PACKET INSPECTION TO IDENTIFY NETWORK LAYER ATTACKS USING MAACHINE LEARNING

Samoju Lavanya

Department of Computer Science and Systems Engineering, Andhra University College of Engineering(A), Visakhapatnam, Andhra Pradesh

ABSTRACT

Network security has benefited from intrusion detection, which may spot unexpected threats from network traffic. Modern techniques for detecting network anomalies typically rely on established machine learning models like KNN, SVM, etc. Despite the fact that these methods can produce some exceptional features, they are somewhat inaccurate and mainly rely on manually designed traffic features, which are no longer relevant in the age of big data. An intrusion detection feature engineering challenge and a traffic anomaly detection model (BAT) are also addressed. BLSTM (Bidirectional Long Short-Term Memory) and attention mechanisms are combined in the BAT model. The network flow vector made up of packet vectors produced by the BLSTM model is screened using an attention mechanism, which can obtain the key features for network traffic classification. We also use many convolutional layers to capture the regional characteristics of the traffic data. We refer to the BAT model as the BAT-MC since several convolutional layers are used to process data samples. Network traffic classification is done using the softmax classifier. The suggested end-to-end model may automatically pick up the most important features of the hierarchy without the need for feature engineering expertise. It can effectively explain the behaviour of network traffic and enhance the ability to detect anomalies. We evaluate our model using a publicly available benchmark dataset, and the experimental findings show that it performs better than existing comparison techniques.

Keywords: — BAT-MC., BLSTM, attention mechanism, KNN, SVM

1 INTRODUCTION

Network information security is significantly aided by intrusion detection. In order to recognise malicious communications, machine learning techniques have been extensively employed in intrusion detection. These approaches, however, are part of shallow learning and frequently place an emphasis on feature engineering and selection. Low recognition accuracy and a high false alarm rate are the results of their inability to successfully address the enormous intrusion data classification problem and trouble choosing features. Deep learning-based intrusion detection techniques have been proposed repeatedly in recent years. To effectively capture the local aspects of traffic data, we use many convolutional layers. We refer to the BAT model as the BATMC since several convolutional layers are used to process data samples. Network traffic classification is done using the softmax classifier.

2. RELEATED WORK

2.1 A Survey: Intrusion Detection Techniques for Internet of things

AUTHORS: Sarika Choudhary and Nishtha Kesswani

The Internet of Things is now the newest buzzword in internet technology. The Internet of Things (IoT) is a constantly expanding network that will turn everyday objects into virtual objects that are smart or intelligent. The Internet of Things (IoT) is a heterogeneous network where devices using various protocols can join to share information. Nowadays, intelligent entities and their activities are essential to human life. Consequently, it is difficult to deploy protected communications on the IoT network. An intrusion detection system is required because, despite authentication and encryption, the IoT network is not protected against cyberattacks. The introduction, architecture, technologies, assaults, and IDS are the main topics of this study piece. This article's primary goal is to give readers a general understanding of the Internet of Things, various

2.2 Network Intrusion Detection

AUTHORS: B. Mukherjee, L.T. Heberlein and K.N. Levitt

Intrusion detection is a new, retrofit approach for providing a sense of security in existing computers and data networks, while allowing them to operate in their current "open" mode. The goal of intrusion detection is to identify unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators. The intrusion detection problem is becoming a challenging task due to the proliferation of heterogeneous computer networks since the increased connectivity of computer systems gives greater access to outsiders and makes it easier for intruders to avoid identification. Intrusion detection systems (IDSs) are based on the beliefs that an intruder's behavior will be noticeably different from that of a legitimate user and that many unauthorized actions are detectable. Typically, IDSs employ statistical anomaly and rulebased misuse models in order to detect intrusions. A number of prototype IDSs have been developed at several institutions, and some of them have also been deployed on an experimental basis in operational systems. In the present paper, several host- based and network-based IDSs are surveyed, and the characteristics of the corresponding systems are identified. The host-based systems employ the host operating system's audit trails as the main source of input to detect intrusive activity, while most of the network-based IDSs build their detection mechanism on monitored network traffic, and some employ host audit trails as well. An outline of a statistical anomaly detection algorithm employed in a typical IDS is also included.

2.3 Survey on sdn based Network Intrusion Detection System using Machine

Learning approaches

AUTHORS: N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad

With the advent of programmable features, network security issues may now be properly detected and tracked thanks to Software Defined Networking (SDN). In order to safeguard computer networks and address network security challenges, machine learning (ML) techniques have recently been included into SDN-based Network Intrusion Detection Systems (NIDS). Deep learning technology (DL) is starting to emerge as one of a number of cutting-edge machine learning techniques in the context of SDN. We looked at a number of current studies on machine learning (ML) techniques that use SDN to construct NIDS in this survey. More particular, we assessed the deep learning methodologies used to create SDN-based NIDS. The tools that can be used to create NIDS models in an SDN environment were covered in this survey in the interim. The survey's conclusion includes a discussion of current difficulties.

2.4 Network Intrusion Detection System: A Machine Learning approach

AUTHORS: Mrutyunjaya Panda, Ajith Abraham, Swagatam Das and Manas Ranjan Patra

As a crucial component of system defence, intrusion detection systems (IDSs) are currently generating a lot of interest. IDSs gather data on network traffic from a specific location on the network or computer system and use it to secure the network. Recent advancements in machine learning approaches have made it possible to detect network intrusions (or attacks), which further enables the network administrator to take preventative actions. The ten machine learning techniques that we propose to use in this paper are Decision Tree (J48), Bayesian Belief Network, Rotation Forest, Hybrid Na ve Bayes with Decision Tree, Hybrid J48 with Lazy Locally Weighted Learning, Discriminative multinomial Na ve Bayes, Combining random Forest with Na ve Bayes, and finally ensemble of classifiers using J48 and NB with AdaBoost.

