DEEP LEARNING OF ATTACK DETECTION AND LOW RATE TESTS ON DDoS ATTACKS

Dr. R. Rajesh M.C.A., M.Phil., PhD., Guest Faculty & Software Consultant [Brioworkx IT Service Pvt. Ltd] Department of Computer Applications, School of Information Technology, Madurai Kamaraj University, Palkalainagar, Madurai – 625021. E-Mail: vrrajeshmca@gmail.com

Dr. M. Ramakrishnan, M.E., Ph.D., Ph.D. Professor and Head Department of Computer Application Chairperson - School of Information Technology Madurai Kamaraj University Madurai – 625 021.

P. Ganesan M.E., Guest Faculty Department of Computer Applications, School of Information Technology, Madurai Kamaraj University, Palkalainagar, Madurai – 625021. E-Mail: pganeshcse@gmail.com

Abstract

The complexity of distributed denial of service (DDoS) attacks is escalating swiftly, which makes protecting against these threats are bigger and very important for all layers. A DDoS attack may sound complicated, but it is actually quite easy to understand. The process of sending and receiving data from one host to another, data encapsulation, is possible due to the existence of a seven layer protocol suite presented as the OSI model. Although while investigating DoS attacks, rarely refer to various layers of this OSI model, special weight age is to be laid upon the seventh layer, the application layer. In essence, it procures an interface to end-user tasks, and facilitates programs such as web browsers, email services, and photo applications in sending network communications (e.g., SMTP or HTTP).

Key Words: (DDoS), Distributed Denial of Service, layers, attacks.

1. Introduction

I. Layer seven DDoS Attacks Compared to Other Types

The inclination of DDoS attacks indicates faultlessly that culprits focus and climb the OSI arrange model after some time. The migration of the practical objective is legitimate, since more DDoS protection frameworks center their essential recognition controls around lower layers (Imperva, 2016). Along these lines, assaults on the web application layer are progressively prominent. Besides, layer seven entrance, the top layer in the OSI model, gives an outlet on a business rationale layer, which is viewed as a dynamic expansion of the previously mentioned network protocol suite.
Given that the internet is built vertically by multiple protocol layers, it would be perfectly understandable if internet DDoS attacks assume a vertical classification, as well.

If we adopt this approach, some common types of DDoS attacks include:

- IP attacks on the network bandwidth – Layer 3 (Network Protocol)
- TCP attacks on server sockets – Layer 4 (Transport Protocol)
- HTTP attacks on Web server threads – layer seven (Application Protocol)
- Web application attacks on CPU resources – layer seven+

As of now we take hold of the difference between DDoS attacks, in terms of OSI model classification, let's go through some general

features that distinguish layer seven DDoS attacks from others:

1. While network layer DDoS attacks attempt to overwhelm the victim server with bogus requests, the application layer DDoS attacks rely on legitimate ones.

2. In layer seven DDoS attacks, attacking computers have to set up a full TCP connection. Thus, while providing genuine IP addresses is something you cannot dispense with, the entire action proceeding may seem legitimate in the absence of traffic spikes. They may virtually swindle even a vigilant DDoS defense mechanism, and they're stealthy.

3. A layer seven DDoS attack, in contrast to the others, may exploit vulnerabilities in application software, thus circumventing detection and aiming directly at the targeted Web server. In other words, they are more sophisticated, since they do not count entirely on a brute force to achieve desired ends.

4. Perhaps the most notable difference; so-called volumetric DDoS attacks strive to bring down network infrastructure and servers by employing high-bandwidth-consuming flooding. That benefits from an inherent blind spot of the internet medium. On the other hand, layer seven DDoS attacks take the victim server in the rear, first engaging well-known applications such as Hypertext Transfer Protocol (HTTP), Voice Over Internet Protocol (VoIP), or Domain Name System (DNS) (Arbor Networks, Inc. 2016).

