Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 8, August 2018, pg.1 – 7

Efficient DDoS Attack Detection and Prevention Framework Using Two-Level Classification in Cloud Environment

Ayman A. A. Ali[1], Prof. Saif Aldeen F. Osman[2]

[1]Lecturer, Taif University, Saudi Arabia

[2]Dean, Emirates College for Sciences and Technology, Sudan

[1] ayman.a.a.ali@hotmail.com; [2] saifefatoh@hotmail.com

Abstract— Cloud computing is one of the most important technologies in the IT industry. It has serious security threads such as the Distributed Denial of Service attack. In this kind of attack, the attacker targeted the victim cloud using zombie hosts. This paper proposes a novel framework to detect and prevent these types of attacks using feature extraction and selection methods to reduce the computation time and select optimal features from received packets to help in classification. This classification uses two-level method that is based on fuzzy type-2 logic and support vector machine - neural networks (SVM-NN). CloudSim simulator and KDD CUP dataset of DDoS attack are used to simulate the proposed framework. Finally, this framework shows effective results in terms of detection accuracy and false positive rate.

Keywords— Cloud Computing, DDoS, fuzzy type-2 logic, SVM-NN, feature selection, feature extraction.

I. INTRODUCTION

Cloud computing provides the infrastructure, platform and application as a pay-as-you-use manner to the end users. The main advantage of cloud computing is that the user is not required to purchase any expensive computer resources. The cloud computing allows access to data in a full virtualized manner by offering a single system view[8]. Because of its distributed nature, the cloud has multiple security threads. The most important security thread is the distributed denial of service DDoS attack. In this kind of attack, the attacker aims to use unsecured hosts over the Internet called zombies for sending a flood requests to the cloud system. The target of attacker is to make service unavailable for legitimate cloud users which affects the cloud availability [5].

In this paper, a novel framework is proposed to detect and prevent DDoS in cloud environment. This framework comprises two different techniques, feature extraction and feather selection. The feature extraction technique is used to extract redundant features from packets. The selection technique is used to remove irrelevant features to reduce the computation time. In addition, this framework provides two-level of classification based on fuzzy type-2 logic and SVM-NN to insure a good detection. Moreover, a prevention technique using a hash message authentication code (HMAC) is proposed to attain privacy and security for legitimate users' packets. Also, a black list is implemented to prevent attacks from the same attacker.

The paper proceeds as follows, In Section 2, the related work is discussed. In Section 3, the proposed system architecture is demonstrated. In Section 4, a simulation environment is installed. In Section 5, the simulation results are presented and discussed. Finally, the conclusion is introduced in Section 6.

II. RELATED WORK

Many techniques can be used to detect and prevent the DDoS attacks. Some of these techniques adopted feature selection and classification in an efficient way such as machine learning algorithm, supervised and unsupervised algorithms. Ensemble based multi-filter feature selection technique was addresed in [5] to select the optimal features from packets by combining the output of four filter methods such as information gain, gain ratio, chi-squared and relief. Furthermore, in the classification process, the decision tree considered only the features which are the outcomes of information gain filter. The main disadvantage of this technique is the high computation time of feature selection, due to combine output of four feature selection methods. However, the classification phase considers only the outcomes of information gain to detect attack by using decision tree method.

A Radial Basis Function Neural Network (RBF-NN) technique was proposed in [7] to detect the DDoS attacks. Feature selection was performed to detect the DDoS attack in cloud by using Bat algorithm. The main disadvantage of this technique is failed to detect the attacks in cloud system due to random selection of features. The correlation between the packets to detect attacks in the cloud was considered in [9]. The flow correlation co-efficient based protocol free detection algorithm was used to determine the correlation co-efficient between network flows. This technique was less efficient to detect DDoS attacks because there is possibility to anyone of the flow being normal or malicious. Based on correlation co-efficient, there is possibility to anyone in the network flow being normal or malicious. Hence, the technique is less efficient for detecting DDoS attacks in the system.

