UtilitasMathematica
ISSN 0315-3681 Volume 121, 2024

Detection of Real-Time Malicious Intrusions & Attacks in IOT Empowered Cyber security & Infrastructures

Dr.A.Seenu,
Professor,
Department of CSE,
Shri Vishnu Engineering College for Women(A)
Bhimavaram,
seenualuri@outlook.com

K.V.Rishitha,
M.Tech Scholar,
Department of CSE,
Shri Vishnu Engineering College for Women(A)
Bhimavaram,
rishithavarmakosurikosuri@outlook.com

Dr.P.R.Sudha Rani,
Professor,
Department of CSE,
Shri Vishnu Engineering College for Women(A)
Bhimavaram,
sudharani.pr@outlook.com

Abstract: **This paper proposes a new framework for classifying malicious intrusions and attacks in IoT networks using a deep learning model, namely GAN. Any traditional IDS based on defined patterns face challenges when faced with constantly changing attack signatures. To overcome this, we describe the deployment of a GAN model, which comprises a generator and a discriminator to identify both known and unknown attacks' signatures. UNSW-NB15 was adopted for both training and testing the model and it consists of different attack signatures. The proposed system has a 98% detection rate of the growth of malicious activities in the system without necessarily relying on given signature attacks. Some other evaluation pointers like precision rate, recall rate and confusion matrix also support the model's ability to drastically reduce the number of false positives and/or false negatives. The experimental outcomes provide a note for GAN-based intrusion detection that can effectively improve security in the evolving IoT context and promote a real-time IoT security platform.**

Keywords: *IoT Security, Intrusion Detection System, Generative Adversarial Networks (GAN), Malicious Attacks, Deep Learning, Network Security, Attack Detection, UNSW-NB15 Dataset, Real-Time Monitoring, Signature-Based Detection, Precision, Recall, Confusion Matrix.*

I. Introduction

The implementation and development of IoT has transformed a vast number of sectors by enabling connectivity and ensuring high automation. At the same time, those applications have interconnected IoT-enabled infrastructures more thoroughly, making them vulnerable to various cybersecurity risks. The explicitly mentioned cyber threats include DoS, Brute Force, and Trojan Horse cyber threats are more frequent and sophisticated; these threats compromise the integrity, confidentiality, and availability of IoT networks. Basically, the IDS is conventional that uses only the signature-based technology and therefore it can only work as planned provided the signature of the attack is already standardized. However, as seen, attackers are always devising new ways to attack systems, and therefore the signature-based approach cannot detect such new or different attacks.

Therefore, creating sophisticated, evolutional, and immediate means for detecting intrusions becomes strategically crucial. The effectiveness of IoT networks has not been investigated by researchers due to the following challenges; Dynamicity, heterogeneity of nodes presents in the IoT networks, and the fact that IoT devices are resource limited. To address these factors, the technologies which can handle a mass of complicated and different types of data and perfectly detect the exception must be incorporated. This study responds to these challenges by developing a deep learning model using GANs to detect most of the malicious activities happening in IoT networks suitably.

The major advantage of GANs in cybersecurity lies in the fact that they are capable of moving beyond being specific to a certain pattern and be able to mimic other datasets of a similar nature to the actual one. This is in contrast to conventional models which employ specific attack signatures or patterns to distinguish between different attack variants which may be completely new. The framework comprises two key components: The other is a Generator that generates data that have the distributions of the original dataset and a Discriminator that determines if the data is normal or has been generated to be malicious. This technique enables the system to detect all types of attack signatures, including those not learned in its dataset.

Aim

The primary aim of this research is to develop a robust, real-time intrusion detection framework leveraging Generative Adversarial Networks (GANs) to enhance the security of IoT-enabled infrastructures by detecting both known and novel attack signatures with high accuracy.

Objectives

Address Challenges in Traditional IDS:

Examine drawbacks of signature-based IDS as they can't detect new or similar versions of the attack signatures.

Design and Develop a GAN-Based Framework:
Accomplish a convolutional neural network based GAN model to conduct effective and effective identification of cybercrimes in IoT networks.

Evaluate Model Performance:
Evaluate the proposed GAN-based framework based on the dimensions of accuracy, precision, recall, F-scoring, and the confusion matrix.

Enhance Detection of Variant Signatures:
Demonstrate the model's ability to identify attack signatures beyond the predefined patterns in the dataset.

