Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021: 3677-3686

Network Intrusion Detection System Using Deep Learning Perspective: A Survey

SabeehaAfzal[a], Anjna Jayant Deen[b]

[a] Student, Dual Degree Integrated Post Graduate Programme, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, 462033, India .
[b] Assistant Professor, Department of Computer Science and Engineering, University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, 462033, India .

Abstract:-
Network Intrusion Detection plays a very vital role in shielding a Network.However, there are apprehensions regarding the practicality and sustainability of current approaches when looked with the needs of modern networks. Elaborating it more, these concerns relate to the increasing levels of required human interaction in understanding and manipulating the datasetsthus resulting in decreasing levels of detection accuracy. In this paper we have tried to present various techniquesfor intrusion detection, which addresses these concerns. We have detailedvarious Deep Learning techniques with their evaluation using the benchmark KDD Cup '99 and NSL-KDD andUNSW-NB15 and CICIDS-2017 datasets. Promising results have been obtained from variousmodel, givingimprovements over existing approaches and the strong potential for use in modern NIDS. In this paper endeavours have been made to study Deep Learning model which enable NIDS operation within Modern Networks

Keywords:-Network security, Anomaly Detection, Deep Learning, ANN, RNN,DNN, LSTM, FFDNN, KDD Cup'99,NSL-KDD, CICIDS-2017.

Introduction: -

Network Intrusion detection system (NIDS) acts as a watchdog for our network and monitors anomalous activities. Although they monitor our network potentially from unwanted attacks, it's prone to create false alarms several times. Therefore with the growing technology our IDS must be updated enough to differentiate between Normal and anomalous data.

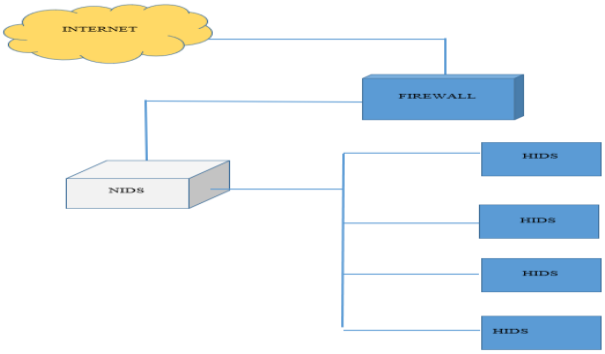

Figure 1:- IDS

Intrusion Detection can be classified in the following ways:-

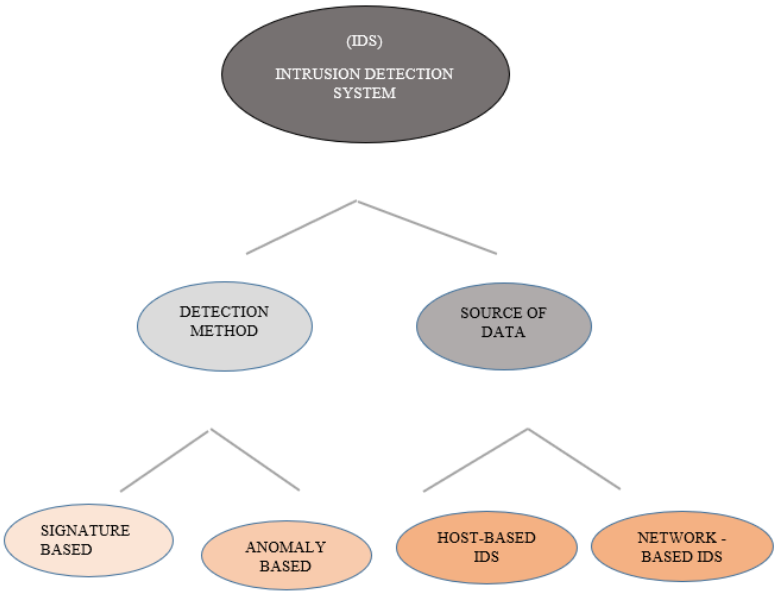

Figure 2:- IDS Classification.