2.5 A New Intrusion Detection System based on KNN classification Algorithm in wireless Sensor Network

AUTHORS: W. Li, P. Yi, Y. Wu, L. Pan, and J. Li

The Internet of Things has broad application in military field, commerce, environmental monitoring, and many other fields. However, the open nature of the information media and the poor deployment environment have brought great

risks to the security of wireless sensor networks, seriously restricting the application of wireless sensor network. Internet of Things composed of wireless sensor network faces security threats mainly from Dos attack, replay attack, integrity attack, false routing information attack, and flooding attack. In this paper, we proposed a new intrusion detection system based on K -nearest neighbor (K -nearest neighbor, referred to as KNN below) classification algorithm in wireless sensor network. This system can separate abnormal nodes from normal nodes by observing their abnormal behaviors, and we analyse parameter selection and error rate of the intrusion detection system. The paper elaborates on the design and implementation of the detection system. This system has achieved efficient, rapid intrusion detection by improving the wireless ad hoc ondemand distance vector routing protocol (Ad hoc On-Demand Distance the Vector Routing, AODV). Finally, the test results show that: the system has high detection accuracy and speed, in accordance with the requirement of wireless sensor network intrusion detection. a modified version of the popular KDDCup 1999 intrusion detection benchmark dataset was used to test the effectiveness of our suggested machine learning methods for network intrusion detection. Detection rate, false positive rate, and average cost for misclassification are among the experimental results with five classes that are finally presented. These are employed to help researchers in the field of network intrusion detection gain a better knowledge.

3 Implementation Study

Most algorithms have been considered for use in the past. In [16], the authors make a summary of pattern matching algorithm in Intrusion Detection System: KMP algorithm, BM algorithm, BMH algorithm, BMHS algorithm, AC algorithm and AC-BM algorithm. Experiments show that the improved algorithm can accelerate the matching speed and has a good time performance. In [17], Naive approach, Knuth-MorrisPratt algorithm and RabinKarp Algorithm are compared in order to check which of them is most efficient in pattern/intrusion detection. Pcap files have been used as datasets in order to determine the efficiency of the algorithm by taking into consideration their running times respectively.

4 **PROPOSED WORK AND ALOGRITHAM**

The accuracy of the BAT-MC network can reach 84.25%, which is about 4.12% and 2.96% higher than the existing CNN and RNN model, respectively. The following are some of the key contributions and findings of our work:

1) We propose an end-to-end deep learning model BAT-MC that is composed of BLSTM and attention mechanism. BAT-MC can well solve the problem of intrusion detection and provide a new research method for intrusion detection.

. The experimental results show that the performance of BAT-MC is better than the traditional methods.

2) We introduce the attention mechanism into the BLSTM model to highlight the key input. Attention mechanism conducts feature learning on sequential data composed of data package vectors. The obtained feature information is reasonable and accurate.

3) We compare the performance of BAT-MC with traditional deep learning methods, the BAT-MC model can extract information from each packet. By making full use of the structure information of network traffic, the BAT-MC model can capture features more comprehensively.

4) We evaluate our proposed network with a real NSL-KDD dataset

4.1 ADVANTAGES OF PROPOSED SYSTEM:

1.The BAT-MC model consists of five components, including the input layer, multiple convolutional Layers, BSLTM layer, attention layer and output layer, from bottom to top.

2. At the input layer, BAT-MC model converts each traffic byte into a one-hot data format. Each traffic byte is encoded as an n-dimensional vector. After traffic byte is converted into a numerical form, we perform normalization operation

5 METHODOLOGIES

1.Upload Network Packets Dataset

In module user upload kddcup.csv file.

2.Preprocess &Normalized Dataset

In module we can see dataset loaded .we can see data contains alpha numeric data and ML algorithms accept only numeric values so we need to preprocess and normalize them and in graph we can see different attack names in x-axis and total attack types on y-axis.

3.Build Deep Learning Neural Network

In module we can see CNN algorithm got 80% accuracy and in confusion matrix we can see total 5 different attacks are found and in confusion matrix we can see which attack predicted how many times. For example attack 2 predicted 3239 times in entire test data.

4.Build BAT-MC Model.

In module BAT-MC model generated and its prediction accuracy is 95.

