Received: April 23, 2018

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

SDN Based DDoS Attack Detection System by Exploiting Ensemble Classification for Cloud Computing

Sindia Thuraipandian Vimala [1]* **Julia Punitha Malar Dhas [2]**

[1]*Noorul Islam Centre for Higher Education, India*
[2]*Department of Computer Science and Engineering, Noorul Islam University, Kumaracoil, India*
* Corresponding author's Email: sindia.niu@gmail.com

Abstract: The usage of cloud computing is skyrocketing now-a-days and so is the network traffic. The adversaries intend to attack the cloud servers due to some intentional reasons. The most frequent attack is the data theft, which is followed by the DDoS attack. Though numerous solutions exist to handle DDoS attack, SDN based solutions for cloud computing is scarce. Understanding the need of the DDoS attack detection system, this work proposes a SDN based solution for detecting DDoS attacks in cloud computing environment, which relies on ensemble classifier. This work collects the real time traffic data with the help of Wireshark network analyser tool. The ensemble classification relies on the classifiers k-Nearest Neighbour (k-NN), Support Vector Machine (SVM) and Extreme Learning Machine (ELM). The performance of the proposed approach is analysed in terms of accuracy, sensitivity, specificity and the results are compared with the existing approaches. Additionally, in order to prove the potentiality of the ensemble classification, this work employs the classifier individually and the results are compared. Finally, the average attack detection time is measured and compared. From the experimental results, it is observed that the proposed approach proves better results in terms of accuracy, sensitivity and specificity.

Keywords: Cloud computing, DDoS, Ensemble classification.

1. Introduction

Cloud computing is one of the promising technologies that offers a broader range of services to the cloud users. The popular services being provided by cloud computing technology are infrastructure, platform, software and storage services. In order to access the services, the cloud users must comply with the cloud owner with a Service Level Agreement (SLA). Though, SLAs contain all the information about the service to be offered along with the security measures, the cloud users are still very much concerned about the security. Although the cloud servers are protected against attacks, certain attacks are triggered silently. It is highly challenging to sniff the occurrence of such attacks. For instance, Distributed Denial of Service (DDoS) is one such attack that aims to halt the actual operation of the cloud server temporarily. DDoS attack is the second common attack happening in the cloud computing environment [1].

As cloud computing paradigm is based on distributing computing, the cloud servers are distributed widely and cloud users can access the service from anywhere. This is the major advantage of the cloud computing environment and the concept of virtualization enhances the user experience. Due to some enmity or business clash, the cloud servers are attacked purposely, so as to stop the normal functionality of the cloud server. In spite of the maintenance of several replicas of the information, the cloud server has to be recovered from the attack. The DDoS is a silent attack, which triggers voluminous and abnormal traffic towards the cloud server. The cloud server cannot handle such unusual traffic and halts temporarily.

It is a tough task to recover the cloud server and bring it back to the normal state. The task of recovery involves considerable resources and energy,

which are unnecessary when the attacks are treated in advance. The DDoS attacks can be prevented before the happening of DDoS attack by cautious traffic tracking. In the literature, there are so many solutions to deal with DDoS attacks. However, Software Defined Networking (SDN) based solutions are very limited for DDoS attack detection. SDN is a technology that involves network controllers, which are responsible for controlling and managing all the activities being performed in the cloud environment. The network controllers build a rule base to distinguish between the normal and abnormal traffic.

The SDN based DDoS attack detection scheme embeds the code onto the network controller, such that the controller can handle all the situations, provided the corresponding code is fed. The main advantage of SDN is that it segregates the control and the data plane, such that all the controlling activities are done by the network controller and it observes the network with an eagle-eye. The network controller strictly follows the code being embedded, which is advantageous to achieve a particular task.

Taking the advantages of SDN and the severity of DDoS attack into consideration, this paper presents a DDoS attack detection and prevention system based on SDN. The proposed approach relies on ensemble classifier, which can effectively classify between the normal and abnormal traffic. The final decision is made by the maxvote strategy. Though there are numerous solutions to handle DDoS attacks, most of the existing solutions lack accuracy, speedy detection and efficiency [2]. The contributions of the work are as follows.

- This work collects the real-time traffic data with the help of Wireshark tool [3].
- Ensemble classification is incorporated in this work, which exploits k-Nearest Neighbour (k-NN), Support Vector Machine (SVM) and Extreme Learning Machine (ELM).
- This work does not rely on the decision of a single classifier, but a group of classifiers which results in better accuracy rates.
- In order to make quicker decision, this work employs three classifiers for the purpose of differentiation.
- The False Positive (FP) rates are considerably minimized, owing to the incorporation of ensemble classification.

The remaining content of the paper is organized as follows. The related review of literature is presented in section 2. The proposed DDoS attack detection scheme is explained in section 3. The performance of the proposed system is analysed in section 4. The concluding notes of the article are presented in section 5.

