A Reliable Friedman Hypothesis-Based Detection and Adaptive Load Balancing Scheme for Mitigating Reduction of Quality DDoS Attacks in Cloud Computing

V Loganathan, S Godfrey Winster

Abstract-The computing resource availability in a cloud computing environment is considered as the vital attribute among the security essentialities due to the consequence of on its on demand service. The class of adversaries related to the Distributed Denial of Service (DDoS) attack is prevalent in the cloud infrastructure for exploiting the vulnerabilities during the implementation of their attack that still make the process of providing security and availability at the same time as a challenging objective. In specific, The in cloud computing is the major threat during the process of balancing security and availability at the same time. In this paper, A Reliable Friedman Hypothesis-based Detection and Adaptive Load Balancing Scheme (RFALBS-RoQ-DDOS) is contributed for effective detection of RoQDDoS attacks through Friedman hypothesis testing. It also inherited an adaptive load balancing approach that prevents the degree of imbalance in the cloud environment. The simulation results of the proposed RFALBS-RoQ-DDoS technique confirmed a superior detection rate and a adaptive load balancing rate of nearly 23% and 28% predominant to the baseline DDoS mitigation schemes considered for investigation.

***Keywords*: Cloud, Security, attack .router, traffic. Kruskal-Wallis, malicious.**

I. INTRODUCTION

From the recent past, cloud computing is considered as the suitable and comfortable environment for the users to access the applications and resources through the internet as a service[1]. This cloud computing is responsible for transforming the desktop computing into the utility-oriented computing, since huge amount of data is aggregated and stored in the enormous data centers spatially placed at a diversified number of locations [2]. Nowadays, industries and organizations are following a pay on use, self service and on-demand model rather than concentrating on the objective of deployment.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author

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

Moreover, this pay on use, self service and on-demand model of cloud computing that enhances the rate of metered service, pooling of resources and scalability are determined as the indispensable characteristics of cloud computing [3]. This cloud computing environment can be built into a public, private, hybrid and community model based the requirements. This cloud computing environment is potent in delivering infrastructure, platform and software as a service. In spite of cloud computing technology facilitating numerous merits to users, it possesses the challenges of security features that include access control, integrity, encryption, traceability, key management, identity determination and availability[4]. The aforementioned security features' vulnerability is utilized by adversaries for launching the attacks in the cloud infrastructure. Further, the attacks in cloud computing are categorized into storage-based, network-based, VM-based and application-based depending on the impact induced by the adversaries over the core entities of cloud environment [5]. Thus, the users need to be careful in storing their sensitive data in the infrastructure of the cloud. However, the cloud resources need to be available throughout the data for attaining the objective of cloud environment by maximizing the availability and security.

From the recent decade, most of the researchers are focusing on the availability as the indispensable point in the area of cloud computing security [6]. In particular, Denial of service is considered as the crucial attack that targets on the availability of the system resources in the cloud environment. Furthermore, when the denial of service attack is launched in a cooperated and distributed way in the large scale network like cloud environment, it is termed as Distributed Denial Of Service (DDoS) attack[7]. This DDoS attack is considered as the serious threat among the different forms of attack in today's internet. This DDoS attack is responsible for influencing the data, resources, services and applications availability in the cloud computing environment. This DDoS attack is induced by flooding the data traffic that gets originated from thousands of compromised nodes termed as zombies for focusing on attacking the victim in the cloud environment. In classical DDoS, the core objective of the attacker concentrates on bringing down the services requested by the legitimate users[8]. This classical DDoS attack suffers from two significant weaknesses from the perspective of the attackers.

First, it is highly detected through the incorporated defense approach due to the high intensity of data attack traffic. Secondly, It necessitates a considerable number of zombies for implementing this kind of attack [9].

Thus the intruders are now leaning to move around a potent strategy in which the resources are made unavailable through the utilization of low rate attack packets [10]. This new category of attack in which low rate attack packets are utilized for bringing down the availability of the resources in the cloud environment is termed as a low rate DDoS attack [11].

The low rate DDoS attack pertains to be quite different than the flooding kind of attack due to its low rate traffic and stealthy characteristics. This low rate DDoS attacks are capable of compromising defense mechanism that works on the characteristic feature of traffic flow as the attack transmits malevolent packets at a considerably very low rate [12]. This low rate DDoS attack also necessitates only a limited number of zombies for bringing down the Quality of Service (QoS) requested by the legitimate users of the cloud environment instead of completely ceasing the legitimate traffic flow in the network [13]. This low rate DDoS attack is divided into low rate attack against application server, reduction of quality attack and shrew attack depending on the method launching attacks. The reduction of quality DDoS attack is launched by bypassing the threshold through the transmission of attack packets that prevents the legitimate users from accessing the potential resources[14]. In specific, the adaptation mechanism (load balancing and admission control) is determined to be responsible for facilitating superior stability, efficiency and fairness under mitigation of reduction of quality DDoS attack [15].