5.Comparison Graph

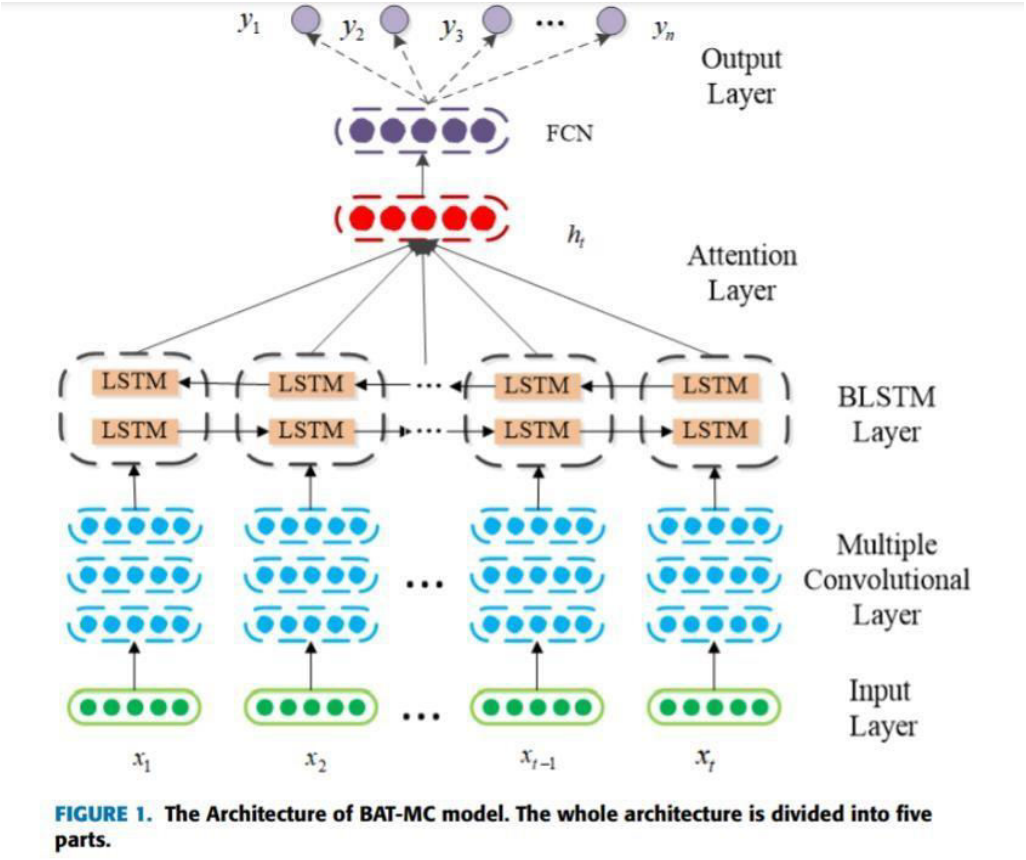


FIGURE 1. The Architecture of BAT-MC model. The whole architecture is divided into five parts.

Fig. 1: propose Architecture

For the time series data composed of traffic bytes, BLSTM can effectively use the context information of data for feature learning. The BLSTM is used to learn the time series feature in the data packet. Traffic bytes of each data packet are sequentially input into an BLSTM, which finally obtain a packet vector. BLSTM is an enhanced version of LSTM (Long ShortTerm Memory) [36], [37]. The BLSTM model is used to extract coarse-grained features by connecting forward LSTM and backward LSTM. LSTM is designed by the inputgate i, the forget gate f and the output gate o to control how to overwrite the information by comparing the inner memory cell C when new

information arrives [38]. When information enters a LSTM network, we can judge whether it is useful according to relevant rules. Only the information that meets algorithms authentication will be remained, and inconsistent information will be forgotten through forget gate.

6 RESULTS AND DISCUSSION

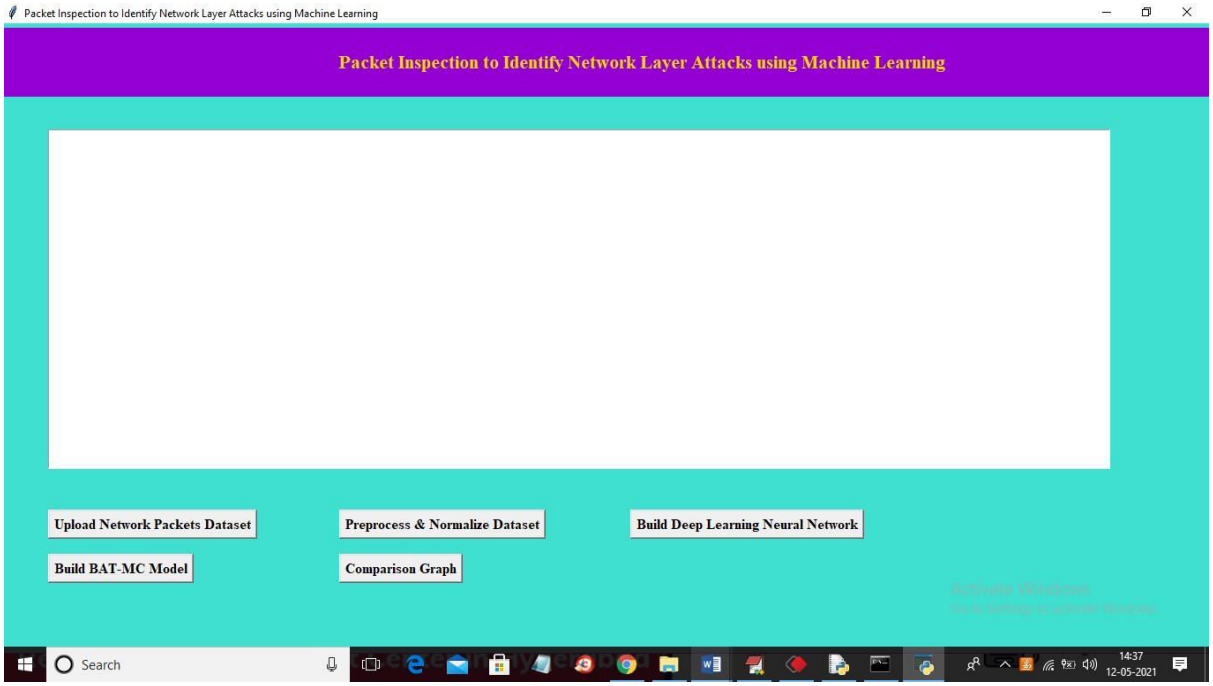
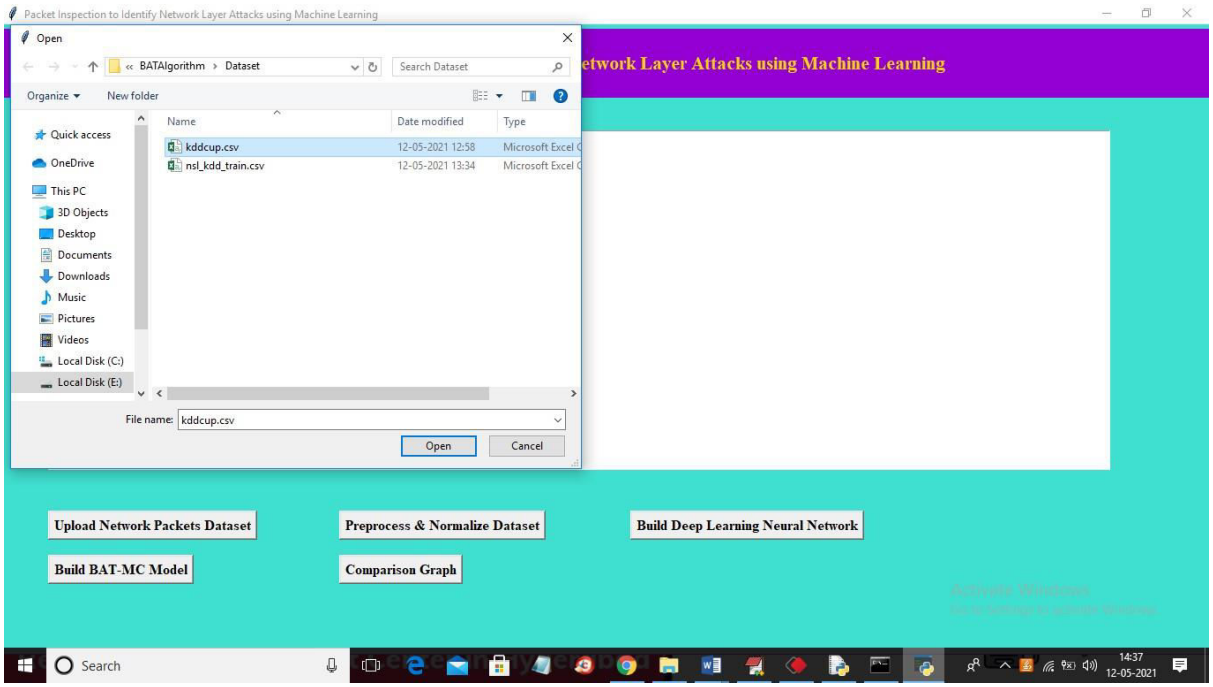


