An Efficient Adaptive Load Balancing Scheme for Mitigating Reduction of Quality-Based DDOS Attack on Cloud File Storage Environment

V Loganathan, S Godfrey Winster

Abstract: -Availability of cloud resources to the cloud users is considered as the serious challenge that pose security essentialities during the process of on-demand service provision. Moreover, a specific type of attack named Reduction of Quality (RoQ)-based DDoS attack is determined to be vulnerable in the cloud computing since it exploits the benefits of the embedded adaptive load balancing and admission control methods of the environment. In this paper, an Efficient Adaptive Load Balancing Scheme-based on Wilcoxon–Mann–Whitney Hypothesis Test (EALBS-WMW-HT) is proposed for mitigating Reduction of Quality-based DDoS attack in order to minimize its influence for enhancing the degree of availability to the cloud users. This proposed EALBS-HT scheme uses the merits of statistical testing on the traffic flow and contributes to the detection of RoQ-based DDoS attack such that they does not disturb the inherent load balancing process of the cloud environment. The experiments of the proposed EALBS-HT scheme revealed an excellent detection accuracy, true positive rate and true negative rate with minimized false negative rate studied on par with the baseline approaches considered for analysis.

Keywords : Cloud, Security, attack, router, traffic, DDoS, SVM, U Test, RoQ

I. INTRODUCTION

The cloud computing is considered as the effective computational platform that wide open the option of hosting a diversified pool of resources in order to ensure its availability to the on demand customer [1]. This process of resource sharing in the cloud environment necessitates least degree of involvement from the dimension of the cloud service provider [2]. The rich and potential characteristics of the cloud computing environment have induced the incorporation of them in most of the organizations in the new technological era. Thus, the cloud computing environment has extended its benefits mutually to the cloud service providers and the diversified number of on-demand cloud consumers [3]. This cloud environment is vulnerable to a specific type of attack called Low-rate distributed denial-of-service attack, which is comparatively different from flooding attack that is complex to be detected due to its low data rate and stealthy attack traffic intent [4]. The complexity in the detection of low-rate distributed denial-of-service attack is mainly due to the generation and transmission of legitimate traffic at a very low rate, since this feature is quite easy to exploit any kind of DDoS defense mechanism exploring the characteristics of traffic flow [5]. Further, this attack is very easy to be implemented by an attacker because it necessitates only a low number of zombies [6]. This low-rate distributed denial-of-service attack focuses only on the reduction of the Quality of Service essential for the legitimate user rather than completely stopping the flow of normal traffic in the cloud environment [7]. This low-rate distributed denial-of-service attack is categorized into three types such as low rate DDoS attack against application server, shrew attack and reduction of Quality (RoQ) attack. Among these low-rate distributed denial-of-service attacks, the RoQ attack is a specific kind of attack that exploits the weakness that are introduced during the implementation of load balancing and control admission-based adaptation approaches that are essential for optimal fairness, superior stability and efficiency in the cloud environment [8]. In specific, the RoQ attacker concentrates on surpassing the thresholds of admission control for eliminating normal traffic to access the resources of the cloud [9]. This RoQ attacker also aims at reducing the requests that need to be served by the servers ate . This RoQ attacker also introduces load imbalance in the cloud by generating huge data traffic in a very short period of time. Most of the RoQ attacker mitigation approaches fail to handle the detection.

In this paper, an Efficient Adaptive Load Balancing Scheme-based on Wilcoxon–Mann–Whitney Hypothesis Test (EALBS-WMW-HT) is proposed for mitigating Reduction of Quality-based DDoS attack for confirming maximum availability to the cloud users. This EALBS-WMW-HT uses the merits of. In This admission control and load balancing approach. The simulation experiments of the proposed EALBS-WMW-HT was conducted for identifying its predominance over the benchmarked Reduction of Quality-based DDoS attack detection schemes of the literature.

Manuscript published on November 30, 2019.

V Loganathan*, Research Scholar, Saveetha School of Engineering, SIMTS, Chennai, India. Email: loganathan@saveetha.ac.in

S Godfrey Winster, Professor, Saveetha Engineering College, Chennai, India. Email: godfreywinster@saveetha.ac.in

Retrieval Number: D9717118419/2019©BEIESP
DOI:10.35940/ijrte.D9717.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

II. RELATED WORK

In this section, the research works contributed from the recent decade towards the mitigation of Reduction of Quality (RoQ)-based DDoS attack in cloud computing is reviewed with the merits and limitations.

Initially, a two-staged low rate DDoS attack detection scheme was proposed for generating a high rate of traffic in order to investigate the packet flow in a shorter period [11].

