International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 01 | Jan 2022 www.irjet.net p-ISSN: 2395-0072

Detecting Various Intrusion Attacks using A Fuzzy Triangular Membership Function

Richa Mishra[1], Sakshi Koli[2], Shubham Gupta[3]

[1]*Mrs. Richa Mishra, Assistant Professor, Dept. of CSE*
[2]*Ms Sakshi Koli, Assistant Professor, Dept. of CSE*
[3]*Mr. Shubham Gupta, Assistant Professor, Dept. of CSE*
Tula's Institute Dehradun

Abstract - *In recent years, the area of intrusion detection has received a lot of consideration. One factor is the internet's exponential growth and the vast number of networked systems found in various organizations. As a result of this growth, the number of cyber-attacks against these devices and services has increased as well.. Each sort of attack has distinct characteristics that can be identified and prevented using supervised learning techniques. Many advances have been made thanks to the efforts of various academics who are actively researching on various techniques to improve ID performance. However, advancements in a number of other processes and technologies continuously present new opportunities to add a sharp edge to IDS and to make it more reliable and robust. In this paper we make to detect various attacks by using fuzzy and of triangular membership function and to normalize huge data standard deviation is used. This template, modified in MS Word 2007 and saved as a "Word 97-2003 Document (Size 10 & Italic , cambria font)*

Key Words: , **Supervised Learning , Fuzzy Logic ,Triangular Membership Function**

1.INTRODUCTION

A computer network contains a set of hardware and software components in order to establish a wide network. Both hardware and software components have their own risks, vulnerabilities and security problems. The software makes the data in open environment of computer network very vulnerable due to the attack . Computer networks are being attacked every day and therefore they are unreliable and unsafe, which means that the users may experience malicious activities and may lose their privacy, personal data or any other important information that is available on-line, depending on the nature of attacks. To protect the system from all the internal and external malicious attacks we use various network security .The external attacks by the intruders can be detected by IDS(Intrusion Detection System). Network intrusion detection system (NIDS) is used for detection of attacks in computer networks. NIDS is installed on server side to monitor the incoming and outgoing traffic for detection of intrusion. The objective of IDS to give a mass protection to stand up to the attack of computer system in internet. The intrusion detection system works on the collected information.

In this paper we present an intrusion detection system that uses triangular membership function to detect the type of intrusion in the network.

1.1 Intrusion Detection System

Intrusion in a computer network is a group of activities that degrade, disrupt, deny or destroy information and services on the computer network. Intruders are executed through data which flow through the computer networks and may disturb the integrity, confidentiality, or availability of the computer networks. Examples of intruders are viruses attached to email, internet worm, unauthorized usages of system, denial of services, probing of the system to collect information. Intruders are often called hackers and there are three different classes of intruders' masquerades, social engineering intruders and abuse of functionality intruders. First, the masquerades, prevent individuals from using their computer systems and then penetrate the computer systems entry by utilizing credentials of the individuals. Second, the social engineering intruders, in which unauthorized user obtain the internal information of the computer systems to get access to a required computer system. Third, abuse of functionality intruders, in which attacker perform unwanted activity for a computer system failure by overdoing a legitimate action.

Intrusion detection system (IDS) is an equipment for checking, distinguishing and breaking down the infringement incidents. The IDS monitors network traffic for distrustful activity and can send alarms to the network administrators. The IDS may respond to malicious also called abnormal traffic by taking appropriate actions. The appropriate actions may be taken such as blocking the source IP address or user credential information from accessing the network IDS can collect data from a host based system or from a network based system. In the host based system data are collected from system log files and audit log files. In the network based system data are collected and analyzed by analyzing the network packets

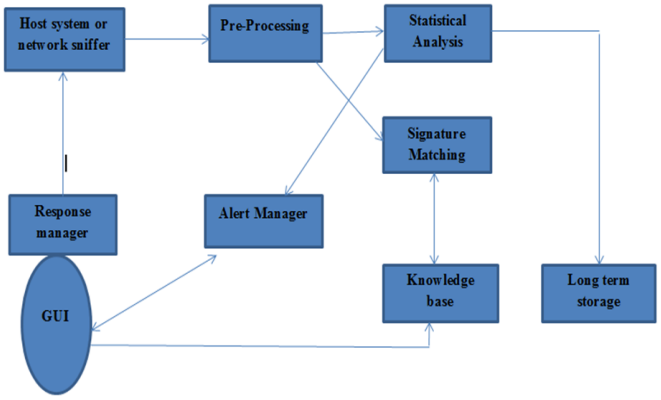

Figure 1.1 Standard IDS

Figure 1.1 shows the detail working of an intrusion detection system. In this data are collected from host or network. After collection and pre-processing of data is performed, the collected data are matched with the defined signature. If attacks are detected, it will generate an alert to the system. If collected data does not match to the existing signature then it will be defined as a normal traffic.

There are two types of IDS based on deployment of the IDS as following:

1. HIDS (Host based intrusion detection system)
2. NIDS (Network based intrusion detection system)

1. Host based intrusion detection system (HIDS) is installed on a single system. The HIDS detects intrusion in local environment and analyzes the host system. A sensor which can be installed on the host system can obtain data from system log files. The system log files are generated from operating system (OS) installed on the host system. The HIDS does not appear in the OS audit logging mechanism. The HIDS depends on audit trails and are easy to install and maintain. the audit trails verify success or failure of the attacks on the host system.

