

A NEW DISTRIBUTED DENIAL-OF-SERVICE DETECTION SYSTEM IN CLOUD ENVIRONMENT BY USING DEEP BELIEF NETWORKS

Ibrahim Yousif IBRAHIM¹, Sefer KURNAZ²

¹Altınbaş University, Information Technology, Istanbul, TURKEY


²Altınbaş University, Computer Engineering, Istanbul, TURKEY

ABSTRACT. This study presents new method to detect Distributed Denial-of-Service (DDoS) attacks by using Deep Belief Networks (DBN). The input data which represented the DDoS features in cloud environment are first analyzed by using DBN to extracted high level and sensitive features. The output of the DBN wired to the classifier (SoftMax and SVM). The aim of using the DBN is to extracted features that have ability to present the best classification results and to speed up the processing time by reducing the dimension of features. In the last stage, the Classifier trained in supervised method to classify the features into two labels there is attack or not. The obtained results compared with common researches deal with cloud security.

1. INTRODUCTION

Several potential descriptions are to be found for cloud computing. Greatest of them emphasis on the expertise only. studies have been done in order to mixes all these dissimilar descriptions to come up with one (planned) unchanging meaning. Cloud computing can best be labelled as a huge pond which covers hardware, software and other facilities that can be retrieved finished the “cloud”. All these capitals can be retrieved when essential. In common suitcases the breadwinner of the cloud vends his service as pay-per-use. This funds that there is great suppleness in the apply of these services as additional capitals are continuously obtainable. The description as defined above still greeneries a lot of queries around what cloud computing really is. The huge pool as stated previous denotes to the offered hardware, software and facilities as providing by cloud providing governments. [1, 2].

Keyword and phrases. Cloud computing, DDoS, DBN, SoftMax, SVM.

 ahmedsoft97@yahoo.com; sefer.kurnaz@altinbas.edu.tr-Corresponding author
 0000-0002-6946-2030; 0000-0002-6946-2030

The cloud computing features and models provided in the previous section provide improved, enhanced, and low-cost services to customers. The above models that provide the above mentioned features are applied using various techniques, for example virtualization and multiple simulations. Technologies combined with deploying cloud service models and deploy cloud security vulnerabilities and vulnerabilities in conjunction with traditional IT infrastructure [9]. Security risks in the cloud may differ from the risks of traditional IT infrastructure, whether in nature, severity, or both. In the end there has to be somebody accountable for that all occurs as labelled overhead. There have to be sure purposes that chequered whether all normal events are shadowed by all the operators.

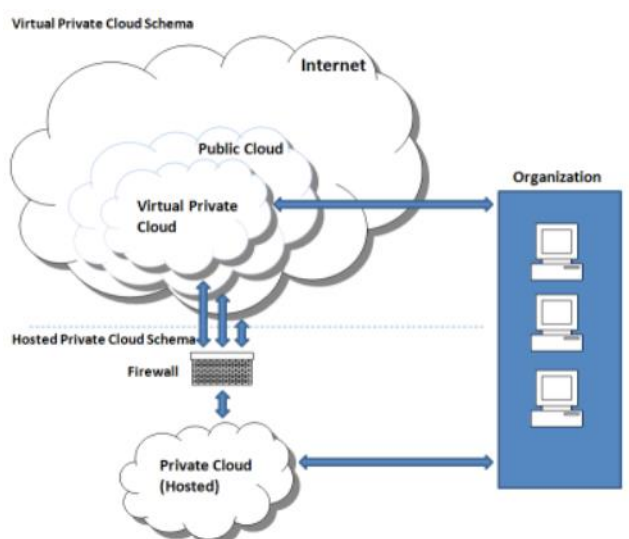


Figure 1. Private and Public Cloud Computing Structure [5].

2. SECURITY IN CLOUD COMPUTING

Data security is a mutual anxiety to all skills. Though, it develops a chief challenge when used to an unrestrained setting similar Cloud Computing. It is significant to differentiate between the security dangers related with all IT organizations and those presented by the applied of Cloud Computing. These dangers are usually related with open, communal and dispersed milieus. Consequently, when analysing the dangers, it is significant to distinct current glitches from those elevated by Cloud Computing. The cloud computing features and models provided in the previous section provide improved, enhanced, and low-cost services to customers. The above models that provide the above mentioned features are applied using various techniques, for

example virtualization and multiple simulations. Technologies combined with deploying cloud service models and deploy cloud security security vulnerabilities and vulnerabilities in conjunction with traditional IT infrastructure [6]. Security risks in the cloud may differ from the risks of traditional IT infrastructure, whether in nature, severity, or both. The ability to link cloud services as well with security concerns. Cloud transfer enables cloud users to switch between different clouds Service supplier without being influenced by the need to alteration delivery methods Tasks in various methods. In the end there has to be somebody accountable for that all occurs as labelled overhead. There have to be sure purposes that chequered whether all normal events are shadowed by all the operators.

