [22].

4.3 Feature Selection using Information Gain and information Ratio Technique

In this paper, we proposed a feature selection based on Information Gain (IG) and Gain Ratio (GR) with the ranked top 50% features to select relevant features in the large redundant attribute values which are efficient in detecting DDoS attacks in Internet of Things [23].The model selects IG and GR filter-based feature selection technique which selects the best top 50% ranked features among the total number of features present in the dataset [23].The system selects IG and GR and obtains IG-TFP-FS which consist of Top ranked 18 features and GR-TFP-FS subsets consists of 18 features by selecting the top 50% features in the 36 available features in the dataset . The subset RFS-1 that consists of 16 features majorly used for DDoS attack detection.

4.4 Intrusion detection using Hybrid Deep Learning based GAN network

In this proposed work, HD-GAN is introduced for more accurate intrusion detection for the given dataset. The proposed deep learning based intrusion method achieves higher accuracy. The Fig 3 shows the function of Deep-GAN algorithm. The GAN applies the idea of adversarial learning to train the model to deal with the density of high-dimensional data from the IoT network. The purpose of the generator is to deceive IDS, and the target of the discriminator is to imitate the IDS on classifying inputs whether it is correct or wrong and provide response to the generator.

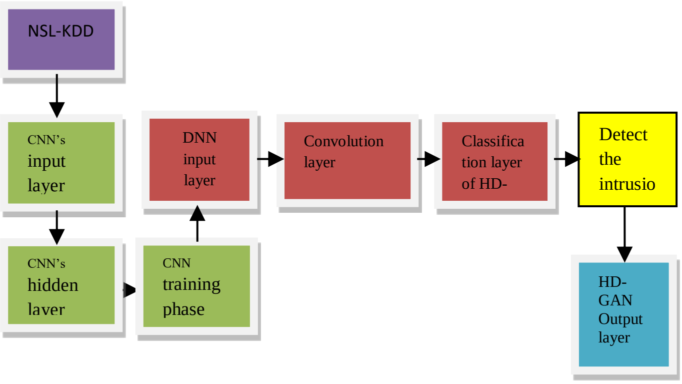

Figure 3. Function of HD-GAN model

ANN is utilized for collecting information by discovering. CNN has three various layers namely, input layer, hidden and output layer. The first input layer gathers incoming data and is analyzed and produces 'n' inputs. All the process is performed based on weights.

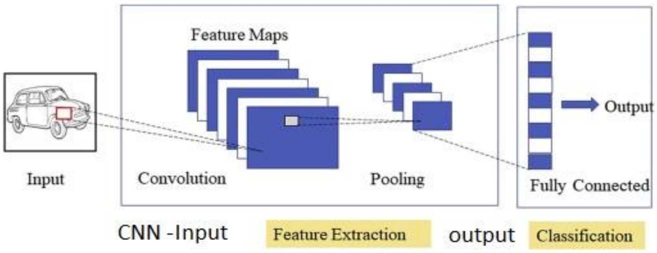

Figure 4. Architecture of CNN

The CNN has long duration for training and testing process. To overcome these problems, deep learning-based CNN is hybrid with D-GAN and combined with ANN for more accurate intrusion detection with less computation time. The basic HDNN contains an input and output layer, in addition to many hidden layers. Input layer accepts intrusion features from training examples and convert the data to combined form to deliver the data to subsequent layers properly. Once if every data passes throughout many convolution layers, output feature maps' size constantly reduces. can be executed as steps1.Process IDS dataset from NSL-KDD 2. For all input feature, describe intrusion feature ∈ IDS dataset does 3. For each neuron, input features do 4. Train the CNN for the given dataset 5. Hybrid Deep-CNN with CNN in D-GAN. 6. Transform input into convolution and classification layers.7. identify intrusion features using abnormal behavior.8. Select more informative and relevant features.9. Perform training and testing procedure for specified database.10. Replicate the predefined intrusion feature label for every feature as specified by the input database.11. Detect additional accurate intrusion results.

