# Novel Framework to Filter DoS attack in Cloud Environment

Vijay G.R
PhD Scholar, Dept. of CSE
JNTUA
Anantapur, Andhra Pradesh

Dr. A. Rama Mohan Reddy
Prof.,Dept of CSE.
SVU College of Engineering
Tirupathi, Andhra Pradesh

***Abstract*—Cloud computing has emerged as a successful technology for all requirements ranging from academic to business ,defense to service due to on dynamic nature ,service on demand and pay as you use feature and its ability of providing storage without need to spend on infrastructure routinely. As in any technique cloud computing is also prone to variety of security challenges which as possessed uncertainty in the customer's willingness in opting to cloud service. Denial of Service (DOS) is a form attack where in the authorized user is denied the service by the malicious attacker which results in low delivery of service as well as the resources are made unavailable to the authorized user which results in poor service and unnecessary resource consumption and maintaince cost for the service provider. In this paper we suggest a novel framework to filter the DoS attack in the cloud environment using in the filtering algorithm. From the simulation result it is found that proposed system successfully detects and mitigates the DoS attack in cloud environment.**

***Keywords—cloudcomputing,Denial of service,Queue,Resource allocation,virtual machine.***

## I. INTRODUCTION.

Cloud computing is mechanism which facilitates convenient, on-demand network accessing for a pool of configurable as well as reliable computing resources which are quickly allotted and released with minimal customer management effort or service provider interaction. The various essential characteristic of the cloud computing are self service on demand, ubiquitous network access, resources sharing, locality independence, scalability and measurable service. Cloud service involves different service models such as Cloud software as service (SaaS), Cloud platform as service (PaaS) and Cloud infrastructure as service (IaaS).Cloud is deployed in different forms like private cloud, public cloud, hybrid cloud and community cloud [1]. In cloud computing pool of shared resources are unified using virtualizations or job scheduling mechanism. Wherein virtualization process of creating a set of logical resources be it hardware platform, operating system, network resources or any other kind of resources which are implemented in the form of software component that acts like physical resource. Through cloud computing we can access hardware as well as system software available in the remote datacenter and avail services on the basis of these resources by accessing through internet. These resources are managed in such a way that they dynamically scale matching the load and run on a business model of pay as you use policy. The features like multi-tenancy, enhanced resource utilization, scalability allows advantages of virtualization, resource management and job scheduling to be used in huge infrastructures such as data centers [2].

Despite the success, popularity and extensive availability of tools and service providers for cloud computing. There also exist a huge number of drawbacks or limitations associated with this technology. In order to maximize the benefits from cloud providers, developers as well as the user must consider these challenges. Several issues related to security and service play a significant role in assessing the performance of the cloud. Few of the issues are user privacy, service availability, and security of data, data lock-in, and recovery during disaster, programmability, energyefficiency, performance, scalability [3]. A denial of service (DoS) attack is mainly characterized as attack wherein the user or organization is deprived from service or resources they have paid for. Generally the loss of service is seen as the inability of the network service like email to be unavailable or temporary loss of network connectivity as well as services. In worst scenario for instance a website

which is accessed by billions of user might be occasionally forced to be temporarily unavailable. Another major threat is DoS can also eliminate programs and files present in the system. The attack has maximum effect when both the target and attacker are equally well equipped in terms of bandwidth and computing resources. In order to maximize the impact distributed Denial of Service (DDoS) is used wherein the attacker can successfully flood sophisticated web server which is comprised of web servers that are serviced powerful load balancer. In DDoS the attacker uses multiple systems to launch attack on single or multiple targets. In order to magnify the impact the perpetrator uses client or server technology. [4].

IN this paper we present a novel framework to detect and mitigate the impact of DoS attack on the cloud computing environment. Section II discusses about various work carried on this domain. Section III illustrates problem description. In section IV discussion about the design methodology used in our proposed system is provided. Section V discusses about result analysis and section VI will provide conclusion and future of our work.

