EFFICIENT DETECTION OF DOS ATTACK USING FUZZY ANN

[1] Ankita Mahadik, [2] Rohini Bhosale, [3] Dr. Ashok Kanthe
[1] Lecturer, [2] Assistant Professor, [3] Professor
Department of Information Technology
Pillai HOC College of Engineering and Technology, Rasayani

***Abstract* – It has been evident in the vast majority of applications on the internet platform that there has been a significant growth in the number of users as well as the data generated. This large amount of data has been difficult to analyze and process effectively which has led to the creation of the cloud platforms and big data approaches. This also increases the incidents of DoS attacksoversuch data storage platforms and networks that support such large systems.DoS attacks can cripple the systems and prevent legitimate users from accessing the services. Unauthorized access is also highly detrimental to the approach as it introduces a lot of security concerns for the users. Therefore, this publication aims to provide a better solution to this problem through the utilization of machine learning approaches that can accurately identify the intrusions in the network for Denial of Service attacks. The proposed methodology utilizes K means clustering, along with the Fuzzy Artificial Neural Networks (ANN) on the KDD dataset to achieve highly accurate intrusion detection technique. The technique has been tested extensively to illustrate its superiority compared to the some of the past approaches towards intrusion detection to measure the exactness of the model in the constrained environment.**

Keywords: - *DoS, KDD Dataset, K-Means Clustering,Fuzzy ANN, Threshold Normalization.*

I. INTRODUCTION

Cyber-attacks are any type of objectionable action that preys on computer infrastructures, networks information systems, or personal computer systems utilizing diverse techniques to destroy, steal, or alter the data or the system. There are various ways to compromise the security of a particular computer system. People with malicious intent will always find a way to gain unauthorized access to computer systems to carry out their nefarious tasks.

Some attackers wouldn't want to steal data, but incapacitate the resources of a system so that it is unable to respond to genuine service requests. Such a type of attack is known as DDoS, which stands for Denial of Service attack. This attack is of no benefit for the attacker as it does not steal or manipulates any data. The only satisfaction is that the website or service ceases to operate as such a high load is being generated and eventually shutdown.

Majority of the DoS attacks the attacker wants certain data or wants to modify certain data stored in a location closely guarded and allows only authorized personnel to access it. Such as sensitive data from a government website, or a banking website to steal account details of people. The attackers come with an objective of harm, most of them use malware to affect the target computer and gain access to areas restricted to professionals and attempt to steal data for sale or utilization for their benefit. Most attackers resort to locking down the device unless the owner pays certain ransom money to gain access to their computer devices.

Cyber-attacks are quite a lot in number and variety too, a one-stop solution to all of the attacks is not an easy task. There are two distinctive types of attacks, passive attacks are the ones where the malicious software hibernates until it encounters vulnerability and that is when it attacks. Whereas, active attacks are where the attack is performed with an intention and a plan to target an already discovered weakness in the system, such as DDoS attacks.

A network attack is an attack on the network infrastructure by an infiltrator that would first analyze the network and collect information to look for vulnerabilities to exploit. Once the vulnerability is found, the attacker launches its attack. The attacksespecially the DoS attacks that cripples the service provider and crashes the website or it would utilize social engineering to gain access to confidential information. To overcome such network-based attacks, the providers need to bake in DoS protection and make the networks resilient enough to phishing attacks. There is also a need to develop strong passwords that help in immensely reducing the chances of a DoS attack.

The researchers explore the possibilities of pre-empting cyber-attacks with the help of Extreme Values. The researchers explain the ability to understand the extent of prediction and its perspective. As this problem didn't receive much attention before the researchers have proposed a technique that involves the use of grey-box prediction which favors the use of statistical phenomenon shown by the data for prediction.

Some system introduces an innovative technique of the utilization of grey-box models in conjunction with Long-Range Dependence. This methodology can predict the number of attacks per unit of time. This can be done about an hour in advance with an average certainty of about 10.2%-82.1%.

The data can be used to predict the nature and possibility of an attack by applying it to the proposed framework. The technique utilizes the recent concept of mathematics called a stochastic cyber-attack process to extract the semantic data related to the attack. This allows for the detection of an intrusion effectively and allows for a course to prevent such actions in the future. This can be done by the implementation of effective machine learning approaches that can be utilized to perform fast and efficient detection of the intrusion. For the purpose of clustering the data the use of the K means clustering algorithm has been utilized.

