DESIGN AND DEVELOP INTRUSION DETECTION SYSTEM FOR DETECTING AND CLASSIFYING CYBER ATTACKS AT NETWORK LEVEL USING DEEP LEARNING MODELS

Dr. D.J. Samatha Naidu1 , C. Shalini2 ,

[1]Principal, APGCCS, Rajampeta, Kadapa, A.P. India

[2]MCA Department & APGCCS, Rajampeta, Kadapa, A.P. India

samramana44@gmail.com ; shalinicheri850@gmail.com

Abstract

Deep learning techniques are being widely used to develop an IDS (Intrusion Detection System) for detecting and classifying cyberattacks at the network level. In existing system many challenges raised since malicious attacks are continually changing and occurring in very large volumes requiring a scalable solution.

In proposed work a hybrid intrusion detection alert system using a highly scalable framework on commodity hardware server which has the capability to analyze the network and host-level activities. The framework employed distributed deep learning model with CNN (convolutional neural network) and LSTM (Long short term memory) for handling and analyzing very large scale data in real-time. In addition, we collected host-based and network based features in real-time and employed the proposed CNN and LSTM models for detecting attacks and intrusions. In all the cases, we observed that CNN and LSTM exceeded in performance when compared to the classical machine learning classifiers . To the best of our knowledge this is the only framework which has the capability to collect network -level and host-level activities in a distributed manner using CNN and LSTM to detect attack more accurately.

Date of Submission: xx-xx-xxxx Date of acceptance: xx-xx-xxxx

I. INTRODUCTION

The primary purpose of an intrusion detection system is to ensure that IT personnel are notified when there may be an attack or an intrusion into the network. A network intrusion detection system (NIDS) monitors inbound and outbound network traffic as well as data traversing between network systems. The IDS network tracks network traffic and activates warnings when unusual activity or known threats are observed, there by allowing IT staff to investigate more closely and take necessary measures to prevent or avoid an attack.

This article studies the identification of network interference based on convolution neural networks (CNN), LSTM and integrates convolution and grouping operations to help extract the function relationship between the results. This not only struggles to address the problem in conventional machine learning models. Deep extraction of the interaction between the features of the application and a deeper understanding of the interactions between features than the general neural network.

II EXISTING WORK

Traditional machine learning techniques are very successful in detecting interference, but have drawbacks, since the conventional machine learning system has to create sample characteristics artificially. Their success depends on their consistency. Researchers have implemented deep learning techniques to solve this problem. Gao et al implemented deep network trust in intrusion identification and performed better than many conventional machine learning approaches. Raman applied probabilistic neural networks to detection techniques.

Algorithms used in Existing Work:

- Using machine learning algorithms
  - K- means clustering
  - Bayesian classification
  - Random Forest Classification
- Using Neural Networks
- Using Deep Neural Networks

Limitations of Existing Work:

- Constant update of database with new signatures
- False alarm
- Accuracy is less

III PROPOSED WORK

we built a neural convolution network. The entire network is made up of there secret layers. The first 2 layers each comprise a secret layer comprising both a convolutional layer and a grouping layer. The third layer is an output size LSTM layer. With each hidden layer, the number of convolution nuclei is different. The network uses convolution cores and shared cores to increase efficiency by constantly expanding the network configuration. The number of conversions should improve accuracy. We build 2 convolution layers one with 64 filters and 128 filters on the other.

- The primary purpose of an intrusion detection system is to ensure IT personnel is notified when an attack or network intrusion might be taking place.
- Although we have different intrusion detection systems using machine learning approaches their accuracy is less.
- So we are trying to enhance the systems performance using deep learning model.
- In deep learning model we are going to use CNN i.e CONVOLUTION NUERAL NETWORKS model and LSTM i.e. LONG SHORT TERM MEMORYfor building an intrusion detection system.

