SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TMLAI TRANSACTIONS ON
MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

VOLUME 5 NO 4, 2017
ISSN 2054-7390

Mitigating Economic Denial of Sustainability Attacks to Secure Cloud Computing Environments

Marwane Zekri[1], Said El Kafhali[2], Mohamed Hanini[3] and Noureddine Aboutabit[1]
[1]IPOSI laboratory, National School of Applied Sciences, Hassan 1st Univ, Settat, Morocco
[2]Computer, Networks, Mobility and Modeling laboratory
National School of Applied Sciences, Hassan 1st Univ, Settat, Morocco
[3]Computer, Networks, Mobility and Modeling laboratory
Faculty of Sciences and Technology, Hassan 1st Univ, Settat, Morocco
marwane.zekri@gmail.com, noure049@gmail.com; said.elkafhali@uhp.ac.ma;
haninimohamed@gmail.com

ABSTRACT

In cloud computing environment where the infrastructure is shared by millions of users, attackers have the opportunity to ensure more damage to the compromised resources. The main aim of such attacks is to saturate and overload the system network through a massive data packets size flooding toward a victim server and to block the service to customers. The Distributed Denial-of-service (DDoS) attack is considered one of the largest threats to the Quality of Service (QoS) of cloud services which is used to deny access for legitimate users of an online service. However, Economic Denial of Sustainability (EDoS) attack is a special breed of DDoS attack that attack exploits auto scaling feature of cloud. The Cloud Service Provider (CSP) scales the architecture automatically to serve those requests for which cloud consumer is charged. A consumer expects a sustainable profit after hosting his application on cloud. The attacker purpose is to guarantee the service unavailability and maximize the financial loss costs by increasing the cost and decreasing the profit. Hence, in this paper we propose a novel mitigation system against the EDoS attacks. Our system consists of source Checking, Counting, and Turing Test. The obtained simulation results show that our system works efficiently to mitigate the EDoS attack in cloud environment.

Keywords-component; Security, Cloud Computing, DDoS attack, EDoS attack, Mitigation

1 Introduction

Cloud computing refers to a type of Internet-based computing that provides shared pool of resources that can be rapidly provisioned on demand over the Internet [1], [2]. For instance networks, memory, computer processing, and user applications [3]. The cloud computing services can be categorized into three models: Software-as-a-service (SaaS), Platform-asa-Service (PaaS) and Infrastructure-as-a-Service (IaaS) [4], [5], and it can be deployed as private, public, community or hybrid cloud [2] (Figure 1). The benefits of cloud computing are several such as being cost savings, the scalability feature, reliability, maintenance, and mobile accessible. But besides all these benefits, cloud computing does come at the cost of increased security risks in which is at the moment one of the biggest challenges this technology is facing today, limiting the number of organizations willing to embrace it wholeheartedly [6]. DDoS [7] is

DOI: 10.14738/tmlai.54.3220
Publication Date: 15th August, 2017
URL: http://dx.doi.org/10.14738/tmlai.54.3220

one type of aggressive attack, which causes serious impact on cloud servers, and according to the list of cloud security threat by the CSA (Cloud Security Alliance) as one of the most severe security threat for the cloud Computing and hinder it.

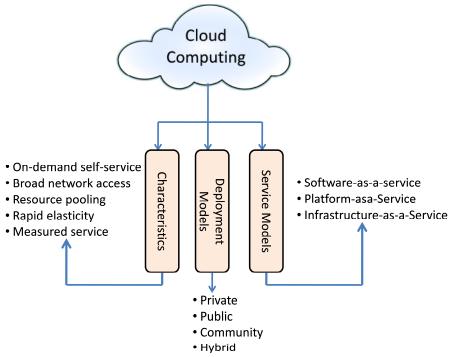


Figure. 1. Cloud computing characteristics, service and deployment models

DDoS attacks exhaust resources of a target [8], by flooding the target with spurious packets. The target could be a servers computing capability or network bandwidth such that the legal users could not access the services provided (Figure 2). EDoS attack is a special breed of DDoS attack that attack exploits auto scaling feature of cloud computing [9]. In EDoS attack, the goal in mind of the attacker is to manipulate service usage billing in orders of magnitude that could be disguised easily as legitimate use of the service [10]. This drives costs to unmanageable levels and maximizes the financial loss by decreasing the profit. Hence, an EDoS mitigation system becomes a technical and economical necessity to defense EDoS attacks in cloud system.

