Innovative Empirical Approach for Intrusion Detection Using ANN

Brijpal Singh, Dr. Anil Kr. Ahlawat

Abstract - **Intrusion detection system based on Artificial Neural Network (ANN) is a very active field that detects normal or attack connection on the network and can improve the performance of Intrusion detection system (IDS), the flash alarm rate in establishing intrusive activities can be reduced. At present computer network and cloud based computing technology is used by an increasing number of users. Computer and network security has received and will still receive much attention. Any unexpected intrusion will damage the network. The areas like business, finance, medical, security sectors have made us reliant on the computer networks. It is important to secure system for which we require strong intrusion detection system which is capable of monitoring network which carries huge amount of data packets as well as reports malicious activity that occurs in the system. Therefore some strategy is needed for best promising security to monitor the anomalous behavior in computer network. A discussion of the upcoming technology and various methodologies which promise to improve the capability of computer system to detect intrusions is offered. In the proposed approach the Artificial Neural Network (ANN) algorithms are used as classifiers for detecting the normal and attack records by training and testing the KDD CUP 99 dataset. It is proved that the FFNN with 10 neurons and 2 layers has performed better over FFNN with different number of neurons and 2 layers.**

Keywords - **Intrusion Detection System (IDS), Artificial Neural Network (ANN), Principal Component Analysis (PCA), Network Security.**

I. INTRODUCTION

An intrusion can be termed as an unauthorized entry to another's property or area, but in terms of computer science, it is the activities to compromise the basic computer network security goals viz. confidentiality, integrity, and privacy. Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents of threats and violations of computer security practices, acceptable use policies or standard security policies.

Network intrusion detection system inspects all the incoming and outgoing traffic and identifies malicious pattern that indicates network attack from someone that is not authorized to break in to system. An artificial neural network is composed of many neurons that are linked together according to specific network architecture.

Manuscript Received May 14, 2016
BRIJPAL SINGH, Research Scholar Department of Computer Science, Mewar University. Chittorgarh, Rajasthan, India,
DR. ANIL KR. AHLAWAT, Department of Computer Science & Application , Krishna Institute of Engineering and Technology, Ghaziabad, UP, India,

Network intrusion detection system based on artificial neural network not only detects normal or attack connection but also classify the attacks into attack types [1].

Intrusion detection is the act of detecting unwanted traffic on a network or a device. An Intrusion Detection System (IDS) can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies. Many IDS tools will also store a detected event in a log to be reviewed at a later date or will combine events with other data to make decisions regarding policies or damage control. it is more efficient to take up a proactive measure to intrusions. Intrusion Detection Systems (IDS) are primarily focused on identifying probable incidents, monitoring information about them, tries to stop them, and reporting them to security administrators in real-time environment, and those that exercise audit data with some delay (non-real-time). The latter approach would in turn delay the instance of detection. In addition, organizations apply IDSs for other reasons, such as classifying problems with security policies, documenting existing attacks, and preventing individuals from violating security policies. IDSs have become a basic addition to the security infrastructure of almost every organization [2].

A usual Intrusion Detection System is demonstrated in Figure 1

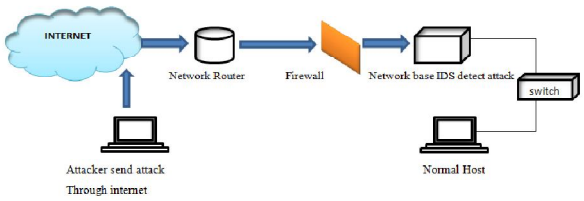

Figure 1: Simple Intrusion Detection System

Intrusion Detection Systems are broadly classified into two types. They are host-based and network-based intrusion detection systems. Host-based IDS employs audit logs and system calls as its data source, whereas Network-based IDS employs network traffic as its data source. A host based IDS consists of an agent on a host which identifies different intrusions by analyzing audit logs, system calls, file system changes (binaries, password files, etc.), and other related host activities. In network-based IDS, sensors are placed at strategic position within the network system to capture all incoming traffic flows and analyze the contents of the individual packets for intrusive activities such as denial of service attacks, buffer overflow attacks, etc. Each approach has its own strengths and weaknesses. Some of the attacks

can only be detected by host-based or only by network-based IDS.

The two main techniques used by Intrusion Detection Systems for detecting attacks are Misuse Detection and Anomaly Detection. In a misuse detection system, also known as signature based detection system, well known attacks are represented by signatures. A signature is a pattern of activity which corresponds to intrusion. The IDS identifies intrusions by looking for these patterns in the data being analyzed. The accuracy of such a system depends on its signature database. Misuse detection cannot detect novel attacks as well as slight variations of known attacks.