2. Review of literature

This section reviews the related state-of-the-art literature with respect to SDN based DDoS attack detection and classification.

A detailed survey on the topic of SDN's security is presented in [4], which focussed on security attacks and control. In [5], a DDoS defence system is proposed for SDN that is based on four modules such as attack detection trigger, attack detection, trace-back and mitigation. A trigger is generated to handle the DDoS attack. The attack detection system works in parallel, which is based on neural networks. The track-back system is based on SDN and a DDoS mitigation scheme is also proposed. However, the main drawback of this work is that it consumes more resources. A threat detection system for cloud computing is presented in [6], which is made by three important components such as monitoring agents, cloud infrastructure and operation centre. This work utilizes real world dataset to carry out the research. Though, this work involves more computational complexity.

In [7], an advance reservation access control system based on SDN. This work automates the reservation process by means of multi-domain SDN orchestration. This work utilizes token based authorization to promote end to end flow of the user request. This work automates the reservation at the cost of high computational overhead. A defence system for distributed denial of service is reviewed in [8]. This article classifies the DDoS cloud protection systems into knowledge and anamoly based systems for purpose of review. The security aspect of the networking technology is focussed in [9], which attempts to improve the security of wireless mobile networks with SDN concepts. This work focuses to enhance the overall security of the system and does not focus on a particular attack.

The quality aspect of SDN based solutions for mobile networks is presented in [10]. The important merits of SDN are discussed in this paper and the review of recent SDN techniques is presented. Cost aware routing system for geographically dispersed Cloud Data Centres (CDC) is proposed in [11]. This work constructs the cost minimization problem by Mixed Integer Non-Linear Programming (MINLP). Additionally, this work focuses on load balancing too. This work consumes more time and energy as

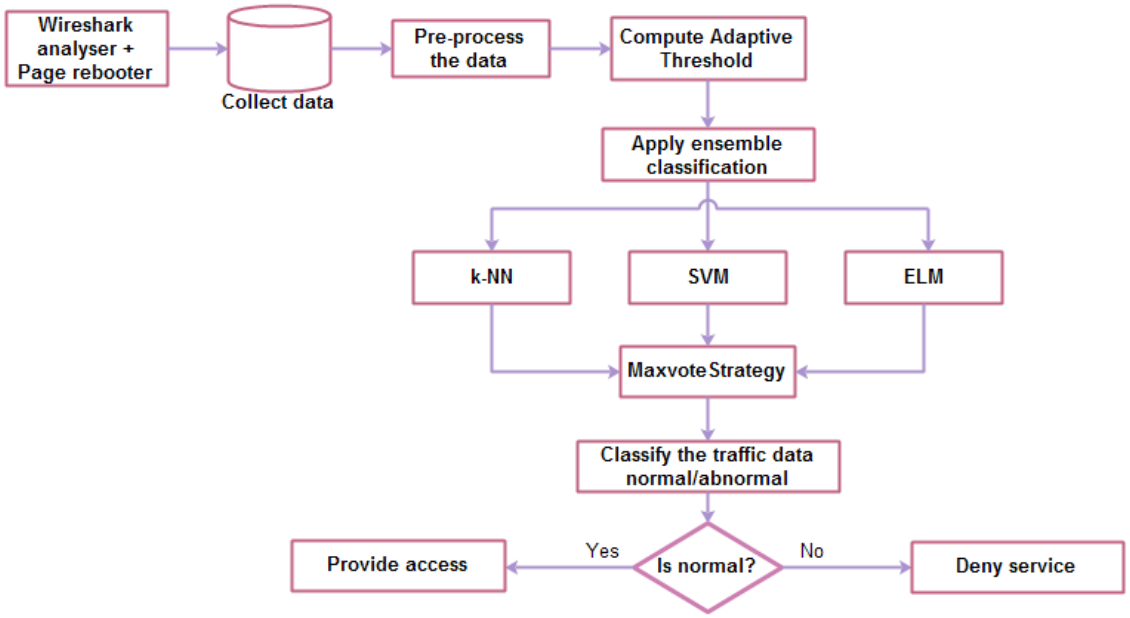

Figure. 1 Overall flow of the work

well. A work to protect cloud hosts in cloud data centres by means of SDN is proposed in [12]. This work is named as HostWatcher and is designed based on the concept of SDN, which aims to mitigate DDoS attacks. This work aims to mitigate the DDoS attacks with increased false positive alarms.