A new classifier detection system was proposed in [6] to identify the DDoS attacks in clouds. In this system, k- Nearest Neighbour was proposed to detect the DDoS attack which considers IP address to classify the packets as normal or malicious. The classification of packets is inefficient due to the consideration of single feature, in this system, the classification is performed by the k-NN classifier based on IP address of the packets. The IP address is inefficient to detect attacks in cloud system. Multi-variance correlation analysis-based detection approach was constructed in [1] to detect the DDoS attacks based on variance between the observed co-variance matrix and expected co-variance matrix. This method is less efficient to classify the packets as malicious or normal due to stable value of threshold matrix. The threshold matrix is not suitable for various types of network traffic to provide better classification results.

Multipath scheme was proposed in [4] to detect the DDoS attack based on path error count. The huge amount of information loss due to the transmission of packets in the malicious path which continues until the TCP keep alive time expired. The disadvantage of this system, the attacks are detected in multiple paths based on path error count and identified the path as attacked and broken path. However, the packets are transmitted in the attacked path until the TCP keep-alive time expired. It leads to information loss during the transmission process. Fuzzy min-max neural network was addressed in [2] to detect the DDoS based on minimum point, maximum point and membership function. DDoS detection was performed by three phases such as hyper box expansion, hyper box overlap and hyper box contraction. This detection system is only suitable for high frequent attacks due to limitation of fuzzy min-max neural network.

III. SYSTEM ARCHITECTURE

The proposed framework contains four phases to detect and prevent DDoS attack, namely; feature extraction phase, feature selection phase, detection phase, and prevention phase as displayed in Fig. 1. The following subsections introduce a brief discussion for each component.

A. *Feature Extraction phase*

The feature extraction is the first phase in the proposed framework. In this phase, the Correlation based Sequential Backward Selection is applied to calculate the degree of redundancy for each feature in the packet. Features with highest redundancy are eliminated one by one to extract the features.

B. *Feature Selection Phase*

The mutual information with recursive feature elimination is performed to select the best features for classification. In this process, the relevance between the features is calculated based on marginal probability distribution function of packets and the least relevance features are eliminated.

C. *Detection Phase*

The detection phase consists of two levels of classification processes. In level one, the packets are classified as normal, malicious and suspicious based on type-2-fuzzy logic classifier with consideration of features such as

packet count, congestion window record and duration. The normal packets are allowed to pass to cloud system for further process, while the malicious packets are dropped, and the suspicious packets are given as input to level two SVM based neural network. Level two classifies the suspicious packets into normal and malicious based on maximum margin between the packets. After that The IP address of the malicious packets is updated in the blacklist for preventing the resources from malicious users.

D. *Prevention Phase*

The user packets are subjected to blacklist that checks IP address of each packet whether it is presented or not in the list. If the IP address of the packet is presented in blacklist, it is identified as malicious and dropped. Otherwise, the user is authenticated by Hash Message Authentication Code (HMAC). By using this technique, we enhance the privacy of user by attaching HMAC with each packet which prevents the user packets from attackers.