An anomaly-based intrusion detection system inspects ongoing traffic, malicious activities, communication, or behavior for irregularities on networks or systems that could specify an attack. The main principle is that the attack behaviour differs enough from normal user behavior that it cannot be detected by cataloging and identifying the differences involved. By creating supports of standard behavior, anomaly-based IDS can view when current behaviors move away statistically from the normal one. This capability gives the anomaly-based IDS ability to detect new attacks for which the signatures have not been created. The main disadvantage of this method is that there is no clear cut method for defining normal behaviour. Therefore, such type of IDS can report intrusion, even when the activity is legitimate.

The Intrusion Detection System (IDS) is also carried out by implementing Genetic Algorithm (GA) to efficiently identify various types of network intrusions. The genetic algorithm is applied to achieve a set of classification rules from the support-confidence framework, and network audit data is employed as fitness function to judge the quality of each rule. The created rules are then used to classify or detect network intrusions in a real-time framework. Unlike most available GA-based approaches remained in the system, because of the easy demonstration of rules and the efficient fitness function, the proposed system is very simple to employ while presenting the flexibility to either generally detect network intrusions or precisely classify the types of attacks[3].

II. LITERATURE REVIEW

The literature survey gives many results to solve the limitations of methods for number of data mining techniques that have been introduced.

ANN is the commonly used techniques and has been successfully applied to intrusion detections .

According to Horeis, (2003) Joo et al., (2003) Kevin, Rhonda, & Jonathan, (1990), Tan, (1995) ANN techniques are distributed into three categories:

1. Supervised ANN-based intrusion detection.
2. Unsupervised ANN based intrusion detection.
3. Hybrid ANN-based intrusion detection.

In first Supervised ANN, and the same applied to IDS, mainly includes multi-layer feed-forward (MLFF) neural networks and recurrent neural networks .

Mukkamala, Janoski, & Sung, (2002) Ryan et al. (1998) and Tan (1995) applied MLFF on detection based techniques based on users behaviours. And in practice the number of training set is large.The distribution of training set is imbalanced and the MLFF neural networks is easy to reach for local minimum and thus stability is lower.

For low-frequent attacks, the detection precision is very low, Some researchers have compared the effectiveness of supervised ANN with other methods such as support vector machine (SVM) and multivariate adaptive regression splines (MARS).

Supervised ANN had been shown to have lower detection performance than SVM and MARS as per Mukkamala, Sung, Abraham, & Ramos, (2004), Mukkamala et al., (2002).

In the second unsupervised ANN uses to categoerise input data and distinct normal behaviors from abnormal or intrusive ones (Endorf et al., 2004). Using unsupervised ANN in intrusion detection has many advantages. And main advantage for unsupervised ANN can improve their analysis of new data without retraining.

SOM Self-Organizing Map was firstly appplied by Fox (Kevin et al., 1990) to learn the characteristic of current system activity to identify statistical variations from the normal trends.The performance of unsupervised ANN is also lower using supervised learning ANN. For low-frequent attacks, the unsupervised ANN also gets lower detection precision (Beghdad, 2008).

The third category is hybrid ANN, that combines supervised ANN and unsupervised ANN or combine ANN with other data mining

techniques to detect intrusion Han & Cho, (2005) Jirapummin, Wattanapongsakorn & Kanthamanon, (2002). For using the hybrid ANN is to overcome the limitations of individual ANN.

A hybrid ANN for visualizing intrusions using Kohenen's SOM and classifying intrusions using resilient propagation neural networks was proposed by Jirapummin et al. (2002)

Horeis (2003) used a combination of SOM and RBF (Radial Basis Function) networks. The system offers generally best results than IDS based on RBF networks alone.

Han and Cho (2005) proposed an IDT (intrusion detection technique) based on evolutionary neural networks in order to determine the structure and weights of the call sequences.

Hybrid flexible neural tree based Intrusion Detection Technique based on neural tree for evolutionary algorithm and particle swarm optimization (PSO) proposed by Chen, Abraham and Yang (2007). Observed results indicated that the proposed method is efficient, for ANN based intrusion detection, hybrid ANN has been the trend but different ways to construct hybrid ANN will highly influence the efficiency of intrusion detection.. Different hybrid ANN models should be properly constructed in order to serve different objectives [4].

The detailed features and properties of KDD-Cup'99 dataset were identified and performances were calculated based on different classifiers. And the feature selection was performed on dataset KDD Cup'99. The complete featured dataset was divided into 4 groups. The same approach is conducted with K-means clustering, Fuzzy C means clustering, and Fuzzy entropy clustering . [5] [6].

In the year 1998 Cannady found 91% successful detection rate using MLFF on Real secure network monitor.