## II. RELATED WORK.

In this section we discuss about the various work performed by different authors in related to Denial of service threat in cloud environment.Intially mitigation effort starts with identifying or detecting the attack one such work is carried out by Saleh and Manaf et al [5] suggested a Protective framework to mitigate the effect of DoS and DDoS in HTTP based network. The authors have designed a framework known as FCMDPH.Wherein the authors suggested framework operates in three layers by initially blocking the attacking IP source if it is present in the blacklisted table, second layer authenticates request by validating if it is generated from automatic tool or human. Finally the last layer is used to eliminate flash crowd attack as well as high rated DDoS attack. Although it protects web based application from DDoS and DoS attack it suffers from low rate of false negatives as well in detecting all forms of flash crowd attacks and also failed in validating incoming request. Similar work was proposed by Latif et al [6] suggested a algorithm based on decision tree to detect DDoS attack in cloud -assisted WBAN.Authors suggest that the proposed EVFDT successfully detects occurrence of DDoS attack in WBAN.various techniques like adaptable tie breaking threshold, lightweight repetitive pruning mechanisms are used in order to achieve it. Evaluation of Enhanced very fast detection tree EVFDT is performed on the basis of Performance matrices like accuracy of classification, size of tree, memory and time. From the simulation it is found to have high detection accuracy and reduced false alarm. Deshmukh and Devadkar[7] illustrated the DDoS attacks and its implication on cloud environment and have highlighted on the features needed to considered at time of selecting an appropriate defense strategy against DDoS attack.

Different kind of DoS attacks are there one such type is DDoS ,identifying of Attack is first phase in reducing the aftermath effect of the attack one such work related to DDoS is carried out by Lonea et al [8] where the authors have proposed a solution based on the evidence that are received through Intrusion Detection System (IDS) which are used in virtual machines present in the cloud along with data fusion methodology. Authors have suggested a quantitative solution to analyze the alerts generated by the IDSs through Dempster Shafer theory (DST) and Fault tree Analysis (FTA) for flooding attacks. Lastly Dempster combination rule is applied to collaborate evidence from multiple independent sources. Another similar work is carried out by Rahman and Cheung [9], have proposed a secured model to Detect and mitigate Dos as well DDoS attack in cloud. The authors have investigated different mechanism which can be used for DoS as well as DDoS attacks and suggested hardware based watermarking framework mechanism to secure the organization against such attacks. The availability of cloud resource is crucial in cloud computing Dos and DDoS attack makes it difficult for the user to avail cloud service, in order to overcome this Farahmandian et al [10] as suggested a secured virtualization model to defend cloud against DDoS attack and thereby improving the availability of resources to the user. The authors also suggest that by using their model it is possible to enhance availability of resource in virtual machine in a real time basis whenever the perpetrator tries to disrupt cloud resources. Another similar work is carried by Singh and Panda [11] have proposed a framework

which detects the DDoS attacks which also takes into account degradation of network performance. The authors have utilized signature Based as well as anomaly based DDOs identification method which encompasses the need of dynamic and algorithm based on multithreshold approach. Application are used to identify or detect the form of attacks in different networks one such application is developed by Citrix[12] known as Citrix Netscaler, Citrix Netscaler application Delivery Controller (ADC) ensures a robust as well as affordable defense for organization against DoS attacks. It is capable of withstanding DoS attacks across every layer in computing stack. Flooding is a form of DoS attack in order to mitigate this a work was carried out by Zunnurhain et al [13] have proposed a model to detect and protect against flooding which is a form of attack in DoS. Authors propose that their model will identify and filter packets at the time of DoS attack. Authors also propose that the FAPA is independent from service provider.FAPA performs the analysis of traffic pattern to detect flooding and flood removal is done through filtering. Another similar work is carried by Ismail et [14] have proposed a model to detect DoS attack based on flooding in cloud. Authors suggests use of a multi phase model wherein the initial phase responsible for modeling traffic pattern required for baseline profile and second phase involved in intrusion detection stage and finally preventive measure. In order to detect flooding authors have utilized covariance mathematical model. Ismail et al[15] has suggested a framework for detecting and preventing DoS in cloud environment.Here authors focused on overcoming challenges associated with different phases. Authors have used covariance matrix in detection stage to determine time to life of attack source. For prevention they have used honey pot technique. Through simulation and uml class diagram authors have exhibited where there model is applicable in cloud. Another similar work on detection and prevention is carried by Wang et [16] suggested a DDoS mitigation model based on highly programmable network monitoring mechanism which allows to detect attacks and also provides a flexibility in order to take swift action against the attack. Authors suggest through simulation they have found the technique to be effective as well as efficient. another work related to detecting and filtering DOS is carried by Chonka [17] et al suggest a framework which will detect HTTP DoS attack and XML Dos attack and filter such traffic. The authors also suggest that the framework identifies the source of the attack in very short time.