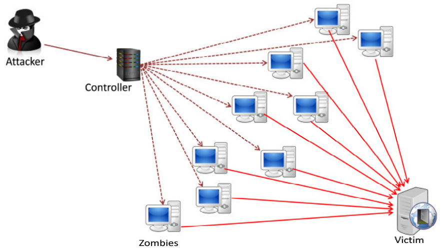


Figure. 2. A typical Architecture of DDoS/EDoS Attacks

To mitigate these risks, the cloud providers adopted many methods and techniques [11], [12] that can be used to prevent, detect and respond to attacks against the cloud. But in the other hand, as cloud strengthens its defense, the attackers find more creative and sophisticated ways targeting the cloud by using or creating loopholes in the cloud defense system. To keep up with this challenge and ensure the continuation and the existence of the cloud, we must improve, revise and upgrade our mitigation strategies. To this end, in this work we propose a novel mitigation technique against EDoS attack in cloud computing, to verify whether the requests coming from the users are from a legitimate person or generated by bots. In our mitigation technique we use a virtual firewall based on white, black and block lists filtering mechanism. The first request is forwarded to a Test Node. This node is responsible for updating the white, block and black lists based on the results of a text based verification challenge. The next requests coming from the bots will be blocked by a virtual firewall if their IP addresses source is found in the black list. On the other hand, the requests coming from legitimate clients will be forwarded directly to the target cloud service since their IP addresses will be found in the white list. As a result, only the requests from legitimate clients will reach the Protected Target. If bots succeeded in bypassing the verification process it will be detected by the EDos Detecting Module which will put their IP Source in the block list.

Our main contributions in this paper can be summarized as follows:

- A text-based question which uses less bandwidth than an image based challenge.
- An algorithm for mitigation in case bots succeeded in bypassing the verification process.
- A simulation results that validate our proposed mitigation strategy.

The rest of the paper is organized as follows. First, in Section II, we discuss the related works. Section III presents the proposed architecture. The experimental setup including the simulation model and results are discussed in Section IV. Finally, the conclusion and the future work are presented in Section V.

2 Related work

Cloud computing EDoS Security has earned a lot of attention in the past few years, and a plethora of literature has been published on the subject. In this section we present published papers related to mitigate EDoS cloud computing system. EDoS Armor [13] protects E-commerce applications in cloud environments, with the assumption that an attacker does not follow regular workflow by purchasing the items instead idle surfing. EDoS Armor proposes muti-layered defense system that includes two modules:

- Admission control module: identifies whether the request is from legitimate client or bot by either image or cryptographic based challenge. Thus, it authenticates number of users in the system. Then, it allows limited number of valid clients to send the requests simultaneously through port hiding. This avoids over burdening.
- Congestion control module: this module handles the maximum resources available to legitimate clients. The client is categorized judging upon his browsing behavior using Decision tree algorithm J48 to classify the clients over the log file using parameters like Purchasing History, CPU Processing time, Session information, Resources Access Pattern.

Random Port Hopping Technique [14] is an In-client server communication scenario. Clients are using IP address and port number. Initially, server share cryptographic key to client for generating random port numbers. Authorized clients can use and determine the server port numbers and access the authorized information. Control measures are also unable to detect the application layer denial of service attacks. But attackers gain this information to target the high profile web servers to degrade their performance.

CloudWatch [15] is an auto scaling technique enabled by Amazon that reduces the effects of the EDoS attacks. CloudWatch is a web service that provides monitoring for cloud resources by which clients will be able to define boundaries that would limit the elasticity of their cloud platforms and thus reducing the effect of the EDoS attacks. In [16], the authors proposed a defending system by combining the filtering and detection mechanisms in order to mitigate the Denial of Service (DoS) attack in cloud data center environment. However, they presented an analytical model based on queueing model to evaluate the impact of flooding attack on cloud environment regarding service availability and QoS performance.

