DEEP NEURAL NETWORK MODEL FOR INTRUSION DETECTION SYSTEM

Agarsha Merin John , Divya James

Mtech in Network Engineering Rajagiri School of Engineering & Technology,Assistant Professor Rajagiri School of Engineering &Technology

Department of information technology, Department of information technology, Kerala, India.

Abstract : Intrusion Detection System (IDS) can distinguish rising assaults and a few peculiarity discovery plans. There is a need to ensure against any irregular practices and assaults that endeavor to damage the respectability, classification or accessibility of valuable data. The vast majority of the intrusion detection system uses information mining or AI methods to get familiar with the contrasts among ordinary and vindictive practices. The profound learning strategies in the intrusion detection system (IDS) can be utilized to improve detection and can accomplish higher characterization precision and secure the system from different sorts of assaults. The AI calculations that can be utilized to identify precious assaults are support vector machines (SVMs), K-NN. These AI classifiers can be utilized to foresee between two potential results (for example vindictive and non-noxious system traffic). In Deep learning, a Deep neural system (DNN) can be utilized to create a successful intrusion detection system to identify and characterize capricious digital assaults and perform better in contrast with AI classifiers. This venture proposes an examination between various sorts of deep learning calculations dependent on exactness, review, and precision with various datasets.

Index Terms- Machine Learning, Deep Learning, Intrusion Detection system.

I. INTRODUCTION

Intrusion Detection alludes to the issue of observing and separating such system streams and exercises from the ordinarily expected conduct of system which can unfavorably affect the security of data frameworks. The quest for solid arrangements by Governments and associations to shield their data resources from unapproved exposures and illicit gets to has brought intrusion discovery and anticipation at the front line of the data security scene. The utilization of the system is changing at an exceptionally quick rate. The measure of system traffic volume is additionally quickly expanding. Checking system traffic for inconsistency identification is anything but another idea as there are numerous kinds of assaults other than the infection and malware. Those assaults can affect the host PCs, yet besides the system execution essentially, or in the direst outcome imaginable, it can stop some system administrations. System traffic oddity identification is expected to recognize and forestall the assault. In this way, the location of innovation must be exceptionally productive and viable. With the ceaseless advancement and utilization of information mining and AI innovation, interloper recognition innovation analysts have started to apply these two advances to the interruption identification framework. It is attractive to distinguish the irregular conduct by mining the different social qualities of the system information, creating the ordinary conduct form, and afterward coordinating the new information after the component extraction. With the improvement of innovation, new assaults are continually rising, In this manner, the intrusion detection system needs to have a solid capacity to adjust and learn. In the current research, the issue of over-fitting has not been successfully comprehended. To tackle the issue of over-fitting and structure advancement calculations, and to consider the consequences of four sorts of assault identification, this paper proposes an improved DNN model dependent on the investigation of profound figuring out how to demonstrate its viability.