In the next section the paper will discuss about the various limitations as well loopholes in the existing system and will concentrate on illustrating the solution to overcome such limitations and loopholes. size.

## III. PROBLEM DESCRIPTION.

This section identifies the various problems associated with Dos attacks in the cloud environment. There are various set of research work being carried in the direction of security related challenges as well as issues in cloud. Various researchers have opted different approaches in developing solution to security issues in cloud. The approaches may be based on the cryptographic mechanism or non-cryptographic approach. But these available solutions have certain flaws and hence they fail to meet the demands of the dynamic behavior of the cloud. In majority of the attack cases the primary attacks are performed in the initial phase such as authentication .In majority cloud application the security of the cloud is depended on the client browser such Google chrome,mozilla Firefox and internet explorer and so on which are developed by a third party. Whose security features is also dependent on the reliability of the internet connectivity. Since the internet is itself is prone to several security limitations which are also capable of having a adverse effect on the cloud environment such as hacking clouds [18].It is evident that from the existing solution there is not clear solution available and large gap between the ongoing research to meet the real time demands in terms of cloud security.

The work carried by Saleh and Manaf [5] though provides some sort of prevention, it is not completely acceptable as it inherent flaws like low rate of false negativing.Morever this work also fails in identifying requests as well incoming flash crowds. The work carried by Latif et al [6] developing a framework called EVFDT which is implemented on the based on Leach protocol as certain flaws due to the LEACH protocol limitation like insufficient clarity of positional sensor,

increased power consumption for communication among cluster head and base stations with long distance .The DDOS mitigating work proposed by Lonea et al [7] based on IDS which is prone to produce False negative and false positive error. The work carried by Rahman and Cheung [9] framework using hardware based watermarking technique in securing an organization in which the reliability of this hardware water marking mechanism depends on the router which should poses security against TCP SYN attack'. The work of securing clouds using virtualization [10] which is based on the identification of Virtual machine relies on the success of virtual machine identification. Different approaches and application are used in [11,12,13,14,15,16,and 17] to detect and prevent the DDoS attack wherein the approaches are similar and slightly varying in the mechanism followed. The success of these approaches and application are dependent on several constituent components used in developing these approach or application. From the available resources it is observed that though the ongoing research works have mitigated certain security issues still there are several issues which are needed to addressed at earliest. In order to provide an appropriate solution a framework based on filter is proposed in this paper. In the following section of the paper the design and implementation of the proposed system is illustrated.

## IV. PROPOSED SYSTEM.

This section discusses about the design methodology used in designing and implementing the proposed system.

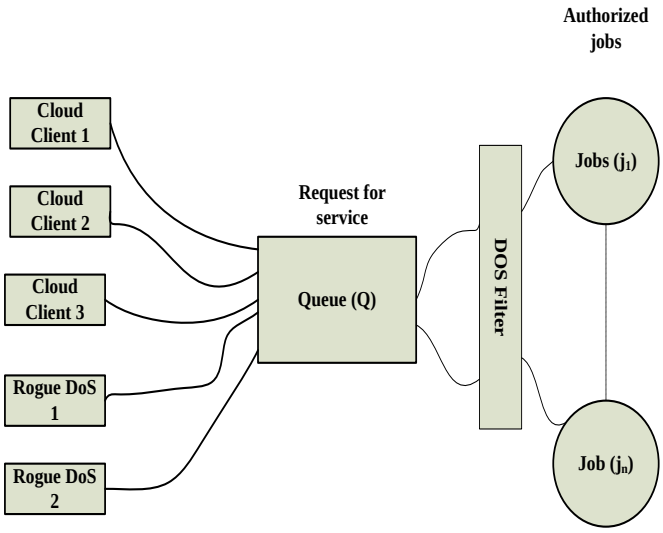


Figure 1:Architecture of the system.

