Communication Papers of the 18th Conference on Computer Science and Intelligence Systems pp. 223–228
DOI: 10.15439/2023F1425
ISSN 2300-5963 ACSIS, Vol. 37

Efficient Feature Selection On Adversarial Botnet Detection

Farsha Bindu[1], Sheikh Sanjida[2], Nafiza Tabassoum[3], Tamima Binte Wahab [4], Raqeebir Rab[5], and Anonnya Ghosh[6]
[1,2,3,4,5]Department of Computer Science and Engineering
[1,2,3,4,5]Ahsanullah University Of Science and Technology (AUST), Dhaka, Bangladesh
[6]Software Developer, SOFTEKO Bangladesh
Email- farshabindo,sanjidasheikh7,nafisatabassum2016,wahabtamima@gmail.com
raqeebir.cse@aust.edu, 114anonnya@gmail.com

***Abstract*—Botnet attacks now pose a significant hazard to the security and integrity of computer networks and information systems. However, due to technological advancements and the proliferation of malware, machine learning-based Intrusion Detection Systems (IDS) are incapable of protecting against such cyberattacks. IDS cannot detect novel bots because the vast majority of them are programmed systems. Keeping IDS up-to-date with new malware varieties is, therefore, a crucial task. In this paper, we employ Generative Adversarial Networks (GANs) in which two neural networks compete and endeavor to outperform each other, which will serve as self-training for IDS. Our paper's primary objective is to develop an IDS capable of detecting novel malware with fewer attributes in real-time. To accomplish this, we present a method for feature selection that trains GAN models with a minimal subset of features so that the Generator can generate similar false bots with fewer features and the discriminator's ability to identify fake data improves. We used Pearson Correlation, the Wrapper method, and Mutual Information to select the best training model characteristics. The experimental evaluation suggests the GAN model in conjunction with Mutual Information is superior at detecting novel malware.**

***Index Terms*—Generative Adversarial Network, feature selection, Mutual Information, Wrapper Method, CNN**

I. Introduction

CURRENTLY, there is a growing interest in cyber security globally. As technology advances, hackers face new threats and opportunities for criminal activities. As more people, devices, and programs are added to modern business, as well as more data, the majority of which are sensitive or confidential, the significance of cyber security will only increase. This issue is exacerbated by the increase in the quantity and sophistication of hackers' attack methods. In its 2023 Cyber Security Report, the Check Point reflects on the challenging year 2022, when cyberattacks peaked as a result of the Russo-Ukrainian War [1]. A group of Ukrainian hackers has been interfering with Russian web services as a form of retaliation for Russia's invasion of the country. Compared to 2021, cyberattacks worldwide increased by 38 percent by 2022 [3]. We must be aware of the most significant intrusions of the previous year and what we learned from them as we approach 2023. [2]

Every business requires a secure digital infrastructure for conducting transactions. To achieve this goal, network architects and researchers are continuously attempting to create systems that provide impenetrable security for commercial websites. To promote economic growth, prosperity, efficiency, and security, governments must secure global digital infrastructure. With the rise of cyberattacks, machine learning and data mining have become crucial tools for addressing these problems. An anomalous network flow consists of outliers that deviate from typical user traffic patterns. Machine learning and data extraction enable more precise and rapid network traffic detection. They captured the data, analyzed the network flow, and classified the flows for detection purposes. However, data can be abundant, leading to low levels of precision, high computations, overfitting, and other issues. Only the correct selection of features can capture the correct network trace patterns. In other words, the essential characteristics of the network packets must be chosen. Additionally, redundant or irrelevant features must be eliminated.

We use generative adversarial networks (GANs) in this paper to build an adversarial machine learning attack on machine learning or deep learning-based intrusion detection systems (IDSs) when the adversary is uninformed of the ML technique used by the IDS. GANs are a type of generative model that is built on generator networks with recognizable outputs. A generator network and a network of discriminators compete in an interactive environment similar to that of game theory. The discriminator network's goal is to distinguish between samples from the original data and created data, whereas the generator network's goal is to build the best approximation of the training data.