In this paper, A Reliable Friedman Hypothesis-based Detection and Adaptive Load Balancing Scheme (RFALBS-RoQ-DDOS) is contributed for effective detection of RoQ DDoS attacks through Friedman hypothesis testing and the imbalance in the load of cloud environment is balanced through the adoption of the technique. The simulation results of the proposed RFALBS-RoQ-DDoS technique confirmed a superior detection rate and a adaptive load balancing rate of nearly 23% and 28% predominant to the baseline DDoS mitigation schemes considered for investigation.

II. RELATED WORK

In this section, the comprehensive review of some of the predominant existing RoQ-based DDoS attack detection and isolation approaches propounded in the literature in the recent years are detailed with their pros and cons.

A RoQ-based DDoS attack mitigation scheme using a centralized router was proposed with two important phases that includes the detection of available per flow information in the initial step and attack filtering in the second step [16]. This router-based mitigation scheme assumes that only the IP address of the source and destination are used by the attacker for introducing spoofing attack. It included a simple filtering process for the purpose of dropping attack packets based on the utilization of formulating thresholds. The utilized filtering process considered long-lived flows for forwarding and dropped packets based on the estimation of the queue length. It is also considered to successfully detect and isolate RoQ-based DDoS attack mitigation scheme even when the IP addresses of the source and destination are spoofed. An Information Metric-based RoQ-based DDoS attack mitigation scheme was propounded for evaluating the deviation that could be possibly realized in network traffic based on probability distributions [17]. This RoQ-based DDoS attack mitigation scheme used information distance and generalized entropy metrics for estimating the deviation between the attack and genuine traffic flows. The generalized entropy metric used in this mitigation scheme is capable enough in detecting attacks rapidly o par with the classical Shannon metric. The information distance metric is potent in diversifying adjudicated distance in order to estimate optimal sensitivity under detection. This Information Metric-based RoQ-based DDoS attack mitigation scheme was considered to be phenomenal in detection with highly minimized false positive rate. Another RoQ-based DDoS attack mitigation scheme using Congestion Participation Rate (CPR) was proposed for filtering the malicious traffic with high resistance to congestion in the network [18]. The parameter of CPR played a vital role in identifying LDDoS flows based on pre-established threshold for dropping of malicious data traffic introduced into the network. The utilization of CPR is also quantified theoretically based on the determination mean deviation identified between LDDoS flows and TCP flows. The performance of this CBR-based RoQ-based DDoS attack mitigation scheme was identified to be superior over the classical Discrete Fourier Transform (DFT)-based detection schemes.

A RoQ-based DDoS detection approach was proposed for detecting a specific category of Economical-Denial-Of-Sustainability (EDoS) attack that are most possible in the cloud computing environments [19]. This detection scheme was proposed completely based on pattern attack recognition. It was been propounded for minimizing the impact of EDoS attack that are intruding into the network based on the collection of BOTNETs and some specific tactical strategies. It considered to be potent in terms of resource utilization and response time independent to the amount of data traffic introduced into the network. Another EDoS attack detection approach named Enhanced APART model was proposed for improving the degree of availability pertaining to the cloud resources under the existence of malicious traffic flows [20]. This Enhanced APART model considered the method of pre-sharing for the purpose of accessing the legitimate cloud service users through the incorporation of authentication scheme that includes key-sharing and time-based resistance. It is also concluded to prevent replay or replication attack with improved response time and classification accuracy. A RoQ-based DDoS detection scheme using Hurst parameter was proposed for determining the deviation between legitimate traffic and DDoS attack traffic [21].The Hurst parameter used in this approach played a primitive role in identifying the legitimacy of the data traffic. This Hurst parameter is also potential in enhancing the response time, resource utilization with reduced false positive rate.

Then, a Multi Variant Analysis-based DDoS Detection Scheme (MVA-DDoS-DS) was proposed for differentiating low and high rate data traffic attacks in the network [22].

This MVA-DDoS-DS utilized a predominant factor named Feature Feature Score (FFS) for identifying the difference between normal and malicious traffic in the network. It extracted three parameters such as packet rate, source IPs deviation and source IPs entropy for exploring the characteristic behavior of data traffic under attack mitigation.