4.4.1 Performance Metrics

Accuracy is defined as the percentage of all predictions that are correctly detected either as Attack or Normal.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (3)$$

$$\text{False Positive Rate} = \frac{FP}{FP+TN} \quad (4)$$

5. EXPERIMENT AND RESULTS

We simulated the FANET network communicating with drone devices and monitor the packets transmission in the network. The packets are gathered from the NSL-KDD dataset and they are sent over HDGAN model. In the simulation their about 1, 25,000 packets have been monitored in which 70% packets have been used as trained data and balance to test dataset for avoiding over fitting. Deep-GAN is does have intrinsic metric exist which better model for training and with proven performance in complex outputs. The entire experimentation is implemented in python IDE environment.

5.1 Discussion

The simulation was conducted using Python (PyOpenCL) programming with NSL-KDD dataset with a 2.4 GHz Intel Core i3 processor and windows 10. The hybrid deep learning algorithm for intrusion detection with GAN and DNN is applied on FANET network simulation. The overall model performance is given in the *Table 2* and *Table 3*. The proposed NSL-KDD dataset has the significant importance that it consists of two separate files for training and testing. Test file contains different unknown attacks which not included in the training file which help us to detect unknown attacks. For purpose of training this model 70% dataset is employed which has 85000 records. The GAN is competent in classifying the outcome from trained sample, but still GAN has no intrinsic metric evaluation for better model training and generating complex outputs. Hence even though it has well designed system of data generation it is complex to train GAN and generate output with 99% accuracy.

Table 2. Overall Model Performance of HD-GAN

Attack type	Detection Rate
Denial of Service	99.09
Wormhole	98.2
Sinkhole	97.2
DDoS	99.02
Black hole	94.2

Table 3. Comparison values for IDS NSL-KDD dataset

Methods / Metrics (%)	Centralized GAN	D-GAN with ANN	D-GAN with EWO-HDLCNN+ ANN	DD-GAN with HDCNN	HD-GAN with DNN
Accuracy	76	86	91	94	99
Precision	66	87	92	94.45	98.5
Recall	76	86	91	93.6	98
F-measure	70	86	91	93.84	96.6
FPR	4.670	2.73	1.870	1.22	1.02

The HD-GAN provides higher accurateness of recall, precision, F-measure, also lower-FPR and higher detection rate for diverse attacks in *figure 5*.