5. The goal of application layer DDoS attacks usually have nothing to do with overwhelming bandwidth. Some IT experts call them "low and slow" for a reason. Frequently, at close range are exhausted CPU or memory resources. Hence, layer seven DDoS leverage as well inherent flaws and limitations of applications, for example, system resources are always finite. There's surprise here actually. Heavy resource consumption will eventually render the server incapacitated (Imperva, 2016).

6. Protection and mitigation of common volumetric attacks is something that IT specialists are well familiar with. In contrast, layer seven DDoS attacks often stand as a more formidable challenge (Breaking Point Labs, 2011).

The outlined picture of importance and future prevalence of application layer DdoS attacks was shared by experts from the OWAS Foundation in 2010: "We believe layer seven attacks may supersede layer four as the modus operandi of DDoS bot nets in this new decade."

Layer Seven DDoS Attacks Statistics

To continue the layer seven DDoS topic, let's review a couple of interesting sources of relevant statistics. First, according to Arbor's statistical information, with an over 102% increase of DDoS attack size when compared to the previous year, 2010 appears to be a cornerstone in DDoS evolution. A year later, a Hardware Security Survey: Attack Count by Type and Bandwidth claims that application layer attacks are prevalent:

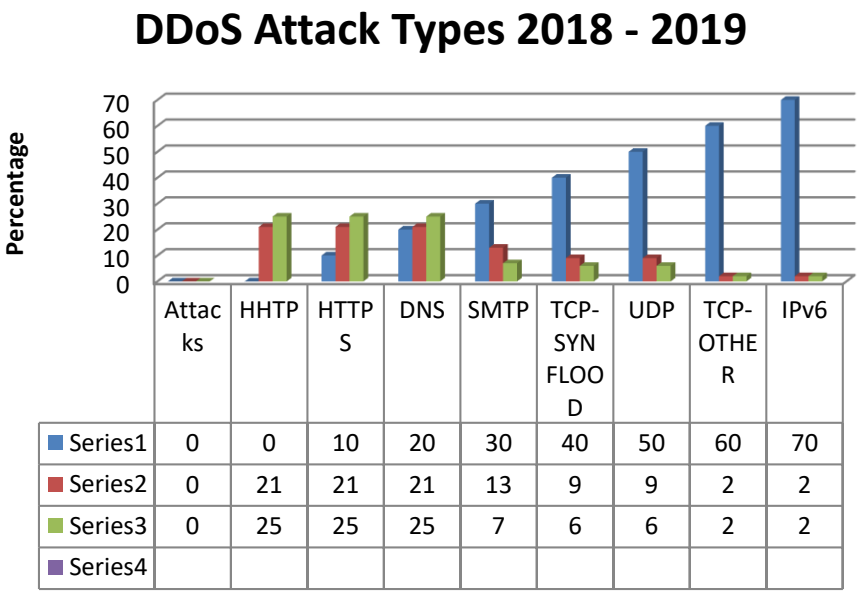


Fig 1.1 DDoS Attack Types 2016- 2017

In 2016, information passed in the survey that 49.92 % growth in layer seven DDoS attacks.

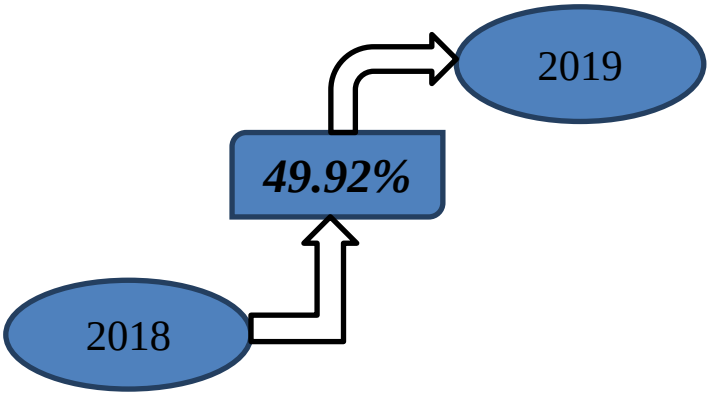


Fig 1.2 Total Application Layer Attacks 2018 vs. 2019

In addition, quarterly reports by Prolex show a definite tendency of increasing popularity, particularly of HTTP GET DDoS attacks in the period from April 2018 to June 2019.

