Cyber Attack Type Detection Using Deep Learning Algorithm

Mohan M[a], Sankavi[b], and Sharmitha V[c]

[a]
Assistant Professor, Dept. of CSE, KPR Institute of Engineering and Technology,
Coimbatore, Tamil Nadu, India
[b,c] G Student, Dept. of CSE, KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 16 April 2021

Abstract: Network safety alludes to the cluster of advances, cycles, and practices meant to make sure networks, gadgets, projects, and data from assault, harm, or unapproved access. Network safety might likewise be alluded to as information innovation security. Network safety is important on the grounds that administration military company financial and clinical associations gather interaction and store fantastic measures of data on PCs and completely different gadgets. A important phase of that data may be delicate information whether or not that be licenced innovation financial data individual information, or different types of data that unapproved access or openness might have negative results. In our methodology is we are able to discover the assault sorts utilizing in profound learning techniques.

Keywords: CyberAttack, Attack Types,Accuracy,Dataset,Train-Data,Test-Data.

1. Introduction

Network protection or knowledge innovation security area unit the ways of protecting PCs networks comes and knowledge from unapproved access or assaults that area unit targeted on exploitation.The reason for network safety is to assist forestall digital assaults, info penetrates and wholesale fraud and might facilitate in hazard the executives. At the purpose once AN association encompasses a solid feeling of organization security and a strong episode reaction arrange, it's higher able to forestall and moderate digital attacks.

In this venture we tend to area unit finding a digital assault varieties with help of profound learning calculations.

2. Challenges in “Intrusion Detection” :

In this undertaking we are finding a what kinds of digital assault happen The paper which has generally centered around the most recent three years presents the most recent uses of DL in the field of interruption location. Shockingly the best technique for interruption discovery has not yet been set up. Each way to deal with executing an interruption recognition framework has its and a point obvious from the conversation of examinations among the different strategies. Accordingly it is hard to pick a specific strategy to carry out an interruption identification framework over.

3. Literature Survey:

Kazuki Fukuyama, Yoshiaki Taniguchi, Nobukazu Iguchi has projected Education of network security has attracted tons of attentions because of increasing unauthorized access, lack of engineers World Health Organization have network security skills, and so on. though follow victimization actual pc networks is very necessary for network security education, it needs prices to organize a electronic network for follow. we've projected a network security learning system by constructing a virtual network on one computer so low-priced, simple and safe follow are often accomplished. during this paper, we tend to introduce associate degree wrongdoer agent that mechanically attacks servers in a very mounted pattern for supporting sensible learning of defense techniques safely on a virtual network.

S. Sreenivasa Chakravarthi, Suresh Veluru has developed, Over past few years, among wireless technologies, MANETs has become one amongst the foremost necessary and effective space in extending analysis capabilities. an excellent array of scope is lying as platform for analysis students as MANETs square measure susceptible to attacks as a result of their high volatility in location and motion. Protocols assume that no malicious trespasser node is gift, that impacts all the layers by some means; principally, the network layer. This paper could be a transient review on such attacks whose focus is on degrading MANETs potency. It extends in apprising well known intrusion detection and detection techniques for big selection of attacks. Also, a comprehensive study is carried on the aforesaid space to forecast and explore on futurist analysis areas. The findings of this review ought to offer helpful insights into this IDS literature and be a decent supply for anyone World Health Organization is inquisitive about the approaches to intrusion detection techniques and systems.