In [13], a detailed survey of the cloud DDoS attacks is discussed. The survey presents the recent developments of DDoS attacks with respect to the attack detection, mitigation and prevention mechanism. A DDoS attack mitigation system is proposed in [14], which combines the network governing and controlling systems together. This combination supports in achieving better speed and attack detection. The attack detection system of this work is based on graphical model, which can deal with different datasets effectively. This work serves better but the false positive rates are bit higher, so as to improve the accuracy rates. A traffic sampling strategy is proposed in [15], which computes the average sampling rate for each and every switch and the traffic flow is sampled based on the sampling rates. The traffic flow sampling is attained by SDN based framework. In [16], a software defined firewall rule generator for network intrusion detection is presented. However, this work is meant for detecting intrusions and the scope of the work is different.

In spite of the presence of numerous solutions for DDoS attack detection in cloud computing, SDN based solutions for the issue are very rare. Owing to the advantages of SDN mechanism, this work employs SDN for detecting DDoS attacks in cloud computing environment. Besides this, greater accuracy rates do not ensure minimal FP rates always. Thus, this work aims to present a SDN based solution for detecting DDoS attacks by ensemble classification in cloud computing environment. The main goal of this work is to reduce the FP rates rather than to attain greater accuracy rates. The following section elaborates the proposed approach.

3. Proposed DDoS attack detection system based on ensemble classification

This section presents all the ins and outs of the proposed DDoS attack detection system that is meant for cloud computing environment. Initially, the general workflow of the proposed approach is presented followed by the detailed description.

3.1 General workflow of the proposed approach

The main goal of this article is to present a DDoS attack detection system for cloud computing environment. The goal of the work is attained by incorporating ensemble classification methodology. The reason for the employment of ensemble classification methodology is to reduce the FP as much as possible. The objective is to minimize the FP rates, which paves way for conserving the resources by means of minimized time and computational overheads. The research goal is attained by decomposing the work into three phases and they are data collection, threshold fixation and classification. This work collects the real time traffic data of a specific site by exploiting wireshark

network analyser tool. The webpage is refreshed by pagereboot page [17]. The traffic data is collected and exported to a separate file, which is then accessed by the proposed approach. The overall flow of the work is presented in Fig. 1.

As soon as the data collection process is completed, the collected data are categorized with respect to the similarity measure. After this process, a threshold is fixed based on the learnt traffic data. The data is then fed to the classifier to distinguish between the normal and the abnormal traffic. The ensemble classification methodology relies on k-NN, SVM and ELM classifiers. All these classifiers make decision about the data and maxvote strategy is applied to take final decision. Based on the result, the traffic is differentiated into normal and abnormal.

The merit of ensemble classifiers is the reduced FP rates. Inclusion of single classifier may provide wrong results, which cannot be the case in ensemble classification. In ensemble classification, all the classifiers work independently to make decision and the maxvote strategy is applied to choose the majority of the decisions. Hence, least possibility is there to arrive at wrong results. The reason for the choice of three classifiers is to minimize the computational overhead. When more classifiers are involved in the decision process, the increase in time consumption and computational overhead is observed. As this work is meant for detecting the DDoS attack, it is essential to make decision at the earliest. Hence, the choice of three classifiers is optimal.

3.2 Data collection

This work attempts to exploit real time traffic data for analysis. The traffic data is collected by means of Wireshark network analyser tool, which can capture the real time traffic data. The page is refreshed by utilizing pagereboot, which automatically refreshes the page for every user defined time interval. The Wireshark network analyser captures the data till the user stops the application. Finally, the captured data is exported to the proposed system.

3.3 Threshold fixation for training

Let the tailored dataset possess $\{1,2,3,\dots N\}$ traffic records, which can either be normal or abnormal. The probability of a record (pr_i) to be normal or abnormal can be represented by the following equation.

$$pr_i = \frac{n}{N}; pr_i > 0 \quad (1)$$

In the above equation, n is any record in the database and N is the total number of records in the database. A record can be classified as normal or abnormal by means of threshold, which indicates that the value lies within threshold forms a class and the value above the threshold forms another class. This work can have two classes only, which are normal (cl_1) and abnormal (cl_2). This can be represented as follows.

$$cl_1 = \{1,2,3,\dots th\} \quad (2)$$

$$cl_2 = \{th+1, th+2, \dots N\} \quad (3)$$

The probability distribution (PD) of traffic data for the two classes is denoted by

$$x_1 = PD(cl_1) = \sum_{i=1}^{th} pr_i \quad (4)$$

$$x_2 = PD(cl_2) = \sum_{i=th+1}^{N} pr_i \quad (5)$$

This step is followed by the calculation of mean values of both classes y_1 and $y2$.