There has been a lot of significant researches in the field of Network Security, even though we face challenges. As majority of researchers still prefer to work on signature based techniques in spite of the better one anomaly based technique; it because of various reasons such as Handling lot of training data, better processing capacities, and then arising of false alarms will lead to a point where believing in such a technique may lead to ineffective and erroneous detection. Therefore one of the major challenge is in the making of a strong and efficacious Network Intrusion Detection System (NIDS) which may deal with Modern attacks and handling of new data efficiently.

Some of the limitations that contribute to network security challenges are:-

- The increasing growth in the volume of the network data with increase in the use of internet: - Dealing with this big huge data size is very difficult, hence we need techniques that can examine these increasing data in an efficient way. More things keep on getting added to the network, hence more vulnerabilities.
- Lack of tool interoperability: - Only a few people know about the tools information and its handling. So a lot of people suffer from attackers.
- Insider's Attack: - An insider attack is a malicious attack which commits on a network or computer system by a person with sanctioned system access.
- Outdated hardware: - With the increase in the network data, we need good hardware's that can handle this huge data, do in depth monitoring in order to increase the accuracy of the model.

Handling different protocols and variety of modern networks data are significantly the major challenge in this era because this creates a high level of complexity and difficulty while attempting to differentiate between Normal and Anomalous data. Its solution opens space for exploring Zero-day Attacks.

In the recent years researcher's working on NIDS have mainly used Machine Learning[1] and Shallow learning techniques such as Naïve Bayes, Decision Trees and Support Vector Machines.

These techniques have been improving the accuracy of detection. However, they have certain limitations also such as Handling and interpreting the required data, which needs lots of human expert's interactions. Thereby these can be prone to a lot of errors. Similarly, a huge amount of training data is required for operation (with associated time overheads), which can become challenging in a heterogeneous and dynamic environment.

To overcome the said limitations, there is an Overwhelming demand and the researchers has moved their attention towards Deep Learning[2] in various domains. Deep learning is positioned as a branch of Machine Learning which in turn is a subset of Artificial Intelligence. In this we don't have to programme anything specifically. Deep learning models are proficient enough to focus on the required features themselves by acquiring little guidance from the programmer, and hence very helpful in solving the problem of dimensionality and handling huge dataset. Researchers have found out that this helps in faster identification of anomalies. In this paper efforts have been made to explain the role of Deep Learning in Intrusion Detection System.

Deep Learning:

After professor Hinton [3] put forward the theory of deep learning in 2006, Deep Learning static and technology went through an speedy rise in the field of Machine Learning. It's implemented with the help of neural networks (NN), and the idea behind this motivation is the biological Neurons (Brain cells). In this we don't have to explicitly programme anything, Deep Learning models are themselves capable to focus on required/accurate features by giving a little guidance by the programmer. Further they are very useful in solving the problem of Dimensionality.

Methods of Deep Learning are as:-

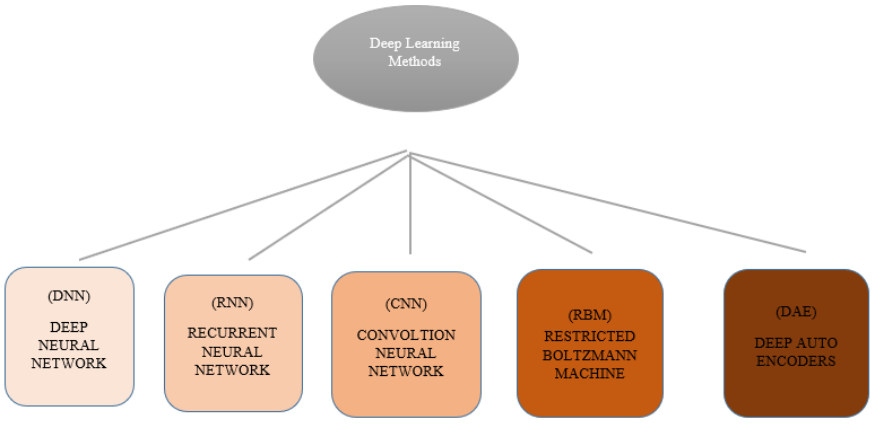

Figure 3:- Deep Learning Types.