Our contribution is an inclusion-exclusion-based feature selection integrated with Mutual Information (MI) for detecting bots. The objective of the proposed generative adversarial networks (GANs) model is to eliminate insignificant and redundant features as well as improve accuracy in detecting bots. We evaluated a number of feature selection strategies, including Pearson correlation, the wrapper method, and Mutual Information, to determine the optimal solution. Mutual Information combined with the exclusion-inclusion method

Topical area: Network Systems and Applications

demonstrates the optimal solution. In addition, GAN was used to generate false data and evaluate certain features with Convolutional Neural Networks (CNN). The experimental results based on the dataset CSE-CIC-IDS2018 [18] and dataset KDD-99 [16], demonstrate that the GAN model combined with the mutual information selection performs exceptionally well for IDS in detecting novel bots, with an accuracy of 85% and 83%, respectively.

II. Related Works

An intrusion detection system (IDS) is a system that monitors and analyzes data to detect any intrusion in the system or network. As they detect network attacks, intrusion detection systems (IDS) are currently one of the most crucial security solutions. Numerous machine learning and deep learning-based intrusion detection strategies have been proposed over the years [5] [6]. However, the majority of these methods have demonstrated significant false-positive rates and class imbalance problems. Muhammad Usama et al. [8] proposed a generative adversarial network (GAN)-based adversarial machine learning (ML) attack capable of evading an ML-based IDS. They extracted four crucial features necessary for a successful intrusion attack. A GAN framework includes three elements: a generator network, a discriminator network, and a classifier. The IDS model is trained using a generative model against known and unknown adversarial attacks. As evaluation criteria for the evasion assault, they used accuracy, precision, recall, and the F1 score. Among them, the Logistic Regression algorithm had the highest accuracy at 86.64%.

Chuanlong Yin et al. [7] presented the concept of modified GAN for creating false adversarial samples in order to improve the network system's performance in detecting bots. The name of the modified model is BOT-GAN. It is a framework for augmenting botnet detection models with generative adversarial networks, thereby enhancing detection performance and decreasing false positives. It retains the essential features of the original model. However, this paradigm is inefficient because it does not optimize network flow characteristics. The primary objective of this work is to detect novel botnets that are indifferent to network payloads and reduce the false-positive rate. Similarly, Rizwan Hamid et al. [9] proposed a technique called "Botshot" that generates plausible botnet traffic data using GANs to enhance detection. Two GANs (vanilla and conditional) are utilized to generate realistic botnet traffic. Using the classifier two-sample test (C2ST) with a 10-fold cross validation, the effectiveness of the generator is determined. In terms of average accuracy, precision, recall, and F1 score across six distinct ML classifiers, they evaluated the achieved results with benchmark oversampling techniques that included additional botnet traffic data. The showed the using the recall method, and the result was 98.65%. This system will detect a greater number of novel bots, and performance uncertainty will decrease. Francisco Villegas Alejandre et al. [10] proposed a genetic algorithm (GA) and a machine learning algorithm (C4.5), a novel technique for selecting features to detect botnets in their command and control (C&C) phase is presented. Their results demonstrated a reduction in the number of features and an increase in the detection rate. Giovanni Apruzzese et al. [11] proposed research in which they re-trained and re-tested each classifier with feature sets that do not contain the flow duration, sent bytes, received bytes, or exchanged packets, as well as all derived features. Multiple botnet detectors based on distinct machine learning classifiers were utilized. The accuracy increased from 72% to 75% by utilizing multilayer perceptrons and k-nearest neighbors.

So, based on previous research, we can conclude that there have been numerous studies on the performance improvement of IDS with GAN or feature selection separately. However, no work has proposed combining these two approaches for an effective solution for feature selection to detect botnets.

III. Dataset

To evaluate our model, we used two datasets one is known as KDD-99 and the CSE-CIC-IDS2018. KDD-99 has 42 features with binary class levels. The data are divided into two classes: Anomaly (53.1%) and Normal (46.1%). The data distribution of the KDD-99 is shown in Fig.1.

