A GAN-based Hybrid Deep Learning Approach for Enhancing Intrusion Detection in IoT Networks

Mr. S. Balaji[1], Dr. G. Dhanabalan[2], C. Umarani[3], Dr. J. Naskath[4]
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[1, 2]
Department of Computer Science and Engineering, National Engineering College, Kovilpatti,
Tuticorin District, Tamil Nadu, India[3, 4]

***Abstract*—Internet of Things (IoT) strongly involves intelligent objects sharing information to achieve tasks in the environment with an excellence of living standards. In resource-constrained it is extremely difficult chore to impart security against intrusion. It is unprotected from Distributed Denial of Service (DDoS), Gray hole, sinkhole, wormhole attacks, spoofing, and Sybil attacks. Recent years, deep neural network (DNN) methodologies are widely used to detect malicious attacks. We develop a Hybrid deep learning based GAN Network to detect malicious attacks in IoT networks. Due to composite and time-varying vigorous environment of IOT networks, the model trainig samples are insufficient since intrusion samples combined with normal samples will lead to high false detection rate. We created a dynamic distributed IDS to detect malicious behaviors without centralized controllers. Preprocessing sets threshold values to identify malicious behaviors. Experimental results show HDGAN outperforms existing algorithms with higher accuracy 98%, precision 98% and 95% lower False Positive Rate (FPR).**

Keywords*—Distributed Denial of Service (DDoS); Internet of Things (IoT); Deep Neural Network (DNN); intrusion detection; Generative Adversarial Network (GAN)

I. INTRODUCTION

The Internet of Things (IoT) is a system of interconnected computing objects which are in high demand and the capability to convey data above a network without the presence of humans. IoT provides system connectivity and computing capability with devices and sensors to consume data with nominal individual involvement. The IoT makes its impact in various applications in day to day life such as healthcare, military, environment [22] etc. IoT is controlled in all perspectives such as in processing speed, storage, power and size. In an IoT environment the internet based smart system senses and collects the data through the gateway and then it is sent for investigation. As the demand for IoT service increases there have always been challenges in the security issues.

The security measures are overcome by providing authentication, access controls and confidentiality but still face security problems through attacks and intruders. Distributed Denial Service of Service (DDoS) attacks provide a serious pitfall to the IoT environment which has its types Internet Control Protocol (ICMP), SYN flood, UPD flood and DNS attack. Other types of attacks are the Sybil attack, WormHole attack and the sinkhole attacks. Fig. 1 shows the intrusion detection process using the Deep Learning Techniques. Data generated within the IoT environment undergoes collection and scrutiny by Deep Learning algorithms [23] [24] to detect potential attacks. Alert will be given when there is an attack and the malicious node or the hacker will be blocked. In this paper Hybrid Modified principle Component analysis and Firefly-based optimization approach is specified to find out the invasion attacks. The Generative prototype for Intervention Detection System will detect whether the collected is real or fake. The HDGAN (Hybrid Deep Learning-based Generative Adversarial Network) was developed specifically to detect malicious activities within IoT networks, emphasizing IoT security.

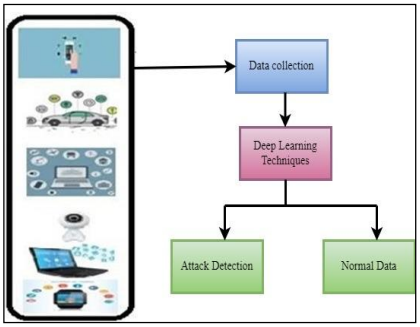

Fig. 1. The deep learning-based attack detection in IoT.