3. DEEP-BELIEF NETWORKS (DBN)

A DBN can be distinct as a stack of restricted Boltzmann machines, in which each RBM layer connects with together the preceding and following layers. The bulges of any single layer don't connect with apiece additional crosswise. This stack of RBMs strength end with Softmax layer to make a classifier, or it might simply assistance cluster unlabeled data in an unsupervised learning situation. With the exclusion of the first and final layers, every layer in a DBN has a dual part: it helps as the hidden layer to the bulges that originate beforehand it and as the input layer to the bulges that originate afterward. It is a network constructed of single-layer networks [7]. The structure of DBN presented in the Figure 2.

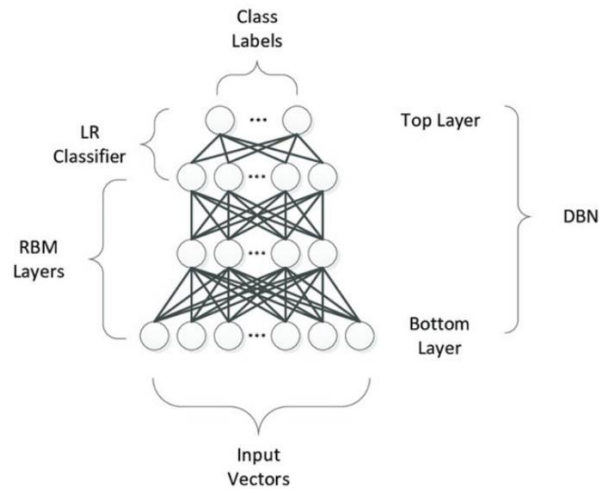


FIGURE 2. Deep-belief networks structure.

4. DDOS DETECTION FRAMEWORK BASED STACKED DBN BASED SVM AND SOFTMAX

The proposed method DBN used both unsupervised and supervised learning for gaining best effects which is the simple idea of deep learning.

DBN proposed for classifying the DDOS attacks which is new method displayed in Figure.3. As shown above the DDoS dataset contain from 27 attributes. Stacked DBN extracted high level feature from the input data. The reduce of dimension of feature mean gain in the computational time and it's also increase the performance of the classification. The number of neurons in the first and second hidden layers determined by using trial and error technique to select optimal features that produce the best results. Furthermore, the number of neurons in the hidden layers is not ruled by laws or mathematical model.

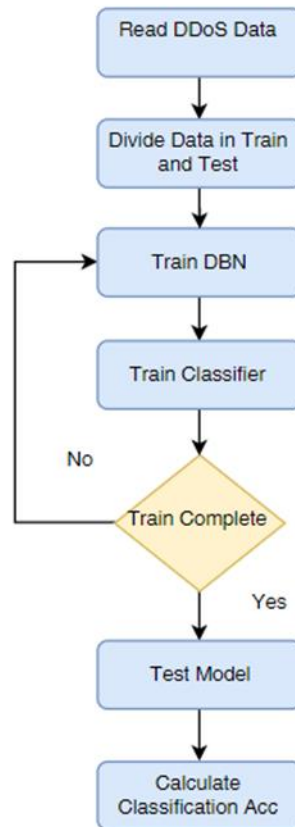


FIGURE 3. DDOS Detection Framework Based Stacked DBN.

The output of DBN wired to the SoftMax classifier which is supervised learning and trained to learn the classification of the extracted features from DBN that there is attack or not. Furthermore, DBN compared with SVM which the output of the DBN wired to the SVM and the SVM trained in supervised technique.

5. EXPERIMENTS AND DISCUSSION

In this section several experiment executed for DDoS detection in cloud environment. The data that obtained from [10] and [11] are to train and test the proposed methods. Several parameters are calculated and presented as shown in Eqs. (4.1), (4.2), (4.3).

$$ACC = \frac{(TP + TN)}{(P + N)} \quad (4.1)$$

$$TPR = \frac{TP}{(TP + FN)} \quad (4.2)$$

$$SPC = \frac{TN}{(FP + TN)} \quad (4.3)$$

The obtained results are compared in Figure 4.

