The Impact of AI Using Deep AI Methods In Network Intrusion Detection Using NSL-KDD Dataset and metaheuristic algorithm for global optimization

Dr. Saragadam Sridhar[1]
Associate Professor.
Miracle Educational Society Group of Institutions

Paila Lalit Kumar
Student.
Miracle Educational Society Group of Institutions

ABSTRACT

Interruption location can distinguish obscure assaults from network deals and has been a successful methods for network security. These days, existing techniques for network inconsistency recognition are typically founded on conventional AI models, like KNN, SVM, and so on Albeit these strategies can acquire some exceptional highlights, they get a generally low exactness and depend intensely on manual plan of traffic highlights, which has been outdated in the period of large information. To tackle the issues of low exactness and highlight designing in interruption identification, a traffic oddity location model BAT is proposed.

The BAT model consolidates BLSTM (Bidirectional Long Short-term memory) and consideration component. Consideration instrument is utilized to screen the organization stream vector made out of bundle vectors created by the BLSTM

model, which can get the critical highlights for network traffic arrangement. Furthermore, we receive numerous

convolutional layers to catch the neighborhood highlights of traffic information. As different convolutional layers are utilized to handle information tests, we allude BAT model as BAT-MC.

INTRODUCTION

With the development and improvement of Internet technology, the Internet is providing various convenient services for people. However, we are also facing various security threats. Network viruses, eavesdropping and malicious attacks are on the rise, causing network security to become the focus of attention of the society and government departments. Fortunately, these problems can be well solved via intrusion detection. 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 behavior characteristics are becoming increasingly complex, which brings great challenges to
intrusion detection [1], [2].

..

MOTIVATION

The intrusion detection technology can be divided into three major categories: pattern matching methods, traditional machine learning methods and deep learning methods. At the beginning, people mainly use pattern matching algorithms for intrusion detection. Pattern matching algorithm [14], [15] is the core algorithm of intrusion detection system based on feature matching. 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.

Existing System

An Intrusion Detection System (IDS) is a mechanism that detects intrusions or attacks against a system or a network by analyzing the activity of the network and the

system. Such intruders can be internal or external [14]: Internal intruders are users inside the network that attempt to raise their access privileges to misuse non-authorized privileges while external intruders are users outside the target network attempting to gain unauthorized access to the network [15]. The IDS monitors the operations of a host or a network, alerting the system administrator when it detects a security violation. There are mainly three components of the IDS [16]:

Limitations of existing system

we review the technologies involved in the Intrusion Detection System to handle security issues in IoT environments.

Applications

It can use in IoT application to detect attacks

LITERATURE SURVEY

B. B. Zarpelo, R. S. Miani, C. T. Kawakani, and S. C. D. Alvarenga, "A survey of intrusion detection in internet of things," vol. 84, no. C, 2017, pp. 25–37

Web of Things (IoT) is another worldview that coordinates the Internet and actual items having a place with various spaces like home computerization, mechanical interaction, human wellbeing and natural checking. It extends the presence of Internet-associated gadgets in our every day exercises, bringing, notwithstanding numerous advantages, challenges identified with security issues. For over twenty years, Intrusion Detection Systems (IDS) have been a significant instrument for the security of organizations and data frameworks. Nonetheless, applying customary IDS methods to IoT is troublesome because of its specific attributes, for example, compelled asset gadgets, explicit convention stacks, and guidelines. In this paper, we present a study of IDS research endeavors for IoT. Our goal is to distinguish driving patterns, open issues, and future exploration prospects. We ordered the IDSs proposed in the writing as per the accompanying ascribes: recognition technique, IDS position procedure, security danger and approval methodology. We likewise talked about the various opportunities for each property, specifying parts of works that either propose explicit IDS plans for IoT or foster assault identification methodologies for IoT dangers that may be implanted in IDSs.

O. Tirelo and C. H. Yang, "Network intrusion detection," IEEE Network, vol. 8, no. 3, pp. 26–41, 2003.Prologue to Intrusion Detection Systems In Cisco Security Professional's Guide to Secure Intrusion Detection Systems, 2003 Organization IDS

Organization based interruption location frameworks (NIDS) are gadgets brilliantly dispersed inside networks that inactively assess traffic navigating the gadgets on which they sit. NIDS can be equipment or programming based frameworks and, contingent upon the maker of the framework, can connect to different organization mediums like Ethernet, FDDI, and others. As a rule, NIDS have two organization interfaces. One is utilized for paying attention to arrange discussions in unbridled mode and the other is utilized for control and announcing.

With the appearance of exchanging, which confines unicast discussions to entrance and departure switch ports, network framework merchants have conceived port-reflecting strategies to reproduce all organization traffic to the NIDS. There are different methods for providing traffic to the IDS, for example, network taps. Cisco utilizes Switched Port Analyzer (SPAN) usefulness to work with this capacity on their organization gadgets and, in some organization hardware, incorporates NIDS segments straightforwardly inside the switch. We'll talk about Cisco's IDS items in the following part.