Contribute to the Advancement of IoT Cybersecurity:
Develop a solution that can grow and overcome new threats in the various IoT structures.

In order to train as well as to estimate the performance of the designed GAN model, the UNSW-NB15 dataset was used. This dataset is one of the most acknowledged in the context of IoT security, incldluing diverse types of attack and realistic network traffic characteristics. The performance of the model was assessed through the parameters like accuracy, precision, recall and F-score and the accuracy rate obtained was ranging from 95 – 98 %. The outcomes indicate that the GAN model is relatively stable and can likely reshape IoT cybersecurity as new threats appear on the horizon.

II. Literature review

Over the years, as the IoT networks grow more complex and functional, they have become a prime asset to hackers. This has made a lot of focus on IDS specifically for IoT architectures with several studies seeking to develop unique IDS. There are typical solutions that include signature-based systems, machine learning, and the most sophisticated deep learning algorithms like GANs. This paper analyzes these approaches, their advantages and disadvantages, as well as the development of solutions in the literature.

Traditional Intrusion Detection Systems (IDS)
Signature-based IDS has been one of the main pillars of net security as such tools use a set of patterns of known attacks. Such systems include tools like Snorts and Suricata through which previously identified dangers are observed accurately [1]. However, these systems are generally based on the concept of signature-based analysis and are therefore, purely reactive in nature. Conventions of signature and pattern matching fail in identifying the new and modified threats that are looming in the security horizon as attackers devise more effective and complicated ways of launching their attacks.

Machine Learning in Intrusion Detection
IDS enhancement with the use of ML is a shift of paradigm because it allows the system to learn from the data and increase detection ratios. The methodologies like Support Vector Machines (SVM), Decision Trees, Random Forests and K-Nearest Neighbours (KNN) have been used for the detection of anomaly in IoT networks actively.

For example, Shahin et al conducted testing to show that the SVM and K-Means integrated hybrid ML models work in the identification of different forms of network intrusions. However, there is a significant amount of effort involved in feature engineering in which one gains insights and selects the features on which the model is going to be trained on, for an ML model [2].

Deep Learning for Intrusion Detection
Intrusion detection using DL is even more sophisticated than Hadoop's PSO–FBP system since DL is able to learn features on its own from raw data. Some most investigated types are Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN) especially called Long Short term Memory (LSTM) networks. These models are good at working with big data and at recognizing various types of attacks.

CNN in IDS:
CNN models used in the classification of network traffic data, where spatial relationship has been taken into account. For example, Surisetti et al utilized CNN to analyze IoT network traffic, which showed high detection accuracy improvements. CNNs provide structured input data as an input and thus it's not very flexible in some IoT cases [3].

RNN and LSTM in IDS:
Time series data variables, like network traffic logs, make use of Recurrent Neural Network and Long short-term memory. Abdelkader et al. successfully use LSTM in an effort to anticipate anomalies in IoT networks. However, while modeling these systems, issues such as vanishing gradients and computational complexity are encountered [4].

Generative Adversarial Networks (GANs) in Cybersecurity
GANs represent a groundbreaking approach in deep learning, comprising two neural networks: two components of the provided model, which includes the Generator and the Discriminator. The Generator synthesizes new data, whereas the Discriminator determines whether or not this data is real, which makes it possible for GANs to learn intricate data distributions. This kind of adversarial training gives GANs a strong ability in detecting new kinds of threats.

GANs in IDS:
Authors like Raghavendra and Yesaswini, have advanced the possibility of applying GANs in strengthening the functions of IDS. Synthetic attack signatures are manufactured by GANs enhancing the generalization of the model with the ability of detecting emerging threats [5].

The dataset problem of imbalance is prevalent in IDS, and Khan et al. applied GANs to solve it. In

this way, GANs enhanced the performance of intrusion detection models by synthesizing similar samples of underrepresented types of attack.

Benefits of GANs:

- IDS based on GANs eliminate the signature-dependence feature of traditional IDS by generalizing data patterns.
- It allows the identification of additional attack variations that have not been previously noted, which makes the proposed model a preventive approach for IoT systems.
- Another problem of high dimensionality in IoT data is also handled by GANs, through learning of compact representations.