Peter Tino, Michal conditioned emotional response conditioned emotional response ˇ nanský, and ˇ Lubica Be ˇ nuˇ ková elaborate upon the claim that clump within the repeated layer of repeated neural networks (RNNs) reflects purposeful science states even before coaching [1], [2]. By concentrating on activation clusters in RNNs, whereas not discard the continual state house network dynamics, we tend to extract prophetic models that we tend to decision neural prediction machines (NPMs). once RNNs with sigmoid activation functions square measure initialized with little weights (a common technique within the RNN community), the clusters of repeated activations rising before coaching square measure so purposeful and correspond to Andre Markoff prediction contexts. during this case, the extracted NPMs correspond to a category of Andre Markoff models, referred to as variable memory length Andre Markoff models (VLMMs). so as to understand what quantity info has extremely been evoked throughout the coaching, the RNN performance must always be compared thereupon of VLMMs and NPMs extracted before coaching because the "null" base models. Our arguments square measure supported by experiments on a chaotic symbolic sequence and a context-free language with a deep algorithmic structure.

4. Proposed System:

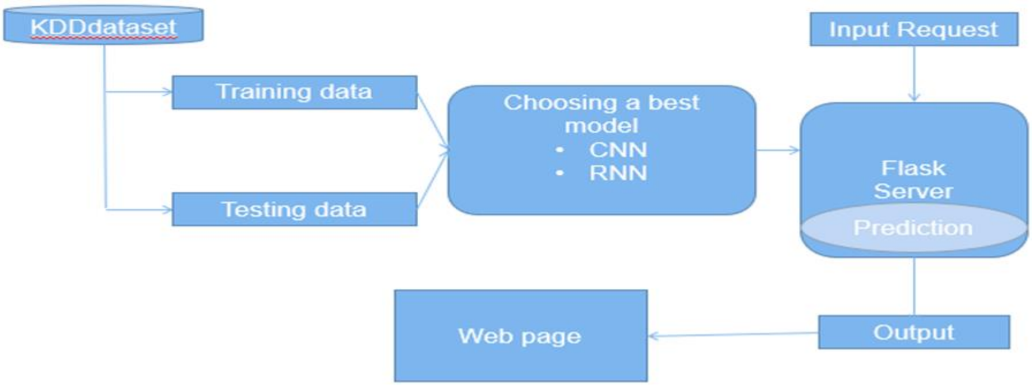


Figure1:Flowchart diagram.

First we tend to get our dataset from UCI repository or any open supply like Kaggle.com.For choosing a model we tend to split our dataset into train and take a look at.Here data's area unit split into 3:1 quantitative relation which means ,Training information having seventy % and testing information having thirty % .In this split method preforming supported train_test_split model.After cacophonous we tend to get xtrain xtest and ytrain ytest .

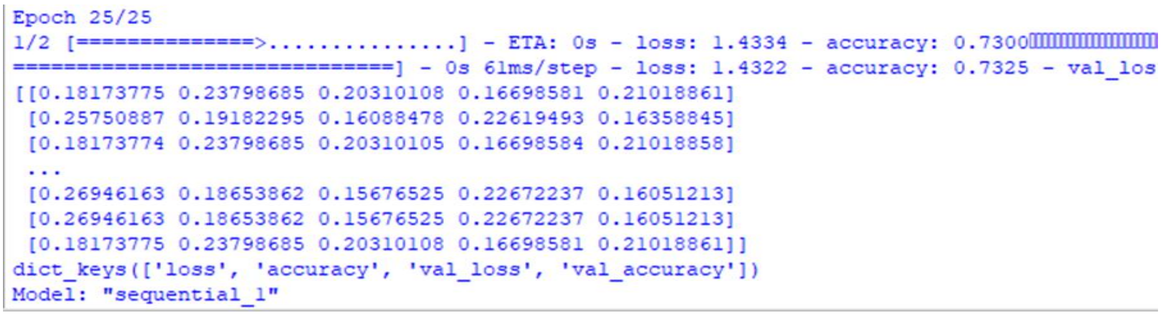
Here we tend to area unit mistreatment deep learning approach to finding the cyber attack varieties. Here we tend to take CNN RNN and MLP algorithms for locating the classifications. and at last select the most effective rule which supplies high accuracy.