1. Deep Neural Networks:-

It's a Neural Network that assimilates the difficulty up to a certain level i.e., several number of hidden layers are there in between the input and the output layers. All the layers are interconnected, and the output layer predicts the final result.

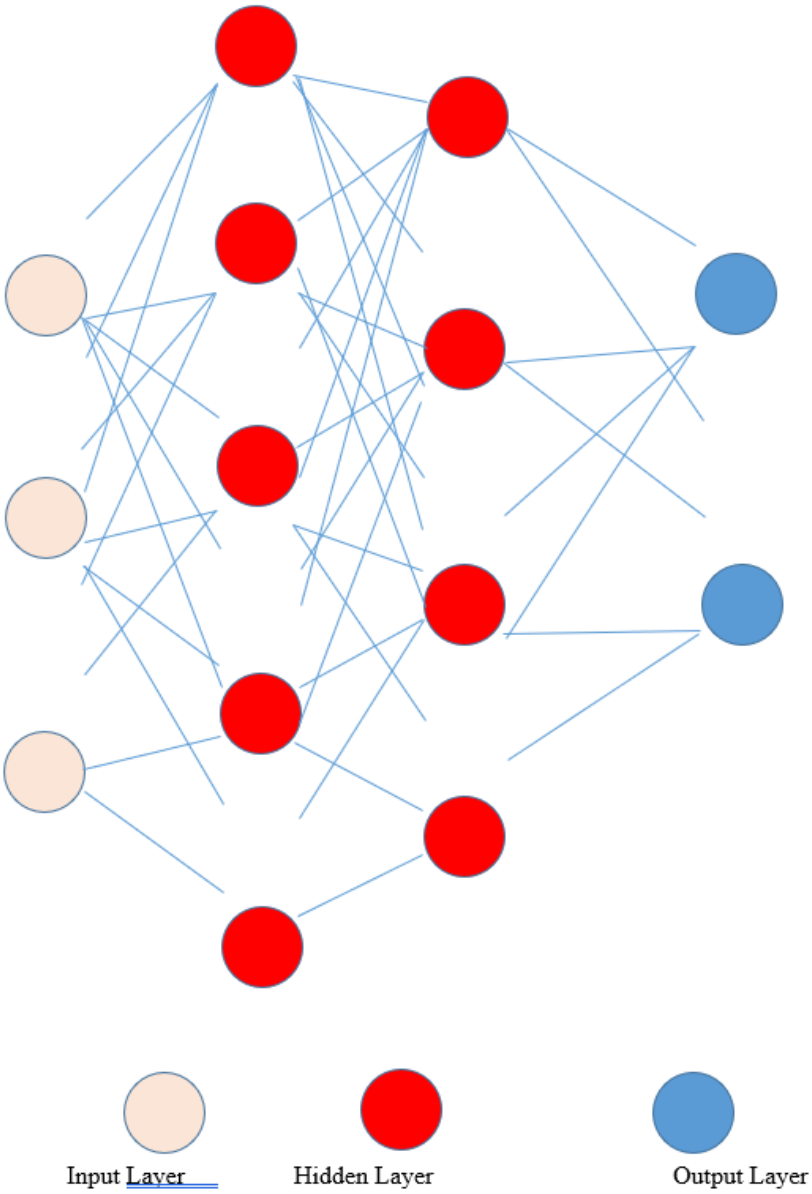

Figure 4:- DNN diagram

DBN Deep Belief Network is a kind of DNN that consists of Multi-layer Belief Networks. Bayu et al.[4]Proposed "Attack Classification Analysis of IoT Network via Deep Learning Approach" in this paper they have focused on feed forward architecture of neural network. The network possesses a two-layer architecture, in which the visible binary stochastic v are connected to the hidden binary stochastic h, and the units within a layer are not connected.The experiment has been performed on standard dataset of UNSW-NB15, CICIDS-001, and GPRS. Then Abien et al. [5] proposed "Deep Learning using Rectified Linear Units (ReLU)" usually ReLU is used as an activation function in DNNs along with Softmax function as their classification function. In this paper they have abided in using softmax as classification function instead they used ReLU at the classification layer of deep learning. Experimental results shown good detection rate and lower false alarms. In 2019 Kayvan et al. [6] proposed "Anomaly Analysis for the Classification Purpose of Intrusion Detection System with K-Nearest Neighbors and Deep Neural Network" in this paper they have conducted the research on anomaly detection using the KNN for Machine Learning and using DNN for Deep learning .the

results have shown classification performance based on Matthews Correlation Co-efficient(MCC) for both ML and DL. Experimental results have shown that DNN outperformed KNN .

In this with the support of Contrastive Divergence Algorithm, a layer of feature is learned from perceptible units. Next the previously trained features are considered as Visible Feature Units, which further performs learning of features and this continues until the last, i.e., the final hidden layer has done the learning of features. After this the whole DBN is trained. And then the testing is done on the model to predict the accuracy.