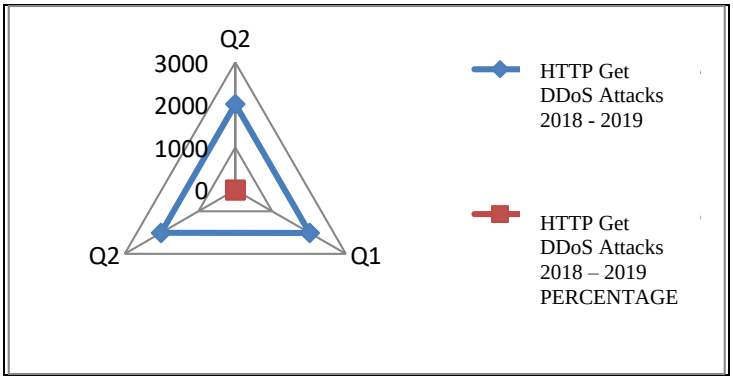


Fig 1.3 DDoS attacks 2016-2017

Why Are Application-Layer DDoS Attacks Such a Vexing Threat?

The top layer of the internet protocol suite has two main categories of protocols: protocols that directly service users (e.g., HTTP, FTP, IMAP, Telnet, SMPT/POP, IRC, XMPP, SSH etc.) and support protocols that underpin various system functions (e.g., DNS, SNMP, BOOTP/DHCP, TLS/SSL, SIP, RTP, NTP etc.) (Abliz, 2011).
According to general practice, layer seven DDoS attacks are often customized to target a specific web application. For example, web servers that run a combination of Java, PHP5, and ASP.NET may be targeted by specially crafted HTTP requests, which may collide with the web server's hashing operation "when unique requests return non-unique and overlapping responses (Katz, 2016, p. 3)." A great amount of these "hash-busting" requests sent in a short time, like a MG-42 machine gun, would deplete essential web resources and create a denial of service.

Simplicity of layer seven

It's thought that if thousands of users simultaneously keep pressing the refresh button on their browsers that would crash the server soon or later. Whether or not it's possible, many hackers use layer seven DDoS attacks time and again. An unsophisticated "low and slow" attack, for instance, is the one that struck a major credit card company that ceased providing services to

Here are seven reasons of why layer seven DDoS attacks represent such a vexing threat:

May affect many different applications
Any one of the protocols examined above may be subject to a DDoS attack (Abliz, 2011). Many of them target HTTP to exhaust a web server's vitality (Breaking Point Labs, 2011).

Highly-targeted strikes

WikiLeaks in 2010. In this case, the first experienced downtime was caused by a brute-force HTTP traffic flood towards application, originating from approximately 940 computers.

Maximum Results with Limited resources

Unlike other denial of service attacks, layer seven requires very little investment by attackers. In fact, along with the ulterior nature of the weaponry in question, a feasible execution presupposes tactics reminiscent of guerrilla warfare.

Conducive to collateral damageApplication layer DDoS attacks carry a special mark. A DNS attack, for instance, directed at single DNS provider, may spread and affect all of its clients.

Appearance of legitimacy in Slow traffic, legitimate as far as protocol rules and rates are concerned, and normal and complete TCP connections, are the main prerequisites that entail

the benign appearance typical of layer seven DDoS attacks.

Bypass one security shield or take the “shortcut”

As a usual practice, applications that are subject to attack are usually “allowed” through security devices such as firewalls or IPS devices (e.g., HTTP or DNS traffic). Hence, one security layer can be eliminated with ease.

