Journal of Computer Science

Review

Critical Review of Economical Denial of Sustainability (EDoS) Mitigation Techniques

Parminder Singh Bawa and Selvakumar Manickam

National Advanced IPv6 Centre, Universiti Sains Malaysia, Penang, Malaysia

Article history
Received: 04-03-2015
Revised: 22-06-2015
Accepted: 14-10-2015

Corresponding Author:
Parminder Singh Bawa
National Advanced IPv6 Centre, Universiti Sains Malaysia, Penang, Malaysia
Email: parminder@nav6.usm.my

Abstract: Many organizations and service providers have started shifting from traditional server-cluster infrastructure to cloud-based infrastructure. The threat of Distributed Denial of Service (DDoS) attack continues to wreak havoc in these cloud infrastructures. In addition to DDoS attacks, a new form of attack known as Economic Denial of Sustainability (EDoS) attack has emerged in recent years. EDoS which is unique to cloud infrastructure may not be easily detected as with DDoS. Although EDoS attack is small at the moment, it is expected to grow in the near future in tandem with the growth in cloud usage. As EDoS has a major impact economically, it can considered to be more serious than DDoS and many defence and mitigation mechanisms have been proposed to combat these attacks. This paper introduces EDoS and how it differs from DDoS. The existing mitigation techniques are described and the drawbacks of these techniques are explained.

Keywords: EDoS, Cloud Computing, Security, Review, DDoS

Introduction

Cloud Computing (CC) brings the paradigm shift in distributed computing community. According to IDC survey (Gens, 2009), It is evident that people are more concern about security in cloud computing. Kresimir Popovie (Popovic and Hocenski, 2010) gives a clear idea about the security issues related to the cloud computing. Zissis and Lekkas (2012) have classified the security requirements and threats exist at various cloud service levels. Distributed Denial of Service (DDoS) (Versign, 2012) attacks are one of the key issue for Internet security. DDoS flooding attack is an attempt to disrupt genuine user's access to services. Attackers typically compromise computers by exploiting their vulnerabilities to create them zombies (Cooke *et al*., 2005). Sizable amount of compromised systems are indulged to initiate a DDoS attack on one or more targets by flooding with serious traffic or by flooding malformed packets to exhaust the resources.

A variant of DDoS, unique to CC infrastructure is known as Economic Denial of Sustainability (EDoS). The goal of EDoS is to bankrupt a particular cloud-hosted service by attacking its billing structure directly affecting the cost of service provisioning. In terms of detection, unlike DDoS which is can easily detected as the indicator is increase in traffic volume, EDoS attacks may not be easily detected, due to the absence of instrumentation and business logic in the stacks of applications and infrastructure to measure the relationship between "requests" and "successful" transactions. In this study, we introduce the concept of EDoS and how it differs from DDoS followed by a critical review of existing mitigation techniques that can be used to combat these attacks.

State of Cloud Attack

The eighth annual Worldwide Infrastructure Security Report (Arbor Networks, 2014), from security provider Arbor Networks, reveals the follow statistics:

- 94% of data center managers reported some type of security attacks
- 76% had to deal with Distributed Denial-of-Service (DDoS) attacks on their customers
- 43% had partial or total infrastructure outages due to DDoS
- 14% had to deal with attacks targeting a cloud service

Due to the nature of CC in which the resources will be expanded when allocation of current resource is no longer sufficient, i.e., elastic resource allocation. A variant of DDoS attacks, specific to subscription-based CC infrastructure and services, has been discovered, it is called EDoS. The Economic Denial of Sustainability

(EDoS) in the cloud is only because of DDoS attack, where the service to the legitimate user is never restricted and utilization of server and network resources are dynamically expanded to serve excess traffic. The client who is using cloud will incur a debilitating bill by using highly elastic (auto-Scaling) capacity to serve a large amount of undesired traffic in order to maintain the QoS as per the SLA.

In our previous paper (Singh *et al*., 2014) we studied that In an EDoS attack, the target is to make the costing model unsustainable and therefore making it no longer viable for a company to affordability use or pay for their cloud-based infrastructure.