5. CNN-Convolution Neural Network:

Convolution Neural Network, additionally referred to as CNN or ConvNet may be a category of neural networks that focuses on process information that includes a grid-like topology, like a picture. A digital image may be a binary illustration of visual information by employing a CNN. however here we tend to area unit mistreatment CSV file that may be a array. Convolution neural network: one among the deep learning model its having 3 methodology

1. 1dimention
2. 2dimention
3. 3dimention

Our model mistreatment 1dimention convolution neural network it's the most effective means for analyzing data's. we tend to additionally re-scale the info within the vary 0-1 as a result of it'll be quicker to method. Here we tend to area unit mistreatment RELU Layer for activation. The accuracy we tend to get mistreatment CNN rule was 0.7325 %.



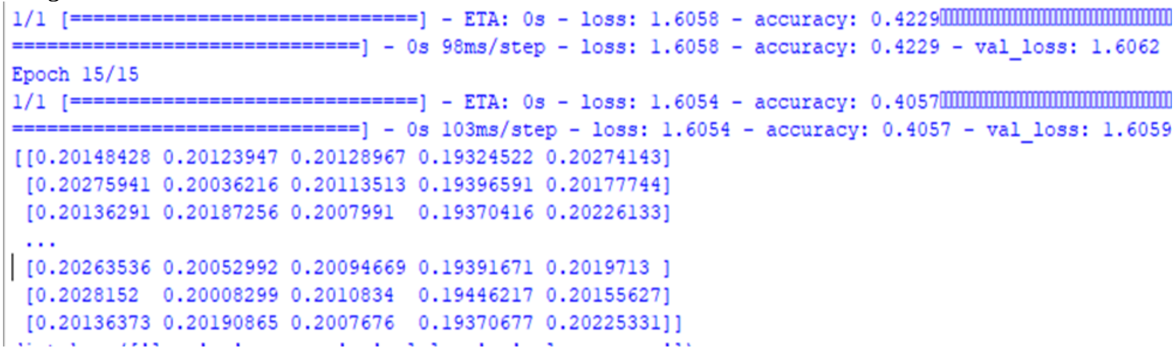
```
Epoch 25/25
1/2 [==============>...............] - ETA: 0s - loss: 1.4334 - accuracy: 0.7300▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯
==============================] - 0s 61ms/step - loss: 1.4322 - accuracy: 0.7325 - val_los
[[0.18173775 0.23798685 0.20310108 0.16698581 0.21018861]
 [0.25750887 0.19182295 0.16088478 0.22619493 0.16358845]
 [0.18173774 0.23798685 0.20310105 0.16698584 0.21018858]
 ...
 [0.26946163 0.18653862 0.15676525 0.22672237 0.16051213]
 [0.26946163 0.18653862 0.15676525 0.22672237 0.16051213]
 [0.18173775 0.23798685 0.20310108 0.16698581 0.21018861]]
dict_keys(['loss', 'accuracy', 'val_loss', 'val_accuracy'])
Model: "sequential_1"
```

Figure 2.Result generated while running CNN algorithm

6. RNN-Recurrent neural networks:

Recurrent neural networks area unit a robust tool that permits neural networks to handle impulsive length sequence information. Of course, they need that the sequence be a discourse sequence, within which the context is entirely generated by things within the continuing portion of the sequence. This is often fairly giant simplifying assumption, it seems that continual neural networks area unit still terribly powerful.

In CNN we tend to use 1dimention for analyzing the info wherever as in RNN we tend to use LSTM- Long immediate memory (LSTM) is a man-made continual neural network (RNN) design employed in the sector of deep learning. LSTM networks area unit well-suited to classifying, process and creating predictions supported statistic information. . Here we tend to area unit mistreatment SIGMOID Layer for activation. The accuracy we tend to get mistreatment RNN rule was 0.4057 %.



