Decentralization for Securing Data with Cloud Firewall Framework to Increase QoS

S. Dhivya* and T. Kamalakannan
Department of Computer Science, Vels University, Chennai - 600117, Tamil Nadu, India; sdivyadevi@gmail.com, kannan722003@yahoo.co.in

Abstract

Objectives: To implement the cloud decentralized firewall concept. Methods/Statistical Analysis: A balanced approach is always needed while satisfying the user’s need and at the same time the Quality of Service (QoS) is to increase. The solution could be in allocating the resource dynamically to handle the multiple users and to optimize the cost of the resource provision. Mostly, queuing theory is used for quantitative system analyze. Markov Chain and Z-transform is used to obtain the mean packet in the response time to closed form of expression. Findings: The M/M/1 model is our proposed M/Geo/1 model for better firewall real system. The experimental results also prove that we can set up the firewall in cloud with comfortable cost to cloud users.

Keywords: Cloud Computing, Firewall, Resource Allocation, System Modeling, Virtualization

1. Introduction

Cloud storage has emerged as a hopeful result providing the present, expedient, and on-demand to a large amount of data shared through internet. Current days millions of users stored private data, such as photos and videos, through social network applications based on cloud storage on a day by day basis. All the sizes influence the cloud to enhance improvement and collaboration. To Despite the profuse profit of cloud computing, privacy of concerns, persons and users enterprise are loath to outsource their receptive data, including emails, personal health records and government classified files, to the cloud. This is because once sensitive data are outsourced to a remote cloud; the consequent data owners lose direct control of these data. Cloud Service Providers (CSPs) would assure to ensure owners’ data protection by mechanisms like virtualization2 and firewalls3. Various types of attacks occupy the cloud to spread various viral data in cloud. Denial of service attack attacks the cloud to delay the user’s process and disprove the cloud’s reputation. Cause of these attacks users are scaring about their data whether the data will secure or not. Protecting cloud data center’s data from these types of attack is crucial and effective one. This process is done by cloud firewall.

Cloud firewall works against the traffic malicious attack. Firewall3 has lot of types. In that rule based firewall is important among traditional firewall. Traditional firewall is only working on private networks which deploy particular services5. Based on our knowledge, existing system worked on centralized cloud firewall. The centralized cloud firewall to the entire cloud data center, the complex attacks and the spreading of various services mean improvement of packet arrival rate and
large rule set. But it is not work on the quality of service. In attacking time it is concentrate on only prevent cloud from attack not on QoS.\(^5\) Prizing this service is a big issue in cloud firewall. Users are willing to get the cloud firewall on low cost. Financial reward is the crucial aim to firewall providers. Providers are working on how to satisfy the user’s prize without loss of profit. Along with the cost we need to provide the better QoS service to satisfy the customers. Cloud service provider is the main entity in cloud firewall. Cloud customers pay rent to cloud service provider to store their application. These hosting services are grouped together to form a clusters. The resources are allocated dynamically to set up the cluster in firewall. But these all firewalls are working together to note the incoming data packets and improve the QoS service in cloud. Our contributions are follows:

- Handle multiple users simultaneously is done by dynamically allocate the resource to the customers.
- Embedded Markov Chain and Z-transform are used to obtain the mean packet response time in closed form expression. Compared with the M/M/1 model our new M/Geo/1\(^8,9\) model gives better firewall real system and also our experimental results prove that we can set up the firewall in cloud with comfortable cost to cloud users.

### 2. Cloud Firewall Frame Work

To begin with we talk about the sorts of attributes in firewall structure then learn about decentralized cloud firewall system

#### 2.1 Cloud Firewall

##### 2.1.1 Packet Arrival Rate

Fundamentally, Customers cloud administrations to their own and hierarchical employments. Yet, these cloud applications are frightened about different assaults. Long time assaults are exceptionally uncommon due to they can be effectively distinguished. Approaching bundles are endured by long haul assault. This landing of bundle in cloud is fluctuating for each record. Typical parcels will get at low rate and pernicious bundles are gotten at high rate. The required static entry rate in both typical and pernicious bundle are landing rate. The principle danger to the cloud accessibility, here we picked DDoS assault for demo. The assigns standard of DDoS\(^10\) assault period is roughly 5 minutes; with the normal DDoS assault rate are around 500 demand for every second. The mean entry rate is to be test to e-business site in run of the mill time frame is lower than 10 demands for every second.