In network security, there are various types of attacks available which can affect the network resources and services. Distributed Denial of Service (DDoS) is foremost notable attacks. Main focus is to deny access to the legitimate user from accessing the network resources or restrict the availability of the network resources by exhausting bandwidth (Kumar *et al*., 2012). To emphasize on the impact of DDoS, a new variant of DDoS attack known as Economical Denial of Sustainability (EDoS) was introduced (Hoff, 2008). EDoS can be classified as packet flood that can extend the elasticity of metered-services provisioned via cloud infrastructure, EDoS attack can be formulated by remotely run bots to flood the targeted cloud service by fake requests at slow rate to hide themselves from the security devices (Sqalli *et al*., 2011). Therefore, the cloud service will pump up additional resources to satisfy the on-demand requests.

Public cloud services offered on pay-as-use bases. In case of EDoS attack, client will be charged for these fake requests, making the service not viable to afford by user (Khor and Nakao, 2011). As a result, the cloud provider will lose its customers and it will be more viable to run in-house data centre, cheaper than the cloud. Hence, the cloud service providers are affected negatively by EDoS attacks more than their customers (Hoff, 2009; Kumar *et al*., 2012).

Review of EDOS Mitigation Techniques

In order to understand the security in cloud environment, we should be aware of the objective and requirement of Confidentiality, Integrity and Availability (CIA) (Zissis and Lekkas, 2012). In this section we will review the various EDoS mitigation techniques available.

EDoS-Shield

This mechanism has two main components, the cloud verifier node and virtual firewall. Firewall does the packet filtering based on the White list and Black list method.

Al-Haidari *et al*. (2012) proposed the Enhanced EDoS-Shield framework as an enhancement to their DoS Shield framework as shown in Fig. 1, to mitigate the EDoS attacks originating from spoofed IP addresses. They make use of the Time-To Live (TTL) value found in the IP header to facilitate detecting the IP spoofed packets. The TTL is a field in the IP packet header determines the maximum lifetime of the packet to forbid it from circling on the network without end in a routing loop existence. The packet will be discarded when its TTL value is zero. Otherwise, the packet passes through router will decrease the TTL field by one (Al-Haidari *et al*., 2012).

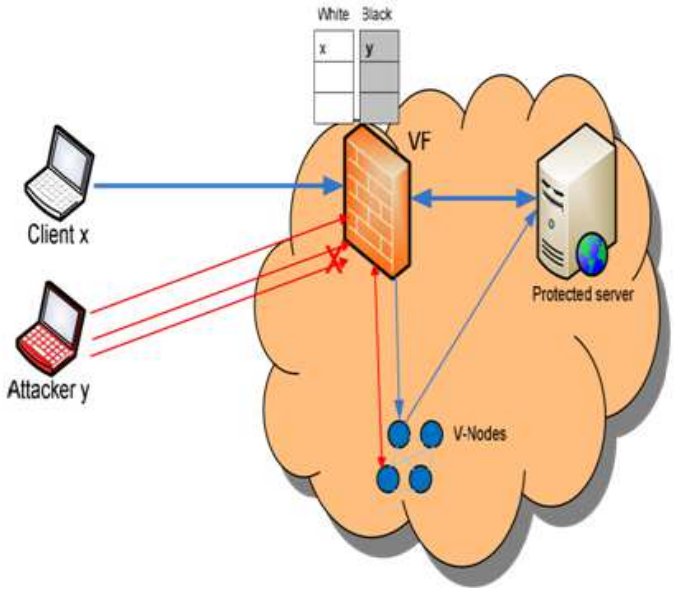

Fig. 1. EDoS-shield

sPoW

Khor and Nakao (2009) introduced sPoW to mitigate an application and network layer eDDoS mitigation mechanism as shown in Fig. 2. The main function of this method is to filter the attack traffic before it start over committing of resources. The concept of self-verifying Proof of Work (sPoW) is introduced to transform the network level eDDoS traffic to distinguishable traffic that can be filtered using pattern matching. In second phase it sends crypto puzzles to client to resolve by brute force method.

This framework requires high computation power to solve crypto-puzzles for client, which can create overheads on the machine to brute force harder puzzles, which makes this method unviable for mobile devices. If brute force traffic may not get processed, it adds up utilization cost. On server side, server generate more harder crypto puzzles in case of high connection request, which utilize more computing power and expand resources. Secondly sPoW relies on client-server architecture and DNS like services, which requires a large channel identity namespace, will increase the latency and service access time.