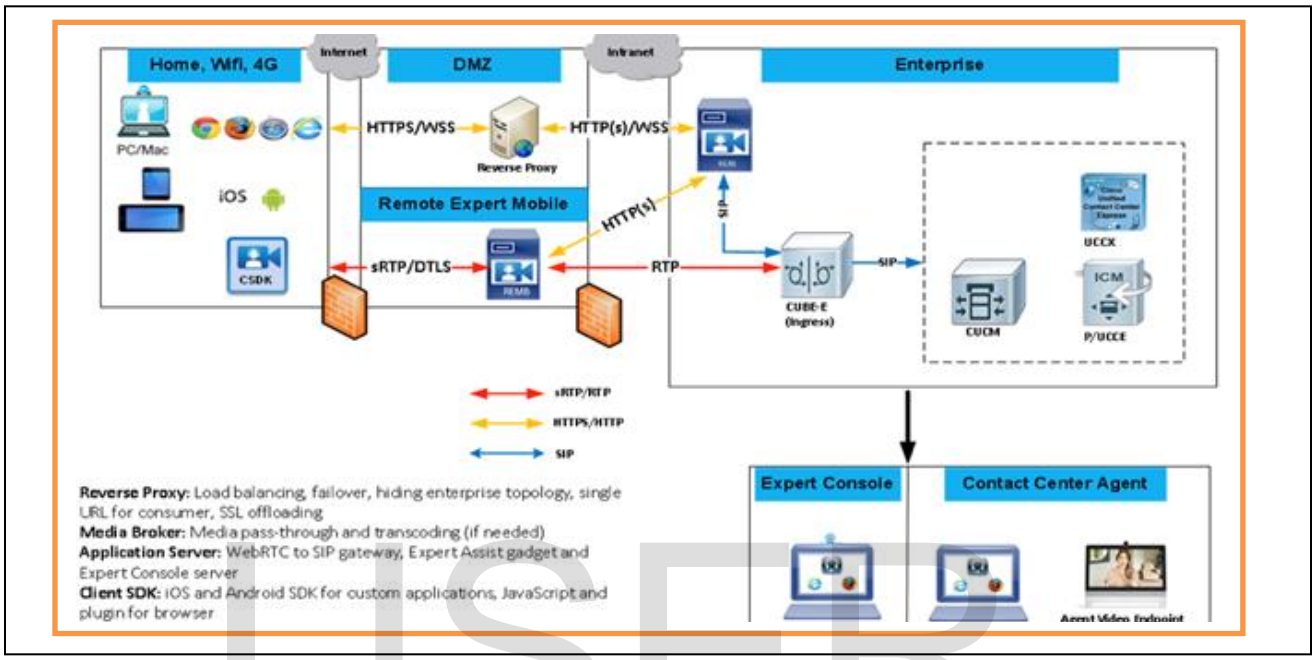


Fig 1.4 Application Zone

What's more, though a Network DDoS assault works in the intelligent "Access Zone," an application DDoS assault focuses on the "Application Zone." That comprises of the web front-end and the information stockpiling for it. All together for an application DDoS assault to be effective, it needs to circumvent the whole arrangement of "Access Zone" gadgets and components set up, exploit a security hole on the "Application Zone," and after that at long last infuse a payload that proceeds to build up an immediate correspondence line with the web server, to strike either the server itself or application.
Layer seven DDoS methods and attacks, Types of common layer seven DDoS attacks are divided into four basic categories:

Request-Flooding Attacks

High rates of apparently real application demands, for example, HTTP GETs, DNS inquiries and SIP INVITEs, storm web servers to debase and upset its ordinary working.