The K Means clustering approach is one of the most common approaches towards the implementation of efficient clustering of the data. The K means clustering approach utilizes a random K number of clusters around a calculated centroid. The centroid is achieved through the extensive process of evaluation of the attributes and parameters that are selected for the effective implementation of the clustering mechanism. It is an iterative algorithm that performs a collection of steps repeatedly to achieve the effective clustering of the data. The data points in the dataset are assigned together based on their similarities and the centroid calculation does not change and the K number of clusters is achieved. It is one of the most efficient approaches towards clustering in this methodology.

The Fuzzy Artificial Network is one of the most innovative concepts that combine the Artificial Neural Networks along with the Fuzzy Inference system that produces a highly specialized and efficient algorithm. ANN is one of the most powerful algorithms that utilize the natural processing power of the organic human brain. It is a computational network that models the nervous system of a human being to be able to do complex calculations and interpretations. The neurons created in this approach of Fuzzy ANN utilize the Fuzzy system for the boundary conditions that allow for the finer control over the prediction accuracy of the proposed system for Intrusion detection.

Section 2 of this research article describean analytical survey of some past research works. Section 3 describes the steps that are carried in the proposed model.The obtained results are evaluated in the section 4 and finally this research article is concluded along with the traces of the future work extension possibilities insection 5.

II. LITERATURE REVIEW

This section of the literature survey eventually reveals some facts based on thoughtful analysis of many authors work as follows.

J. Jiao et.al in [1] The DDoS attacks are a type of denial of service attacks that can cripple a datacenter by leveraging TCP traffic and can be very complicated to analyze and predict. Therefore, the authors in this approach design an innovative DDoS detection technique based on the TCP on the datacenters. The experimental results conclude a very high level of accuracy. The main drawback of the proposed techniques is that it has only been implemented in a simulation environment.

Kansalet.al in [2] There are a lot of different security concerns that should be taken into consideration for various services being offered online. The online platform has been growing considerably in the past few years and so have the attacks been increasing steadily in recent years. The most common type of attack on the different services being offered online is the DDoS attacks [2]. These attacks have been very disastrous to the web service provider as it can do a lot of damage to the bandwidth and the other resources of the system. Most of the time these attacks have been done by insiders that can launch this attack easily. Therefore, the proposed methodology in this paper outlines an innovative technique to mitigate insider DDoS attacks by using attack proxies to identify the attacker.

Daveet.al in [3] The various cyber-attacks that have been happening over the internet platform. The others state that there has been an increase in the number of DOS attacks or distributed denial of service attacks that have been shutting down a lot of services over the internet. The denial of service attacks is difficult to identify and can be highly disruptive in their methods and prevent legitimate users from accessing the service. Therefore, the authors in this publication outline a novel concept that provides early detection and isolation policy to prevent such attacks. The proposed methodology is useful as it does not overload and balances the load of the proxies.

Somaniet.al in [4] There has been a significant rise in the number of cyber threats that have been utilizing different types of attack vectors for their nefarious purposes. This increase in cyber-attacks has also been highly detrimental to the cloud platform and the various cloud services that have been offered by such organizations [4]. Therefore, to provide a solution to this problem the authors in this paper propose a scale Inside Out approach which reduces the utilization of resources during a DDOS attack. The presented technique has been experimentally evaluated and showed that it can achieve a very high accuracy of about 95% in the detection of the DOS attacks.

Nijimet.al in [5] The cybersecurity platform as one of the most important aspects of security which can and be considered on terms with the government and International Security. This is due to the fact that cybersecurity is inherently licked with governments and other private sectors and the compromised nature of these platforms can lead to an overall increase in the incidents of national importance [5]. Most of these attacks are in the form of DOS attacks that can cripple even one of the biggest Infrastructures and organizations. Therefore, the authors in this paper revised an innovative technique to combat and prevent such DDOS attacks through the use of a data mining engine called fast to detect.

Vishwakarmaet.al in [6] There has been tremendous growth in various platforms and services on the Internet paradigm. The services have been increasingly important for enabling convenience and ease of use for the different users on the Internet platform. The Rise of the internet of things

platform has also increased the security concerns related to such a platform [6]. These are the biggest attacks on these platforms are the DDOS attacks which are very difficult to combat. Therefore, the authors in this paper provide an efficient technique for the detection of dos attacks through the use of machine learning and the honeypot approach.