#### 2.1.2 Provide Resource

Giving asset in view of the client demand is the huge undertaking. Here we have to get the demand first. At that point these solicitations send to cloud specialist co-op. He will acknowledge and virtualizes the asset. In light of the demand they will be coordinated to the comparing asset. While accepting gigantic measure of information virtual machine will get ruined. So we have to distribute the virtual machine to begin with, then we have to enhance the nature of administration. We have to enhance the bundle landing rate. As indicated by QoS imperative, bundle entrance rate and VM events benefit rate, firewall specialist co-ops need to give more assets on-request by starting other VM cases. New VM occurrences can be multiplied in light of the picture record of the extraordinary firewall utilizing the current clone innovation. Especially, firewall suppliers need to progress diverse measure of assets in assault and ordinary period.

#### 2.1.3 Cost and Performance Trade-Off

The two objectives are: Satisfying QoS prerequisite: The parcel reaction times are signified in QoS fulfilled.

- Resources cost is advancement of cloud firewall ought to be diminished the QoS requirement\(^8\).

#### 2.2 A Firewall Framework for Decentralized Cloud

VM has a backcountry advantage utmost of the cloud in the firewall application. A cloud firewall in a unit-VM event is even the most able one to cumbersome to getup customer specific the need of QoS. It is to attestation that the response time in the midst of a united cloud firewall. Along these lines, we propose a decentralized framework where a couple firewall continue running in parallel. The Figure 1, encouraging the servers were collected into the few gatherings and a VM event is begun to pass on an individual firewall for each bundle. The package section rate to the few parallel firewalls was impelled in a privilege VM case for each cluster. The bundle passage rate of into a couple parallel firewalls and impelling right VM case for the firewall in the response of time in the midst of each firewall is to be fulfilling with the QoS essential.
Each and every firewall cloud customer is hosting their application in the cloud data center. So there are M servers in cloud server farm. Packet arrival time is denoted as \( n \) in this scenario for non-attack time. Clusters \( j \) is formed from the server’s \( m \) to work on the legitimate packet data. Then the packet arrival time is,

\[
\sum_{j=1}^{J} m_j^n = M
\]

\[
\sum_{j=1}^{J} \lambda_j^n = \chi^n
\]

Denote the packet arrival time in hosting application.
Packet arrival rate in each firewall, we are having,

\[
\sum_{k=1}^{K} m_k^a = M
\]

\[
\sum_{k=1}^{K} \lambda_k^a = \chi^a
\]

### 3. Cost Optimization in Resource Provisioning

In this area, we first get ready assets provisioning cost. As firewall check rate demonstrating is critical to assets provisioning cost enhancement, we make a logarithmic model relating to cloud firewall govern coordinating direction and build up that framework benefit times take after geometric distribution.11,12

#### 3.1 Resource Optimization

Give \( T_n \) a chance to demonstrate the low maintenance crevice that CSPs blame VM occasions. \( T_n \) shows standard assault length in \( T_n \). For ease, the circumstance that an assorting of assaults occurs in the unequal assault rate and assault term is not canvassed in this work. Our model is been effortlessly to stretched out to this all inclusive case. In the essential objective to enhance saves provisioning cost, while fulfilling QoS prerequisite at a similar minute. It is intuitive that assets provisioning charge for our proposed cloud firewall relies on upon bundle landing rate. Given \( -a \) and \( -b \), it additionally depends on what number of bunches (\( J \) and \( K \)) are framed. Plus, it is chosen by VM occurrence course of action for the parallel firewalls. To confront the immense cloud firewall related farthest point space, the assets provisioning expense is defined as takes after, Limit

\[
T^n \sum_{j=1}^{J} P_j^n + T^a \sum_{k=1}^{K} P_k^a
\]

Subject to,

\[
\forall j \in [1, J], \begin{cases} \lambda_j^n \leq \mu_j^n \\ r_j^n \leq \Delta T \end{cases}
\]

\[
\forall k \in [1, K], \begin{cases} \lambda_k^a \leq \mu_k^a \\ r_k^a \leq \Delta T \end{cases}
\]

Here \( p_j \) and \( p_k \) demonstrate unit cost of VM case \( V_j \) in the non-assault period, \( V_k \) in assault period, in a specific order, other two mean the administration rate of the two VM examples is handling the cloud firewall, which are in the terms of bundles every second and is given instantly. \( r_j \) and \( r_k \) are response time through firewall for gathering \( m_j \) and \( m_k \) in non-assault and assault period in a specific order, and they additionally will be given later. \( \Delta T \) is a satisfactory reaction time entrance determined in firewall clients QoS prerequisite.