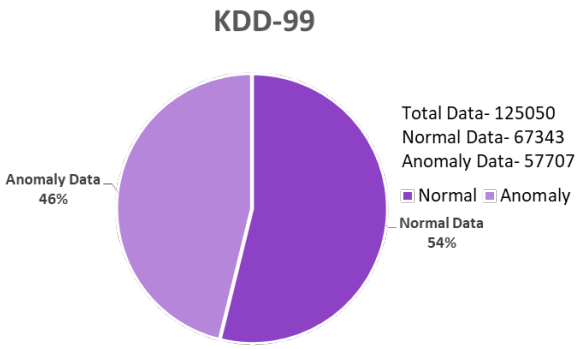

Fig. 1. Data Distribution of KDD-99 dataset

CSE-CIC-IDS2018 dataset contains 80 features for two binary classes. One class is named BOT, whereas another is named as benign. It is an imbalanced dataset. Benign data is 72.7% and Bot data is 27.3%. The data distribution of the CSE-CIC-2018 is shown in Fig.2.
Typically, a network connection consists of two flows, one for the uplink and the other for the downlink. Both the dataset contained the combination of a pair of up-and-down link flows. A short overview of some of the important features of both datasets is given in Table.I and Table.II

IV. Generative Adversarial Networks(GAN)

A generative adversarial network (GAN) is a well-known machine learning model for approaching generative artificial intelligence. In June 2014, Ian Goodfellow and his associates first conceived of the idea [4]. When two neural networks compete against one another in a GAN, a zero-sum game in

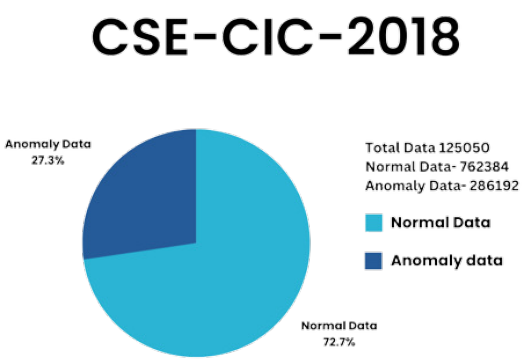

Fig. 2. Data Distribution of CSE-CIC-2018 dataset

TABLE I
DESCRIPTION ABOUT SOME FEATURES OF CIC-IDS2018

Features	Description
Dst Port	Destination port address
Flow Duration	The time elapsed between receiving the first and last packets in the flow
TotLen Fwd Pkts	Total number of forward packets
Fwd Pkt Len	forward packet length
Bwd Pkt Len Max	Maximum backward packet length
Flow Byts/s	Flow-Byte stands for the number of bytes transmit in one flow per second
Flow IAT	IAT is the arrival time difference between two packets. Flow IAT Mean is the average time gap between all sent packets in the flow(18).
Fwd IAT Mean	The average time between two packets sent in the forward packets flow.
Fwd IAT Std	The standard deviation of the time between two packets sent in the forward flow.

TABLE II
DESCRIPTION ABOUT SOME FEATURES OF KDD-99

Features	Description
duration	The length (number of seconds) of the connection
service	The network service on the destination, e.g., http, telnet, etc.
flag	The connection status (normal or problem)
src bytes	Quantity of data bytes transferred from source to destination
dst bytes	Quantity of data bytes from destination to source
wrong fragment	The amount of “wrong” fragments
logged in	1 if successfully logged in; 0 otherwise
is guest login	1 if the If the login is a "guest" login, 1; otherwise, 0.
count	Number of previous connections to the same host as the current connection in the last two seconds
srv count	Number of connections in the last two seconds to the same service as the current connection

which one agent’s gain is another agent’s loss occurs. The GAN training procedure is iterative, with the generator and discriminator networks trained in succession. The overview of the GAN model is shown in Fig. 3. The generator G learns to deceive the discriminator by transforming noise variables z into samples G(z), whereas the discriminator D is trained to maximize the probability of distinguishing between training examples and G(z). Both D and G use the following expression to maximize and minimize V (D, G) in an effort to enhance their learning process.