Bhosaleet.al in [7] Ever since the introduction of the platform various innovative services have been offered for increased convenience of the users on the internet. This includes the cloud platform and where is other Web Services utilize the internet for providing such services to the users. Due to the increase of such services being offered online increasing amount of traffic has been generated which leads to a lot of attackers moving their bases online. The most used attack vectors are the DDOS attack which can completely cripple a data center and bring it to its knees. Therefore, the authors in this paper provide a novel prevention mechanism for the DOS attacks on the application layer [7]. This technique is a very different approach that has been successfully discussed by the authors in this Publication.

Sukumaret.al in [8] The internet platform is being widely used for a lot of purposes by increasing the number of individuals across the globe. This has been instrumental in bringing about technological advancements and scientific breakthroughs through the use of this innovative platform [8]. The one side effect of such a large-scale growth of the internet has been the consistent increase in the number of intrusions and network intrusion on this platform. Therefore, to provide a solution to this problem the authors in this paper provide an innovative intrusion detection system that utilizes the k-means algorithm along with an improved genetic algorithm.

Xiaofenget.al in [9] There have been increasing amounts of traffic load tests on the Internet platform due to the significant increase in the affordability of the internet across the world. This leads to a large number of users utilizing the platform which also increases the number of malicious attackers that tried to perform intrusion attacks on the network [9]. This is a highly difficult debilitating technique utilizing the DOS attacks to cripple an online system. Thus, to prevent such attacks the authors in this paper have devised an innovative technique for intrusion detection through the use of support vector machines. The main drawback of the proposed methodology is that the authors have not improved the algorithm to suit this use case.

Chenet.al in [10] The widespread use of the internet platform in various different fields and applications across different use cases. The increased dependence of the internet platform has caused a lot of useful services to be dependent on the Internet platform significantly. Platforms such as Healthcare have been using this infrastructure to implement network control systems into their hospitals [10]. They have been a significant increase in the number of dos attacks that are used to jamming these networked control systems. Therefore, the authors in this paper have provided in augmented fancy technique for the tracking of these dos jamming attacks.

Alheetiet.al in [11] The various uses of the internet platform that is nothing but a wired network of interconnected computers as big as the whole planet. This interconnected network has been responsible for implementing a large number of services that have been utilizing by the various users for a long time. This is led to a number of problems such as dos attacks that have been used to prevent legitimate users accessing the platform [11]. This has become an increasing problem in-vehicle networks of self-driving cars that can be highly susceptible to these attacks. Therefore, the authors in this application provide an innovative technique for the production of dos attacks utilizing of fuzzy Petri net model.

Anet.al in [12] The use of the internet platform for a large number of innovative approaches that would not have been possible without the creation of this massive framework. This includes the paradigm of Cyber-physical systems that have been deployed on this internet framework. The cyber-physical systems large scale systems that are complex and interconnected for providing communication capabilities [12]. computational resources and physical process integration for various fields and purposes. Most of the systems are highly critical and are subject to do intermittent dos attacks that can cripple such a system. Therefore, the authors in this paper propose a fuzzy secure control that can provide security in such systems against the intermittent dos attacks.

Hosseinpouret.al in [13] The internet platform has received a lot of potentials that have been utilized through various researchers that have been performed for implementing innovative and useful features into this platform. One such feature is the VOIP feature or the voice over internet protocol. This protocol allows for sending your voice over the internet platform for cheap and high-quality calls [13]. These protocols are not highly secure and are subject to a number of dos attacks. Therefore, to prevent any intrusion on these VOIP systems the author has implemented a Fuzzy Logic technique. The major limitation of the proposed methodology is the authors have not optimized the Fuzzy system to increase the accuracy.

Aravindet.al in [14] The growth of the internet has had its pros and cons. On one hand, it has been one of the most useful to that has enabled a lot of technological advancements. On the other hand, it has introduced a lot of malicious users that are determined to cause a lot of harm to legitimate users on the platform [14]. These activities reduce the security of the internet as an Intruder gains a lot of access to the various personal data of the users. Therefore, to prevent such a situation the authors in this paper have defined an introduction detection system that detects a large number of attacks including dos attacks through the use of ensemble classifiers and K means clustering.

Hasnatet.al in [15] The growth of the internet platform has included a lot of different Infrastructures that are connected in a network for the purpose of achieving communication. This allows the power grids to be interconnected with a communication system that allows

information flow to the system for the purpose of Management and enabling control mechanisms. Some of the individuals with malicious intent have known to perform dos attacks on such systems which can be highly replying to the power service of the area. Therefore, to prevent attacks on such systems the authors in this Publication utilize state correlations for dynamic state estimation and prevention of the DOS attacks.