CloudWatch

As shown in Fig. 3, CloudWatch (CloudWatch, 2013) is professional service from Amazon to reduce the impact of the EDoS attacks by providing monitoring service for cloud resources, which enable organisations to define upper limits to the elastic resource utilization of their cloud infrastructure. This is an inefficient solution against the EDoS as user can still be charged for over utilization in case of DDoS attempt. Also it defeats the purpose of cloud computing as the elasticity touches the upper limit, the cloud service freezes and users service access will not be available.

As this passive approach only provides the monitoring and alert service, final decision will be dependent on the client's administrator to look into the problem and take action accordingly. In most of the cases, client responds only after the cloud commits the resources using auto scaling and customer has to pay for the time they use the resource. In case of volumetric DDoS attack, cloud expands itself to the max limit defined by the end user before admin get any attention on it. Cloudwatch, collects statistical data, which can be utilized for analytical purposes.

EDoS Armor (Masood et al., 2013)

This technique works on admission and congestion control, a twofold solution. This method has three components (i). Challenge server (ii). Admission control (iii). Congestion control as shown in Fig. 4. Challenge server provides image or cryptographic based challenge to client initiating a connection. If client resolve the challenge only then request forward to admission control. Admission control rate limit the clients who resolved the challenge and provide the random access key and hide port number to communicate with server. Congestion control allocate server resources within the permitted clients using client priority table which keeps the current priority level for each client.

