International Journal of Informatics and Computation (IJICOM)
Vol. 5, No.1, August 2023
ISSN: 2685-8711, E-ISSN: 2714-5263 DOI : 10.35842/ijicom

IDS-GAN: Stepping up Intrusion Detection Method using GAN Algorithm

H. Y. Fan[1], Sarah Anjani[2]

Abstract

Many computer network threats cause the security aspect to become the most critical problem. The intrusion detection system is a widely used practical security tool to prevent malicious traffic from penetrating networks and systems. To solve the issue, we construct a novel algorithm using Generative Adversarial Networks (GAN) to address the IDS security problem. In this paper, we propose an intrusion detection model using GAN by analyzing the extracted features of the network. To build our detection model, we collect the dataset, conduct pre-processing, train our model with several hyper-parameters to get the best accuracy, and then test the model using the new data. Based on experimental results, the proposed model can produce a 0.00539 error rate and indicate a more accurate model to detect anomalies in the network traffic.

Keywords

Detection, IDS, Deep Learning, GAN.

1. Introduction

Computer networks have developed rapidly, contributing significantly to social and economic development. This has led to an increasing interest in the security of computer networks. A denial of Service (DoS) attack denies legitimate users' resources on a network by producing unwanted traffic. An IDS is a detection system put in place to monitor computer networks. IDS monitors the activities of computer and network systems and classifies them as either normal or abnormal—the traditional method of IDS analyzing data patterns to detect threats [1].

IDS is a popular solution to protect systems from malicious attacks. To build IDS protection, it would be necessary to use a class method. It is a process of categorizing objects through knowledge extracted from a data set during a learning step. Data are grouped into homogeneous classes based on the common properties during the detection step. Therefore, classification aims to construct a model that can predict a new object class by taking advantage of existing information [5].

Machine learning is the most popular approach to deal with multiple issues in computer science, including voice, face, image recognition, and cybersecurity research. Two causes hinder the practical application of machine learning to the IDS. Firstly, the required accuracy is high because the false detection risk is very high on IDS. In addition, trends in network traffic subject to IDS change daily, and new attacks continue to be generated [1]. Various communities presented supervised and unsupervised techniques to establish IDS in recent years. Using the learning techniques, IDS can improve its performance by training the model and predicting future attacks [2].

Many scholars explore various machine learning algorithms for building detection techniques. Traditional machine learning, such as Random Forest (RF) can be a practical

[1] **Corresponding Author:** H. Y. Fan, Harbin University of Science & Technology, China (haoyifan@hrbust.edu.cn).
1 H. Y. Fan, Harbin University of Science & Technology, China (haoyifan@hrbust.edu.cn).
2 Sarah Anjani, Universitas Gadjah Mada, Indonesia (sarah.anjani@gmail.com)

solution to construct a detection model. However, conventional ML architecture remains a drawback in the detection accuracy. In addition, deep learning can be a more promising approach to dealing with image recognition, motion analysis, natural language processing, or intrusion detection. It imitates the human brain's thinking and discriminating behavior through many neurons [3].

A study presented an Improved Genetic Algorithm (IGA) to construct a DNN based on inconsistent NIDS. GA is improved through optimization techniques, including Parallel Processing and Fitness Value Hashing to build the model. It proposed a learning technique for interruption detection, called non-symmetric deep auto-encoder (NDAE) for analyzing feature learning. Moreover, the learning classification model utilized a meta-heuristic Ant Lion optimization to reduce the error rate. Nevertheless, DL algorithms such as DNN, CNN, and LSTM take too long to train the model. Therefore, a single machine learning or deep learning algorithm cannot meet the requirements of the modern IDS [4].

Therefore, we propose a novel approach using GAN architecture to detect intrusion on the network by analyzing and extracting features for detecting intrusions and organizing them into regular and anomaly classes. In detecting network intrusion problems, we present several significant contributions to this research, as follows:

1. We introduce a novel technique for detecting intrusion on the network to train the data set and develop a viable model. We use several network intrusion data features on the internet to build our model.
2. We build a model that can detect intrusion into the network. This model can be a solution to distinguish between normal and abnormal networks. This step updates the method that still uses conventional techniques to detect network intrusion.
3. We tested the proposed model to achieve high-accuracy results to detect intrusion on the network quickly and accurately based on features. We set the parameters to achieve the best results to get the best accuracy values.