Fig.2:-In above screen click on 'Upload Network Packets Dataset' button to upload dataset and to get below screen



62

Fig3:-In above screen selecting and uploading 'kddcup.csv' file and then click on 'Open' button to load dataset and to

get below screen

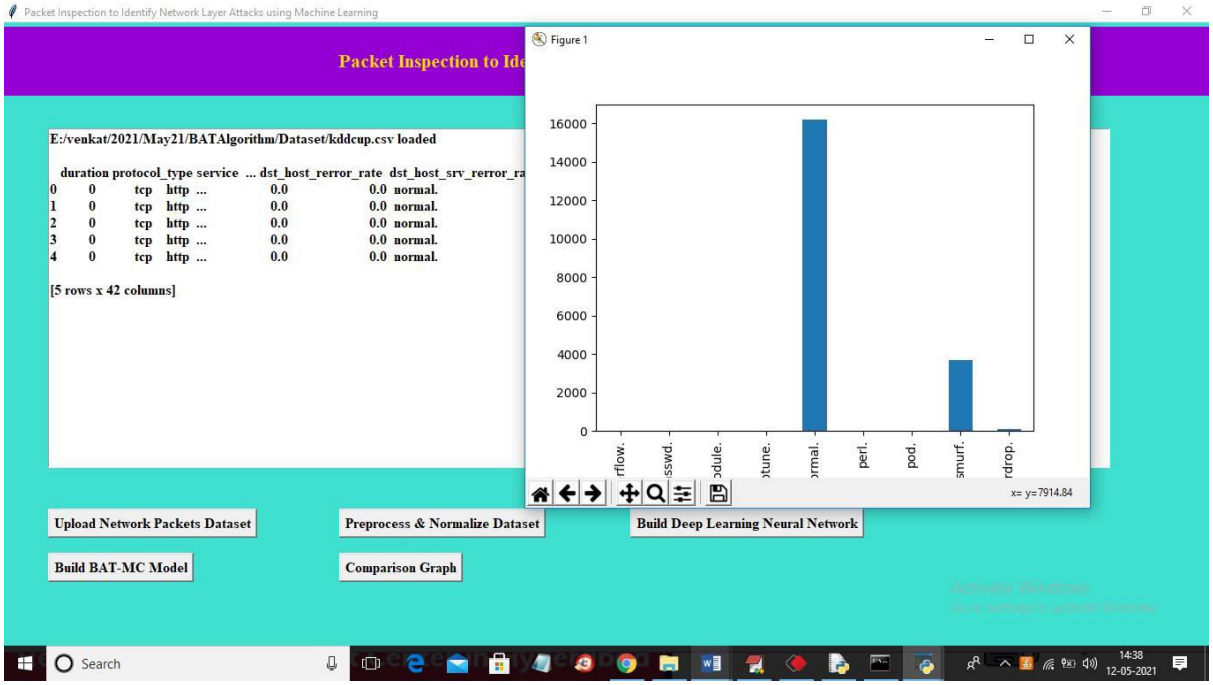
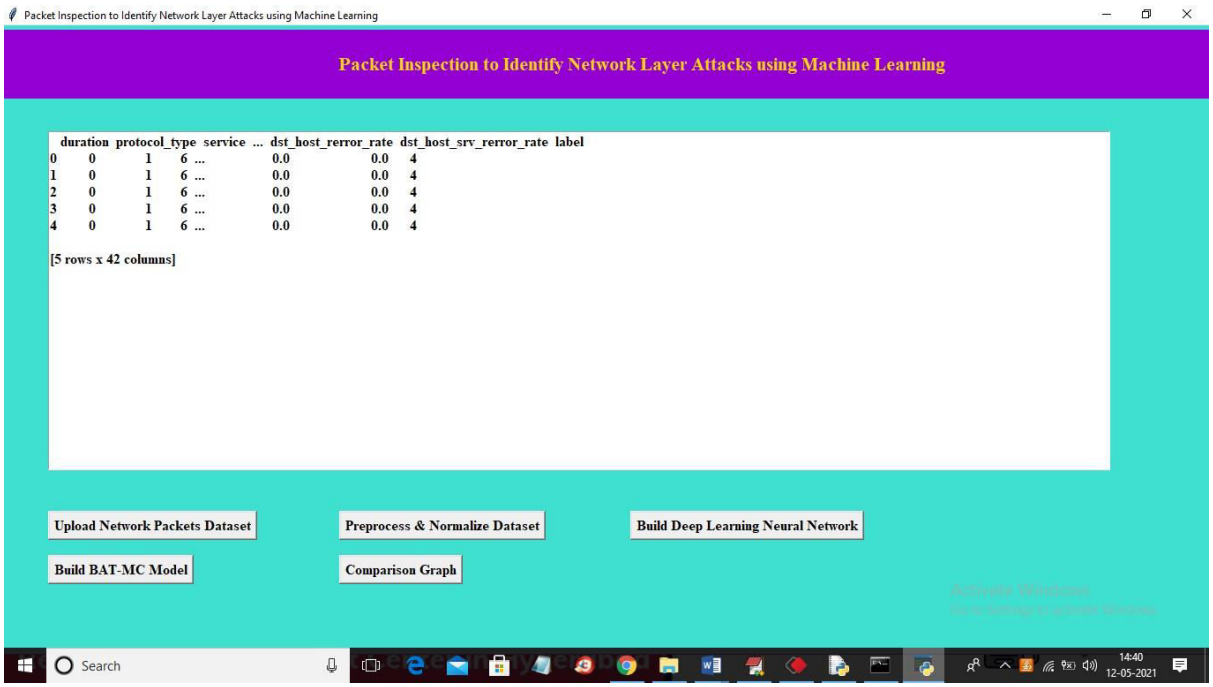