At the second level, a proactive approach is incorporated for differentiating between normal traffic and malicious traffic from the network for the remaining period of investigation. This proactive mechanism is traditionally contributed to prevent low rate DoS attacks by eliminating the cooperative operation in the specific operation of the utilized protocols under data dissemination. This proactive mechanism also uses the advantages of a botnet for classification through the leverage of confirming normal flow that confirms the features of network protocols. Then, a RoQ-based DDoS mitigation approach was proposed using the merits of router for mitigating its impact at the router point in the internet [12]. This specific RoQ-based DDoS mitigation approach is facilitated in two steps. In the first step, the monitored information about per flow is considered for detecting the existence of RoQ attack and in the second step, a significant filtering algorithm is used for dropping detecting the RoQ attacked packets in the cloud environment.

Further, Then, an Entropy Enhanced DDoS Detection Mechanism (EA-DDoSDM) was contributed for effective isolation of RoQ DDoS attacks on the cloud environment [14]. This EA-DDoSDM included a lower and upper limit for minimizing the objective function through the incorporation of genetic algorithm. This EA-DDoSDM approach was also determined to be capable of choosing an optimal value from a feasible number of child network resources in each and every iterations that are used for triggering the alarm under the RoQ DDoS attack detection process. The accuracy and precision in detection of the proposed EA-DDoSDM approach were estimated to be a maximum up to a level of 94% and 96% respectively.

Further, a Support Vector Machine (SVM)-based DDoS attack mitigation scheme was proposed using the property of entropy for determining the source that has generated the attack traffic in the clouds [15]. This SVM-based detection approach used an approximation-based adaptive autoregressive model that incorporates a HTTP time series for effective transformation of influential data into a vector data series. This SVM-based detection approach was also identified to detect application layer DDoS attacks in the cloud environment. [16]

Furthermore, an integrated Multilayer Perceptron and Genetic Algorithm-based learning algorithm was contributed to ensure effective RoQ-based attack detection [17]. This integrated approach utilized the classified scheme that inspires hypertext properties is responsible for discriminating normal traffic from malicious traffic in a cloud environment. This integrated approach used entropy, variance, request count for every link in the Multilayer Perceptron network classifier for the effective classification process. This integrated approach facilitated a superior accuracy and sensitivity and specificity to a appreciable degree of 98.31%, 0.0561 and 0.9962 respectively. Then, Self Similarity-based DDoS Detection Mechanism (SS-DDoSDM) was contributed for effective and rapid isolation of RoQ attacks from the cloud environment [18]. This SS-DDoSDM utilized the merits of a Hurst Factor for discriminating the quality of the data traffic in exploring the legitimacy of the cloud data independent of the kind of network protocol used for data transmission. The utilization of Hurst Factor aided in facilitating a Multi Attribute Decision Method (MADM) for analyzing the parameters that aided in accurate detection and prevention of DDoS attacks. The accuracy and recall value of SS-DDoSDM was visualized to be maximum even under an increased number of attacker's flow in the cloud computing.

Finally, an Economic Denial of Sustainability Attack Dimensionality Secure for DDoS Detection Mechansism (EDoS-ADS-DDoSDM) was proposed for improving the rate of data dissemination in the cloud computer environment [19]. This EDoS-ADS-DDoSDM handles the EDoS attack by preventing the complete NAT-based network for accessing the data in the cloud storage. The throughput, cost, CPU utilization and response of the proposed EDoS-ADS-DDoSDM under Cloudsim simulator was confirmed to be potent in classifying attacker's flow from the legitimate data traffic flow in the cloud environment. The F-Score, accuracy and anomaly detection rate of this EDoS-ADS-DDoSDM was significant under different rates of normal and malicious traffic packets in the cloud environment. In addition, a t-statistic inspired Hypothesis Test-based Low rate DDoS attack Detection Mechanism (HT-Lr-DDoSDM) was proposed for removing the impacts of malicious activity in the network [20]. This scheme initially investigates the problem of fraudulent resource utilization through the aid of possible parameters that contribute towards low rate DDoS attack. This scheme handles the challenge of mitigating RoQ DDoS attack with the minimized false positive rate in an appropriate real time. The precision, recall and F-Score of this scheme was determined to get maximized under varying traffic flow with normal and malicious traffic packets in the cloud environment.

III. PROPOSED WORK

1) Proposed Efficient Adaptive Load Balancing Scheme-based on Wilcoxon–Mann–Whitney Hypothesis Test (EALBS-WMW-HT)

This section presents the detailed view of the EALBS-WMW-HT proposed for mitigating Reduction of Quality-based DDoS attack in order to minimize its influence for enhancing the degree of availability to the cloud users. In this proposed EALBS-WMW-HT approach, the option of sampling out the cumulative amount of the incoming data traffic is made possible in the edge routers of the cloud computing environment. Further, the edge routers need to ensure superior cooperation among them in order to ensure its potential during the implementation process.