The principle goal of the Assignment (3) is to lessen the assets provisioning expense of proposed cloud in the firewall. Conditions (4) and (5) are all together so that will be accumulated in arranging VM examples of every firewall in the assault and non-assault period. QoS prerequisite are the restriction to meet the appearance rate of every firewall to be not as much as the repair rate to
Decentralization for Securing Data with Cloud Firewall Framework to Increase QoS

remain in the arrangement of consistent state. The short figuring is to figure the bundle entry rate to each of the firewall is in respect to the quantity of servers is incorporated into the group. The mean parcel entry rate to the firewall for group mnj and mak is given,

\[ \lambda_j^n = \frac{\chi^n m_j^n}{M} \]

(6)

\[ \lambda_k^n = \frac{\chi^n m_k^n}{M} \]

(7)

3.2 Service Rate Modeling

Service rate modeling is assumed is to give the exponential distribution. Govern control must be given into id in the organization in the cloud firewall. In run based firewall, there is part of guidelines in the database. All solicitations will be prepared organized run by manage until a match is found. Remaining access are dropped or passed. In Figure 2 some cases we have no successive information about control coordinating, so n rules share the equivalent likelihood coordinating. The likelihood of geometric dissemination

\[ \Pr[Y = i] = \begin{cases} (1 - p)^{i-1}p & 0 < i < N \\ (1 - p)^N & i = N \end{cases} \]

For virtual machine instance the service rate is, Total n rules are having only same knowledge,

\[ \tilde{t} = \frac{T(1 - q^N)}{p} \]

\[ i = \frac{mp}{T(1 - q^N)} \]

\[ \mu = m\sqrt{t} \]

Service rate for firewall is depends on parameters and number of computing cores in virtual machine. These are relevant to firewall settings.

4. Analytical Model

In this part we are explaining the execution model of the cloud firewall. We give full analysis on this system.

4.1 Markov Chain

Initially we declare some variables to our process. \{an\} describe the random variable at discrete time. Then we give the limit to that random variable. \[ \tilde{a} = \lim_{n \to \infty} a \] Denotes means value of a. The Poisson distribution of the service request arrival time for the cloud is,

\[ \Pr[X = k] = \frac{\lambda^k e^{-\lambda}}{k!}, \quad k = 0, 1, \ldots \]

Probability k in a given time interval, the mean rate is \[ \lambda \]. The request of displaying the examination conceivable and down to earth, we make one sensible supposition as broadly connected in cloud introduction broke down.

The administration times are solicitations to assume their self-ruling is indistinguishably separated\[14\] the irregular factors is sought after a geometric circulation as characterized in the last subsection with mean administration time t. Benefit solicitations are given by first-start things out served (FCFS) queue14 direction. As indicated by number of figuring centers, VM examples initiated for facilitating the cloud firewall administration displayed a M/Geo/1 lining framework. A M/Geo/1 system of lining might be taken as a semi-Markov process, is examined
by the implanted Markov chain strategy. The essential thought of this procedure is that we need to choose Markov focuses were the condition of the framework is anticipated. In the proposed work the arrangement of takeoff moments from administration as the minutes at which we demonstrate the quantity of courses in framework.

Let us assume $q_{n+1}$ and $q_n$ symbolize the number of requests absent after leaving of the $n$th and $(n + 1)$th requests from examine, respectively, while $v_{n+1}$ stands for the number of requests arriving during the service of the $(n+1)$th request. So we compute,

$$q_{n+1} = \begin{cases} q_n - 1 + v_{n+1} & q_n > 0 \\ v_{n+1} & q_n = 0 \end{cases}$$

We have selected the exit directs of Markov points, it is clear that $q_{n+1} < q_n - 1$ is impossible; on the other hand, $q_{n+1} > q_n - 1$ is possible to all values are arrivals of $v_{n+1}$. To believe two cases with view to $q_n$. Whether the $n$th request leaves last an empty system (i.e., $q_n = 0$) or not directs to a slight difference in the $v_{n+1}$. So, we compute $p_{ij}$ is

$$p_{ij} = \begin{cases} 0 & j < i - 1 \\ P(\bar{V} = j - i) & j \geq i - 1 \& i = 0 \\ P(\bar{V} = j - i + 1) & j \geq i - 1 \& i > 0 \end{cases}$$