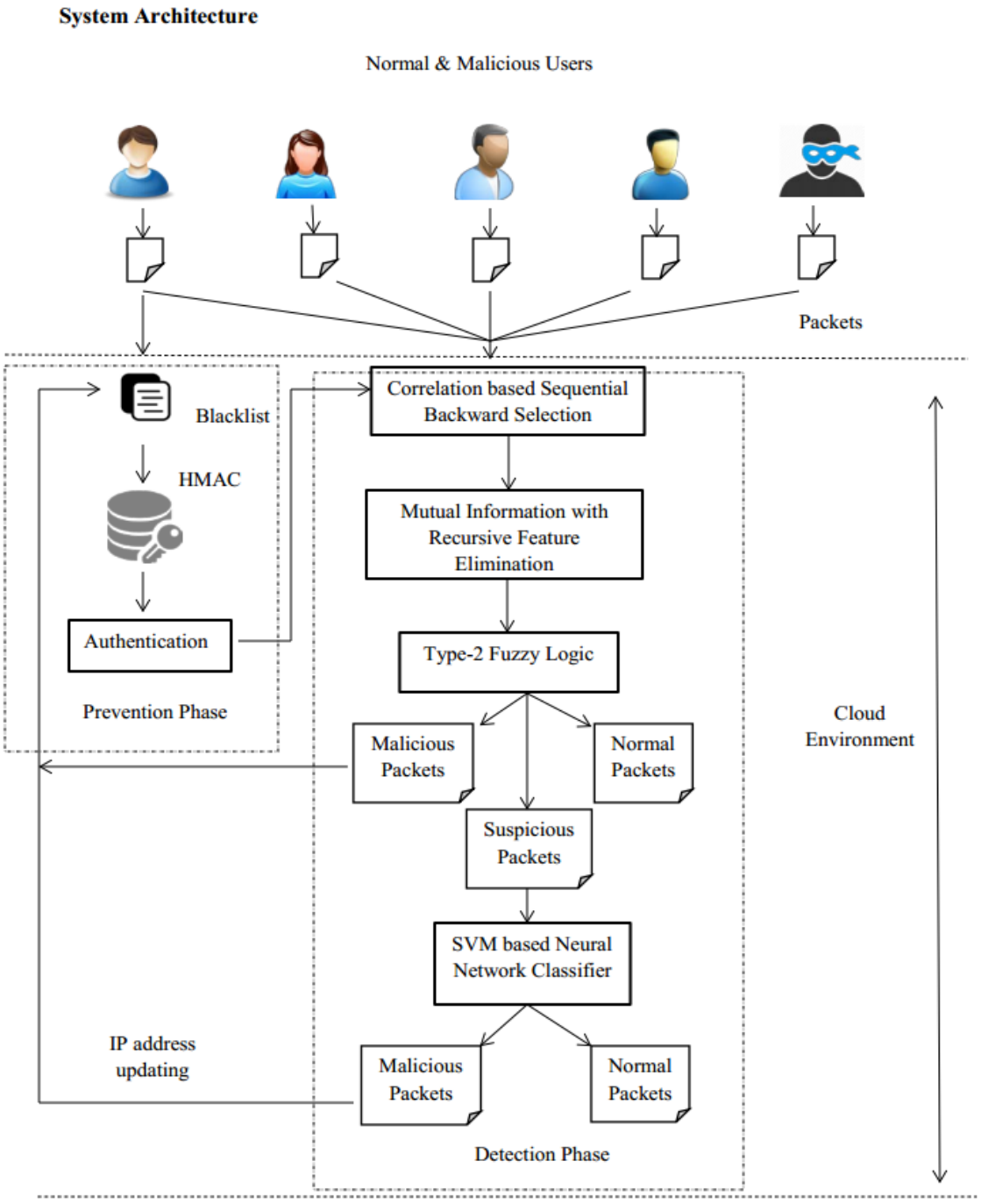

Fig. 1 Proposed system architecture.

IV. SIMULATION ENVIRONMENT

The framework of DDoS detection and prevention have been simulated using CloudSim toolkit, see Fig. 2. CloudSim is a multi-layered simulation module for cloud infrastructure and cloud services. Also, it's one of the most popular open source simulators for cloud computing in the academic environment as it's completely written by java. CloudSim designed in University of Melbourne, Australia by Cloud Computing and Distributed Systems (CLOUDS) Laboratory [3].