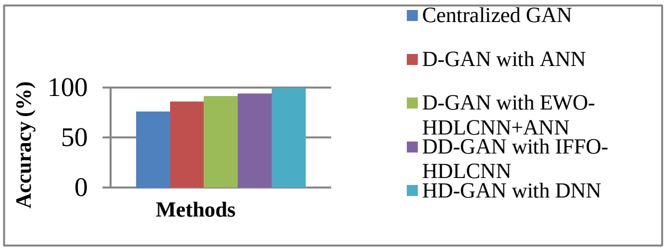

Figure 5 (a). Accuracy

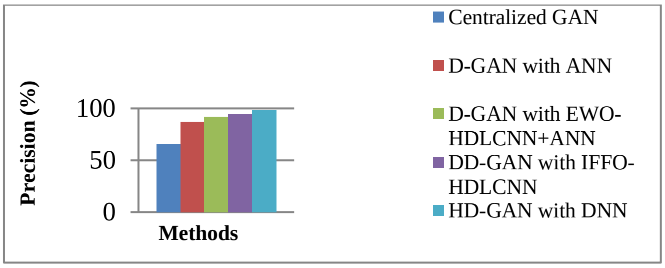

Figure 5 (b). Precision

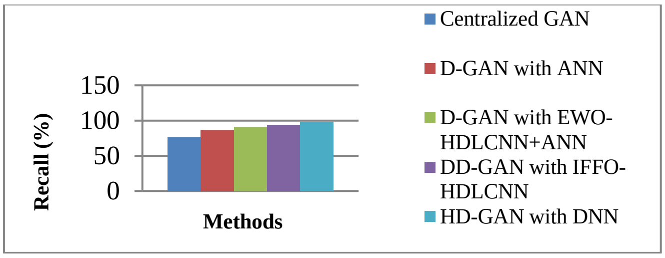

Figure 5 (c). Recall

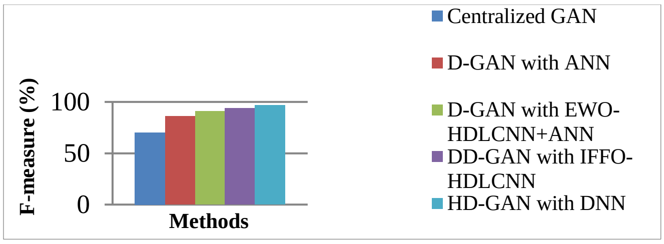

Fig 5 (d). F-Measure

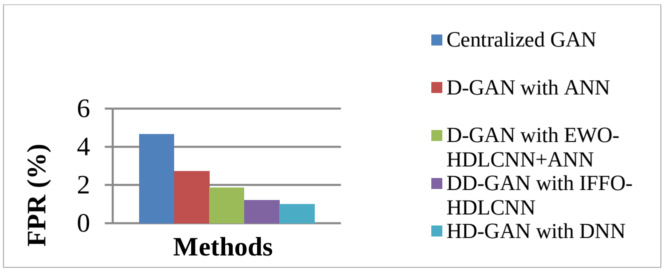

Fig 5 (e). FPR

6. CONCLUSION

The proposed hybrid deep neural network with Generative Adversarial Network (HD-GAN) efficiently detects the intrusions and abnormal behavior in the IoT drone networks.

The DNN model has been trained with feature samples extracted from the smart transport environment further fed into GAN network for intrusion classification. The experimental result shows that HD-GAN can detect intrusion attack with a comprehensively accurate detection ratio of 99% and also lower FPR ratio 1.02%. In future work IDS system can be implemented on real-time mission critical sensitive environment where high security protection is mandatory for detecting intrusion and preventing malicious actions.

CONFLICT OF INTEREST:
The Author(s) declare no conflict of interests.

REFERENCES

[1] Mengmeng Ge, Xiping Fu, Naeem Syed, Zubair Baig, Gideon Teo, Antonio Robles-Kelly, “Deep Learning-based Intrusion Detection for IoT Networks” IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), pp.1-10,2019.

[2] K.V.V.N.L. Sai Kiran, R.N. Kamakshi Devisetty, N. Pavan Kalyan, K. Mukundini, R. Karthi, Building an Intrusion Detection System for IoT Environment using Machine Learning Techniques, Procedia Computer Science, Volume 171,2020, Pages 2372-2379.

[3] A. Remesh, D. Muralidharan, N. Raj, J. Gopika and P. K. Binu, "Intrusion Detection System for IoT Devices," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020, pp. 826-830, doi: 10.1109/ICESC48915.2020.9155999.

[4] Yi-Wen Chen; Jang-Ping Sheu; Yung-Ching Kuo; Nguyen Van Cuong Design and Implementation of IoT DDoS Attacks Detection System based on Machine Learning, European Conference on Networks and Communications (EuCNC),2020

[5] Mayur Rahul, Namita Tiwari “A New Hybrid Approach for Efficient Emotion Recognition using Deep Learning” International Journal of Electrical and Electronics Research (IJEER), vol 10(1),Forex publication, 2022

[6] Tanzila Saba, Amjad Rehman, Tariq Sadad, Hoshang Kolivand, Saeed Ali Bahaj, Anomaly-based intrusion detection system for IoT networks through deep learning model, Computers and Electrical Engineering, Volume 99,2022.

[7] Tsimenidis, S., Lagkas, T. & Rantos, K. Deep Learning in IoT Intrusion Detection. J Netw Syst Manage 30, 8 (2022). https://doi.org/10.1007/s10922-021-09621-9

[8] Z. K. Maseer, R. Yusof, S. A. Mostafa, N. Bahaman, O. Musa et al., "Deepiot.ids: hybrid deep learning for enhancing iot network intrusion detection," Computers, Materials & Continua, vol. 69, no.3, pp. 3945–3966, 2021.