2. Recurrent Neural Network:-

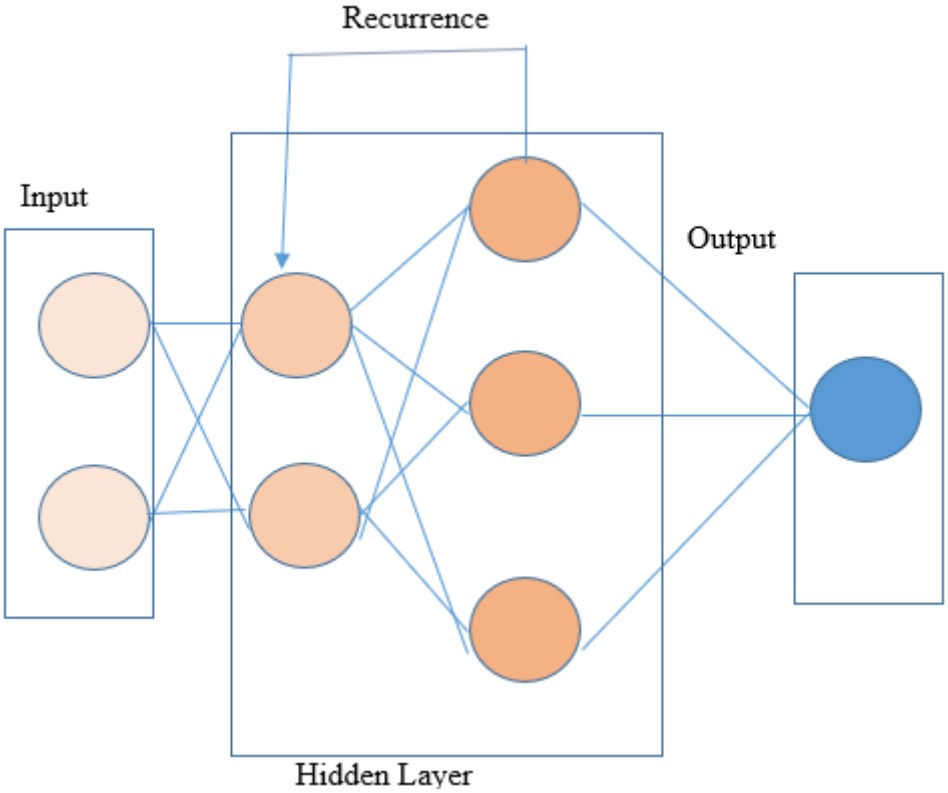

Figure 5 :- RNN diagram

These are basically alternatives of Feed Forward Neural Network, here the neurons present in the hidden layers receives an input with a specific delay in time. The RNN's mainly access the preceding information of foregoing iterations. It apart from processing the inputs, shares the length as well as the weights crossways anytime. One of the major problem with RNN is its slow computing speed and that it does not predicts any future input for the present state, i.e., it has a problem with memorising earlier information.Yin Chuan-long et al. [7] proposed "A Deep Learning Approach for Intrusion Detection using Recurrent Neural Networks" in this paper they have studied the performance of the model in binary classification as well as multi-class classification on the NSL-KDD benchmark dataset having 41 features and 1 class label. The training part of the model consisted of two parts Forward Propagation and Background Propagation. Further have compared the metrics of this model to that of Machine Learning models such as RF,SVM,DT etc. Experimental results using the aforementioned techniques has yield a better accuracy and low false alarm rates. Again Mansour Sheikhan et al. [8] put forward "Intrusion detection using reduced-size RNN based

on feature grouping". In this they have used three-layer Recurrent Neural Network (RNN) Architecture using clustered features as input and attack classes as output of RNN is proposed as Signature based IDS or Misuse Based IDS. The model has been trained using 10% of the Benchmark dataset of KDD-CUP'99 having 41 features and one class label. Experimental results have shown better detection rate.