In addition, RoQ-based DDoS attack detection approach using PCMA was proposed for mitigating the impact of the attacks in the cloud computing environment [23]. The method of PCMA is included for resisting the influence of the network based on the process of continuous monitoring. They used the method of F-test for identifying the variance parameter influence introduced by the malicious network traffic in the clouds. It is also capable of handling the diversified issues that lie behind the exploration and differentiation of data traffic into genuine and normal data flows. A t-test-based detection approach (t-test-DA) was propounded for detecting RoQ-based DDoS attack based on potential exploration of data associated with the cloud traffic [24]. This t-test-DA is capable in identifying the direct and indirect influencing factors that plays a significant role in impacting the data flow in the clouds. The classification accuracy, precision, recall and F-Measure was identified to be improved independent to the number of data flows entering into the cloud.

III. PROPOSED WORK

The systematic steps involved in the implementation of the proposed RFALBS-RoQ-DDOS scheme for achieving the detection of RoQ-based DDoS attack is presented as follows.

In the proposed RFALBS-RoQ-DDOS scheme, the malicious data traffic from the normal traffic is differentiated based on the exploration carried out over the cloud data traffic transmitted between the edge routers and the gateways. But, the intensities of data traffic flowing out of the edge routers are not similar to one another. At this juncture, non-parametric such as Friedman Hypothesis Test is highly suitable and significant in mitigating the impacts introduced by the RoQ-based DDoS attack.

The hypothesis formulated for the implementation of the Friedman Hypothesis Test are described as follows. Two hypothetical statements, namely null and alternative hypothesis are formulated for stating the existence and non-existence of malicious data traffic in the data being investigated in the edge router. In this context, the pair wise comparison count is estimated as $N_k * N_m$, since the number of factors determined from the two different flows { $k_1, k_2, k_3,'...k_n$ } and { $m_1, m_2, m_3, ...m_n$ } identified during the process of monitoring RoQ-based DDoS attack on the cloud computing environment. This Friedman Hypothesis Test is potent in comparing and discriminating individual parameter that are determined from the flows considered for investigation. At the juncture, the value of k_i is considered to be 0.5, which is identified to be relatively greater than the individual value of m_i respectively. In this scenario, the null hypothesis and alternative hypothesis considered for the proposed RFALBS-RoQ-DDOS scheme is presented based on Equation (1) and (2).

$$H_0 : P(k_i > m_i) = 0.5 \qquad (1)$$

$$H_A : P(k_i > m_i) \neq 0.5 \qquad (2)$$

Then, Friedman test statistics are computed based on Equation (3)

$$T_{stat-Friedmann} = \frac{12}{km(m+1)} \sum_{i=1}^{R} R_i^2 - 3k(m+1) \qquad (3)$$

Where the value of is determined based on Equation (4)

$$R_i^2 = (r_1 + r_2 + r_3 + ...r_k)^2 \qquad (4)$$

This Friedman test statistic plays a vital role in differentiating the normal traffic with malicious data traffic.

The systematic steps of Friedman Hypothesis Test is mainly for detection of malicious traffic. However, the utilization of adaptive congestion control scheme is necessary for handling the issues of RoQ-based DDoS attacks on a cloud computing environment. Further, an Adaptive Load Balancing Approach using Markov Renewal process (ALBA-MRP) is utilized for exploring the queue state of mobile nodes in order to prevent congestion in the cloud environment. ALBA-MRP uses the advantages of Semi-Markov chain for investigating the change in queue state that reactively varies with dynamic variation in the number of packets forwarded by each mobile node. The time required for queue state is influenced by its present and past states. In the context of maximum congestion, transition time incurred for change in queue state, mostly depends on the past state of the queue that follows Exponential distribution. Hence, the Semi-Markov chain inspired transition modeling used in ALBA-MRP is replaced by a continuous parameter influencing the Markov chain.

In ALBA-MRP, the queue state is determined based on the calculation of conditional probabilistic queue transition time $CPQ(t)$ which is calculated based on the ratio of cumulative transition probability ($JTP_{ij}(t)$) and distinct transition probabilistic value ($IP_{ij}(t)$) related to each transition in queue state.