II. LITERATURE REVIEW

Bayan Alsughayyir et.al built up a network attack detection system using deep learning based on the autoencoder.With the advancement of systems, the quantity of system assaults is expanding exponentially. The requirement for a system security framework is turning out to be increasingly more significant since there is a great deal of delicate data being put away and sent through the Web. We have to locate the most ideal approaches to shield our frameworks from any irregular practices that endeavor to abuse the trustworthiness, classification or accessibility of valuable data. Various strategies have been utilized either to forestall or to identify assaults. In this paper, a Deep Learning (DL) approach is utilized that can make a superior and increasingly viable Intrusion Detection System (IDS). The planned methodology depends on characterizing ordinary conduct on the system from abnormality conduct. The proposed approach beats all the traditional methodologies with an exactness of 99% for preparing and 91.28% for the testing stage, exhibiting its potential for constant and useful applications [1]. Vinayakumar R et.al proposed a deep learning approach for the intelligent intrusion detection system. In this paper, a deep neural system (DNN), a sort of deep learning model is investigated to create adaptable and viable IDS to distinguish and arrange unexpected and unusual digital assaults. The ceaseless change in organizing conduct and fast advancement of assaults makes it important to assess different datasets that are produced throughout the years through static and dynamic methodologies. This kind of study encourages recognizing the best calculation which can adequately work in identifying future digital assaults. An extensive assessment of analyses of DNNs and other old-style AI classifiers have appeared on different openly accessible benchmark malware datasets. The ideal system parameters and system topologies for DNNs are picked through after hyperparameter determination strategies with KDDCup 99 dataset. All trials of DNNs are hurried to 1,000 ages with learning rates differing in the range [0.01-0.5]. The DNN model which performed well on KDDCup 99 is applied to different datasets, for example, NSL-KDD, UNSW-NB15, Kyoto, WSN-DS and CICIDS 2017 to lead the benchmark. Our DNN model learns the theoretical and high dimensional element portrayal of the IDS information by passing them into many concealed layers. Through thorough exploratory testing, it is affirmed that DNNs perform well in contrast with the traditional AI classifiers. At long last, we propose an exceptionally adaptable and half breed DNNs structure called Scale-Hybrid-IDS-Alert Net (SHIA) which can be utilized continuously to successfully screen the system traffic and host-level occasions to proactively alarm conceivable digital assaults [2],[6].Hongpo Zhang et.al proposed a deep learning-based approach for network intrusion detection using denoising auto-encoder (DAE) is executed. A weight reduction work is incorporated which helps in choosing a set number of significant highlights for lessening highlight dimensionality. The chose information is then ordered utilizing a multilayer perceptron (MLP) as the classifier. Examinations are led utilizing the UNSW-NB dataset. Results show that the component determination yields good recognition execution with low memory and figuring power prerequisites. Denoising auto-encoder is an extraordinary auto-encoder that gets tainted information as information and is prepared to foresee unique information as to its yield. The proposed approach comprises two profound learning-based parts to perform include determination and arrangement. The determination is performed by DAE where a key procedure is to add loads to its misfortune work which improves choice outcomes by putting more accentuation on assault tests. The grouping is finished by MLP with the assistance of a limited number of parameters while as yet accomplishing the elite. The primary preferred position is that right off the bat, highlight determination for IDS is improved utilizing weighted misfortune work since highlights that portray assault tests are chosen wisely giving better identification execution. Besides, the classifier, for example, MLP is utilized because after component determination includes dimensionality is diminished altogether and henceforth key utilization of MLP gives superior even with fewer parameters. The general exactness of the methodology is high 98.80 % with an F-score of 0.952, an accuracy of 95.98 % and a review of 94.43 %. The element determination proportion is 5.9% choosing 12 out of 202 highlights of which 2 have a place with a similar class making the chose highlights to be 10 [3]. Nathan Shone et.al proposed a deep learning approach to network intrusion detection.Network intrusion detection systems (NIDS) assume a vital job in protecting PC systems. In any case, there are concerns in regards to the achievability and supportability of current methodologies when confronted with the requests of present-day systems. All the more explicitly, these worries identify with the expanding levels of required human association and the diminishing degrees of location exactness. This paper proposed a non-symmetric deep autoencoder (NDAE) for unaided element learning. Moreover, it additionally proposes our novel deep learning grouping model built utilizing stacked NDAE. Our proposed classifiers have been actualized in the illustrations preparing unit (GPU)- enabled tensor flow and assessed utilizing the benchmark KDD Cup '99 and NSL-KDD datasets. Promising outcomes have been acquired from our model up to this point, exhibiting upgrades over existing methodologies and the solid potential for use in current NIDS [4]. Gozde Karatas et.al proposed deep learning in intrusion detection systems. As of late, because of the rise of an unlimited correspondence worldview and an expanded number of organized advanced gadgets, there is a developing worry about cybersecurity which attempts to protect either the data or the correspondence innovation of the framework. Gatecrashers find new assault types step by step, in this way to forestall these assaults initially they should be distinguished effectively by the pre-owned intrusion detection systems (IDS), and afterward, legitimate reactions ought to be given.IDSs, which assume a pivotal job in the security of the system, comprising of three primary segments: information assortment, include choice/transformation, and choice motor. The last part of legitimately influences the effectiveness of the framework and the utilization of AI systems is one of the most encouraging exploration zones. As of late, deep learning has developed as another methodology that empowers the utilization of Large Information with low preparation time and a high precision rate with its unmistakable learning system. Therefore, it has been begun to use in IDS frameworks. In this paper, it is expected to study a deep learning-based intrusion detection system approach by making a near work of the writing and by giving the foundation information either in deep learning calculations or in intrusion detection systems [5],[6][7][8].