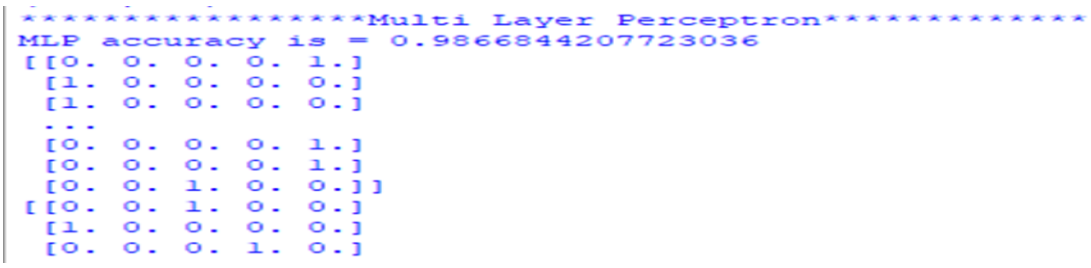
```
1/1 [==============================] - ETA: 0s - loss: 1.6058 - accuracy: 0.4229
==============================] - 0s 98ms/step - loss: 1.6058 - accuracy: 0.4229 - val_loss: 1.6062
Epoch 15/15
1/1 [==============================] - ETA: 0s - loss: 1.6054 - accuracy: 0.4057
==============================] - 0s 103ms/step - loss: 1.6054 - accuracy: 0.4057 - val_loss: 1.6059
[[0.20148428 0.20123947 0.20128967 0.19324522 0.20274143]
 [0.20275941 0.20036216 0.20113513 0.19396591 0.20177744]
 [0.20136291 0.20187256 0.2007991  0.19370416 0.20226133]
 ...
 [0.20263536 0.20052992 0.20094669 0.19391671 0.2019713 ]
 [0.2028152  0.20008299 0.2010834  0.19446217 0.20155627]
 [0.20136373 0.20190865 0.2007676  0.19370677 0.20225331]]
```

Figture 3.Result generated while running RNN algorithm

7. MLP-Multilayer Perception:

Perceptron may be a single layer neural network and a multi-layer perceptron is termed Neural Networks. Perceptron may be a linear classifier (binary). additionally it's employed in supervised learning. It helps to classify the given computer file.

In this from sklearn neural network we tend to foreign the MLP Classifier, Since it utilizes a supervised learning technique we tend to simply work the trained information set into a variable and predict the output. . The accuracy we tend to get mistreatment MLP rule was 0.9557 %.

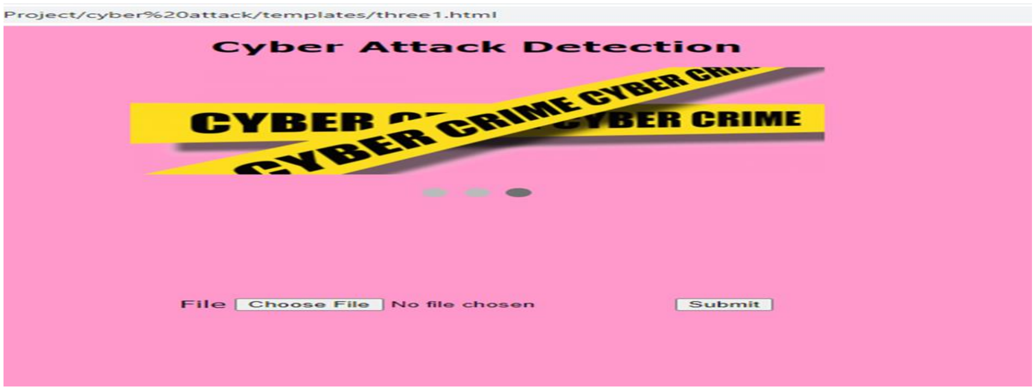


```
*****************Multi Layer Perceptron*************
MLP accuracy is = 0.9866844207723036
[[0. 0. 0. 0. 1.]
 [1. 0. 0. 0. 0.]
 [1. 0. 0. 0. 0.]
 ...
 [0. 0. 0. 0. 1.]
 [0. 0. 0. 0. 1.]
 [0. 0. 1. 0. 0.]]
[[0. 0. 1. 0. 0.]
 [1. 0. 0. 0. 0.]
 [0. 0. 0. 1. 0.]
```