2. Network based intrusion detection system (NIDS) collects data from computer networks. The NIDS conducts audit of attacks on the computer networks by watching the packets across the computer network . In NIDS audit, sensors are deployed on the networked systems and are well armed with rules which are formed by signature based - observations .to examine network packet headers . NIDS is easy and cheap to implement and monitors attacks like DoS attacks and root attacks.

1.2 Function of IDS :

An IDS has four main functions i.e., Data Collection, Feature Selection, Analysis and Action.(as shown in fig2).
1.Data collection: The Data collection section, collects data for the IDS. The data are collected from different sources and are stored in files and then analysed.

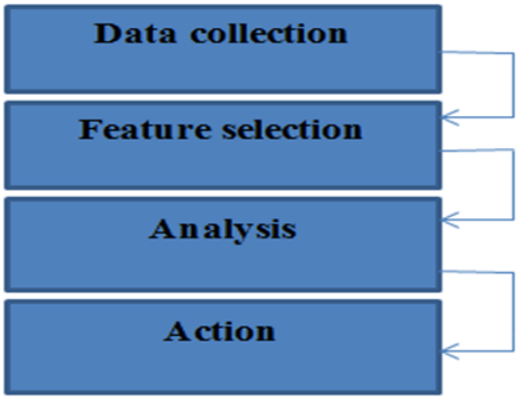

Fig1.2(Function of IDS)

The NIDS collects data and manipulates the collected data for better analysis wherein the HIDS collects data from system log files and audit log files for evaluation.

2.Feature selection: In feature selection module, a specific attribute is selected for the IDS. The specific attribute decreases the computational time and increases the performance. The feature selection is performed based on internet protocol (IP) addresses of the source and target systems., Types of protocols, header length and size of packets are considered as main fields to detect an intrusion.

3.Analysis: The collected data are analyzed in this function. This module plays important role in intrusion detection. There are two key ways for Intrusion Detection- Rule Based and Anomaly Based. The Rule Based technique work on information collected from real time environment. In anomaly based detection, data matching is performed with a normal profile data to check the deviations. An intrusion is considered when any deviation is found in the match.

4. Action: In this section attack detections and alert generations are the main tasks. The network administrator will generate an alarm or it will drop an email message in the event of any attack.

1.3 Intrusion Detection techniques:

Today computer networks are increasing rapidly. That's why security is a measure concern in the computer networks. These techniques are different from their working method and way of implementation. These techniques are being used to detect intrusion in the computer networks. Network attacks prevention can be done only when a reliable intrusion detection system is used. Broadly, there are three techniques for intrusion detection: Supervised learning, Unsupervised learning, and Reinforcement Learning.

1.Supervised learning: In supervised learning labelled datasets are used. Training is done under the supervision of a teacher. The labelled training datasets are used in training phase. There are different types of supervised learning

algorithms. Bayesian Statistics, ANN, Lazy learning, Gaussian Process Regression, Nearest Neighbor algorithm, Support Vector Machine, Hidden Markov Model, Bayesian Networks, Decision Trees, Perceptron, SVM and Quadratic classifiers are some of the most popular supervised learning algorithms

2 Unsupervised learning: When learning is done without any guidance then it is called unsupervised learning. Clustering is basically an unsupervised learning. For example, a fish kid does not know swimming, with her mother they learn swimming by their own. This is unsupervised learning. In this, unlabelled datasets are used as training datasets. Outside feedback is not required in unsupervised learning. There are various important clustering algorithms for unsupervised learning like Cluster analysis (K-means clustering, Fuzzy clustering), Hierarchical clustering, Outlier detection (Local outlier factor), Self-Organizing Map, Apriority algorithm, Éclat algorithm.

3 Reinforcement learning: Reinforcement learning is acritic based learning. In this learning algorithm, outside feedback is required. In this learning computer can interact with the environment for learning. A user can label the datasets in reinforcement learning.

1.4 Classification in IDS :

Various types of classifiers are used for intrusion detection, which are :

a) Support Vector Machine
b) Hierarchical K-Map
c) Neural Network
d) Data Mining
e) Fuzzy Logic.

1.Support Vector Machine does not work on large volume of dataset and takes more computational time. Because of high complexity more memory is required.

2. Hierarchal k-map does not work on KDD dataset, because it does not work on more than 5 variables.

3. Neural network require more computational resources. Later data addition in training network is difficult in neural network.

4.Data mining provide facility to perform operation on large dataset, but have some issues of security, privacy. Fuzzy logic provides more accurate detection rate as equated to support vector machine, neural network, data mining. Fuzzy logic does not have fine-tuned classifier, not have selected features for reduced computational time and improved detection rate. Entropy based features selection and layered classifier using fuzzy controlled logic is used to overcome this limitation. It will decrease the false positive rate of detection of attacks, and reduces the computational time.

1.5 KDD Dataset in IDS

KDD dataset is used as a training dataset. For testing dataset, data are collected from Wireshark.