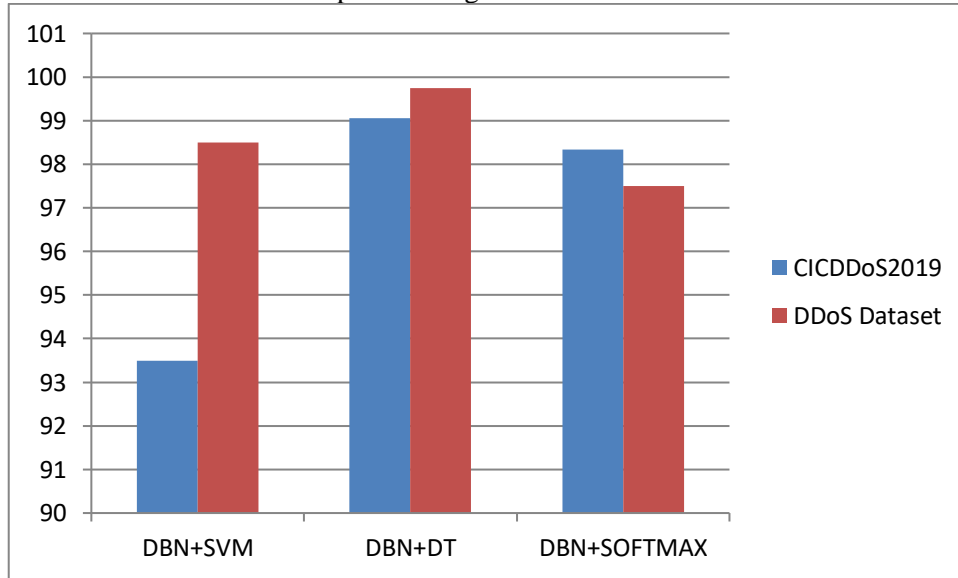


FIGURE 4. Results compression.

As shown in the Figure 4, the DBN+DT presented best results than DBN+SVM and DBN+SOFTMAX. This is new idea to use the DBN+DT to detect the DDoS in cloud environment. Furthermore, the execution time also compared between the two datasets in both CICDDoS2019 and DDoS dataset. The execution time of the proposed methods presented and compared in Figure 5.

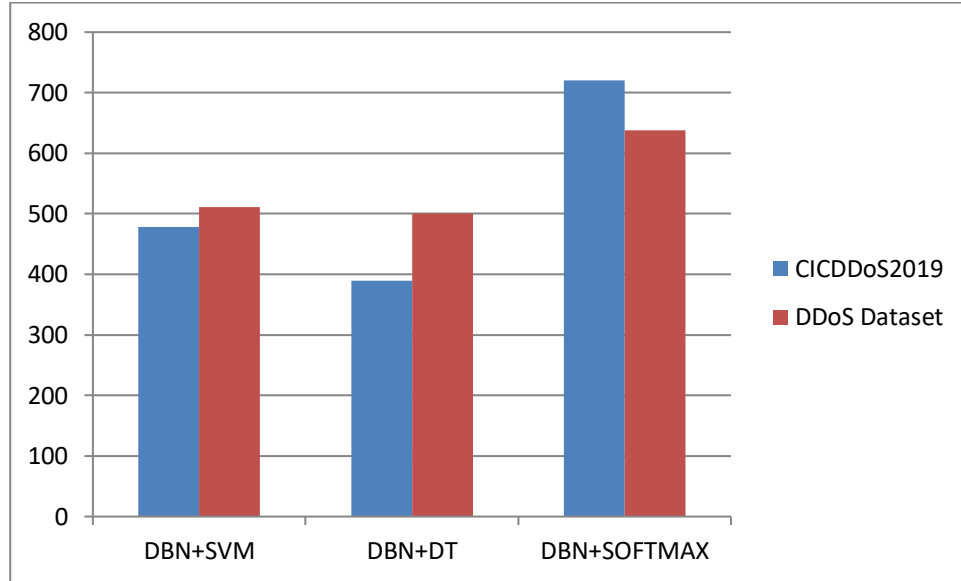


FIGURE 5. Execution time compression.

Furthermore, the author advises to use the DBN+DT in low size of data because its presented high accuracy and low computation time when compared with DBN+SVM and DBN+SOFTMAX.

Finally, our proposed methods compared with well-known researches presented in this field see Table 1.

