International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

GAN Model for Network Intrusion and Malicious Detection in Network Security

ALK Bilahari,
Research Scholar, bilahari89@klh.edu.in

Dr. M Saidi Reddy,
Associate Professor, msreddy33@klh.edu.in
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad-500075, Telangana, Hyderabad

Abstract

As of late, the utilization of Internet of Things (IoT) is persistently grow- ing, while IoT frameworks are experienced in applications from various spaces, similar to brilliant urban communities, industry, agribusiness, and so on. The Internet of Things is made up of billions of connected devices that can send and receive data over the internet. The Internet of Things (IoT) is at risk of cyberattacks because of this interconnection, which compromises its security. In this context A Malicious Attack Detector (MAD) is developed for the Internet of Things (IoT) with the primary objective of preventing attacks on IoT systems. In order to first learn about poisoning datasets and then identify malicious activities, MAD employs a GAN-based model. In this paper we present the accuracy per- formance of the discriminator on central generator using total number of epochs. We also highlight the recent risks and solutions for the malicious activities.

Keywords: GAN, IoT, Deep Learning, Malicious Attack Detector (MAD)

1 Introduction

With the spread of IoT (Internet of Things), IoT systems are being used in various fields such as smart cities, industry, and agriculture. The Internet of Things consists of billions of connected devices that can send and receive data over the Internet. The Internet of Things (IoT) is subject to cyberattacks and security compromises because of this connectivity. As part of the IoT NGIN project, a Malicious Attack Detector (MAD) has been developed with the primary goal of preventing attacks on IoT systems. To first learn about record poisoning and then identify malicious activity, MAD uses a GAN-based model. For generative modeling, a type of neural network architecture known as Generative Adversarial Networks (GANs) is used. Ian Goodfellow et al. were the first to propose GAN architecture. In the 2014 article "Generative Ill-disposed Organizations". A GAN model's goal is to learn how the training data are distributed and arranged so that the model can use the properties of the training data to generate new data. In practice, two neural network mod- els make up a GAN model: a discriminator and a generator. Discriminators I differentiate between real data from the domain and fake data generated by generators by training generators to produce credible fake data. There is com- petition between these two models. This is because both the discriminator andthe generator are attempting to deceive each other.

The exciting field of GANs promises to produce examples from the real world in a variety of fields. Anomalies like these can be detected using GAN models when hackers carry out adversarial attacks, the detection of fraudulent or malicious attacks. Most of the time, IoT networks have a lot of wearable devices, like sensors, that connect to each other and talk to each other to share information everywhere without anyone having to do anything. Multi- ple security threats have made these systems susceptible due to the growing scale of IoT networks and the fact that IoT devices are connected to the Inter- net and contain personal information. As a result, IoT device cybersecurity is crucial. All of these methods for protecting networks, systems, and programs from digital attacks are referred to as cybersecurity. Cyberattacks against IoT networks expect to get to IoT gadgets and adjust or annihilate private infor- mation and sharing models. Malicious nodes carry out the majority of attacks. As a result, it's critical to find these malicious

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

nodes in IoT networks. With- out legitimate safety efforts, IoT frameworks are presented to weaknesses and IoT hubs can be harmed by vindictive assaults. To get IoT networks with IoT-GAN, a Distraught was formed and incorporated into the framework to recognize malignant hubs. As attackers become more creative, it is very diffi- cult to create an effective her MAD module. The IoT-GAN MAD module is effective, accurate, and able to detect malicious nodes in real time.

IoT devices and networks [24] [25] can be protected from attacks and abnormal behavior with the help of powerful machine learning models [23]. It distinguishes between normal and malicious traffic by employing conventional monitoring techniques like support vector machines (SVMs) and decision trees to identify anomalies. However, these models exhibit decision bias due to the prevalence of anomalous samples, or samples with a significantly lower number of attacks than usual. The GAN model can deal with this case well. Specifically, the solid generative force of GAN models permits them to become familiar with the appropriation of ordinary information and recognize unusual infor- mation. Moreover, GAN models can produce a wide assortment of assaults, including beforehand unidentified assaults that are not ordinarily present in the informational index. As a result, GAN techniques are extremely effective in cybersecurity for systems where regular threats and unexpected attacks occur. Future attacks can be predicted before they are even recognized by the attacker by making use of GANs.

The GAN model is used by IoT-GAN MAD to train on network proto- cols that contain both normal activity and attacks, as well as other poisoning datasets that contain malicious activity against IoT systems. This improves the performance of IoT networks. The Fig .1 shows the complete process of IOT-GAN-MAD system.