Long Short Term Memory(LSTM) is a kind of RNN that are programmed to learn and adapt for dependencies for the long term. Its default and sole behaviour is that it can memorize and recall past data for a greater period of time. Sara A. Althubiti et al. [9] proposed "Long Short Term Memory (LSTM) for Anomaly-Based Network Intrusion Detection System". The LSTM model has been trained using the CIC-IDS 2017 dataset using 13 features and one attack class. This trained LSTM model utilized 10 neurons i.e., 10 features in the input layer, a hidden layer with 6 neurons and the output layer with 5 neurons. Experimental results have shown good detection accuracy.

3. Convolutional Neural Network:-

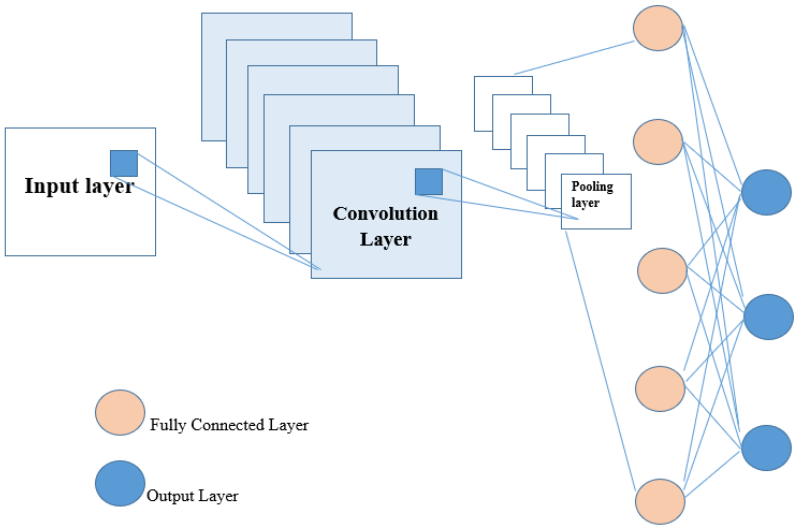

Figure 6 :- CNN Diagram

To achieve best accuracy, deep convolutional neural network are preferred more than any other neural networks. CNN processes the data by passing it, through multiple layers and extracting features to exhibit convolutional operations. Further these Convolutional layers consists of many Rectified Linear Units(ReLU) which outlasts to rectify the feature maps. In this we have a Pooling Layer, which is used to modify these feature map to the next feed {Pooling is basically a sampling algorithm which is used to reduce the dimensions of a feature map}.The next layer is the fully connected layer which forms the flattened matrix or 2 D array brought up from the Pooling Layer as input and identifies the anomalies by classifying it. Further it has come to my notice that researches on IDS using Deep Belief Networks (DBN), Stacked Auto-Encoders(SAE) have been more compared to CNNs.