III. SYSTEM ARCHITECTURE

The key of intrusion detection is to separate the attributes of system conduct and to portray the contrast between ordinary conduct and system assault conduct. At that point, we plan the order model to include space to distinguish. System abnormality recognition, for the most part, incorporates two sections: the development arrangement model and intrusion identification. Fig. shows an outline of the intrusion detection system. The intrusion detection system is separated into two sections. The initial segment is the intrusion model preparing, and another part is testing. Both the preparation set and the test set should be preprocessed, which is the sign component digitization and the advanced mark standardization. After the model pre-preparing, switch change and cycle to the last combination, the model of a deep neural system is for the most part made out of completely associated layers, dropout layer, and the delicate max layer. We can get a more precise outcome than a shallow neural system by utilizing the prepared model for testing with a test set.

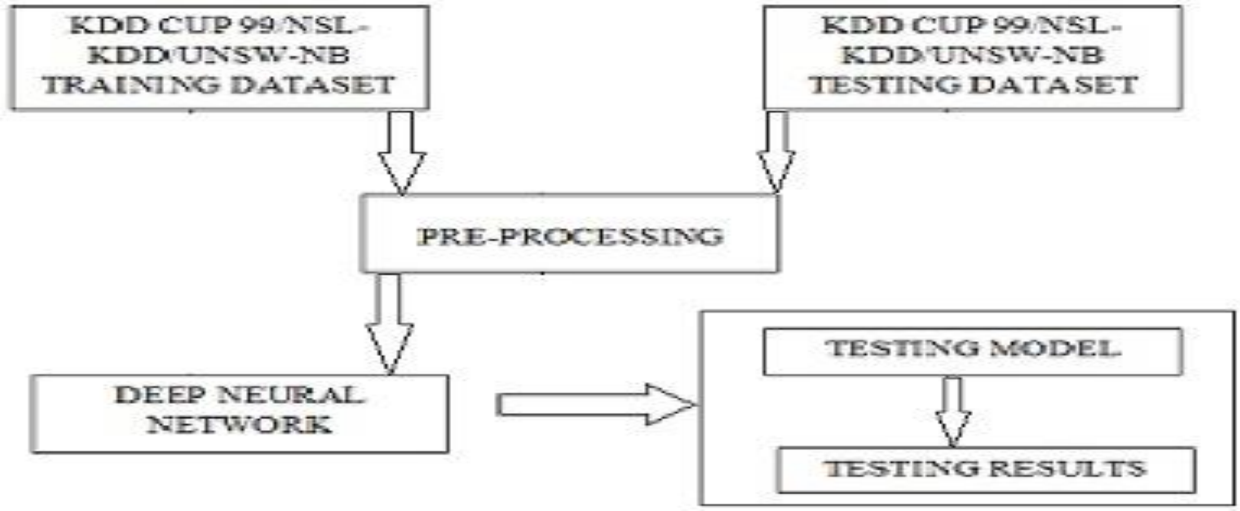

KDD CUP 99/NSL-KDD/UNSW-NB TRAINING DATASET
KDD CUP 99/NSL-KDD/UNSW-NB TESTING DATASET
PRE-PROCESSING
DEEP NEURAL NETWORK
TESTING MODEL
TESTING RESULTS

Fig a Framework design.

A DATASET PRE-PROCESSING

Pre-Processing alludes to the changes applied to our information before encouraging it to the calculation. Information Preprocessing is a system that is utilized to change over the crude information into a spotless informational index. In python, sci-kit learn library has pre-constructed usefulness under sklearn.preprocessing. Content may contain numbers, extraordinary characters, and undesirable spaces. Contingent on the issue we face, we might need to evacuate these extraordinary characters and numbers from the content. Fundamentally in this progression, the dataset needs to experience a cleaning procedure to expel copy records, as the NSL KDD/KDD CUP 99/UNSW-NB dataset was utilized which has just been cleaned.