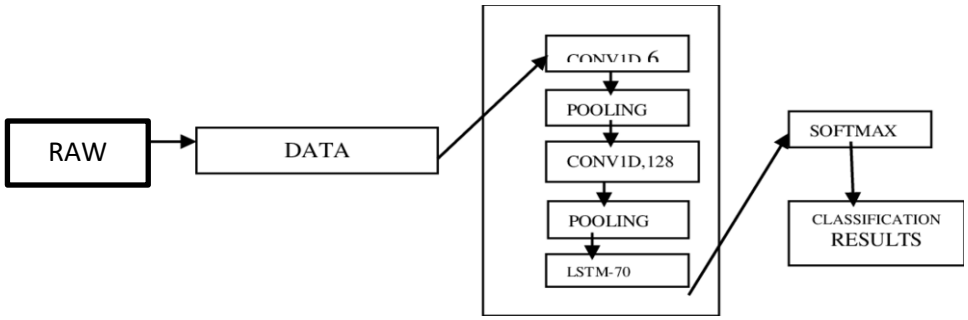

Figure1: Proposed model for intrusion detection system

Features of proposed work:

- Adaptability
- Pattern recognition and possibly detection of new patterns
- Learning abilities
- flexibility

Convolutional Neural Network

The Convolutional layers transform the input into a Convolution Neural network and transfer the output to the next line. Fully linked feed forward neural networks can be used to learn characteristics and to identify data. Given the very large input sizes associated with photos, where each pixel is a specific vector, a large number of neurons will be needed, also in a shallow architecture.

Long Short Term Memory

Short-term wide memory (LSTM) is a model of artificial recurrent neural network (RNN) that is used in deep learning. LSTM has input links, unlike normal advancing neural networks. It can process not only individual data points (such as images), but also entire data streams. LSTM, for example, refers to activities such as non-segmented handwriting recognition, voice recognition and the identification of irregularities in network traffic or Intrusion Detection Systems.

Proposed Architecture of CNN-LSTM Model

CNN based on are deep learning feature extraction models that have recently been shown to be quite effective in image recognition . As of today, numerous business giants like Google, Twitter, and Amazon are using the templates. And recently, Google researchers applied CNN to video data [11]. It is achieved by performing separate transformations of the filter values as trainable weights in the image. Several filters are added to each path, and they form feature maps along with Neural activation functions. A grouping scheme accompanies this, where only the relevant details of the function maps are group.

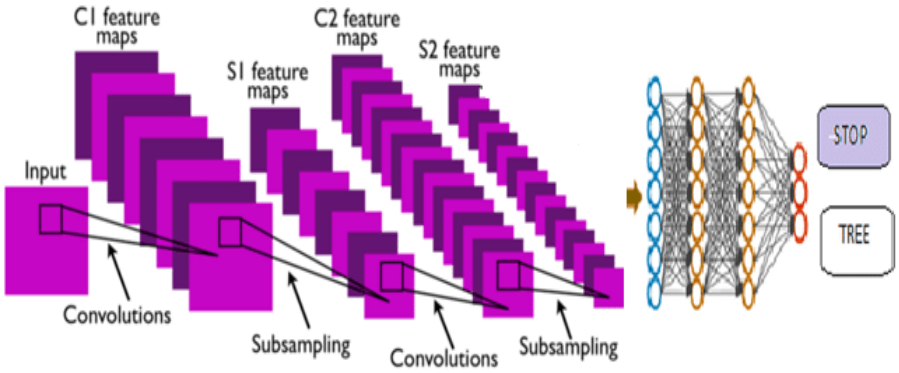

Figure: 2. CNN model for intrusion detection system

Experiments and Analysis

In this section we will revise the performance CNN-LSTM algorithm with SVM, DBN, CNN*. The Accuracy is measured with and compared with SVM, DBN and CNN*. CNN-LSTM an enumeration based hybrid approach algorithm has shown its better performance on Intrusion Discovery system.