Problem statement

The above section has been utilized for the purpose of surveying the traditional researches in the DoS attack detection. The survey has indicated that most of the approaches have not been up to the mark where there were limitations in the accuracy and complexity of the approach. Therefore, the proposed methodology overcomes this problem by implementing a deep learning neural network approach that achieves significant improvement in the accuracy. The methodology also utilizes a large dataset for the execution unlike most of the techniques outlined in the literature survey.

III. PROPOSED METHODOLOGY

The proposed methodology for efficient detection of DoS attack in the network is depicted in the above figure 1. The steps that are involved in the construction of the system is broadly defined in the below mentioned points.

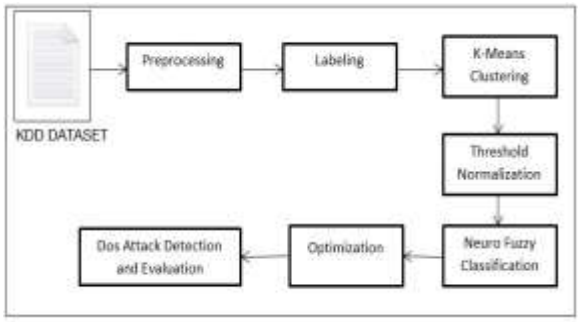

Figure 1: Proposed System for Dos Attack Detection and Evaluation

Step 1: Dataset Collection and Preprocessing– This is a preliminary step of the proposed model. To test our proposed model, we are using KDD99 dataset[16].

Knowledge Discovery and Data mining competition (KDD)is a renowned source of Dataset all around the world for the researchers in the network intrusion paradigm. This Dataset is well prepared for the network intrusion detection system where each packet of data is described with its 43 attributes as shown in the table of the next segment of this research article.

Step 2: K-Means Clustering- The size of the preprocessed list and then the packets that are reasoned for the DoS Attack based on their attack attributes are counted. If the counted numbers of packets are more than 15% of the total packets, then the system is assumed to evaluate the DoS attack in depth. Hence the system is tending to cluster the data based on the K-Means clustering algorithm.

From the preprocessed list three important entities like network packet serial number, attribute and type are added into a list to form a double dimensional list, which is then labeled to feed to K- means clustering algorithm. This can be described with the following five steps.

Distance Evaluation- Here each row of the double dimension list subjected to evaluate the distance using the Euclidean equation between all other rows for the entities like packet attributes and type. The evaluated distance averaged to get a mean distance for that row to call it as Row distance RD.This row distance is appended at the end of the each of the rows to form a distance list. And then the Average of the all the row distances forms to get the Average Euclidean distance of the whole input list. This distance evaluation is done based on the below mentioned equation 1 and 2.

$$\boldsymbol{RD = \sqrt{(x1 - x2)^2 + (y1 - y2)^2}} \_\_\_\_\_ \quad (1)$$

$$A_{ED} = \sum_{k=0}^{n} RD \_\_\_\_\_ \quad (2)$$

Where,
RD- Euclidean distance of a specific row.
x1, x2, y1, and y2 are the labeled value of attribute and type
A_{ED} = Average Euclidean Distance
n= Number of Rows

Sorting-The obtained distance list is sorted based on the Row distance of each row using the Bubble sort technique. This makes the each of the similar row to come together to form the higher quality of the cluster.

Data Point selection–K Number of random numbers are selected in between the 1 to 100. These random numbers are aggregated to the size of the list to the obtain K number of Data points.

Centroid Selection- The Row distance at each data point form the centroid of the proposed model, these centroids is then stored in a list to call it as centroid list.

Cluster formation - Here for each of the centroid a cluster boundary is evaluated. This can be done by subtracting and adding the Average distance A_D to each of the row distance R_D. This process yields the lower and upper boundary of the cluster with respect to the row distance. These boundaries are made to accept the respective rows based on the row distance to yield the fine grained clusters.

Step 3: T-Normalization and Neuro Fuzzy – This is the most important step of the proposed model, where the key and value pair for Neuro fuzzy attributes are stored in a map object. These attributes and their values are like noofTimes=10,connectionstatus=S,loginAccess=1,durationofconnection=10,service=htt,src_bytes=10 and dst_bytes=10.

Then for each of the rows of the preprocessed list the map object is analyzed to match the key value of that row. If the key values are matched, then a status is set as “YES” else status is set as “NO”. If the status is “YES” then this indicates the probability of the presence of the Dos Attack attribute.