$$y_1 = \sum_{i=1}^{th} \frac{ipr_i}{x_1} \quad (6)$$

$$y_2 = \sum_{i=th+1}^{N} \frac{ipr_i}{x_2} \quad (7)$$

The sum (T_m) of the so computed mean values is computed by

$$T_m = x_1 y_1 + x_2 y_2 \quad (8)$$

The variances (σ^2) of the classes cl_1 and cl_2 are given by

$$\sigma_{cl1}^2 = \sum_{i=1}^{th} (i - y_1)^2 \frac{pr_i}{x_1} \quad (9)$$

$$\sigma_{cl2}^2 = \sum_{i=th+1}^{N} (i - y_2)^2 \frac{pr_i}{x_2} \quad (10)$$

When the variances of the classes are found out, the variance within the class (wc) and between the classes (bc) are found out by the following equations.

$$\sigma_{wc}^2 = \sum_{E=1}^{J} x_E \sigma_E^2 \quad (11)$$

$$\sigma_{Bc}^2 = x_1 (y_1 - T_m)^2 + x_2 (y_2 - T_m)^2 \quad (12)$$

From the within and between class variances, the total variance is computed by

$$\sigma_{TV}^2 = \sigma_{wc}^2 + \sigma_{Bc}^2 \quad (13)$$

The main intention of the concept of thresholding is to maximize the variance of BC and to minimize the wc. The optimal threshold is selected by

$$th = arg\left\{\begin{matrix} max \\ 0 \le th \le N \end{matrix}\{\sigma_{Bc}^2(th)\}\right\} = arg\left\{\begin{matrix} min \\ 0 \le th \le N \end{matrix}\{\sigma_{wc}^2(th)\}\right\} \quad (14)$$

In the above equation, th is the threshold. By this way, the threshold is selected and is used by the forthcoming process, which is classification.

3.4 Ensemble classification

This phase relies on three different classifiers which are k-NN, SVM and ELM classifiers. The decisions of all the classifiers are obtained and the maxvote strategy is applied. The maxvote selects the decision with majority votes. This makes the entire decision more accurate with reduced FP rates. The following subsections provide the work principle of all the three classifiers. The classifiers are trained with the traffic data along with the knowledge about the threshold.

3.4.1. k-NN classifier

The k-NN classifier is a supervised classifier, which gains knowledge from the training data and equips itself to distinguish between the normal and abnormal traffic. The k-NN is explained in [18]. The classifier computes the Euclidean distance between the obtained traffic data and the trained dataset. The standard Euclidean distance is computed by

$$E_D = \sum_{i=1}^{N} \sqrt{u_i^2 - v_i^2} \quad (15)$$

In the above equation, u_i and v_i are data items. The choice of ' k ' determines the quality of classification. Hence, the value of k must be chosen with intense care and it depends on the traffic data. It is difficult to set the value of k explicitly and it is not effective. Hence, this work employs k-fold cross validation, which selects the k value by itself. The process is carried out by subdividing the training data into several k entities and a single entity is assigned as the test entity and the rest of the entities are treated as the training entities. This process is carried out for k times by changing the test entity, until all the entities have been chosen as the test entity. Finally, the mean value is found for the obtained k results and this value is fixed as k. This way of k value fixation is optimal and improves the Quality of Service (QoS), as the human intervention is not required. By this way, the k-NN classifier performs to distinguish between the normal and the abnormal traffic data.

3.4.2. SVM classifier

SVM is a supervised classification algorithm, which is trained with the collected traffic data along with the threshold being computed [19]. Let there are {1,2,3,…N} traffic data that has to be classified as normal and abnormal. The two different classes are separated by means of a hyperplane, which has to be chosen carefully, as the classification accuracy depends on the hyperplane. The hyperplane is separated by the following equation.

$$f(x) = \sum_{i=1}^{N} \beta_i \psi_i(cl_1, cl_2) + th \quad (16)$$

In the above equation, β_i is the lagrange multiplier that segregates the hyperplane of the classifying area $\psi_i(cl_1, cl_2)$. The threshold being employed to classify between the normal and abnormal data is denoted by th. By this way, SVM makes decision to classify between the normal and abnormal traffic data.

3.4.3. ELM classifier

ELM is a promising classifier and the learning speed of the ELM is quite faster [20]. Let the traffic data is denoted by (x_i, y_i), which can be represented as follows. $x_i = [x_{i1}, x_{i2}, \dots, x_{in}]^T \in D^n$ and x_i is the i^{th} training entity in n^{th} dimension. $y_i = [y_{i1}, y_{i2} \dots, y_{ic}]^T \in D^c$ represents the i^{th} label of the train dataset with c^{th} dimension, where c is the number of classes being involved in the classification process. In this case, the number of classes is 2. A Single hidden Layer Feed forward Neural network (SLFN) is formed as follows.

$$\sum_{j=1}^{N} \gamma_i q(wt_j . x_i + b_j) = y_i;\ i = 1,2, \dots, n \quad (17)$$

In the above equation, wt_j is the weight that can be represented by $\left[wt_{j1}, wt_{j2}, \dots, wt_{jn}\right]^T$. This wt_j connects the j^{th} neuron with the input neurons and j is represented as $j = [j1, j2, \dots, j_c]^T$. The wt_j interlinks the j^{th} hidden neuron with the output neurons. The bias of j^{th} hidden neuron represented by b_j.