Fig 4:-In above screen in text area we can see dataset loaded and we can see data contains alpha numeric data and ML algorithms accept only numeric values so we need to preprocess and normalize them and in graph we can see different attack names in x-axis and total attack types on y-axis and now close above graph and then click on 'Preprocess & Normalize Dataset' button to normalize data



63

Fig 5:-In above screen we can see dataset converted to numeric values by assigning ID's to each unique non-numeric data and now dataset is ready and now click on 'Build Dee Learning

Neural Network' button to train CNN above dataset and then calculate prediction accuracy

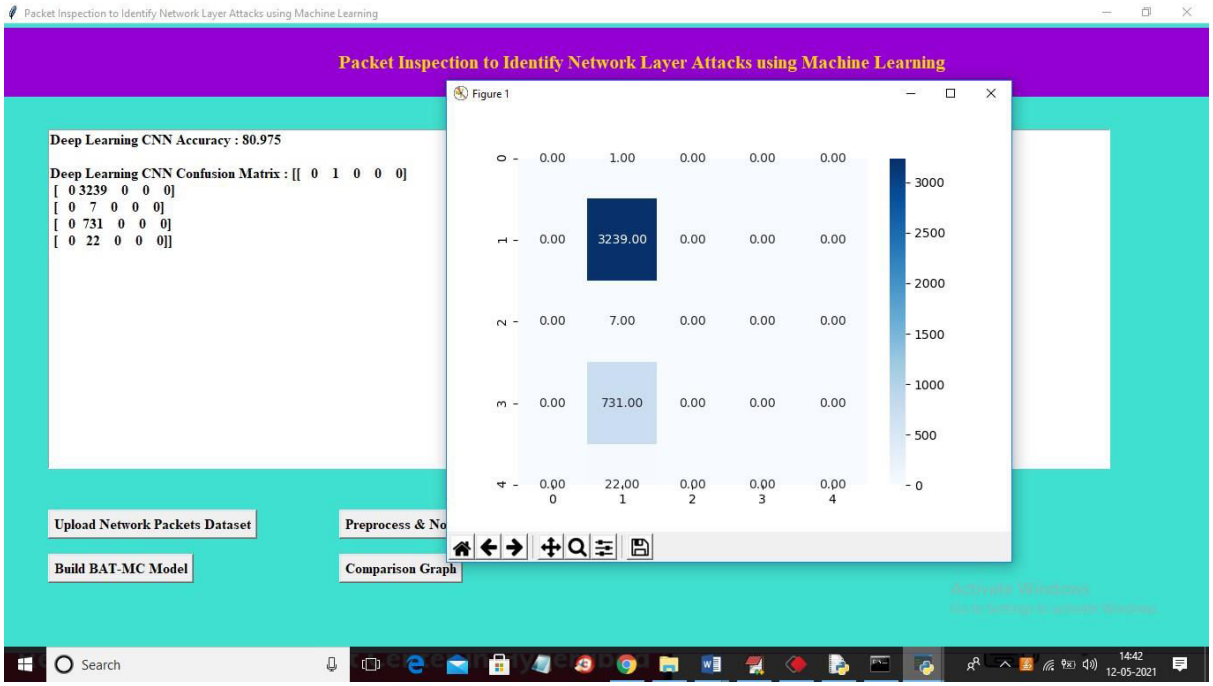


Fig 6:-In above screen we can see CNN algorithm got 80% accuracy and in confusion matrix we can see total 5 different attacks are found and in confusion matrix we can see which attack predicted how many times. For example attack 2 predicted 3239 times in entire test data.