Proposed System

he 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. 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 operations. At the multiple convolutional layer, we convert the numerical data into traffic images. Convolutional operation is used as a feature extractor that takes an image representation of data packet. At the BLSTM layer, BLSTM model which connects the forward LSTM and the backward LSTM is used to extract features on the the traffic bytes of each packet. BLSTM model can learn the sequential characteristics within the traffic bytes because BLSTM is suitable to the structure of network traffic. In the attention layer, attention mechanism is used to analyze 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 behavior. Finally, the fused features are fed into a classifier to get the final recognition results.:

Advantages

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.

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.

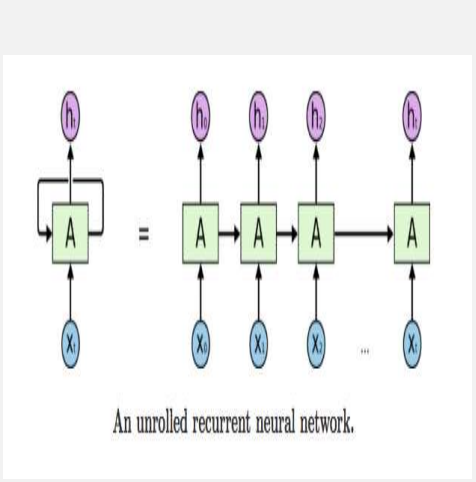
3) We compare the performance of BAT-MC with traditional deep learning methods, the BAT-MC model can extract information from each packet. By making full use of the structure information of network traffic, the BAT-MC model can capture features more comprehensively. 4) We evaluate our proposed network with a real NSL-KDD dataset. The experimental results show that the performance of BAT-MC is better than the traditional methods.

Algorithms

What is Recurrent Neural Network (RNN)?

Recurrent Neural Network is a generalization of feedforward neural network that has an internal memory. RNN is recurrent in nature as it performs the same function for every input of data while the output of the current input depends on the past one computation. After producing the output, it is copied and sent back into the recurrent network. For making a decision, it considers the current input and the output that it has learned from the previous input.

Unlike feedforward neural networks, RNNs can use their internal state (memory) to process sequences of inputs. This makes them applicable to tasks such as unsegmented, connected handwriting recognition or speech recognition. In other neural networks, all the inputs are independent of each other. But in RNN, all the inputs are related to each other.



An unrolled recurrent neural network.

First, it takes the X(0) from the sequence of input and then it outputs h(0) which together with X(1) is the input for the next step. So, the h(0) and X(1) is the input for the next step. Similarly, h(1) from the next is the input with X(2) for the next step and so on. This way, it keeps remembering the context while training.

The formula for the current state is

$$h_t = f(h_{t-1}, x_t)$$

Applying Activation Function:

$$h_t = \tanh (W_{hh}h_{t-1} + W_{xh}x_t)$$

W is *weight*, **h** is the *single hidden vector,* **Whh** is *the weight at previous hidden state,* **Whx** is the *weight at current input state,* **tanh** is the *Activation funtion,* that implements a Non-linearity that squashes the activations to the range[-1.1]

Output:

$$y_t = W_{hy}h_t$$

Yt is the *output state*. **Why** is the *weight at the output state.*

Advantages of Recurrent Neural Network

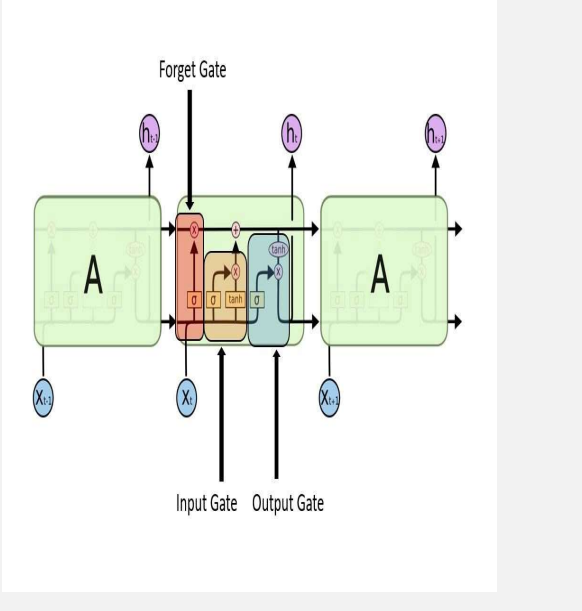
1. **RNN** can model sequence of data so that each sample can be assumed to be dependent on previous ones
2. Recurrent neural network are even used with convolutional layers to extend the effective pixel neighbourhood.