For achieving this purpose of coordination, the cooperation between the edges are facilitated based on the utilization of cloud service provider in the cloud network.

The assumptions considered for the proposed EALBS-WMW-HT approach is listed as follows. i) The attacker does not have the possibility of accessing the log of the victim cloud users and its resources, ii) The attacker does not possess the capability of reproducing the pattern of the legitimate client without the granting of the permission used for accessing the web log of the cloud user. iii)

The total number of utilized botnet is considered to be very large since the attack is facilitated using genuine IP addresses such that attacker compromised clients do not utilize the benefits of duplicate IP addresses, iv) Each and every client of the cloud environment is considered to be trusted until they are estimated to be malicious, v) The packet length of the data traffic is considered for estimating the probability distribution since they are significant in investigating multi-dimensional aspects that are responsible in introducing DDoS attacks in the clouds and vi) The possibility of an attack is only possible at the single instant of time with the cloud service provider ensuring the complete control and synchronization of the edge routers in the cloud environment.

In this proposed EALBS-WMW-HT approach, the process of classifying the normal data traffic from the malicious data traffic is achieved based on the observations determined from the investigation of the existing DDoS attacks mitigation approaches contributed in [21-23]. The geographical region enveloped by the attacker clients is considered to be always lesser than the geographical area bounded by the cooperative clients of the cloud environment. The clients' request patterns are utilized for determining the size of the packets such that the source IP distribution pattern is considered to be highly diffused on par with the attack traffic pattern. This proposed EALBS-WMW-HT approach is contributed as the statistical method for predominant detection of RoQ-based DDoS attack. The statistical method used in the proposed EALBS-WMW-HT approach derives the benefits from the non-parametric hypothesis test named the Mann-Whitney U Test. This Mann-Whitney U Test is considered as the potential replacement of an unpaired t-test statistics, when the number of parameters determined from one data traffic flow during an investigation is greater than the number of parameters determined from other data traffic.

2) The Detailed Description of the Utilized Mann-Whitney U Test for Detecting RoQ-Based DDoS Attack

The sequence of statistical steps involved in the Mann-Whitney U Test used for detecting RoQ-based DDoS attack is discussed as follows.

Initially, the cloud data traffic flows forwarded from the edge routers to the gateways are investigated for legitimate and malicious data traffic. However, the amounts of data traffic flows emerging from each edge routers are different and greater than each other. Thus, non-parametric Mann-Whitney U Test is suitable and applicable for the detecting process of the RoQ-based DDoS attack.

Step 1: The hypothesis for the enforcement of the Mann-Whitney U Test is predefined as follows: The Null hypothesis and alternate hypothesis is considered for genuine and malicious data traffic. Suppose, if the number of parameters $\{a_1, a_2, ..., a_n\}$ extracted from the process of monitoring the first data traffic flow and the number of parameters $\{b_1, b_2, .. b_n\}$ extracted from the process of monitoring the second data traffic flow, then the maximum number of pairwise comparison that are feasible in this context is $N_a * N_b$. This Mann-Whitney U Test is capable of comparing each and every parameter elucidated from the first data traffic flow with each and other parameter elucidated from the second data traffic flow. If the considered data traffic flows have the same median value, then each value of a_i possess the probability of 0.5, which is comparatively smaller or greater to each and every value of b_i.

In this context, the null hypothesis are formulated based on Equation (1)

$$H_0 : P(a_i > b_i) = 0.5 \qquad (1)$$

Under the alternative hypothesis defined through Equation (2)

$$H_0 : P(a_i > b_i) \neq 0.5 \qquad (2)$$

At this juncture, two vital parameters, namely F_a and F_b are estimated for determining the relative degree of how much the first compared data flow is greater or smaller than the second compared data flow used for hypothesis testing. In the case of null hypothesis, the values of F_a and F_b are expected to be equal. Further, the steps used for carrying out the hypothesis test are as follows.

Initially, the sorting of the observed parameters is facilitated, then estimate the value of the calculated 'U' based on Mann-Whitney U Test is represented in Equation (3)

$$U_{CALCULATE} = Min(N_a, N_b) \quad (3)$$

In this case, if the number of observations related to the investigation of data traffic is greater than the threshold number of samples used for exploration, then the mean and variance pertaining to the Mann-Whitney U Test is represented in Equation (4)

$$Mean(\mu) = \frac{N_a * N_b}{2}$$

and

$$Std - dev(\sigma) = \sqrt{\frac{(N_a * N_b)(N+1)}{12}} \qquad (4)$$

The principle of Mann-Whitney U Test is used for detecting the presence of RoQ-based DDoS attacks. But, the process of admission or load balancing based adaptive systems are determined to be predominant in facilitating superior stability, fairness and efficiency in the cloud computing environment.