II. RELATED WORK

Intrusions must be detected before a specified time elapses, which can be challenging within typical time constraints. GAN leverages the LSTM-DNN algorithm for effective intrusion prediction before the designated time threshold [1]. Deep learning models with training and evaluation of models done by Feed-forward neural network, auto encoder, deep belief mesh work and extended small label term memory network by selecting and classifying two datasets (KDD 99, NSL-KDD). Machine learning algorithms help to learn the patterns of intrusion in datasets. The supervised deep feed-forward neural networks (ANN) check the standards such as precision, F1score, false negatives, training and inference together it shows better performance [2]. Network intrusion detection is crucial for addressing network imbalances. TMG-GAN is employed to prevent various types of attacks, followed by addressing classification loss, and ultimately focusing on improving sample quality. Through these techniques, effective intrusion prediction is achieved [3]. To mitigate the DDoS attacks an innovative

procedure called Learning-Driven Detection Mitigation (LEDEM) is proposed which make use of semi supervised training to find and prevent DDoS. Two different strategies is followed in LEDEM fixed IoT and Mobile IoT and the phases are Data Capture, DDoS Detection and DDoS Mitigation . The attack detection got improved and throughput got increased based on LEDEM [4]. To enhance system performance and address data imbalance, integrate Artificial Intelligence (AI) with Network Intrusion Detection Systems (NIDS) using datasets such as NSL-KDD and UNSW-NB15 for prediction. Additionally, prioritize the utilization of real-world datasets to further improve model effectiveness. This demonstrates that the proposed model effectively addresses the issue of load imbalance [5]. Extreme Learning Machines proves efficient learning machines for pattern classification. ELMs based on Semi-Supervised ELM (SS-ELM) and Un Supervised ELM (US-ELM) are proposed that demonstrate better computing capability, proceed to multiclass classification and can grasp unknown information during evaluation time span. Based on the results the Unsupervised ELM shows better performance [6].

Anomaly detection is a significant challenge in data security, and Time Series Data Augmentation (TSDA) plays a crucial role in addressing this issue. DCT-GAN (Dilated Convolutional Transformer) integrates coarse and fine-grained time series data to enhance generalization using a weight-based technique [7]. Deep anomaly detection is critical for accurate data labeling and handling low-rate anomalies. To address this, FlowGAN-NIDS combines discriminator and generator components, diverging from traditional encoder-decoder methods. This approach enhances anomaly detection performance, particularly in scenarios with low anomaly occurrence rates, validated through various experiments to confirm prediction accuracy [8]. The violation prediction framework, integrated with Routing Protocol, specifically targets the identification of wormhole attacks. These attacks pose significant threats to routing nodes and are identified through the utilization of Contiki OS and Cooja Simulator, achieving a detection success rate of up to 90%.[9] Machine learning and cybersecurity are crucial components of GAN networks. Previously, significant effort was needed to train datasets for effective intrusion detection [10]. The Bayesian GAN-based technique can detect cyber attacks while addressing data imbalance and ensuring security during data transfer. It accurately predicts intrusions even in the presence of noise [11]. Utilizing the NSL-KDD dataset with twenty-three categories, it enhances recognition results for binary classification, particularly improving accuracy in handling unbalanced network traffic. Ultimately, it focuses only on five specific categories for conducting our experiments [12].

A novel approach, the Modified Density Peak Clustering Algorithm (MDPCA), along with Deep Belief Networks (DBNs), is suggested for fuzzy aggregation. It is particularly useful when dealing with a complex training set that requires segmentation. The training set is divided into subsets and the training is done by Sub-DBNs classifiers. The fuzzy membership weight is calculated and they are aggregated to provide the output. It achieves better accuracy and good detection rate [13]. In the world of IoT, security is a top priority, especially given the susceptibility to DoS attacks due to memory usage. To combat these issues, a hybrid DoS Intrusion Detection System (IDS) has been devised to detect both known and unknown attacks. This system has been tested across different datasets, consistently outperforming existing methods in terms of detection rates [14]. A Feed-Forward Neural Networks model is devised for identifying DDoS attacks and information theft incidents occurring within the IoT environment [15]. The MQTT protocol is widely utilized in IoT due to its simplicity and lightweight nature. However, IoT devices are susceptible to intrusion by hackers. To enhance security in data transmission using protocols, GAN-AE (Generative Adversarial Network - Autoencoder) is effectively employed [16]. The NIDS aims to enhance accuracy in intrusion detection by leveraging parallel computing, resulting in improved networking traffic analysis and effectiveness [17]. The GAN utilizes network packet capture techniques like Wireshark to collect data sets for identifying different types of attacks, resulting in improved performance compared to existing methods [18]. The main aim is to identify the attacks at the earlier stage and so a machine is built in the IoT environment, The steps are creating an IoT environment using a test bed, Generating attacks by building an adversarial systems a, capturing the network data flow to identify normal and abnormal event behaviors and finally knowledge engineering instructions are used to discover the offense in the network [19]. In the realm of IoT, the Sybil attack infiltrates the network by posing as a genuine node. Through this tactic, the Sybil node disseminates numerous identities of devices, masquerading as authorized entities by mimicking environmental observations. The analysis of the Sybil attack and its worst-case scenarios are performed based on the compromise, deployment and launching phase to overcome from this attack in future [20].