Then this attribute is verified by taking the 41st attribute of the row of the preprocessed list and then it is matched with the random Dos Attribute list which was stored in a config file of the proposed system. By doing this all the packets that are responsible for the Dos attack are segregated for the set Threshold status of "YES". This process can be illustrated in the below mentioned algorithm 1.

ALGORITHM 1: Threshold Normalization

```
//Input : Preprocessed List PL ,Map List ML
// Input: DOS attributes List DL
//Output: Dos Count DS
1: Start
2:      DS = 0
3:  for i=0 to Size of PL
4:      set STATUS=NO
5:  for j=0 to Size of ML
6:          RL = ML [j]
7:          KEY=RL[0]
8:          VALUE=RL[1]
9:          ATVAL=PL[i]+KEY
10: if( ATVAL=VALUE),then
11:           STATUS=YES
12:           break
13: end if
14: if (STATUS=YES), then
15:          TMPLST=PL[i]
16:          ATR=TMPLST[41]
17:  if(ATR ∈ DL), then
18:          DS ++
19: end if
20: end if
21: end for
22:  end for
23: return DS
24: Stop
```

After the Threshold normalization the selected DoS attack prone packets are subject to estimate the score of the threat type. Then the count and score attributes are listed to form a double dimension list of two columns for the attributes count and score respectively with N number of rows. This list is known as the neuron input list.

This Neuron input list is used to estimate the Hidden layer and the output layer to predict the possibility of the DOS attack prone packets. Using the values of count and score attributes two targets values are decided as Target1 and Target2.

After the estimation of the target values 10 random weight values are estimated which are in the ranges of 0 and 1 for the values of the Fuzzy crisp sets. The Fuzzy Crisp set is divided to form the crisp values like VERY LOW, LOW, MEDIUM, HIGH and VERY HIGH to for the random weights.

These random weights are labeled as W1,W2,W3,W4,W5,W6,W7,W8,B1,B2. Here B1 and B2 are the bias values which are used to stabilize the neurons. Then by using the Equation 2 and 3 for Hidden layer and Activation function Output layers are estimated using the algorithm 2. The obtained output layers, and then aggregated with the target values to achieve the new prediction list of DoS attack prone packet list.

$$X= (AT1* W1) +(AT2*W2) +B1 \quad \text{_____ (3)}$$

$$H_{LV}= \frac{1}{(1+\exp(-X)} \quad \text{_____ (4)}$$

Where AT1 is the count and AT2 is the score. Then the sigmoid function is given by Equation 4 of the neural network.

ALGORITHM 2: Neuron prediction List

```
//Input : Neuron input List NL
//Input:        {     W1,W2,W3,W4,W5,W6,W7,W8,B1,B2}
Random Weights
// Output :  Prediciton List PL
1: Start
2:   for i=0 to Size of NL
3:        TL= Ø [TL = Temporary List]
4:                RL= NL [i]
5:        AT1 = RL[0] , AT2 = RL[1]
6:         X1= (AT1* W1) +(AT2*W2) +B1
7:         X2= (AT1* W3) +(AT2*W4) +B1
8:         HLV1= 1/ (1+EXP^(-X1))
9:         HLV2= 1/ (1+EXP^(-X2))
10:          Y1= (HLV1* W5) +( HLV1*W6) +B2
11:          Y2= (HLV2* W7) +( HLV2*W8) +B2
12:          OL1= 1/ (1+EXP^(-Y1))
13:          OL2= 1/ (1+EXP^(-Y2))
14:          PS= T1 ⇒ OL1 +T2 ⇒ OL1
15:          TL[0]=AT1 , TL[1]=AT2 , TL[2]=PS
16:         PL = PL + TL
17:  end for
18:   return PL
19: Stop
```

Step 4: Optimization and Dos Attack Detection- Here in the process of optimization different attributes that can catalyze the DoS attack are added into the Prediction list. Different attributes are like apche2, back, buffer overflow, file write and guess password etc.,. After adding these parameters the obtained prediction list is filtered out for these parameters to provide the best possible output of the DoS attack prone packet list as the outcome of the proposed model.

duration	su_attempted	same_srv_rate
protocol_type	num_root	diff_srv_rate
service	num_file_creations	srv_diff_host_rate
flag	num_shells	dst_host_count
src_bytes	num_access_files	dst_host_srv_count
dst_bytes	num_outbound_cmds	dst_host_same_srv_rate
land	is_host_login	dst_host_diff_srv_rate
wrong_fragment	is_guest_login	dst_host_same_src_port_rate
urgent	count	dst_host_srv_diff_host_rate
hot	srv_count	dst_host_serror_rate
num_failed_logins	serror_rate	dst_host_srv_serror_rate
logged_in	srv_serror_rate	dst_host_rerror_rate
num_compromised	rerror_rate	dst_host_srv_rerror_rate
root_shell	srv_rerror_rate	

This model is extensively evaluated using the techniques that are mentioned in the next segment of this research article.