Consider H_l as the hidden layer output matrix of the classifier, which makes sense that the j^{th} column of H_l indicates the j^{th} hidden neurons

output vector with respect to the inputs $x_{i1}, x_{i2}, \ldots, x_{in}$.

$$H_l = \begin{bmatrix} ac_f(wt_1.x_1 + b_j) & \ldots & ac_f(wt_N.x_1 + b_N) \\ \vdots & \vdots & \vdots \\ ac_f(wt_1.x_n + b_j) & \ldots & ac_f(wt_N.x_n + b_N) \end{bmatrix} \quad (18)$$

$$\gamma = \begin{bmatrix} \gamma_1^T \\ \vdots \\ \gamma_N^T \end{bmatrix} \quad (19)$$

$$R = \begin{bmatrix} r_1^T \\ \vdots \\ r_N^T \end{bmatrix} \quad (20)$$

The matrix form is represented as

$$H_l \gamma = R \quad (21)$$

Output weights are calculated by the norm least-square solution and is represented by

$$\gamma = H_l{}^{\dagger} R \quad (22)$$

In the above equations, $H_l{}^{\dagger}$ is the HL's Moore-Penrose generalized inverse. During the process of training the number of classes, hidden neurons and activation function ac_f are passed. The training entities are represented by $\{x_i, y_i\}$ and the classifier is trained with the help of γ, as in eqn. (22). Thus, the ELM classifies between the normal and the abnormal traffic. The overall algorithm is presented below.

Proposed DDoS attack detection system

Input : Traffic data
Output : Attack detection
Begin
For all collected data
Compute the similarity between the data;
Impart knowledge to the ensemble classifiers;
Obtain decisions from all the classifiers;
Apply maxvote strategy;
Select the dominant decision;
Declare the decision as final;
End for;
End;

Now, the final decisions of all the classifiers are collected and the maxvote strategy is applied. The objective of maxvote strategy is to pick up the decision with majority votes. This work involves three classifiers and hence there are eight possible cases. The final decision is based upon the decisions of all the classifiers and the matrix is formed. Each column of the matrix represents the classifiers k-NN, SVM and ELM.

$$Dec_m = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} \Rightarrow FDec_m = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \quad (23)$$

In the above equation, Dec_m is the decision matrix and $FDec_m$ is the final decision matrix. The Dec_m is the combination of the decisions provided by the classifiers and the $FDec_m$ is obtained after the application of maxvote strategy. In the first case, two classifiers end up with abnormal traffic and so the final result is abnormal. Similarly, the majority of votes is taken into consideration to make up the final decision. This work shows promising results, as multiple classifiers are involved in the process of classification. The forthcoming section evaluates the performance of the proposed approach.

4. Experimental results and discussion

The simulation of this work is carried out in a stand alone system with the configuration of 16 GB RAM and 7th generation Intel core processor with 4 MB cache, 3.5 GHz. The work is simulated by using Java. The traffic data is collected by the wireshark network analyser tool, which is an opensource. The performance of the proposed work is analysed in terms of accuracy, sensitivity, specificity and execution time. The experimental outcome of the proposed approach is compared against anti-DDoS [5], DDoS attack protection [14], suspicious traffic sampling [15].

Accuracy is the important performance metric that measures the classification accuracy of the DDoS attack detection system. The classification accuracy of an attack detection system must be as high as possible. As the attack detection system roots on the security, high accuracy rates detect the attacks. Conversely, lower accuracy rates do not satisfy the objective of an attack detection system. Sensitivity rate measures the correctness of the attack detection system with respect to the sum of correctly identified attacks and the attacks that are