KDD dataset can be used as training dataset. It is very popular dataset for intrusion detection. KDD dataset contain millions of records where each record comprises 41 attributes. Some attribute have more influence on attacks detection, and some have less influence on attack detection. There are several methods used for attribute selection. For attribute selection Feed forward neural network can be used and it requires extensive training.

Support vector method can also be used for attribute selection. Genetic algorithm is used as attribute selection method as well for reduction of dimensionality. All these selection method does not simultaneously provide the minimum and maximum values which are in within range.

Entropy based attribute selection method is used for attribute selection. This method uses minimum and maximum value for attribute selection.

Fuzzy logic provides base to handle imprecision and vagueness as well as mature influence mechanisms using changing degree of truth .In Fuzzy logic boundaries are not always evidently clear. Fuzzy logic include the identification of complex pattern or behaviour variations. Fuzzy logic uses the membership degree to determine the strength of an object belongs to different class .

2. LITERATURE REVIEW

Ding et al. Proposed optimization based cluster analysis approach with feature selection with a fuzzy and real coded chemical reaction for the intrusion detection system. The results showed that FMIFS-RCCRO-FCM outperforms the other methods in terms of both efficiency and accuracy .With the help of FMIFS approach with RCCRO-FCM model processing of a large number of features can be avoided easily.

S Douzi, S et al. proposed a combined algorithm based on feature selection techniques such as Weighted Fuzzy C-Mean Clustering Algorithm (WFCM) and Fuzzy logic. The methodology reduced the input data and introduced weights into each of the data dimension. This main focus of this article was to lower the false alarm rates which are very problematic for IDS, and ensure the flexibility of intrusion detection systems in an environment with inaccuracy and uncertainty.

Cristiani´ et al. proposed FROST(An IDS based on the fuzzy sets theory)to identify various kinds of cyber-attacks on IoT networks. Main concept of FROST was to suggestively decreased the number of occurrences related to a new type of attack classified as one of the identified attacks. Due to the attack classification, a lower error rate is shown.

Saidi, F et al. introduced a Fuzzy IDS as a Service which consider fuzzy rules base and the Mamdani method to gather the rules. It enabled network administrators and cyber security specialists to follow the real time the network traffic behaviour. Network traffic behaviour includes the Port Scanning Criticality Level (PSCL). A SaaS dynamic dashboard is used to swiftly and efficiently recognize spiteful port scanning activity. Experiments and assessments revealed that the suggested system outperformed Snort and related IDS systems in multilevel port scanning detection.

Kumar et al. presented the architecture of the Distributed Intrusion Detection System using Cloud Computing Infrastructure and Blockchain. The strategy was built on a Distributed Intrusion Detection System (DIDS) that combined evolving and promising technologies such as Blockchain with a solid foundation such as cloud infrastructure

Valli Kumari V et al. proposed a hybrid mechanism .It shows higher processing speed compared to multi-classification and requires less training time compared to full-SVM, it also found out low Labelling cost as instead of fully-labelled SVM. Since small amount of labelled set was used. This paper showed a hybrid semi-supervised machine learning technique that includes Active learning Support Vector Machine (ASVM) and Fuzzy C-Means (FCM) clustering in the creation of an effective IDS.

Warzyński, A et al. performed the verification of the anomaly detection systems that has an ability to counter different type of attacks. This paper affords the initial outcomes to examine the investigate presence of attack vector, that may use adverse examples to hide a actual outbreak from being detected intrusion detection systems.

Zhan X et al. demonstrated that the characteristics that block chain information cannot be changed at will, network resources are managed and monitored to ensure the uniqueness of data information. Block chain technology and Internet of Things technology are integrated to label and manage tangible assets to improve the trustworthiness and controllability of tangible asset management. Using block chain technology to increase network infrastructure protection can provide stable services for a variety of network applications while avoiding the maltreatment caused by network security hazards.

Sukumar et al developed an intrusion detection system that uses IGKM algorithm to detect the type of intrusion and the number of clusters (k) is not fixed beforehand. It included the k-means++ set of rules and an intrusion detection system that used IGKM algorithm whilst using smaller subset of KDD . KDD dataset contained ninety nine dataset with thousand instances .The Shown experiment result indicated that the intrusion detection with IGKM algorithm was more accurate compared to k-means++ algorithm.

Imen Gaied,Farah et al. demonstrated that their approach based on NEFCLASS model is morepowerful in classifying intrusions than the one based on ANFIS model. The proposed model is the Neuro-Fuzzy model accurately the NEFCLASS (Neuro Fluffy Classification) model of a generic fuzzy perceptron which is in the form of a grouping of neuron and fuzzy system networks.

Haider x al. proposed NGIDS-DS which has a medium-high quality of realism and is generated by the intelligent use of the commercial-scale security test hardware platform IXIA Perfect Storm. The NGIDS-DS comprised labeled network and host logs. It reflects the current critical cyber infrastructures. It included both normal and abnormal scenarios where abnormal scenario adds accurate attack behaviors and normal scenarios adds normal traffic dynamics of real-world networks.

