Journal of Theoretical and Applied Information Technology
31st December 2017. Vol.95. No 24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

COLLABORATIVE DETECTION AND FILTERING TECHNIQUES AGAINST DENIAL OF SERVICE ATTACKS IN CLOUD COMPUTING

[1]IMAN EL MIR, [1]ABDELKRIM HAQIQ, [2]DONG SEONG KIM

[1]Computer, Networks, Mobility and Modeling laboratory, Hassan 1st Univ, Settat, Morocco

[2]Department of Computer Science and Software Engineering, University of Canterbury, New Zealand
E-mail: [1]{iman.08.elmir, ahaqiq}@gmail.com, [2]dongseong.kim@canterbury.ac.nz

ABSTRACT

Nowadays, cloud computing technology is experiencing a fastest growing in terms services demand and number of cloud clients which make the business organizations against a critical issue must be addressed "How to Secure Cloud Data Center (CDC)". As result, this major challenge has attracted the attention of several research works. The attacker is looking for unavailability of service, dysfunctioning of resources and maximization of financial loss costs. There are many types of attack such as Denial of service (DoS) and Distributed Denial of Service (DDoS) where the key objective for the attacker is to cause an overloading of the system network. They seek to send through a victim server a huge size of data as flooding packets so as to block and prevent the users to be served. This paper introduced a defending system for DoS attack mitigation in CDC environment. Generally, it discussed the different techniques of DoS attacks and its countermeasures as well proactive filtering and detection mechanisms. Consequently, to validate our proposed solution, we have implemented our analytical model in Discrete Event Simulator. The proposed mathematical model considers many performance parameters including response time, throughput, drop rate, resource computing utilization, and mean waiting time in the system, mean number of legitimate clients in the system when varying the attack arrival rate. Indeed, we have estimated the incurred cost from the attack. Implementing performance analysis using queueing theory and simulation experiments, the proposed solution would improve the flexibility and accuracy of DoS attack prevention, and would obviously make the cloud computing environment more secured.

Keywords: *Queueing Theory, Cloud Computing, Security, Performance Modeling, Dos Attacks.*

1. INTRODUCTION

Cloud computing has emerged as a potential segment of IT which characterized by its dynamic scalability and virtualization of computing resources to be delivered as services over the Internet. However, flexibility, high availability, 'pay-per-use' for cost savings, and uncomplicated scalability are the essential benefits of cloud computing. Cloud computing has been identified by Gartner as the prime of the ten top strategic technologies for a considerable effect on organizations for few years ago [1]. A cloud computing infrastructure delivers multiple services through a data center, which can be accessed from a web browser anywhere in the world [2]. It allocates dynamically a big number of computing resources in order to run applications so that the legitimate users are served. Due to its elasticity, cloud providers are designed to provide storage, networks, servers, development platforms, and applications as computing resources to the cloud clients on the basis of their demand and their form of payment [3]. As result of this strong demand, the service availability and cloud security are under a big challenge and issues such as SYN flooding attack, DoS and DDoS attacks. Besides, the outstanding question to be answered is how to mitigate the impact of DoS attacks in cloud environments? The attacker launches a DoS attack by sending a malicious flow of packets over the network that blocks and prevent the communication of legitimate users.

A denial of service attack is to paralyze an online service by sending a huge stream of packets through a single host to a target victim machine performing the service. Hence, the attack traffic consumes completely the network bandwidth so that the normal traffic will be dropped and rejected. The DDoS attacks flood the target machine with malicious packets from multiple distributed sources

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

which lead to bandwidth depletion and the unavailability of the service to the legitimate clients [4]. DDoS attack is defined as one of the offensive attacks which leads to serious effect on cloud servers and presents the critical threat among the list of cloud security threat pronounced by Cloud Security Alliance (CSA) for cloud computing infrastructures [5]. The attack packets generally use the TCP protocol. However, applying its three-way handshake, TCP based DDoS attacks, makes half-open connections on the target server and sends a SYN flooding packets in order to cripple the server resources and block all new ongoing client requests [6].

Generally, HTTP DoS attacks attempt flooding web applications and making user access denied. The services are disrupted and blocked by establishing an invalid connection; creating SQL queries with resource utilization intensive to block the application database. However, the system overload on the flooded services is caused by the saturation of the network bandwidth. By exploiting the IP address, the attacker executes a flooding attack so as to make the service fully unavailable [7]. Therefore, there have been increasing interests on countermeasures and defense mechanisms in terms of detection, prevention and filtering techniques against DoS and DDoS attacks. The cloud computing security grows as a complex research area which involves multiple dimensions depending on problem scope. In this paper, we defined a defense system containing three sub-models for attack mitigation in the cloud data center environment. The first sub-model is designed for filtering and detection of DoS attack. The second sub-model is the load balancing server for dispatching the client requests on each physical machine and the last sub-model represents data center where on each physical machine several virtual machines are running for data processing.

The main contributions of this work can be summarized as follow:

- For securing the cloud environment from DoS attack, a collaborative filtering and detection mechanisms were presented and described.
- The proposed solution was modeled using queueing theory; it considers defense queuing model, scheduling model and execution queueing model.
- An analytical model for the proposed mechanism is presented, and mathematical equations are derived for performance parameters considering two scenarios; the first one is without mitigation (attack) and the second one is with mitigation technique.
- Numerical results are given to show how this filtering and detection mechanism positively impacts the security of system and its performance metrics.

In this paper, we evaluate the impact of DoS attack on system performance parameters. We present a stochastic model for integrated detection and filtering mechanisms against DoS attacks. We provide greater details for our proposed solution. As well we carry out more results and analysis to discuss the effectiveness of the proposed model considering two different scenarios "Without mitigation (attack)" and "With mitigation". We present the analytical and simulation results of multiple parameters to analyze the attack impact on security and QoS of CDC. In addition, we estimate the system cost resulting from the attack.

The rest of this paper is organized as follows. The Section 2 presents the related work. Different forms of DoS attack are discussed and defending security tools are described in section 3. The proposed stochastic queueing model for the full proposed system is presented in section 4. Section 5 presents numerical analysis. Finally, section 6 is devoted to the conclusion and future work.