Organization: The following is a breakdown of the journal's structure: Part II delves further into past findings. Part III discusses the study's issue description. Section IV explains the experimental design, including a feature learning algorithm, a dataset, and preprocessing, while Section V gives the study's findings and extensive analysis. Finally, section VI summarizes the research's unresolved difficulties.

2. Related Works

An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and alerts when such activity is discovered. One significant issue with IDS is that they regularly alert you to false positives. In many cases, false positives are more frequent than actual threats. Various techniques have been proposed to deal with IDS issues in the current years. In today's network, heavy traffic causes significant technical challenges for IDS monitoring and detecting network activities. The incapability of IDS to process the critical, diverse traffic causes the dropping of packets and low detection accuracy. Extensive studies are conducted on the performance of IDS in high-speed networks due to the potential challenges that occur during heavy traffic presented by the various difficulties of packet-capturing systems in high-speed networks, which can be solved using multithreaded architectures. Since the overloading of the IDS misses malicious activities in high-speed networks, the multithreaded architecture optimizes IDS. It maximizes its performance by reducing the overloading of IDS, which decreases packet drop and increases CPU utilization. Moreover, the studies describe that the detection capacity of the IDS will decrease with the increase in the packet drop rate. It depicts that the effectiveness of the IDS will degrade with packet loss [28].

Dozens of works have explored network intrusion detection on the full dataset feature. Network intrusion detection systems use various methods with high-performance results. Previous works discuss ML-IDS based on Machine learning to build binary classification to detect regular or malicious networks such as DoS, U2R, and R2L. IDS can be implemented in many industries including the electrical industry. For instance, IDS is tested on a simulated SCADA testbed to maintain, change, and operate less costly than an actual device network. The attack target is a simple SCADA network consisting of two tanks using Modbus over TCP [17]. Another paper was conducted on multiple feature selection, and dimension reduction approaches to address low detection rates issues and poor generalization capabilities in large network environments [20]. However, there remain shortcomings in classifying significant traffic [16].

IDS generates an alert if there is a deviation between normal and observed behavior. The basic idea of the approach is to detect if a user has abnormal behavior when comparing previous activities. A study proposed a statistical method based on several random variables and analyzed a user's normal behavior. And they calculate the difference between the current and prior behaviors. The IDS is not programmed to recognize specific attacks but to report abnormal activities. They use the profile generated from past events and compare it to the current collector profile. However, this approach can give many false alarms as it might not be able to detect some attacks [25].

Common approaches utilize antivirus, firewalls, and IDS to determine unauthorized system behavior, including internal and external intrusion. Nowadays, researchers are focusing on using technologies like ML and DL to construct IDSs. Famous ML algorithms include KNN, SVM, Decision Tree, and Bayes. DBM, CNN, and LSTM [23]. A study proposed ANN to optimize Network IDS (NIDS) based on Software Defined Network (SDN). The proposed IDS detects DDoS attacks increasing Distributed Denial-of-Service (DRDoS) detection and defense model based on the Deep Forest model (DDDF) [29].

On the other hand, various data mining techniques are proposed to be applied with IDS to find or learn abnormal behavior patterns. IDS scans the network activities and finds malicious activity in the network systems to enhance accuracy and provide better Security and works well in detecting anomaly attacks. Data mining techniques give way to processing, training, and classifying network information through IDS [26].

Deep learning is a growing research area in the current year [32][33][34][35][36]. A paper presented Multi-Layer Perceptron (MLP) to investigate the performances of the adversarial attack algorithms against deep network intrusion detection on the NSL-KDD dataset. The MLP uses two hidden layers, each containing 256 neutrons, and the activation function is the Rectified Linear Unit (ReLU). The author mainly evaluates white-box adversarial attacks' effect on deep MLP architecture using one dataset without specifying defenses. There is still a lack of internal understanding of the deep-learning algorithms that trigger neuron activation. However, mitigation techniques are complicated for IDS to defend against white-box and backdoor adversarial attacks [24].