The state transition probability is,

When request has to wait,

$$P_Q = P_{\text{Queuing}} = \frac{(mp)^m}{m!(1-p)}P_0$$

When expected number of waiting in queue is,

$$N_Q = \frac{t^2 \rho}{2t^2 (1-\rho)}P_Q$$

So, totally mean waiting time is, Response time is,

$$\bar{\omega} = \frac{N_Q}{\lambda}$$

$$\bar{r} = \bar{\omega} + \frac{N_Q}{\lambda}$$

5. Performance Evaluation

We will examine our analytical model for our proposed system. And tradeoff between QoS and virtualization cost are explained.

5.1 Validation of Analytical Model

The virtual machine's service rate is explained in above things. Small, medium, large, extra large are the various types in service rate calculation. Instance configuration and instance price, rate are explained in Table 1.

| Instance Type | Instance Configuration | Instance Price | Service Rate |
|---------------|------------------------|----------------|--------------|
| SMALL         | 1 ECU, 1.7 GB RAM, 160GB DISK | $0.080          | 58           |
| MEDIUM        | 2 ECU, 3.75 GB RAM, 410GB DISK | $0.160          | 117          |
| LARGE         | 4 ECU, 7.5 GB RAM, 850GB DISK | $0.320          | 234          |
| EXTRA LARGE  | 8 ECU, 15 GB RAM, 1690GB DISK | $0.640          | 468          |

And the comparison between M/M/1 and M/Geo/1 is,
8. Future Work

We suggested by improving our cloud firewall to catch application level personalized details and at the same time to keep it cost effective. Our concentration is fully on the above two concepts.

9. References

1. Armbrust M, Griffith R, Katz R, Lee G. A view of cloud computing, in X.kio, Firewall policy change-impact analysis. ACM Transactions Security on Net Technology (TOIT). 2012; 11(6):1–15.
2. Kumar A, Sathasivam C, Periyasamy P. Virtual machine placement in cloud computing. Indian Journal of Science and Technology. 2016 Aug; 9(29):1–5.
3. Diallo L, Hashim AHA, Olanrewaju RF, Islam S, Zarir AA. Two objectives big data task scheduling using swarm intelligence in cloud computing. Indian Journal of Science and Technology. 2016 Jul; 9(28):1–10.
4. Liu AX. Firewall policy change-impact analysis. ACM Transactions on Internet Technology (TOIT). 2012; 11(4):1–15.
5. Zhu J, Jiang Z, Xiao Z. Twinkle: A fast resource provisioning mechanism for internet services. INFOCOM, Proceedings IEEE; China. 2011. p. 802–10.
6. Tahir Z, Jamil M, Liaqat SA, Mubarak L, Tahir W, Gilani SO. State space system modeling of a quad copter UAV. Indian Journal of Science and Technology. 2016 Jul; 9(27):1–5.
7. Fatima SN, Begam SJ, Muneera NS. Reverse auction to trade unused cloud computing resources. Indian Journal of Science and Technology. 2016 Aug; 9(30):1–7.
8. Jain R, Kop F. The art of computer system performance analysis techniques for experimental design, measurement, simulation and modeling. New York: John Willey; 1991. p. 720.
9. Hokstad P, Yum Y. Approximations for the m/g/m queue. Operations Research. 1978; 26(3):510–23.
10. Moore D, Brown G, Mop M, Savage S. Inferring internet denial-of-service attack activity. ACM Transactions on Computer Systems (TOCS). 2006; 24(2):115–39.
11. Hwang RH, Chen YR, Lee CN. Cost optimization of elasticity cloud resource subscription policy. IEEE Transactions on Services Computing. 2014; 7(4):561–74.
12. Li K, Cao J, Zimaya A. Optimal multi-server configuration in profit maximization in cloud computing. IEEE Transactions on Parallel Distributed Systems. 2012; 24(6):1087–96.
13. Sharma U, Shaikh A. A cost-aware full elasticity provisioning system for the cloud. IEEE 31st International Conference on Distributed Computing Systems (ICDCS); USA. 2011. p. 559–70.
14. Kleinrock L. Zip Theory, Queueing systems. Wiley Inter Science; 1975.