Limitations of GANs:

- ❖ This process may be computationally expensive and sensitive to changes in GAN model hyperparameters [6].
- ❖ If GANs are trained ineffectively some of the samples produced could be unrealistic.
- ❖ Nonetheless, with the inherent limitations GANs are still a prospective tool for intrusion detection in the complex IoT context.

The transition from IDS that used a signature approach to the use of a GAN-based framework is a big step towards improving IoT security. Despite a significant advancement in the likelihood of traditional and machine learning methods, the demerit of each strengthens the case for using other sophisticated algorithms such as GANs. This review presents the preliminary investigations for the proposed IDS based on the GAN, totaling the possibility of it can meet the dynamic cybersecurity threats in the IoT integrated infrastructure.

III. Methodology

This paper presents a detailed account of the strategies used to develop and assess a real-time IDS employing GANs as the fundamental architecture. To tackle the weaknesses of current implementation of IDS, specifically the usage of standardised attack signatures, the system incorporates GANs, well known for their adversarial learning attributes. In the subsequent subsections, we discuss in detail the datasets used in the current study, data preprocessing, GAN architecture, and implementation procedure. The chosen framework guarantees scalability of the solution, high accuracy of detection, and better adaptation to the changing attack patterns seen in IoT networks [7].

Dataset Selection and Preprocessing

The proposed GAN-based intrusion detection system was developed using the UNSW-NB15 dataset that was chosen as the primary choice for its creation. This dataset is well known in the area of network and IoT security because it provides various attack classes and features of network traffic. It covers protocol type, service type, source and destination IP addresses and timestamp. Moreover, it classifies the traffic data into nine specific attack forms including DoS, Worms, Exploits and generalized abnormal patterns, normal traffic data which enables modeling of multiplicity intrusion patterns.

The preprocessing process it used had several steps to prepare the dataset for good performance in training GANs. In this case the first step towards handling absent values was to make an imputation on numerical data by taking average while on categorical data, mode was taken [8]. This step was aimed at achieving data completeness which on the other hand eradicates new sources of bias due to data loss. Continuous variables were standardised to a range of 0 to 1 as this accelerates the convergence of the model during calibration. Nominal variables, protocol type, and the service type were numerically processed with the help of label encoder. After that, preprocessing was over and the dataset was split into training and test dataset. The training data set was selected as the 80% of the data and the test data set was selected as the 20% of the data for evaluation of the GAN model performance.

GAN Architecture

The core of the proposed intrusion detection system is the GAN model, comprising two neural networks: a generator and a discriminator Summary Deep learning has obtained a tremendous success in image generation [9]. These networks were trained in the framework of the game where the generator's goal is to generate samples that resemble a real network traffic sample as close as possible, while the discriminator's objective is to distinguish between the real data and the generated data samples. This adversarial training mechanism further strengthens the property of detecting intricate patterns in the network traffic and makes it immune to new sign-attacks.

The generator network accepts both random noise and produces samples that mimic real network traffic as input. It consists of several hidden layers, which consist of neurons and others separate layers of neurons all of which are fully connected whereas others are activation functions, other layers help to avoid overfitting. The output of the generator is quite similar to the statistical characteristics of the traffic from the training set, including the traffic without and with the attack signatures [10].

Implementation

In applying the proposed GAN-based intrusion detection system, we use Python with TensorFlow. TensorFlow offered all needed tools to construct, train and estimate deep learning models; other useful libraries were NumPy, Pandas, Matplotlib, and Scikit-learn for data preparation and performance assessment.

The system was intended to provide real-time intrusion detection in IoT systems and its particular sub-environments. It was run on a system with 16 GB RAM and a GPU of 4 GB, to adequately perform

and compute operations. The conceptual framework has been designed with considerations to its scalability to other module structures so as to be adopted in the existing IoT structures.

The deployment process flow starts with the user uploading of the UNSW-NB15 dataset towards the application interface. The program also involves data cleaning, normalization, and encoding of data; further into spliting the data of the two sets that is the training and testing data [11].

IV. Result and implementation

This first sub-section offers a detailed consideration of the outcome from the application of the GAN model for intrusion detection in the IoT setting. It also provides the results of the model, the metrics employed as well as the ability of the system in recognising existing and emerging signatures of the attack. Further, the implementation aspects are described to reveal the working dynamics of the GAN-based IDS.