The current investigation introduced a DNN model for network intrusion detection in software-defined networking from the NSL KDD dataset and achieved a detection rate of 76%. The paper applied Principal Component Analysis (PCA) for the feature transformation of the NSL-KDD dataset. Then, the feature subset obtained from PCA is optimized using the Genetic Algorithm (GA) and PSO algorithms. The optimized features and a Modular Neural Network (MNN) model for network intrusion detection are used. They obtained (DR=98.2%, FAR=1.8%) for GA and (DR=99.4%, FAR=0.6%) for PSO [21].

Another study presented DBN for developing an efficient and flexible intrusion detection system to detect intrusion behaviors. The success of learning algorithms depends on data representation called feature learning, which is a technique to learn the explanatory factors of variation behind the data, combining spectral clustering and deep neural network algorithms. However, these research methods construct their models to learn representations from manually designed traffic features. Not taking advantage of DNN’s ability showed that an improved traffic feature set can obtain a higher detection and

accuracy rate with a lower false rate. However, learning features directly from raw traffic data should be feasible, such as in computer vision and natural language processing [27]. It took more time to detect and alert if there was any abnormality [6].

Therefore, we propose a novel approach using a generative learning model to handle IDS by analyzing the feature dataset and training model. To conduct our experiment, we collected various network intrusion detection features to build our dataset to train our model and to deal with intrusion detection issues.

3. Proposed Method

A. Problem Definitions

This study focuses on IDS based on the dataset's features using GAN. There are features in the dataset, and z is a noise that is randomly generated initially. G (z) means that the generator G tries to learn a distribution P_G from the distribution of noise P_z and make P_G as close as possible to accurate data distribution (P_{data}). Discriminator D tried to identify whether the sample was accurate or not. Adjust G and D until D cannot distinguish between actual and generated data during training. We achieve the optimality of $P_G = P_{data}$ [16]. G tries to confuse D, but D does its best to distinguish between the standard and generated samples, so you can define the objective function for G and D as follows:

$$min_G E_{z\sim p_z}[\log\left(1 - D\left(G(z)\right)\right)] \quad (1)$$

$$max_D E_{x\sim p_{data}}[\log(Dx)] + E_{z\sim p_z}[\log\left(1 - D\left(G(z)\right)\right)] \quad (2)$$

Therefore, GANs can be described as a min-max problem $min_G max_D V(G, D)$ with the value function V(G, D):

$$V(D,G) = E_{x-p_{data}(x)}[logD(x)] + E_{Z-p_{z(z)}}[\log\left(1 - D\left(G(z)\right)\right)] \quad (3)$$

As a result, large images are output when an actual image is inserted, and small values are output when a fake image is inserted. The classification model becomes robust against data transformation by constantly generating synthesized data as the learning continues.

Therefore, this study intends to use the data generation techniques of the GAN model to create datasets that contain highly imbalanced classes and use the datasets for classification after balancing the data.

B. Proposed Method

The proposed GAN is based on the Wasserstein GAN. Generative adversarial networks are based on game theory; by adding a small number of subtle disturbances to the original traffic sample, the attacker tries to trick the discriminator into believing that the model is accurate. The discriminator tries to distinguish between the sample extracted from the original data and the adversarial sample generated by the generator. In the case of gradual convergence, the negative model is as similar as possible to the original piece. To obtain the appropriate adversarial samples, two constraints should be satisfied: one is to maintain the function of the traffic samples, and the other is to be aggressive so that the intrusion detection system will not detect the adversarial examples. Fig. 1 illustrates the overall architecture of the attackman, which mainly consists of three parts: the generator G, the discriminator D, and the intrusion detection system IDS [15].

Firstly, the input of the generator G is the noise sample or the attack sample Z, and the output is the adversarial sample G(z). The adversarial sample G(z) is fed into the discriminator D, distinguishing the generated adversarial sample G(z) from the usual traffic sample X. The goal of D is to encourage that the generated sample is indistinguishable from the representative from its average class. The loss function is LWGAN, representing the difference between predicted and actual labels.

$$L_{WGAN} = E_{x\sim p_r}[D(x)] + E_{z\sim p_g}[1 - D(z)] \qquad (4)$$

where p_r is the distribution of the standard sample, p_g Is the distribution of the generated sample.