In the year 2004 Moradi found 91% successful detection rate using 2 hidden layers MLP on KDD99.
In the year 2004 Siddiqui found 81.37% successful detection rate for BP and 80.52% for fuzzy ARTMAP (overall PSC=80.945) using Back Propagation and fuzzy ARTMAP on KDD99.
In the year 2009 sheikhan found 91% successful detection rate using Fuzzy AR on KDD99, and againin the same year he found 91% successful detection rate using K-NN on KDD99.
And againin the same year he found 80% successful rate using data mining on KDD99.
In the year 2015 Chhavigoel 96.31% successful detection rate using FFNN 2 hidden on NSL-KDD

III. DESIGN OF PROPOSED MODEL

The proposed model as depicted in Figure 2 is divided into four stages. In this section, we elaborate our new approach, FC-ANN. We firstly present the whole framework of the new approach. Then we discuss the three main modules, i.e., clustering module, ANN module, and aggregation module.

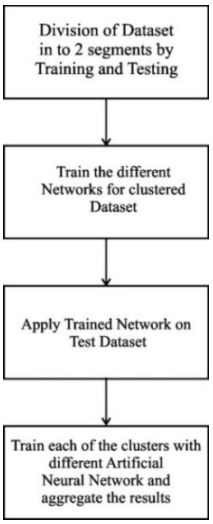

Figure 2: Proposed Model

IV. PROPOSED ARCHITECTURE OF IDS

The system is described and divides dataset into Training and Testing data and then cluster the train dataset with clustering. And then, train different Artificial Neural Networks for different clusters, and cumulate the ANN on the last stage. Subsequently, it trains the different ANN using different subsets. After aggregation and testing its determines membership grades of these subsets and combines them via a new ANN to get final results as show in Figure 3 .
The Proposed Architecture has four stages.

- Stage 1: Divide the dataset into two sets-

  [A] Training dataset and

  [B] Testing dataset. Cluster the training dataset with numbers of cluster.

- Stage 2: Train the different networks for clustered data set by using MATLAB.
- Stage 3: Apply this trained network on test dataset.
- Stage 4: Finally aggregate the ANN and improve the target results from the different neural network functions.

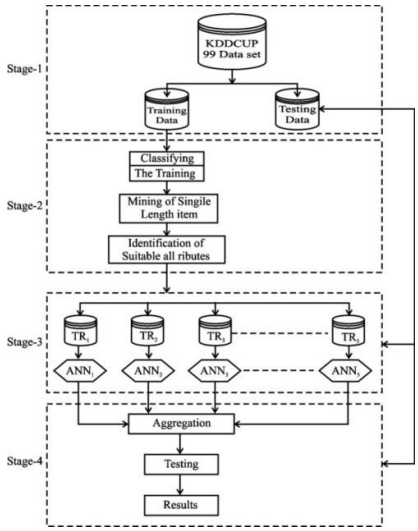

Figure 3: Proposed Architecture of IDS

V. PROPOSED TECHNIQUE

Following procedure has been applied for the present work:

1. PCA is applied to the complete KDD99 train dataset to reduce the number of features that can best describe our output class and to reduce the size of dataset vertically and complexity involved.
2. The reduced dataset with lessened features is removed off all duplicate values, leading to reduction in number of records. This reduces the size of dataset horizontally.
3. Normalization is applied that helps in bringing the record values within same range in neural networks using min/max formula.

   NewV = V - MinX / MaxX - MinX
4. The following Neural Network Algorithms are applied for training and simulation consecutively and results and plots are stored.
   (A) Feed Forward Neural Network (FFNN) is chosen as first ANN algorithm with number of neurons at layers 2 ranging from 05 to 30.
   (B) FFNN with distributed delay is next algorithm for our application in which time delay is added to feed forward network.
   (C) Cascading Neural Network
   (D) NARX Neural Network
5. The network and training properties were set same for all the algorithms so that results can be compared on similar parameters:

Training: 84971 records, testing: 10866 records, Training Function- TRAINLMAdaptive Learning Function-LEARNGDM, Performance Function- MSE Number of Layers- 2

VI. EXPEREMENTAL WORK

The KDD99 is used for the detection. KDD99 training dataset has 41 features labeled in text form as either normal or an attack with a type with approximately 4,900K single connection records. Out of 41 features for one record, includes 34 continuous and 7 symbolic features. The training and testing data is made up of 19 different Attributes out of the 41 present. Data is classified into five separate classes: normal, denial of service attacks (DOS), probe, user to super user (U2R) and remote to local attacks (R2L).