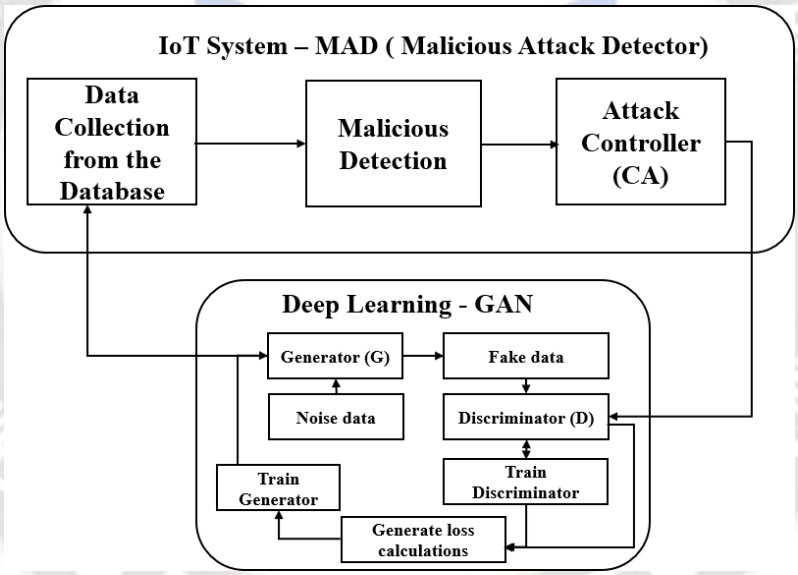

Fig. 1 Architecture view of IOT-GAN-MAD sytem

1.1 Research Challenges

Existing methods face a number of implementation difficulties as a result of the use and effectiveness limitations imposed by the deployment of resource-constrained IoT devices [19]. This study has made the following contributions:

1. The security issues posed by malicious insiders are addressed and a detec- tion mechanism for the Internet of Things is presented by the proposed algorithm, which is based on Artificial Intelligence (AI) and aims to ensure the security of critical and sensitive IoT data.
2. This method presents a method for smoothing input data to increase pre- dictive performance and reduce false positives in comparison to previous prediction methods that primarily treat insider threat as a single category.
3. The dataset that was produced by the NS-2 simulation that was based on the Computer Emergency Response Team (CERT) is used to simulate the proposed method.

1.2 Motivations and Contributions

Cyber-physical applications and systems are built with high levels of depend- ability in mind. As a consequence

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

of this, the information that is gleaned from these frameworks typically consists of typical working conditions as well as odd occurrences from time to time. Many datasets used by researchers to model system profiles in this field are highly imbalanced [20] due to the rarity of these unusual incidents. This has the following effects:

1. When unbalanced data is used, bias is built into models. Due to the imbal- ance in the data, random guess is guaranteed to return high accuracy, rendering machine learning models redundant.
2. Due to bias differences between systems, anomaly detection frameworks that are able to adapt to various systems with varying ratios of typical to anomalous samples perform poorly. Due to the diverse composition of the various datasets, generalization is challenging.

As a result, our obligations in this examination work are as follows:

1. Creation of a GAN for the purpose of contextually modeling normal and malicious attacks.
2. The creation of a framework for multiple stages of transfer learning that makes use of GANs to generate distinct clusters from data that isimbalanced.

The rest of the paper is organized as, Chapter 2 gives the complete Literature review, followed by Chapter 3 shows the proposed model and Chap- ter 4 section shows the results and discussion, and finally chapter 5 is the Conclusion.

2 Related Work

The Internet of Things, or IoTs, are set to revolutionize our lives and are cur- rently gaining widespread acceptance. Savvy modern organizations, medical care, and shrewd homes [24] are only a couple of the many purposes for IoT gadgets. Due to the fact that IoT devices generate and manage a large amount of sensitive data, their security is always a challenge. A security breach has been observed to have the potential to affect individuals and ultimately the entire world. In contrast, artificial intelligence (AI) is extensively studied for providing security for IoT devices and has numerous applications. Malicious insider attacks pose the greatest threat to IoT device security [25]. However, the majority of IoT security research has concentrated on methods for pre- venting unauthorized and illegal access to data and systems; Tragically, an IoT network's most damaging pernicious insider threats, typically the resultof internal abuse, are ignored. As a result, the primary objective of this inves- tigation is to use computer-based intelligence to distinguish malicious insider attacks in the IoT environment. This chapter shows some of the backgorund work done by researchers in the past.

Yanpeng Guan.et.al [1] in their research explains, For networked cyber- physical systems under physical and cyber attack, the issue of joint distributed attack detection and distributed safety estimation is the focus of this paper. A sensor network that is wireless keeps an eye on the system. Readings from a group of sensors that are spatially dispersed in a wireless sensor net- work are sent to remote estimators over the wireless network medium. In order to intentionally alter system states, malicious attackers can simultane- ously launch physical system layer fake data injection attacks and cyber layer jamming attacks to compromise wireless transmission channels between sen- sors and remote estimators. block. Sensor readings can be randomized with numerical likelihood assuming an assailant intentionally disrupts the relating transmission channel.