Kumari, V et al proposed a. hybrid semi-supervised machine learning technique that uses Active learning Support to perceive attacks in the network. It included Vector Machine (ASVM) and Fuzzy C-Means (FCM) clustering in the design of an efficient IDS. Set of rules is examined on NSL KDD bench mark IDS data set and was initiated to be promising.

Shanmugavadivu, R et al developed an intrusion detection system based on anomaly to detect an intrusion behaviour over a network. It designed a fuzzy decision-making to structure the system more accurate for attack detection by using the fuzzy inference approach. It also used automated strategy for generation of fuzzy rules, which are obtained from the definite rules using frequent items. The experimental results clearly showed that the proposed system accomplished higher precision in identifying whether the records are normal or attack one.

Balan et al proposed a system that detects the spiteful behaviour of node by intrusion detection system with fuzzy logic technique and also to categorize the type of attacks .The system is strong enough to detect attacks including black hollow attack and grey hollow attack and additionally able to avert the ones type of attacks by using efficient node blocking mechanism such that the proposed system provides a secure communication between nodes.

3. METHODOLOGY

In the process of attack detection, the fuzzy controlled language is used. The layered model is useful for classifying the main classes of attacks and the sub classes of attacks. A fuzzy controlled architecture describes how the process of attack detection takes place. Fig 3.1 shows the fuzzy controlled architecture. It contains the following steps which have been taken in the process.

1. Methods of attribute selection.
2. Layered Fuzzy control language.
3. Testing dataset

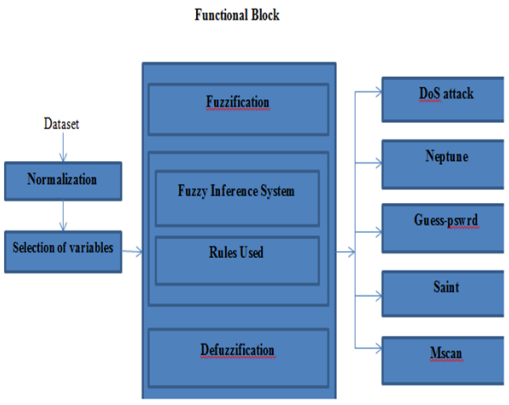

Fig3.1(Function Block)

1 Methods of attribute selection: KDD cup datasets are used for study of main classes of attacks and their sub attacks. The datasets contain 41 attributes, in which 7 are discrete and 34

are continuous with a large domain of values. Some attributes have limited contribution in detection of attacks. The attributes which do not contain any valuable information for attacks are eliminated from the datasets. 21 attributes are considered which have valuable information about the attacks. The values which are not useful are eliminated. So, the features which contain valuable information for attacks are used for attack detection and classification. Various steps are performed for selection of attributes from KDD datasets.

1.1 A) Attribute normalization: There are different types of values present in a KDD dataset. It includes 41 attributes, 7 discrete and 34 continuous variables. The 34 attributes are taken for normalization. In this KDD dataset, some values are high and some values are very low. These elements contain very large range of values ie.0 to 5,13,1424. To avoid this, normalization is performed on selected values . With the help of normalization, the values are normalized in the range of 0 and 1.

B) Method used for normalization- Standard deviation method is used for normalization of data. Standard deviation gives better result than any other method which is used for normalization. Standard deviation is calculated with the following equation:

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(x_i - \mu\right)^2} \quad \text{.....3.1}$$

σ = Standard deviation

N= No of instances

μ = Mean

X= Sample mean.

B) Attribute selection: A KDD dataset contains 41 elements. Some attributes play important role in attack detection and some have not any role in attack detection. Performance of attack detection is reduced with these unnecessary attributes. Computational time also increases with more attributes. Selection of useful attributes will increase the performance of the detection rate. Entropy is calculated for the selection of attributes. Entropy is measure of uncertainty and randomness. Very low values and very high values which come after entropy calculation are selected for attack detection. Entropy is calculated with this formula.

$$et = -\sum_{i=1}^{nf}\left(\left(\frac{ai}{nf}\right)\times\left(\frac{\log(ai)}{nf}\right)\right) \quad \text{.....3.2}$$

et= Entropy of the dataset, is number of features, a is dataset

2.Layered Fuzzy Controlled language: The proposed architecture of fuzzy controlled language contains normalization and selection of attributes before fuzzification. The process contains fuzzy inference system, rule box and defuzzification units.

a.Fuzzification: In the process of fuzzification conversion of crisp value to fuzzy value takes place for defining the membership function.

b.Fuzzy Inference System: Fuzzy inference system is the way toward planning the mapping from a given input to the output using fuzzy logic. With the help of mapping of input to the output decisions can be made, or patterns recognized. The process of fuzzy inference system includes all the parts that are described logical operation, membership function and If-Then rules. Rules which are used for inference system are given in table 3.2