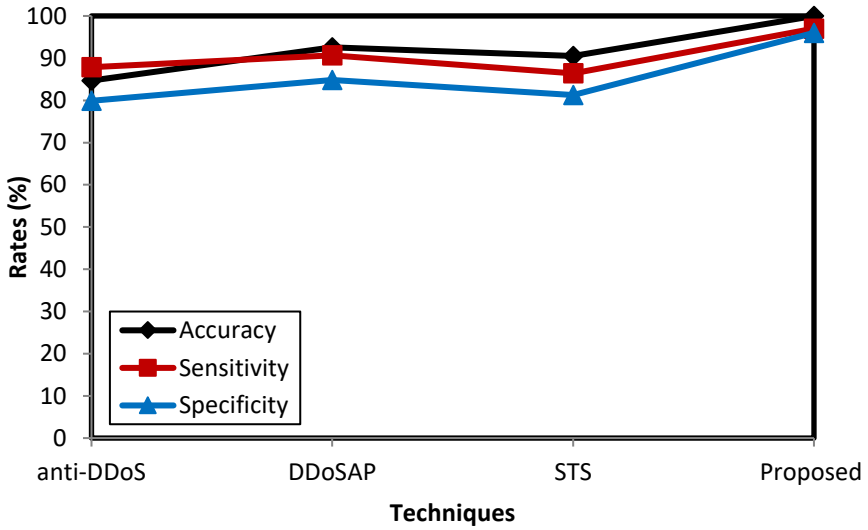

Figure. 2 Performance analysis w.r.t accuracy, sensitivity and specificity

not detected. The sensitivity rates are expected to be greater, which means that the FN rates are considerably minimal. The lesser the FN, the greater is the sensitivity rates.

Specificity rate is fraction of the correct classification of normal traffic rates against the summation of normal traffic data, which is misclassified as attack and the traffic data that is correctly classified as normal. Specificity rates depend on the FP rates, which makes sense that the greater the specificity rate, the lesser is the specificity rates. When the FP rate is 0, then the system can achieve cent percent specificity. Similarly, cent percent sensitivity is achieved, when the FN rates is zero. The following equations represent the computation of accuracy, sensitivity and specificity respectively.

$$detection_{accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (24)$$

$$detection_{sensitivity} = \frac{TP}{TP+FN} \times 100 \quad (25)$$

$$detection_{specificity} = \frac{TN}{FP+TN} \times 100 \quad (26)$$

In the above equations, TP, TN, FP, FN are True Positive, True Negative, False Positive and False Negative respectively. The experimental results are presented in Fig.2.

From the experimental results, it is observed that the accuracy of the proposed approach is greater than the analogous techniques. The reason for the better performance of the proposed approach is the incorporation of the ensemble classification. The classification result of the proposed approach does not rely on a single classifier but ensemble classifiers. Obviously, the ensemble classification enhances the accuracy rates. The accuracy rate of the proposed approach is cent percent and the second better performer is the DDoS attack prevention scheme that shows 92.5 percent. The least performer among all the approaches is the anti-DDoS, which shows 84.7 percent.

Though the accuracy rate has nothing to do with the sensitivity rates, the proposed approach shows greater sensitivity rate, which is 97 percent. Sensitivity rates are inversely proportional to the FN rates. False Negative rate increases, when the attack detection system misclassifies the abnormal traffic as normal traffic. This is really harmful for the attack detection system, as the system allows service to the node which has to be blocked. Finally, the DDoS attack may happen, which is not favourable. This is the case in which the attack detection system cannot distinguish between the traffic data. On analysis, the sensitivity rate of the proposed approach is greater by showing the value of 97 percent. The second performer with great sensitivity rate is the DDoS attack prevention system that shows 90.7 percent.

The specificity rate of the proposed work is then evaluated. When the specificity rate of an attack detection system is greater, then it indicates that the FP rate is minimal. FP rate increases when the attack detection system claims the normal traffic to be abnormal. This is equally harmful to the system, as that of the FN rate. FP rates may boost up the accuracy rates, however higher FP rates triggers the system with increased false alarms. These false alarms alert the controller, which consumes more