$$CPQ(t) = \frac{JTP_{ij}(t)}{IP_{ij}(t)} \qquad (5)$$

where ‘ $IP_{ij}(t)$ ‘ needs to be positive and can associate any arbitrary value. In this computation of $CPQ(t)$, cumulative transition probability ($JTP_{ij}(t)$) is derived based on equation (6)

$$JTP_{ij}(t)=\sum_{j=0}^{\infty}TP_{ij}(t) \quad (6)$$

This cumulative transition probability ($JTP_{ij}(t)$) highlights the joint distribution function which quantifies the immediate transition of queue states from an initial queue state 'i'. ALBA-MRP uses an imbedded Markov Renewal process 'X_n' for modeling the transition states of queue as it is studied based on its transition from state 'i'. The possible number of transitions that could be realized by ALBA-MRP in the time interval (0-t) is considered as '$M_i(t)$' which represents a positive vector that consists of $M_i(i)$ as the ith element. This '$M_i(t)$' is also found to be a Markov Renewal Process which inspires a similar kind of probability that is associated with the characteristic probabilities of Semi-Markov process. But, the Markov Renewal Process of ALBA-MRP must be uniquely differentiated from the traditional Semi-Markov process associated with queue state transition. Thus the renewal process in ALBA-MRP is a counting scheme that elucidates an exhaustive number of states that the queue could transit from any arbitrary state 'i' in a time instant 't' which is found to be contradicting to the definition of Semi-Markov process that defines itself in any one of the possible queue state of transition. Three types of queue models such as M/M/1/ ∞ , M/M/c/ ∞ and M/G/1/ ∞ are analyzed by incorporating the striking characteristics of Markov chain for understanding the potential of the proposed ALBA-MRP.

In the initial case of Markov renewal process inspired analysis of M/M/1/∞model, the queuing mechanism used for forwarding data packets through the mobile nodes of the network uses Semi-Markov process (δ and γ as arrival and service rates of packets) with

$$JTP_{01}(t)=1-e^{-\gamma t} \quad (7)$$

$$JTP_{i,i-1}(t)=(1-e^{-(\gamma+\delta)t})\frac{\delta}{\gamma+\delta},(i\geq 1) \quad (8)$$

$$JTP_{i,i+1}(t)=(1-e^{-(\gamma+\delta)t})\frac{\gamma}{\gamma+\delta},(i\geq 1) \quad (9)$$

The incorporation of M/M/1/ ∞ queuing model in ALBA-MRP proves that the utilized Markov chain seems to resemble the potential features of a Semi-Markov chain which is always independent of its influential factors. This striking feature of Semi-Markov chain emphasizes that the queuing state transition is independent of its continuous and discrete impactful parameters that are necessary for determining the queue state in the event of congestion. The queue state in ALBA-MRP is modeled using Markov chain for quantifying the an adaptive rate of load under congestion by inspiring the principles of a Semi-Markov process. The transition time of queuing in ALBA-MRP is found to be constant when the influencing factors responsible for load balancing are discrete and it follows an exponential distribution when the impactful factors are continuous as represented in equations (10-14).

$$TP_{01}(t)=1, \quad (10)$$

$$TP_{i,i-1}(t)=\frac{\delta}{\gamma+\delta},(i\geq 1) \quad (11)$$

$$TP_{i,i+1}(t)=\frac{\delta}{\gamma+\delta},(i\geq 1) \quad (12)$$

$$TF_{01}(t)=1-e^{-\gamma t} \quad (13)$$

$$TF_{i,i-1}(t)=TF_{i,i+1}(t)=1-e^{-(\gamma+\delta)t}(i\geq 1) \quad (14)$$

In addition, ALBA-MRP is also analyzed using the MRP approach based on M/G/1/ ∞ queuing model. In this M/G/1/ ∞ queue based investigation, the process of forwarding packets in response to congestion state depends on Semi-Markov process or Markov process. Thus the Markov renewal process that is used for calculating the average response of ALBA-MRP in terms of packet forwarding ($Average_{time(i)}$) rate in order to balance the network load is given by

$$Average_{time(i)}=\sum_{j=0}^{\infty}TP_{ij}(t)*T_{sp(q)_{iij}} \quad (15)$$

Where $T_{sp(q)_{ij}}$ denotes the queue's cumulative time in the state 'i' before its transition to the state 'j'. The aforementioned analysis of ALBA-MRP with three kinds of queuing models confirms that Markov Chain features of Markov renewal process are positive recurrent and irreducible in property. The adaptive rate of load balancing $LBP_j(Adaptive)$ enabled by ALBA-MRP under congestion in the network is given by

$$LBP_j(Adaptive)=\frac{\lambda_j*Average_{time(j)}}{\sum_{i=0}^{\infty}\lambda_i*Average_{time(i)}} \quad (16)$$

where 'λ_j' is the stationary probability of ALBA-MRP that quantifies the state transition of the queue using the Markov process that also uses the features of the geometric distribution with an Imbedded Markov renewal process.