Ahmed Yar Khan .et.al [2] in their research says, A man-made, reasoning- based solution for identifying and assessing malicious insider attacks in the IoT environment is proposed in this study. The proposed framework primarily consists of three phases: 1) data collection and classification, 2) establishing thresholds, and 3) identifying malicious threats, contrasting malicious activ- ities with benign ones, and predicting the outcome. The proposed algorithm establishes the method for distinguishing benign devices from malicious ones and evaluates the degree of maliciousness in order to facilitate the IoT envi- ronment. Traditional AI algorithms such as Deep Learning, Neural Networks, and the Hidden Markov Model are regarded as resource-intensive.

Zhihai Yang et.al [3] explains, Probabilistic derivation and reliability assess- ment of conduct joins are the focal point of this article, which likewise gives an original viewpoint on a brought together discovery system for distinguish- ing different malignant dangers. An association graph is first constructed using the atomic propagation rules of coupled networks and users' inherent rating motivation from the initial rating matrix. They then re-identify the relevant links in the targeted network and evaluate the trustworthiness of link behav- iors in the coupled association network by utilizing a factor graph model of a coupled network. Finally, it is possible to empirically infer suspicious users and items by conducting a comprehensive evaluation of the trustworthiness ofthe targeted network's links and nodes.

Taehoon Kim and Wooguil Pak et.al [4] and Nayak, Sharmistha [18] in thier work explains that, The early detection of intrusions is an essential component of network security. However, it is challenging to detect

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

intrusions prior to the end of a session because the majority of studies on network intrusion detection systems use features for entire sessions. To solve this problem, the proposed method makes use of features in packet data to determine whether packets are malicious traffic. Dishonestly recognizing typical bundles as interruptions or interruptions as typical traffic for the underlying meeting is increased by this method unavoidably. As a solution, the proposed method learns the patterns of harmful packets to classify both malicious sessions and network intrusions. A new Generative Adversarial Network (GAN) training dataset is created using misclassified data by the LSTM-DNN model that was trained on the original training dataset. Using the GAN that was trained using this dataset, the LSTM-DNN is able to accurately classify the currently received packet.

Okwudili M.Ezeme et.al [5] in their research explains, The vast majority of datasets that represent the state of systems, whether in the realm of soft- ware or hardware, are skewed in one direction or another. The fact that these systems' reliability requirements make anomalies extremely rare causes this imbalance. Consequently, the anomaly is only captured by a small number of anomaly detection datasets. GANs (generative adversarial networks) have recently demonstrated promising results in image generation tasks. To resolve the issue of information lopsidedness in oddity identification errands and to introduce an original structure for irregularity discovery, they utilize restric- tive GANs (CGAN) to create conceivable conveyances of a given profile in this review.

Chen, Xiaofei, et al.[16] in their research explained about unsupervised model for anomaly detection for time series using the generative adversarial networks (GANs), that learns the normal patterns of time series data, andthen use the reconstruction errors to recognize anomalies. Chen, Zhenzhu, et al [17] in their research explained use of Deep Learning in IoT devices to make contradiction between the data collection and privacy concerns.

Chhabra, S et al.[21] in their research explained the importance of collection of data through multiple Electrical and Sensors. Here they mentioned about 5G and 6G technologies for Smart City building. In their work they have also mentioned the importance of finding and avoidance of attacks like malicious and intrusions in the communication networks.

Table 1 Survey report on Attacks and their Limitations

Ref.No	Type of Attacks	Methodology	Limitations
[1]	FDI, Jamming	Distributed secure	A two-step attack
[2]	Malicious	IoT-Malicious insider	Attack prevention
[3]	Malicious	Probabilistic evaluation	Real world data
[4]	Network Intrusion	GAN-LSTM-DNN	Real time intrusion
[5]	Anomaly detection	AD-CGAN	single class CGAN
[16]	Anomaly detection	IOT-GAN	Time series data
[17]	GAN Attacks	Deep Learning-IoT	Collaborative data
[18]	Reliable routing	Deep Learning-SVM	Classifiers

3 Proposed Method

In this chapter, we have considered all the required implementations and limi- tations from the previous chapter and designed a IOT-GAN-MAD model which is a Light weight, IoT environment and AI capability system.

Generative Adversarial Networks (GAN) have a capability of classifying the attacks on real time data and time series data because of its presence of Generator and Discriminator. At present moment, it is very much neededto classify attacks in advance, because of many cyber crimes happening and increasing day by

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

day. In the Table 1, we have mentioned the survey on Attacks and their Limitations. Some of the required implementations needed like

1. Using IOT-GAN, model should be designed to classify both the Anomaliesand Malicious detection.
2. A designed model should work on the both Time series data and Real timedata.
3. A designed model should have the Light weight, IoT environment and AI capability, so that it can produce the high performance accurate results.

The Internet of Things (IoT) is one of the upcoming big ideas that can support societal changes and economic growth. It is one of the ICT segments that is expanding at the fastest rate. A particular obstacle is how to create solutions that support European industry and values by making use of existing technological advantages.