2. RELATED WORK

The whole network and cloud infrastructures are threatened by diverse attack types such as DoS and DDoS attacks. These attacks cause massive losses including the service downtime and the unavailability of resources and services delivered by Cloud providers [8]. The DoS attack is a particular case of DDoS attack. The DoS attack can be launched by a single host while in DDoS attack, the victim machine is attacked by multiple attack sources. Many research works have been conducted for Dos attack prevention and network security protection [9]. There have been various mechanisms and techniques of detection and attack filtering proposed in the literature [10], [11]. The aim is to predict the attacker's behavior and to analyze the normal from malicious traffics. Anomaly based detection or signature based detection are proactive or reactive mechanisms to scan the incoming traffic and to filter the attacks which can be propagated in the network in order to limit the networking losses. Cloud computing is designed to provide the availability of computing resources and servers for response to user demands. However, the cloud service models delivered according to a pay-per-use

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

manner of network resources open the door to multiple attacks to occur. Moreover, to capture the attacker's behavior and to estimate the impact of attacks, monitoring, detection, and filtering are enabled for attack traffic blocking, collection the network flows so as to offer a fine-grained analysis of attack sources [12].

Hussain *et al.* [9] have presented a framework for DoS attacks classification. They used the header content to analyze the DoS attacks and they have suggested two approaches initial ramp-up transients and spectral analysis based on the attack packet stream information. Their proposed framework was validated and evaluated in term of automatizing the detection and response systems based on the number of attacks captured. The localization of DoS attacks is defined by identifying the sources of DoS attacks in the presence of IP spoofing. The well-known techniques are ingress and egress filtering [13] where all ongoing network traffic is filtered. The ingress filtering technique is deployed to guarantee that the ongoing packets are transferred from network sources by their correct IP addresses. This technique involves integrated routers for source IP address monitoring and dropping all incoming packets with incorrect IP address which not appeared in the list of IP addresses on which the router is connected. While the egress filtering is technique which controls the outbound network traffic in order to ensure that the spoofed packets cannot be outside to the internal networks. Other research works seek to perform the mechanisms to keep track of packets incoming over Internet where their source addresses are unknown.

The authors in [14] have proposed a DDoS attack detection technique using half interaction anomaly degree. To deal with the problems occurred by the current methods which increase the false positive rate and false negative rate, their proposed method extracts the features of DDoS attacks from malicious flows and provides rapidly the DDoS attack reconnaissance. In [15] the authors have proposed a DDoS attack mitigation based on queueing theory. They have suggested a mitigation mechanism to estimate the number of resources needed to beat the DDoS attack and they deployed their approach in a real-world data set experiments. In [16], the authors proposed EDoS-Shield as a novel mitigation technique against Economic Denial of Sustainability (EDoS) attack in Cloud Computing environment. Their aim is to check if the requests are sent from legitimate users or generated by bots. They have proposed an architecture of which they have defined a responsible node on the verification process and the update of the white and black lists. The legitimate requests since their IP addresses exist in the white list are forwarded directly to the cloud service destination. In contrast, the requests generated by the bots whose their IP addresses are on the black list will be blocked by a virtual firewall. Through a discrete simulation experiment, they have evaluated the system performance and discussed the obtained results which conclude that the proposed solution is efficient for EDoS mitigation.

In [17], the authors presented a potential Denial of Service (DoS) attack that seeks to compromise the security policy of a firewall especially its last matching rules. These rules are defined as the rules that are situated at the bottom of the ruleset of policy security of the firewall and that need more time so as to be processed by the firewall. They have suggested a probing technique to remotely locate the last-matching rules of a firewall. They have executed some test experiments to discuss the effectiveness of the proposed solution. They have evaluated the performance parameters for firewall including CPU utilization, throughput, packet loss, and latency to discuss the effect of launching a low-rate DoS attack on the performance of firewalls. Ficco *et al.* [18] have proposed a scalable intrusion detection solution in a federated cloud environment for cloud providers. Their solution is designed to facilitate monitoring the hosted applications by cloud providers. In addition, they have presented a framework which investigates several features and interfaces for development and deployment of security components for attack prevention. In the work [19], the authors have proposed a reliable model to filter the abnormal traffic by controlling in real time the quality of service performance in function of user's behavior through three principal phases monitoring, detection, and identification. They have suggested a method that improves the reliability of traffic filtration and predicts the normal from malicious traffic. Therefore, there are several research works in the literature that demonstrate that queuing models and Markov chains have been implemented as an efficient tool to model the system behavior at each time and to perform network performance evaluation and security analysis. For example, in [20] a digital model has been proposed which early identifies the attacks and marks in real time their sources. It generates warning alarms for identification of attacker who seeks to launch an attack. They have modeled their proposed solution using Markov chains and across simulation experiments, they demonstrated its effectiveness in term of distributed attacks detection when the network is under congestion and the user services are not completely denied. The previous researches [21], [22] have

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

incorporated the preventive and detective rules to find a trade-off between network performance and security based on queueing theory.

The trace back model of distributed attack in their initial phases offers more benefits including minimizing the bandwidth consumption by malicious users while keeping the continuity of the normal traffic sent from the same sources. In [23], the authors have presented an analytical model to evaluate the performance of EDoS-Shield based on queueing theory modeling. They have defined multiple scenarios for EDoS-shielding analysis so as to mitigate the economic denial of sustainability attack which threatened the cloud computing services deployed. They have also calculated the key performance parameters which CPU utilization, system throughput and response time, to discuss the efficiency of the proposed solution. In [24], [25], the authors introduced a novel technique based on client puzzles as an effective tool for denial of service attacks mitigation and involves heavily overhead to zombies. They suggested a puzzle distribution mechanism where the aim is to establish access communication channel to clients. The authors in [26] have presented the SYN flooding attack as the best known DoS attack and proposed a simple queuing model. Hence they have discussed the different DDoS attacks and presented the existing solutions of defense. Otherwise, in [27] the authors have evaluated the packet delay jitter and loss probability as two security metrics according a two queuing models for DoS attacks. The finality of their research work is to improve the performance using the mitigation techniques based on packets filtering. In addition, the authors of the work [28] have analytically analyzed the impact of flooding attacks. They have presented a detection mechanism so as to study three key performance metrics which request arrival rate, queue-growth rate and response time.