ALGORITHM

Step 1) Import Libraries that will be needed in the program.

```
Import numpy as np
import matplotlib.pyplot as plt
import pandas as pd
```

Step 2) Import the Dataset.

```
dataset = pd.read_csv('kdd.csv')
```

Step 3) Classifying the dependent and Independent Variables.

```
# Splitting the attributes into independent and dependent attributes
X = dataset.iloc[:, :-1].values # attributes to determine dependent variable / Class
Y = dataset.iloc[:, -1].values # dependent variable / Class
```

Step 4) Taking care of missing data in dataset.

```
# handling the missing data and replace missing values with nan from numpy and replace with mean of all the other values
imputer = SimpleImputer(missing_values=np.nan, strategy='mean') imputer = imputer.fit(X[:, 1:])
X[:, 1:] = imputer.transform(X[:, 1:])
```

Step 5) Encoding categorical data.

```
# encode categorical data
from sklearn.preprocessing import LabelEncoder, OneHotEncoder
labelencoder_X = LabelEncoder()
X[:, 0] = labelencoder_X.fit_transform(X[:, 0])
```

```
onehotencoder = OneHotEncoder(categorical_features=[0])
X = onehotencoder.fit_transform(X).toarray()labelencoder_Y = LabelEncoder()
Y = labelencoder_Y.fit_transform(Y)
```

Step 6) Splitting the Dataset into Training set and Test Set.

```
# splitting the dataset into training set and test set
X_train, X_test, Y_train, Y_test = train_test_split(X, Y, test_size=0.2, random_state=0).
```

B INTRUSION DETECTION MODEL

A DNN model (Fig. b) with four concealed layers and 100 shrouded units was utilized for the intrusion detection mode of this examination as its arrangement calculation.

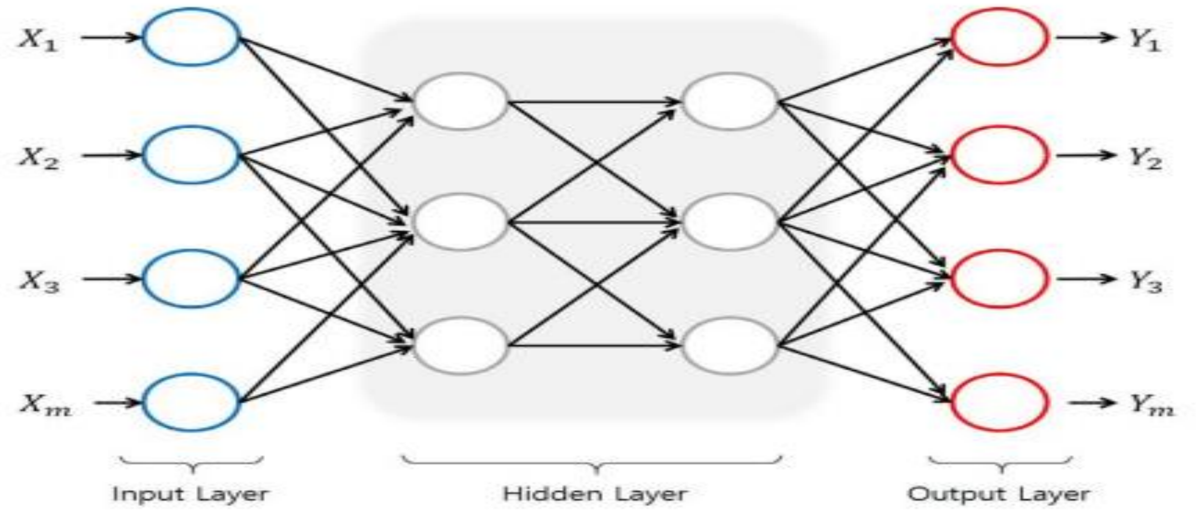
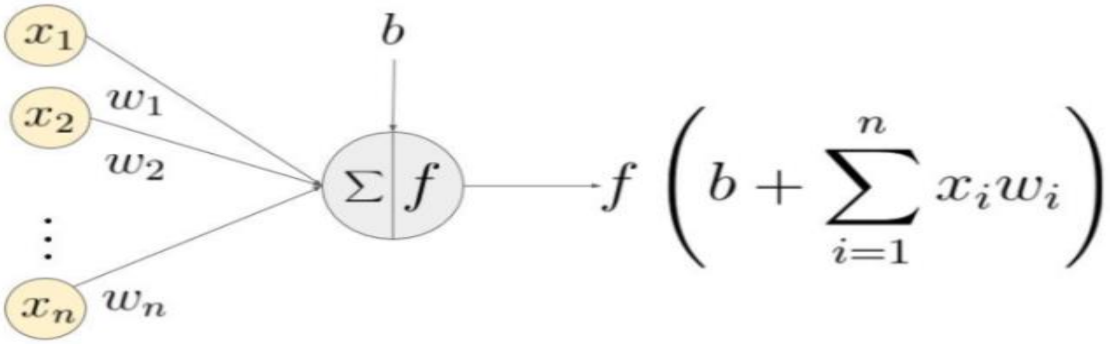