IoT-GAN will power the coming generation of IoT. It reveals a meta- architecture based on patterns that includes current, past, and potential IoT architectures. IoT systems can also be self-aware and autonomous thanks to augmented reality (AR) support for humans and privacy-preserving feder- ated machine learning (ML) [22] and Artificial Intelligence (AI). Implementing Meta-Level Digital Twins with interconnected DLTs and Self-Sovereign Iden- tities is one way that distributed IoT cybersecurity and privacy are given priority by IoT-GAN. The proposed method is shown Fig 2.

Take into consideration an IoT system with a set of 'N' IoTDs (IoT devices). A set of previously transmitted data points known as Di belongs to each IoTDi in this system, and their distribution is 'pdatai (x)'. Contingent upon the IoT application,' x' could be time series, monetary records, or wellbeing observ- ing datasets. We assume that 'D1UD2U. UDn = D', where D is the total amount of data that is available and has a distribution 'pdata', and that 'Di' contains data points from the normal 'IoTD state', in which there is no mali- cious activity in the IoT. In this model, each 'IoTDi' tries to learn a generator distribution, 'pgi', over the dataset it has available, 'Di', so that 'pgi = pdatai', and uses that distribution to find malicious systems. Any action by an assailant that makes an IoTD convey information focuses that don't stick to its informa- tion appropriation 'pdi' is a noxious into our framework. In point of fact, if an 'IoTD' knows the distribution of its own normal state, it can easily distinguish a data point that is not comparable to the normal state distribution.

Each 'IoTDi's generator GAN(Generative Adversarial Network) endeavors to deliver information of interest close to the normal state data to find the best estimate of 'pdatai'. Conversely, the discriminator for each IoTD means to recognize the created data of interest from its own dataset. The generated data points actually mimic the system's anomalous state because they are generated from a distribution 'pgi' that is not equal to 'pdatai', and 'gi' are chosen at random for an untrained GAN. The discriminator therefore gives the generator zero values. Therefore, in this regard the generator and discriminator at each IoTD as the best 'gi' and 'di' so that the generator can produce information guides that are close to the normal state and the discriminator can distinguish between the strange (abnormal) and normal data of interest.

$$(Di,\ Gi) = \epsilon_{x\sim}\ pdata\ [log D_i(x)] + \epsilon_z\ -pzilog(1 - D_i(G_i(z)))$$

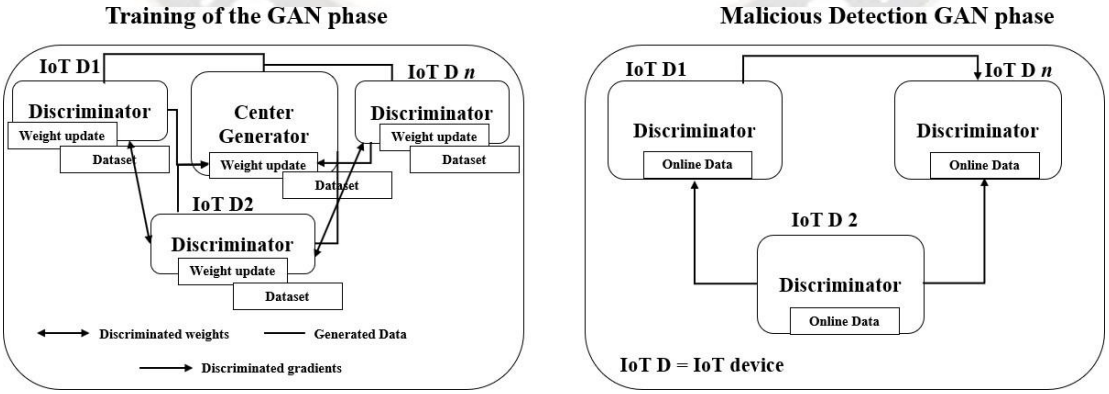

Fig. 2 Proposed method of IOT-GAN-MAD sytem

first term in (eq.1) requires the discriminator to produce values that are exactly one for real data. In contrast, any abnormal point generated by the generators is penalized in the second term. The discriminator aims to maximize the value of the value function defined in (eq.1), whereas

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

the generator of every IoTD will strive to minimize it. As a result, the following minimax problem can be used to determine the discriminator and generator's best possible solutions.