$$\min \max \text{V(D,G)} = E\_x \sim p\_data(x)[logD(x)] + E\_z \sim p\_z[1 - logD(G(z))]$$

where V (D, G) = binary cross entropy function for binary classification problems, Pdata(x) = real data and Pz(z) = noise variable. [19]

V. DATA PREPROCESSING

The data must be processed prior to being fed into the machine learning models. Regarding the CSE-CIC-IDS2018 dataset for data processing, we initially converted all string-type data into numeric values. To accomplish this, we parsed the object data type into date and time data types of the timestamp feature. Subsequently, we converted the data and

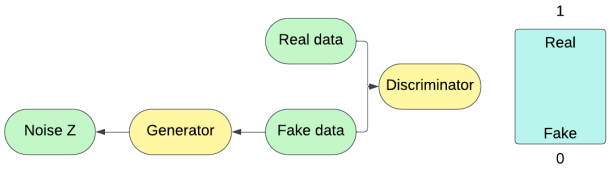

Fig. 3. Architecture of Generative Adversarial Networks

time data types to floats. Then, we normalized the binary label classes to zero and one. Here, Benign is regarded as zero, and Bot as one. (All samples of all features were also converted between 0 and 1). First, we identified constant characteristics, yielding a total of 12 constant characteristics. By eliminating 12 constant characteristics, we were left with 68 of 80 features. Additionally, duplicate attributes were identified. Five pairs of duplicate samples were identified. From each combination, the second characteristic was eliminated. Thus, we selected 63 out of the 68 features. In the final step of data preprocessing, we searched for null values and obtained no results. Then, we cell-transformed our dataset, which resulted in column names being converted to numbers. By completing all of these procedures, we have completed the preprocessing of our dataset. Our dataset was cleansed, normalized, and preprocessed so that our proposed models could be utilized effectively. Fig.4 depicts the data preprocessing processes.

Fig. 4. Data Preprocessing

Second, the KDD-99 dataset contained a single constant feature with no duplicates or missing values. Therefore, one feature was eliminated from the original 42 features, leaving us with 41 features. There were three categorical features in this dataset that were converted to numeric values. Additionally, we changed our class identifiers to 0 and 1. Here, 0 is an anomaly and 1 is normal. Then, we normalized all the values in the range 0 to 1 as a concluding step.

VI. Methodology

The objective of feature selection approaches in machine learning is to identify the optimal set of characteristics that permits the development of efficient models of studied phenomena. To get efficient features we employed three different feature selection methods–Correlation method, Wrapper method, and Mutual information.

A. Correlation method

We used the Pearson feature selection correlation method on our dataset CSE-CIC-IDS2018, to find the best-correlated feature pairs among the 63 features [13]. We took the pairs that had correlated values above 90%. The Pearson feature selection correlation method was used to select the best-correlated feature pairs, resulting in 38 features with 75% discriminator accuracy. To calculate the Pearson correlation coefficient, we take the covariance of the input feature X and output feature Y and divide it by the product of the standard deviation of the two features.

$$\rho X, Y = \frac{\sigma XY}{\sigma X \sigma Y}$$

B. Wrapper method

The feature selection wrapper method was tested on the dataset CSE-CIC-IDS2018 where firstly we did the forward selection method, which works with a p_value. It started with a null model and fitted it with each individual feature one at a time, selecting the feature with the minimum p_value. This process was repeated until the set of selected features had a p_value of individual features less than the significance level. However, 55 features were obtained from 63 using the forward selection, which did not produce the desired feature selection outcome [12]. Backward elimination was used to remove insignificant features from the discriminator model, resulting in 48 features out of 63 with the highest accuracy of 85%, almost the same as the initial accuracy. The same dataset CSE-CIC-IDS2018 was used for this method[12].