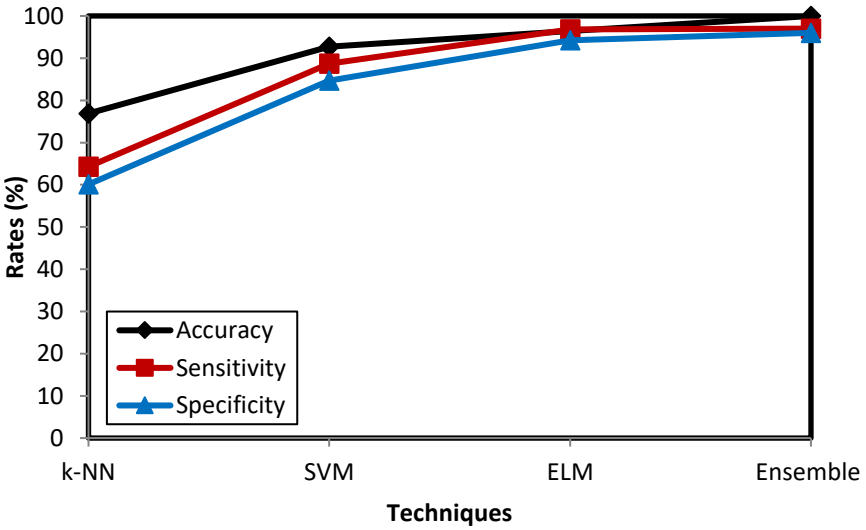

Figure. 3 Performance analysis w.r.t classifiers

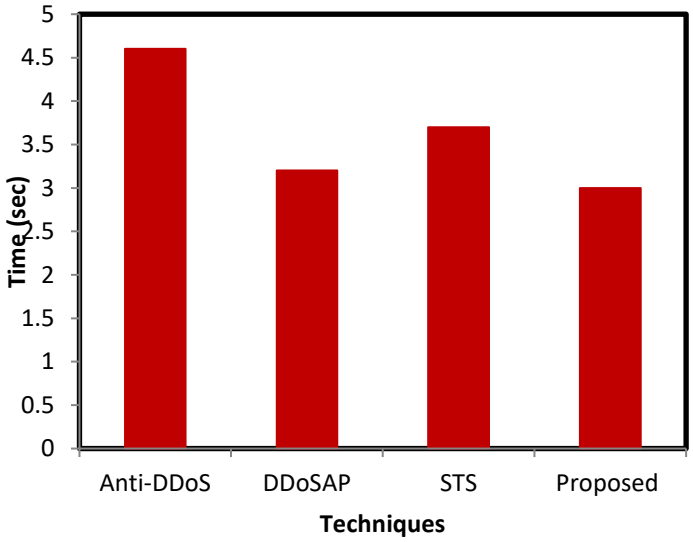

Figure. 4 Average detection time analysis

energy and resources. This is not beneficial to the attack detection system. Hence, the main objective of this work is fixed to reduce the FP rates and the specificity rates being shown by the proposed work is 96 percent. The least specificity value is shown by the anti-DDoS system, which is 79.9 percent.

The power of ensemble classification is justified by employing the classifiers individually. For instance, the attack detection system is classified with individual classifier and the results are presented in Fig.3.

From the experimental results, the potentiality of ensemble classifier is justified. This work computes the accuracy, sensitivity and specificity values by incorporating all the classifiers individually and the results are compared against the ensemble classifier. Out of all the classifiers, k-NN is the least performing classifier with 76.9 percent accuracy rates. The SVM and ELM classifiers perform more or less similar to each other with the accuracy rates of 92.7 and 96.4 percent respectively. The sensitivity and specificity rates of SVM and ELM classifiers are 88.7, 84.7 and 96.8, 94.2 precent respectively. Though the results of SVM and ELM are satisfactory, the ensemble classification technique provides better results. The time complexity of the proposed approach is then computed and compared with the existing approaches. Fig. 4 shows the experimental results.

Most of the DDoS attack detection systems consumes more time to process the traffic data. This is because of the incorporation of complex algorithms and methodologies to distinguish

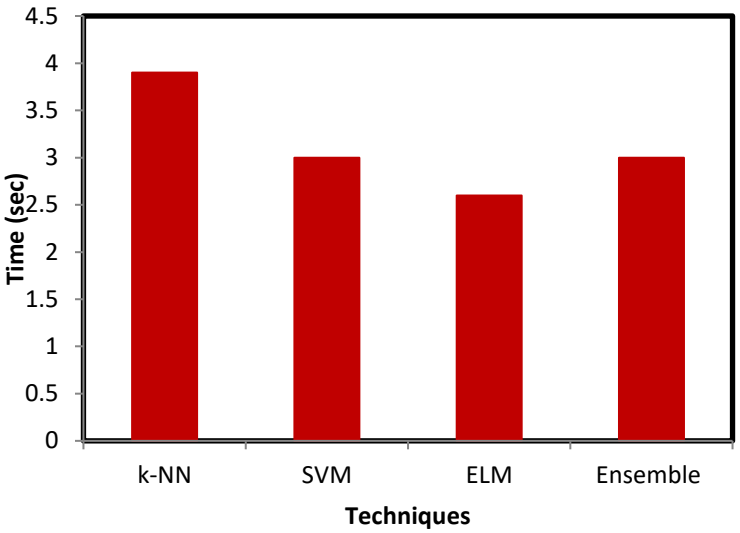

Figure. 5 Detection time analysis w.r.t classifier

between the traffic data. The proposed approach employs lightweight techniques, so as to reduce the time consumption. Additionally, the reduced time consumption contributes in attaining energy conservation as well. The average attack detection time of the proposed approach is three seconds, whereas the maximum time for attack detection is 4.6 seconds and is shown by the Anti DDoS system. The coming section measures the average attack detection time by employing the classifiers individually and the results are given in Fig.5.

On analysis, it is found that the ensemble classifier consumes time greater than the time consumption of SVM and ELM. However, on considering the accuracy, sensitivity and specificity rates, the time consumption of ensemble classifier is reasonable. k-NN classifier consumes more time than the ensemble classifier, because it processes the record individually. The performance of the proposed approach is satisfactory in terms of accuracy, sensitivity and specificity rates. Thus, the objective of the DDoS attack detection system is attained.