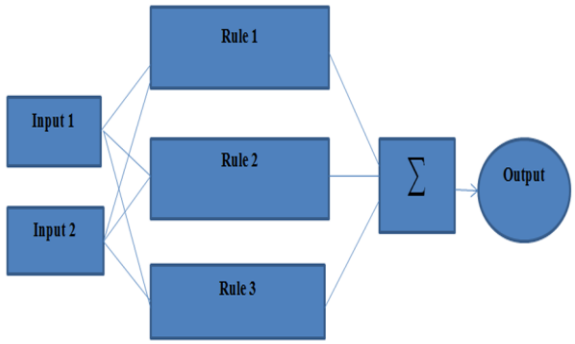

Figure 3.2 Fuzzy Inference System

Membership function: Triangular membership function is used in this process of membership declaration Three variables a, b and c are used, a and c locate the base of the triangle and b locates peak of the triangle. The triangular membership function value of variable V0 is defined as [(VL:0.00 0.05 0.10 0.15), (L:0.10-0.16, 0..27-0.35), (M:0.27-0.36,0.50-0.60), (H:0.50-0.62,0.70-0.80), (VH:0.70-0.82,0.90-1.00)]. Values of all variables are given in table 3.1

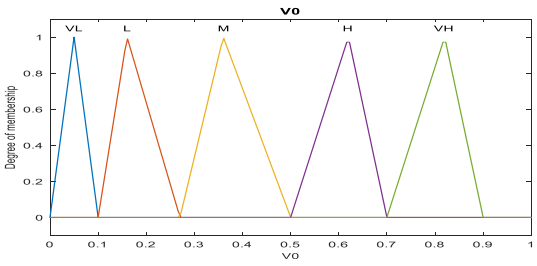

Figure 3.3 Membership values of the variable

////

a)Defuzzification: Defuzzification is the process in which fuzzy values are converted into crisp values for identifying the attacks using a layered approach. Centroid method is used for defuzzification.

$$COG = \frac{\int_{min}^{max} tu(t)dt}{\int_{min}^{max} \mu(t)dt} \text{.....3.3}$$

Denote the algebraic integration, this method is also known as centre of gravity.

3 Testing datasets: Testing data are collected with the help of Wireshark. The fuzzy rule is tested on data generated from Wireshark. Wireshark is an open source packet tracer. A network packet tracer captures real time network packets and tries to display all the details of the captured packets .

3.2Rules used for attack detection:

Fuzzy inference system works based on the rules given in below table. Rules will detect main classes of attacks and their sub classes. Rules are designed with the help of variables which are identified by the process of normalization. These are the membership values range from variable V0 to V22.

4. Proposed Algorithm for identifying attacks

Step 1 Read data

Step 2 Manage Data

Step 3 Normalize Data

Step 4 Create Fuzzy Inference systems.

a) Create input membership function
b) Create output membership function
c) Create rules

d) d)Parse rules c) Generate fuzzy

e) Step 5 Read Fuzzy values

f) Step 6 Evaluate Fuzzy values

g) Step 7 Loop from number 1 to the length of data

h) Step 8 Pass to fuzzy
i) Step 9

Sr. No	Rules Designed For Fuzzy Inference System
1	If (Port is icmp) or (s is http) or (f is S1) then (Attack is DOS) (1)
1.1	If (V0 is VL) and (V1 is VH) and (V2 is VL) and (V11 is VL) then (SubAttack is smurf) (1)
1.2	If (V0 is L) or (V1 is L) or (V2 is L) or (V11 is L) or (V12 is L) or (V13 is H) or (V15 is L) or (V16 is M) then (SubAttack is neptune) (1)
1.3	If (V0 is M) and (V1 is H) and (V2 is L) and (V5 is VL) and (V13 is VH) then (SubAttack is mailbomb) (1)
1.4	If (V0 is VL) and (V1 is M) and (V2 is M) and (V11 is VL) and (V13 is VH) and (V15 is L) then (SubAttack is back) (1)
1.5	If (V0 is VL) or (V1 is VL) or (V2 is VL) or (V7 is H) or (V8 is VH) or (V11 i L) or (V13 is VH) or (V20 is H) or (V21 is H) then (SubAttack is apache2) (1)
2	If (Port is icmp) or (s is all_u) or (f is RSTR) then (Attack is probe) (1)
2.1	If (V0 is VL) and (V1 is M) and (V2 is H) and (V5 is L) and (V6 is L) and (V11 is VL) and (V13 is VH) then (SubAttack is snmpgetattack) (1)
2.2	If (V0 is VL) or (V1 is VL) or (V2 is M) or (V4 is VH) or (V5 is VH) or (V6 i VH) or (V11 is VH) or (V18 is VL) or (V19 is L) or (V20 is M) or (V21 is M then (SubAttack is guess_passwd)(1)
2.3	If (V0 is M) and (V1 is VL) and (V2 is VL) and (V5 is L) and (V6 is VL) an (V9 is M) and (V13 is M) and (V14 is VH) and (V16 is L) then (SubAttack i satan) (1)
2.4	If(V0 is VH) and (V1 is VL) and (V2 is VL) and (V4 is VL) and (V7 is VH) and (V15 is L) and (V16 is H) then SubAttack is mscan
2.5	If (V0 is VL) and (V1 is VL) and (V2 is VL) and (V5 is VL) and (V11 is VH and (V15 is VH) and (V16 is VH) then (SubAttack is saint) (1)
2.6	If (V0 is L) and (V1 is VL) and (V2 is VL) and (V5 is VL) and (V6 is VL) an (V9 is VH) and (V10 is VH) and (V11 is VL) and (V13 is VH) and (V14 is VL and (V16 is M) and (V20 is VH) and (V21 is VH) then (SubAttack is portsweep (1)
2.7	If (V0 is VL) and (V1 is VL) and (V2 is L) and (V6 is VL) and (V9 is VH) an (V10 is VH) and (V11 is VL) and (V13 is VH) and (V14 is VL) and (V16 is M and (V20 is VH) and (V21 is VH) then (SubAttack is ipsweep) (1)
3	If (Port is icmp) or (s is ftp) or (f is S2) then (Attack is R2L) (1)
3.1	If (V0 is L) and (V1 is VL) and (V2 is L) and (V11 is M) and (V13 is VH) an (V15 is M) then (SubAttack is processtable) (1)
3.2	If (V0 is VL) and (V1 is L) and (V2 is L) and (V3 is VL) and (V5 is VL) and (V is VL) and (V11 is H) then (SubAttack is pod) (1)
3.3	If (V0 is L) and (V1 is L) and (V2 is VL) and (V11 is M) and (V13 is VH) an (V14 is M) and (V15 is H) then (SubAttack is snmpguess) (1)
3.4	If (V0 is VL) and (V1 is VL) and (V2 is VL) and (V11 is VL) and (V13 is VL) and (V14 is VL) and (V15 is VL) then Attack is nomal