C. Exclusion/Inclusion with Mutual_Information

In this research, we present a novel method for selecting features that combine mutual information with feature exclusion and inclusion depending on the accuracy generated by the GAN model. The comprehensive overview of the suggested model is shown in figure5. Algorithm1 of our model are discussed below:

- In the CSE-CIC-IDS2018 dataset, we first applied mutual information (MI). Mutual information basically estimates the information about the amount of data one variable relates to another [14]. This allowed us to select the top 30 features with the highest information dependencies.
- From 30 features we started working top 5 features in the discriminator model which gave us 68% accuracy.
- We then included one-by-one features and checked if the accuracy of the discriminator was increased and continued the inclusion-exclusion process until the accuracy reached the initial accuracy with all 63 features, which was 85%. As a result, we got 20 features with 85% accuracy.

To verify the validity of our model, we used another binary dataset, KDD-99. The final methodology was used for this dataset. We estimated the mutual information of 41 features of this dataset after data preprocessing. The initial accuracy was 83% with 41 features. Then, using mutual information, we selected the top 30 features and started working with the top five features. Then, we included one-by-one features and checked if the accuracy was increased and continued the inclusion-exclusion process until the accuracy reached the initial accuracy with all 41 features, which was 83%. Consequently, we obtained 24 features with 83% accuracy.

Algorithm 1 Feature Selection Algorithm for proposed methodology

Require: Features
Ensure: Feature Set
Initial accuracy is calculated by all features;
FinalFeatureSet ← 5 features;
Accuracy a_m ← Top 5 feature Set;
Set N ← Top features for which accuracy $a_m \approx$ Initial feature;
i=6;
while i=N features of Set **do**
  Calculate accuracy a_i;
  if $a_i \leftarrow > a_m$ **then**
    FinalFeatureSet ← add i feature;
  else {}
    excludeSet ← i feature;
  end if
end while
FinalFeatureSet;

In our proposed algorithm Algorithm. 1 initial accuracy with all the features was calculated in Initial accuracy . Then FinalFeatureSet with the top 5 features, selected from mutual information was declared. Accuracy a_m with these features was calculated. In set N , the Top features with whom accuracy reached equal to the initial accuracy were stored . One by one feature was taken from this set and checked accuracy including or excluding it in the FinalFeatureSet and then it was added to FinalFeatureSet or excluded according to its performance.

D. Evaluating features using GAN

The Generator sub-model of GAN generated false novel data that resembled the original data, which was then optimized using feature selection and sent to the Discriminator sub-model to evaluate the accuracy of each feature. Discriminator made use of the Convolutional Neural Network (CNN). A CNN contains multiple layers, each of which learns to recognize the various characteristics of input data. A filter or kernel is applied to each data layer to generate an output that is progressively more accurate and detailed [15] [19].

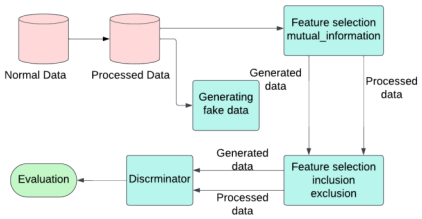

Fig. 5. Proposed Feature Selection Model

VII. Result Analysis

Both datasets were evaluated with the proposed feature selection model. As demonstrated in Table. III Mutual Information Feature Selection in conjunction with exclusion inclusion produces an optimal feature set with the utmost accuracy, comparable to the initial accuracy of all feature sets. The top five features selected by Mutual Information for Dataset CSE-CIC-IDS2018 began with an accuracy of 68%. Using inclusion and exclusion, we subsequently obtained 15 additional features with an initial accuracy of 85%. The same results were obtained for the KDD-99 dataset. The best five features of this dataset had a 56% accuracy rate. Using inclusion and exclusion, we subsequently obtained 19 additional features and attained an accuracy of 83%.

TABLE III
Performance Analysis with GAN

Dataset	**Number of selected features**	**Accuracy before feature selection**	**Accuracy after feature selection using MI with exclusion & inclusion**
CSE-CIC-IDS2018	20 from total 63	85%	85%
KDD-99	24 from total 41	83%	83%

Table IV displays the names of the features with the highest accuracy after exclusion and inclusion with Mutual Information.

A number of researches have been conducted to detect botnets implementing GANs. TableV outlined the comparative analysis of our model with other GAN-based models.