3. SYSTEM DESCRIPTION

In this section, we consider that the DoS attack has two main techniques one to block the legitimate users from implementing the computing service i.e. the on-line services are unavailable and the other is to produce collisions and harm in the services. To mitigate the DoS attack in cloud computing, we proposed a defending system that consists of three components the Packet Filter (PF), the Bandwidth Analyzer (BA) and the Packet Analyzer (PA). These network security analysis tools are powerful to examine the traffic details, to detect the legitimate from malicious flows and to monitor the behavior of the attacker. Based on predefined rules, the PF filters and examines the incoming traffic. It checks the IP address of the packet so as to determine the traffic source if it is normal or malicious and then take decision about its processing to BA or to PA. The BA analyzes the packet size compared with the predefined threshold. If there is any bandwidth depletion attack then the packet is sent to PA else it will be processed by the Load Balancing (LB). The DoS attack creates a flooding attack by duplicating the requests using TCP or UDP packets. The attacker's aim is to use the bandwidth of legitimate clients and prevent them from being served which involves the bandwidth depletion attack. The PA inspects the traffic, controls the privilege and the priority of the incoming packet. The attacker can launch a DoS attack using a false address and causes an overloading of network resources. The packet analyzer is responsible on dropping and blocking the packet if it's abnormal or sending it to the load balancing for data processing if it is normal request.

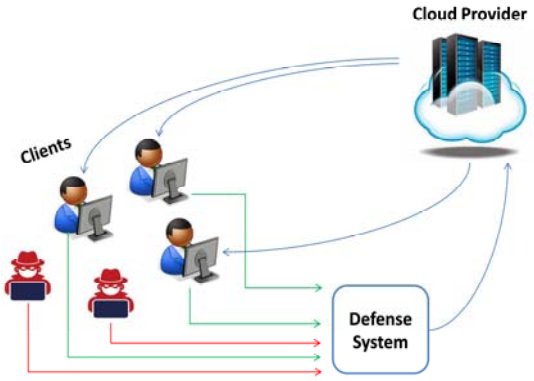

Figure 1: Description of the system architecture

The proposed architecture (see Figure 1) consists on many legitimate users and DoS attackers (i.e. two types of traffic normal and malicious traffic), defending system which is described above and summarized in the Flowchart depicted in Figure 2 and implemented in the algorithm below, the LB for dispatching and routing only the normal traffic to the specific physical server for data processing and the data center which consists on multiple Physical Servers (PS) hosting several Virtual Machines (VMs). In other hand, we focused on IaaS which provides virtualized computing resources over the Internet such as Amazon Web Services (AWS), Microsoft Azure, and Google Compute Engine (GCE) while all services delivered by the Cloud service provider are implemented across the VMs.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Algorithm: Filtering and detection Countermeasures against DoS attack

```
Input:
 Rq: new arrival packet
 Th: The threshold of packet size
 L: The packet size
 V: The list of IP address range
 PA: Packet Analyzer
 BA: Bandwidth Analyzer
 PF: Packet Filter
 IF IP_Req ∈ V
      The PF sends the Rq to BA
      IF L ≤ Th Then
           Rq is routed to the LB
        LB patches it to the Physical server for data processing
      Else L > th Then
          Rq is routed to PA
              IF The Rq is legitimate Then
                  The Rq is transferred to LB
              endIF
              IF The Rq is malicious attack Then
                  The Rq is dropped and the connection is blocked
              EndIF
        EndIF
      Else
          The PF sends the Rq to PA
              IF The Rq is legitimate Then
                  The Rq is transferred to LB
              endIF
              IF The Rq is malicious attack Then
                  The Rq is dropped and the connection is blocked
              endIF
      endIF
```