III. Security Attacks in IoT Networks

A. Black Hole Attack

A black hole attack discards a packet in a router by compromising itself as an authorized user. It is considered one of the Denial of Service attacks and it is difficult to detect and prevent the packet loss once occurred.

B. Sinkhole Attack

The Sinkhole attack executes its network infiltration by presenting itself as the shortest route to the intended destination. The nodes get compromised by the path and they move towards the sink holes allowing the sink holes to access their information. The hacker can then modify the data. Sinkholes can be started either within the network or outside the network.

C. Sybil Attack

In the Sybil attack the hacker destabilizes the trust system of a network service by flooding the network with a large number of anonymous state identities providing excessively high traffic demand.

D. Wormhole Attack

The wormhole attack, alternatively known as a network layer attack, involves strategically positioning hackers within

the network.The malicious nodes are dominant to normal nodes and act as a node providing better communication in the network. The data packets, believing the wormhole attack as a normal node, proceeds and discard or modify the data packet.

E. DDos Attack

A DDoS attack is the one in which the executor approaches the network or server making it not available to authorized users by interrupting the services from the internet. The server flooded with more unwanted requests in a challenge to disrupt other authorized services. Various types of DDoS attacks are delineated within the IoT context, encompassing ICMP flood, SYN flood, and UDP flood, targeting network data.

IV. Deep Learning Techniques

Deep Learning is inspired by artificial neural networks and confined to machine learning with ANN algorithms. DL methods deal with large amounts of datasets. DL can manually extract the data in complex vector space. DL methods provide a deep connection in IoT environment.

The Deep Learning technique provides a sophisticated computational framework comprising multiple layers of processing, enabling the acquisition of diverse data representations.

1) Supervised deep learning: It is a machine learning function that plots an input to a preferred output. The data are referred to as training objects providing a supervisory signal based output. Different approaches of Supervised Learning are Convolutional Neural Networks CNNs and Recurrent Neural Networks (RNNs) where the former denotes gaining knowledge of data with reduced parameters and the later refers to consecutive data.

2) Unsupervised deep learning: It is a method of algorithm that uses the design from unlabelled data. Different type of approaches of Unsupervised DL are Deep AutoEncoders(AEs), Deep Belief Networks(DBN), Restricted Boltzmann Machines(RBMs) in which the DBN denotes the replication of its input to its output , RBMs denote two layers visible and hidden that denotes known input and latent variables. Finally Deep Belief Networks (DBNs) deal with greedy layer training of data to perform strong performance in the environment.

3) The Semi-Supervised or Hybrid Deep Learning combines both Supervised and Unsupervised Learning using GAN (Generative Adversarial Network).

V. Proposed Method

Hybrid Deep Learning Based Intrusion Detection System (HMFFGAN) Using Generative Adversarial Network.

GAN is the latest structure for approximate abundant model replica via an adversarial setup, we simultaneously train two models: a generative model G, which captures data distribution, and a discriminative model D, which evaluates the likelihood that a sample originates from the training data rather than G [16].

GANs are frequently utilized to produce synthetic images resembling real ones. Our emphasis is on this principle, and we structured our IDS accordingly. The GIDS comprises two discriminative models: the first discriminator and the second discriminator, which are trained using the following procedure. The primary method utilized is Generative Adversarial Network (GANs), which involves the sequential training of two models: generative and discriminative, as depicted in Fig. 2.

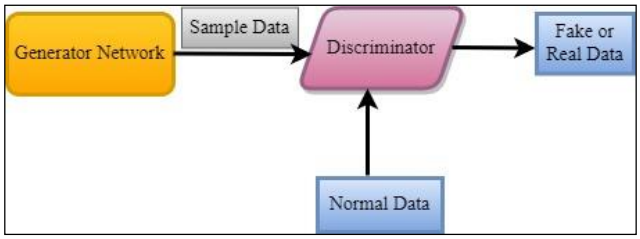

Fig. 2. Basic working of generative model.