Secondly, to evade the attack, the black-box attack is considered. The black-box intrusion detection system IDS input is the adversarial sample G(z). The output result of IDS is fed back to the generator G to help generate more effective negative attack samples. The goal of G is that the discrimination results of the generative adversarial models are the standard samples. The loss function is L_{ids}, which represents the difference between the output detection result and target label t_{adv}.

$$L_{ids} = E_{z-p_g} l_f[IDS(z), t_{adv}] \qquad (5)$$

where t_{adv} represents the target label and l_f Represents the cross-entropy function.

L_{WGAN} is used to encourage the adversarial samples to be similar to the original samples X, and L_{ids} It is used to generate more effective adversarial samples. Finally, by jointly optimizing G and D, the generator and the discriminator are obtained by solving the maximum-minimum game, and then the black-box attack is achieved. The overall objective function is as follows:

$$\min_G \max_D L = L_{WGAN} + \lambda L_{ids} \qquad (6)$$

Where λ ∈ (0, 1) represents the relative importance of the mentioned two loss functions.

4. Experimental Setup

This paper aims to create a detection model based on dataset features to detect network intrusion using the GAN algorithm. Anomaly data samples are taken from standard data using GAN, optimizing the detector and increasing the detection rate when dealing with enemy instances. This method aims to detect disturbances and classify them into existing labels. GAN has mostly found success in the image field. Recently, GAN has made extensions for areas such as Security. The GAN is researching extensively in the security field as a new generator. Detecting invisible threats using a GAN provides a defense mechanism with a more robust way to prepare for future attacks. Due to the high degree of accuracy achieved by the GAN algorithm, it is very suitable for dealing with difficulties in Detection. GANs have great potential for learning to emulate any data distribution and to generate accurate data [9].

A. Dataset

In this experiment, we collect a dataset consisting of datasets in information data about normal and abnormal tissues. We separate the dataset into two parts to create the model, namely the training dataset, to construct or train the model, and the testing dataset to

evaluate our model's performance or the model's accuracy. In this study, we divide the dataset by 80% for training and 20% for testing datasets. Table 1 shows the details of the dataset distribution table in this study as follows:

Table 1. Details distribution of the dataset

Dataset	Sample
Data Training (80%)	20.000
Data Testing (20%)	5.000
Total	**25.000**

B. Pre-processing

In the pre-processing, we perform data processing and filtering by looking at the data type of each variable and checking for NA or empty data. If there is NA data or open data, we eliminate it to obtain cleaner and more efficient data. On the other hand, if there is open data, it is necessary to handle missing values. Then, we undergo vectorization, normalization, missing value handling, and feature extraction. We divide the dataset into training and testing parts in this pre-processing.

5. Result and Analysis

To conduct our experiment, we collect normal and anomalous network data. Fig. 1 depicts a normal dataset and an anomaly dataset. The normal and anomaly network detection graphs display in the range of 40, indicated by the blue line plot.