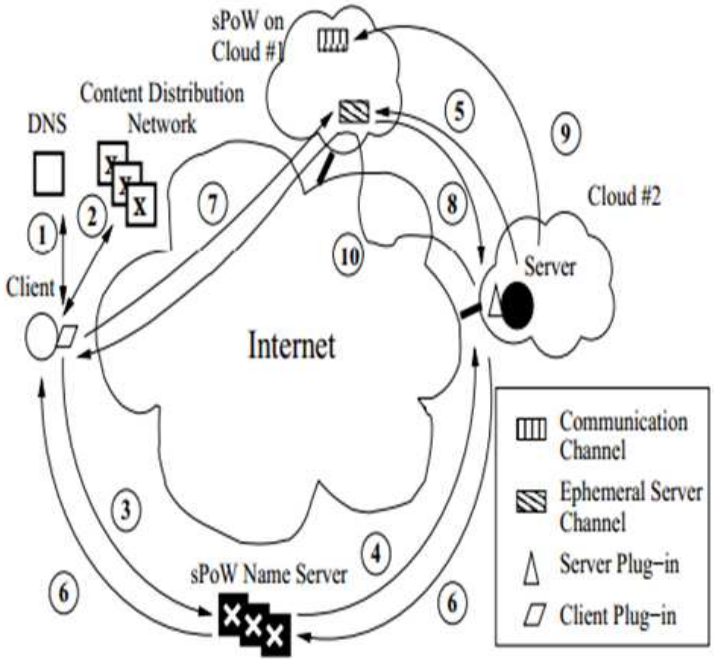

Fig. 2. sPoW

DOI: 10.3844/jcssp.2015.855.862

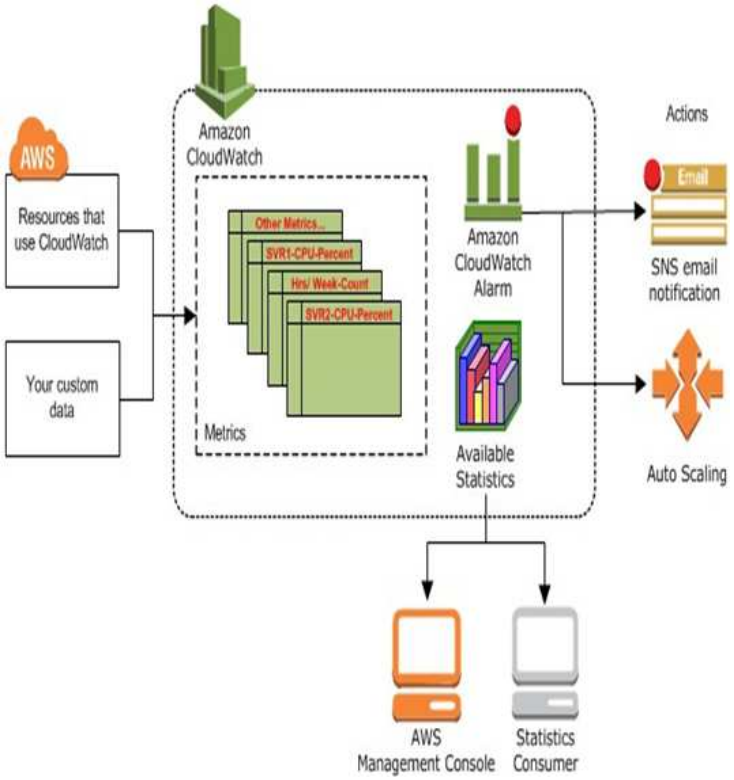

Fig. 3. Cloud watch

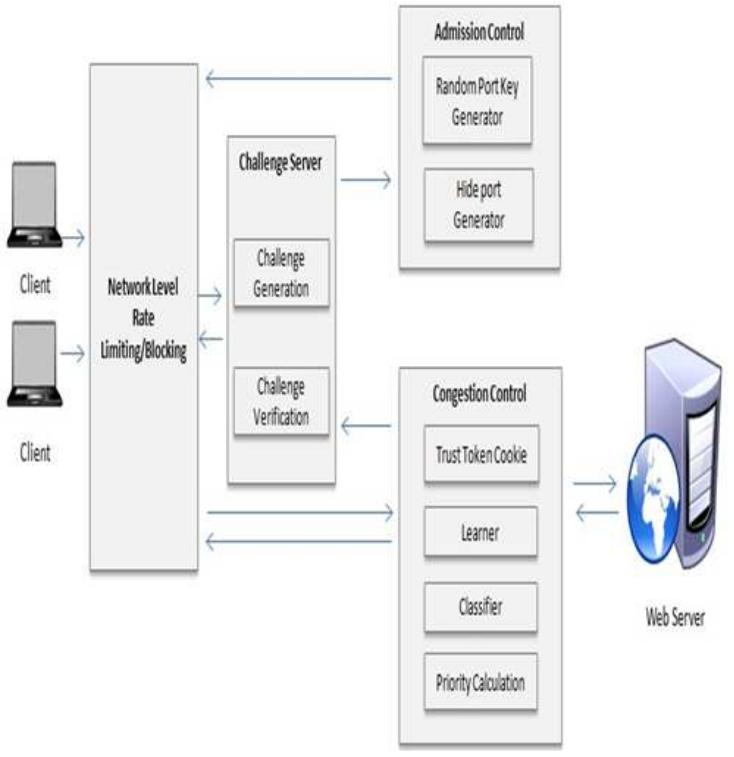

Fig. 4. EDoS-Armor

DOI: 10.3844/jcssp.2015.855.862

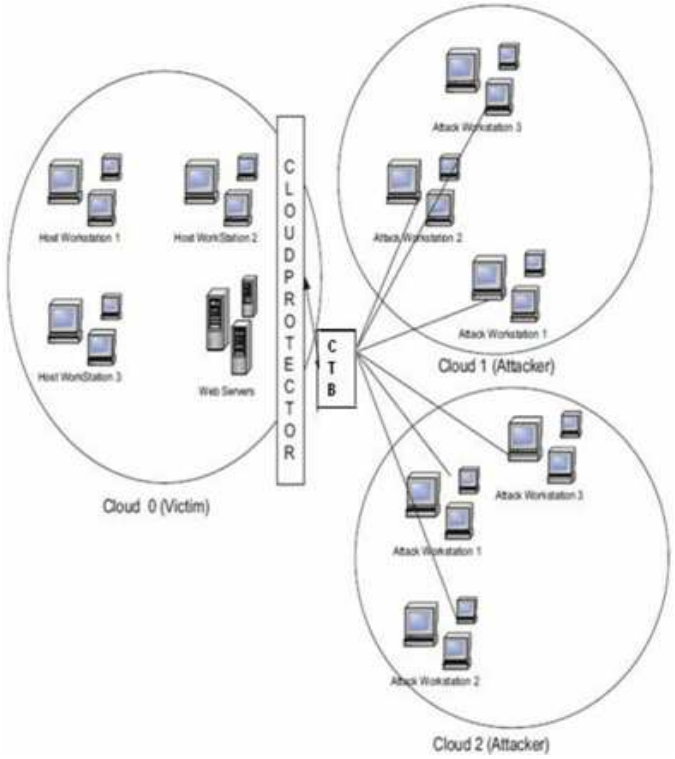

Fig. 5. Cloud Trace Back

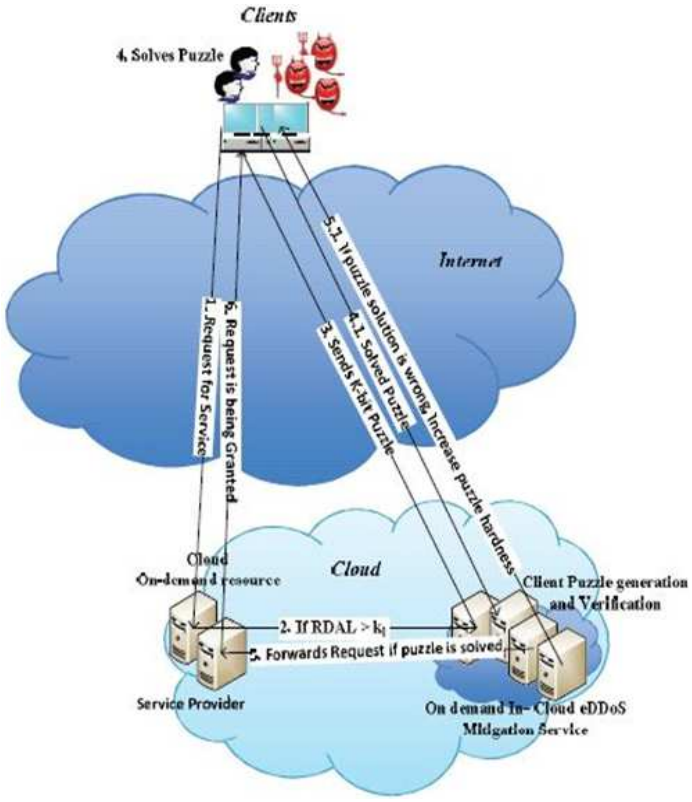

Fig. 6. In-cloud Scrubber

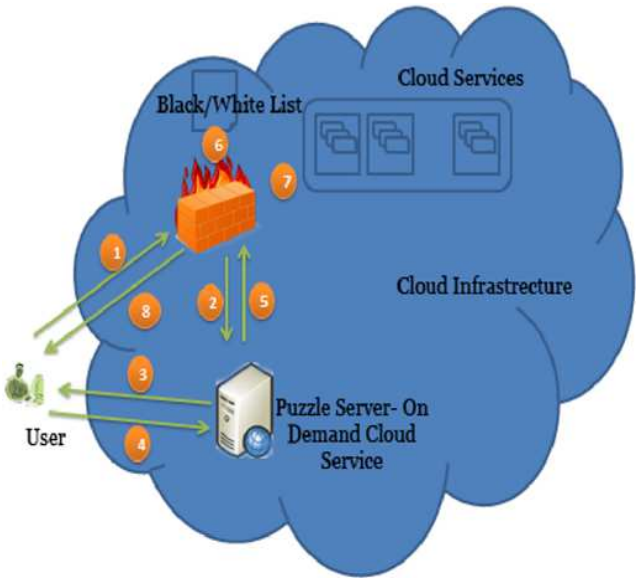

Fig. 7. Vivinsandar's framework

EDoS Armor works by defining number of clients that can send requests and the prioritized clients based on the activity and type of resources they access. This method provides the network rate limiting which is good for internal use of organisations. You can limit the connection from specific network but it creates overheads in port translation, generating challenge for authentication and in verification of trusted node and prioritizing them.

Cloud Trace Back (Chonka et al., 2011)

This method use the packet marking and trace back mechanism to shield from the application level XML based DoS attack. This mechanism has two components, Cloud Trace Back (CTB) and Cloud Protector (CP) as shown in Fig. 5. Incoming traffic marked by CTB and packet filtration done by CP.