The admission control strategies used for handling RoQ-based DDoS attacks are capable of limiting the number of requests being policed by the server any instant of time. In case of load balancing scheme, they incorporate a novel mechanism that can balance the load of the network in an effective manner of handling the issue introduced by RoQ-based DDoS attacks. Hence, a load balancing scheme using an adaptive queue model is incorporated in the proposed EALBS-WMW-HT for handling the issues of RoQ-based DDoS attacks on a cloud computing environment.

3.2 Load balancing scheme of the proposed EALBS-WMW-HT using Engset Queue Length Estimation.

In this load balancing scheme, four vital factors that include packet size, last accessed time, packet count and created time as the input to the Engset Queue Length Estimation process. This load balancing scheme incorporated a filtering mechanism based Engset through the estimation of queue length that dynamically varies during the operating period of the RoQ-based DDoS attacks on a cloud computing environment. This Engset Queue Length Estimation model is initially represented as a state-state equations of the queue state that inspires the merits of finite state birth and death process as derived in the following Equations.

$$\pi_0 N\lambda = \pi_1\mu \qquad (5)$$

$$\pi_1(N-1)\lambda = \pi_2 2\mu \qquad (6)$$

$$\pi_2(S-2)\lambda = \pi_3 3\mu \qquad (7)$$

And in general

$$\pi_n(N-C)\lambda = \pi_{C+1}(C+1)\mu \qquad (8)$$

Under the condition $0 \le n \le \min(S,C)-1$.

Then, the method of standard algebraic manipulations is applied over the Equations (5)-(6) for identifying the state of the queue (π_k) based on its initial queue state length (π_0) as portrayed in Equation (9).

$$\pi_k = NC_k(\frac{\lambda}{\mu})\pi_0 \qquad (9)$$

Further, the hybridization of queue initial state and normalization state equations is facilitated based on Equation (10) for highlighting the initial queue length state that aids in determining threshold that focuses on the load balancing phenomenon in the cloud environment.

$$\pi_0 = \frac{1}{\sum_{j=0}^{Min(N,C)} NC_c(\rho)^j} \qquad (10)$$

Since the traffic intensity in the queue model is $\rho = \frac{\lambda}{\mu}$.

Finally, the Engset model that determines the load balance parameter under which the process of load balancing in cloud computing is triggered is defined in Equation (11)

$$L_{BF}(t) = \frac{(N-1)C_c(\rho)^c}{\sum_{i=0}^{c}(N-1)C_c(\rho)^c} \qquad (11)$$

Thus, if the value of the load balance parameter is less than the threshold of 0.4 (determined through simulations), then the burst load of data traffic is policed to prevent the impacts of RoQ-based DDoS attack in clouds.

IV. SIMULATION RESULTS AND DISCUSSIONS

The suitability and predominant performance of the proposed EALBS-WMW-HT approach as a RoQ-based DDoS attack is investigated using CAIDA and DARPA, since the former comprises of attack packets and the latter consists of legitimate packets. These two significant datasets is mainly used as they were determined to be highly suitable for investigating the possible dimensions of parameters that attribute to the detection feasibility of the RoQ-based DDoS attack. The performance of the proposed EALBS-WMW-HT approach is explored in three folds such as detection accuracy, precision and recall value under false positive rate

In the first investigation, the potential of the proposed EALBS-WMW-HT approach is investigated using detection accuracy, precision and recall under varying degrees of false positive rate. Figure 2 glorifies the detection accuracy of the proposed EALBS-WMW-HT approach over the compared HT-Lr-DDoSDM, EDoS-ADS-DDoSDM and SS-DDoSDM approaches by increasing the rate of false positive rates. The detection accuracy of the proposed EALBS-WMW-HT approach is determined to improve, even when the false positive rate is increased depending on the effective computation of Engset model that estimates the dynamic queue state. Thus the detection of the proposed EALBS-WMW-HT approach is enhanced by 21%, 17% and 14% compared to the baseline HT-Lr-DDoSDM, EDoS-ADS-DDoSDM and SS-DDoSDM approaches. Figure 3 exemplars the precision of the proposed EALBS-WMW-HT approach over the compared HT-Lr-DDoSDM, EDoS-ADS-DDoSDM and SS-DDoSDM approaches by increasing the rate of false positive rates. The precision of the proposed EALBS-WMW-HT approach is visualized to be enhanced even when the false positive rate is increased depending on the effective method of hypothesis testing and adaptive load balancing scheme used for determining the dynamic queue state. Thus, the precision of the proposed EALBS-WMW-HT approach is enhanced by 18%, 14% and 11% compared to the baseline HT-Lr-DDoSDM, EDoS-ADS-DDoSDM and SS-DDoSDM approaches. Figure 4 exemplars the recall value of the proposed EALBS-WMW-HT approach over the compared HT-Lr-DDoSDM, EDoS-ADS-DDoSDM and SS-DDoSDM approaches by increasing the rate of false positive rates. The recall value of the proposed EALBS-WMW-HT approach is visualized to be enhanced even when the false positive rate is increased depending on the effective method of Engset model used for determining the dynamic queue state.