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

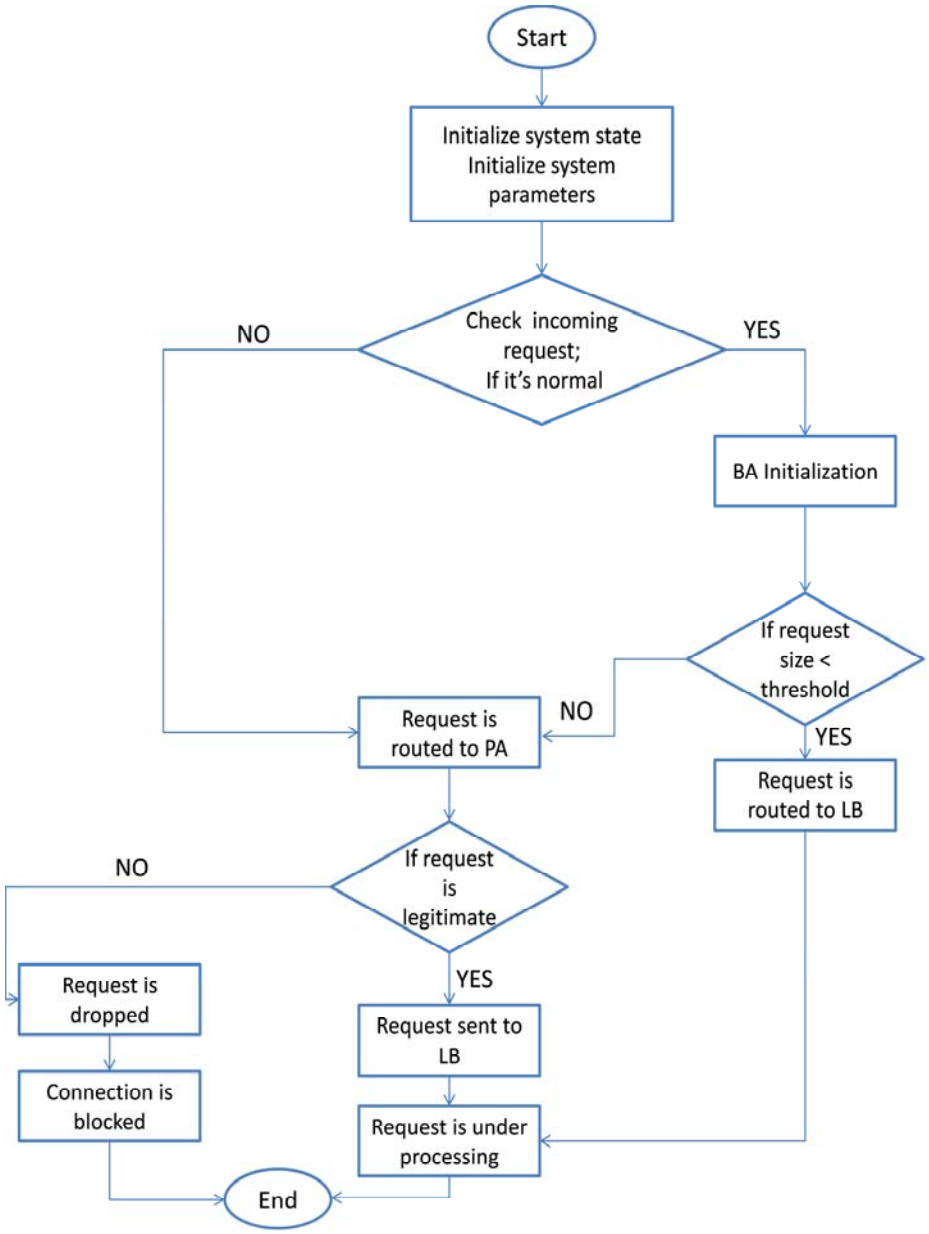

Figure 2: System architecture Flowchart

4. ANALYTICAL MODELING OF THE STUDIED STRUCTURE

We modeled in Figure 3, the preventing DoS attacks in CDC as three stages queuing system. In the first time, The DoS attack arrives with rate λ_a , and the legitimate traffic with rate of λ_c per second. The DoS attack behavior has been formulated as Poisson process in many research works [29, 30]. So, The DoS attack behavior has been modeled as a Poisson process so as the normal connection arrival. The two flows are considered to be independent. Consequently, the ongoing traffic including the both normal and malicious flows is Poisson process with rate $\lambda_T = \lambda_a + \lambda_c$.

The packet Filter receives the both normal and abnormal traffic with rate λ_T and checks the IP address of the incoming packet. We have two possible cases: The BA accepts the packet arrival with rate λ_c and the PA accepts the packet arrival with rate λ_a . The three components of defending system are modeled as M/M/1 queueing system (i.e.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Q_{FA}, Q_{BA} and Q_{PA}) where requests arrive according to Poisson process, and are probably routed from one queue to another queue [31]. The service time in each queue obeys an exponential distribution. In each queue, the service time of the client requests is drawn independent of the service times in other queues. After, the packet analyzed by BA it will be sent to LB with p probability and it was sent to Q_{PA} with $(1-p)$ probability. Hence, the PA receives the packet from PF with rate λ_a and from the BA with rate $(1-p)\lambda_c$ and after checking the priority and the privilege of the packet; it sends only the normal traffic to the LB and drops the abnormal and malicious traffic. In addition, it updates the database by storing all new malicious activities detected. Furthermore, the LB receives the legitimate traffic coming from BA with $p\lambda_c$ and from PA with $(1-q)(\lambda_a+(1-p)\lambda_c)$ and dispatches them to N Physical Servers. The LB routes the request clients with the same probability $\frac{1}{N}$ to each physical server for data processing.

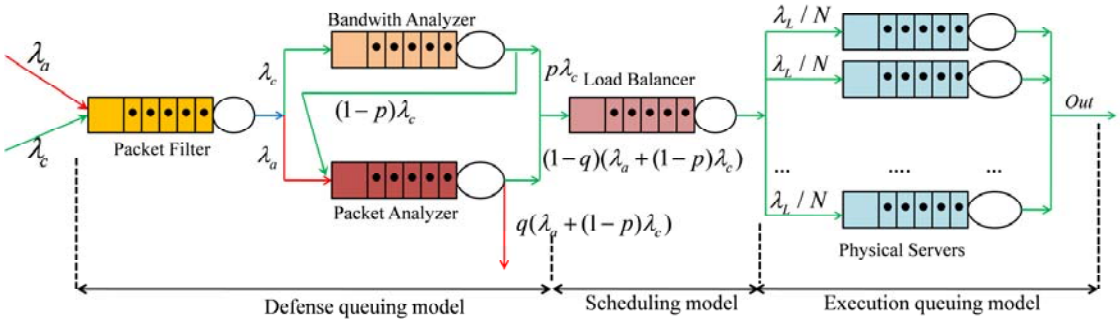

Figure 3: Queueing Model of the proposed system.

4.1 Defense Module Queueing Model

The Packet Filter, Bandwidth Analyzer and the Packet Analyzer are modeled as M/M/1 queue. We propose that all connections arrive with λ_T rate to the PF and are served with rate μ_{PF}. In other words, $\lambda_c+\lambda_a$ is the average arrival rate of normal jobs and malicious packets to Packet Filter Q_{PF}. In addition, we propose that the normal packets arrive with λ_c rate to the BA and are served with rate μ_{BA} and, the normal packets arrive with $(1-p)\lambda_c+\lambda_a$ rate to PA and are served with rate μ_{PA}.

The Average traffic load offered at the Packet Filter queue Q_{PF}, the Bandwidth Analyzer queue Q_{BA} and at the Packet Analyzer queue Q_{PA}: ρ_{PF}, ρ_{BA} and ρ_{PA} respectively are given by :

$$\rho_{PF}=\frac{\lambda_T}{\mu_{PF}};\ \rho_{BA}=\frac{\lambda_c}{\mu_{BA}};\ \rho_{PA}=\frac{\lambda_a+(1-p)\lambda_c}{\mu_{PA}} \quad (1)$$

Mean number of requests $\overline{N_{PF}}$ in Q_{PF}, Mean number of requests $\overline{N_{BA}}$ in Q_{BA} and Mean number of requests $\overline{N_{PA}}$ in Q_{PA} are:

$$\overline{N_{PF}}=\frac{\rho_{PF}}{1-\rho_{PF}};\ \overline{N_{BA}}=\frac{\rho_{BA}}{1-\rho_{BA}};\ \overline{N_{PA}}=\frac{\rho_{PA}}{1-\rho_{PA}} \quad (2)$$

Mean sojourn time $\overline{T_{PF}}$ in Q_{PF}, Mean sojourn time $\overline{T_{BA}}$ in Q_{BA} and Mean sojourn time $\overline{T_{PA}}$ in Q_{PA} are given by :

$$\overline{T_{PF}}=\frac{\overline{N_{PF}}}{\lambda_T};\ \overline{T_{BA}}=\frac{\overline{N_{BA}}}{\lambda_c};\ \overline{T_{PA}}=\frac{\overline{N_{PA}}}{\lambda_a+(1-p)\lambda_c} \quad (3)$$

The Mean number of client requests $E(N)$ in the defending system:

$$E(N)=\frac{\rho_{PF}}{1-\rho_{PF}}+\frac{\rho_{BA}}{1-\rho_{BA}}+\frac{\rho_{PA}}{1-\rho_{PA}} \quad (4)$$

The Mean Sojourn Time W : The mean total time spent in the defending system by a client request before being sent to the LB.