IV RESULT AND DISCUSSIONS

The proposed methodology for the Intrusion Detection system through the utilization of the K means clustering along with Fuzzy ANN is coded in the java programming language through the utilization of the NetBeans Integrated Development Environment. The presented technique is implemented on a development machine consisting of an Intel Core i5 processor achieving the processing requirements supplemented by 500GB of Hard drive and 4GB of RAM. The dataset collected for this purpose is known as the KDD or Knowledge Discovery in Database. This is an extensive dataset with the required attributes that are elaborated in further detail.

Knowledge Discovery dataset

The KDD dataset utilized in this approach has been generated through the use of the TCP raw dump data that has been generated over the course of 9 weeks through a Local Area Network. The KDD dataset consists of an excess of 50 lakh connection records that are recorded over a set time period for the purpose of identification and testing of the intrusion detection systems. The Dataset consists of a large number of attributes that can be analyzed for the incidence of any intrusion performed by an attacker. There are a variety of attacks that are performed in the dataset that have been instrumental in achieving the Intrusion detection.

The types of attacks performed in the dataset among which DoS attacks have also been performed through syn flooding which denies the service to the legitimate users through the flooding mechanism. These attacks have been well documented in this KDD dataset utilized for this Intrusion detection approach.

The attacks performed in this dataset are hidden in the various attributed of the connection records. The connection records have a large list of attributes that describe the different types of attacks through the use of labels. These labels are assigned to each of the connections describing it as a normal connection or an attack type such as, back, buffer_overflow, ftp_write, guess_passwd, imap and many more.

The various different attributes that are detailed in the dataset along with their type are given as follows,

Table 1: Attribute lists of KDD Cup Dataset

These attributes are analyzed by the approach stipulated in this publication based on Fuzzy ANN through the use of extensive experimentation and comparison to the conventional approaches that utilize the CRF or the Conditional Random Field approach. The precision, recall, and accuracy approach has been utilized for achieving the performance evaluation of the proposed methodology.

Precision, Recall, and Accuracy – The precision, recall, and accuracy performance metrics are one of the most accurate markers of performance that can allow for an in-depth assessment of the proposed system. The parameters are explained mathematically in the equations given below.

Precision = TP/(TP+FP)

Recall = TP/(TP+FN)

Accuracy = (TP+TN)/(TP+FP+FN+TN)

Where,

TP = True Positive
TN = True Negative
FP = False Positive
FN = False Negative

The Fuzzy Neuro approach in the proposed methodology has been contrasted with the performance metrics of the CRF approach. For the purpose of the evaluation a total of 11850 packets have been processed, out of which the 1998 K means DoS packets have been generated, along with 362 T-norm and Fuzzy Logic DoS packets which result in the creation of the 359 optimization packets. The resultant packets are utilized to generate the values of True Positive, True Negative, False Positive, and False Negative values for the respective approaches.

The values obtained by the Neuro-Fuzzy approach and the CRF are tabulated in table 2 below. The tabulated values indicate that the TP and TN values for the Neuro are higher than the CRF along with the FP and FN which are lower than the CRF values plotted in the graph given in figure 2 below which indicates a higher accuracy attained by the Neuro-Fuzzy approach.

Parameters	CRF	Neuro Fuzzy
True Positive	5	362
True Neagtive	8902	9146
False Positive	244	0
False Negative	2699	2342