The figure 1 depicts architecture of system .wherein it is observed that several cloud clients denoted by $C_c$ are using the cloud resource and service which are denoted by $C_R$ and $S_c$ respectively. The services requested are aligned in the queue system denoted by Quoin the basis of this queue the clients are allotted resource or the service subscribed by them. But as shown in the figure 1.The presence of Rogue or malicious entity with cause a service impact on the performance in term of various feature related to cloud. The attacker will use single or multiple compromised nodes to flood the cloud service so that the eligible or authorized client are deprived from the cloud services. In order to overcome this issue and ensure the authorized client is benefitted by the cloud service and cloud resource ,This work has introduced a filter which performs filtering of the malicious packets generated by the perpetrator. In the proposed system the filter is used to filter the unwanted packets generated by the perpetrator. In order to achieve this proper method of scrutiny is performed. Wherein the incoming packet is checked for whether it is user generated or packet is generated by an automated tool or system to flood the network.

Initially the source of the request that is user source is identified using various consideration such as to which region this user source belong, number of thread generated from that particular user source ,how many jobs are generated from these threads, how many threads are requesting for the cloud services and the requests from these threads are processed in the form of queue in which on the

basis of the scheduling the threads are allotted with resources or services from the cloud. in order to validate the authorized user generated requests filtering process is carried out, once the filtering is done the request is sent to the virtual machine ($V_m$) for processing of the jobs. This is illustrated in the flowchart depicted figure 2.user request which are in the form of packet are scrunitized.In this process of scrutiny takes advantage of the information present in the packet header which contains necessary information such as source ID,Packet generation time, authenticated user session ID,data content of the packet, Service ID and so on. Based on these information

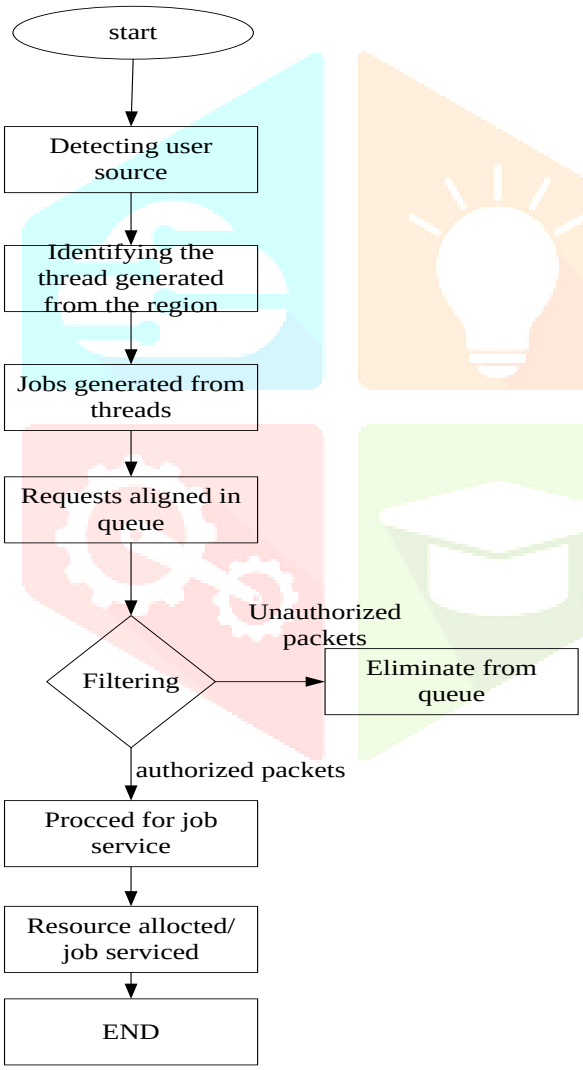


**Figure 2:Flowchart illustrating the process**.

Virtual machine ($V_m$).

The requests from the authorized user as well as the malicious attacker which are aligned in the queue requesting the cloud resource are allotted with a virtual machine. The cloud will check for the available free virtual machine which will be allocated to the jobs. Allocation of the virtual machine is entirely dependent on the cloud service provider. The cloud service provider will opt for a suitable scheduling policy in order to identify the status of the virtual machine. So that there is no long waiting of the requests at the queue. The cloud will compute the capacity of the $V_m$ by considering various factors like the number requests that can be handled by the $V_M$ simultaneously, number of processors available for processing and so on. cloud service provider must also ensure that no $V_m$ is allocated with excess of job request.The following algorithm illustrates the process of virtual machine allocation to the user requests.