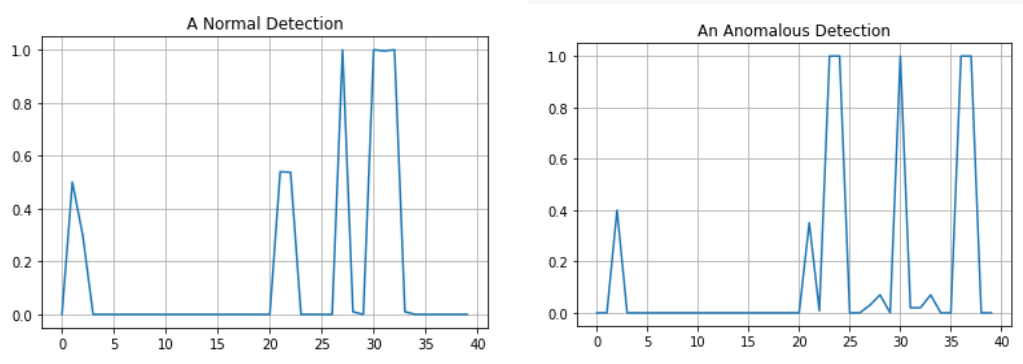

Fig. 1 Intrusion Detection Dataset

To classify normal and anomaly networks, an anomaly label is if the reconstruction error is more significant than one standard deviation from the regular training sample. Our proposed model calculates the regular network from the training set in this process. This model conducts the reconstruction data using the GAN Autoencoder and calculates the reconstruction error in the test phase. Fig.2 shows the regular detection test and anomaly detection test.

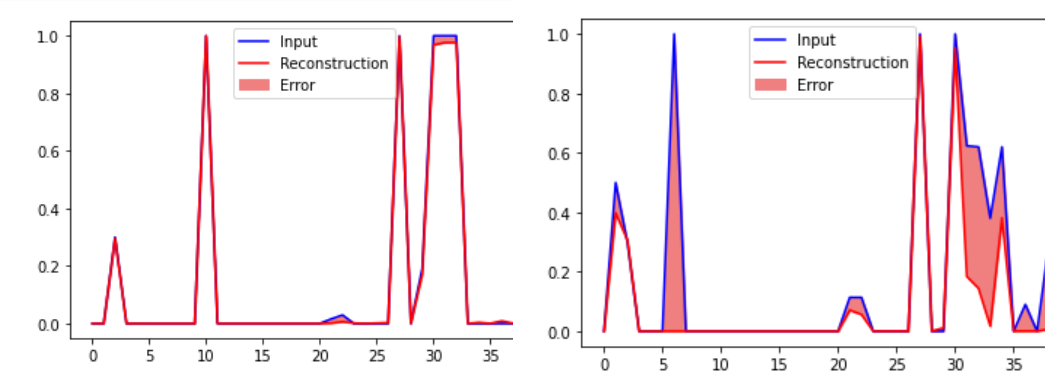

Fig. 2 Normal and anomaly classification test

Fig.2 depicts the standard network test with a low error rate and shows the anomaly network test with a higher error rate. In the testing process, the blue line indicates the input data, the red line describes the reconstruction data, and the thick red line between the blue and red lines presents the error data. We also conduct training and testing models using the samples to construct effective models by training various features of the training dataset and testing the produced model using an unseen dataset to measure the model performance. Fig.3 shows the accuracy and loss in the training and testing process to obtain the model for IDS protection.

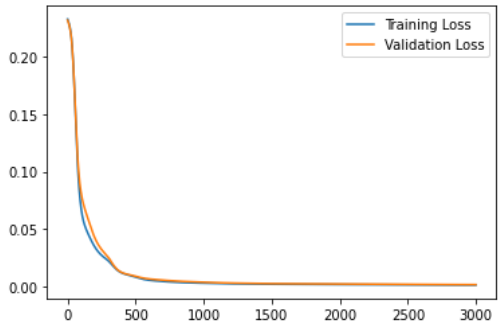

Fig. 3 Training loss and validation loss

In this experiment, we adjust various hyperparameters to get the best network performance. We set epoch = 3,000 and batch size = 512 during the training and testing phase. The blue line plot shows training loss, and the red line shows test loss. We set a high hyperparameter to get a good training model result. The higher the epoch value, the lower the training loss in the training process. Low training loss indicates that the model's performance is getting better.

We analyze the detection results by calculating the threshold to test the detection model. We calculate the threshold value by calculating the sum of the mean values and standard deviation values of the training loss. Our approach achieves a threshold value of 0. 00539. A smaller threshold value indicates a more accurate detection model and a lower error rate. The model detects anomalies by comparing whether the reconstruction loss is higher than a fixed threshold. The model calculates the mean error for the regular sample

from the training set, and then classifies the sample as an anomaly if the reconstruction error is higher than one standard deviation. Therefore, our model can produce more accurate results to solve the anomaly detection problem than the previous traditional detection methods