Asymmetric Attacks

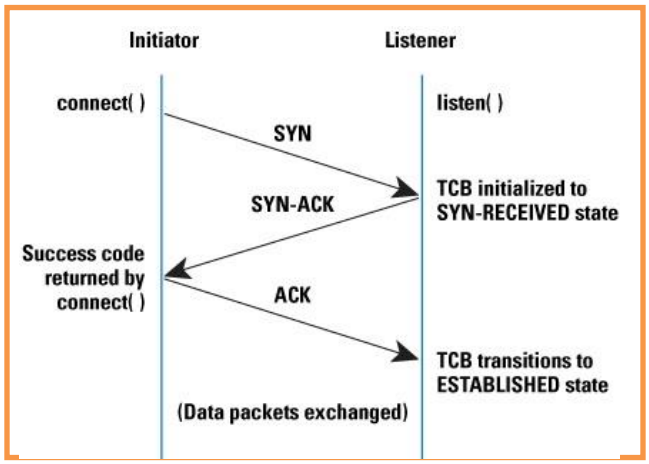
“High-workload” requests that take a heavy toll of server resources such as CPU, memory or disk space.

Repeated Single Attacks

An isolated “high-workload” request being sent across many TCP sessions, a stealthier way to combine asymmetric and request-flooding layer seven DDoS attacks.

Application-Exploit Attacks

The attack vectors here are vulnerabilities in applications, for instance, hidden-field manipulation, buffer overflows, scripting vulnerabilities, cross-site scripting, cookie poisoning, and SQL injection.



DDoS ATTACK Architecture - TCP SYN Flood

Layer seven DDoS methods

First and foremost, it's important to note that this means of attack manages to complete the three-way TCP handshake, hereby evading devices and measures that give protection against layer four DdoS attacks. These attacks often appear normal and fly under the radar. The second phase of the DDoS attack is different, however, contingent on application type and the methodology chosen by the aggressive side. Some examples of HTTP attacks:

HTTP GET approach uses GET requests; meant to acquire particular data at a URL point. By entering a URL in the relevant bar, a GET request is also ready (Pornin, 2017).

HTTP GET flooding is when many of these requests, sometimes tens of thousands, are sent within a short period of time, attempting to drain server resources. Simplicity itself makes this type of DDoS attack more common.

Other HTTP GET-based methods are HTTP Malformed Attacks that dispatch invalid HTTP packets (e.g., ZafiB worm), and HTTP Idle Attacks that slowly send incomplete HTTP requests.

HTTP POST is the method used to employs HTTP POST requests used with forms whose entire set of headers is sent correctly, including the Content-Length number. However, the distinction here is a POST message body that is sent at a very low rate (Content-Length transmitted byte by byte). They preclude connection from proper completion (Imperva, 2016). Hence, practically any website that has forms accepting HTTP POST requests (for example, submitting feedback, login, uploading photo/video attachments, sending email and etc.) is susceptible to this method (The OWASP Foundation, 2010).

HTTP Slow Read
The modus operandi here functions the other way around, the data isn't being pushed slowly to the server, the malicious entity himself forces the targeted server to forward a large amount of data, which, in turn, is read again in a drawn-out, protracted manner. When the connection process is established, the attacker produces a tiny receive window, which compels the server to break down the response to many small fragments that'll fit the buffer size, leading eventually to extremely slow ongoing responses (Imperva, 2016).

As the author of this method says, "the idea of the attack I implemented is pretty simple; bypass policies that filter slow-deciding customers, send a legitimate HTTP request and read the response slowly, aiming to keep as many connections as possible active".

Others

Although HTTP is the most targeted protocol, other application types are attacked as well, such as; DNS dictionary attacks, VoIP (SIP INVITE Flood Attack), SMTP buffer overflow attacks.

2. Implementation and Simulation

In this simulation, we are going to use NS2 to generate data packets and flood the target computer, client or server and attackers.The topology in the wired network is set-up using the node and link creation APIs. The tcl script in DDoS_attack.tcl creates the DDoS attacks of denying normal service. In Distributed Denial of Service (DDoS) attacks vast amount of requests are generated to victims through hacked computers. Data transmission is carried out between the genuine client and also from attacker(hacker) to victim using the CBR applicationandTCP connection.