**Table 1:Algorithm 1:Virtual Machine allocation.**

| |
|---|
| **Input :Request from Client** |
| **Output:$V_M$ allocation** |
| **Start:** |
| **1.Q→User request** |
| **2.$C_{sp}$ checks $V_m$** |
| **3.if ($V_m$_capacity > current job** |
| **4. min_range=0;** |
| **5.max_range=cjobs;** |
| **6.$J_{allot}$→ same $V_m$** |
| **7.$V_m$ Satus → Busy** |
| **8. VMM=new VMM(svm, oVmJobs, min_range, max_range);** |
| **9.else** |
| **10. min_range=cjobs-vm_Capacity** |
| **11.max_range=cjobs;** |
| **12. $J_{allot}$→ Prt of job as per $V_m$ capacity** |
| **13. Set current $V_m$ Status busy.** |
| **14. VMM=new VMM(svm, oVmJobs, min_range, max_range)** |
| **End** |

The above table 1 illustrates algorithm 1.which explains the process of job allocation to the Virtual machine. The process of virtual machine allocation is as follows. the requests in the queue requiring the

$V_m$ is considered by the $C_{sp}$ which denotes cloud service provider which is responsible for the allocation of the virtual machine and resources to the client request. $C_{sp}$ examines the status of the $V_m$ available in the cloud. $C_{sp}$ also checks for the $V_m$ capacity. The assessing of the $V_m$ is done by defining a range for the jobs and considering the total number of requests or jobs available in queue for servicing. the $C_{sp}$ finds the $V_m$ capacity greater than the jobs present in the queue ,the job is allocated to the same $V_m$ and the status of the $V_m$ is set to busy.The Csp takes the note of the new status of the $V_m$ along with its request list for servicing. When the $C_{sp}$ encounters a $V_m$ with capacity less the jobs present in the queue,the new job is allocated to same $V_m$ as per its processing capacity which is available and the status of the current $V_m$ is set to busy. This is iterative process and is performed for all the available $V_m$ in the cloud. By this way it is ensured that that $V_m$ is idle or no excess job is assigned to any of the $V_m$.

At the time of the servicing the request ,$V_m$ will check if the request is authenticated one or unauthorized one. By using this principle it is possible to identify the DoS attack using different attributes such as authorized session, valid source, valid service request, and number of requests generated and so on. A threshold value for request is set ,so that to distinguish between manual generated request and automated generated request.

**Table 2:Algorithm 2:Virtual Machine filters DoS**.

| **Input: Service request to $V_m$** |
|---|
| **Output:Processed request** |
| **Start:** |
| **1.$N_{job} \rightarrow V_m$** |
| **2.$V_m$ ? $N_{job}[A_{User}, Un_{User}]$** |
| **3.Vm? [authUser,i,Region_id,,new JobTs]** |
| **4.if (authUser,i,Region_id,,new JobTs== Authenticate)** |
| **5.else** |
| **6.Filter the request** |
| **7.display current jobs** |
| **End.** |

The above algorithm 2in Table 2, illustrates the $V_m$ activity corresponding to Dos filtering. When a new job or request arrives at the $V_m$,it is scrutinized to validate whether it is a authenticated request or automated request generated by a system to disrupt the cloud.$V_m$ checks the job header for information related to authorized user, the region ID from where it is generated,Time of the job generation, Source of the job, and service requested by the job. if the parameters are matched then the job is considered as authenticated and is processed. If the parameters fail then it is considered as a request generated for DoS attack. The $V_m$ filters or eliminates the entire request which fail the authentication and the valid request are filtered and list of current requests are displayed.

**Table 3:Algorithm 3:Filtering Process.**

| Input:User request present in Queue |
|---|
| Output:Processed request/Job. |
| Start: |
| 1.$V_m$ initiated |
| 2.Fetch request from Queue. |
| 3.Check (Request==True) |

| |
|---|
| 4.{ |
| 5.Request_Authenticated user==True |
| 6.Source ID==True |
| 7.Request_time==True |
| 8.Service_ID==True |
| 9.} |
| 10.Process User_request |
| 11.else |
| 12.Delete request |
| 13.Display {JobId,Ext_Time,Used_Cpu,Free_Cpu,Used_memory ,Free_memory,Used_disk,Free_disk} |
| End. |