$$W=\frac{\overline{N_{PF}}}{\lambda_{PF}}+\frac{\overline{N_{BA}}}{\lambda_{BA}}+\frac{\overline{N_{PA}}}{\lambda_{PA}} \quad (5)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.2 Load Balancing Queueing Model

The load balancing server provides a scheduling queue to accept all client requests from defense module and after forwards them to each physical server running in the cloud based defined strategies and policies. Based on scheduling algorithms, LB optimizes the data center performance. In this paper, the load balancing server is presented as M/M/1/C queue. Where the LB forwards the user's requests to one of the PS_i; $i = 1,...,N$. The inter-arrival times between successive arrival legitimate requests are independent and exponentially distributed with rate $\frac{1}{\lambda_L}$. We assume that the service time of the LB server queue is exponentially distributed with mean service time $\frac{1}{\mu_{LB}}$. The maximum number of jobs accepted is C. Hence when a new request arrives it will be accepted if the length of queue is less than C otherwise it will be rejected. Solving the balance equations and the conservation equation, the steady state probabilities $\pi_{k'}$ (k' is the number of requests in the system) are calculated as follows:

$$\pi_{k'} = \frac{1-\frac{\lambda_L}{\mu_{LB}}}{1-(\frac{\lambda_L}{\mu_{LB}})(C+1)}(\frac{\lambda_L}{\mu_{LB}})^{k'} \quad (6)$$

4.3 Data center Queueing Model

We assume that on each physical server k virtual machines are running. However each physical server is presented as M/M/k/K queueing system. Each PS can process at maximum K client requests. We suggest that all PSs are homogeneous service. Where the service times in each PS is exponentially distributed with $\frac{1}{\mu}$ mean service time. Considering the Continuous Time Markov Chain (CTMC) for the new arrival job in PS_i, solving the balance equations and the conservation equation, the steady state probabilities $\pi_i(n)$ for n requests in the ith PS in the data center are calculated as follows:

$$\pi_i(n) = \begin{cases} \frac{\pi_0(\lambda)^n}{n!\mu^n}, & \forall n < k \\ \frac{\pi_0(\lambda)^n}{k!k^{n-k}\mu^n}, & \forall n \geq k \end{cases} \quad (7)$$

where $\lambda = \frac{\lambda_L}{N}$, n is the number of the jobs in PS_i and π_0 is equal to :

$$\pi_0 = (1+\frac{(\frac{\lambda}{\mu})^k(1-\frac{\lambda}{k\mu}^{K+1-k})}{k!(1-\frac{\lambda}{k\mu})}+\sum_{i=1}^{k-1}\frac{(\frac{\lambda}{\mu})^i}{i!})^{-1} \quad (8)$$

The effective requests arrival rates to the service λ_E is formulated as:

$$\lambda_E = (\frac{\lambda_L}{N})(1-\pi_i(K)) \quad (9)$$

The load consumed by the normal requests U is defined as:

$$U = \frac{\lambda}{k\mu} \quad (10)$$

When the DoS attack was propagated in the system network, it causes several losses and business costs. We can presented two important measurements for system cost formulation ; the cost of computing resources and cost of waiting time by clients in the system. We formulated the cost of waiting time in function of request arrival rate to service , the mean waiting time T and the cost occurred when the requests are in waiting state C_{WT}. While the cost of computing resources is calculated based on number of VMs Nbr_{VM} in the system and the cost due to bandwidth utilization by a single VM C_{BW}. Then, the system cost is as follows :

$$Cost_S = T*[(\lambda_{LB}*C_{WT})+(Nbr_{VM}*C_{BW})] \quad (11)$$

5. SIMULATION MODEL

In the simulation model, we have carried out two different scenarios. In the first scenario, we have proposed that the CDC environment was not protected. There is any defense system to mitigate DoS attack risk. In the second scenario, we have implemented the proposed defense module described above so as to reduce the DoS attack impact and to enhance the security of the cloud computing network.

Discrete Event Simulator: To analyze the performance of cloud computing, there are several Cloud simulators such as CloudSim [32], iCanCloud [33] and JMT [34]. We have selected JMT as simulator tool due to its capability to capture with more precision the internal behavior of the cloud computing environment. JMT is designed to evaluate

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the performance of the proposed mathematical model. It's defined as a suite of open source toolkits performed for evaluation and analysis of system performance using the queueing theory [35]. Among of the tools offered by JMT, there are solutions of queuing networks with analytical algorithms (JMVA), simulation of general purpose queuing models (JSIM).

Experimental Setup: The collaborative filtering and detection techniques have been evaluated and validated according cloud service performance. We have suggested a defense module in the proposed architecture as mitigation technique to prevent the DoS attack. To conduct these simulation experiments and capture the attacker's behavior, we have used JMT as simulator network. In our simulation, we have respected the queuing model depicted in Figure **3** with two different traffics (i.e. legitimate and abnormal traffic). The CDC contains 10 *PSs* and 30 VMs. The arrival rate of legitimate traffic is fixed on 1000 requests per second while the arrival rate of attack traffic is varied from 1000 to 3000 requests per second. We have measured six main performance parameters throughput, response time, drop rate, computing resources utilization, mean number of legitimate clients and mean waiting time so as to evaluate the impact of DoS attacks in cloud service. Moreover, the system cost is evaluated under the two scenarios.

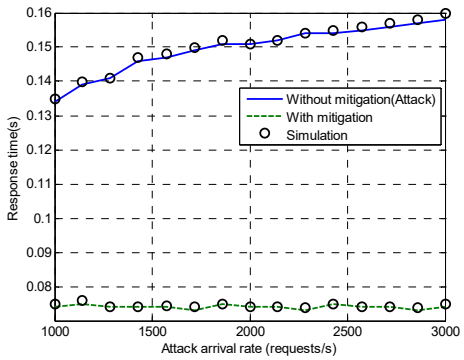

Figure 4: Response time in relation to Attack Arrival rate.

The Figure 4 illustrates the response time when the arrival rate of attack is varied regarding two cases: with mitigation case and without mitigation. As expected, when the attack arrival rate increases and with applying the mitigation techniques, the response time still constant and less than 80*ms*. We can justify the high level of response time in the other scenario with the attack traffic load and the limitation of the number of normal requests in the queue. Because, the attacker keeps the server busy then the normal client requests spent more in waiting service. But, when we have protected the cloud service through the proposed defense system which blocks the malicious requests, we see that the attacks don't have any influence on the response time and the clients have been properly served.