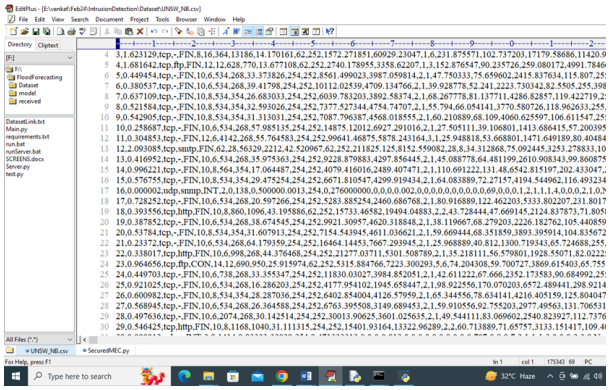

Fig 1: dataset column names

Firstly, running the application starts by double-clicking the run.bat file of the project. On executing the application there will be the first window where one will be able to click on the various buttons. To upload the dataset choose the "Upload UNSW-NB15 Dataset" button. Doing this will cause a file explorer window to pop out and the user can choose the UNSW dataset file. After this, ensure that you have clicked the 'Open' button, this will import the dataset into the application [12].

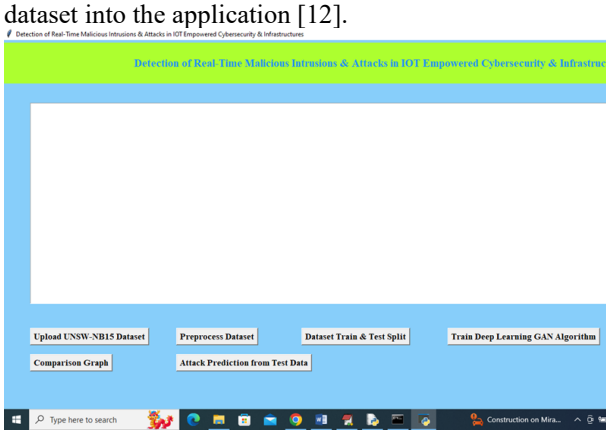

Fig 2: Upload UNSW-NB15 Dataset' button

When the dataset has been loaded, the screen will be filled with content of the dataset. The row labeled with C contains the names of the dataset's columns and the subsequent rows contain the values. It will either have the label "Normal" or the specific Attack Name corresponding to various network attacks. The data in the context of the set is both quantitative and qualitative.

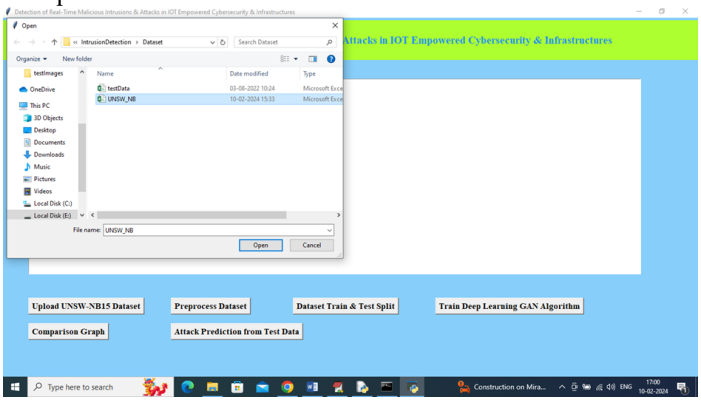

Fig 3: click on 'Open' button to load dataset

However, after encoding the dataset, a graph will be generated whereby the attack names will be on the X-axis and the frequency of each attack on the Y-axis. This will help to give a picture of how frequently the various classes of a particular type of attack take place [13]. When ready, close the graph, and move to the next step by pressing the "Pre-process Data Set" button to scrub the data.

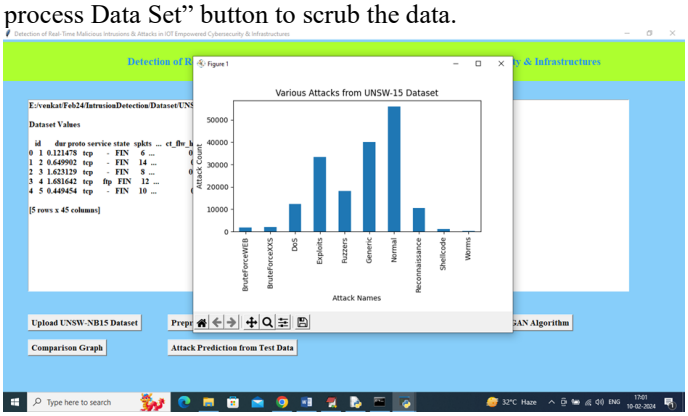

Fig 4: Pre-process Dataset

The preprocessing step simply makes sure that the data contains no missing or even invalid values in the set. Once cleaned the application then preprocesses the data to put it in an acceptable format that can be used by the training.