The generative model Fig. 3 creates data samples from the training data set and generator network. The discriminator model assesses the authenticity of sample data through binary classification using sigmoid functions, predicting whether the data is genuine or counterfeit. This functionality aids in detecting anomalies within the environment, including potential attacks.

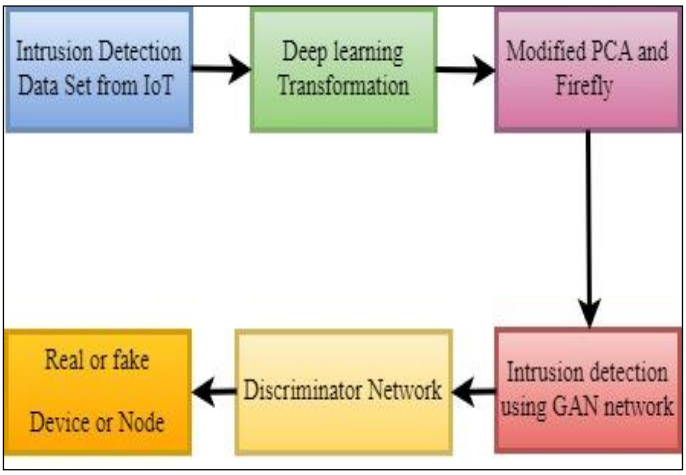

Fig. 3. The hybrid distributed GAN intrusion detection system.

1) Pre-processing Synthetic Minority Oversampling Technique (SMOTE): In this paper, pre-processing involves the utilization of the SMOTE technique to enhance the efficiency of handling imbalanced datasets. This technique addresses minority sampling, aimed at improving the accuracy of intrusion detection for the provided dataset. Balancing classes aims to increase the frequency of minority classes while decreasing the frequency of majority classes, with the goal of achieving a similar number of instances for both classes. In this study, SMOTE is utilized to balance the classes. This involves oversampling the outnumbered category by creating synthetic examples for each minority class sample along the line segments connecting any of the k nearest

neighbors from the opposition class. Additionally, when exceeding the required oversampling level, neighbors are randomly selected from the k nearest neighbors. SMOTE employs k-nearest neighbors for generating the artificial data [17].

The subsequent procedures are executed for the minority class in the SMOTE technique.

- Contrast linking the feature characteristic (sample) less than deliberation and its close neighbor is taken.
- An arbitrary integer between 0 and 1 is multiplied with this difference.
- Results are attached to the characteristic vector lower than the deliberation.
- This makes the choice of an arbitrary tip through the rule fragment between two particular features.
- Allocate a value to the newly generated synthetic minority class sample.
- Iterate the process for the identified feature vectors.

It is essential to identify the nearest neighbors of a point in a d-dimensional space in order to synthetically interpolate selections (for minority class) among these nearest neighbors. Random assignment of data to separate nodes in an allocated set may lead to points that are closest to each other being assigned to different nodes, making it difficult for respective nodes to be aware of these nearest neighbors. Therefore, it is crucial that nearest points are grouped together and also allocated to different nodes in such a way that nearest points are consistently processed on the same node. As a result, the challenge of imbalanced data is effectively addressed using the SMOTE approach.

2) Feature extraction using Modified Principal Component Analysis (MPCA): In this paper, MPCA algorithm is offered for feature extraction applied to degrade the composition of features. The aspiration of PCA is to dimensionality deduction of the data space (obeyed variables) to the lower natural dimensionality of feature space (self-dependent variables), which are demanded to portray the data economically. By discarding smaller factors, the PCA effectively reduces the piece of features and displays the data set in a low dimensional subspace [18] [19]. PCA is a classical multivariate data analysis system that's useful in direct point birth. The PCA system can not guarantee that the data bonded to the applicable classes is effectively compacted. To avoid the overmentioned backwashes, qualified PCA is propounded.