[9] Yanqing Yang , Kangfeng Zheng , Chunhua Wu , Xinxin Niu and Yixian Yang ,“Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks”,2019.

[10] Dr. S. Smys, Dr. Abul Basar, Dr. Haoxiang Wang, “Hybrid Intrusion Detection System for Internet of Things (IoT)”, Journal of ISMAC, Vol.02, No.04 Pp: 190-199, 2020.

[11] Snehal Deshmukh-Bhosale, Santosh S. Sonavane,“A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things “ Procedia Manufacturing- The 12th International Conference Interdisciplinarity in Engineering,Vol. 32,pp. 840–847,2019.

[12] Alekha Kumar Mishra, Asis Kumar Tripathy, Deepak Puthal, and Laurence T. Yang, “Analytical Model for Sybil Attack Phases in Internet of Things, IEEE Internet of Things Journal,Vol.6 ,No.1,pp.379-387,2019.

[13] Dr Anil Kumar Yaramala1 ,Dr Sohail Imran Khan “Application of Internet of Things (IoT) and Artificial Intelligence in Unmanned Aerial Vehicles” International Journal of Electrical and Electronics Research (IJEER), vol 10(2),Forex publication, 2022.

[14] Guangjie Han , Xun Li, Jinfang Jiang , Lei Shu and Jaime Lloret,” Intrusion Detection Algorithm Based on Neighbor Information Against Sinkhole Attack inWireless Sensor Networks”,IEEE The Computer Journal , Volume: 58, No: 6, 2015.

[15] Christian Cervantes, Diego Poplade, Michele Nogueira and Aldri Santos,“Detection of Sinkhole Attacks for Supporting Secure Routing on 6LoWPAN for Internet of Things”, IFIP/IEEE International Symposium on Integrated Network Management (IM2015): Mini-Conference,2015.

[16] Nanda Kumar Thanigaivelan, Ethiopia Nigussie, Rajeev Kumar Kanth, Seppo Virtanen and Jouni Isoaho”Distributed Internal Anomaly Detection System for Internet-of-Things” 13th IEEE Annual Consumer Communications & Networking Conference (CCNC),2016.

[17] Ulya Sabeel, Shahram Shah Heydari (2021) “Building an Intrusion Detection System to Detect Atypical Cyberattack Flows “, IEEEACCESS 2021.

[18] Ghanshyam Prasad Dubey, Dr. Rakesh Kumar Bhujade “Investigating the Impact of Feature Reduction Through Information Gain and Correlation on the Performance of Error Back Propagation Based IDS” International Journal of Electrical and Electronics Research (IJEER), vol 9(3),Forex publication, 2021.

[19] Ramadan RA, Emara A-H, Al-Sarem M, Elhamahmy M. Internet of Drones Intrusion Detection Using Deep Learning. Electronics. 2021; 10(21):2633. https://doi.org/10.3390/electronics10212633

[20] Aidin Ferdowsi and Walid Saad “Generative Adversarial Networks for Distributed Intrusion Detection in the Internet of Things”,IEEE Global Communications conference.

[21] An-Da Li, Bing Xue, Mengjie Zhang,”Improved binary particle swarm optimization for feature selection with new initialization and search space reduction strategies”, Applied Soft Computing, Volume 106,2021,https://doi.org/10.1016/j.asoc.2021.107302.

[22] Sulaiman, A.; Sadiq, M.; Mehmood, Y.; Akram, M.; Ali, G.A. Fitness-Based Acceleration Coefficients Binary Particle Swarm Optimization (FACBPSO) to Solve the Discounted Knapsack Problem. Symmetry 2022, 14, 1208.https://doi.org/10.3390/sym1.

[23] Farah Jemili and Hajer Bouras “Intrusion Detection Based on Big Data Fuzzy Analytics”open data, DOI: 10.5772/intechopen.99636, 2021.

[24] Pushparaj Nimbalkar, Deepak Kshirsagar, Feature selection for intrusion detection system in Internet-of-Things (IoT), ICT Express, Volume 7, Issue 2,2021, Pages 177-181.