CTB can be implemented over Virtual Machines (VM) to deploy in cloud and become a Service Oriented Architecture (SOA) (Ye and Singh, 2007) product. CTB incorporated in edge router to monitor the all incoming packet to cloud. Using this mechanism, source of attack can be identified and filtered.

This technique can provide the trace back to the attack source based on the Packet Marking technique, but in case of spoof IP, it may be a false location. Also the storage of all incoming packet is a challenge for a cloud environment. It needs a dataset to train himself for protection. Policy based behavior make it worst if not defined properly. CTB itself is prone to DDoS attack.

In-Cloud Scrubber

Naresh (Kumar *et al*., 2012) proposed this reactive technique is based on puzzle generation and verification process as shown in Fig. 6. Each client accessing web based cloud resources will have to resolve the puzzle. According to the result, scrubber services allow or deny the access to web service.

Service provider works in either of two states suspected mode or normal mode. In suspected mode access request sent to scrubber services which generate puzzles to get it resolved by clients. Puzzle based approach generally used to detect network layer attacks and this framework focus on network load than server utilization.

Resolving and generating hard cryptographic puzzles consume system resources at both client and server end. As mobile devices have limited resources, it may not be an appropriate solution. This framework lacks in addressing end-to-end latency issue as every packet will be inspected and verified.

VivinSandar and Shenai (2012) framework depends on firewall filter engine as shown in Fig. 7. All request from clients get redirected to puzzle server which send a puzzle to client to resolve, based on the client feedback client get added to white list or black list. Drawback of this approach is if any legitimate client failed to answer or do not provide answer to puzzle it will get blacklisted. Also it does not provide any protection if attack originated from the whitelisted host.

Summary

As most of the above reviewed mitigation techniques are based on application layer and handled directly by the client machines and all the EDoS traffic is already in cloud service provider's network consuming network resources leading to the bottleneck of cloud service provider's network resulting in the poor services to the end clients. A new mitigation technique is required to filter the EDoS/DDoS traffic by the cloud service provider to protect the interest of their clients. Summary of countermeasure is listed in Table 1.

Table 1. Summary of countermeasures

Approaches	Focus	Methodology	Distribute approach	Learning ability	Scalability
CloudWatch	EDoS attack	Traffic monitoring	Yes	No	Yes
EDoS-shield	EDoS attack	Virtual firewall and authentication	No	Yes	Yes
Cloud traceback	HTTP and XML based DoS attack	Packet marking and traceback	Yes	Yes	Yes
sPoW	EDoS attack	Packet filtering	Yes	Yes	Yes
In-cloud scrubber	EDoS attack	Puzzle generation and verification	No	Yes	No
EDoS armor	EDoS attack	Packet filtering and authentication	No	Yes	Yes

Future Work

Software Defined Networks (SDN) provides a deep control over the network transparency and ability to manage the network efficiently in cloud environment. We are working on proposing a new mitigation framework using SDN to mitigate the EDoS/DDoS in cloud network from cloud service provider's perspective to protect the interest and provide uninterrupted resources to clients.

Conclusion

Embracing cloud computing can eliminate traditional computing scenario and open up new security challenges. DDoS is still the major threat to traditional and cloud infrastructure, EDoS is a variant of DDoS in subscription based cloud computing, makes it even worst. Most of the approaches use only HTTP attack mitigation against EDoS and ineffective against ICMP and UDP attack. This paper reviewed that more robust approach is required to counter EDoS as the methods available are either ineffective or inefficient to handle zero day and known attacks.

Funding Information

The authors have no support or funding to report.

Author's Contributions

Parminder Singh Bawa: Contribution to conception and acquisition of data, analysis and interpretation of data, drafting and reviewing it for significant intellectual content.

Selvakumar Manickam: Contribute in drafting the article and critically reviewed the content and give final approval of the version to be submitted.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Al-Haidari, F., M.H. Sqalli and K. Salah, 2012. Enhanced edos-shield for mitigating edos attacks originating from spoofed IP addresses. Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Jun. 25-27, IEEE Xplore Press, Liverpool, pp: 1167-1174. DOI: 10.1109/TrustCom.2012.146

Arbor Networks, 2014. Insight into the global threat landscape. Arbor Networks, Inc.