3) Feature selection using Improved Firefly Optimization (IFFO) algorithm: In this study, an enhanced firefly algorithm for feature selection is employed. The Firefly algorithm (FA), introduced by [20], is a biologically-inspired stochastic optimization approach. FA operates as a population-based metaheuristic, where each firefly within the population represents a feasible solution in the search space. It simulates the behavior of fireflies, which emit light signals to communicate and attract mates. Additionally, they utilize flash lighting to attract potential prey and serve as an alarm system.

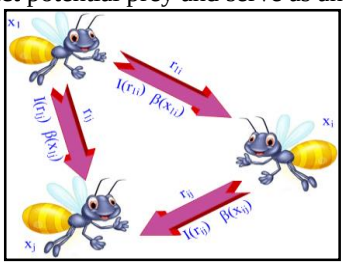

Fig. 4. Firefly algorithm.

Fig. 4 above illustrates the Firefly algorithm. The FA algorithm begins by initializing a swarm of fireflies, with each firefly determined by its luminous intensity.

It compares the flare aggressiveness of the firefly, the inferior glare aggressiveness firefly will displace to the advanced flare aggressiveness firefly. Depending on enchantment the displacing length may differ. The new firefly blaze aggressiveness will be estimated and streamlined once it has displaced.

Algorithm 1: IFFO for Feature Selection

Input: Input: Population size (n), Maximum of iteration (maxIter), Absorption coefficient (γ), Randomization parameter (α), Attractiveness value ($\beta_0 = 1$)

1. Objective function (x), $x = (x1,...,)T$ consider higher accuracy of classifier as objective function
2. Produce initial population of fireflies xi $(i = 1, 2, \ldots, n)$
3. Light intensity Ii at xi is found via $f(xi)$
4. Describe light absorption coefficient γ
5. while (t < Max_generation)
6. for i=1:n all n fireflies
7. for j=1:i all n fireflies
8. if ($Ij > Ii$), Move firefly i towards j in d-dimension;
9. end if
10. Attractiveness changes along with distance r via exp[$-\gamma r$]
11. Compute fitness function using (14)
12. Compute objective model using (13)
13. Estimate new solutions and update light intensity using (11)
14. Update the optimal features using (16)
15. end for j
16. end for i
17. Rank the fireflies and find the current best
18. end while
19. A firefly i shifts to a more attractive

In this script, the IFFO algorithm is utilized to achieve optimal outcomes by refining both energy and detection criteria. In the IFFO algorithm, fireflies are evaluated and the most optimal ones are selected based on their fitness values. Selected fireflies undergo crossover and mutation to produce new, improved solutions. These refined solutions are incorporated into the firefly population, and the process of selecting and refining fireflies continues iteratively.

Generative model intrusion detection system algorithm

Input: Let Input X denotes real data
Z denotes data from generator

IOT denotes set of N items
Pdata(x)=Distribution of real data
Pdata(z)=Distribution of generator

1) Data collection

Let Xi=X1,X2……Xn
and Zi=Z1,Z2……Zn
D(Xi)=Discriminator Network
G(Zi)=Generator Network
Data Collection is denoted as

$$\left\{D_i^*, G_i^*\right\} = \arg\arg\min_{Gi} \arg\arg\max_{Di} V_i\left(D_i, G_i\right)$$

2) Training phase: To find the optimal value it is denoted as,

$$V(D_i, G_i) = \mathrm{E}_{x\sim P_{xi}}[\log D_i(x)] + \mathrm{E}_{z\sim P_{zi}}[\log(1-G(Z))]$$
$$V(D_i, G_i) = \mathrm{E}_{x\sim P_{xi}}[\log\log D(x_i)] + \mathrm{E}_{z\sim P_{zi}}[\log(1-G(Z_i))] \quad (1)$$

Anomaly Detection Phase

The Anomaly Detection is done by Threshold Based Intrusion Detection

Assume True Positive (TP) ->Attack denoted as positive

False Negative (FN)->Attack denoted as negative

False Positive (FP)-> Normal data denoted as positive

True Negative (TN)-> Normal data denoted as Negative

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (2)$$

Assume Threshold T which denotes the range from 0.85 to 1

Let Yi=Xi+Zi denotes the overall data

if Yi<Threshold Ti
then Yi is intruder
else
Yi is normal data
End

1) Intrusion detection metrics: The metrics used to evaluate the performance of Intrusion Detection are Accuracy, Detection Rate (DR), Precision, Recall and False Positive Rate (FPR).To indicate these metrics four parameters have been considered.