Table 3 illustrates algorithm 3 corresponding to the pre-Execution filtering process .It should be noted that there is two levels of filtering associated with the $V_m$.The second level of filtering is performed in order to save the virtual machine resources and datacenters being used to for execution of unauthorized requests. On receiving the request from queue, the srcutinization of the request is stared. This scrutinization is achieved using the information present in the header. The header contains various information related to request such as the Request ID,User ID,region ID,Source ID,Request generation time,service ID and so on. This information's are cross verified with the information present in the cloud. As we are aware the $C_{SP}$ will have all relevant information corresponding to the user/client. The request is checked for user ID,region ID,number of request sent by that user over a period of time,service iD and so on.every request is checked from user Id,to verify it's a authorized request or not,Region ID is also used to validate the user since using a authorized user ID attacker may intend to flood request from different region. Number of requests sent over a time is used to verify if the requests are genuinely generated by a user or an automated tool or system. this is achieved by using a threshold value for the request sent by the user i.e every is user is allotted a threshold value $R_{TH.}$Since the cloud will aware how many request a user can generate manually ,it can easily distinguish between the requests generated by the user as well automated tool or system on the basis of the $R_{TH}$.

This $R_{TH}$ value is defined by the cloud service provider. Service ID is used so that it can be easily track the DOS attack. Wherein when the attacker will flood cloud with request with service ID which are not valid or the service corresponding to that ID is not provided by the cloud. By this way the attacker can keep the cloud resource busy performing unauthorized task and achieving his goal of denying the cloud service or resource to a genuine user. In order to overcome this service ID is used, once it is found that the service ID is invalid such requests are deleted .The above mentioned process is followed to identify and eliminated DoS attacks. The second level of filtering mainly concentrates on reducing the requests for execution in the datacenter. Next section discusses about the observation and outcomes of the proposed system.

## V. Outcomes And Performance Analysis

In this section we discuss about the outcome of our proposed system ,and analyze its performance based on the performance matrices like delay, channel bandwidth, response time and so on. The simulation of the proposed framework is carried through simulation, the algorithm is programmed using the

java .The simulation is performed on the system with following configuration.

CPU:intel i3 processor
Processing speed:2.7 ghz
Memory :4Gb
Storage :500 Gb.

The simulation was performed using 1000 users, four virtual machines and 13 datacentres in order to evaluate the performance of the proposed system.

The table 4 below shows the Simulation of the framework in cloud from intial phase.It specifies the user base configuration and regions,request per user per hour,data size per request ,average peak user and average off-peak user and so on.

Table 4:Configuration of Cloud

| | |
|---|---|
| Enter the user base = 10 | |
| User Base Configuration: | |
| Region [1-5] | |
| Request per user per hour :120 | |
| Data size per request :100 byte | |
| Average peak users :10000 | |
| Average off peak user :1000 | |

The selection of user base can be performed by user or the user can opt for default configuration. It also provides the hardware description that is the physical hardware availability.

The table 5 below illustrates resource allocation and Virtual machine availability.

Table 5:Processing Details

| $V_m$-ID | Job_ID | No of jobs | Used CPU | Free CPU | Transmission region | Execution time |
|---|---|---|---|---|---|---|
| 1 | 3444-13847 | 10403 | 26% | 74% | 1-5 | 250 ms |

The table 5 illustrates the processing details such as number of jobs processed,percentage of CPU used ,memory used and available, execution time and son

Request delivery Ratio (RDR):represents the ratio of number of request that is processed.RDR signifies the processing capacity of the network, request analysis of the network. It also symbolizes integrity, dependability as well as effectiveness and efficiency of framework.

RDR= $\frac{\sum \text{Number of requests receiv}}{\sum \text{Number of requests proces}}$

Higher value of RDR signifies better performance of the framework.

End-to-End Delay: Represents the average time consumed by the request to be processed. It also includes the delay caused for route discovery as well as waiting time in queue. End-to-End is only applicable to successfully processed request.

End to End delay= $\frac{\sum(Arrival-tim}{\sum(number\ of\ li}$

Lower the value of End to end delay better is the performance of framework.