In 2018 Yalei et al. [10] proposed "Intrusion Detection System for NSL-KDD Dataset Using Convolutional Neural Networks" using the whole NSL-KDD data set to determine Multi-class

classification. They have further compared the model with Machine learning algorithms such as SVM, RF and Deep learning algorithms such as Deep Belief Networks (DBN) and Long Short Term memory (LSTM). It has come to our notice that CNN outperformed the other algorithms. Then Sasanka et al. [11] proposed "Convolutional Neural Networks for Multi-class Intrusion Detection System" in this paper they have made effort for showing improved efficiency in determining the multiple attack classes using Benchmark dataset of UNSW-NB1 and NSL-KDD. After the entire pre-processing they have transformed the Binary vector of network data into 464 dimensions, which are then transformed into 8x8 grayscale image. These images are then fed to the CNN for training as well as for testing the performance of trained IDS. Experimental results have shown much better accuracy in prediction.

4. Restricted Boltzmann Machine:-

These are variants of Boltzmann machine. In this method, the neurons present in the input layers and the hidden layers encompasses symmetric connections between them. However in this we have no internal association within the respective layers. But this is opposite in the case of Restricted Boltzmann machine, as they do encompass internal associations between the hidden layers. In general RBM's are stacked together to form Deep Belief Networks.

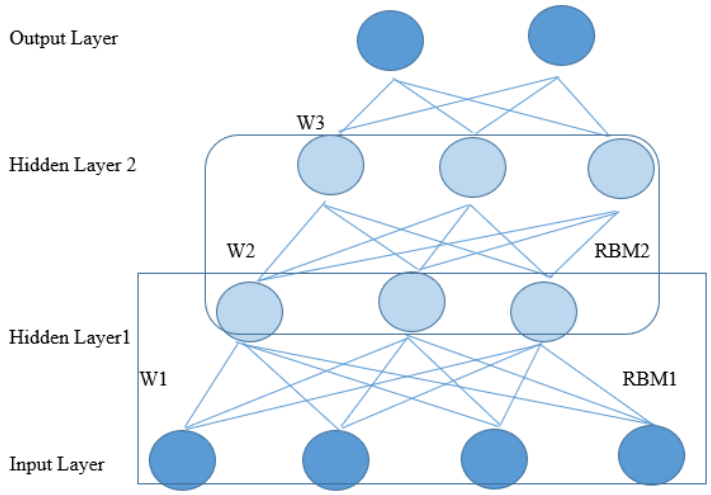

Figure 7 :- RBM Diagram

Nguyen et al. [12] proposed "An anomaly-based Network Intrusion Detection System using Deep learning". It's a multilayer architecture. Model has been trained using Stacked RBMs and Stacked Auto-Encoders on KDDCUP'99 dataset to design a DBN structure. It has used 41 features and one class label to detect the attack in the dataset. They have done multi-class classification and have found out excellent detection accuracy. Md. Zahangir Alom et al. [13] proposed "Intrusion Detection using Deep Belief Networks". Here the training set is modelled using a two layer network called a Restricted Boltzmann Machine. By training a sequence of RBMs a DBN structure is formed, which further helps us in predicting the accuracy. The dataset used in this research was NSL-KDD dataset. Experimental results have shown much better detection accuracy.

5. Deep Auto-Encoders:-

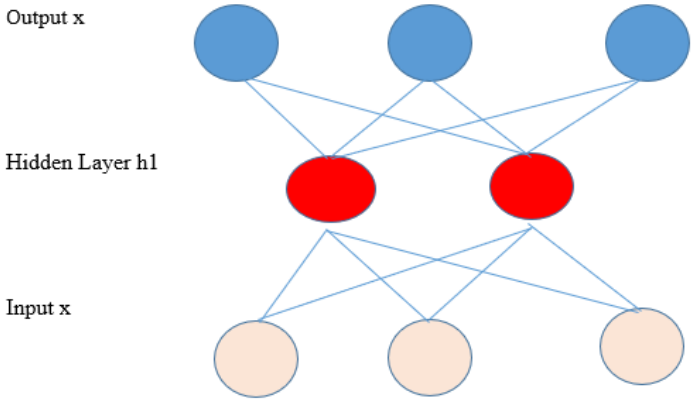

Figure 8:- Auto-Encoder Diagram

In this method the number of hidden cells is merely small than that of the input cells. But the number of input cells is equal to the number of output cells. In this we use Encoders and Decoders; Encoders convert the input data in lower dimensions and then are fed to the hidden layers, then the Decoders are used to reconstruct the compressed data and give it back to the output layer. It basically is a feature extraction algorithm which learns the best parameters required to reconstruct its output as close to its input as possible. But a Deep Auto-Encoder is composed to two simple Deep belief networks[14], which consists of some hidden layers as encoders for encoding and other set of hidden layers as decoders for decoding.