Now close above graph and then click on 'Build BAT-MC Model' to train above dataset with BLSTM algorithm and then calculate prediction accuracy on test data.

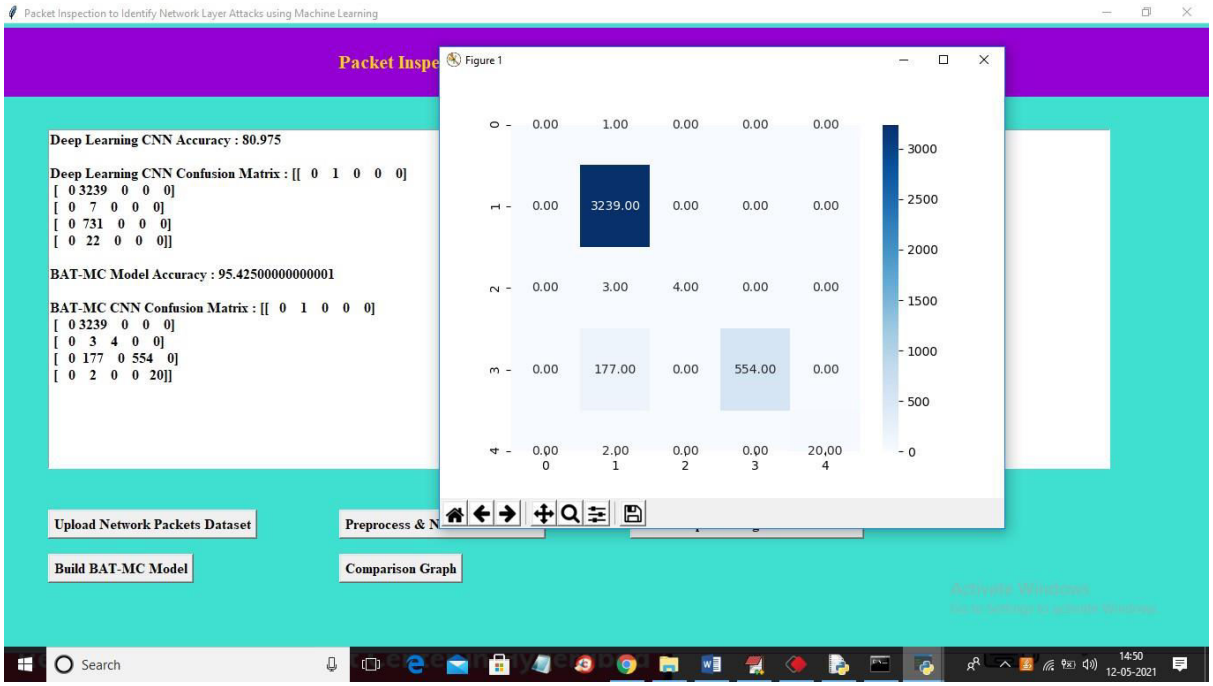


Fig 7:-In above screen BAT-MC model generated and its prediction accuracy is 95 and now close above graph and then click on 'Comparison Graph' button to get below graph

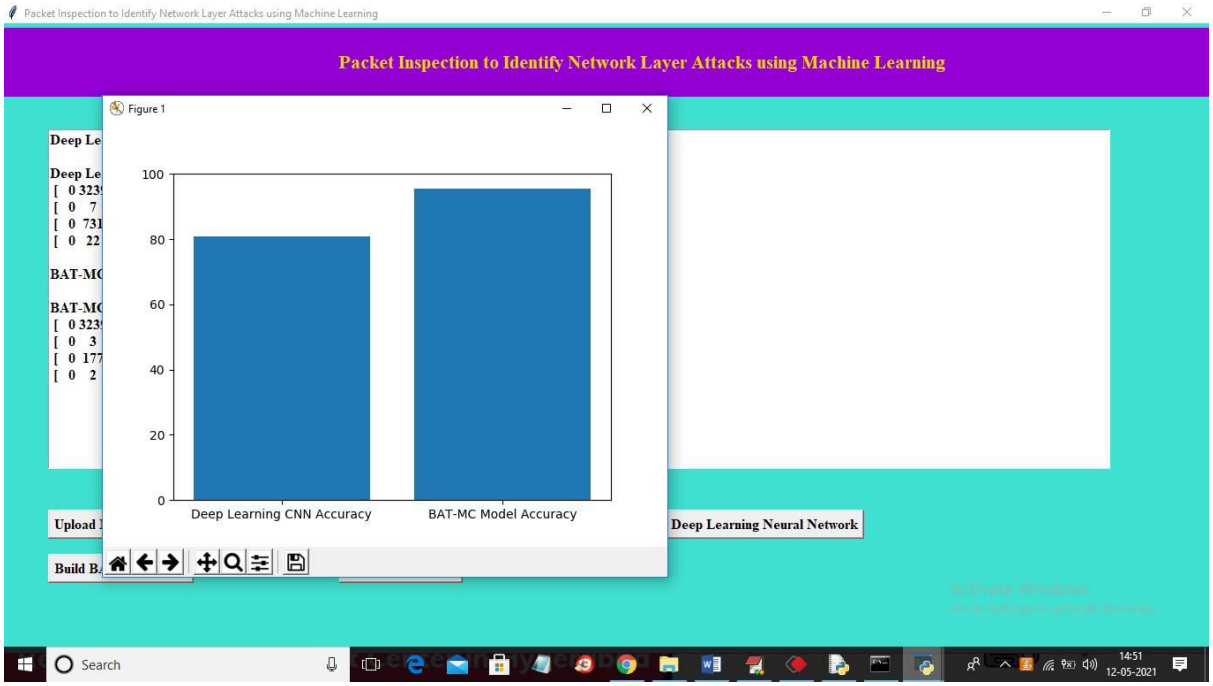


Fig8:-In above graph x-axis represents algorithm name and y-axis represents accuracy and in both algorithm BAT-MC model is giving better accuracy. Similarly you can upload other dataset and can build CNN and BAT-MC model. In below screen you can see NSL dataset accuracy

