International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Network Intrusion Detection Using Deep Learning

Blessy S[1], Samyuktha Ravi[1], Shurabthini S[1], Amudha P[2]
[1]B.E Scholar, Professor[2]
Department of Computer Science and Engineering, School of Engineering, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India

ABSTRACT

Article Info
Volume 8, Issue 3
Page Number: 469-472

Publication Issue :
May-June-2021

Article History
Received : 19 June 2021
Accepted : 22 June 2021
Published: 23 June 2021

Intrusion-detection system aims at detecting attacks against computer systems and networks or, in general, against information systems. Though various part of encryption techniques and firewalls are used to block common attacks, attackers always finds a way in intruding the network. This creates a huge need of dynamic network intrusion detection system where it can protect from nearly all types of attacks. Since dynamic nature of the system is concerned, it should be able to provide with a self-learning mechanism. Deep learning is one of the mostly preferred algorithms in dynamic learning. This paper proposes Convolution Neural Network (CNN) algorithm for intrusion detection.

Keywords : Intrusion Detection, Deep Learning, Convolution Neural Network

I. INTRODUCTION

Cyber Security is a technique used for protecting computer networks by preventing the access of unauthorized users. The main aim of the cyber security is to prevent the network from cyber attack and the identification of theft and aid in risk management. For this purpose, cyber security techniques introduces intrusion detection system, anti- virus software and firewall service. Among them, IDS is the most effective method of protecting hardware's and software's that are running in the network. The ID system reduces the false alarm rate with higher detection rate. Machine learning is a type of artificial intelligence technique that gives a large amount of information about data set. Deep learning is a machine learning's part that achieve higher performance in various fields. Among different approaches in deep learning, Convolutional Neural Network(CNN) produces a better performance in the face and object recognition.

In this paper, Convolution Neural Network (CNN) algorithm is proposed to build a intrusion detection system .The rest of the paper is organised as: section II gives the literature review, section III describes about the methodology, section IV gives the results and finally conclusion is given in section V.

II. LITERATURE REVIEW

A. Krishna et al., (2020) [1], proposed to implement an Intrusion detection and prevention system using Deep Learning that can immediately detect the attacks. The intrusion is detected using a Multi-Layer Perceptron for KDDCUP99 dataset with high accuracy.

B. Y.Dong et al., (2019)[2], proposed a system due to the issues on traditional intrusion detection technologies, a real-time network intrusion detection system based on deep learning, which uses big data technology, natural language processing technology.

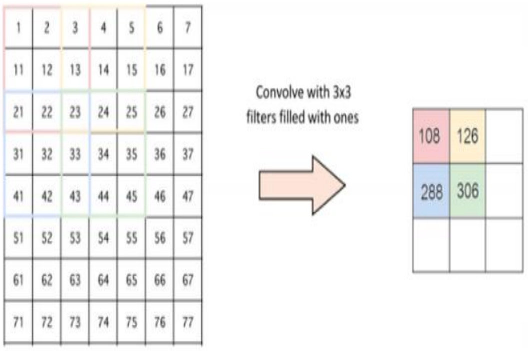
C. R.Devakunchari, et al., (2019)[3], proposed a study on Cyber security using machine learning techniques, a large number of mechanisms have been introduced to protect both network and computer systems. Intrusion detection systems were introduced to determine and also to identify the unauthorized system behaviour such as modification and destruction of data and deep learning technology.

D. W. Peng et al., (2019)[4], proposed a network intrusion detection method based on deep learning, it uses deep confidence neural network to extract features of network monitoring data, and uses BP neural network as top level classifier to classify intrusion types.

III. METHODOLOGY

1. ALGORITHM USED

Convolutional Neural Network also known as CNN is a class of neural networks it specializes in processing data that has a grid-like topology. CNN is a neural network that contains various layers. Convolution is the top most layer to extract features from an input image. Convolution preserves relationship between pixels by learning image features using small squares of input data. It is a mathematical operation that takes two inputs such as image matrix and a filter or kernel. Stride is the number of pixels that are shifted in the input for the purpose of reducing the output size. Figure 1 shows the sample of strides and CNN architecture is shown in Figure 2.