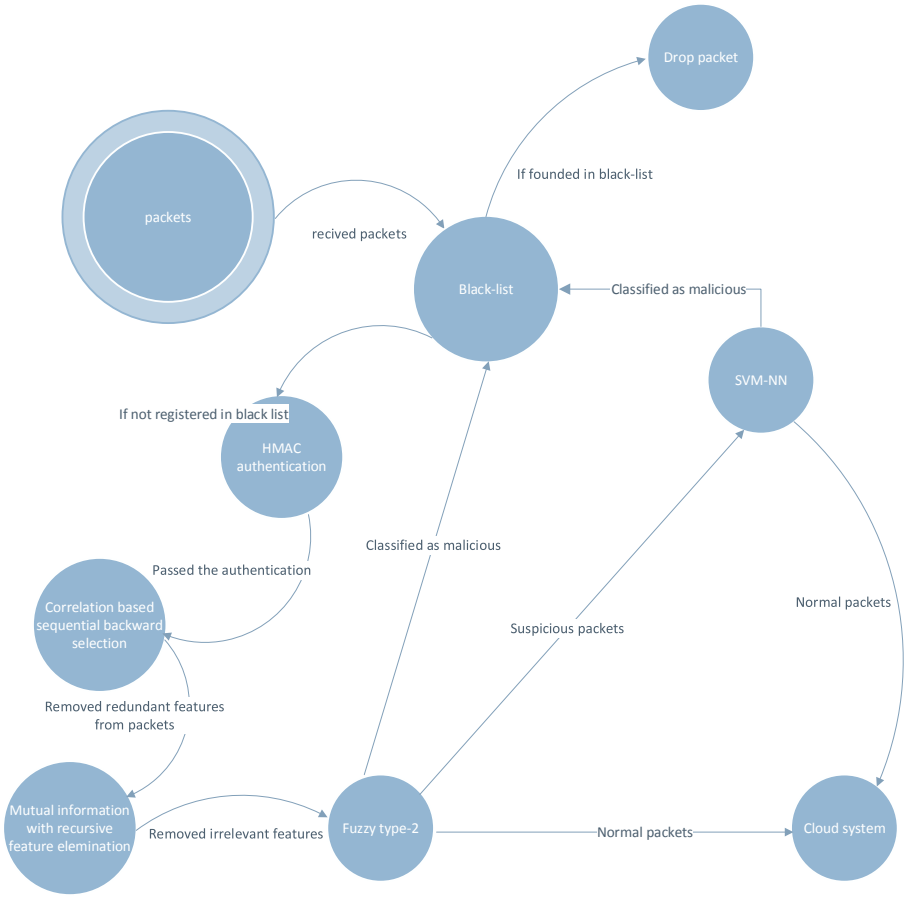

Fig. 2 Frame work of DDoS detection and prevention in cloud environment data-flow diagram.

The CloudSim supports the creation of cloud entities (VM's, datacentres, cloud brokers and services). In addition, it includes simulation of the virtual datacentre, management interfaces for VM's memory , storage and bandwidth [3].

Simulation of the proposed framework using CloudSim has several classes and modules in addition to two types of users, standard user and attacker. These users are constructed in the CloudSim internal engine. In the DDosAttackDetection class, the simulation creates 10 VM's act as a cloud user and 40 cloudlet acts as an attacker, with 512 MB ram and, CPU and image size equal to 10000MB, with bandwidth 1MB, and create cloud datacentres with ram 2GB, Linux OS and 64bit system architecture, and creation a list of cloudlets,

Classes used in the implementation:

A. *Black-List*

When the cloud receives some packets, the framework checks the black-list. Then, if the sender IP is registered in the constructed black-list, it means that the sender is attacker. So, the proposed framework will reject the incoming packets of that sender. But, if the sender is not registered in the black-list, the system will forward packets to the next level in framework. The black-list is stored in the m_BlackList variable, which is the array list of standard java. Additionally, this black-list is called from DDosDection class. Furthermore, the malicious host, which are detected by the Type-2 Fuzzy logic module and SVM-NN module, are stored in this black list.

B. *HMAC*

The next level is the message authentication by the HMAC algorithm, and SHA256 is used for HMAC. The HMAC is implemented by the function called "Signature". And SHA-256 algorithm and secret key generator algorithm are used for HMAC authentication level. If authentication is success, the packet will be given as an input to the Correlation based Sequential Backward Selection.

C. *Correlation based Sequential Backward Selection*

In order to remove any redundant features, the sequential backward selection module is the level-1 in order to select features for detecting the DDOS attack. This module calculates the degree of redundancy for each feature in the packet. And it is implemented in the sequential backward selection class, which is extended from feature selection class.