Table 3.3 Comparison of normalization and membership function

A) If result is rule 1 then DoS attack

a) If rule is 1.1 then sub attack is smurf
b) If rule is 1.2 then sub attack is Neptune
c) If rule is 1.3 then sub attack is mailbomb
d) If rule is 1.4 then sub attack is back
e) If rule is 1.5 then sub attack is apache2

B) If rule is 2 then attack is Probe

a) If rule is 2.1 then sub attack is snmpgetattack
b) If rule is 2.2 then sub attack is guess_psword
c) If rule is 2.3 then sub attack is satan
d) If rule is 2.4 then sub attack is mscan
e) If rule is 2.5 then subattack is saint
f) If rule is 2.6 then subattack is portsweep
g) If rule is 2.7 then subattack is ipsweep

C) If rule is 3 then attack is R2L

a) If rule is 3.1 then subattack is processstable
b) If rule is 3.2 then subattack is pod
c) If rule is 3.3 then sub attack is snmpguess
d) Else Normal

4.1 Implementation of Proposed Algorithm

e) The variables which are taken are plot with the membership values. There are 21 variables are used for attack detection. Some of the graph with their membership

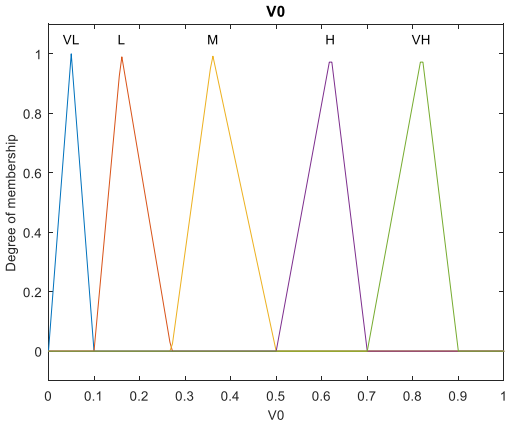

Figure 3.4 Variable V0 with their membership value

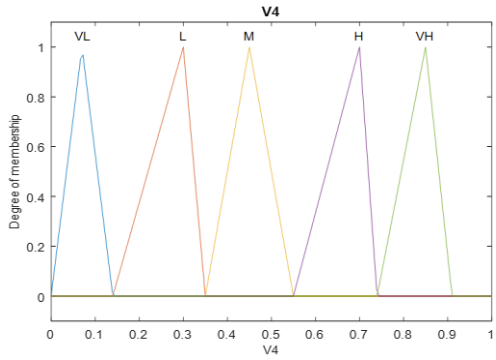

Figure 3.5 Variable V4 with their membership value

Figure 3.4 and 3.5 shows the membership values of variable V0 and V4. This membership have five values ie VL, L, M, H,VH .