Table 1: A list of selected features of the Proposed System given in KDD cup 99 dataset [7]

Attributes Index	Attributes Name	Description	Type
1	duration	length (number of seconds) of the connection	Continuous
2	protocol_type	type of the protocol, e.g. tcp, udp, etc.	Symbolic
3	service	network service on the destination, e.g., http, telnet, etc.	Symbolic
4	flag	normal or error status of the connection	Symbolic
5	src_bytes	number of data bytes from source to destination	Continuous
6	dst_bytes	number of data bytes from destination to source	Continuous
8	wrong_fragment	number of ``wrong" fragments	Continuous
9	urgent	number of urgent packets	Continuous
10	hot	number of ``hot" indicators	Continuous
11	num_failed_logins	number of failed login attempts	Continuous
13	num_compromised	number of ``compromised" conditions	Continuous
16	num_root	number of ``root" accesses	Continuous
17	num_file_creations	number of file creation operations	Continuous
18	num_shells	number of shell prompts	Continuous
19	num_access_files	number of operations on access control files	Continuous
22	is_guest_login	1 if the login is a ``guest" login; 0 otherwise	Symbolic
23	count	number of connections to the same host as the current connection in the past two seconds	Continuous
24	srv_count	number of connections to the same service as the current connection in the past two seconds	Continuous
36	dst_host_same_src_port_rate	same_src_port_rate for destination host	Continuous

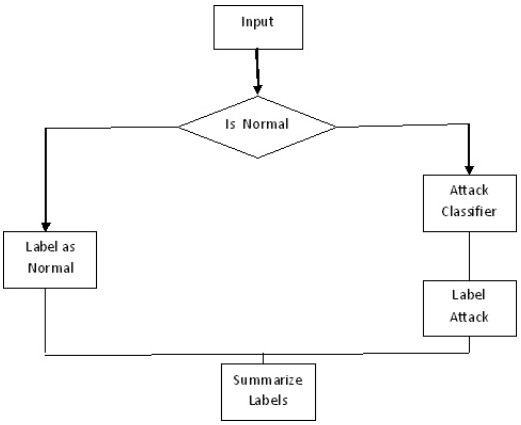

Figure 4: Simple Algorithm of Intrusion Detection System

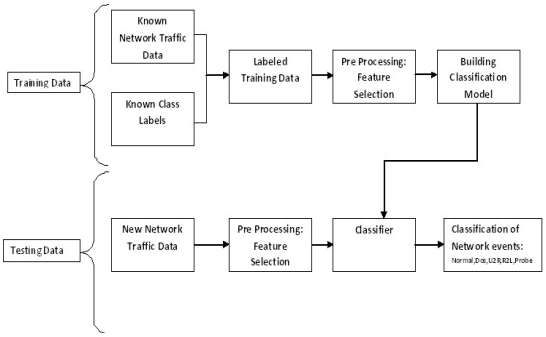

Figure 5: Simple Structure of Training & Testing clustring

A variety of attacks incorporated in the dataset fall into following five major categories:

Denial of Service (Dos) **Attacks:** A denial of service attack is an attack where the attacker constructs some computing or memory resource fully occupied or unavailable to manage legitimate requirements, or reject legitimate users right to use a machine.

Probes: Probing is a category of attacks where an attacker examines a network to collect information or discover well-known vulnerabilities. These network investigations are reasonably valuable for an attacker who is staging an attack in future. An attacker who has a record, of which machines and services are accessible on a given network, can make use of this information to look for fragile points

User to Root (U2R) **Attacks:** User to Root exploits are a category of exploits where the attacker initiate by accessing a normal user account on the system (possibly achieved by tracking down the passwords, a dictionary attack, or social engineering) and take advantage of some susceptibility to achieve root access to the system.

Remote to User (R2L) **Attacks:** A Remote to User attack takes place when an attacker who has the capability to send packets to a machine over a network but does not have an account on that machine, makes use of some vulnerability to achieve local access as a user of that machine [8].

As per the KDD cup dataset these are four major categories of network attacks these as show in Table 2.

Table 2: Various Types of Attacks Described in Four Major Categories

Category	Attack Categories
Normal	Normal
dos	apacha2
	back
	land
	mailbomb
	netpune
	pod
	processtable
	smurf
	teardrop
	udpstorm
u2r	buffer_overflow
	httprunnel
	loadmodule
	perl
	ps
	rootkit
	sqlattack
	xterm
r2l	ftp-write
	guess_password
	imap
	multihop
	named
	phf
	sendmail
	snmpgetattack
	snmpguess
	spy
	warezclient
	warezmaster
	worm
	xlock
	xsnoop
Probe	lpsweep
	mscan
	namp
	portsweep
	saint
	satan