Figure4.Result generated while running MLP algorithm

8. Final Result:

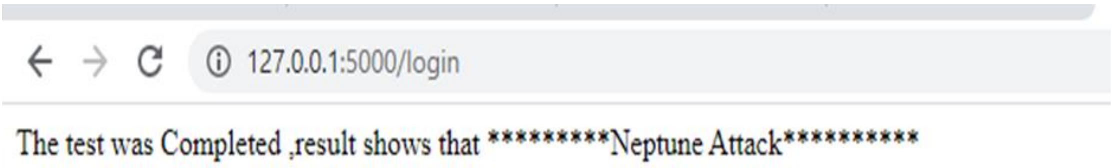
After choosing the most effective rule, we tend to created a flask sever for output prediction. mistreatment flask server will|we will|we are able to} build internet interface for user interaction wherever user can provides a input data to an internet sever as request when obtaining missive of invitation in shows a output to explicit online page.



Project/cyber%20attack/templates/three1.html

Cyber Attack Detection

Figure5:Final Result



The test was Completed ,result shows that *********Neptune Attack**********

Fig 6:Final Result

9. Conclusion:

In this project we tend to area unit finding a what varieties of cyber attack happen. The paper that has largely centered on the last 3 years introduces the most recent applications of deciliter within the field of intrusion detection.

Unfortunately the foremost effective methodology of intrusion detection has not however been established. every approach to implementing associate intrusion detection system has its and a degree apparent from the discussion of comparisons among the assorted strategies.

Thus it's tough to settle on a selected methodology to implement associate intrusion detection system over the others.

Reference:

1. Intelligent stoplight system exploitation Embedded System by Dinesh Rotake and college member.SwapniliKarmore, Innovative Systems vogue And Engineering, ISSN 2222-1727 (paper) ISSN 2222-2871 (online), Vol. 3, No. 5, 2012
2. Wang Wei dynasty, Fang Hanbo , ―Traffic accident automatic detection and remote alarm device‖, Proceedings of IEEE International Conference on electrical knowledge and management Engineering, pages: 910-913, 2011.
3. Road holdup observance and activity exploitation Active RFID and GSM Technology by KoushikMandal, ArindamSen, AbhijnanChakraborty and Siuli Roy, IEEE Annual Conference on Intelligent Transportation Systems, 2011.
4. form of Intelligent auto and management by Sarika B. Kale, and Gajanan P. Dhok. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-5, April 2013.
5. Mr.S.Iyyappan and adult male.V.Nandagopal , ‖Accident Detection and auto Rescue with Intelligent lightweight lightweight, disclosed in International Journal of Advanced Technology and Engineering analysis,2013.
6. K.Athavan; S.Jagadeeshwaran, G.Balasubraminan, N.Dinesh, G.Abhilash, G.Gokul ―Automatic auto rescue System‖, Proceedings of twenty second IEEE International Conference on Tools with technology, pages:190-195, 2012.
7. M.AL-Rousan, A. R. AI-Ali and K. Darwish, GSM-Based Mobile Tele observance and Management System for Inter-Cities Public Transportations, ICIT,2004.
8. R.SGaonkar, semiconductor unit style programming and Application Wiley Japanese Ltd.,New Delhi.
9. P. D. Patinge, N. R. Kolhare (July 2012), wise aboard Public information system exploitation GPS and GSM Integration for transport, International Journal of Advanced analysis in portable computer and Communication Engineering, Vol. 1, Issue V.
10. AmneshGoel ,Sukanya Ray ,Nidhi Chandra, ―Intelligent lightweight System to Prioritized Emergency Purpose Vehicles supported Wireless device Network ‖,published in International Journal of portable computer Applications , Volume 40– No.12, solar calendar month 2012.