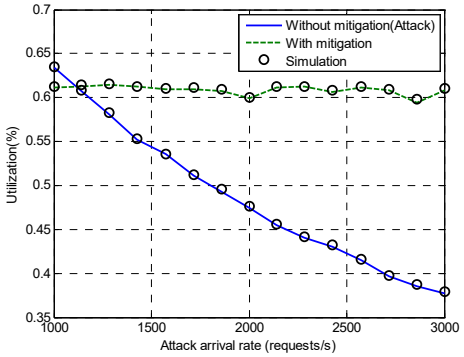

Figure 5: Utilization incurred in relation to attack arrival rate.

The Figure 5 presents the resource computing utilization by the legitimate requests in regards to the variation of attack arrival rate. It is clear that by using mitigation techniques, the resource usage in the PS is fixed at 60%. But in the presence of attack, the attacks prevent the normal clients from using the resources computing.

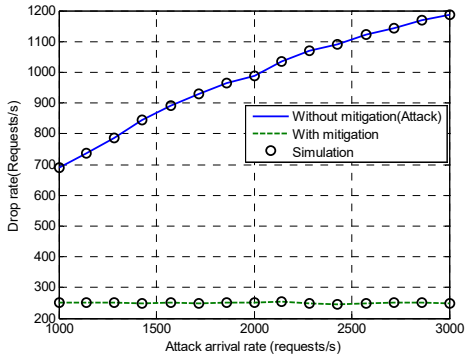

Figure 6: Drop rate versus Attack arrival rate.

The Figure 6 shows the drop rate of legitimate requests as a function of attack arrival rate. We remark that in the presence of attacks, the drop rate of normal requests increases due to the overload system by the attackers. However, in defense scenario, we observe that the drop rate is low and it is fixed on 250 requests per second (25% of legitimate requests).

The Figure 7 exhibits the impact of attack arrival rate on the throughput parameter. The impact of attacks on the throughput becomes more significant

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

for the large values of attack arrival rate. So in the attack scenario, as the attack rate increases the throughput decreases. Moreover, when the mitigation mechanisms are applied, the throughput reaches 1700 requests per second and then the cloud service is well protected.

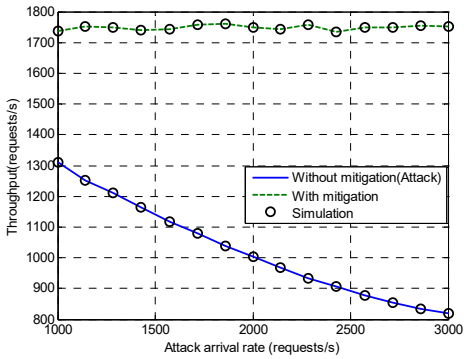

Figure 7: Throughput of legitimate requests versus attack arrival rate.

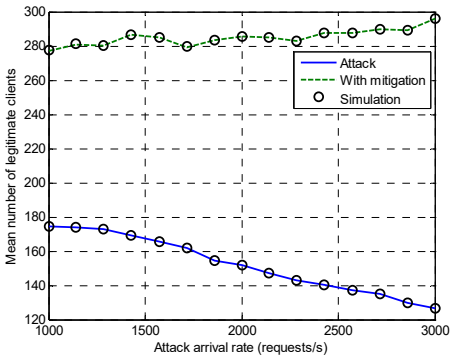

Figure 8: Mean number of legitimate clients versus attack arrival rate.

In Figure 8, we remark that as the attack arrival rate increases the number of the legitimate clients becomes more reduced comparing with the case when we apply the mitigation technique, we can prevent the attacks to overload the system and block the normal users to access to system.

The Figure 9 demonstrates the impact of attack arrival rate on mean waiting time by the legitimate requests in the system queue. It's clear that as the attack arrival rate increases as the mean waiting time increases. But we can reduce its impacts when triggering the mitigation technique and as result, the mean waiting time parameter is reduced.

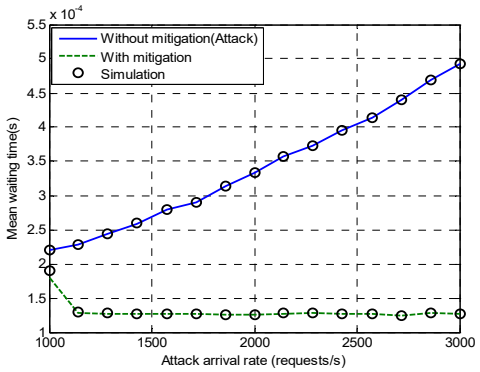

Figure 9: Mean waiting time(s) in relation to Attack Arrival rate.

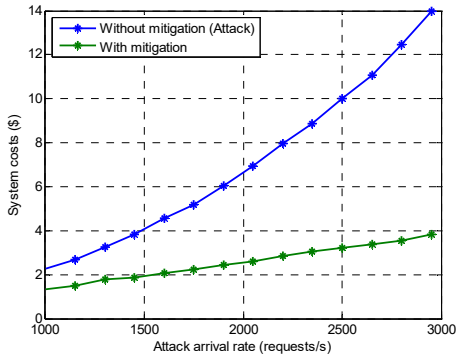

Figure 10: Incurred cost versus Attack Arrival rate.

For the system cost analysis, Figure 10 shows that as the attack arrival rate increases the system cost increases. In the absence of defense, we remark that the cost becomes more important comparing with the mitigation scenario; we see that the cost is minimized and is lower than 4 dollars when the attack arrival rate tends to 3000 requests per second. The values of the cost parameters used to formulate the system cost are based on empirical measurements from prior work [36, 37] and we are based on Amazon EC2 as an example. The prices of Amazon EC2 Pricing for Standard On-Demand Instances are defined in Table 1 [38]. In our numerical results, we consider the default setting of a small Windows instance.

Table 1: Amazon EC2 Pricing for Standard On-Demand Instances

Instance Type	Windows (per hour)	Linux (per hour)
Small (Default)	$0.115	$0.060
Medium	$0.230	$0.120
Large	$0.460	$0.240
Extra Large	$0.920	$0.480

To show the agreements between analytical results and those incurred from the simulation experiments,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

we have compared the obtained results by the two techniques. Hence, this clearly validates our analytical model and we have drew below the tables Table 2 and Table 3 to compare the analytical and the simulation results of the proposed model implementing in JMT tool.