They are True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN).TP, FN denotes the attack and FP, TN denotes the Normal User.

Accuracy refers to the proportion of predictions that are accurately classified as either Attack or Normal, expressed as a percentage.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (3)$$

The detection rate is defined as the proportion of all predicted attack instances that correspond to actual attack records.

$$precision = \frac{TP}{TP + FP} \quad (4)$$

Recall represents the proportion of assessments that represent the ratio of True Positive attack records to the total number of True Positive and False Negative instances.

$$precision = \frac{TP}{TP + FN} \quad (5)$$

The False Positive Rate (FPR) indicates the likelihood of normal data being inaccurately identified as attack data.

$$FalsePostiveRate = \frac{FP}{FP + TN} \quad (6)$$

VI. Result and Discussion

In this study, we evaluated the accuracy of the initial discriminator trained on provided attack data. Results showed that attack data used in the training process were readily detected, while attempt data not included in the training were more challenging to detect. Table I shows the system and software requirements.

TABLE I. System and Software Requirements

System Requirements	Software Requirements
IoT devices with compatible processors	Linux distribution
Reliable network infrastructure	Deep Learning Framework (PyTorch)
Minimum 8 GB of RAM	Data Preprocessing Tools (NumPy)
SSD or HDD storage	Python Environment
Ethernet or Wi-Fi connectivity	Integrated Development Environment (IDE)

This highlights the need for a new detection model capable of accurately identifying attempts even when only average data are used in the training process.

TABLE II. Performance of the HDGIDS in IoT

Attack	Detection rate	Precision	Accuracy	Recall
Black hole attack	98%	98.3%	99%	97%
Sinkhole attack	97.5%	97.3%	98%	98%
Sybil attack	96%	96.2%	98%	95%
DDoS attack	99%	98.7%	97%	90%
Warm hole attack	97%	97.6%	98%	95%

Additionally, we assessed the detection sensitivity of an alternative discriminator trained on arbitrary dummy data instead of genuine attempt data. Table II illustrates the detection performance for each of the four attempted datasets. Results showed that each of the five attempts was detected with 98% delicacy. It is defined as how much accuracy and attack for HDGIDS in IOT. The different attacks are Black

hole, Sink hole, Sybil attack, DDos, Warm hole are considered along with the accuracy.

Fig. 5 illustrates the different phases of accuracy values undergoing change. HMFFGAN- grounded IDS has 98% of accuracy.

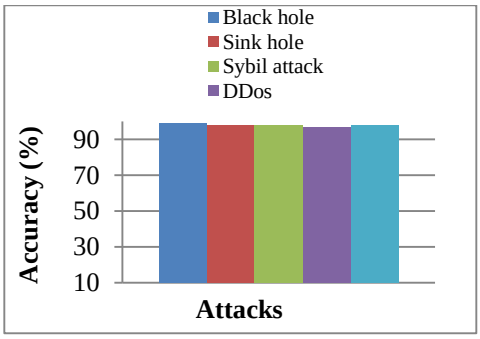

Fig. 5. Accuracy.

Fig. 6 shows the precision % in terms of attacks for Black hole, Sink hole, Sybil Attack, DDos, Warm hole.

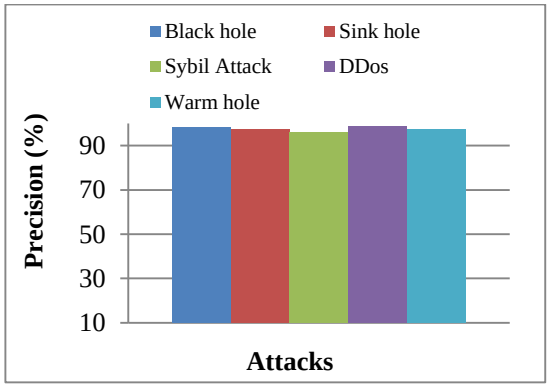

Fig. 6. Precision.