The DBN+SVM presented 98.5 which is comparable when compared with several studies. The DBN+SVM presented best results from [9] Except MLP which three techniques proposed in this study. Furthermore, presented best result than [10] and lower than [11]. Finally, the DBN+DT presented best results than all presented in Table 1.

TABLE 1. Comparison with previous studies.

References	ACC (%)
MLP [8]	98.63
Random Forest [9]	96.91
Naïve Bayes [9]	97.29
SSAE-SVM [10]	97.65
Deep Auto-encoder +Taguchi Method [11]	99.60
Our Method (DBN+DT)	99.75
Our Method (DBN+SVM)	98.5

6. CONCLUSION

Cloud environment security, involves from several rules, strategies, policies and technologies that effort together to defend cloud-based systems, data and infrastructure. Furthermore, deep learning techniques were presented remarkable results in various fields such as image classification, video processing, and language recognition. The DBN is deep learning techniques which applied in various studies. In this study, two new methods presented to detect DDoS attack. The DBN+SVM and DBN+DT new two methods applied to DDoS detection problem in cloud environment. The proposed two new deep learning techniques presented remarkable results when compared with several studies based machine learning and other methods.

On the other hand, the execution time of our methods also suitable compared with SOFTMAX. The both DT and SVM presented lower execution time than SOFTMAX. Moreover, the DT presented faster exaction time than SVM in both datasets.

In the future studies, the author advice to applied other deep learning techniques such as CNN, RNN, and LSTM to the cloud computing security problems. Furthermore, the DBN can be combined with other classifiers to optimize the results. Moreover, the proposed method can applied to various classification problems such as object detection, image recognition, and diseases diagnosis.

REFERENCES

- [1] Mirkovic, J., Reiher, P., A taxonomy of DDoS attack and DDoS defense mechanisms, *ACM SIGCOMM Comput. Commun. Rev.*, 34(2) (2004), p. 39.
- [2] Wang, D., Yufu, Z., Jie, J., A multi-core based DDoS detection method, *Proc. - 2010 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. ICCSIT 2010*, 4 (2010), 115–118.
- [3] Karim, A.M., Kaya, H., Güzel, M.S., Tolun, M.R., Çelebi, F.V., Mishra, A., A Novel Framework Using Deep Auto-Encoders Based Linear Model for Data Classification, *Sensors*, 20 (2020), 6378.
- [4] Karim, A.M., Serdar, G.M., Tolun, M.R., Kaya, H., Çelebi, F.V., A new framework using deep auto-encoder and energy spectral density for medical waveform data classification and processing, *Biocybern. Biomed. Eng.*, 39 (2019), 148–159.
- [5] Karim, A.M., Karal, Ö., Çelebi, F.V., A New Automatic Epilepsy Serious Detection Method by Using Deep Learning Based on Discrete Wavelet Transform, 4 (2018), 15–18.
- [6] Karim, A.M. Güzel, M.S., Tolun, M.R., Kaya, H., Çelebi, F.V., A New Generalized Deep Learning Framework Combining Sparse Auto-encoder and Taguchi Method for Novel Data Classification and Processing, Volume 2018, Article ID 3145947, (2018), 13 pages.
- [7] Hang, B., Hu, R., Shi, W., An enhanced SYN cookie defense method for TCP DDoS attack, *J. Networks*, 6(8) (2011),1206–1213.
- [8] Karim, A.M., Çelebi, F.V., Mohammed, A.S., Software Development for Blood Disease Expert System, *Lecture Notes on Empirical Software Engineering*, 4(3) (2016),179–183.
- [9] Nashat, D., Jiang, X., Horiguchi, S., Router based detection for low-rate agents of DDoS attack, *Int. Conf. High Perform. Switch. Routing, HPSR 2008*, March (2008), 177-182.
- [10] Huang, M.L., Hung, Y.H. Lee, W.M., Li, R.K., Jiang, B.R., SVM-RFE based feature selection and taguchi parameters optimization for multiclass SVM Classifier, *Sci. World J.*, 2014.
- [11] Zuo, W.M., Lu, W. G., Wang, K.Q., Zhang, H., Diagnosis of cardiac arrhythmia using kernel difference weighted KNN classifier, *Comput. Cardiol.*, 35 (2008), 253–256.
- [12] Yu, Z., *et al.*, Prostatic Schistosoma japonicum with atypical immunophenotyping of individual glandular tubes: a case report and review of the literature, *Southeast Asian J. Trop. Med. Public Health*, 44(4) (2013), 568–573.