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

3.1 Discriminator Training phase

For a predetermined, the generator produces two batches every epochs of anomalous points, also known as fake points that do not originate from the actual datasets. In addition, the discriminator samples a batch points from its available dataset Di at each 'IoTDi'. The generator sends each produced clump to each 'IoTDi' which, ascertains the accompanying misfortune esteem.It is shown in Eq (3).

$$L_i(\theta_i) = \frac{1}{b}\left[\sum_{x} \log D_{\theta_i}(x) + \sum_{x} \log(1 - D_{\theta_i}(x))\right]. \quad (3)$$

3.2 Generator Training phase

The following loss, which is an approximation of the value function for each IoTD's generator in (eq.1), is calculated by each 'IoTDi' every epochs using generator

i. Since the discriminator typically converges faster than the gen- erator, it has been demonstrated in [6] that the generator's loss should not include the term for practical purposes. After that, this value is sent to the center by each 'IoTD'. Then, the middle purposes the got misfortune values from IoTD's to ascertain its typical misfortune.

$$L_i(\theta_i) = \frac{1}{b}\left[\sum_{x} \log D_{\theta_i}(x) + \sum_{x} \log(1 - D_{\theta_i}(x))\right].$$

3.3 Discriminator weights updation

Every "IoTD" transmits and receives its discriminator weights to its neighbor- ing "IoTD" at every epoch. As we previously mentioned, keep in mind that the connection graph ought to include a cycle that includes each and every "IoTD." In the end, this makes it simpler for "IoTDs" to receive the discrimi- nator weights of all other IoTDs. Because the IoTDs share only the weights of their discriminators rather than their own data, this phase enables the system to maintain privacy during training. The generator gets the loss value from each discriminator using this approach. Additionally, each dataset will be used to train the discriminator for each "IoTD." As a result, after a sufficient num- ber of preparation times, the focal generator will join the circulation of the complete dataset D. The "IoTD" discriminators will also be comparable to a GAN discriminator that has access to the entire dataset. In the distributed GAN architecture, this means that the discriminator of each "IoTD" can detect intrusion on both its own data and the data of its neighbors.

3.4 Malicious Detection phase

Because all of the discriminators at IoTDs are capable of detecting an intrusion into the system, the central unit will no longer be required after the distributed GAN converges. Because of this, each IoTD, IoTD will use real-time data to run both its own discriminator and one of its neighbors' discriminators. The optimal discriminator, as shown in eq(1), will output 1/2 for a normal state data point. The normal state of the IoTD can be determined by comparing the output of the discriminator to 1/2 in order to identify an intrusion intothe system. However, if the result is closer to 0 or 1, respectively, the IoTD will be attacked. Because each IoTD can also check the data of its neighbors, this method enables the Internet of Things system to detect an intrusion/ malicious without the need for a central unit. The malicious/ intrusion loca- tion period of the proposed GAN-based MADs is portrayed in the figure. 2.The proposed Algorithm is explained step by step with Discriminator and Generator functions shown in Algorithm 1.

4 Results and Discussion

In our experiment work, we choose use of a regular daily activity recognition dataset collecting from different people of ages, heights, and weights using a smartphone. Wearable IoTD-collected health datasets are a good example, so we use this dataset. It's possible that the people who own these health datasets won't want to share them because they keep them private. Twelve activities were the subject of data collection: running ahead, jumping, sleeping, sitting, standing, taking the elevator up and down, and walking ahead, left, right, upstairs, and downstairs are all forms of transportation. The dataset contains 4500 recordings, each with 500 features in the frequency and time domain.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

Algorithm 1 Proposed Algorithm *IoT − GAN − MAD*

Require: *Initialize —database = private− dataset‡ NSLKDD− Dataset*

Ensure: *Train MAD on Hybrid database*

1: *every —epoch ⊂ do*
2: **if** *allabels* > 0 **then**
3: *do ⊂ weightupdate/G(Generator)*
4: *do ⊂ updateonlinedata/D(Discriminator)*
5: **else**
6: *G ⊂ g*
7: *D ⊂ d*
8: **end if**
9: **while** *D* ≠ 0 **do**

$$L_i(\theta_i) = \frac{1}{b}\left[\sum_x \log D_{\theta_i}(x) + \sum_x \log(1 - D_{\theta_i}(x))\right] \quad (5)$$

Train MDA on remaining samples

10: [*G* ≠ 0]

$$L_i(\theta_i) = \frac{1}{b}\left[\sum_x \log D_{\theta_i}(x) + \sum_x \log(1 - D_{\theta_i}(x))\right] \quad (6)$$

Remove pending samples from the database

11: **end while**

We take into account an attacker who is able to inject false data into the features of the training dataset in order to model the malicious detection. In ten unmistakable situations with fluctuating assault to-flag power proportions, arbitrary Gaussian noise principle is applied to each element of the preparationdata of interest. We also consider an outside assault discovery in which each IoTD examines its neighbors and an inward assault recognition in which each IoTD examines its own data.