D. *Mutual information with recursive feature elimination*

This is performed to select the best features for classification. And it is implemented in mutual information class. This level aim to eliminate irrelevant features using the recursive feature elimination class, which is one of the feature selection methods. Moreover, selected features (packet-count, congestion window record and packet duration) are given to the detection level to classify normal and attacks packets.

E. *Detection level*

Here there is a two-level classification model. In the first level fuzzy logic classifies the packets as normal, malicious or suspicious, based on fuzzy rules with consideration of features selected. This first level implemented in the Type2FuzzyLogic class, the main function is the ComputeFuzzyCmeans. second level is the SVM based Neural Network SVM-NN, here we can change the SVM parameters and SVM kernels (POLY, LINEAR, SIGMOID, RBF) to decide if the suspicious packet is normal or malicious packet, the DDosDetection class use the SvmParameter, SvmModel and SvmProblem classes. All those steps shown in fig. 3 the algorithm.

DDoS D&P Algorithm:

Step1: Start with the Full set S
Step2: Remove the high redundant features fi from the set S
Step3: Update the set S as SK={S-fi}
Step4: Go to Step 2
Step5: calculate marginal probability between features
Step6: remove the less relevance rf features from the set S
Step7: Update the set S as SK={S-rf}
Step8: IF the packet-count> Max packet-count **and**
congestion window record> max congestion window **and**
packet duration> MAX packet duration **then**
Step9: It's malicious and update IP in black-list
Step10: IF the packet-count< Max packet-count **and**
congestion window record< max **and**
packet duration< MAX packet duration **then**
Step11: it's normal packet
Step12: else
Step13: IF the margin between packets> maximum margin **then**
Step14: It's malicious and update IP in black-list
Step15: else
Step16: It's normal packet

Fig. 3 Proposed DDoS detection and prevention algorithm.

V. RESULTS

In this section, the simulation results are discussed. The performance metrics, which are used in this simulation, are detection accuracy and false positive rate between the SVM kernels implemented.

Fig. 4 shows the detection accuracy percentage by every SVM kernel. The x-axis represent kernel used in second level of detection and y-axis represent percentage of detection. It shows that when we apply the Sigmoid Kernel, we can get the highest DDoS attack detection accuracy with 98.66%, and the worse result for POLY kernel with percentage 98.46%, in second place the LINEAR kernel with percentage of 98.6, and the third place the RBF with 98.56%.

Fig. 5 shows the false positive rate by every SVM kernel, the false positive used to calculate how many normal data is falsely detected as attack behaviour, We can know that when we apply the SIGMOID Kernel, we can get the lowest False Positive Rate with rate of 0.89%, and the worst case for POLY kernel with rate 1.02%, LINEAR kernel is second best case with rate of 0.94% and number three is RBF with rate 0.96%.

So, the SIGMOID kernel is our best one with high average of detection accuracy 98.66%, with less average of false positive rate 0.89%

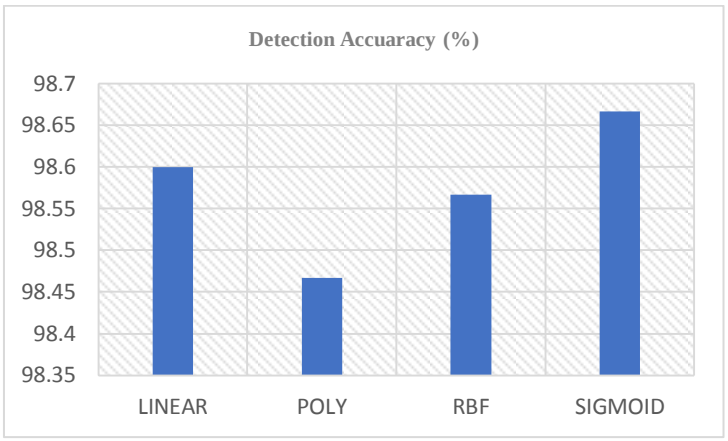

Fig. 4 Detection accuracy percentage.