Fig b Intrusion Detection Model

B.1 ACTIVATION FUNCTION

The investigation utilized the ReLU(Rectified Linear Unit) work as the initiation capacity of the concealed layers. This is a non-direct initiation work that can improve the model's presentation as it communicates a muddled grouping limit superior to anything a straight enactment work. The actuation work chooses whether a neuron ought to be enacted or not by computing the weighted whole and further including predisposition with it. The reason for the initiation work is to introduce non-linearity into the yield of a neuron. We know, the neural system has neurons that work in correspondence of weight, predisposition, and their particular initiation work. In a neural system, we would refresh the loads and inclinations of the neurons dependent on the blunder at the yield. This procedure is known as back-propagation. Actuation capacities make the back-proliferation conceivable since the inclinations are provided alongside the mistake to refresh the loads and predispositions. A neural system without an actuation work is only a direct relapse model. The actuation work does the non-direct change to the info making it competent to learn and perform increasingly complex assignments.

- Equation :- A(x) = max(0,x). It gives a yield x if x is sure and 0 in any case.
- Value Range :- [0, inf)
- Nature:- non-straight, which implies we can without much of a stretch backpropagate the blunders and have multiple layers of neurons being initiated by the ReLU work.
- Uses:- ReLu is less computationally costly than tanh and sigmoid because it includes less difficult numerical tasks. At a time just a couple of neurons are actuated making the system meager making it effective and simple for calculation.



An example of a neuron showing the input (x_1 - x_n), their corresponding weights (w_1 - w_n), a bias (b) and the activation function f applied to the weighted sum of the inputs.

Fig b.1 Activation Function.

B.2 BACK PROPAGATION

The examination additionally utilized the versatile minute (Adam) streamlining agent, a stochastic enhancement strategy for DNN learning. Adam figures the versatile learning rate for each weight with the goal that the system could prepare quicker and forestall over-fitting. The Backpropagation neural organize is a multilayered, feedforward neural arrange and is by a long shot the most broadly utilized. It is additionally viewed as one of the least complex and most broad strategies utilized for supervised training of multilayered neural systems. Backpropagation works by approximating the non-direct connection between the input and the output by altering the weight values inside. It can additionally be summed up for the information that is excluded from the training designs. By and large, the Backpropagation organize has two phases, training and testing. During the preparation stage, the system is "appeared" test inputs and the right orders. For instance, the info may be an encoded image of a face, and the yield could be spoken to by a code that relates to the name of the individual. A further note on encoding data - a neural system, as most learning calculations, needs to have the sources of info and yields encoded by a self-assertive client characterized plot. The plan will characterize the system design so once a system is prepared, the plan can't be changed without making another net. Correspondingly, there are numerous types of encoding the system reaction. The accompanying figure shows the topology of the Backpropagation neural system that incorporates an information layer, one hidden layer, and a yield layer. It ought to be noticed that Backpropagation neural systems can have more than one concealed layer.