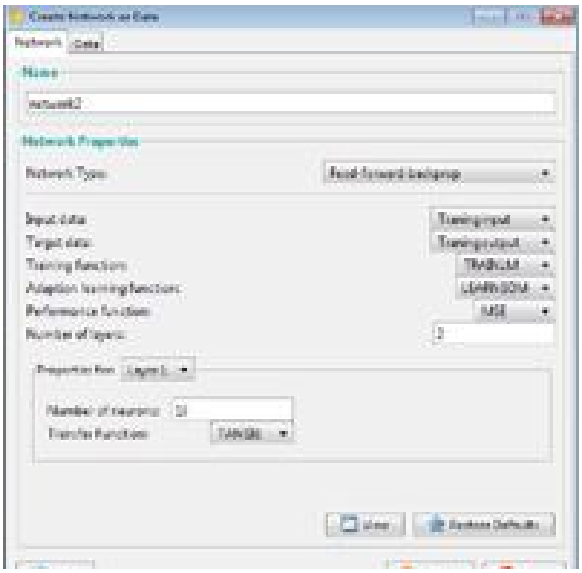

Figure 6: Various Parameters set for Training

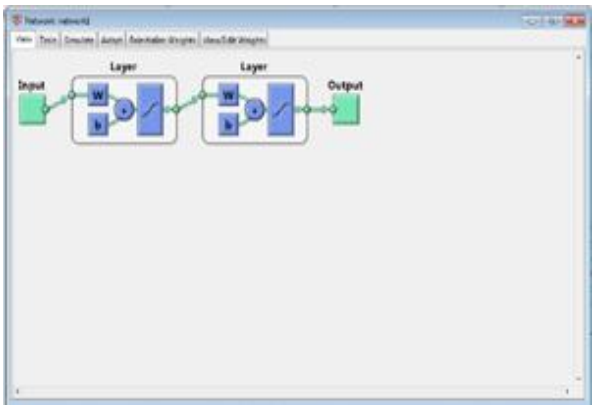

Figure 7: Neural Network Architecture

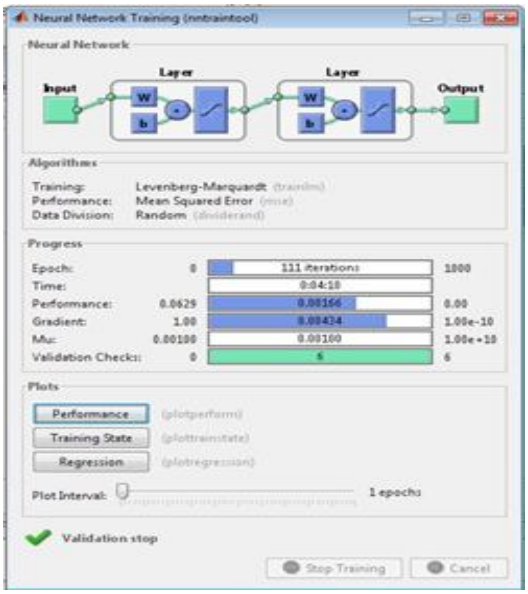

Figure 8: Neural Network Training

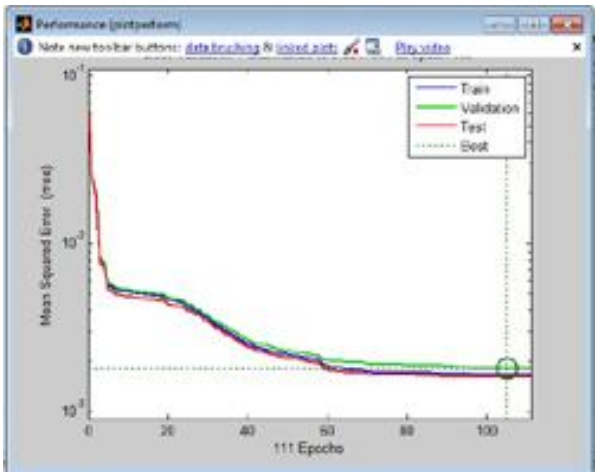

Figure 9: Training Performance of the Network

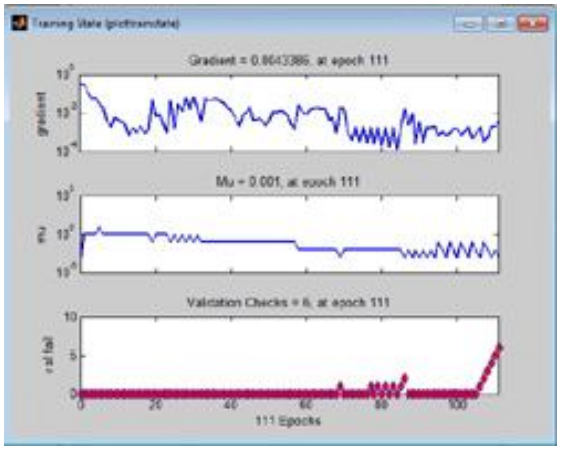

Figure 10: Training State

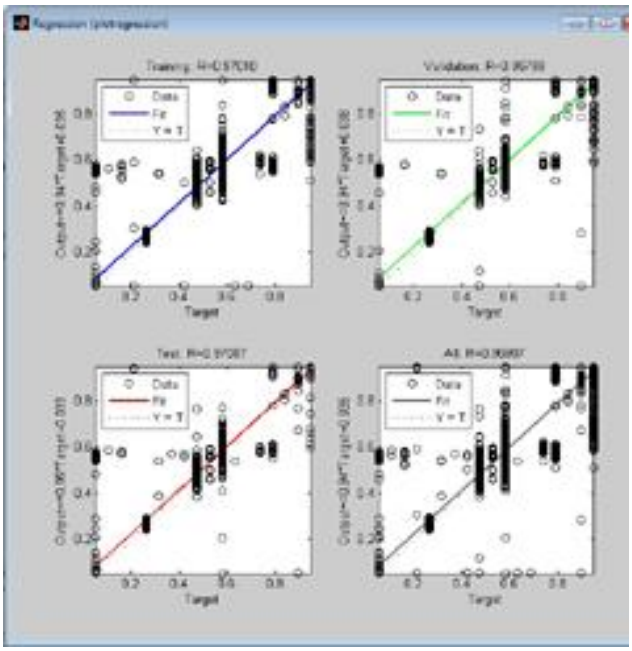

Figure 11: Regression

In the experiment, KDD 99 dataset was selected evaluation. There are total 41 features and according to literature Survey we experiment only 19 selected attributes in this research worked for. And to show comparison of different datasets for differently. complete KDD99 train dataset to reduce the number of features that can best describe our output class and to reduce the size of dataset vertically and complexity involved. The reduced dataset with lessened features is removed off all duplicate values, leading to reduction in number of records. This reduces the size of dataset horizontally.Normalization is applied that helps in bringing the record values within same range in neural networks using min/max formula.

$$NewV = V - MinX / MaxX – MinX$$