1	2	3	4	5	6	7
11	12	13	14	15	16	17
21	22	23	24	25	26	27
31	32	33	34	35	36	37
41	42	43	44	45	46	47
51	52	53	54	55	56	57
61	62	63	64	65	66	67
71	72	73	74	75	76	77

108	126	
288	306	

Fig 1. Strides

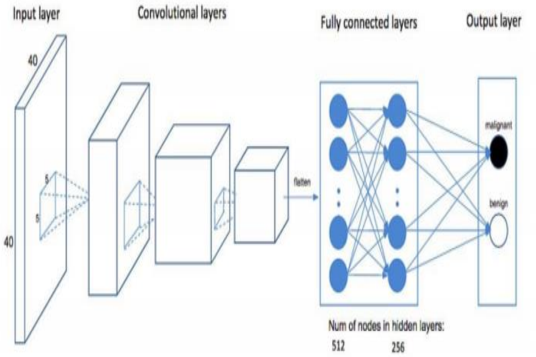


Fig 2. Complete CNN Architecture

For each layer of the Artificial Neural Network, the following calculation takes place g(Wx+b)
Where
x — input vector with dimension
W — weight matrix with dimensions
b — bias vector with dimension
g — activation function, which is usually ReLU

IV. PROPOSED SYSTEM

This work proposes to detect the types of attack that has occurred in the network and that gives the IP address. The time taken for the detection of the attack has been reduced compared to the existing system. The KDDCUP'99 dataset[8] from Kaggle is considered for experimentation. This includes the following methods:

• STEP 1: The input data is in the form of CSV file. The data is then read into the model by using a data reading tool referred to as pandas.

• STEP 2: A Concrete structure of the CNN intrusion detection is modelled. After training the transformed dataset with the CNN, the optimal features are obtained. Five attack states in the dataset are identified using the Softmax classifier. These attack states include Neptune, IPsweep, Portsweep, Satan, and Normal (Normal Records).

•STEP 3: Model training and reverse fine-tuning improve the performance of the model. In the CNN model, the back propagation (BP) algorithm fine-tunes the parameters of the network model. After the optimal parameters of the network model are determined, the performance of the model is evaluated by the classification results of the test dataset. The architecture of the proposed model is given Figure 3.

Advantages

• Less complexity compared to existing algorithm

• Source of attack (IP) is being tracked

•Deep learning performs effective process for huge dataset.

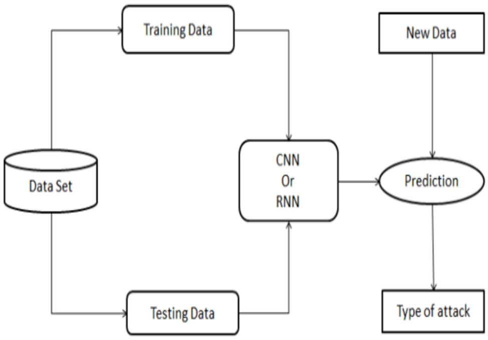


Fig 3. System Architecture

V. EXPERIMENTAL RESULTS

The dataset contains the data of various network parameters of different kinds of attacks. Each of the entry in the dataset are the parameter change in the network for various attack. These changes are duly noted for every attack including normal state of the network under different situations 43 quantitative and qualitative features are obtained from normal and attack data. The class variable has two categories, they are Normal and Anomalous. The ip address and label dataset have been modified using one hot encoding. On comparing the results with CNN and machine learning algorithms, CNN has higher accuracy and is less time consuming.

VI. CONCLUSION

In this work, the deep learning algorithm CNN is used to build an intrusion detection system. The experimental results show that CNN gives a higher accuracy and is less time consuming.

VII. REFERENCES

[1]. A. Krishna, A. Lal M.A., A. J. Mathewkutty, D. S. Jacob and M. Hari, Intrusion Detection and Prevention System Using Deep Learning, In Proceedings of International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 273-278, 2020.

[2]. Y. Dong, R. Wang and J. He, Real-Time Network Intrusion Detection System Based on Deep Learning, In Proceedings of IEEE 10th International Conference on Software Engineering and Service Science (ICSESS), pp. 1-4, 2019.

[3]. R. Devakunchari, Sourabh, Prakhar Malik, A Study of Cyber Security using Machine Learning Techniques, International Journal of Innovative Technology and Exploring Engineering (IJITEE), pp.2278- 3075,Vol.8, Issue-7, 2019.

[4]. W. Peng, X. Kong, G. Peng, X. Li and Z. Wang, Network Intrusion Detection Based on Deep Learning, In Proceedings of International Conference on Communications, Information

System and Computer Engineering (CISCE), pp. 431-435, 2019.

[5]. M. Ishaque and L. Hudec, Feature extraction using Deep Learning for Intrusion Detection System, In Proceedings of 2nd International Conference on Computer Applications & Information Security (ICCAIS), pp. 1-5, 2019.

[6]. C. Yin, Y. Zhu, J. Fei and X. He, A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks, IEEE Access, vol. 5, pp. 21954-21961, 2017.

[7]. G. Zhao, C. Zhang and L. Zheng, Intrusion Detection Using Deep Belief Network and Probabilistic Neural Network, IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), pp. 639-642, 2017.

[8]. https://www.kaggle.com/venkatakanumuru/kddcup99csv

Cite this article as :

Blessy S, Samyuktha Ravi, Shurabthini S, Amudha P, "Network Intrusion Detection Using Deep Learning", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 3, pp. 469-472, May-June 2021.
Journal URL : https://ijsrset.com/IJSRSET2183201