Thus, the recall value of the proposed EALBS-WMW-HT approach is enhanced by 16%, 13% and 10% compared to the baseline HT-Lr-DDoSDM, EDoS-ADS-DDoSDM and SS-DDoSDM approaches.

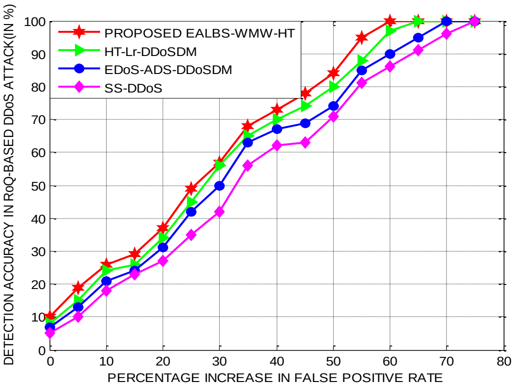

Figure 2: Detection accuracy of the proposed EALBS-WMW-HT under increase in False Positive Rate

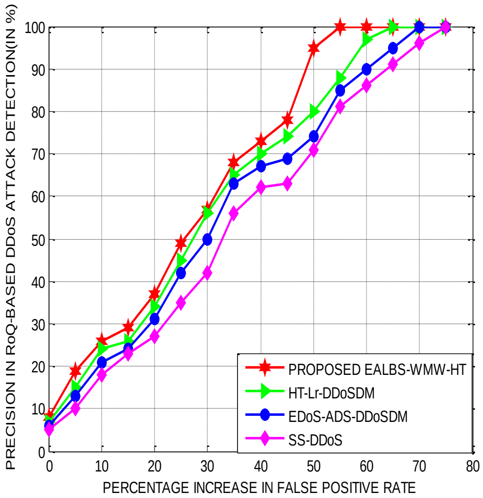

Figure 3: Precision accuracy of the proposed EALBS-WMW-HT under increase in False Positive Rate

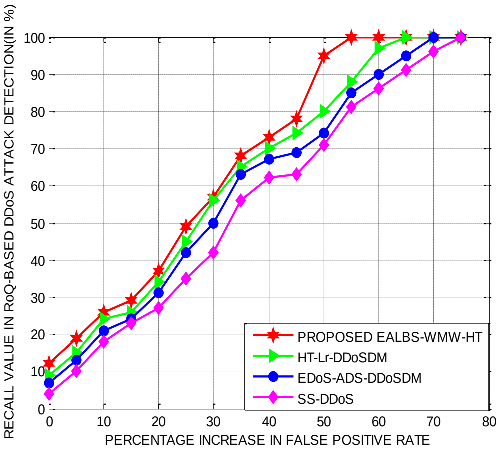

Figure 4: Recall Value of the proposed EALBS-WMW-HT under the increase in False Positive Rate