IV. SIMULATION RESULTS

The experimental investigations of the proposed is conducted using Mata R 2014a. The data considered for investigation are determined based on 60,000 connections, 20,000 of which are normal connections, 20,000 UDP flood attack connections, and 20,000 TCP SYN flood attack connections In the first part of the investigation, the proposed RFALBS-RoQ-DDoS technique and the benchmarked T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes are investigated based on precision, recall value, specificity and F-measure. Figure 1 and 2 demonstrates the performance of the proposed RFALBS-RoQ-DDoS and the benchmarked T-TEST-DA,

MVA-DDoS-DA and PCMA-DA schemes based on the evaluation metrics such as the precision and recall with different intensities of data traffic. The precision and recall achieved by the proposed RFALBS-RoQ-DDoS are considered to be relatively excellent on par with the benchmarked approaches, since it used the benefits of Semi-Markov Renewal Process for adaptation in order prevent congestion introduced by the malicious traffic. Thus, the precision of the proposed RFALBS-RoQ-DDoS with different intensities of data traffic is identified to be 9%, 11% and 13% excellent to the baseline T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes. The recall value of the proposed RFALBS-RoQ-DDoS with different intensities of data traffic is identified to be 12%, 14% and 17% excellent to the baseline T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes. Figure 3 and 4 presents the specificity and F-measure of the proposed RFALBS-RoQ-DDoS quantified under different intensities of data traffic. The specificity and F-measure of the proposed RFALBS-RoQ-DDoS under different intensities of data traffic is also identified to be comparatively minimized on par with the benchmarked approaches, since it includes a Markov Renewal process of congestion state investigation of malicious data traffic. The specificity of the proposed RFALBS-RoQ-DDoS is identified to be 10%, 13% and 16%, improved on par with the benchmarked T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes. The F-Measure of the proposed RFALBS-RoQ-DDoS is identified to be 12%, 15% and 17%, improved on par with the benchmarked T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes.

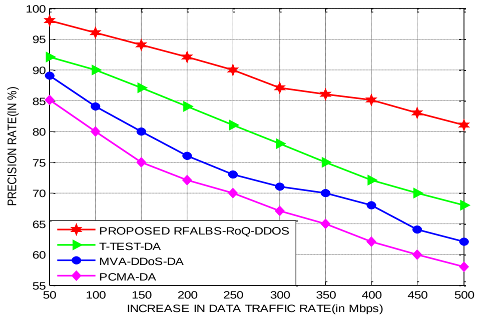

Figure 1: Proposed RFALBS-RoQ-DDOS attack detection scheme-Precision with different intensities of data traffic

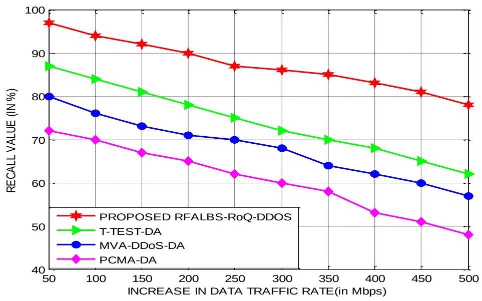

Figure 2: Proposed RFALBS-RoQ-DDOS attack detection scheme-Recall value with different intensities of data traffic

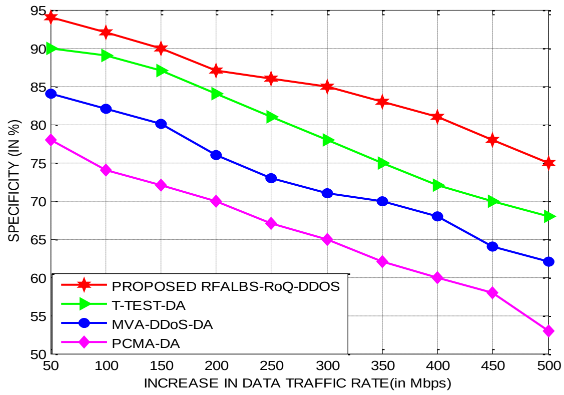

Figure 3: Proposed RFALBS-RoQ-DDOS attack detection scheme-Specificity with different intensities of data traffic.