VIII. Conclusion and Future Works

As Internet usage increases, a growing number of threats are posing increasingly severe information security problems. There have been works of feature selection in network anomaly detection [22]. Despite their great potential, few IDS employ a class of algorithms known as generative adversarial networks. Therefore, we propose a GAN-based model capable of detecting novel malware with fewer features and greater accuracy. The maximum accuracy of the few previous studies that used GAN and feature selection was 74% [5]. Using the GAN and the Mutual Information Method, we achieved an accuracy of 85%. In the subsequent phase of our work, we intend to employ multiclass datasets in addition to binary-labeled datasets.

References

[1] Check point, title=Cyber security report 2023, url=https://pages.checkpoint.com/cyber-security-report-2023.html, note=(Date last accessed 27-July-2023)
[2] Michali, title = Biggest Cybersecurity Challenges in 2022, Check Point Software url=https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/biggest-cybersecurity-challenges-in-2022, note=(Date last accessed 27-July-2023)
[3] Jnguyen, title =What is cyber security? the different types of cybersecurity, Check Point Software, url = https://pages.checkpoint.com/cyber-security-report-2023.html, note=(Date last accessed 27-July-2023)

TABLE IV
SELECTED FEATURES OF BOTH DATASETS USING EXCLUSION-INCLUSION WITH MUTUAL INFORMATION

NO	CSE-CIC-IDS2018	KDD-99
1	Dst Port	duration
2	Flow Duration	service
3	TotLen Fwd Pkts	flag
4	Fwd Pkt Len Max	src bytes
5	Fwd Pkt Len Mean	dst bytes
6	Bwd Pkt Len Max	wrong fragment
7	Flow Byts/s	logged in
8	Flow IAT Mean	is guest login
9	Flow IAT Max	count
10	Flow IAT Min	srv count
11	Flow IAT Mean	srv serror rate
12	Fwd IAT Std	rerror rate
13	Bwd PSH Flags	srv rerror rate
14	Fwd Header Len	same srv rate
15	Bwd Header Len	diff srv rate
16	Fwd Pkts/s	dst host count
17	Bwd Pkts/s	dst host srv count
18	RST Flag Cnt	dst host same srv rate
19	Bwd Pkt Len Std	dst host diff srv rate
20	Init Fwd Win Byts	dst host same src port rate
21		dst host srv diff host rate
22		dst host serror rate
23		dst host terror rate
24		dst host srv terror rate

TABLE V
COMPARISON ANALYSIS WITH OTHER WORK

Title	Methodology	Performance
[7]	GAN & Original Features	74%
[11]	GAN & Features Exclusion Based on ML models	75%
This work[18]	GAN, Exclusion inclusion in feature Mutual Information	85%
This Work[16]	GAN, Exclusion inclusion in feature Mutual Information	83%

[4] Goodfellow, Ian, et al. "Generative adversarial nets in advances in neural information processing systems (NIPS)." Curran Associates, Inc. Red Hook, NY, USA (2014): 2672-2680, doi = 10.1145/3422622, https://doi.org/10.1145\%2F3422622,year = 2020

[5] Chih-Fong Tsai and Hsu, Yu-Feng and Lin, Chia-Ying and Lin, Wei-Yang. "Intrusion detection by machine learning: A review." expert systems with applications 36.10 (2009): 11994-12000, https://www.sciencedirect.com/science/article/abs/pii/S0957417409004801, doi = 10.1016/j.eswa.2009.05.029, https://doi.org/10.1016/j.eswa.2009.05.029

[6] Modi, Chirag, et al. "A survey of intrusion detection techniques in cloud." Journal of network and computer applications 36.1 (2013): 42-57, doi = 10.1016/j.jnca.2012.05.003, https://doi.org/10.1016\%2Fj.jnca.2012.05.003,year = 2013.