We also tested the NSL-KDD dataset in our work. The sensible amount of information in the training and test sets is another advantage of NSL-KDD over KDD'99, providing an incredible opportunity to conduct probes onthe entire set. Due to the fact that it is utilized by numerous researchers to develop Interruption Recognition Frameworks that are productive and precise, the NSL-KDD is one of the most notable datasets that can be accessed for free. The following metrics are used to calculate the proposed algorithm's overall performance, precision for assault discovery, the rate of misleading prob- lems, the cost of computation, and the time required for computation. These

performance metrics must be used to evaluate any attack detection method.

$$Accuracyof Attackdetection = \frac{TruePositive + TrueNegative}{TotalNo.oftestedsamples} \quad (7)$$

$$False - positive - rate(FPR) = \frac{Incorrectlyclassifiedmaliciousbysensors}{TotalNo.ofsamples} \quad (8)$$

$$False - negative - rate(FNR) = \frac{Incorrectlyclassifiedmaliciousactivites}{TotalNo.ofsensoractivites} \quad (9)$$

The accuracy for the internal and external attacks is given as

$$False - negative - rate(FNR) = \frac{TP + TN}{TP + TN + FP + FN} \quad (10)$$

The internal and external attacks evaluation is given as

$$Precisionscore(P) = \frac{TP}{TP + FP} \quad (11)$$

$$Recallscore(R) = \frac{TP}{TP + FN} \quad (12)$$

$$F1score(F1) = \frac{2 * P * R}{P + R} \quad (13)$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

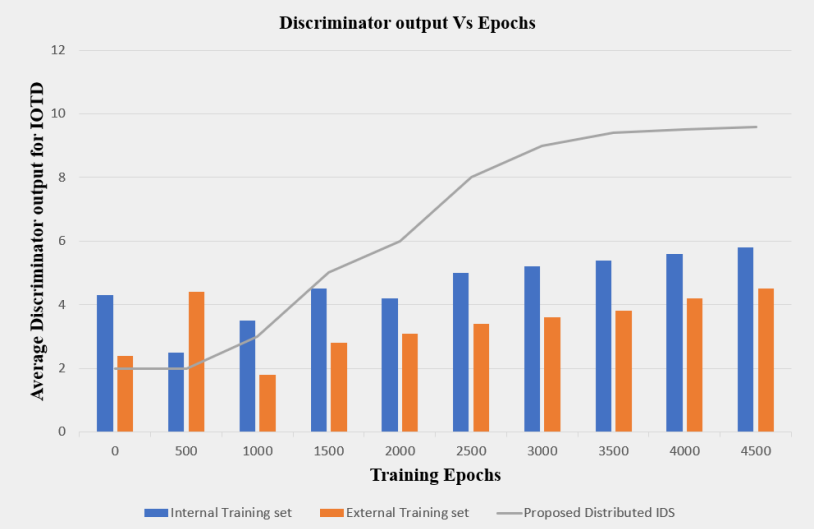

Fig. 3 Discriminator output Vs Training Epochs

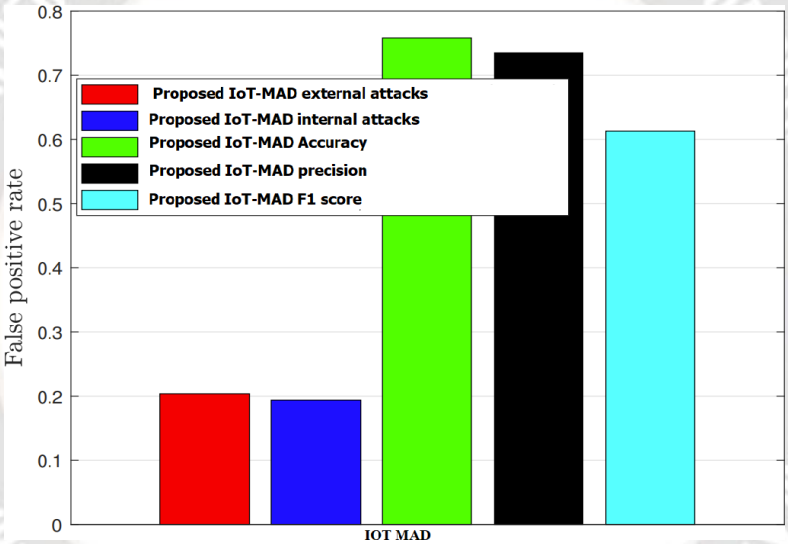

Fig. 4 FPR of IOTDs

The Fig 3. shows the Discriminator output and MAD IoTDs perfor- mance. The result is based on the average discriminator output vs training epochs. We compared them on basis of internal, external and proposed distributed intrusion/ malicious measures attacks observed using NSLKDD dataset. The complete environment of the this work is compared with AI (Artificial Intelligence)-IoT(Internet of Things) parameters on GAN models.

The Fig 4. shows the FPR (False Positive Rate) (eq 8, eq 9, eq 10) of IoTDs on basis of external and internal attacks, also observed their accuracy, precision (eq 11) and F1 score (eq 13). We have generated this using NSLKDD dataset. We also evaluated the internal and external attacks using Precision score, Recall score and F1 score.