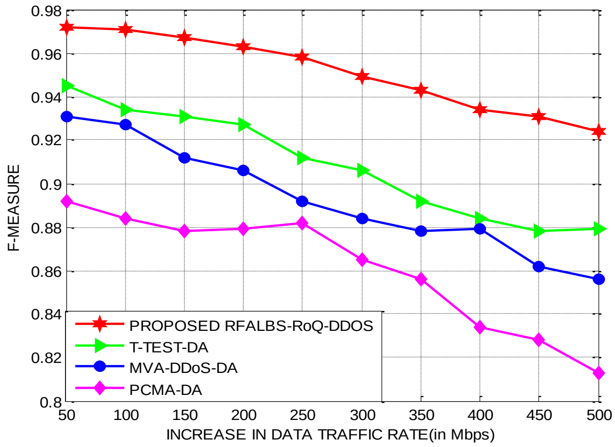

Figure 4: Proposed RFALBS-RoQ-DDOS attack detection scheme-F-Measure with different intensities of data traffic

In the second part of the investigation, the proposed RFALBS-RoQ-DDoS technique and the benchmarked T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes are investigated based on percentage increase in classification accuracy and the percentage decrease in false positive rate with different intensities of data traffic. Figure 5 and 6 demonstrates the performance of the proposed RFALBS-RoQ-DDoS and the benchmarked T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes based on the evaluation metrics such as the percentage increase in classification accuracy and the percentage decrease in false positive rate with different intensities of data traffic. The percentage increase in classification accuracy of the proposed RFALBS-RoQ-DDoS are considered to be relatively excellent on par with the benchmarked approaches, since it used the benefits of Friedman hypothesis testing for phenomenal discrimination of normal data traffic and malicious traffic. Thus, the percentage increase in classification accuracy of the proposed RFALBS-RoQ-DDoS is identified to be 7%, 10% and 13% excellent to the baseline T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes.

Likewise, the percentage decrease in false positive rate of the proposed RFALBS-RoQ-DDoS are considered to be relatively reduced on par with the benchmarked approaches, since it used an adaptive congestion control approach that polices the network traffic under malicious data traffic. Thus, the percentage decrease in false positive rate of the proposed RFALBS-RoQ-DDoS is identified to be 9%, 12% and 15%, minimized on par with the benchmarked T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes.

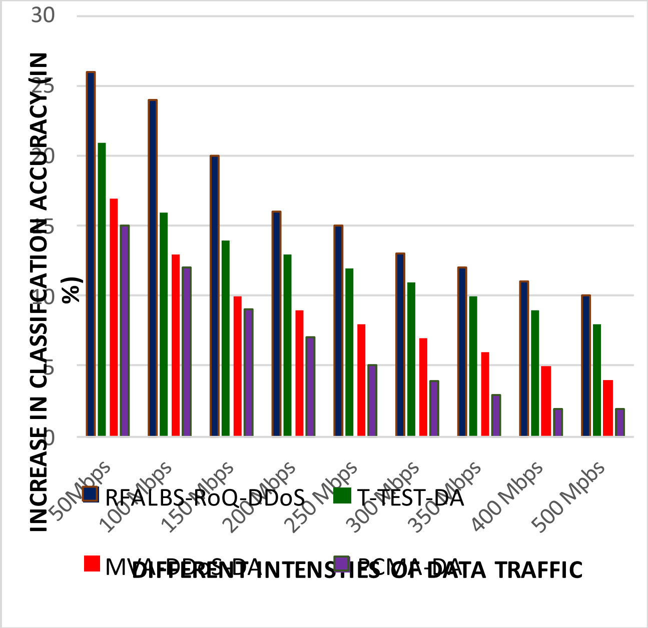

Figure 5: Proposed RFALBS-RoQ-DDOS attack detection scheme-Increase in classification accuracy with different intensities of data traffic

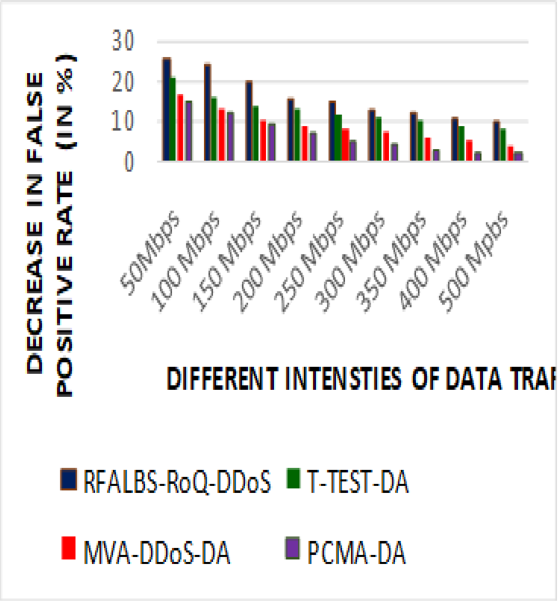

Figure 6: Proposed RFALBS-RoQ-DDOS attack detection scheme-decrease in false positive rate with different intensities of data traffic