And select 95837 records then divide 84971 records for Training and 10866 records testing then use MATLAB for training Neural network FFNN algorithms with numbers of 5, 10, 15, 20, 25 & 30 neurons with 2 Layer are applied for training and simulation consecutively and results are stored. The network and training properties were set same for all the experements so that results can be compared on similar parameters:

VII. RESULT AND DISCUSSION

The functions in MS-Excel are used to calculate all evaluation measures and comparisons among results of all algorithms used.

Table 3: Number and distribution of Training & Testing dataset

Categories of Attacks	Training Dataset	Testing Dataset
Normal	40884	5480
dos	38599	4249
prob	3276	694
u2r	597	120
r2l	1615	323

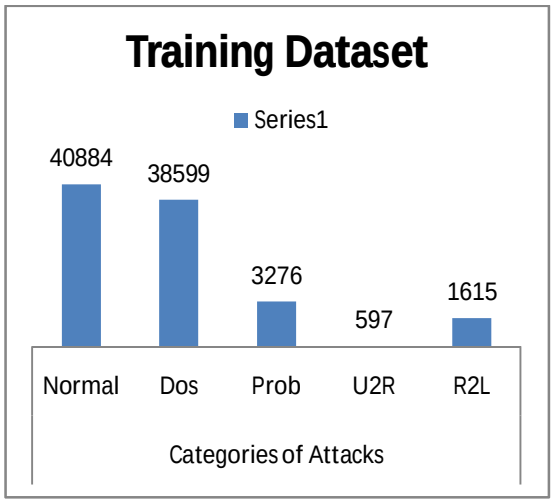

Figure 12: Number of Instance in Training Dataset

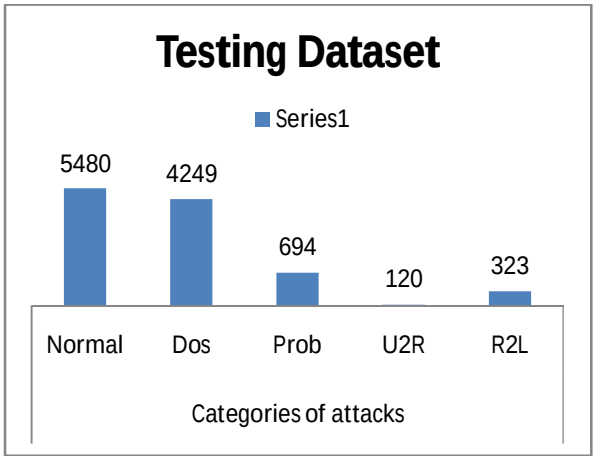

Figure13: Number of Instance in Testing Dataset

Experiments were done repeatedly by using different number of neurons 5,10,15,20,25&30 with 2 layers in each iteration. The results are compared for each neuron and the best result 97.97% is considered for the proposed work. The results are as given below:

Table 4: Test Accuracy for Numbers of different Neurons

S.No.	Technique	No. of Neurons	No. of Layers	Detection Rate(%)
1.	FFNN	5	2	94.77
2.	**FFNN**	**10**	**2**	**97.97**
3.	FFNN	15	2	81.31
4.	FFNN	20	2	97.16
5.	FFNN	25	2	87.21
6.	FFNN	30	2	73.44

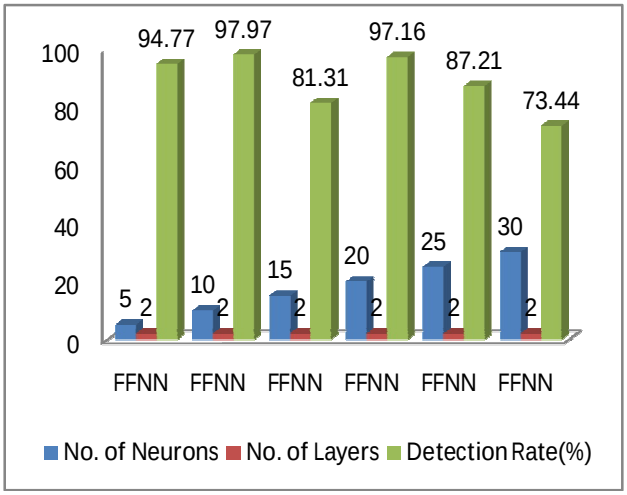

Figure 14: Graphical Representation for Numbers of different Neurons

From the table below it is proved that our proposed number of neurons 10 & number of Layers 2 is better in detection rate on the same dataset over different classifiers referenced in proposed technique respectively.

Table 5: Test Accuracy for Different Algorithm

S.No.	Technique	Detection Rate (%)
1.	Cascade Forward Back Drop	90.5
2.	Feed Forward Back Propagation	97.9
3.	NARX	59.1

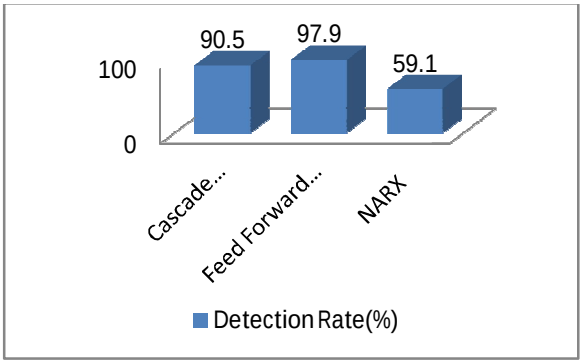

Figure 15: Graphical Representation for Different Algorithm

The results and analysis it is found that Feed Forward Neural Network with 10 Neurons has been best in detection rate and accuracy over other neural network algorithms.

VIII. COMPRESSION RESULT OF IDS ON KDD 99

After experiments we compared various published result to my experimental result on the same datasets show in Table 6. It was found that our IDS detection rate is competitive with the other detection rate. Also our detection rate is much better than others, so it can be said that the proposed IDS found 97.97% successful detection rate using FFNN with number of neurons 10 & number of layers 2 is better in the same dataset.

Table 6: Compression for Intrusion Detection Systems on KDD Cup 99

Research	**ANN type**	**Database**	**% of Successful Detection Rate**
Cannady, 1998 [9]	MLFF	Real Secure™ network monitor	91%
Moradi.2004 [10]	2 hidden layers MLP	KDD99	91%
Siddiqui, 2004 [11]	Back propagation and fuzzy ARTMAP	KDD99	81.37% for BP and 80.52% for fuzzy ARTMAP (overall PSC = 80.945)
Sheikhan, 2009 [12]	Fuzzy AR	KDD99 (15000)	91 %
Sheikhan, 2009 [12]	K-NN	KDD99 (15000)	91 %
Sheikhan, 2009 [12]	Data mining	KDD99 (15000)	80%
Panda. 2010 [13]	Multinomial Naive Bayes + N2B	NSL-KDD	38.89 %
Chhavi Goel 2015[14]	FFNN	NSL-KDD	96.31%
Proposed IDS	**FFNN**	**KDD99**	**97.97%**

IX. CONCLUSION

In previous years, many soft computing techniques such as FFNN, SOM, ANN, BPNN etc and many more have been used. In this proposed work we present a new intrusion deduction approach based on ANN. The Feed Forward Neural Network provides better accuracy over other neural network function. Selection and combination of neurons and layers methods apply in this research and training and simulated using the MATLAB and KDD 99 dataset for evaluating the performance of purposed system and the purposed methods is effective in deducting various intrusions in computer networks. Techniques can be applied to improve better accuracy Combination of Feed Forward Neural Network with Number of Neurons 10 and 2 layers provides the accuracy 97.97% thus to prove a better accuracy rate that the purposed techniques is used.