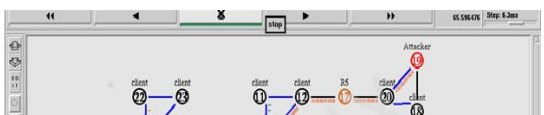


Table 1: Simulation Details

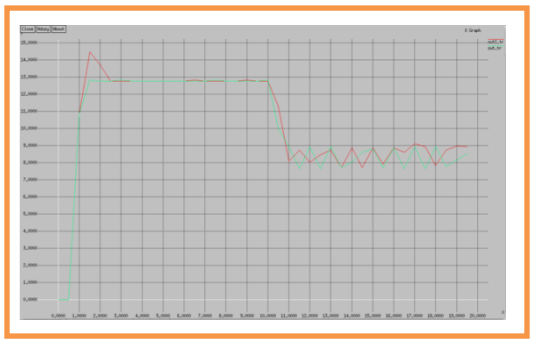


Fig 2.2 Availability of Packets before Attacks for condition

Fig 2.1 Attack Scenario

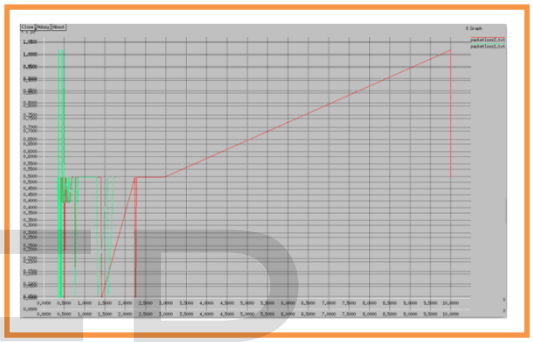


Fig 2.2 Availability of Packets after Attacks

S.No.	Tools	Flooding (or) Attack Methods
1	Tribe Flood N/W	TCP, ICMP, SYN,Smurf
2	Stacheldracht and variants	TCP, ICMP, SYN,Smurf
3	TFN 2K	TCP, ICMP, SYN,Smurf
4	Shaft	TCP, ICMP, SYN,combo
5	Trin00	TCP

From test results got from the above simulation, it tends to be reasoned that the usage and accessibility are great execution measures for a server under a DDoS assault, all victim individual servers of DDoS assaults ordinarily have a low accessibility when contrasted with their qualities under Ordinary condition, anyway their use increment pointedly when they are enduring an onslaught. This data can be verybeneficial to the originators of DDoS protection instruments, as they can make their apparatuses demonstration quickly they sense changes in these presentation measures. It tends to be additionally gathered that the Simulation Events of NS2 can reenact a DDoS assault.

3. Conclusion

A denial of service attack's intent is to deny legitimate users access to a resource such as a network, server etc.There are two types of attacks, denial of service and distributed denial of service.A denial of service attack can be carried out using SYN Flooding, Smurf or buffer overflowSecurity patches for operating systems, router configuration, firewalls and intrusion detection systems can be used to protect against denial of service attacks.

4. Reference

1. Modelling and simulation of DDOS Attack using SimEventsAbubakarBala*1 and Yahya Osais2
2. The Top 10 DDoS Attack Trends, Discover the Latest DDoS Attacks and Their Implications, www.imperva.com.

reserved. Imperva and SecureSphere are registered trademarks of Imperva.