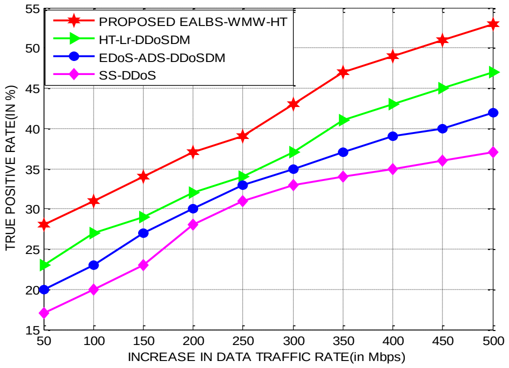

Figure 5: True Positive Rate-EALBS-WMW-HT under varying data rate

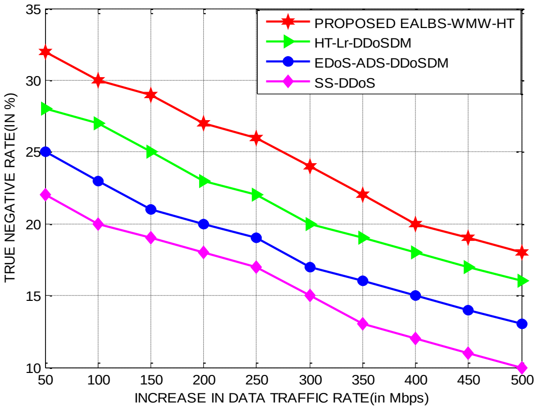

Figure 6: True Negative Rate-EALBS-WMW-HT under varying data rate

Furthermore, Figure 5 and 6 glorifies the predominance of the proposed EALBS-WMW-HT scheme evaluated using True positive rate and true negative rate under varying data rate. The true positive rate of the proposed EALBS-WMW-HT scheme is determined to sustain predominantly even when when the number of data rates is increased from 50 Mbps to 500 Mbps on par with the existing baseline RoQ-based DDoS attack detection scheme, since the incorporation of Markov modulated Bernoulli process in the load balancing process aided in the peculiar maintenance of the True positive rate. The true positive rate of the proposed EALBS-WMW-HT scheme is confirmed to be 19%, 15% and 11% superior to the existing HT-Lr-DDoSDM, EDoS-ADS-DDoSDM and SS- DDoSDM approaches. Likewise, true negative rate of the proposed EALBS-WMW-HT scheme is also estimated to be superior by balancing the load in the network compared to the existing baseline RoQ-based DDoS attack detection scheme. The true negative rate of the proposed EALBS-WMW-HT scheme is confirmed to be 17%, 12% and 9% superior to the existing HT-Lr-DDoSDM, EDoS-ADS-DDoSDM and SS-DDoSDM approaches.

Retrieval Number: D9717118419/2019©BEIESP
DOI:10.35940/ijrte.D9717.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

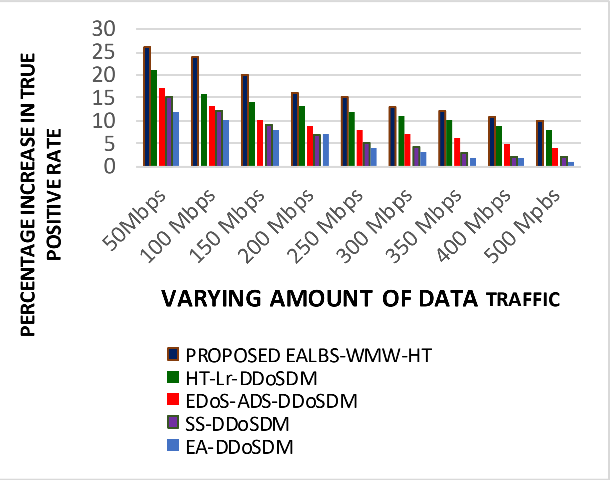

Figure 7: Proposed EALBS-WMW-HT-percentage increase in True Positive Rate under varying amounts of data rate

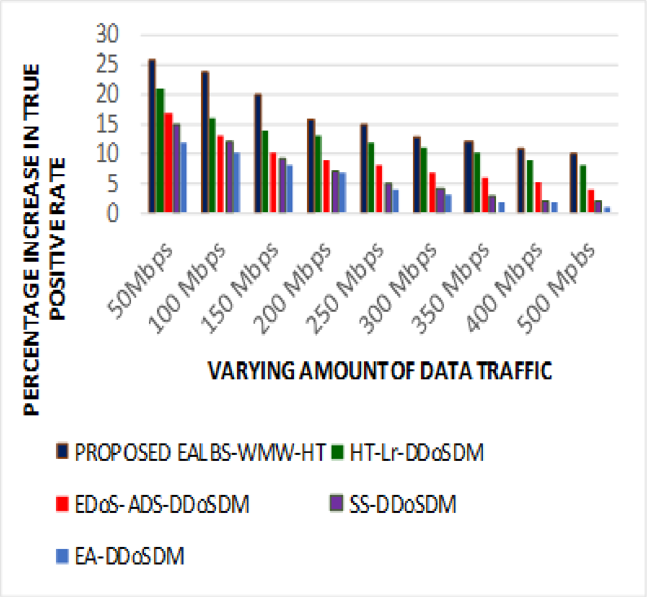

Figure 8: Proposed EALBS-WMW-HT-percentage increase in True Negative Rate under varying amounts of data rate