Table .2 shows the comparative analysis of previous models from [8], [9], [10], [11], [12] , [13], [14], [15], [16], [17] addressing in terms of Light weight, IoT Environment and AI capability. We compared this models with our proposed model IoT-GAN-MAD and found that our model is good in terms of Light Weight, IoT Environment and AI capability. Table .3 gives the comparison of existing and proposed work accuracy results. Here, our model IOT-GAN- MAD scores the highest accuracy. Table .4 gives the comparison of datasets on existing and proposed models. Our model IOT-GAN-MAD scores the highest accuracy on Real time online dataset under 4500 training Epochs. From the Table 1, Table .2 and Table .3, we conclude that our model IOT-GAN-MAD is capable of detecting the attacks like Malicious, Intrusion and Anomalies etc.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

Table 2 AI IoT parameters on GAN model

S.No	Ref. No	Light Weight	IoT Environment	AI Capability
1	[Our Model]	Yes	Yes	Yes
2	[8]	Yes	Yes	No
3	[9]	Yes	Yes	No
4	[10]	No	No	No
5	[11]	No	No	Yes
6	[12]	Yes	No	No
7	[13]	Yes	No	No
8	[14]	No	No	Yes
9	[15]	Yes	No	Yes
10	[16]	No	Yes	Yes
11	[17]	No	Yes	Yes

Table 3 Comparison of Existing and Proposed work

Ref.No	Type of Attacks	Methodology	Accuracy
[1]	FDI, Jamming	Distributed secure	80.4
[2]	Malicious	IoT-Malicious insider	82.6
[3]	Malicious	Probabilistic evaluation	83.4
[4]	Network Intrusion	GAN-LSTM-DNN	84.1
[5]	Anomaly detection	AD-CGAN	85.2
[16]	Anomaly detection	IOT-GAN	85.6
[17]	GAN Attacks	Deep Learning-IoT	86.3
[18]	Reliable routing	Deep Learning-SVM	88.4
Our model	Anomaly	IOT-GAN-MAD	90.5
Our model	Malicious	IOT-GAN-MAD	91.2
Our model	Intrusion	IOT-GAN-MAD	93.5
Our model	GAN Attacks	IOT-GAN-MAD	95.4

5 Conclusion

In this paper the main intention of introducing the GAN-based IDS (Intrusion Detection) or MAD(Malicious Attack Detection) is that, it can recognize IoT interruptions without relying on a single focus. Each IoTD is able to monitor both its own data and the data of its neighbors, allowing for the detection of both internal and external attacks. Additionally, because the proposed dis- tributed GAN-MADs do not necessitate the sharing of datasets among IoTDs, they can be incorporated into IoTs that safeguard user data, such as financial applications or health monitoring systems. Analytically, we have demonstrated that the proposed distributed MADs outperform standalone MADs that only have access to a single MADs' dataset. The proposed distributed GAN-based MADs outperform a standalone MADs by as much as percent average discrim- inator output for IoT Devices shown in Fig 3. The FPR vs

IoT Devices also mentioned in in Fig 4 in terms of accuracy, precision, and false positive rate when simulated with a real-world daily activity recognition dataset. We also addressed the analysis of previous models and our model shown Table 1, Tabl 2 and Table 3. Our model can also works on detecting the intrusions for future works using IoT-GAN-IDS (Intrusion Detecting System).

Table 4 Comparison of Existing and Proposed work on Datasets

Ref.No	Type of Dataset	Training Epochs	Accuracy
[1]	KDD, Time series	4500	75.4
[2]	KDD99	4500	78.7
[3]	KDD	4500	80.4
[4]	KDD, Time series	4500	82.7
[5]	KDD	4500	84.6
[16]	KDD99,KDD	4500	87.8
[17]	NSL, Time series	4500	88.3
[18]	NSL, KDD99	4500	90.4
Our model	NSL-KDD,Time series	4500	95.5
Our model	Real Time online data	4500	96.2

Declarations

- No Funding
- No Conflict of interest/Competing interests
- Ethics approval - yes

References

[1] Yanpeng Guan ”Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks”, IEEE Transactions on Signal and Information Processing over Networks, Volume: 4, Issue: 1, March 2018.

[2] Ahmed Yar Khan ”Malicious Insider Attack Detection in IoTs Using Data Analytics”, IEEE Access, Volume 8, 2020.

[3] Zhihai Yang ”Probabilistic Inference and Trustworthiness Evaluation of Associative Links Toward Malicious Attack Detection for Online Recom- mendations”, IEEE Transactions on Dependable and Secure Computing Volume: 19, Issue: 2, 01 March-April 2022.

[4] Taehoon Kim and Wooguil Pak ”Early Detection of Network Intrusions Using a GAN-Based One-Class Classifier”, IEEE Access, Volume 10, 2022.

[5] Okwudili M.Ezeme ”Design and Development of AD-CGAN: Conditional Generative Adversarial Networks for Anomaly Detection”, IEEE Access, Volume 8, 2020.

[6] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley,S. Ozair, A. Courville, and Y. Bengio, “Generative adversarial nets,” in Advances in Neural Information Processing Systems 27, 2014, pp. 2672–2680.

[7] Nikos Fotiou ”Capabilities-based access control for IoT devices using Verifiable Credentials”, https://iot-ngin.eu/index.php/publications/.