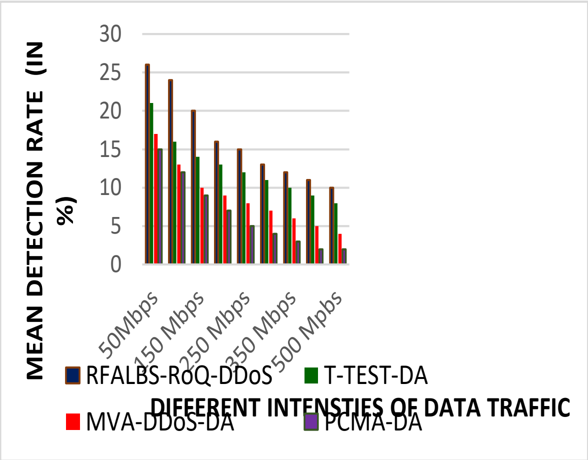

Figure 7: Proposed RFALBS-RoQ-DDOS attack detection scheme-mean detection rate with different intensities of data traffic

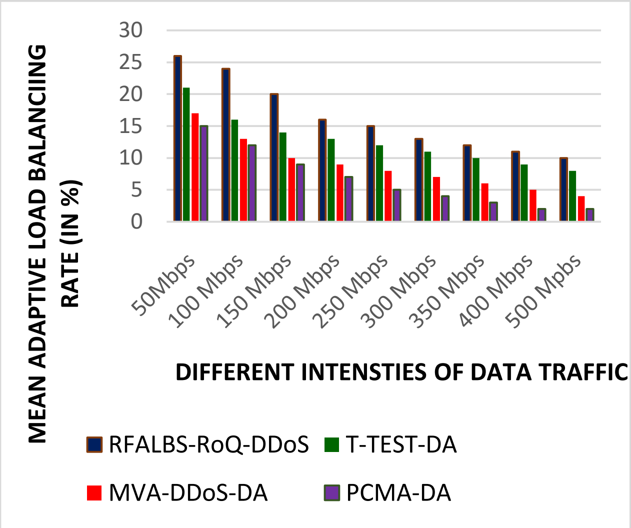

Figure 8: Proposed RFALBS-RoQ-DDOS attack detection scheme-mean adaptive load balancing rate with different intensities of data traffic.

In the final part of the investigation, the proposed RFALBS-RoQ-DDoS technique and the benchmarked T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes are investigated based on percentage increase in the mean detection rate and the percentage mean adaptive load balancing rate with different intensities of data traffic. Figure 7 and 8 exemplars the performance of the proposed RFALBS-RoQ-DDoS and the benchmarked T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes based on the evaluation metrics such as the on percentage increase in the mean detection rate and the percentage mean adaptive load balancing rate with different intensities of data traffic. The on percentage increase in the mean detection rate of the proposed RFALBS-RoQ-DDoS are considered to be relatively excellent on par with the benchmarked approaches, since it used the benefits of Friedman hypothesis testing for phenomenal discrimination of normal data traffic and malicious traffic.

Thus, the percentage mean adaptive load balancing rate percentage increase in classification accuracy percentage increase in classification accuracy of the proposed RFALBS-RoQ-DDoS is identified to be 7%, 10% and 13% excellent to the baseline T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes. Likewise, the percentage decrease in false positive rate of the proposed RFALBS-RoQ-DDoS are considered to be relatively reduced on par with the benchmarked approaches, since it used an adaptive congestion control approach that polices the network traffic under malicious data traffic. Thus, the percentage decrease in false positive rate of the proposed RFALBS-RoQ-DDoS is identified to be 9%, 12% and 15%, minimized on par with the benchmarked T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes.

V. CONCLUSIONS

The proposed RFALBS-RoQ-DDOS attack detection scheme was presented as an attempt for achieving a predominant solution to the issue that emerge under the impact of RoQ-based DDoS attack based on the inclusion of Friedman hypothesis testing. This proposed RFALBS-RoQ-DDOS attack detection scheme also included an adaptive load balancing approach for the objective of resolving the issue that are more common under the differentiation of normal and malicious cloud traffic. It is also identified tobe predominant in provisioning balanced network traffic for preventing congestion in the network, the state of congestion is the major resulting state of RoQ-based DDOS attack influence. The simulation results demonstrated that the proposed RFALBS-RoQ-DDoS technique is predominant in ensuring excellent mean detection rate and mean adaptive load balancing rate of nearly 23% and 28%, compared to the T-TEST-DA, MVA-DDoS-DA and PCMA-DA schemes considered for investigation. As the part of the future plan, it is planned to devise a Kruskal-Wallis Test-based RoQ DDoS attack mitigation mechanism for investigating the traffic flow in a multi-perspective angle.