Disadvantages of Recurrent Neural Network

1. Gradient vanishing and exploding problems.
2. Training an RNN is a very difficult task.
3. It cannot process very long sequences if using *tanh* or *relu* as an activation function.

What is Long Short Term Memory (LSTM)?

Long Short-Term Memory (LSTM) networks are a modified version of recurrent neural networks, which makes it easier to remember past data in memory. The vanishing gradient problem of RNN is resolved here. LSTM is well-suited to classify, process and predict time series given time lags of unknown duration. It trains the model by using back-propagation. In an LSTM network, three gates are present:



LSTM gates

1. **Input gate** — discover which value from input should be used to modify the memory. **Sigmoid** function decides which values to let through **0,1.** and **tanh** function gives weightage to the values which are passed deciding their level of importance ranging from**-1** to **1.**

$$i_t = \sigma\left(W_i \cdot [h_{t-1}, x_t] + b_i\right)$$
$$\tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] + b_C)$$

Input gate

2. Forget gate — discover what details to be discarded from the block. It is decided by the **sigmoid function.** it looks at the previous state(**ht-1**) and the content input(**Xt**) and outputs a number between **0**(*omit this*)and **1**(*keep this*)for each number in the cell state **Ct−1**.

$$f_t = \sigma\left(W_f \cdot [h_{t-1}, x_t] + b_f\right)$$

Forget gate

3. Output gate — the input and the memory of the block is used to decide the output. **Sigmoid** function decides which values to let through **0,1.** and **tanh** function gives weightage to the values which are passed deciding their level of importance ranging from**-1** to **1** and multiplied with output of **Sigmoid.**

$$o_t = \sigma\left(W_o\ [h_{t-1}, x_t] + b_o\right)$$
$$h_t = o_t * \tanh\left(C_t\right)$$