Table 2: CRF Vs Neuro-Fuzzy comparison

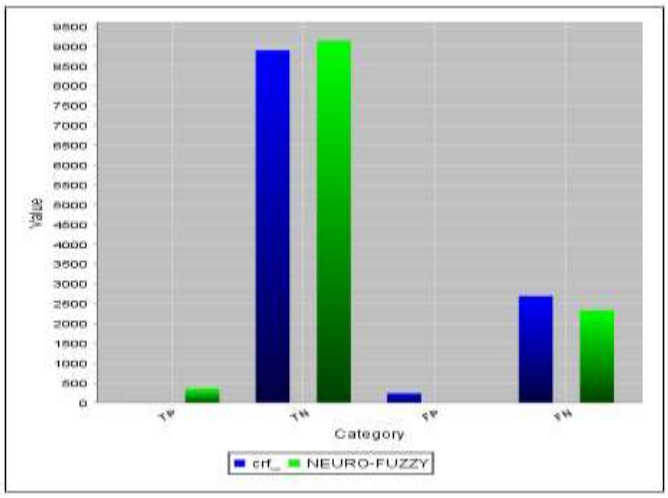

Figure 2: CRF Vs Neuro-Fuzzy Graphical representation

The Naive Bayes approach has also been tested in comparison to the proposed methodology and the values attained are contrasted in Table 3 given below. The comparison of the techniques has indicated that the neuro-fuzzy approach is significantly better than the Naïve Bayes approach which is evident by the graph plotted in Figure 3.

Parameters	Naïve Bayes	Neuro Fuzzy
True Positive	128	362
True Neagtive	6766	9146
False Positive	244	0
False Negative	3141	2342

Table 3: Naive Bayes Vs Neuro Fuzzy comparison

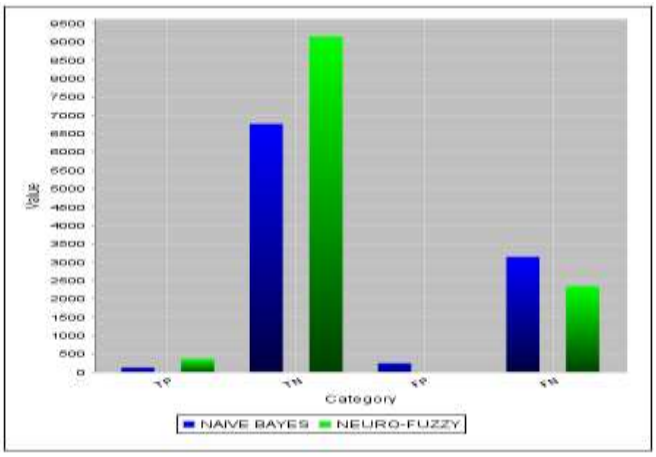

Figure 3: Naive Bayes Vs Neuro-Fuzzy graphical representation

The K Means clustering approach has also been contrasted with the Neuro-fuzzy technique and their findings are detailed in table 4 and the bar graph in figure 4 below. It is evident that the Neuro-Fuzzy methodology performs with great accuracy.

Parameters	K Means	Neuro Fuzzy
True Positive	200	362
True Neagtive	7389	9146
False Positive	244	0
False Negative	3037	2342

Table 4:K means Clustering Vs Neuro-Fuzzy comparison

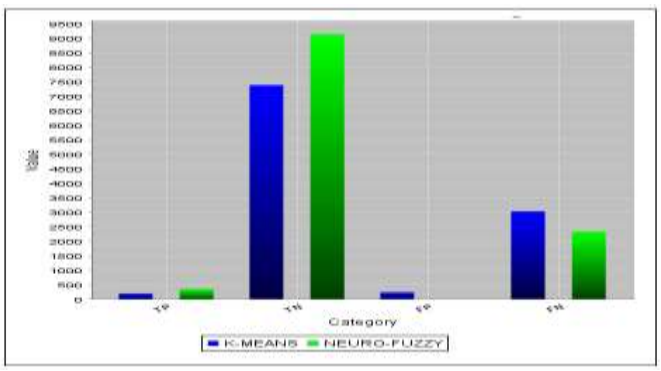

Figure 4: K means Clustering Vs Neuro-Fuzzy graphical representation

The final values of Precision, Recall, and Accuracy attained by the CRF and the optimization performed are tabulated in table 5 given below. The values indicate the increased accuracy attained by the methodology proposed in this paper. The results illustrate the superiority and the increased accuracy achieved by the Neuro-fuzzy approach.

Sr NO	Test Outcome	CRF	Neuro_Fuzzy Optimization
1	FP_Rate	0.02667833	0
2	TP_Rate	0.00184911	0.13387574
3	Precision	0.02008032	1
4	Recall	0.00184911	0.13387574
5	Accuracy	0.75164557	0.802362869

Table 5: Precision-Recall and Accuracy values comparison.

V CONCLUSION AND FUTURE SCOPE

The presented technique for DoS attack detectionthat has been detailed in this publication requires the implementation of software interfaces for achieving the prescribed goals of this research. There has been a large collection of technologies that have been utilized to illustrate the execution of the Intrusion detection system but the vast predominant of the approaches have been not been able to accomplish the high level of accuracy attained in this publication. Therefore, the proposed methodology in this paper leverages the Neuro-Fuzzy platform for expediting highly accurate intrusion detection through the assistance of the K means clustering and Threshold Normalization. The proposed methodology achieves intrusion detection through the KDD or Knowledge Discovery Dataset. The extensive experimentation for the recognition of the errors in the methodology through the use of Precision, Recall, and Accuracy illustrates that the detection system attains significant enhancements in the accuracy of Intrusion detection.