In-cloud scrubber service [17] is an on-demand service to mitigate network and application layers from EDoS. There are two modes based on resource depletion: normal and suspect. If the resource depletion level goes beyond the limit and bandwidth traffic is also very high, then the service provider suspects high rate attack. The system switches to suspected mode and called scrubber Service which generate a puzzle to check legitimacy of the client. In [18], the authors proposed WebSOS to protect web servers by using a filtering mechanism that admits HTTP traffic from only trusted sources known to overlay nodes, to tell Computers and Humans Apart Legitimate clients have to first pass the Completely Automated Public Turing test (CAPTCHA) [19]. The proposed WebSOS presents the performance degradation due to non-direct routing, and also CAPTCHA is being challenged today by bots with the appearance of many algorithms that cracks CAPTCHAs such as Google Maps street address, which reading the algorithm with 99.8 percent accuracy. Furthermore, CAPTCHA based on image challenge [20], [21] needs quite the amount of bandwidth to transmit the CAPTCHA image to the users.

DDos-Shield [22] methodology for mitigating the EDoS in a cloud computing environment, has two main components a virtual firewalls (VF) witch based on a white and black lists filtering mechanism that hold IP addresses of the originating nodes, and the verifier cloud nodes which are represented by a pool of virtual machine nodes implemented based on the cloud infrastructure. The V-Nodes constitute a cloud-based overlay network. A V-Node has the capabilities to verify legitimate requests at the application level using graphic Turing tests, such as CAPTCHA. Another role of the V-Node is to update the lists used by the VF. This approach does not require hiding the location of the protected cloud service and using direct routing, on the other hand it requires the collaboration of an anti-spoofing methodology, and bots may bypass the CAPTCHA test.

In respect to these works, our proposed approach adds a filtering list to the firewall, precisely this list, named Block List, contents malicious IP sources that detected after being successfully blocked permanently or helps to relieve workload on the server.

3 Proposed Model

Figure 3 shows the proposed architecture of our approach for EDoS mitigating in the cloud computing environment. The firewall in our architecture is based on white, black and block lists filtering mechanism. The blacklist is used to hold those unauthenticated source IP addresses so that the firewall will drop the incoming packets originating from these IP addresses. The white list is used to track the authenticated source IP addresses so that the incoming traffic originating from these addresses will be allowed to pass the firewall towards the destined services. The Block list is a list that hold in a temporary manner the packets that are suspected to be malicious or with an abnormal traffic.

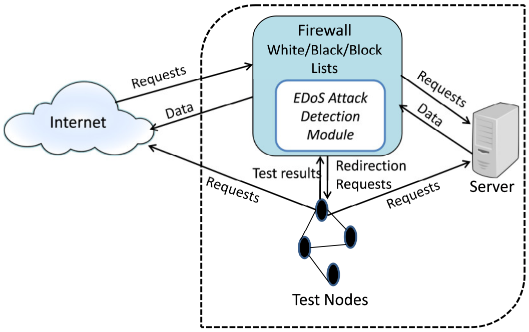
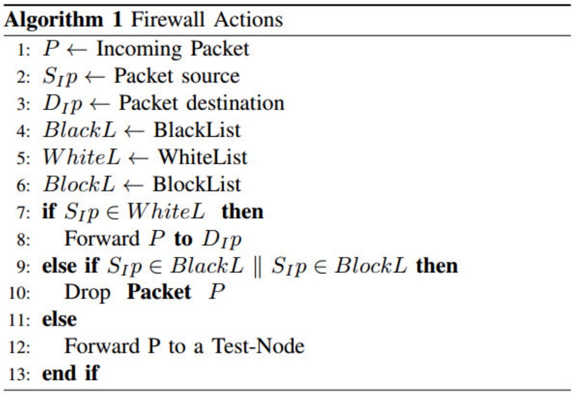


Figure. 3. Proposed mitigation architecture

The packet coming from the Internet will first arrive in virtual firewall. If the IP source exists in the White list, it will be forwarded to its destination. If it IP address source is not figuring in any of lists (Algorithm 1), the packet will be Forwarded to Turing test module by the test Nodes. The Test Nodes constitute a cloud-based overlay network which is represented by a pool of virtual machines. A Test node has the task of verifying the legitimacy of requests at the

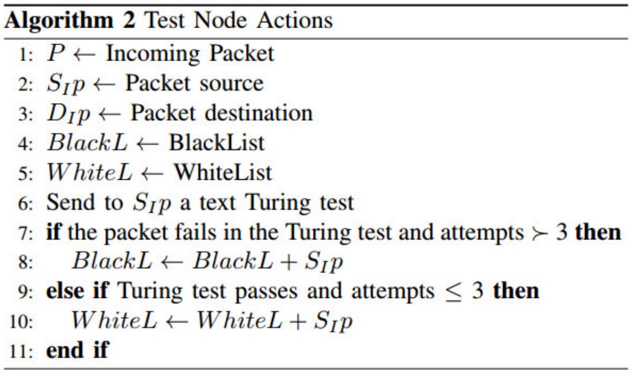
application level using the Text based Turing tests and to update the black and white lists used by the virtual firewall (Algorithm 2).