Finally, the predominance of the proposed EALBS-WMW-HT is investigated using True Positive rate, True Negative Rate, False Positive Rate and False Negative Rate under increasing levels of data rate in the cloud network traffic. Figures 7 and 8 highlights the excellence of the proposed EALBS-WMW-HT quantified in terms of True Positive rate and True Negative Rate under varying amounts of cloud network data traffic. The true negative rate of the proposed EALBS-WMW-HT scheme is confirmed to be 17%, 12% and 9% superior to the existing HT-Lr-DDoSDM, EDoS-ADS-DDoSDM and SS-DDoSDM approaches. The true negative rate of the proposed EALBS-WMW-HT scheme is confirmed to be 17%, 12% and 9% superior to the existing HT-Lr-DDoSDM, EDoS-ADS-DDoSDM and SS-DDoSDM approaches.

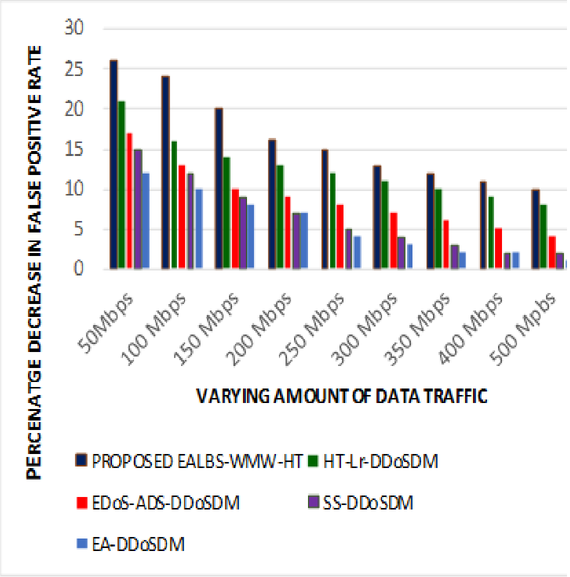

Figure 9: Proposed EALBS-WMW-HT-percentage decrease in False Positive Rate under varying amounts of data rate

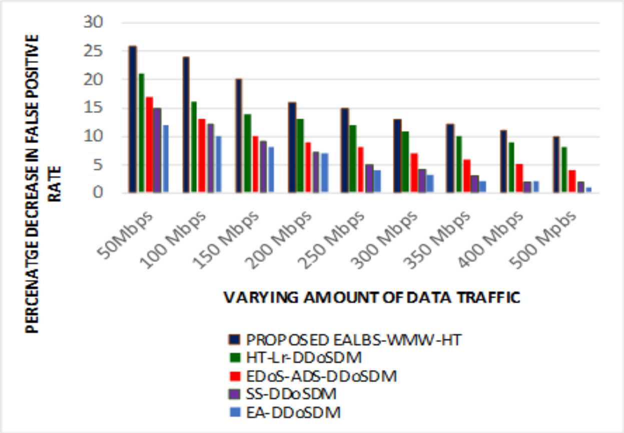

Figure 10: Proposed EALBS-WMW-HT-percentage decrease in False Negative Rate under varying amounts of data rate

Likewise, Figures 9 and 10 exemplars the False Positive Rate and False Negative Rate of the proposed EALBS-WMW-HT estimated under increasing levels of data rate in the cloud network traffic. The true negative rate of the proposed EALBS-WMW-HT scheme is confirmed to be 17%, 12% and 9% superior to the existing HT-Lr-DDoSDM, EDoS-ADS-DDoSDM and SS-DDoSDM approaches. The true negative rate of the proposed EALBS-WMW-HT scheme is confirmed to be 17%, 12% and 9% superior to the existing HT-Lr-DDoSDM, EDoS-ADS-DDoSDM and SS-DDoSDM approaches.

V. CONCLUSION

The proposed EALBS-WMW-HT was presented as a reliable method of preventing the influence of the Reduction of Quality-based DDoS attack in the clouds with the view to enhance the degree of availability to the cloud users.

This proposed EALBS-HT scheme also incorporated the capabilities of the statistical testing in order to potentially investigate the traffic flow such that the detection of RoQ-based DDoS attack can be facilitated without disturbing the implicit load balancing process of the cloud environment. The simulation experiments and its results inferred that the accuracy, precision and recall value of the proposed EALBS-WMW-HT scheme on an average is approximately 12%, 15% and 17% superior to the baseline HT-Lr-DDoSDM, EDoS-ADS-DDoSDM and SS-DDoSDM approaches. Similarly, the anomaly detection rate of the proposed EALBS-WMW-HT scheme is improved at an average by 21% compared to the benchmarked RoQ-based DDoS attack detection and isolation mechanisms considered from the literature. As the part of the future plan, it is also decided to formulate a Self Organizing Maps-based RoQ DDoS attack mitigation mechanism for investigating the traffic flow in a multi-perspective aspect.