It pertains to the degree of agreement among individual measurements; the smaller the CV, the greater the precision of the values. Here Sybil Attack will take the least value for precision. Among all the attack nearly precision value will reach 98% of accuracy. It is defined as recall value for the attacks. Recall is calculated by dividing the number of relevant documents retrieved by a search by the total number of relevant documents, while precision is determined by dividing the number of relevant documents retrieved by a search by the total number of documents retrieved by that search. Each attack takes some amount percentage for recall values in Fig. 7. Since the recall percentage in the current attack is not maximal, it takes less time in order to predict the attacks.

Utmost of the time, we don't indeed know the findings rates of our participators. To compute the discovery grade for a participator, we'd possess to endure how numerous complete UX troubles live in a plan. But that's exactly what we're testing to dig out with estimation. The evaluation of detection models in the proposed method reveals important insights into their performance against various types of IoT attacks. It demonstrate that the systems trained on specific attack data to provide strong accuracy in detecting known attack patterns but struggle with detecting new or untrained attack types, highlighting the need for improved generalization capabilities.

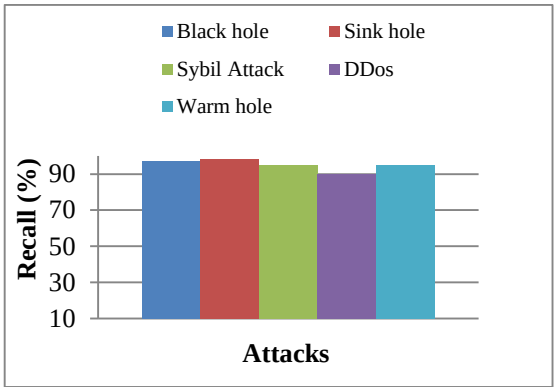

Fig. 7. Recall.

In Fig. 8, it is defined as the detection rate for every attack is calculated.

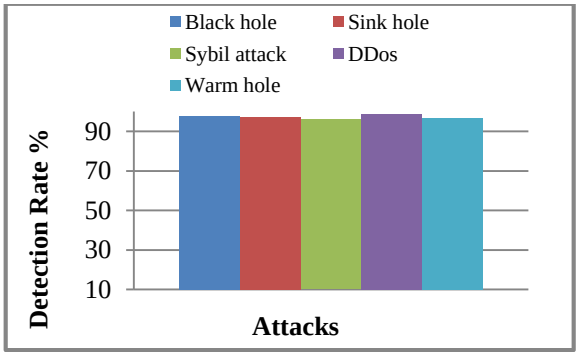

Fig. 8. Detection rate.

Additionally, alternative models trained on arbitrary dummy data provide valuable insights into detection sensitivity under different training conditions. Precision values approach an impressive 98% across all attack types, underscoring the models' effectiveness in correctly identifying relevant attacks. However, variability in recall rates across attack types impacts prediction time and highlights the importance of comprehensive detection approaches. Future research should focus on refining detection algorithms to enhance robustness and adaptability in addressing evolving IoT security threats.

VII. Conclusion

In this paper, we've proposed a crossbred GAN- grounded IDS grounded on modified top element dissection and firefly optimization (HDGAN Network) that can discover intrusion to the IoT. In this allocated framework, every IoTD can cover its own data as well as neighbor IoTDs to descry anomaly geste of the bias. The HDGAN network doesn't bear participating the datasets between the IoTDs it save the sequestration of the delicate data similar as patient medical data in medical center mesh. it pierce the data set from single ID device the HDGAN mesh trained with dataset with SMOTE and Firefly optimization algorithm which allow the GAN mesh to determine intrusion efficiently. The Simulation results display that the offered allocated HMFFGAN-

grounded IDS has 98 accuracy, 98 precision, and 95 false positive rate compared to the being allocated Intrusion discovery network. Future IoT security research should prioritize enhancing model robustness against adversarial attacks with techniques like adversarial training and input perturbation. Dynamic, adaptive intrusion detection models for continuous learning in evolving IoT environments remain essential areas for exploration.

REFERENCES

[1] T. Kim and W. Pak, "Early Detection of Network Intrusions Using a GAN-Based One-Class Classifier," in IEEE Access, vol. 10, pp. 119357-119367, 2022.