RESULTS

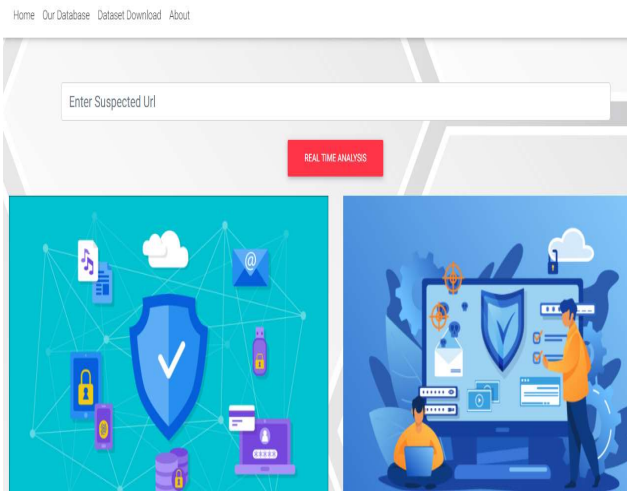


Fig 2: Home Screen

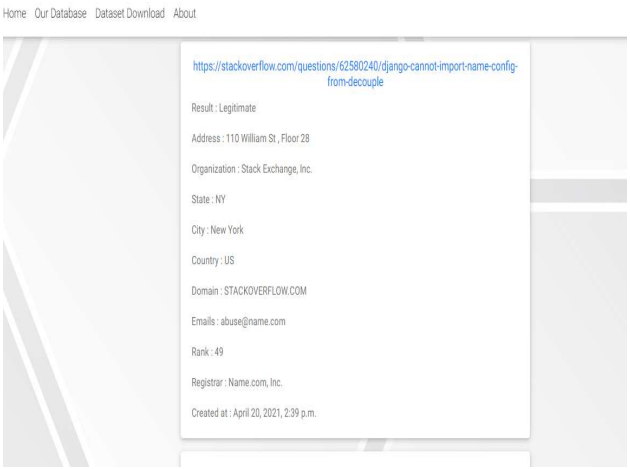


Fig 3: Results Page

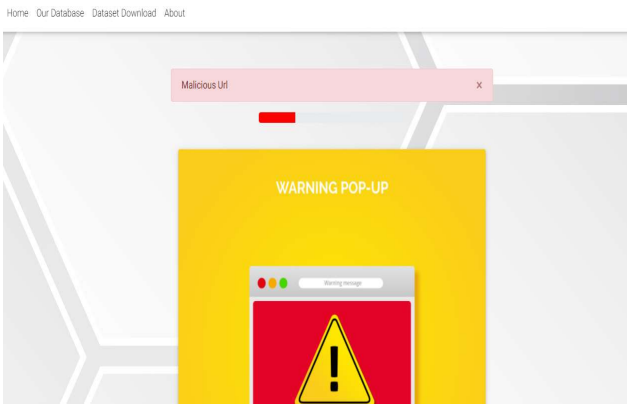
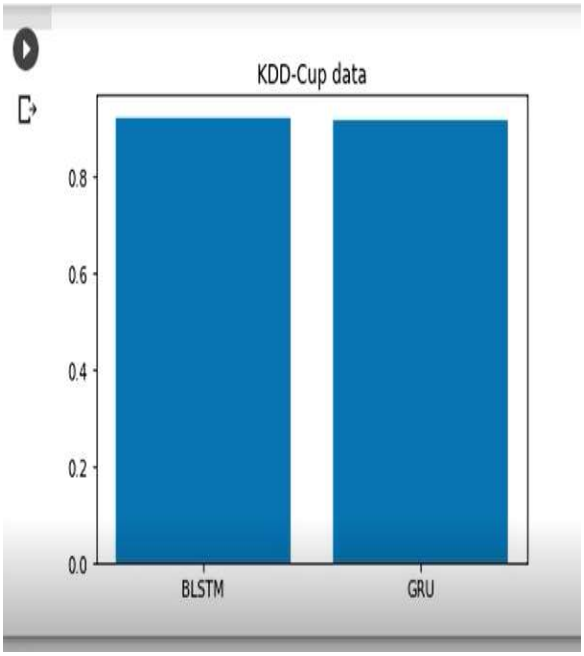


Fig 4: Malicious URL Detected



8. CONCLUSION

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

This model effectively avoids the problem of manual design features. Performance of the BAT-MC method is tested by KDDTest+ and KDDTest-21 dataset. Experimental results on the NSL-KDD dataset indicate that the BAT-MC model achieves pretty high accuracy. By comparing with some standard classifier, these comparisons show that BAT-MC models results are very promising when compared to other current deep learning-based methods. Hence, we believe that the proposed method is a powerful tool for the intrusion detection problem.

REFERENCES

[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. [11] R. C. Staudemeyer and C. W. Omlin, ‘‘ACM press the south African institute for computer scientists and information technologists conference - east London, south Africa (2013.10.07-2013.10.09) proceedings of the south African institute for computer scientists and information technologists co,’’ in Proc. South African Inst. Comput. Scientists Inf. Technol. Conf., 2013, pp. 252–261.

[12] S. Cornegruta, R. Bakewell, S. Withey, and G. Montana, ‘‘Modelling radiological language with bidirectional long short-term memory networks,’’ in Proc. 7th Int. Workshop Health Text Mining Inf. Anal., 2016, pp. 1–11.

[13] O. Firat, K. Cho, and Y. Bengio, ‘‘Multi-way, multilingual neural machine translation with a shared attention mechanism,’’ in Proc. Conf. North Amer. Chapter Assoc. Comput. Linguistics, Hum. Lang. Technol., 2016, pp. 1–10.

[14] H. Zhang, ‘‘Design of intrusion detection system based on a new pattern matching algorithm,’’ in Proc. Int. Conf. Comput. Eng. Technol., Jan. 2009, pp. 545–548.

[15] C. Yin, ‘‘An improved BM pattern matching algorithm in intrusion detection system,’’ Appl. Mech. Mater., vols. 148–149, pp. 1145–1148, Jan. 2012.

[16] P.-F. Wu and H.-J. Shen, ‘‘The research and amelioration of patternmatching algorithm in intrusion detection system,’’ in Proc. IEEE 14th Int. Conf. High Perform. Comput. Commun., IEEE 9th Int. Conf. Embedded Softw. Syst., Jun. 2012, pp. 1712–1715.

[17] V. Dagar, V. Prakash, and T. Bhatia, ‘‘Analysis of pattern matching

algorithms in network intrusion detection systems,'' in Proc. 2nd Int. Conf. Adv. Comput., Commun., Autom. (ICACCA), Sep. 2016, pp. 1–5.

[18] M. S. Pervez and D. M. Farid, ''Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs,'' in Proc. 8th Int. Conf. Softw., Knowl., Inf. Manage. Appl. (SKIMA, Dec. 2014, pp. 1–6. [

19] H. Shapoorifard and P. Shamsinejad, ''Intrusion detection using a novel hybrid method incorporating an improved KNN,'' Int. J. Control Automat., vol. 173, no. 1, pp. 5–9, Sep. 2017.

[20] J. Zhang, M. Zulkernine, and A. Haque, ''Random-forests-based network intrusion detection systems,'' IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 38, no. 5, pp. 649–659, Sep. 2008.

[21] B. Ingre and A. Yadav, ''2015 international conference on signal processing and communication engineering systems (spaces),'' in Proc. Int. Conf. Signal Process. Commun. Eng. Syst., 2015, pp. 1–15.

[22] B. Ingre, A. Yadav, and A. K. Soni, ''Decision tree based intrusion detection system for NSL-KDD dataset,'' in Proc. Int. Conf. Inf. Commun. Technol. Intell. Syst., 2017, pp. 207–218.