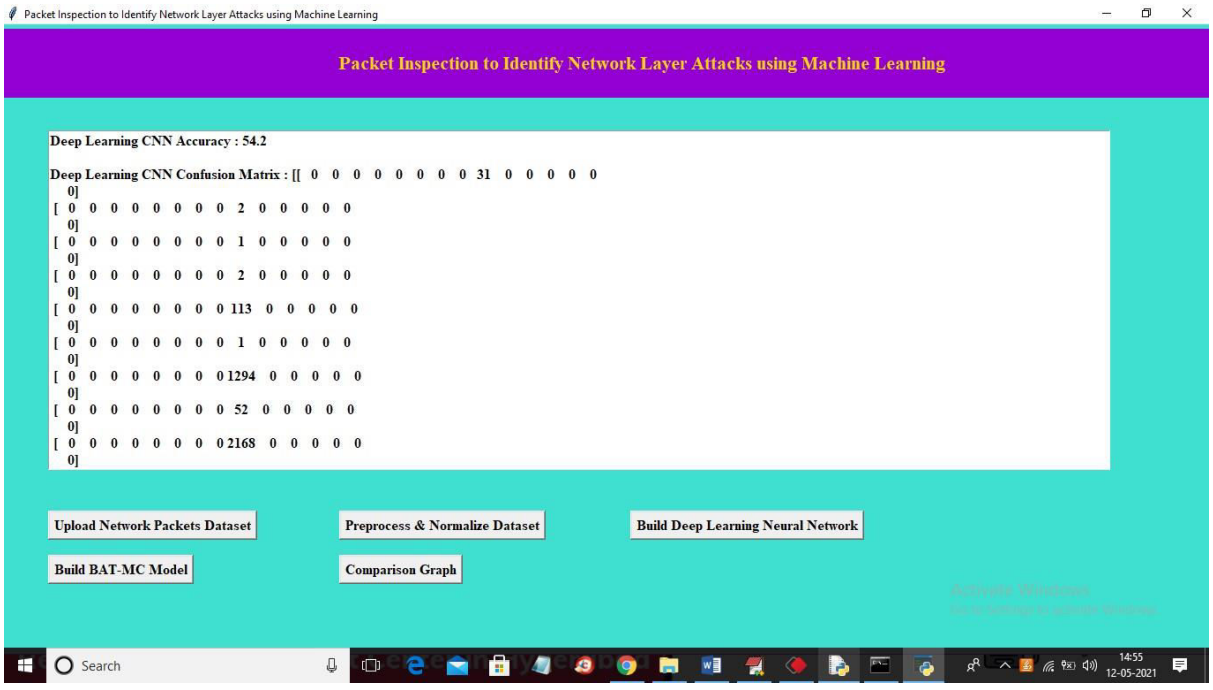


Fig9:_In above screen CNN got 54% accuracy and then scroll down above text area to get BAT-MC accuracy

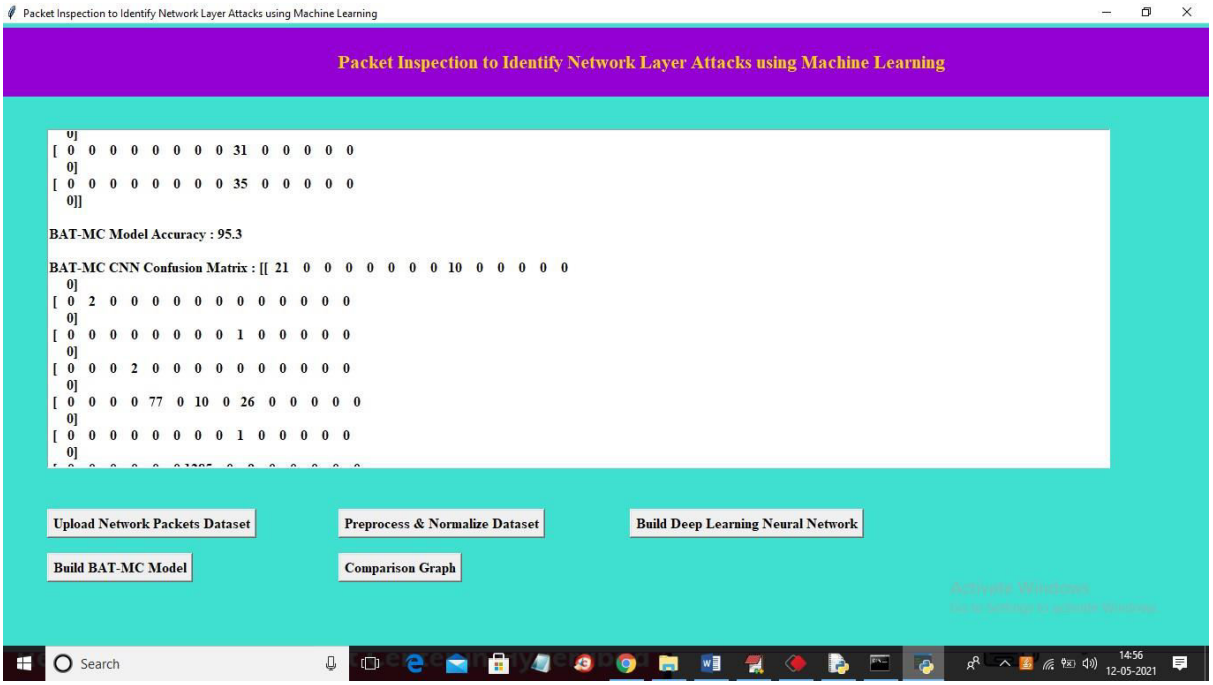


Fig10:-In above screen BAT-MC got 95% accuracy

Below code screen showing how we are creating BLSTM model to build attack detection model