References

1. Somani, G., Gaur, M. S., Sanghi, D., Conti, M., Rajarajan, M., & Buyya, R. (2017). Combating DDoS Attacks in the Cloud: Requirements, Trends, and Future Directions. *IEEE Cloud Computing*, *4*(1), 22-32.
2. Girma, A., Garuba, M., Jiang Li, & Chunmei Liu. (2015). Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment. *2015 12th International Conference on Information Technology - New Generations*, *1*(2), 34-47.
3. Gupta, S., & Kumar, P. (2013). VM Profile Based Optimized Network Attack Pattern Detection Scheme for DDOS Attacks in Cloud. *Communications in Computer and Information Science*, *2*(1), 255-261.
4. Bhushan, K., & Gupta, B. (2017). Security challenges in cloud computing: state-of-art. *International Journal of Big Data Intelligence*, *4*(2), 81-98.
5. Idziorek, J., Tannian, M., & Jacobson, D. (2012). Attribution of Fraudulent Resource Consumption in the Cloud. *2012 IEEE Fifth International Conference on Cloud Computing*, *2*(1), 56-64.
6. Koduru, A., Neelakantam, T., & S, M. S. (2013). Detection of Economic Denial of Sustainability Using Time Spent on a Web Page in Cloud. *2013 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*.
7. Zhang, J., & Qin, Z. (2010). Modified method of detecting DDoS attacks based on entropy. *Journal of Computer Applications*, *30*(7), 1778-1781.
8. Gupta, S., Horrow, S., & Sardana, A. (2012). A Hybrid Intrusion Detection Architecture for Defense against DDoS Attacks in Cloud Environment. *Communications in Computer and Information Science*, *2*(1), 498-499.
9. Girma, A., Abayomi, K., & Garuba, M. (2016). The Design, Data Flow Architecture, and Methodologies for a Newly Researched Comprehensive Hybrid Model for the Detection of DDoS Attacks on Cloud Computing Environment. *Advances in Intelligent Systems and Computing*, *1*(2), 377-387.
10. Agrawal, N., & Tapaswi, S. (2017). Defense schemes for variants of distributed denial-of-service (DDoS) attacks in cloud computing: A survey. *Information Security Journal: A Global Perspective*, *26*(2), 61-73.
11. Shevtekar, A., & Ansari, N. (2007). A Proactive Test Based Differentiation Technique to Mitigate Low Rate DoS Attacks. *2007 16th International Conference on Computer Communications and Networks*, *1*(2), 45-58.
12. Shevtekar, A., & Ansari, N. (2008). A router-based technique to mitigate reduction of quality (RoQ) attacks. *Computer Networks*, *52*(5), 957-970.
13. Zhou, Y., Jiao, C., Chen, H., Ma, L., & Hu, G. (2013). Traffic behavior feature based DoS&DDoS attack detection and abnormal flow identification for backbone networks. *Journal of Computer Applications*, *33*(10), 2838-2841.
14. N.Jadhav, P., & M. Patil, B. (2013). Low-rate DDOS Attack Detection using Optimal Objective Entropy Method. *International Journal of Computer Applications*, *78*(3), 33-38.
15. Gu, X., Wang, H., Ni, T., & Ding, H. (2013). Detection of application-layer DDoS attack based on time series analysis. *Journal of Computer Applications*, *33*(8), 2228-2231.
16. Rong, H., Wang, H., Xian, M., & Shi, J. (2014). A Novel Method for Detecting Reduction of Quality (RoQ) Attack Based on Fast Independent Component Analysis. *Journal of Electronics & Information Technology*, *35*(10), 2307-2313.
17. Johnson Singh, K., Thongam, K., & De, T. (2016). Entropy-Based Application Layer DDoS Attack Detection Using Artificial Neural Networks. *Entropy*, *18*(10), 350.
18. Deka, R. K., & Bhattacharyya, D. K. (2016). Self-similarity based DDoS attack detection using Hurst parameter. *Security and Communication Networks*, *9*(17), 4468-4481.
19. Shawahna, A., Abu-Amara, M., Mahmoud, A., & Osais, Y. E. (2018). EDoS-ADS: An Enhanced Mitigation Technique Against Economic Denial of Sustainability (EDoS) Attacks. *IEEE Transactions on Cloud Computing*, *1*(2), 1-1.
20. Bhushan, K., & Gupta, B. (2018). Hypothesis Test for Low-rate DDoS Attack Detection in Cloud Computing Environment. *Procedia Computer Science*, *132*, 947-955.