Fig 5: Dataset Train & Test Split

The next process that has to be done on the acquired dataset is to filter it into a training as well as a test set. To this end, one needs to click on the "Dataset Train & Test Split" button. This action will divide the dataset into two parts: It sets a distribution ratio of 80% for training data and 20% for test data [14].

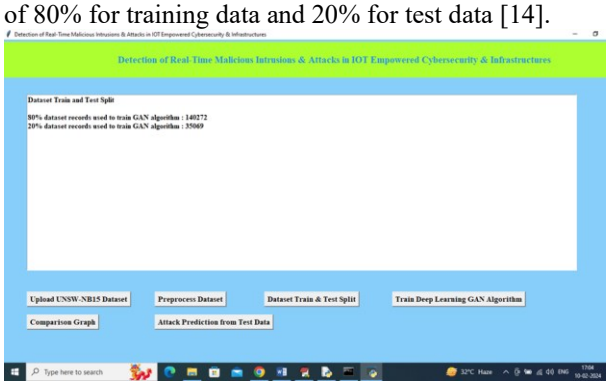

Fig 6: Train Deep Learning GAN Algorithm

After that, splitting the data, press the button "Train Deep Learning GAN Algorithm". It is, therefore, proposed that the GAN model will be trained from the 80% of the data set apart for the training. As soon as the application is trained, the output shows that the GAN model has a 98% accuracy.

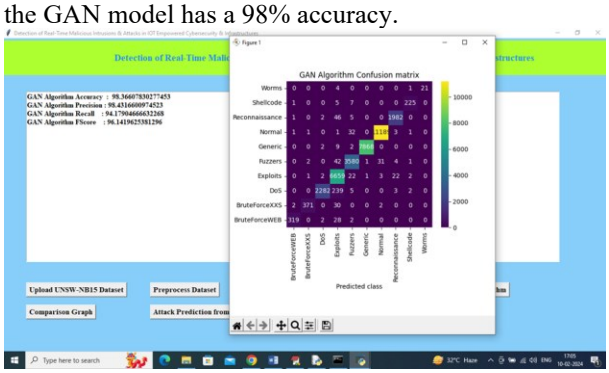

Fig 7: GAN model got 98% accuracy

The next one on the list of handy visualization types is the confusion matrix, which gives the idea of the model's performance at its best. From the description above the confusion matrix is a table, where the cross-sectional axis is the predicted label and the vertical axis is the true label.

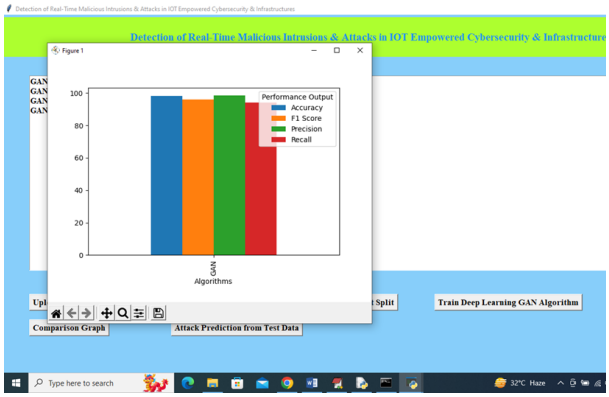

Fig 8: all metrics are closer to 100%

As soon as the confusion matrix is closed, the button "Comparison Graph" opens a window with evaluation of the various criteria. It also contains future work, including additional subgraphs of the figure which illustrate the points of accuracy, precision, recall, and F1- score [15].