REFERENCES

1. Sattar, I., Shahid, M., & Abbas, Y. (2015). A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment. International Journal of Computer Applications, 115(8), 23-27.
2. 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, 1(1), 498-499.
3. Osanaiye, O., Choo, K. R., & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. Journal of Network and Computer Applications, 67, 147-165.
4. Vissers, T., Somasundaram, T. S., Pieters, L., Govindarajan, K., & Hellinckx, P. (2014). DDoS defense system for web services in a cloud environment. Future Generation Computer Systems, 37(1), 37-45.
5. Somasundaram, T. S., & Govindarajan, K. (2014). CLOUDRB: A framework for scheduling and managing High-Performance Computing (HPC) applications in science cloud. Future Generation Computer Systems, 34(1), 47-65.
6. Saini, B., & Somani, G. (2014). Index Page Based EDoS Attacks in Infrastructure Cloud. Communications in Computer and Information Science, 1(1), 382-395.
7. Daffu, P., & Kaur, A. (2016). Mitigation of EDoS attacks in cloud: A review. Communication and Computing Systems, 1(1), 34-49.
8. Khan, M. A. (2016). A survey of security issues for cloud computing. Journal of Network and Computer Applications, 71(1), 11-29.
9. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.
10. Şimşek, M. (2015). A new metric for flow-level filtering of low-rate DDoS attacks. Security and Communication Networks, 8(18), 3815-3825.
11.]Li, H., & Wu, Q. (2012). A distributed intrusion detection model based on cloud theory. 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, 1(1), 45-56.
12. Singh, S., Jeong, Y., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 75(1), 200-222.
13. Daffu, P., & Kaur, A. (2018). Energy Aware Supervised Pattern Attack Recognition Technique for Mitigation of EDoS Attacks in Cloud Platform. International Journal of Wireless and Microwave Technologies, 8(1), 42-49.
14. Wang, B., Zheng, Y., Lou, W., & Hou, Y. T. (2015). DDoS attack protection in the era of cloud computing and Software-Defined Networking. Computer Networks, 81(1), 308-319.
15. Osanaiye, O., Choo, K. R., & Dlodlo, M. (2016). Change-point cloud DDoS detection using packet inter-arrival time. 2016 8th Computer Science and Electronic Engineering (CEEC), 1(1), 23-34.
16. Shevtekar, A., & Ansari, N. (2008). A router-based technique to mitigate reduction of quality (RoQ) attacks. Computer Networks, 52(5), 957-970.
17. Xiang, Y., Li, K., & Zhou, W. (2011). Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics. IEEE Transactions on Information Forensics and Security, 6(2), 426-437.
18. Zhang, C., Cai, Z., Chen, W., Luo, X., & Yin, J. (2012). Flow level detection and filtering of low-rate DDoS. Computer Networks, 56(15), 3417-3431.
19. Thaper, R., & Verma, A. (2015). Adaptive Pattern Attack Recognition technique (APART) against EDoS attacks in Cloud Computing. 2015 Third International Conference on Image Information Processing (ICIIP), 1(2), 12-24.
20. Thaper, R., & Verma, A. (2015). Enhanced-Adaptive Pattern Attack Recognition Technique (E-APART) Against EDoS Attacks in Cloud Computing. Journal of Cases on Information Technology, 17(3), 41-55.
21. Deka, R. K., & Bhattacharyya, D. K. (2016). Self-similarity based DDoS attack detection using Hurst parameter. Security and Communication Networks, 9(17), 4468-4481
22. Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2016). FFSc: a novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis. Security and Communication Networks, 1(1), 45-56.
23. Nathiya, T. (2017). Reducing DDOS Attack Techniques in Cloud Computing Network Technology. International Journal of Innovative Research in Applied Sciences and Engineering, 1(1), 23.
24. Bhushan, K., & Gupta, B. (2018). Hypothesis Test for Low-rate DDoS Attack Detection in Cloud Computing Environment. Procedia Computer Science, 132(1), 947-955.
25. Shamsolmoali, P., Zareapoor, M., & Alam, M. (2019). Multi-Aspect DDOS Detection System for Securing Cloud Network. Cloud Security, 1(2), 1952-1983. doi:10.4018/978-1-5225-8176-5.