[8] F. Kammüller, “Isabelle modelchecking for insider threats,” in Data Pri- vacy Management and Security Assurance. New York, NY, USA: Springer,2016, pp. 196–210.

[9] F. Kammüller, J. R. Nurse, and C. W. Probst, “Attack tree analysis for insider threats on the IoT using isabelle,” in Proc. Int. Conf. Hum. Aspects Inf. Secur., Privacy, Trust. New York, NY, USA: Springer, 2016,pp. 234–246.

[10] J. R. Nurse, A. Erola, I. Agrafiotis, M. Goldsmith, and S. Creese, “Smart insiders: Exploring the threat from insiders using the Internet-of-Things,” in Proc. Int. Workshop Secure Internet Things (SIoT), Sep. 2015, pp. 5–14.

[11] I. Palomares, H. Kalutarage, Y. Huang, P. M.

R. McCausland, and G. McWilliams, "A fuzzy multicriteria aggregation method for data analytics: Application to insider threat monitoring," in Proc. 17th World Congr. Int. Fuzzy Syst. Assoc. 9th Int. Conf. Soft Comput. Intell. Syst. (IFSA-SCIS), Jun. 2017, pp. 1–6.

[12] O. Lo, W. J. Buchanan, P. Griffiths, and R. Macfarlane, "Distance mea- surement methods for improved insider threat detection," Secur. Commun. Netw., vol. 2018, Jan. 2018, Art. no. 5906368.

[13] P. A. Legg, O. Buckley, M. Goldsmith, and S. Creese, "Automated insider threat detection system using user and role-based profile assessment," IEEE Syst. J., vol. 11, no. 2, pp. 503–512, 2015.

[14] B. Böse, B. Avasarala, S. Tirthapura, Y.-Y. Chung, and D. Steiner, "Detecting insider threats using radish: A system for real-time anomaly detection in heterogeneous data streams," IEEE Syst. J., vol. 11, no. 2, pp. 471–482, Jan. 2017.

[15] T. Rashid, I. Agrafiotis, and J. R. Nurse, "A new take on detecting insider threats: Exploring the use of hidden Markov models," in Proc. 8th ACM CCS Int. Workshop Manage. Insider Secur. Threats, 2016, pp. 47–56.

[16] Chen, Xiaofei, et al. "IoT-GAN: Anomaly Detection for Time Series in IoT Based on Generative Adversarial Networks," International Conference on Algorithms and Architectures for Parallel Processing. Springer, Cham, 2021.

[17] Chen, Zhenzhu, et al. "Secure collaborative deep learning against GAN attacks in the internet of things," IEEE Internet of Things Journal 8.7 (2020): 5839-5849.

[18] Nayak, Sharmistha, Nurzaman Ahmed, and Sudip Misra. "Deep learning- based reliable routing attack detection mechanism for industrial Internet of Things." Ad Hoc Networks 123 (2021): 102661.

[19] Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: A survey. "2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). IEEE, 2017.

[20] Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey. "Computer networks 148 (2019): 283-294.

[21] Chhabra, S., Aiden, M.K., Sabharwal, S.M., Al-Asadi, M. (2023). 5G and 6G Technologies for Smart City. In: Ahad, M.A., Casalino, G., Bhushan, B. (eds) Enabling Technologies for Effective Planning and Management in Sustainable Smart Cities. Springer, Cham. https://doi.org/10.1007/978-3- 031-22922-$0_1$4.

[22] M. A. Al-Asadi and S. Tasdem´ır, "Empirical Comparisons for Combining Balancing and Feature Selection Strategies for Characterizing Football Players Using FIFA Video Game System," in IEEE Access, vol. 9, pp. 149266-149286, 2021, doi: 10.1109/ACCESS.2021.3124931.

[23] M. A. Al-Asadi and S. Tasdemır, "Predict the Value of Football Players Using FIFA Video Game Data and Machine Learning Techniques," in IEEE Access, vol. 10, pp. 22631-22645, 2022, doi: 10.1109/ACCESS.2022.3154767.

[24] Chhabra, S., Aiden, M.K., Sabharwal, S.M., Al-Asadi, M. (2023). 5G and 6G Technologies for Smart City. In: Ahad, M.A., Casalino, G., Bhushan, B. (eds) Enabling Technologies for Effective Planning and Management in Sustainable Smart Cities. Springer, Cham. https://doi.org/10.1007/978-3-031-22922-$0_1$4.

[25] Yadav, L., Mitra, M., Kumar, A., Bhushan, B., Al-Asadi, M.A. (2023). Nullifying the Prevalent Threats in IoT Based Applications and Smart Cities Using Blockchain Technology. In: Sharma, D.K., Sharma, R., Jeon, G., Polkowski, Z. (eds) Low Power Architectures for IoT Applications. Springer Tracts in Electrical and Electronics Engineering. Springer, Singapore. https://doi.org/10.1007/978-981-99-0639-$0_1$4.