### A. *Analysis of the outcome:*

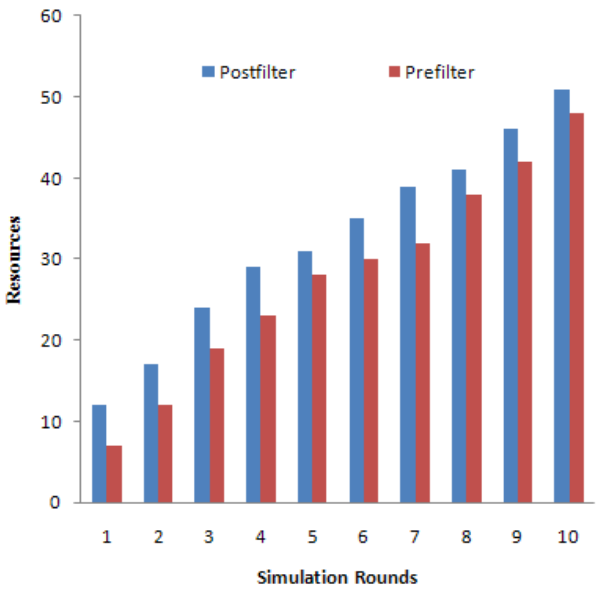


Figure 3:Indivisual Analysis

The above figure illustrates the resource allocation for the request before filtering the request as well as after filtering the request. It is observed that more resources are allocated to the request after the filtering process when compared to pre filtered requests. This highlights the effectiveness and efficiency of our proposed system also the reliability of our framework in mitigating DoS attack.

We perform the hypothetical comparison our proposed system with Sarhadi and Gafori [19].This work is considered for the comparison since the authors have performed similar research. In this

paper the response take has been altered to delay and comparison is carried out with suitable changes. The comparison is carried for Dos attack mitigation attack. The comparison is performed on various attributes like end to end delay, channel bandwidth and execution time.

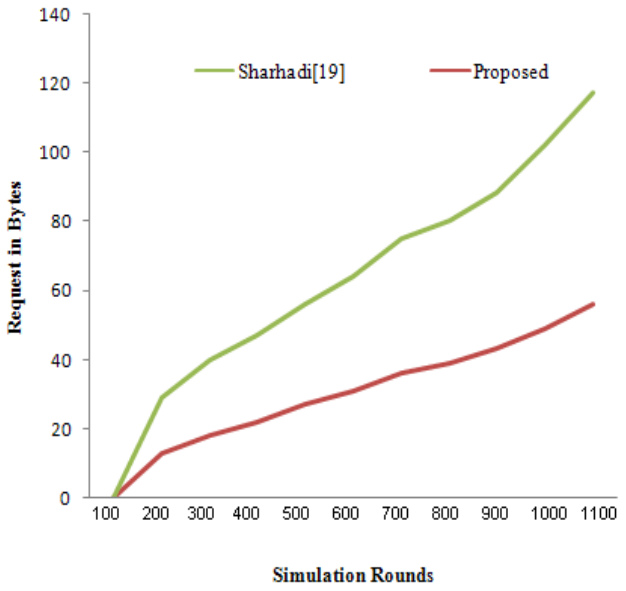


Figure 3:Comparison of End to End delay between proposed system and the existing protocol.

Figure 3 shows the graphical comparison of the End to end delay with varying request size. When there is a DOS attack the number of request increase and thus makes end to end protocol higher. From the figure 3 it is evident that our proposed system has less delay compared to existing protocols. The advantage of filtering the bad request or malicious request has benefitted the reduced delay in the proposed system.

Another parameter used to analyze the performance of the proposed system is the channel bandwidth, in case of DOS attack the channel bandwidth is misused by the attacker by flooding the network with malicious request or unwanted request .Thereby reducing the actual bandwidth usability for the authorized user. The figure 4 depicts the graphical comparison of the channel bandwidth consumption by different existing protocol and the proposed system.

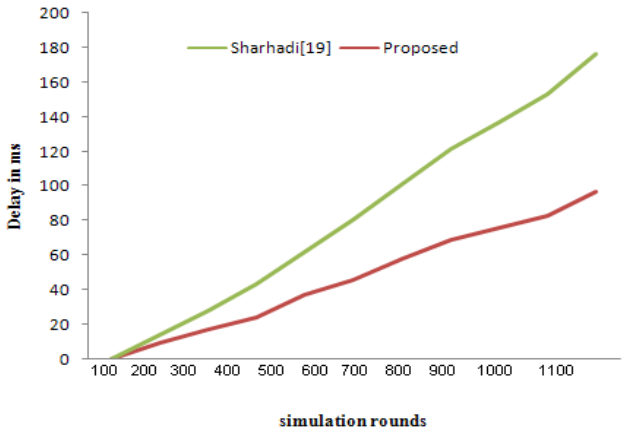


Figure 4:channel bandwidth consumption.