	Response Time (s)				*Drop rate (Req/s)*				*CPU Utilization (%)*			
	Analysis	**Simulation**			**Analysis**	**Simulation**			**Analysis**	**Simulation**		
	Avg	Avg	Min	Max	Avg	Avg	Min	Max	Avg	Avg	Min	Max
attack rate of 1000(Rq/s)	0.134	0.135	0.132	0.137	690.973	690.974	679.317	703.035	0.634	0.635	0.625	0.643
attack rate of 2000(Rq/s)	0.151	0.151	0.149	0.153	988.146	988.147	988.072	1007.987	0.474	0.476	0.466	0.482
attack rate of 3000(Rq/s)	0.158	0.155	0.161	0.137	1187.431	1187.432	1169.596	1205.818	0.377	0.379	0.371	0.383

	Throughput (Req/s)				*Mean number of legitimate clients*			
	Analysis	**Simulation**			**Analysis**	**Simulation**		
	Avg	Avg	Min	Max	Avg	Avg	Min	Max
attack rate of 1000(Rq/s)	1309.438	1309.440	1296.300	1322.845	174.720	174.721	169.835	179.604
attack rate of 2000(Rq/s)	1004.083	1004.084	985.312	1023.583	152.037	152.037	148.475	155.599
attack rate of 3000(Rq/s)	818.025	818.027	806.029	830.383	126.675	126.677	123.831	129.519

Table 2: Comparison of simulation results with analysis for 'without mitigation' scenario

	Response Time (s)				*Drop rate (Req/s)*				*CPU Utilization (%)*			
	Analysis	**Simulation**			**Analysis**	**Simulation**			**Analysis**	**Simulation**		
	Avg	Avg	Min	Max	Avg	Avg	Min	Max	Avg	Avg	Min	Max
attack rate of 1000(Rq/s)	0.074	0.075	0.072	0.076	252.360	252.361	245.791	259.290	0.611	0.612	0.600	0.622
attack rate of 2000(Rq/s)	0.074	0.074	0.0.072	0.075	251.456	251.457	246.006	257.154	0.599	0.6	0.585	0.612
attack rate of 3000(Rq/s)	0.074	0.074	0.072	0.076	249.048	249.049	244.393	253.884	0.608	0.610	0.594	0.622

	Throughput (Req/s)				*Mean number of legitimate clients*			
	Analysis	**Simulation**			**Analysis**	**Simulation**		
	Avg	Avg	Min	Max	Avg	Avg	Min	Max
attack rate of 1000(Rq/s)	1737.327	1737.329	1706.729	1769.043	277.3	277.5	270.4	284.3
attack rate of 2000(Rq/s)	1748.985	1748.985	1718.056	1781.048	285.4	285.6	280.3	290.6
attack rate of 3000(Rq/s)	1750.683	1750.684	1722.636	1779.658	295.8	296	303.2	288.4

Table 3: Comparison of simulation results with analysis for 'with mitigation' scenario

6. CONCLUSION AND FUTURE WORK

During the last decades, cloud computing technology has emerged as a primitive factor for IT industry revolution and it becomes more popular, this is explained by its economic benefits for the both cloud providers and customers. Consequently, the security of the cloud computing remains a major challenge. In other words, how to defeat the attacks as well as to protect the availability of these cloud services and its benefits? DDoS attack appeared as the most popular attack which is classified as potential cybercriminal strategy and DoS attack represents a particular case of DDoS attack. The attacker's goal is to prevent, block the cloud clients and to disturb the continuity and availability of cloud service. On the other hand, the cloud has its potential computing resources and mechanisms for protection and countermeasures against this critic type of attack. Motivated by this, we proposed a framework as a proactive strategy which combines the detection and filtering techniques to achieve a high level of security and good performance for quality of service. We used a queueing theory approach to model the proposed solution for DoS attack mitigation in a cloud environment. The mathematical evaluations of the QoS parameters of the system are derived while considering two different scenarios namely without mitigation scenario and with mitigation scenario. We have formulated mathematically the main performance metrics. Moreover, we proved the feasibility of our proposed model to estimate the system cost resulting from the attack in order to quantify the impact of attacks on cloud service. Using JMT simulator, we validated our analytical model and defended our proposed solution. As future work, we plan to allocate dynamically the filter servers depending on the number of the attack packets so as to mitigate the DDoS attack impact and to ensure a good quality of service for the legitimate users. Thereafter, we seek to implement our model in a real cloud environment.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFRENCES:

[1] J. Rivera, "Gartner identifies the top 10 strategic technology trends for 2014", Gartner, Inc. Retrieved at March, vol. 10, 2013, p. 2016.

[2] W. Voorsluys, J. Broberg, and R. Buyya, "Introduction to cloud computing", Cloud computing : Principles and paradigms, 2011, pp. 1-41.

[3] W. Huang, A. Ganjali, B. H. Kim, S. Oh, and D. Lie, "The state of public infrastructure-as-a-service cloud security", *ACM Computing Surveys (CSUR)*, vol. 47, no. 4, 2015, p. 68.

[4] E. Alomari, S. Manickam, B. Gupta, M. Anbar, R. M. Saad, and S. Alsaleem, "A survey of botnet-based ddos flooding attacks of application layer : Detection and mitigation approaches", in *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*. IGI Global, 2016, pp. 52–79.

[5] G. Somani, M. S. Gaur, D. Sanghi, and M. Conti, "Ddos attacks in cloud computing: collateral damage to non-targets", *Computer Networks*, vol. 109, 2016, pp. 157– 171.

[6] B. Xiao, W. Chen, and Y. He, "A novel approach to detecting ddos attacks at an early stage", *The Journal of Supercomputing*, vol. 36, no. 3, 2006, pp. 235–248.

[7] L. Schubert, K. Jeffery, and B. Neidecker-Lutz, "The future of cloud computing: Opportunities for European cloud computing beyond 2010", *Expert Group report, public version*, vol. 1, 2010.

[8] S. Tripathi, B. Gupta, A. Almomani, A. Mishra, and S. Veluru, "Hadoop based defense solution to handle distributed denial of service (ddos) attacks", *Journal of Information Security*, vol. 4, no. 03, p. 150, 2013.

[9] A. Hussain, J. Heidemann, and C. Papadopoulos, "A framework for classifying denial of service attacks", in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*. ACM, Germany, August 25 - 29, 2003, pp. 99–110.

[10] P. Negi, A. Mishra, and B. Gupta, "Enhanced cbf packet filtering method to detect ddos attack in cloud computing environment", *International Journal of Computer Science Issues*, vol. 10, no. 2, 2013, pp. 1694-0784.