[2] Nagarathna Ravi; S. Mercy Shalinie,"Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture" IEEE internet of things journal, vol. 7, no. 4, pp.3559-3570, 2020.

[3] H. Ding, Y. Sun, N. Huang, Z. Shen and X. Cui, "TMG-GAN: Generative Adversarial Networks-Based Imbalanced Learning for Network Intrusion Detection," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 1156-1167, 2024.

[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] C. Park, J. Lee, Y. Kim, J. -G. Park, H. Kim and D. Hong, "An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks," in IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2330-2345, 1 Feb.1, 2023.

[6] Sunanda Gamage , Jagath Samarabandu" Deep learning Methods in network intrusion detection: A survey and an Objective comparison "Journal of Network and Computer Applications, Vol 169,pp.1-21, 2020.

[7] Y. Li, X. Peng, J. Zhang, Z. Li and M. Wen, "DCT-GAN: Dilated Convolutional Transformer-Based GAN for Time Series Anomaly Detection," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 4, pp. 3632-3644, 1 April 2023.

[8] Z. Li, P. Wang and Z. Wang, "flowgananomaly: Flow-Based Anomaly Network Intrusion Detection with Adversarial Learning," in Chinese Journal of Electronics, vol. 33, no. 1, pp. 5 January 2024.

[9] 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.

[10] Dunmore, J. Jang-Jaccard, F. Sabrina and J. Kwak, "A Comprehensive Survey of Generative Adversarial Networks (gans) in Cybersecurity Intrusion Detection," in IEEE Access, vol. 11, pp. 76071-76094, 2023.

[11] J. Xie, A. Rahman and W. Sun, "Bayesian GAN-Based False Data Injection Attack Detection in Active Distribution Grids With ders," in IEEE Transactions on Smart Grid, vol. 15, no. 3, pp. May 2024.

[12] N. Zhu, G. Zhao, Y. Yang, H. Yang and Z. Liu, "AEC_GAN: Unbalanced Data Processing Decision-Making in Network Attacks Based on ACGAN and Machine Learning," in IEEE Access, vol. 11, pp. 52452-52465, 2023.

[13] Janofer Ibrahima, J., Naskath, J., Lakshmi Prabha, S., Paramasivan, B., "Phone directory using mobile application", International Journal of Scientific and Technology Research, 2020, 9(3), pp. 6495–6498.

[14] Sifan Li, Yue Cao, Shuohan Liu, Yuping Lai, Yongdong Zhu, Naveed Ahmad, HDA-IDS: A Hybrid dos Attacks Intrusion Detection System for iot by using semi-supervised CL-GAN, Expert Systems with Applications, Volume 238, Part F, 2024,122198.

[15] Naskath, J., Paramasivan, B., Mustafa, Z. et al. Connectivity analysis of V2V communication with discretionary lane changing approach. Journal of Supercomputing.

[16] Tej Kiran Boppana, Priyanka Bagade, GAN-AE: An unsupervised intrusion detection system for MQTT networks, Engineering Applications of Artificial Intelligence,Volume 119,2023,105805,ISSN 0952-1976.

[17] Xiang, Z., Li, X. Fusion of transformer and ML-CNN-bilstm for network intrusion detection. J Wireless Com Network 2023.

[18] Jha, K.K., Singh, P., Bharti, N., Sinha, D., Kumar, V. (2023). GAN-Based Data Generation Technique and its Evaluation for Intrusion Detection Systems. In: Kumar Singh, K., Bajpai, M.K., Sheikh Akbari, A. (eds) Machine Vision and Augmented Intelligence. Lecture Notes in Electrical Engineering, vol 1007. Springer, Singapore.

[19] Naskath, J, Paramasivan, B, et al. (2020) A Study on Modeling Vehicles Mobility with MLC for enhancing vehicle-to-vehicle connectivity in VANET. Journal of Ambient Intelligence and Humanized Computing, Springer, ISSN: 1868-5137, https://doi.org/10.1007/s12652-020-02559-x.

[20] J. Rani, A. Dhingra and V. Sindhu, "A Detailed Review of the IoT with Detection of Sinkhole Attacks in RPL based network," 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, 2022, pp. 1-6.