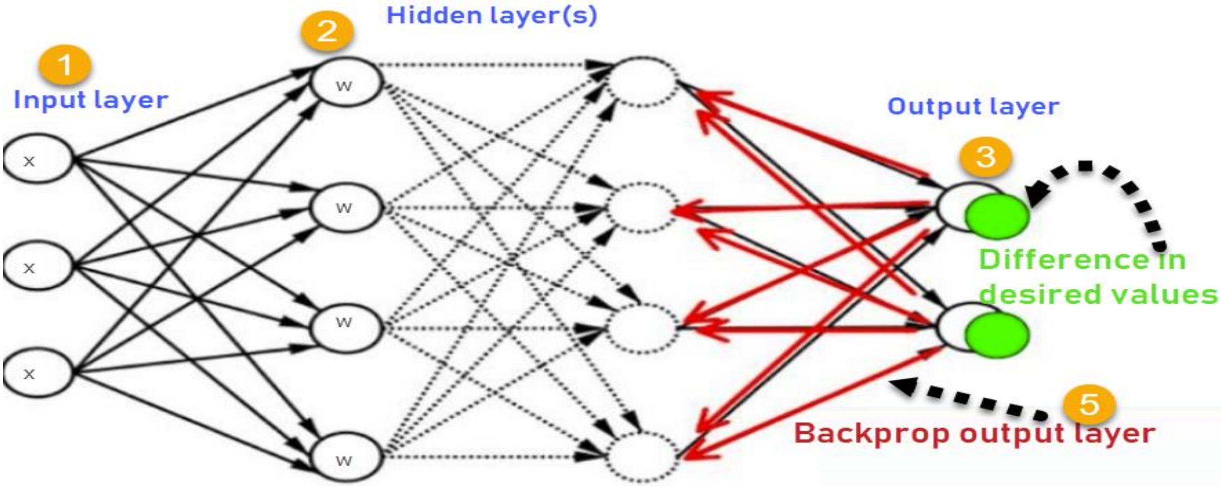


Fig B.2 Back Propagation.

B.2.1 WORKING OF BACK PROPAGATION

- Inputs X, arrive through the preconnected path
- Input is modeled using real weights W. The weights are usually randomly selected.
- Calculate the output for every neuron from the input layer, to the hidden layers, to the output layer.
- Calculate the error in the outputs:

ErrorB = Actual Output - Desired Output.

- Travel back from the output layer to the hidden layer to adjust the weights such that the error is decreased.

The activities of the Backpropagation neural systems can be isolated into two steps: feedforward and Backpropagation. In the feed-forward advance, information design is applied to the info layer and its impact engenders, layer by layer, through the system until the yield is created. The system's real yield esteem is then contrasted with the normal yield, and a mistake signal is figured for every one of the yield hubs. Since all the shrouded hubs have, somewhat, added to the mistakes obvious in the yield layer, the yield blunder signals are transmitted in reverse from the yield layer to every hub in the concealed layer that promptly added to the yield layer. This procedure is then rehashed, layer by layer, until every hub in the system has gotten a mistake signal that depicts its relative commitment to the general blunder. When the mistake signal for every hub has been resolved, the blunders are then utilized by the hubs to refresh the qualities for every association loads until the system meets an express that permits all the preparation examples to be encoded. The Backpropagation calculation searches for the base estimation of the error function in weight space utilizing a procedure called the delta rule or gradient plummet. The loads that limit the mistake work are then viewed as an answer to the learning issue. The system conduct is comparable to a human that is demonstrated a lot of information and is approached to characterize them into predefined classes. As a human, it will think of "hypotheses" about how the examples fit into the classes. These are then tried against the right yields to perceive how exact the conjectures of the system are. Radical changes in the most recent hypothesis are shown by huge changes in the loads, and little changes might be viewed as minor acclimations to the hypothesis. There are additional issues concerning summing up a neural system. Issues to consider are issues related to under-preparing and over-preparing information. Under-preparing can happen when the neural system isn't sufficiently perplexing to recognize an example in a confounded informational collection. This is generally the aftereffect of systems with scarcely any concealed hubs that it can't precisely speak to the arrangement, subsequently under-fitting the information.

C PREDICTION AND EVALUATION

The investigation results on the NSL-KDD/KDD Cup 99/UNSW-NB dataset show the test execution of the intrusion detection system. This procedure more than once constructs a model putting the component aside and afterward rehashing the procedure with the rest of the highlights until all highlights present in the dataset are depleted. At that point, the exactness is determined for each dataset of the DNN calculation to complete the examination. In assessment to gauge the different factual measures, the ground truth esteem is required. The ground truth made out of a lot of association records marked either normal or attack on account of double characterization. Let L and A alone the quantity of normal or attack association records in the test dataset, separately and the accompanying terms are utilized for deciding the nature of the grouping models:

- True Positive (TP) - the number of association records accurately ordered to the Ordinary class.
- True Negative (T N) - the number of association records accurately ordered to the Assault class.
- False Positive (F P) - the number of Typical association records wrongly ordered to the assault association record.
- False Negative (FN) - the quantity of Assault association records wrongly ordered to the typical association record.