Data Set

The data set used in this paper is the 10% of KDD99 data set. The data set contains 5 types of intrusions: Normal, DOS, R2L, U2R, and probing. Each intrusion is classified based on its features. We train the model based on this 10% of KDD99 dataset. This data set is split to train and test samples. It contains 494021 training samples and 311029 test samples. The distribution of various types of intrusions is shown in Table1

Attack Types	Training Examples	Testing Examples
Normal	97277	60592
Denial of service	391458	237594
Remote to User	1126	8606
User to Root	52	70
Probing	4107	4166
Total Examples	494020	311028

Table 1: Distribution of KDD99 dataset

Data Pre-processing

The dataset used contains attributes per record. It contains 41 features in which 38 are numerical and 3 are symbolic. So dataset need to be preprocessed separately. Heuristic based feature attribute selection was presented .Numerical characterization of symbolic features: We created and used a function encode_text_dummy for the three symbolic features, if we have red, blue, green,and we converted the 1Dimensional vector into a 3Dimensional vector. 2) Normalization of numerical features: There are various measurements for numerical details with numerical features; the scale of numerical element differs. Therefore, to reduce the effect of dimensional variations, numerical measurements must be performed .

Experimental Evaluation

In this experiment we calculated True Positives (TP) and True Negatives (TN) to calculate the Accuracy as:

$$AC = (TP+TN) / TP+TN+FP+FN$$

Among such, TP is properly classified number of attack behaviors; TN is properly classified number of usual behaviors; FP is misclassified number of usual behaviors; FN is misclassified number of attack behaviors.

IV RESULTS

The Accuracy of the proposed CNN-LSTM model is measured by setting the Convolution matrix size to 2, convolution duration is set with the duration of the pooling layer by using max pooling. Using the Adam optimization algorithm over convolution matrix the pooling algorithm performs the subsampling to minimize the error function.

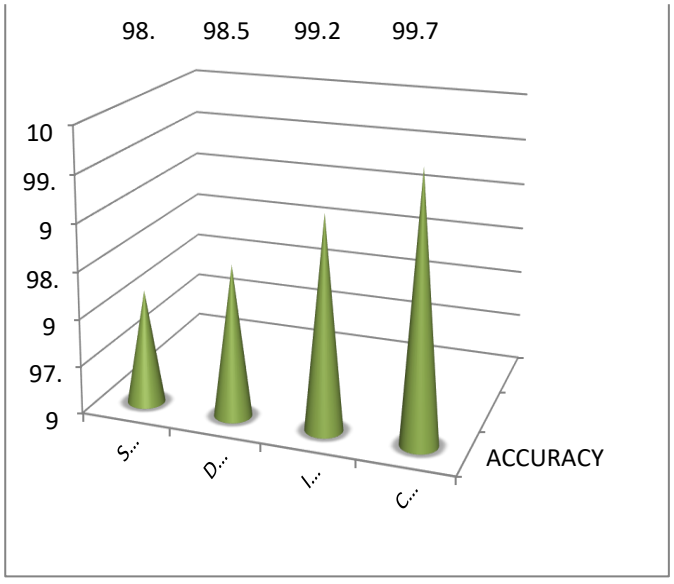

Figure:3 comparison between svm,dbn,cnn,cnn-lstm

V CONCLUSION

Applying the Convolution Neural Network algorithm to intrusion detection is an old concept that gives good accuracy but we tried to combine LSTM with CNN to get more accuracy and render machine more effective. This paper suggests a system by which Convolution Neural Network algorithm and LSTM algorithm are merged. The experimental findings indicate that this model will increase the precision of detection of human interference and boost the efficiency of the detection method for human invasion. It is also pragmatic that the projected representation outperformed with SVM, DBN, and CNN* with CNN-LSTM mode.

In past many machine learning algorithms are used for intrusion detection system like SVM, DBN, CNN. Now we proposed a model based on CNN and LSTM.

In future there will much advancement in developing intrusion detection systems. Transfer learning algorithms like GoogleNET and ResNET are also used to model intrusion detection systems.