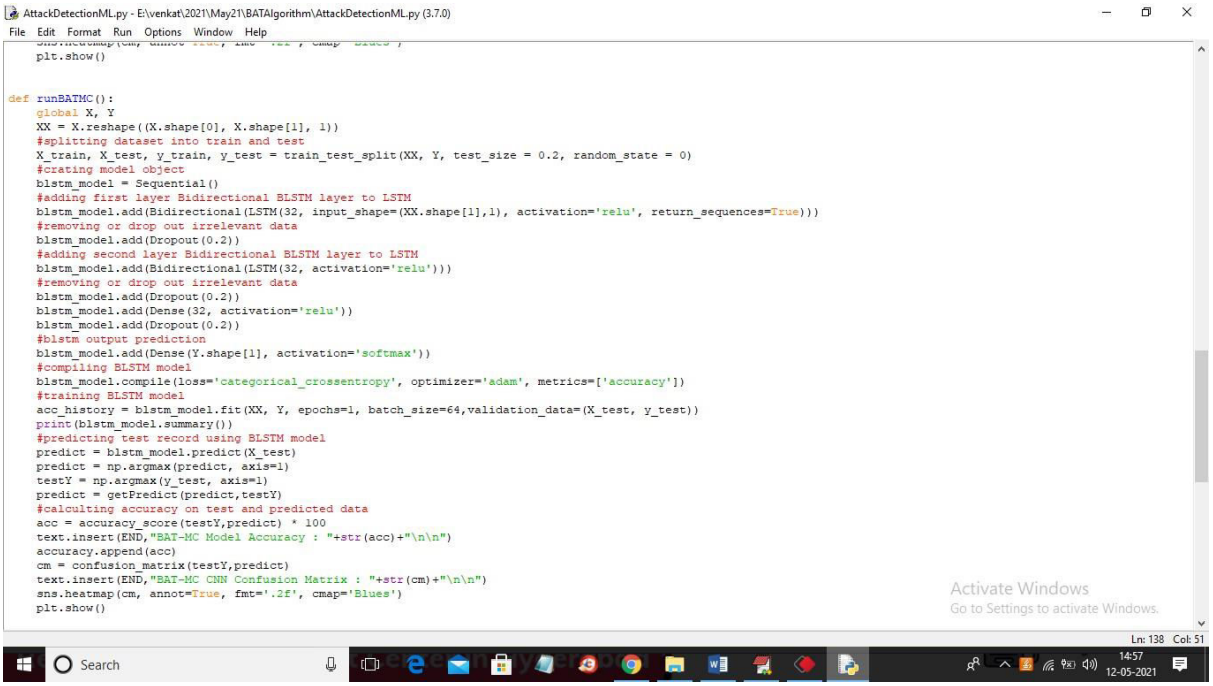


Fig11:-In above screen read red colour comments to understand development of BAT-MC model

7. CONCLUSION AND FUTURE WORK

The network traffic structural information is not fully utilised by the present deep learning techniques in network traffic classification research. By employing the two-phase learning of BLSTM and focusing on the time series characteristics for intrusion detection using the NSL-KDD dataset, we present a novel model called BATMC, drawing on the application approaches of deep

learning in the field of natural language processing. The BLSTM layer, which joins the forward and backward LSTM, is

used to extract features from each packet's traffic bytes. A packet vector can be generated from each data packet. A network flow vector is created by arranging these packet vectors.7. REFRENCES

1. B. B. Zarpelo, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga, ''A survey of intrusion detection in Internet of Things,'' J. Netw. Comput. Appl., vol. 84, pp. 25–37, Apr. 2017.

2. B. Mukherjee, L. T. Heberlein, and K. N. Levitt, ''Network intrusion detection,'' IEEE Netw., vol. 8, no. 3, pp. 26–41, May 1994.

3. S. Kishorwagh, V. K. Pachghare, and S. R. Kolhe, ''Survey on intrusion detection system using machine learning techniques,'' Int. J. Control Automat., vol. 78, no. 16, pp. 30–37, Sep. 2013.

4. N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, ''Survey on SDN based network intrusion detection system using machine learning approaches,'' Peer-to-Peer Netw. Appl., vol. 12, no. 2, pp. 493–501, Mar. 2019.

5. M. Panda, A. Abraham, S. Das, and M. R. Patra, ''Network intrusion detection system: A machine learning approach,'' Intell. Decis. Technol., vol. 5, no. 4, pp. 347–356, 2011.

6 W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, ''A new intrusion detection system based on KNN classification algorithm in wireless sensor network,'' J. Electr. Comput. Eng., vol. 2014, pp. 1–8, Jun. 2014.

7.S. Garg and S. Batra, ''A novel ensembled technique for anomaly detection,'' Int. J. Commun. Syst., vol. 30, no. 11, p. e3248, Jul. 2017.

8. F. Kuang, W. Xu, and S. Zhang, ''A novel hybrid KPCA and SVM with GA model for intrusion detection,'' Appl. Soft Comput.., vol. 18, pp. 178–184, May 2014.

9. W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, ''Malware traffic classification using convolutional neural network for representation learning,'' in Proc. Int. Conf. Inf. Netw. (ICOIN), 2017, pp. 712–717.

10. P. Torres, C. Catania, S. Garcia, and C. G. Garino, ''An analysis of Recurrent Neural Networks for Botnet detection behavior,'' in Proc. IEEE Biennial Congr. Argentina (ARGENCON), Jun. 2016, pp. 1–6.