3. The continued rise of DDoS attacks, Candid Wueest, Principal Software Engineer,Version 1.0 – October 21, 2014, 13:00 GMT. www.symantec.com. Copyright © 2014 Symantec Corporation. All rights reserved.
4. Understanding the Modern DDoS Threat by Gunter Ollmann, VP of Research, Damballa. ID.30.104.0511,Copyright © 2011, Damballa, Inc. All rights reserved worldwide.
5. DDoS attacks: 5 strategies for defending your networkBy Charles Herring on 3 June, 2015.
6. A deep learning based intelligent framework to mitigate DDoS attack infogenvironmentRojalinaPriyadarshini⇑, Rabindra Kumar BarikKIIT University, Bhubaneswar, IndiaarticleinfoArticlehistory:Received 28 September 2018Revised 16 April 2019Accepted 17 April 2019. Journal of King Saud University Computer and Information Sciences journal homepage:www.sciencedirect.com
7. Berral, J.L., Poggi, N., Alonso, J., Gavalda, R., Torres, J., Parashar, M., 2008. Adaptivedistributed mechanism against flooding network attacks based on machinelearning. Proceedings of the 1st ACM workshop on Workshop on AISec. ACM,pp. 43–50.
8. Buyya, R., Dastjerdi, A.V., 2016. Internet of Things: Principles and paradigms.Elsevier.
9. Cassel, M., Lima, F., 2006. Evaluating one-hot encoding finite state machines for seureliability in sram-based fpgas. On-Line Testing Symposium, 2006. IOLTS 2006.12th IEEE International. IEEE, p. 6.
10. C.G.C. Index, Forecast and methodology, 2015–2020 white paper, Retrieved 1stJune.
11. Diro, A.A., Chilamkurti, N., 2018. Distributed attack detection scheme using deeplearning approach for internet of things. Future Generation Comput. Syst. 82,761–768.
12. HTTP flood attack detection in application layer using machine learningmetrics and bio inspired bat algorithmIndraneelSreeram⇑, Venkata Praveen Kumar VuppalaDepartment of CSE, St. Ann's College of Engineering & Technology, Chirala, IndiaarticleinfoArticlehistory:Received 13 May 2017Revised 9 October 2017Accepted 14 October 2017Available online 18 October 2017Applied Computing and Informaticsjournal homepage: www.sciencedirect.com
13. J. Udhayan, R. Anitha, Demystifying and rate limiting ICMP hosted DoS/DDOSflooding attacks with attack productivity analysis, in: IEEE InternationalConference on Advance Computing, 2009, pp:558–564.
14. Xia Chun-Tao, D. Xue-Hui, C. Li-Feng, An algorithm of detecting and defendingCC attack in real time, in: International Conference on Industrial Control andElectronics Engineering, 2012, pp. 1804–1806.
15. S.M. Lee, Distributed denial of service: taxonomies of attacks, tools, andcountermeasures, in: Proceedings of the International Workshop on Security inParallel and Distributed Systems, San Francisco, 2004, pp. 543–550.
16. Raj kumar, ManishaJitendra Nene, A survey on latest DoSattacks:classification and defense mechanisms, Proc. Int. J. Innov. Res. Comput.Commun. Eng. 1 (8) (2013).

17. ErolGelenbe, Michael Gellman, George Loukas, An autonomic approach todenial of service defence, in: Sixth IEEE International Symposium on a World ofWireless Mobile and Multimedia Networks, 2005. WoWMoM 2005, June 2005,pp. 537–541.
18. International Conference on Computational Intelligence and Data Science (ICCIDS 2018)Hypothesis Test for Low-rate DDoS Attack Detection in Cloud Computing Environment KritiBhushana, B. B. Gupta2018 The Authors. Published by Elsevier B.V
19. Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).
20. Idziorek, J., Tannian, M. F., & Jacobson, D. (2013). “The insecurity of cloud utility models.”IT Professional 15(2): 22-27.
21. Idziorek, J., Tannian, M., & Jacobson, D. (2011). “Detecting fraudulent use of cloud resources.” InProceedings of the 3rd ACM workshop on Cloud comp. sec. workshop, 61-72.
22. 1999 DARPA Intrusion Detection Evaluation Data Set,[Online], https://ll.mit.edu/ideval/data/1999data.html [Accessed on: 03rd Sep. 2017].
23. The CAIDA UCSD "DDoS Attack 2007" Dataset [Online]. http://www.caida.org/data/passive/ddos-20070804_dataset.xml. [Accessed on: 03rd Sep. 2017].