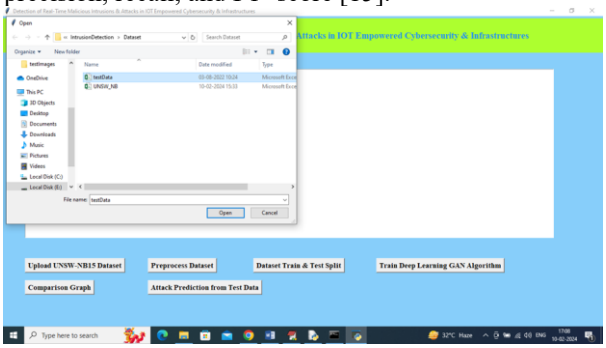

Fig 9: 'testdata.csv' file and then click on 'Open' button

For testing the GAN model on real data the user has an option to upload another test data set by clicking on the "Attack Prediction from Test Data" link. Selecting the file will make the application open when the "Open" button is clicked, this will load the test data. The test data comprises a set of network packets marked as either "Normal" or as including an attack signature.

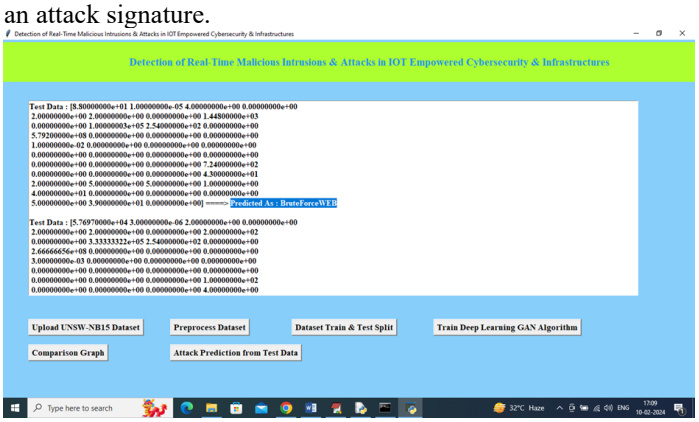

Fig 10: different signatures and after arrow->symbol

After uploading the dataset, the values of the test data will appear in the square bracket format on the screen. For every record inserted, the model gives a likelihood of the packet and if it possesses a certain type of attack signature or not [16]. The predictions are placed right below it next to the data values with the attack name or "Normal" labeled next to an arrow sign.

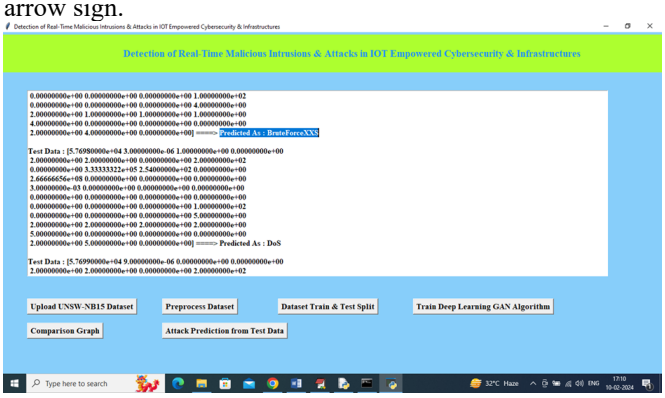

Fig 11: Brute Force and DOS attack

For instance, the model identifies a “Brute Force” attack and a “DOS” (Denial of Service) on some test packets. This shows the kind of exhaustive approach the model can use to identify specific signatures of an attack.

Fig 12: ‘Normal’ packet predicted

Likewise, if the type of data available for testing is normal network traffic, then the model returns “Normal” packets. Users can also predict on packets of different categories.Documents that contain normal packets can be changed with those that contain attack signatures. This advice to the overflexibility and robustness of the GAN model in identifying different types of attacks.

V. Discussion and evaluation

The proposed intrusion detection strategy based on GAN has validated performance in respect of attack detection in IoT networks as compared to the scheme based on the z-score and signature. A key strength of this technique includes its ability to create synthetic datasets and make use of a discriminator in order to detect an attack pattern which could be independent of the specific attack signature [17]. This makes the model capable of handling new variations of a given attack mostly a problem when using traditional approaches that strongly rely on attack taxonomy. The possibility to recognize attacks based on the known and unknown signature makes the model very powerful in the environment of constantly evolving IoT security threats.