VI REFERENCES

- K. Prasanna and M. Seetha, "Mining high dimensional association rules by generating large frequent k-dimension set," 2012 International Conference on Data Science & Engineering (ICDSE), Cochin, Kerala, 2012, pp. 58-63.
- M. G. Raman, N. Somu, K. Kirthivasan Et V. S. Sriram,"A Hypergraph And Arithmetic Residue-Based Probabilistic Neural Network For Classification In
- Intrusion Detection Systems, Neural Networks", Vol. 92, P. 89–97, 2017.
- M. E. Aminanto and K. Kim, "Deep Learning In Intrusion Detection System: An Overview," Proc. Int. Res. Conf. Eng. Technol., Pp. 1–12, 2016.
- N. Gao, L. Gao, Q. Gao Et H. Wang, "An Intrusion Detection Model Based On Deep Belief Networks", In Advanced Cloud And Big Data (CBD), 2014 Second International Conference On, P. 247–252,IEEE, 2014.
- Prasanna, K., Sankara Prasanna Kumar, M., Surya Narayana, G.: A novel benchmark K-means clustering on continuous data. Int. J. Comput. Sci. Eng. (IJCSE) 3(8), 2974–2977, 2011.
- R. U. Khan, X. Zhang R. Kumar, "Analysis Of Resnet And Googlenet Models For Malware Detection", Journal Of Computer Virology And Hacking Techniques, Aug 2018.
- R. U. Khan, X. Zhang, R. Kumar Et E. O. Aboagye, "Evaluating The Performance Of Resnet Model Based On Image Recognition", In Proceedings of the International Conference On Computing And Artificial Intelligence, ICCAI 2018, PP. 86–90, ACM, 2018.
- R. Kumar, Z. Xiaosong, R. U. Khan, I. Ahad Et J. Kumar, "Malicious Code Detection Based On Image Processing Using Deep Learning", In Proceedings Of The 2018 International Conference On Computing And Artificial Intelligence, ICCAI 2018, PP. 81–85, ACM, 2018.
- S. Venticinque A. Amato, "Smart Sensor And Big Data Security And Resilience, in Security And Resilience In Intelligent Data-Centric Systems And Communication Networks" PP. 123–141, Elsevier, 2018.
- S.Chung Et K.Kim,"A Heuristic Approach To Enhance the Performance of Intrusion Detection System using Machine Learning Algoritghms", In proceedings of the Korea Institute of Information Security and Cryptology Conference (Cisc-Wa15),2015.
- S. M. H. Bamakan, H. Wang Et Y. Shi, Ramp, "Support Vector Classification Regression; A Robust And Sparse Multi-Class Approach To The Intrusion Detection Problem", Knowledge-Based Systems, Vol. 126, P. 113–126, 2017.
- S. Jha, K. M. Tan Et R. A. Maxion, "Markov Chains, Classifiers, And Intrusion Detection, In CSFW, Vol. 1, P. 206, 2001.
- S.-J. Horng, M.-Y. Su, Y.-H. Chen, T.-W. Kao, R.-J. Chen, J.-L.Lai Et C. D. Perkasa, "A Novel Intrusion Detection System Based On Hierarchical Clustering And Support Vector Machines", Expert Systems With Applications, Vol. 38, No. 1, P. 306–313,2011.
- S. Peddabachigari, A. Abraham, C. Grosan Et J. Thomas, "Modeling Intrusion Detection System Using Hybrid Intelligent Systems", Journal Of Network And Computer Applications, Vol. 30, No. 1, P. 114–132, 2007.

- S. Vieira, W. H. L. Pinaya, And A. Mechelli, "Using Deep Learning to Investigate The Neuroimaging Correlates Of Psychiatric And Neurological Disorders: Methods And Applications," Neurosci. Biobehav. Rev., 2017.
- W. Leonard, "Resilient Cyber-Secure Systems And System Of Systems: Implications For The Department Of Defense, In Disciplinary