Accuracy

It evaluates the proportion of the accurately perceived association records to the whole test dataset. On the off chance that the precision is higher, the deep learning model is better (precision ∈ [0, 1]). exactness fills in as a decent measure for the test dataset that contains adjusted classes and characterized as follows

$$\text{Accuracy} = \frac{(TP+TN)}{(TP+TN+FP+FN)}$$

Fig c.1 Precision.

Precision

It appraises the proportion of the effectively-recognized assault association records to the quantity of all distinguished assault association records. On the off chance that the Accuracy is higher, the deep learning model is better (precision ∈ [0, 1]). Accuracy is characterized as follows

$$\text{Precision} = \frac{TP}{TP+FP}$$

Fig c.2 Accuracy

True Positive Rate (TPR)

It is additionally called a Recall. It appraises the proportion of the accurately characterized Assault association records to the absolute number of Assault association records. On the off chance that the TPR is higher, the deep learning model is better (TPR ∊ [0, 1]). TPR is characterized as follows

$$\text{Recall} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}}$$

$$= \frac{\text{True Positive}}{\text{Total Actual Positive}}$$

Fig c.3 Recall.

IV. CONCLUSION

System checking has been utilized broadly for security, crime scene investigation and abnormality discovery. The new headways in organizing the intrusion systems have made numerous issues, for example, volume, exactness, diversity, elements, low-recurrence assaults, versatility. The utilization of deep learning methods in intrusion detection systems can secure against unusual practices and assaults that endeavor to damage the honesty, secrecy or accessibility of helpful data. Utilizing deep learning frameworks for the intrusion detection system can improve the presentation and speed up. In deep learning, a deep neural system (DNN) can be utilized to create a successful intrusion detection system to identify and order eccentric digital assaults and perform better in contrast with AI classifiers. In this course, extraordinary deep learning-based calculations for the intrusion detection are talked about and contemplated in detail.

V. REFERENCES

[1] Bayan Alsughayyir, Ali Mustafa Qamar, Rehanullah Khan "Developing a Network Attack Detection System Using Deep Learning", International Conference on Computer and Information Sciences (ICCIS), April 2019.

[2] Vinayakumar R, Mamoun Alazab, Soman Kp, "Deep Learning Approach for Intelligent Intrusion Detection System", IEEE Transactions on Neural Networks, April 2019.

[3] Hongpo Zhang, Chase Q. Wu, Shan Gao "An Effective Deep Learning-Based Scheme for Network Intrusion Detection", 24th International Conference on Pattern Recognition (ICPR), August 2018.

[4] Nathan Shone, Tran Nguyen Ngoc, Vu Dinh Phai, Qi Shi, "A Deep Learning Approach to Network Intrusion Detection", IEEE transactions on emerging topics in computational intelligence, February 2018.

[5] Gozde Karatas, Onder Demir, Ozgur Koray Sahingoz "Deep Learning in Intrusion Detection Systems", International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, December 2018.

[6] Brian Lee, Sandhya Amaresh, Clifford Green "Comparative Study of Deep Learning Models for Network Intrusion Detection" Vol 1, No 1, SMU Scholar, 2018.

[7] Marzia Zaman,Chung-Horng Lung "Evaluation of Machine Learning Techniques for Network Intrusion Detection" IEEE 2018.

[9] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, Wang, C. "Machine Learning and Deep Learning Methods for Cybersecurity." IEEE 2018

[10] Shan Ding, Genying Wang "Research on Intrusion Detection Technology Based on Deep Learning" 3rd IEEE International Conference on Computer and Communications 2017.

[11] Jin Kim, Nara Shin, Seung Yeon Jo "Method of Intrusion Detection using Deep Neural Network" IEEE 2017.
[12] Md. Zahangir Alom , VenkataRamesh Bontupalli, and Tarek M. Taha "Intrusion Detection using Deep Belief Networks" IEEE 2015.