[11] O. P. Badve, B. Gupta, S. Yamaguchi, and Z. Gou, "Ddos detection and filtering technique in cloud environment using garch model", in *Consumer Electronics (GCCE), 2015 IEEE 4th Global Conference on*. IEEE, Japan, October 27-30, 2015, pp. 584–586.

[12] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "Ddos attacks in cloud computing : issues, taxonomy, and future directions", *Computer Communications*, 2017.

[13] T. N. Thinh, C. Pham-Quoc, B. Nguyen-Hoang, T.- C. Tran-Thi, C. Do-Minh, Q. Nguyen-Bao, and N. Q. Tuan, "Fpga-based multiple ddos countermeasure mechanisms system using partial dynamic reconfiguration", *REV Journal on Electronics and Communications*, vol. 5, no. 3-4, 2016.

[14] J. Cheng, X. Tang, and J. Yin, "A change-point ddos attack detection method based on half interaction anomaly degree", *International Journal of Autonomous and Adaptive Communications Systems*, vol. 10, no. 1, 2017, pp. 38–54.

[15] S. Yu, Y. Tian, S. Guo, and D. O. Wu, "Can we beat ddos attacks in clouds ?", *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, 2014, pp. 2245–2254.

[16] M. H. Sqalli, F. Al-Haidari, and K. Salah, "Edosshield-a two-steps mitigation technique against edos attacks in cloud computing," in *Fourth IEEE International Conference on. Utility and Cloud Computing (UCC)*, Washington, DC, USA, December 05 - 08, 2011, pp. 49–56.

[17] K. Salah, K. Sattar, M. Sqalli, and E. Al-Shaer, "A potential low-rate dos attack against network firewalls", *Security and Communication Networks*, vol. 4, no. 2, 2011, pp. 136–146.

[18] M. Ficco, L. Tasquier, and R. Aversa, "Intrusion detection in federated clouds", *International Journal of Computational Science and Engineering*, vol. 13, no. 3, 2016, pp. 219–232.

[19] A. A. Ahmed, A. Jantan, and T.-C. Wan, "Filtration model for the detection of malicious traffic in largescale networks", *Computer Communications*, vol. 82, 2016, pp. 59–70.

[20] A. A. Ahmed, A. S. Sadiq, and M. F. Zolkipli, "Traceback model for identifying sources of distributed attacks in real time", *Security and*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Communication Networks, vol. 9, no. 13, 2016, pp. 2173–2185.

[21] D. I. ELMir, A. Haqiq, "Towards a stochastic model for integrated detection and filtering of dos attacks in cloud environments", in *2nd International Conference on Big Data, Cloud and Applications (BDCA'17)*. ACM, Tetuan, Morocco, 29-30 March 2017.

[22] El Mir, I., Haqiq, A., and Kim, D. S, "Performance Analysis and Security Based on Intrusion Detection and Prevention Systems in Cloud Data Centers", In *International Conference on Hybrid Intelligent Systems* ,Springer, Marrakech, Morocco, November 21–23, 2016, pp. 456-465.

[23] F. Al-Haidari, K. Salah, M. Sqalli, and S. Buhari, "Performance modeling and analysis of the edos-shield mitigation", *Arabian Journal for Science and Engineering*, vol. 42, no. 2, 2017, pp. 793–804.

[24] X. Wang and M. K. Reiter, "Mitigating bandwidth exhaustion attacks using congestion puzzles", in *Proceedings of the 11th ACM conference on Computer and communications security*. ACM, Washington, DC, USA, October 25 - 29, 2004, pp. 257–267.

[25] B. Waters, A. Juels, J. A. Halderman, and E. W. Felten, "New client puzzle outsourcing techniques for dos resistance", in *Proceedings of the 11th ACM conference on Computer and communications security*. ACM, Washington, DC, USA , october 25 - 29, 2004, pp. 246–256.

[26] R. K. Chang, "Defending against flooding-based distributed denial-of-service attacks: a tutorial", *IEEE communications magazine*, vol. 40, no. 10, 2002, pp. 42–51.

[27] M. Long, C.-H. Wu, and J. Y. Hung, "Denial of service attacks on network-based control systems: impact and mitigation," *IEEE Transactions on Industrial Informatics*, vol. 1, no. 2, pp. 85–96, 2005.

[28] S. Khan and I. Traore, "Queue-based analysis of dos attacks," in *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC*. IEEE, West Point, NY, USA, 2005, pp. 266–273.

[29] H. Liu, "A new form of dos attack in a cloud and its avoidance mechanism", in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*. ACM, Chicago, IL, USA, October 04 - 08, 2010, pp. 65–76.

[30] D. Boteanu, J. M. Fernandez, J. McHugh, and J. Mullins, "Queue management as a dos counter-measure?", in 10th International conference, *ISC*. Springer, Valparaiso, Chile, October 9-12, 2007, pp. 263–280.

[31] S. El Kafhali and K. Salah, "Stochastic modelling and analysis of cloud computing data center", in 20th Conference on Innovations in Clouds, Internet and Networks (ICIN'17), IEEE, Paris, France, March 7-9, 2017, pp. 122-126.

[32] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. De Rose, and R. Buyya, "Cloudsim : a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms", *Software : Practice and experience*, vol. 41, no. 1, 2011, pp. 23–50.

[33] A. Nunez, J. L. Vazquez-Poletti, A. C. Caminero, G. G. Castane, J. Carretero, and I. M. Llorente, "icancloud : A flexible and scalable cloud infrastructure simulator", *Journal of Grid Computing*, vol. 10, no. 1, 2012, pp. 185–209.

[34] M. Bertoli, G. Casale, and G. Serazzi, "Jmt: performance engineering tools for system modeling", *ACM SIGMETRICS Performance Evaluation Review*, vol. 36, no. 4, 2009, pp. 10–15.

[35] G. Bolch, S. Greiner, H. de Meer, and K. S. Trivedi, Queueing networks and Markov chains: modeling and performance evaluation with computer science applications. John Wiley & Sons, 2006.

[36] S. El Kafhali and K. Salah, "Performance Analysis of Multi-Core VMs hosting Cloud SaaS Applications", Computer Standards & Interfaces, Elsevier, 2017.

[37] Y.-J. Chiang, Y.-C. Ouyang, and C.-H. Hsu, "Performance and cost-effectiveness analyses for cloud services based on rejected and impatient users", *IEEE Transactions on Services Computing*, vol. 9, no. 3, 2016, pp. 446–455.

[38] http://aws.amazon.com/ec2/pricing/.