From the figure 4 it is seen from the figure ,due to the use of our proposed system the channel bandwidth consumption is reduced. This is due to the fact that the use of filtering technique in the proposed system eliminates the malicious or unauthorized request which consume limited bandwidth and impact the performance of the cloud service by denying as well as delaying the service and or resource to the legitimate request.

## VI. CONCLUSION.

In cloud computing environment, the security concerns are high as it is easily accessible through internet. In order to mitigate the security threats in cloud environment in the form of DOS attack. A novel framework based on filtering is present. From simulation result it is found that the proposed framework exhibits a good responsive result by preventing the DOS attack. The light weighted algorithm also improves the resource allocation time as well as reduces execution time.

References

[1] Nikos Antonopoulos, Lee Gillam,"Cloud Computing: Principles, Systems and Application",Springer Science & Business Media, 16-Jul-2010 - Computers - 382 pages

[2] Ronald L. Krutz, Russell Dean Vines,"Cloud Security: A Comprehensive Guide to Secure Cloud Computing",John Wiley & Sons, 31-Aug-2010 - Computers - 384 pages

[3] Rajkumar Buyya, James Broberg, Andrzej M. Goscinski,"Cloud Computing: Principles and Paradigms",John Wiley & Sons, 17-Dec-2010 - Computers - 664 pages

[4] Nathalie Weiler,"Honeypots for Distributed Denial of Service Attacks",WETICE'02,1080-1383/02

[5] A.Saleh and A.Manaf,"A novel Protective Framework for Defeating HTTP-Based DEnial of service and Distributed Denial of service Attacks",Hindawi Publishing Corporation the scientific World journal vol 2015,Article ID 238230.

[6] R.Latif,H.Abbas,S.Latif and A.Masood,"EVFDT:An Enhanced very Fast DEcision Tree Algorithm for Detecting Distributed Denial of Service attack in Clou-Assisted Wireless Body Area Network",Hindawi Publishing Corporation Mobile Information Systems vol 2015,Article ID 260594.

[7] V.Deshmukh and K.Devadkar,"Understanding DDoS Attack & Effect In cloud Environment ",Elsevier ICAC3'15,Doi:10.1016/j.procs 2015.04.245.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[8] M.Lonea,E.Popescu and H.Tianfield,"Detecting DDoS Attacks in Cloud Computing Environment",Proceedings of the World Congress on Engineering 2013,vol II,WCE 2013,july 2013.

[9] M.Rahman and M.Cheung,"A Novel Cloud Computing Security Model to Detect and Prevent Dos and DDos Attack,IJACSA,vol 5,No 6,2014.

[10] S.Farahmandian,M.Zamani,A.Akbarabadiand M.Zadeh,"A secure virtualization model for cloud computing to Defend against DDos Attack,JNIT,vol 4,No 8,Oct 2013.

[11] b.singh and N.panda,"Defending Against DDoS flooding attacks-A data Streaming Approach",International journal of computer & IT .

[12] Citrix Netscaler:A powerful Defense Against Denial of Service Attacks,"white paper.

[13] K.Zunnurhain,s.Vrbsky and R.Hasan,"FAPA:FLooding attack Protection Architecture in a cloud system",IJCC.

[14] N.Ismail,A.Aborujilah,S.Musa and S.Zad,"Detecting Flooding Based DoS Attack in Cloud Computing Environment Using Covariance Matrix Approach",ICUIMC jan,2013.

[15] N.Ismail,A.Aborujilah,S.Musa and A.Shahzad,"New Framework To Detect and Prevent Denial of Service Attack In Cloud Computing Environment",IJCSS,vol 6,issue 4.

[16] Wang, Bing, et al. "DDoS attack protection in the era of cloud computing and Software-Defined Networking." *Computer Networks* 81 (2015): 308-319.

[17] Chonka, Ashley, et al. "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks." Journal of Network and Computer Applications 34.4 (2011): 1097-1107.

[18] Dykstra, Josiah, and Alan T. Sherman. "Understanding issues in cloud forensics: two hypothetical case studies." *Proceedings of the Conference on Digital Forensics, Security and Law*. 2011.

Sarhadi, Reza Manouchehri, and Vahid Ghafori. "New Approach to Mitigate XML-DOS and HTTP-DOS Attacks for Cloud Computing." *International Journal of Computer Applications* 72.16 (2013