[7] Yin, Chuanlong, et al. "An enhancing framework for botnet detection using generative adversarial networks." 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD). IEEE, 2018, doi = 10.1109/icaibd.2018.8396200, https://doi.org/10.1109\%2Ficaibd.2018.8396200

[8] Usama, Muhammad, et al. "Generative adversarial networks for launching and thwarting adversarial attacks on network intrusion detection systems." 2019 15th international wireless communications & mobile computing conference (IWCMC). IEEE, 2019, doi = 10.1109/iwcmc.2019.8766353, https://doi.org/10.1109\%2Fiwcmc.2019.8766353

[9] Randhawa, Rizwan Hamid, et al. "Security hardening of botnet detectors using generative adversarial networks." IEEE Access 9 (2021): 78276-78292,doi = 10.1109/access.2021.3083421,https://doi.org/10.1109\%2Faccess.2021.3083421

[10] Alejandre, Francisco Villegas, Nareli Cruz Cortés, and Eleazar Aguirre Anaya. "Feature selection to detect botnets using machine learning algorithms." 2017 International Conference on Electronics, Communications and Computers (CONIELECOMP). IEEE, 2017,doi = 10.1109/conielecomp.2017.7891834, https://doi.org/10.1109\%2Fconielecomp.2017.7891834

[11] Apruzzese, Giovanni, Michele Colajanni, and Mirco Marchetti. "Evaluating the effectiveness of adversarial attacks against botnet detectors." 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA). IEEE, 2019,doi = 10.1109/nca.2019.8935039, https://doi.org/10.1109\%2Fnca.2019.8935039

[12] Vikas Verma, title = A comprehensive guide to Feature Selection using Wrapper methods in Python, url=https://shorturl.at/gnqET, note=(Date last accessed 27-July-2023)

[13] Mehreen Saeed, title= Calculating Pearson Correlation Coefficient in Python with Numpy, url=https://shorturl.at/abfim, note=(Date last accessed 27-July-2023)

[14] Guhanesvar, title= Feature Selection Based on Mutual Information Gain for Classification and Regression, url = https://bit.ly/3ofYzmt note=(Date last accessed 27-July-2023)

[15] IBM — ibm.com, title= What are Convolutional Neural Networks?, url = https://www.ibm.com/topics/convolutional-neural-networks. note=(Date last accessed 27-July-2023)

[16] kDD-99 dataset url = http://kdd.ics.uci.edu/databases/kddcup99/task.html, note=(Date last accessed 27-July-2023)

[17] Choudhary, Sarika, and Nishtha Kesswani. "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT." Procedia Computer Science 167 (2020): 1561-1573., doi = 10.1016/j.procs.2020.03.367, https://doi.org/10.1016\%2Fj.procs.2020.03.367 ,year = 2020.

[18] CSE-CIC-IDS2018 dataset, urlhttps://www.unb.ca/cic/datasets/ids-2018.html?fbclid=IwAR2dCUq0TM0kzlKG6eTX23TkEueKSUwmUh5coYQJidfMLn7rcs-4ICt4Fy8, note=(Date last accessed 27-July-2023),

[19] Zhang, Xiran. "Network intrusion detection using generative adversarial networks." (2020). https://ir.canterbury.ac.nz/bitstream/handle/10092/100016/Zhang,\%20Xiran_Master's\%20Thesis.pdf?isAllowed=y&sequence=1

[20] Paolo Caressa, title=How to build a GAN in Python , url=hhttps://www.codemotion.com/magazine/ai-ml/deep-learning/how-to-build-a-gan-in-python/, note=(Date last accessed 27-July-2023),

[21] K. Cabaj and J. Wytrębowicz, S and Kukliński ,P. Radziszewski and K. Truong Dinh. "SDN Architecture Impact on Network Security" Position papers of the 2014 Federated Conference on Computer Science and Information Systems pp. 143–148,year=2014, doi = 10.15439/2014F473, http://dx.doi.org/10.15439/2014F473

[22] Ghosh, Anonnya and Ibrahim, Hussain Mohammed and Mohammad, Wasif and Nova, Farhana Chowdhury and Hasan, Amit and Rab, Raqeebir. "CoWrap: An Approach of Feature Selection for Network Anomaly Detection" In: Barolli, L., Hussain, F., Enokido, T. (eds) Advanced Information Networking and Applications. AINA 2022. Lecture Notes in Networks and Systems, vol 450. Springer, Cham., year=2022, doi = 10.1007/9783030995874_47