Algorithm 1 Firewall Actions

```
$P \leftarrow$ Incoming Packet
$S_{IP} \leftarrow$ Packet source
$D_{IP} \leftarrow$ Packet destination
$BlackL \leftarrow$ BlackList
$WhiteL \leftarrow$ WhiteList
$BlockL \leftarrow$ BlockList
if $S_{IP} \in WhiteL$ then
    Forward $P$ to $D_{IP}$
else if $S_{IP} \in BlackL \parallel S_{IP} \in BlockL$ then
    Drop Packet $P$
else
    Forward P to a Test-Node
end if
```

The Turing Test will challenge the requester by responding to a text-based question as for image challenge needs more bandwidth. To continue with the connection, the requester must succeed the challenge by returning the right answer in less than 3 attempts. As for The test Nodes they have the responsibility to update the lists based on the results of the challenge by marking IP address of the packet in the black, and white filtering lists of the firewall.



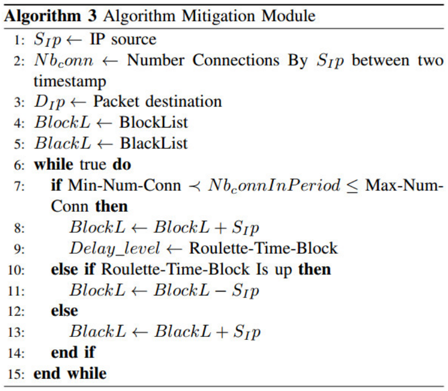
Algorithm 2 Test Node Actions

```
$P \leftarrow$ Incoming Packet
$S_{IP} \leftarrow$ Packet source
$D_{IP} \leftarrow$ Packet destination
$BlackL \leftarrow$ BlackList
$WhiteL \leftarrow$ WhiteList
Send to $S_{IP}$ a text Turing test
if the packet fails in the Turing test and attempts $\succ 3$ then
    $BlackL \leftarrow BlackL + S_{IP}$
else if Turing test passes and attempts $\leq 3$ then
    $WhiteL \leftarrow WhiteL + S_{IP}$
end if
```

The role in Algorithm 3 is trying to find the possible malicious sources and add them into the Block or Black lists. Thus, even if the bots bypass the Request-challenge test or compromised by the attacker it will be detected, and these source IP address will be putted in either the black or block lists of the Virtual Firewall depending on the values of the defined thresholds given by the cloud customer. There are two Modes in the mitigation algorithm approach:

- The first mode named monitor mode (Passive): in this mode the Detection Module collects and records the traffic which will be used to detect the abnormal traffic and malicious packets. If the traffic data statistic is large than the maximum values of the thresholds defined by the cloud customer. The second mode will be triggered.

The second mode (Active): while the monitor mode keep running the second mode work with threshold values which can be enabled or fixed by the cloud customer as to not eventually gets the server overwhelmed. If the number of the connection times of an IP address exceeds Min-Num-Conn and is less than Max-Num-Conn, these IP source will be placed in the block list for a fixed short delay Roulette-Time-Block as for not exhaust the resource of the protected server. Once the delay expired the IP address source are removed from the block list. If the number of the connection times of an IP address is larger than Max-Num-Conn, this IP will be added to the black list (Algorithm 3).



Algorithm 3 Algorithm Mitigation Module

```
$S_{IP}$ ← IP source
$Nb_conn$ ← Number Connections By $S_{IP}$ between two timestamp
$D_{IP}$ ← Packet destination
$BlockL$ ← BlockList
$BlackL$ ← BlackList
while true do
    if Min-Num-Conn $\prec$ $Nb_connInPeriod \leq$ Max-Num-Conn then
        $BlockL \leftarrow BlockL + S_{IP}$
        $Delay\_level$ ← Roulette-Time-Block
    else if Roulette-Time-Block Is up then
        $BlockL \leftarrow BlockL - S_{IP}$
    else
        $BlackL \leftarrow BlackL + S_{IP}$
    end if
end while
```

4 Simulation Results and Discussion

In this section, we have carried out two different simulation scenarios. In the first, we have proposed that the cloud computing environment was not protected. There is any defense system to mitigate EDoS attack risk. In the second, we have implemented the proposed mitigation technique described above so as to decrease the impact of EDoS attack and to achieve a high level of security. Performance curves as those of the CPU utilization, mean response time, and the transmission and reception rate are plotted in the figures.