REFERENCES

[1] Norouzian M.R., Merati. S., "Classifying Attacks in a Network Intrusion Detection System Based on Artificial Neural Networks" Proceedings of the Advanced Communication Technology (ICACT), 2011 13th International Conference on Publication Year: 2011 , Page(s): 868 - 873

[2] B. Abdullah, I. Abd-alghafar, Gouda I. Salama & A. Abd-alhafez, (2009) "Performance Evaluation of a Genetic Algorithm Based Approach to Network Intrusion Detection System", 13th International Conference on Aerospace Sciences and Aviation Technology (ASAT), May 26-28.

[3] J. Gomez & D. Dasgupta, (2002) "Evolving Fuzzy Classifiers for Intrusion Detection", IEEE Proceedings of the IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY.

[4] "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering" Gang Wang a,b,*, Jinxing Hao b, Jian Mab, Lihua Huang a School of Management, Fudan University, Shanghai 200433, PR China
b Department of Information Systems, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong Expert Systems with Applications xxx (2010) xxx–xxx

[5] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani.: "A Detailed Analysis of the KDD CUP Data Set". In: Second IEEE Symposium on CISDA, pp. 1-6. IEEE, Ottawa ON (2009)

[6] Wanli Ma, Dat Tran and Dharmendra Sharma.: "A Study on the Feature Selection of Network Traffic for Intrusion Detection Purpose". In: Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on, pp. 245-247, Taiwan June 17-20 (2008)

[7]. The KDD99 https://archive.ics.uci.edu/ml/machine-learning-databases/kddcup99-mld/kddcup99.html

[8] "NETWORK INTRUSION DETECTION SYSTEM USING FUZZY LOGICR". Shanmugavadivu Assistant professor, Department of Computer Science PSG College of Arts & Science, Coimbatore-14 R. Shanmugavadivu et al./ Indian Journal of Computer Science and Engineering (IJCSE) ISSN : 0976-5166 Vol. 2 No. 1

[9]. Cannady J. (1998). " Artificial neural networks for misuse detection" .Proceedings of the 1998 National Information Systems Security Conference (NISSC'98), 443-456, Arlington, VA.

[10]. Moradi, M.; and Zulkernine, M. (2004). "A neural network based system for intrusion detection and classification of attacks". IEEE International Conference on Advances in Intelligent Systems - Theory and pplications, Luxembourg-Kirchberg, Luxembourg.

[11]. Siddiqui, M.A. (2004). "High performance data mining techniques for intrusion detection". MSc. Thesis, University of Engineering & Technology,School of Computer Science, College of Engineering & Computer Science at the University of Central Florida.

[12]. Sheikhan, M.; and Gharavianm, D. (2009). "Combination of Elman neural network and classification-based predictive association rules to improve computer networks security", World Applied Sciences Journal, 7, Special Issue of Computer & IT, 80-86

[13]. Panda, M. (2010). "Discriminative multinomial Naïve Bayes for network intrusion detection". 2010 Sixth International Conference on Information Assurance and Security (IAS), 5-10.

[14]. Chhavi Goel and Arun Sharma,(2015)"Network Intrusion Detection Using Artificial Neural Networks" CSI-2015 50thGolden Jubilee Annual Convention on "Digital Life", December, 2015, New Delhi.

[15] Brijpal Singh & Prof. Dr. Anil A. Ahlawat, (2013), "Intrusion detection of Network AttacksUsing Artificial Neural Networks & Fuzzy Logic", International Journal of Engineering & Management Technology IJEMT (March) 2013, ISSN: 2320-7043

[16] Anil Ahlawat et.al, "A Novel Self-Organizing Map (SOM) learning algorithm with nearest and farthest neurons",Allexandria Engineering Journal(Elsevier),Vol 53,827-831,October 2014

BRIJPAL SINGH, Research Scholar Department of Computer Science, Mewar University. Chittorgarh, Rajasthan, India,.

DR. ANIL KR. AHLAWAT, Department of Computer Science, Krishna Institute of Engineering and Technology, Ghaziabad, UP, India,
Research / Specialisation Neural Network, Algorithm Design, Device Modeling and Soft Computing Technique