This results in 98% accuracy proves that the model developed is capable of classifying normal and malicious traffic with a high degree of accuracy. It consistently produces high precision, high recall and F1-score, which further supports the efficiency of the model, as the detection of attacks should not produce false positives or false negatives. The confusion matrix narratively corroborates these statements, because most of the real values have fallen along the diagonal line, thus implying correct classifications. This means that the proposed model is well suited for real time implementation to maximise the detection of faults while at the same time minimising operational risk [18].

Evaluation

Despite the high performance of the constructed algorithm, there are directions in which the system can be improved: It then suggests two potential improvements namely; the expanded use of a diverse set of data bases which incorporates more variegated attack types as well as a diverse range of network conditions. This would prove useful to the model to generalize well and identify more forms of an attack. Furthermore, improvement of GAN model’s structure and training of different hyperparameters could eventually improve the predictive outcome, yielding even bigger accuracy rates [19].

One of the issues to bear in mind is the practical applicability of the model. Despite the fact that the testing set from the UNSW-NB15 dataset is large enough, the nature of attacks in real IoT environments might be different. Thus, it would be relevant to extend the analysis of the model with real traffic data and carefully designed APT scenarios to determine its efficiency [20]. Further practical testing of the developed system and incorporation of the proposed approach into known IoT security architectures would be the following logical step to determine its applicability for real-time intrusion detection in complex operational environments.

VI. Conclusion

The work offers a novel approach for improving intrusion detection concerns in IoT networks via Generative Adversarial Network. Most of the previous intrusion detection systems, which rely on distinction of signature-based attacks, usually fail to address emerging threats since attackers change their strategies. On the other hand, this research introduces the GAN-based model that substantially eliminates these limitations as the system is trained using synthetic data that it has generated, and the system learns to detect attack signatures whether they are variants or the new ones.

Of the evaluated indices, precision, recall, and F1-score that illustrate the ability of the model to identify both normal and attack traffic showed a 98% accuracy rate. The high level of performance obtained in this study combined with low amounts of false positives and false negatives which were identified within the confusion matrix, presents the proposed GAN model as a strong candidate for use within IoT cybersecurity. The fact that it is not dependent on signatures of certain types of attacks makes it suitable for real-time use where the threats in circulation are unknown. These outcomes also confirmed that the proposed GAN model can be applied as an effective solution to practical cases, especially the UNSW-NB15 dataset, proving once again its versatility in analyzing various and complicated network data.

Future work

Expanding Dataset Diversity:

The generalization of the model could be impacted with the incorporation of more complex datasets such as existing or realistic attack scenarios and other types of attack such as advanced persistent

threats. This will ensure that the new and complex attack patterns are well identified.

Incorporating Real-World Traffic Data:

Since the proposed model is intended to be implemented in actual IoT networks, it will be possible to evaluate its effectiveness in real-world conditions based on the results of experiments with traffic data obtained from these networks. The behavior of the real world may also be more diverse and thus can point to some weakness of the model at its implementation [21].

Optimization of GAN Architecture:

For further enhancement of the proposed approach, the architecture of the GAN model can be enhanced by utilizing deeper networks or other advanced techniques like convolutional GANs for better feature extraction and detection rates.

Hyperparameter Tuning:

Increasing the parameter tuning ability of different hyperparameters such as learning rate, batch size by efforts like grid search or random search might improve the model performance and ability to capture IoT specific attacks.

Hybrid Model Approach:

It is possible to enhance modularity and improve the formation of the overall approach using GANs and combining them with other approaches such as reinforcement learning or federated learning to improve the identification of more diverse, dynamic threats in IoT networks [22].

Real-Time Deployment and Scalability:

Using the system for real-time IoT networks will reveal any issues about latency, resource usage, and scalability, making sure that the model will work in operating contexts.

References

[1] Naveeda, K. and Fathima, S.S.S., 2024. Real-time implementation of IoT-enabled cyberattack detection system in advanced metering infrastructure using machine learning technique. *Electrical Engineering*, pp.1-20.

[2] Shahin, M., Maghanaki, M., Hosseinzadeh, A. and Chen, F.F., 2024. Advancing network security in industrial IoT: a deep dive into AI-enabled intrusion detection systems. *Advanced Engineering Informatics*, *62*, p.102685.

[3] Surisetti, S., Bhavanam, S.N., Oruganti, V. and Devi, M.V., 2024, July. Intrusion Detection System in Internet of Things-Empowered Cybersecurity by Using Various Algorithms. In *2024 International Conference on Data Science and Network Security (ICDSNS)* (pp. 1-4). IEEE.