Figure 4 shows the obtained results regarding the response time. The results show that the response time increases considerably when not applying the mitigation technique. On the other hand, with the proposed mitigation technique, the response time corresponding to legitimate clients is approximately constant and low. The increasing of the response time when not applying the mitigation technique is due to the fact that legitimate requests suffer from more delays caused by the load of the attack traffic, which reaches the queues of the targeted cloud service. However, when using the proposed mitigation technique, the attacks requests will not affect the response time of the legitimate requests.

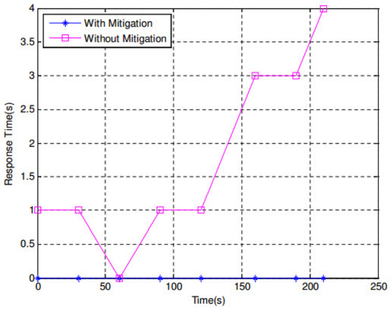


Figure. 4. Impact of EDoS attack on response time

Figure 5 shows the performance of the two scenarios in terms of the computing power utilization. The results show that, without a mitigation technique, when the arrival attack rate increases (by time), the computing power utilization increases indicating a high consumption of the computing resources by the attack requests. With the proposed mitigation technique, the computing power utilization is weakly affected due to the attack rate since the attack requests will not reach the protected cloud service. As a result, the computing power utilization with mitigation is not being changed significantly since the arrival rate of the legitimate requests is fixed.

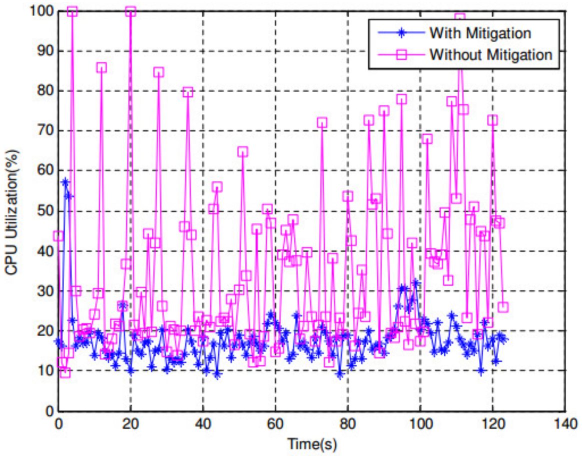


Figure. 5. Impact of EDoS attack on CPU utilization

Figure 6 shows the Transmission and Reception rates (TX/RX) in the two cases with and without applying mitigating. We remark that the approach with mitigation performs better for either Transmission or Reception rate parameter.

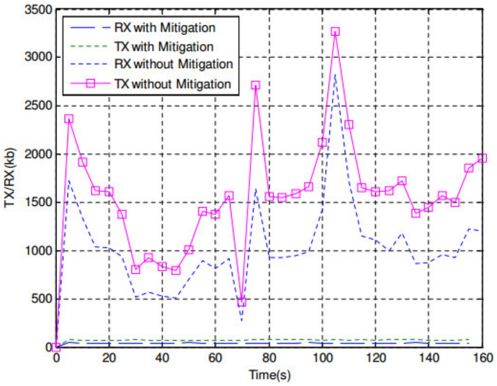


Figure. 6. Impact of EDoS attack on TX-RX rate

5 Conclusion and future work

EDoS attack seeks to disrupt the financial viability in cloud by exploiting utility pricing model by increasing the cost and lowering the profit. In this manuscript, we have proposed an EDoS mitigation system which consists of Source Checking, Counting and turning test. Algorithms that describe different operations of the proposed system are presented and discussed. The obtained results show that our approach reduces Computing Power Utilization and Response time, and performs better for Transmission and Reception rate in case of EDoS attack. As future work, we are planning to enhance our Attack Detection module and integrate it with the proposed mitigation technique in order to rise the efficiency. We also aim to enhance our mitigating strategy to consider IP spoofing attacks.