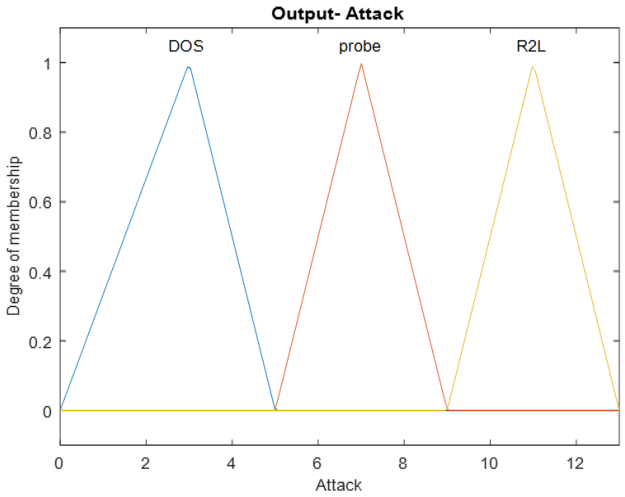

Figure 3.6 Output values of various attacks

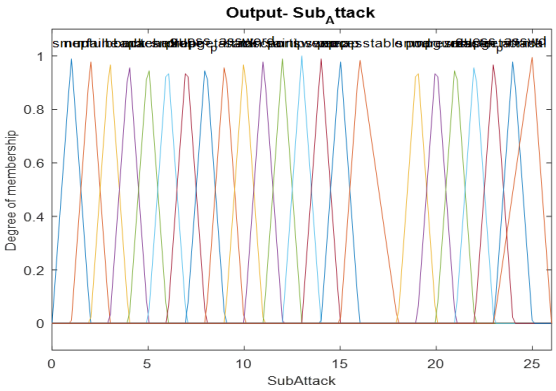

Figure 3.7 Output values of various sub attacks

Figure 3.6 and 3.7 give the membership values of main attacks and their sub attacks.

4.2Results and Analysis

More than 10,000 records taken for attack detection. Main classes of attack are detected and their sub attacks are also detected.

Results
Normal Data = 10899
Dos Attack = 529
Probe Attack = 448
R2L Attack = 65
Total Packet = 11941
Smurf Attack = 121
Neptune Attack = 60
Mailbomb Attack = 92
Back Attack = 27
Teardrop Attack = 1
Snmepge Attack = 55
Guess Attack = 213
Guess Password Attack = 28
Mscan Attack = 8
Saint Attack = 112
iPsweep Attack = 14

Port Sweep Attack = 3
map Attack = 1

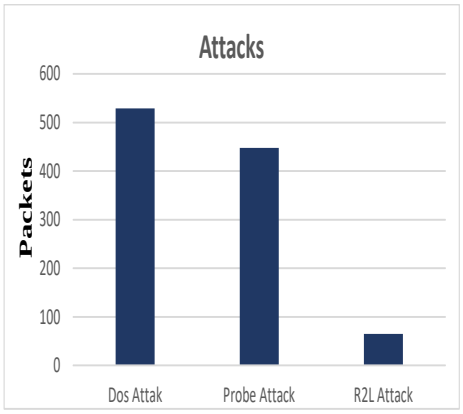

Figure 3.8 Bar graph showing Dos, Probe and R2L attacks.

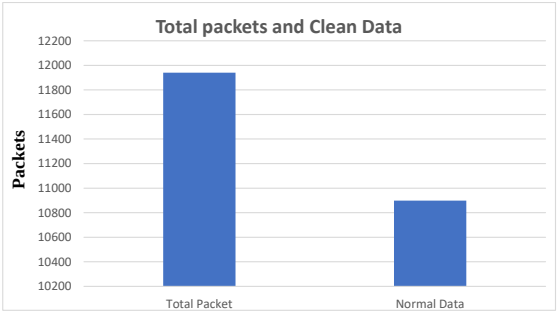

Figure 3.9 Bar graph showing total Packets checked and clean data detected.

Figure 3.8 shows the number of main attacks detected, and figure 3.9 shows the graph of total packet and the normal data.

5. RESULTS AND DISCUSSIONS

The results obtained showed that an accuracy was 61.53% and performance was 44.44% which were better than the Attack's Feature Selection-Based Network Intrusion Detection System Using Fuzzy Control Language. The proposed system uses a self-formulated normalization as shown in table 3.1 The formula used has been explained above. The membership function used by the proposed system is Triangular which was found to give better results as it takes minimum, maximum and peak values resultantly the range is clearly defined for the system to arrive at the results. The rules are also designed in such a way that they can detect maximum possible attacks.

Method used	Attack's Feature Selection-Based Network Intrusion Detection System Using Fuzzy Control Language.	Proposed
Normalization	$Var_n = \frac{Var - \min(Var)}{\max(Var) - \min(Var)}$	$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2}$
Membership function	Trapezoidal	Triangular

Formula used for accuracy

Accuracy: $$100 - \left(\left(\frac{TA - R}{R}\right) \times 100\right) \quad \text{.....3.4}$$

With use of the layered approach, the sub classes of attacks are detected. Attacks are detected over 11000 datasets. Frist of all, it detects main class of attacks and then the sub classes of attacks are detected.

Figure 3.10 shows the graph of numbers of the sub attacks detected. These attacks are smurf, Neptune, mailbomb, back, teardrop, snmpgetattack, Guess-passwd, mscan, saint, portsweep, ipsweep,Nmap, snmpguess.

Table 3.4 Improvement in number of attack detected

Attacks	Attack's Feature Selection-Based Network Intrusion Detection System Using Fuzzy Control Language.	Propose
Do's	Yes	Yes
Probe	Yes	Yes
R2L	Yes	Yes
Smurf	Yes	Yes
Neptune	Yes	Yes
Mailbomb	No	Yes
Back	Yes	Yes
Apache2	-	-
Teardrop	Yes	Yes
Snmpgetattack	No	Yes
Guess-psswd	Yes	Yes
Satan	-	-
Mscan	No	Yes
Saint	No	Yes
Portsweep	Yes	Yes
Ipsweep	Yes	Yes
Processtable	-	-
Pod	-	-
Snmpguess	No	Yes
Warezmaster	-	-

Table 4.1 Number of sub attacks detected by layered classifier.