Chonka, A., Y. Xiang, W. Zhou and A. Bonti, 2011. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. J. Netw. Comput. Appli., 34: 1097-1107. DOI: 10.1016/j.jnca.2010.06.004

CloudWatch, A., 2013. Monitoring for AWS cloud resources.

Cooke, E., F. Jahanian and D. McPherson, 2005. The zombie roundup: Understanding, detecting and disrupting botnets. Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop, (TIW'05), USENIX Association Berkeley, CA, USA, pp: 6-6.

Versign, 2012. DDoS Mitigation: Best Practices for a Rapidly Changing Threat Landscape.

Gens, F., 2009. New IDC IT cloud services survey: Top benefits and challenges.

Hoff, C., 2008. Cloud computing security: From DDoS (Distributed Denial of Service) to EDoS (Economic Denial of Sustainability). Blog.

Hoff, C., 2009. A couple of follow-ups on the EDoS (Economic Denial of Sustainability) Concept. Rational Survivability.

Khor, S.H. and A. Nakao, 2009. SPoW: On-demand cloud-based EDDoS mitigation mechanism. Proceedings of the 5th Workshop on Hot Topics in System Dependability.

Khor, S.H. and A. Nakao, 2011. DaaS: DDoS mitigation-as-a-service. Proceedings of the IEEE/IPSJ 11th International Symposium on Applications and the Internet, Jul. 18-21, IEEE Xplore Press, Munich, pp: 160-171. DOI: 10.1109/SAINT.2011.30

Kumar, N.M., P. Sujatha, V. Kalva, R. Nagori and A.K. Katukojwala *et al*., 2012. Mitigating Economic Denial of Sustainability (EDoS) in cloud computing using in-cloud scrubber service. Proceedings of the 4th International Conference on Computational Intelligence and Communication Networks, Nov. 3-5, IEEE Xplore Press, Mathura, pp: 535-539. DOI: 10.1109/CICN.2012.149

Masood, M., Z. Anwar, S.A. Raza and M.A. Hur, 2013. EDoS armor: A cost effective economic denial of sustainability attack mitigation framework for e-commerce applications in cloud environments. Proceedings of the 16th International Multi Topic Conference, Dec. 19-20, IEEE Xplore Press, Lahore, pp: 37-42. DOI: 10.1109/INMIC.2013.6731321

Popovic, K. and Z. Hocenski, 2010. Cloud computing security issues and challenges. Proceedings of the 33rd International Convention MIPRO, May 24-28, IEEE Xplore Press, Opatija, pp: 344-349.

Singh, P., S. Manickam and S.U. Rehman, 2014. A survey of mitigation techniques against Economic Denial of Sustainability (EDoS) attack on cloud computing architecture. Proceedings of the 3rd International Conference on Reliability, Infocom Technologies and Optimization, Oct. 8-10, IEEE Xplore Press, Noida, pp: 1-4. DOI: 10.1109/ICRITO.2014.7014767

Sqalli, M.H., F. Al-Haidari and K. Salah, 2011. Edos-shield-a two-steps mitigation technique against EDoS attacks in cloud computing. Proceedings of the 4th IEEE International Conference on Utility and Cloud Computing, Dec. 5-8, IEEE Xplore Press, Victoria, NSW., pp: 49-56. DOI: 10.1109/UCC.2011.17

VivinSandar, S. and S. Shenai, 2012. Economic Denial of Sustainability (EDoS) in cloud services using http and xml based DDoS attacks. Int. J. Comput. Appli., 41: 11-16. DOI: 10.5120/5807-8063

Ye, X. and S. Singh, 2007. A SOA approach to counter DDoS attacks. Proceedings of the IEEE International Conference on Web Services, Jul. 9-13, IEEE Xplore Press, Salt Lake City, UT., pp: 567-574. DOI: 10.1109/ICWS.2007.23

Zissis, D. and D. Lekkas, 2012. Addressing cloud computing security issues. Future Generation Comput. Syst., 28: 583-592. DOI: 10.1016/j.future.2010.12.006