For Future Research direction, the proposed system can be further improved by utilizing more parameters which can increase the accuracy further. And also, the intrusion detection can be implemented in the real time devices like servers, router etc.

REFERENCES

[1] J. Jiao,Benjun Ye, Yue Zhao, Rebecca J. Stones, Gang Wang, Xiaoguang Liu,Shaoyan Wang andGuangjun Wei, “Detecting TCP-based DDoS Attacks in Baidu Cloud Computing Data Centers”, IEEE 36th Symposium on Reliable Distributed Systems, 2017.

[1] Jiao, Jiahui, Benjun Ye, Yue Zhao, Rebecca J. Stones, Gang Wang, Xiaoguang Liu, Shaoyan Wang, and GuangjunXie. "Detecting TCP-based DDoS attacks in Baidu cloud computing data centers." In *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, pp. 256-258. IEEE, 2017.

[2] Kansal, Vaishali, and Mayank Dave. "DDoS attack isolation using moving target defense." In *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 511-514. IEEE, 2017.

[3] Vaishali Kansal and Mayank Dave, "Proactive DDoS Attack Detection and Isolation", International Conference on Computer, Communications and Electronics (Comptelix), 2017.

[4] Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti andMuttukrishnanRajarajan, "Scale Inside-out: Rapid Mitigation of Cloud DDoS Attacks", IEEETransactions on Dependable and Secure Computing, 2017.

[5] MaisNijim, Hisham Albataineh, Mohammad Shoeb KhanAndDeepak Rao, "FastDetict: A Data Mining Engine for Predicting and Preventing DDoS Attacks", IEEE, 2017.

[6] R. Vishwakarma and Ankit Kumar Jain, "A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks", Proceedings of the Third International Conference on Trends in Electronics and Informatics, ICOEI, 2019.

[7] K. Bhosale,Maria Nenovaand Georgi Iliev, "The Distributed Denial of Service Attacks (DDoS) Prevention Mechanisms on Application Layer", European Union, Telsiks, 2017.

[8] A. Sukumar,I Pranav, MM Neetishand Jayasree Narayanan, "Network Intrusion Detection Using Improved Genetic k-means Algorithm", International Conference on Advances in Computing, Communications, and Informatics (ICACCI), 2018.

[9] Z. Xiaofengand Hao Xiaohong, "Research on Intrusion Detection Based on Improved Combination of K-means and Multi-level SVM", 17th IEEE International Conference on Communication Technology, 2017.

[10] X. Chen,Songlin Hu, "Event-based output tracking control for networked T-S fuzzy systems under non-periodic DoS jamming attacks", Australian & New Zealand Control Conference (ANZCC), 2018.

[11] K. Alheeti,Anna Gruebler, Klaus D. McDonald-Maier and Anil Fernando, "Prediction of DoS Attacks in External Communication for Self-driving Vehicles Using A Fuzzy Petri Net Model", IEEE International Conference on Consumer Electronics (ICCE), 2016.

[12] L. An and Guang-Hong Yang, "Decentralized Adaptive Fuzzy Secure Control for Nonlinear Uncertain Interconnected Systems Against Intermittent DoS Attacks", IEEE Transactions on Cybernetics, 2018.

[13] M. Hosseinpour,Seyed Amin Hosseini Seno, Mohammad Hossein Yaghmaee Moghaddam and Hossein KhosraviRoshkhari, "An Anomaly Based VoIP DoS Attack Detection and Prevention Method Using Fuzzy Logic", 8th International Symposium on Telecommunications (IST'2016), 2016.

[14] M. Aravind and V.K.G. Kalaiselvi, "Design of an Intrusion Detection System Based on Distance Feature Using Ensemble Classifier", International Conference on Signal Processing, Communications and Networking (ICSCN -2017), 2017.

[15] M. Hasnatand MahshidRahnamay-Naeini, "A Data-Driven Dynamic State Estimation for Smart Grids under DoS Attack using State Correlations", North American Power Symposium (NAPS), 2019.

[16] KDD 99 [Avaliableonline]http://kdd.ics.uci.edu/databases/kddcup99/

*****