5. Conclusion

This article proposes a SDN based DDoS attack detection system that exploits ensemble classifier. The main objective of this article is to minimize the FP rates as much as possible. This is because of the fact that FP rates trigger unnecessary alarms, which results in increased time consumption and computational overhead. In order to achieve the goal, this work utilizes ensemble classification technique that employs k-NN, SVM and ELM classifiers. The performance of the proposed approach is analysed and compared with the existing techniques. Additionally, the potentiality of the ensemble classification is proven by comparing the results with the individual classifiers. Though the time consumption is a bit higher in ensemble classification, it is tolerable and reasonable, when the accuracy, sensitivity and specificity rates are concerned. However, when the average time for attack detection is compared with the existing techniques, the proposed approach proves its efficiency. In future, this work plans to reduce the execution time.

References

[1] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, “The Economic Impact of Cyber-Attacks”, *Congressional Research Service Documents*, CRS RL32331, Washington, DC, USA, 2004.

[2] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection”, *Pattern Recognition Letters*, Vol. 51, pp.1-7, 2015.

[3] https://www.wireshark.org/

[4] I. Alsmadi, D. Xu, "Security of Software Defined Networks: A survey", *Computers & Security*, Vol. 53, pp. 79-108, 2015.

[5] Y. Cui, L. Yan, S. Li, H. Xing, W. Pan, J. Zhu, and X. Zheng, “SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks”, *Journal of Network and Computer Applications*, Vol.68, pp. 65-79, 2016.

[6] Z. Chen, G. Xu, V. Mahalingam, L. Ge, J. Nguyen, W. Yu, and C. Lu, "A Cloud Computing Based Network Monitoring and Threat Detection System for Critical

Infrastructures", *Big Data Research*, Vol.3, pp. 10-23, 2016.

[7] J. Chung, E. Jung, R. Kettimuthu, N.S.V. Rao, I.T. Foster, R. Clark, and H. Owen, "Advance reservation access control using software-defined networking and tokens", *Future Generation Computer Systems*, Vol.79, pp.225-234, 2017.

[8] A. Carlin, M. Hammoudeh, and O.Aldabbas, "Defence for Distributed Denial of Service Attacks in Cloud Computing", In: *Proc. of the International Conference on Advanced Wireless, Information, and Communication Technologies*, Vol. 73, pp.490-497, 2015.

[9] K. Yap and Y. Chong, "Software-Defined Networking Techniques to Improve Mobile Network Connectivity: Technical Review", *IETE Technical Review*, pp. 1-13, 2017.

[10] H. Yuan, J. Bi, B.H. Li, and W. Tan, "Cost-aware request routing in multi-geography cloud data centres using software-defined networking", *Enterprise Information Systems*, Vol.11, No.3, pp.359-388, 2017.

[11] B. Yuan, D. Zou, H. Jin, S. Yu, and L. T. Yang, "HostWatcher: Protecting hosts in cloud data centers through software-defined networking", *Future Generation Computer Systems*, Article in Press, 2017.

[12] G. Somani, M.S.Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions", *Computer Communications*, Vol.107, pp. 30-48, 2017.

[13] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "DDoS attack protection in the era of cloud computing and Software-Defined Networking", *Computer Networks*, Vol.81, pp. 308-319, 2015.

[14] Y. Jararweh, M.A. Ayyoub, A. Darabseh, E. Benkhelifa, Ml. Vouk, and A. Rindos, "Software defined cloud: Survey, system and evaluation", *Future Generation Computer Systems*, Vol.58, pp. 56-74, 2016.

[15] T. Ha, S. Kim, N. An, J. Narantuya, C. Jeong, J. Kim, and H. Lim, "Suspicious traffic sampling for intrusion detection in software-defined networks", *Computer Networks*, Vol.109, No.2, pp.172-182, 2016.

[16] N. Muthukumaran and J. Chinnappan, "FlowAgent: Software Defined Firewall Rule Generator for Network Intrusion Detection System", *International Journal of Intelligent Engineering & Systems*, Vol.10, No.3, pp. 299-306, 2017.

[17] http://pagereboot.com/

[18] R.O. Duda, P.E. Hart, and D.G. Stork, "Pattern classification", Second Edition, *Wiley-Interscience*, 2000.

[19] C. Chang and C.J. Lin, "Libsvm: A library for support vector machines", *ACM Transactions on Intelligent Systems and Technology*, Vol. 2, No.3, pp. 1-39, 2013.

[20] G. Huang, H. Zhou, X. Ding, and R. Zhang, "Extreme Learning Machine for Regression and Multiclass Classification", *IEEE Transactions on systems, Man and Cybernetics - Part B*, Vol.42, No.2, pp.513-529, 2012.