Fahimeh et al[15] proposed "A Deep Auto-Encoder based Approach for Intrusion Detection System". This model is trained in a greedy layer-wise fashion in order to avoid over fitting and local optima. In this model they have made use of four auto-encoders where output of each encoder is given as the input to the other one. Further when the training of one encoder gets over, then only the next encoder can be trained. And in the last hidden layer a softmax classifier classifies the attack into different classes based on the input dataset. In this they have made use of KDD CUP'99 dataset and the experimental result shows a better improvement when compared with other deep learning models with respect to the following metrics accuracy, false alarm rates, and detection rates.

Table 1:- Deep Learning Methods applied on IDS

References	**Methods**	**Dataset**	**Achievement**
B. A. Tama and K.-H. Rhee [4]	Feed forward architecture of neural network	UNSW-NB15 CIC-IDS 001 GPRS	94.04% 99.99% 92.48%
A. F. Agarap[5]	Deep Learning using Rectified Linear Units (ReLU)	MNIST Wisconsin Diagnostic Breast Cancer (WDBC).	Better Accuracy is predicted.

K. Atefi, H. Hashim, and M. Kassim[6]	K-Nearest Neighbours and Deep Neural Network	KDD-CUP'99	KNN-82.26% DNN-92.87%
C. Yin, Y. Zhu, J. Fei, and X. He[7]	RNN-IDS	NSL-KDD	99.53%
M. Sheikhan, Z. Jadidi, and A. Farrokhi[8]	Reduced size RNN based on feature grouping	KDD-CUP'99	94.10%
S. A. Althubiti, E. M. Jones, and K. Roy[9]	LSTM	CIC-IDS 2017	84.83%
Y. Ding and Y. Zhai[10]	CNN	NSL-KDD	80.13%
S. Potluri, S. Ahmed, and C. Diedrich[11]	CNN	NSL-KDD UNSW-NB15	99.14%
N. T. Van, T. N. Thinh, and L. T. Sach[12]	RBM and Auto-Encoders	KDD-CUP'99	Use of Auto-Encoder is better compared to RBM
M. Z. Alom, V. Bontupalli, and T. M. Taha[13]	Stacked RBMs	NSL-KDD	97.5%
S. Naseer[14]	Deep Auto-Encoder	NSL-KDD	93.7%
F. Farahnakian and J. Heikkonen[15]	Stacked Auto-Encoders (SAE)	KDD-CUP'99	94.71%
Quamar Niyaz[16]	Self-Taught Learning (STL), Sparse Auto Encoder (SAE)	NSL-KDD	98%
Hongpo Zhang [17]	Deep Auto-Encoder (DAE)	UNSW-NB15	98.80%

Conclusion:-

By going through the above papers it's clear that Deep Learning Techniques can handle the network data and classify it in a much better way. We detect the IDS using metrics such as accuracy, detection rates, false alarm rates, true positive, true negative, False positive and False negative. Further we have also noticed that Convolution Neural Networks (CNN) have been least used in developing of an IDS model. Recurrent Neural Networks have also proved their mettle by showing improvements in their accuracy. A number of researches have been made using Deep Neural Networks (DNN) in various fashion. RBMs or the Auto-Encoders are trained layer by layer and it's

easier to construct a Deep Belief Network (DBN) Structure with these trained RBMs OR Auto-Encoders. And this is done in order to increase the detection performance.

References:-

[1] B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," *Proc. 2016 8th IEEE Int. Conf. Commun. Softw. Networks, ICCSN 2016*, pp. 581–585, 2016, doi: 10.1109/ICCSN.2016.7586590.

