**BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset**

**ABSTRACT:**

Intrusion detection can identify unknown attacks from network traffics and has been an effective means of network security. Nowadays, existing methods for network anomaly detection are usually based on traditional machine learning models, such as KNN, SVM, etc. Although these methods can obtain some outstanding features, they get a relatively low accuracy and rely heavily on manual design of traffic features, which has been obsolete in the age of big data. To solve the problems of low accuracy and feature engineering in intrusion detection, a traffic anomaly detection model BAT is proposed. The BAT model combines LINEAR REGRESSION, 3 LAYER NEURAL NETWORK and attention mechanism. Attention mechanism is used to screen the network flow vector composed of packet vectors generated by the 3-layer DNN model, which can obtain the key features for network traffic classification. In addition, we adopt multiple convolutional layers to capture the local features of traffic data. As multiple convolutional layers are used to process data samples, we refer BAT model as BAT-MC. The softmax classifier is used for network traffic classification. The proposed end-to-end model does not use any feature engineering skills and can automatically learn the key features of the hierarchy. It can well describe the network traffic behavior and improve the ability of anomaly detection effectively. We test our model on a public benchmark dataset, and the experimental results demonstrate our model has better performance than other comparison methods.

**PROBLEM STATEMENT:**

Intrusion detection plays an important part in ensuring network information security. However, with the explosive growth of Internet business, traffic types in the network are increasing day by day, and network behaviour characteristics are becoming increasingly complex, which brings great challenges to intrusion detection . How to identify various malicious network traffics, especially unexpected malicious network traffics, is a key problem that cannot be avoided.

**OBJECTIVE:**

intrusion detection can be considered as a classification problem. By improving the performance of classifiers in effectively identifying malicious traffics, intrusion detection accuracy can be largely improved. Machine learning methods have been widely used in intrusion detection to identify malicious traffic. However, these methods belong to shallow learning and often emphasize feature engineering and selection. They have difficulty in features selection and cannot effectively solve the massive intrusion data classification problem.

**EXISTING SYSTEM:**

* In existing methods analysis of the viability of Recurrent Neural Networks (RNN) to detect the behavior of network traffic by modeling it as a sequence of states that change over time.
* In existing methods verify the performance of Long ShortTerm memory (LSTM) network in classifying intrusion traffics. Experimental results show that LSTM can learn all the attack classes hidden in the training data.

**DISADVANTAGES:**

* All the above methods treat the entire network traffic as a whole consisting of a sequence of traffic bytes. They don’t make full use of domain knowledge of network traffics.
* Existing methods treats traffics as independent and ignore the internal relations of network traffics.

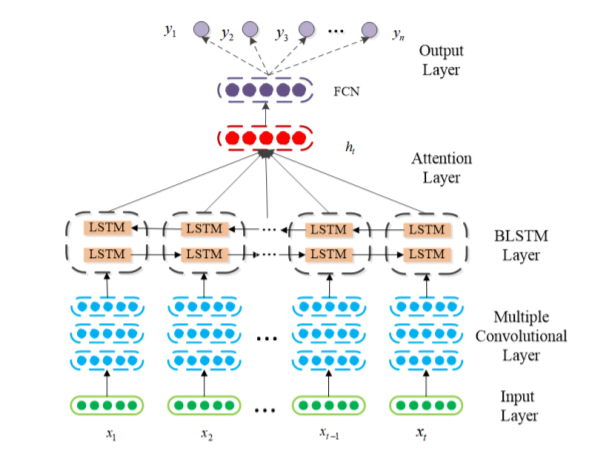
**PROPOSED SYSTEM:**

* We propose an end-to-end deep learning model DNN that is composed of DNN and attention mechanism. DNN can well solve the problem of intrusion detection and provide a new research method for intrusion detection
* We compare the performance of DNN 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 DNN model can capture features more comprehensively. 4) We evaluate our proposed network with a real NSL-KDD dataset. The experimental results show that the performance of BAT-MC is better than the traditional methods

**ADVANTAGES:**

* This method is used to analyse the important degree of packet vectors to obtain fine-grained features which are more salient for malicious traffic detection.
* At the output layer, the features generated by attention mechanism are then imported into a fully connected layer for feature fusion, which obtains the key features that accurately characterize network traffic behaviour.

**SYSTEM ARCHITECTURE:**

****

**SOFTWARE HARDWARE REQUIREMENT:**

#### HARDWARE REQUIREMENTS:

#### System : Pentium IV 2.4 GHz.

#### Hard Disk : 100 GB.

#### Monitor : 15 VGA Color.

#### Mouse : Logitech.

#### RAM : 1 GB.

#### SOFTWARE REQUIREMENTS:

#### Operating system : Windows XP/7/10

* Coding Language : Html, JavaScript,
* Development Kit : Flask Framework
* Database : mysql
* IDE : Anaconda prompt

**REFRANCES:**

* 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