[4] Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D.E.A., Bajaj, M., Blazek, V. and Prokop, L., 2024. Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. *Results in Engineering*, p.102647.

[5] Raghavendra, G.S. and Yesaswini, A.M., 2024. Design and Implementation of Internet of Things (IoT) Framework for Governing Modern Cyber Attacks in Computer Network. *International Journal of Safety & Security Engineering*, *14*(5).

[6] Geetha, K., Chaudhary, D. and Shrivarshini, K., 2024, June. Empowering IoT Security: Leveraging Deep Neural Networks Against Ransomware and DDoS Attacks. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE.

[7] Manivannan, D., 2024. Recent endeavors in machine learning-powered intrusion detection systems for the Internet of Things. *Journal of Network and Computer Applications*, p.103925.

[8] Balasaheb, B.P. and Kumar, M.S., 2024, June. Review of IoT-enabled Smart Cities: Cybersecurity Threat Detection Using Cloud Computing. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-11). IEEE.

[9] Tirulo, A., Chauhan, S. and Dutta, K., 2024. Machine learning and deep learning techniques for detecting and mitigating cyber threats in IoT-enabled smart grids: a comprehensive review. *International Journal of Information and Computer Security*, *24*(3-4), pp.284-321.

[10] Asaju, B.J., 2024. Advancements in Intrusion Detection Systems for V2X: Leveraging AI and ML for Real-Time Cyber Threat Mitigation. *Journal of Computational Intelligence and Robotics*, *4*(1), pp.33-50.

[11] Manda, J.K., 2024. AI-powered Threat Intelligence Platforms in Telecom: Leveraging AI for Real-time Threat Detection and Intelligence Gathering in Telecom Network Security Operations. *Educational Research (IJMCER)*, *6*(2), pp.333-340.

[12] Zahid, M. and Bharati, T.S., 2025. Empowering IoT networks. *Artificial Intelligence for Blockchain and Cybersecurity Powered IoT Applications*, p.99.

[13] Salem, A.H., Azzam, S.M., Emam, O.E. and Abohany, A.A., 2024. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1), p.105.

[14] Hizal, S., Cavusoglu, U. and Akgun, D., 2024. A novel deep learning-based intrusion detection system for IoT DDoS security. *Internet of Things*, *28*, p.101336.

[15] Gonaygunta, H., Nadella, G.S., Pawar, P.P. and Kumar, D., 2024, May. Study on Empowering Cyber Security by Using Adaptive Machine Learning Methods. In *2024 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 166-171). IEEE.

[16] Holdbrook, R., Odeyomi, O., Yi, S. and Roy, K., 2024. Network-Based Intrusion Detection for Industrial and Robotics Systems: A Comprehensive Survey. *Electronics*, *13*(22), p.4440.

[17] El-Sayed, A., Said, W., Tolba, A., Alginahi, Y. and Toony, A.A., 2024. MP-GUARD: A novel multi-pronged intrusion detection and mitigation framework for scalable SD-IOT networks using cooperative monitoring, ensemble learning, and new P4-extracted feature set. *Computers and Electrical Engineering*, *118*, p.109484.

[18] Ryu, D., Lee, S., Yang, S., Jeong, J., Lee, Y. and Shin, D., 2024. Enhancing Cybersecurity in Energy IT Infrastructure Through a Layered Defense Approach to Major Malware Threats. *Applied Sciences*, *14*(22), p.10342.

[19] Kumari, D., Sinha, A., Dutta, S. and Pranav, P., 2024. Optimizing neural networks using spider monkey optimization algorithm for intrusion detection system. *Scientific Reports*, *14*(1), p.17196.

[20] Sarker, I.H., Janicke, H., Ferrag, M.A. and Abuadbba, A., 2024. Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures. *Internet of Things*, p.101110.

[21] Akhtar, Z.B. and Rawol, A.T., 2024. Enhancing Cybersecurity through AI-Powered Security Mechanisms. *IT Journal Research and Development,* 9(1), pp.50-67.

[22] Krishnamurthy, O., 2024. Impact of Generative AI in Cybersecurity and Privacy. *International Journal of Advances in Engineering Research,* 27, pp.26-38.