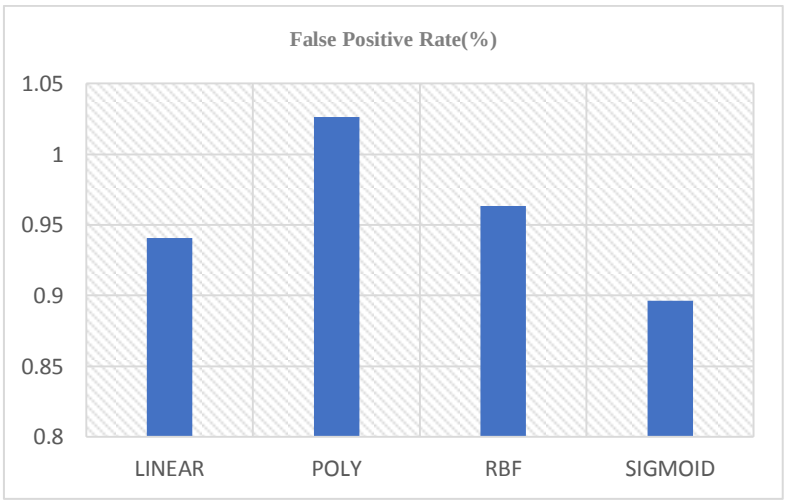

Fig. 5 False positive rate percentage.

VI. CONCLUSIONS

In this paper, a novel detection and prevention framework to detect and prevent DDoS attacks in the cloud system is proposed. This framework used two-level of classification and feature selection methods. Fuzzy type-2 logic is used to classify packets into normal, malicious or suspicious. If these packets are normal, it will complete their trip to the cloud. But, if these packets are malicious, it will be dropped, and their senders' IPs will be stored in the black list. Finally, if these packets are suspicious, then it will be given to the SVM-NN classifier to calculate the margin between packets using one of four SVM kernels which provides a decision if these packets are normal or malicious. The same actions for normal and malicious packets will be executed. For more security, the proposed framework used HMAC to ensure the authentication of legitimate users. This framework is simulated using CloudSim toolkit and KDD CUP dataset implementing DDoS attack types. The simulation results proved that the proposed framework is efficient because it reduced the false positive rate and provided a high detection rate.

REFERENCES

[1] A. ABORUJILAH and S. A MUSA, *Cloud-Based DDoS HTTP Attack Detection Using Covariance Matrix Approach*, Journal Comp. Netw. and Communic., 2017 (2017).

[2] C. AZAD and V. K. JHA, *Fuzzy min–max neural network and particle swarm optimization based intrusion detection system*, Microsystem Technologies, 23 (2017), pp. 907-918.

[3] R. N. CALHEIROS, R. RANJAN, A. BELOGLAZOV, #X00E9, S. A. F. D. ROSE and R. BUYYA, *CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms*, Softw. Pract. Exper., 41 (2011), pp. 23-50.

[4] Y. CAO, F. SONG, Q. LIU, M. HUANG, H. WANG and I. YOU, *A LDDoS-Aware Energy-Efficient Multipathing Scheme for Mobile Cloud Computing Systems*, IEEE Access, 5 (2017), pp. 21862-21872.

[5] O. OSANAIYE, H. CAI, K.-K. R. CHOO, A. DEHGHANTANHA, Z. XU and M. DLODLO, *Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing*, EURASIP Journal on Wireless Communications and Networking, 2016 (2016), pp. 130.

[6] A. SAHI, D. LAI, Y. LI and M. DIYKH, *An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment*, IEEE Access, 5 (2017), pp. 6036-6048.

[7] S. VELLIANGIRI and J. PREMALATHA, *Intrusion detection of distributed denial of service attack in cloud*, Cluster Computing (2017).

[8] W. VOORSLUYS, J. BROBERG and R. BUYYA, *Introduction to Cloud Computing*, in R. Buyya, J. Broberg and A. Goscinski, eds., *Cloud Computing*, 2011.

[9] L. XIAO, W. WEI, W. YANG, Y. SHEN and X. WU, *A protocol-free detection against cloud oriented reflection DoS attacks*, Soft Comput., 21 (2017), pp. 3713-3721.