6. Conclusion

Network security is one of the most critical security issues. However, the vast increase in Internet development lifted the spread of security threats. The traditional method for intrusion detection is no longer sufficient to detect attacks with unexpected patterns. Therefore, the challenge of keeping systems safe from hacking vulnerabilities and attacks should also increase. In this paper, we build a learning model to detect intrusions in the network by analyzing features extracted from network traffic. Based on the experimental result, our detection model can produce a threshold score of 0. 00539. A smaller threshold value indicates a more accurate detection model and a lower error rate. Moreover, the proposed learning methods can quickly detect intrusions to address or prevent these intrusions before they enter and damage the network rather than using traditional statistical techniques. Therefore, the proposed model can be a promising solution to deal with the problem of intrusion on the network.

Acknowledgment

The research was conducted with the Harbin University of Science & Technology support in providing research facilities.

References

[1] K. Hara and K. Shiomoto, "Intrusion Detection System using Semi-Supervised Learning with Adversarial Auto-encoder," NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, pp. 1-8. 2020.

[2] R. Chauhan and S. Shah Heydari, "Polymorphic Adversarial DDoS attack on IDS using GAN," 2020 International Symposium on Networks, Computers, and Communications (ISNCC), pp. 1-6. 2020.

[3] C. Liu, Z. Gu and J. Wang, "A Hybrid Intrusion Detection System Based on Scalable K-Means+ Random Forest and Deep Learning," in IEEE Access, vol. 9, pp. 75729-75740, 2021.

[4] T. Thilagam, R. Aruna, “Intrusion detection for network-based cloud computing by custom RC-NN and optimization”, ICT Express, Vol. 7, Issue 4, pp. 512-520, 2021.

[5] F. Z. Belgrana, N. Benamrane, M. A. Hamaida, A. Mohamed Chaabani and A. Taleb-Ahmed, "Network Intrusion Detection System Using Neural Network and Condensed Nearest Neighbors with Selection of NSL-KDD Influencing Features," 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS), pp. 23-29, 2021.

[6] S. Singh, S. V. Fernandes, V. Padmanabha and P. Rubini, "MCIDS-Multi Classifier Intrusion Detection system for IoT Cyber Attack using Deep Learning algorithm," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), pp. 354-360, 2021.

[7] Haiming Gan, Mingqiang Ou, Fengyi Zhao, Chengguo Xu, Shimei Li, Changxin Chen, Yueju Xue, Automated piglet tracking using a single convolutional neural network, Biosystems Engineering, Volume 205, pp. 48-63, 2021.