REFERENCES

[1] Shawish and M. Salama, "Cloud computing: paradigms and technologies," in Inter-cooperative Collective Intelligence: Techniques and Applications. Springer, 2014, pp. 39–67.

[2] P. Mell and T. Grance, "The nist definition of cloud computing," 2011.

[3] M. Hanini and S. El Kafhali, "Cloud computing performance evaluation under dynamic resource utilization and traffic control," in ACM Second International conference on Big Data, Cloud and Applications (BDCA17). ACM, 2017.

[4] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," Future Generation Computer Systems, vol. 29, no. 4, pp. 1012–1023, 2013.

[5] S. El Kafhali and K. Salah, "Stochastic modelling and analysis of cloud computing data center," in 20th ICIN Conference Innovations in Clouds, Internet and Networks. IEEE, 2017, pp. 122–126.

[6] M. T. Khorshed, A. S. Ali, and S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," Future Generation computer systems, vol. 28, no. 6, pp. 833–851, 2012.

[7] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed denial of service (ddos) resilience in cloud: review and conceptual cloud ddos mitigation framework," Journal of Network and Computer Applications, vol. 67, pp. 147–165, 2016.

[8] 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.

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

[10] M. Ficco and M. Rak, "Economic denial of sustainability mitigation in cloud computing," in Organizational Innovation and Change. Springer, 2016, pp. 229–238.

[11] N. Z. Bawany, J. A. Shamsi, and K. Salah, "Ddos attack detection and mitigation using sdn: Methods, practices, and solutions," Arabian Journal for Science and Engineering, vol. 42, no. 2, pp. 425–441, 2017.

[12] N. Agrawal and S. Tapaswi, "Defense schemes for variants of distributed denial-of-service (ddos) attacks in cloud computing: A survey," Information Security Journal: A Global Perspective, pp. 1–13, 2017.

[13] M. Masood, Z. Anwar, S. A. Raza, and M. A. Hur, "Edos armor: a cost effective economic denial of sustainability attack mitigation framework for e-commerce applications in cloud environments," in 2013 16th International Multi Topic Conference (INMIC), IEEE, 2013, pp. 37–42.

[14] R. P. Kumar, J. Babu, T. Gunasekhar, and S. B. Bhushan, “Mitigating application ddos attacks using random port hopping technique,” International Journal of Emerging Research in Management &Technology, vol. 4, no. 1, pp. 1–4, 2015.

[15] A. CloudWatch, “Amazon cloudwatch,” 2014.

[16] I. EL Mir, D. S. Kim, and A. Haqiq, “Towards a stochastic model for integrated detection and filtering of dos attacks in cloud environments,” in ACM Second International conference on Big Data, Cloud and Applications (BDCA17). ACM, 2017.

[17] M. N. Kumar, P. Sujatha, V. Kalva, R. Nagori, A. K. Katukojwala, and M. Kumar, “Mitigating economic denial of sustainability (edos) in cloud computing using in-cloud scrubber service,” in 2012 Fourth International Conference on Computational Intelligence and Communication Networks (CICN). IEEE, 2012, pp. 535–539.

[18] A. Koduru, T. Neelakantam, and S. M. S. Bhanu, “Detection of economic denial of sustainability using time spent on a web page in cloud,” in 2013 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM). IEEE, 2013, pp. 1–4.

[19] L. Von Ahn, M. Blum, N. J. Hopper, and J. Langford, “Captcha: Using hard ai problems for security,” in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2003, pp. 294–311.

[20] R. Datta, J. Li, and J. Z. Wang, “Imagination: a robust image-based captcha generation system,” in Proceedings of the 13th annual ACM international conference on Multimedia. ACM, 2005, pp. 331–334.

[21] A. Gupta, A. Jain, A. Raj, and A. Jain, “sequenced tagged captcha: generation and its analysis,” in IEEE International Advance Computing Conference, 2009. IACC 2009. IEEE, 2009, pp. 1286–1291.

[22] M. H. Sqalli, F. Al-Haidari, and K. Salah, “Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing,” in 2011 Fourth IEEE International Conference on Utility and Cloud Computing (UCC). IEEE, 2011, pp. 49–56.