Sr.No.	Layer	Attack type	No of attack detected
1	DoS	Smurf	121
		Neptune	60
		Mailbomb	92
		Back	27
		Apache	-
		Teardrop	1
2	Probe	Snmpgetattack	28
		Guess_passwd	213
		Satan	-
		Mscan	8
		Saint	121
		Portsweep	3
		Ipsweep	14
		Nmap	1
3	R2L	Processtable	-
		Pod	-
		Snmpguess	55
		Warezmaster	-

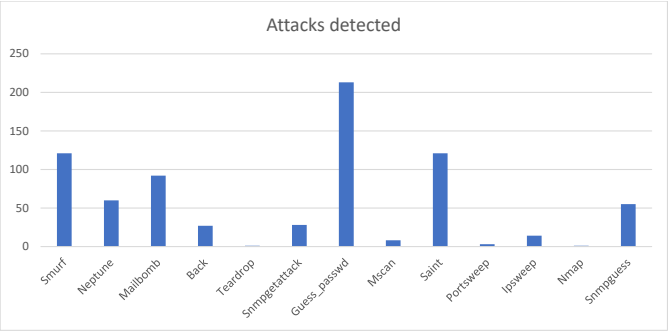

Figure 4.2 Bar graph showing Attacks detected.

6. CONCLUSIONS

Intrusion detection technology has always been a major topic in the realm of computer network security. The purpose of intrusion detection technology is to efficiently monitor anomalous data traffic in the network in real time, prevent it while it is still budding, and isolate it from the target region, to keep track of malicious activity in a timely and efficient manner. We have shown that the-Fuzzy model is highly efficacious for the reduction of and for its higher accuracy rate in comparison with other models. The result obtained showed an accuracy of 61.53% ,The attacks detected were Mailbomb, Snmpgetattack, Mscan, Saint, Snmpguess are improved name of detected attacks.In the future, it may be possible to develop a realistic application based on unsupervised learning methods that may not only identify an intrusion but also provide users with alternate defence mechanisms.

REFERENCES

[1] Ding, W., Nayak, J., Naik, B., Pelusi, D., & Mishra, M. (2020). Fuzzy and Real-Coded Chemical Reaction Optimization for Intrusion Detection in Industrial Big Data Environment. IEEE Transactions on Industrial Informatics, 17(6), 4298-4307.

[2] Douzi, S., Benchaji, I., & ElOuahidi, B. (2018, October). Hybrid approach for intrusion detection using fuzzy association rules. In 2018 2nd Cyber Security in Networking Conference (CSNet) (pp. 1-3). IEEE.

[3] Cristiani, A. L., Lieira, D. D., Meneguette, R. I., & Camargo, H. A. (2020, November). A Fuzzy Intrusion Detection System for Identifying Cyber-Attacks on IoT Networks. In 2020 IEEE Latin-American Conference on Communications (LATINCOM) (pp. 1-6). IEEE.

[4] Saidi, F., Trabelsi, Z., & Ghazela, H. B. (2019, November). Fuzzy logic based intrusion detection system as a service for malicious port scanning traffic detection. In 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA) (pp. 1-9). IEEE.

[5] Kumar, M., & Singh, A. K. (2020, June). Distributed intrusion detection system using blockchain and cloud computing infrastructure. In 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184) (pp. 248-252). IEEE.

[6] . Kumari, V. V., & Varma, P. R. K. (2017, February). A semi-supervised intrusion detection system using active learning SVM and fuzzy c-means clustering. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 481-485). IEEE.

[7] Warzyński, A., & Kołaczek, G. (2018, July). Intrusion detection systems vulnerability on adversarial examples. In 2018 Innovations in Intelligent Systems and Applications (INISTA) (pp. 1-4). IEEE..

[8] Zhan, X., Yuan, H., & Wang, X. (2019, September). Research on Block Chain Network Intrusion Detection System. In 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA) (pp. 191-196). IEEE.

[9] Sukumar, J. A., Pranav, I., Neetish, M. M., & Narayanan, J. (2018, September). Network intrusion detection using improved genetic k-means algorithm. In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 2441-2446). IEEE.

[10] Gaied, I., Jemili, F., & Korbaa, O. (2015, November). Intrusion detection based on neuro-fuzzy classification. In 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA) (pp. 1-8). IEEE..\

[11] Haider, W., Hu, J., Slay, J., Turnbull, B. P., & Xie, Y. (2017). Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. Journal of Network and Computer Applications, 87, 185-192.

[12] Kumari, V. V., & Varma, P. R. K. (2017, February). A semi-supervised intrusion detection system using active learning SVM and fuzzy c-means clustering. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 481-485). IEEE.

[13] Shanmugavadivu, R., & Nagarajan, N. (2011). Network intrusion detection system using fuzzy logic. Indian Journal of Computer Science and Engineering (IJCSE), 2(1), 101-111.

[14] Balan, E. V., Priyan, M. K., Gokulnath, C., & Devi, G. U. (2015). Fuzzy based intrusion detection systems in MANET. Procedia Computer Science, 50, 109-114.