[2] S. Moraboena, G. Ketepalli, and P. Ragam, "A deep learning approach to network intrusion detection using deep autoencoder," *Rev. d'Intelligence Artif.*, vol. 34, no. 4, pp. 457–463, 2020, doi: 10.18280/ria.340410.

[3] Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015, doi: 10.1038/nature14539.

[4] B. A. Tama and K.-H. Rhee, "Attack classification analysis of IoT network via deep learning approach," *Res. Briefs Inf. Commun. Technol. Evol.*, vol. 3, no. 15, pp. 1–9, 2017, doi: 10.22667/ReBiCTE.2017.11.15.015.

[5] A. F. Agarap, "Deep Learning using Rectified Linear Units (ReLU)," no. 1, pp. 2–8, 2018, [Online]. Available: http://arxiv.org/abs/1803.08375.

[6] K. Atefi, H. Hashim, and M. Kassim, "Anomaly Analysis for the Classification Purpose of Intrusion Detection System with K-Nearest Neighbors and Deep Neural Network," *2019 IEEE 7th Conf. Syst. Process Control*, no. December, pp. 269–274, 2019.

[7] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, no. c, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[8] M. Sheikhan, Z. Jadidi, and A. Farrokhi, "Intrusion detection using reduced-size RNN based on feature grouping," *Neural Comput. Appl.*, vol. 21, no. 6, pp. 1185–1190, 2012, doi: 10.1007/s00521-010-0487-0.

[9] S. A. Althubiti, E. M. Jones, and K. Roy, "LSTM for Anomaly-Based Network Intrusion Detection," *2018 28th Int. Telecommun. Networks Appl. Conf. ITNAC 2018*, pp. 1–3, 2019, doi: 10.1109/ATNAC.2018.8615300.

[10] Y. Ding and Y. Zhai, "Intrusion detection system for NSL-KDD dataset using convolutional neural networks," *ACM Int. Conf. Proceeding Ser.*, pp. 81–85, 2018, doi: 10.1145/3297156.3297230.

[11] S. Potluri, S. Ahmed, and C. Diedrich, *Convolutional neural networks for multi-class intrusion detection system*, vol. 11308 LNAI. Springer International Publishing, 2018.

[12] N. T. Van, T. N. Thinh, and L. T. Sach, "An anomaly-based network intrusion detection system using Deep learning," *Proc. - 2017 Int. Conf. Syst. Sci. Eng. ICSSE 2017*, pp. 210–214, 2017, doi: 10.1109/ICSSE.2017.8030867.

[13] M. Z. Alom, V. Bontupalli, and T. M. Taha, "Intrusion detection using deep belief networks," *Proc. IEEE Natl. Aerosp. Electron. Conf. NAECON*, vol. 2016-March, pp. 339–344, 2016, doi: 10.1109/NAECON.2015.7443094.

[14] S. Naseer *et al.*, "Enhanced network anomaly detection based on deep neural networks," *IEEE Access*, vol. 6, no. 8, pp. 48231–48246, 2018, doi: 10.1109/ACCESS.2018.2863036.

[15] F. Farahnakian and J. Heikkonen, "A deep auto-encoder based approach for intrusion detection system," *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2018-Febru, pp. 178–183, 2018, doi: 10.23919/ICACT.2018.8323688.

[16] Q. Niyaz, W. Sun, A. Y. Javaid, and M. Alam, "A deep learning approach for network intrusion detection system," *EAI Int. Conf. Bio-inspired Inf. Commun. Technol.*, 2015, doi: 10.4108/eai.3-12-2015.2262516.

[17] H. Zhang, C. Q. Wu, S. Gao, Z. Wang, Y. Xu, and Y. Liu, "An Effective Deep Learning Based Scheme for Network Intrusion Detection," *Proc. - Int. Conf. Pattern Recognit.*, vol. 2018-August, pp. 682–687, 2018, doi: 10.1109/ICPR.2018.8546162.