[8] Yichiet, A., Khaw, YM.J., Gan, ML. et al. A semantic-aware log generation method for network activities. Int. J. Inf. Secur. 21, pp.161–1772022.
[9] Wijaya, N., Hiswati, M.E. & Anjani, S. DeepIDX: sophisticated IDS model using the generative adversarial network (GAN) algorithm. Iran J Comput Sci 5, pp. 197–204, 2022.
[10] K, Kim." GAN based Augmentation for Improving Anomaly Detection Accuracy in Host-based Intrusion Detection Systems". International Journal of Engineering Research and Technology.2020.
[11] Yan, Q., Wang, M., Huang, W. et al. Automatically synthesizing DoS attack traces using generative adversarial networks. Int. J. Mach. Learn. & Cyber. 10, pp. 3387–3396, 2019.
[12] Yiming, W." A new blind image denoising method based on asymmetric generative adversarial network". IET Image Processing.2021.
[13] P. Freitas de Araujo-Filho, G. Kaddoum, D. R. Campelo, A. Gondim Santos, D. Macêdo and C. Zanchettin, "Intrusion Detection for Cyber–Physical Systems Using Generative Adversarial Networks in Fog Environment," in *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6247-6256, 2021.
[14] L. Qi, L. Wang, J. Huo, Y. Shi, X. Geng and Y. Gao, "Adversarial Camera Alignment Network for Unsupervised Cross-Camera Person Re-Identification," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 32, no. 5, pp. 2921-2936, May 2022
[15] Shuang Zhao, Jing Li, Jianmin Wang, Zhao Zhang, Lin Zhu, Yong Zhang, attackGAN: Adversarial Attack against Black-box IDS using Generative Adversarial Networks, Procedia Computer Science, Volume 187, 2021, Pages 128-133,
[16] Lee, J., Park, K. GAN-based imbalanced data intrusion detection system. Pers Ubiquit Comput 25, 121–128, 2021.
[17] J. Gao et al., "Omni SCADA Intrusion Detection Using Deep Learning Algorithms," in IEEE Internet of Things Journal, vol. 8, no. 2, pp. 951-961, 15 Jan.15, 2021.
[18] A. S. Joshi, A. Dabouei, J. Dawson and N. M. Nasrabadi, "FDeblur-GAN: Fingerprint Deblurring using Generative Adversarial Network," *2021 IEEE International Joint Conference on Biometrics (IJCB)*, 2021, pp. 1-8,
[19] J. Chen, X. Gao, R. Deng, Y. He, C. Fang and P. Cheng, "Generating Adversarial Examples Against Machine Learning-Based Intrusion Detector in Industrial Control Systems," in *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1810-1825, 1 May-June 2022
[20] Lee, J.; Park, K. AE-CGAN Model based High Performance Network Intrusion Detection System. Appl. Sci., 9, pp.4221, 2019.
[21] Elmasry, W." Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic" .2019.
[22] Wisam Elmasry, Akhan Akbulut, Abdul Halim Zaim, Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic, Computer Networks, Vol. 168, 2020, 107042,
[23] Mohandas, V." Detection of blackhole and wormhole attacks in WSN enabled by optimal feature selection using self-adaptive multi-verse optimiser with deep learning".International Journal of Communication Networks and Distributed Systems, Vol. 26, No. 4, 2021.
[24] H. Chaudhary, A. Detroja, P. Prajapati and P. Shah, "A review of various challenges in cybersecurity using Artificial Intelligence," *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, 2020, pp. 829-836
[25] K. Alrawashdeh and S. Goldsmith, "Optimizing Deep Learning Based Intrusion Detection Systems Defense Against White-Box and Backdoor Adversarial Attacks Through a Genetic Algorithm," *2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, 2020, pp. 1-8
[26] P, Wanda. " A Survey of Intrusion Detection System." International Journal of Informatics and Computation, Vol.1, No.1, 1-10, 2019.
[27] K. singh and K. J. Mathai, "Performance Comparison of Intrusion Detection System Between Deep Belief Network (DBN)Algorithm and State Preserving Extreme Learning Machine (SPELM) Algorithm," *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 2019, pp. 1-7.
[28] Sun, P." DL-IDS: Extracting Features Using CNN-LSTM Hybrid Network for Intrusion Detection System" Security and Communication Networks, .2020.
[29] J. E. Varghese and B. Muniyal, "An Efficient IDS Framework for DDoS Attacks in SDN Environment," in *IEEE Access*, vol. 9, pp. 69680-69699, 2021

[30] Kim, J.; Kim, J.; Kim, H.; Shim, M.; Choi, E. CNN-Based Network Intrusion Detection against Denial-of-Service Attacks. Electronics, Vol. 9, pp.916. 2020.
[31] P Wei, Z Zhang, and B. Chen, " A method of eliminating false alarm based on deep learnin" Journal of Physics: Conference Series, Vol. 1087, Issue. 6, 2018.
[32] Wanda P, Jie HJ, DeepProfile: finding fake profile in online social network using dynamic CNN. J Inf Secur Appl 52: 102465.2020.
[33] Wanda P, Marselina Endah H, Jie HJ, DeepOSN: Bringing deep learning as malicious detection scheme in online social network. IAES Int J Artif Intell (IJ-AI) 9(1):146, 2020.
[34] H. J. Jie and P. Wanda, "RunPool: A Dynamic Pooling Layer for Convolution Neural Network," vol. 13, no. 1, pp. 66–76, 2020.
[35] Wanda, P., Jie, H.J. DeepFriend: finding abnormal nodes in online social networks using dynamic deep learning. Soc. Netw. Anal. Min. 11, 34 (2021).
[36] Wanda, P. RunMax: fake profile classification using novel nonlinear activation in CNN. Soc. Netw. Anal. Min. 12, 158 (2022).