International Journal of Engineering & Technology, 7 (2.30) (2018) 33-38

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Slow flooding attack detection in cloud using change point detection approach

Dr. Baldev Singh [1] *, Dr. S.N. Panda [2], Dr. Gurpinder Singh Samra [3]

[1]Asst. Professor, Lyallpur Khalsa College Jalandhar, Punjab, India
[2] Director(Research), Chitkara university Rajpura, Punjab, India
[3] Principal, Lyallpur Khalsa College Jalandhar, Punjab, India
**Corresponding author E-mail:*

Abstract

Cloud computing is one of the high-demand services and prone to numerous types of attacks due to its Internet based backbone. Flooding based attack is one such type of attack over the cloud that exhausts the numerous resources and services of an individual or an enterprise by way of sending useless huge traffic. The nature of this traffic may be of slow or fast type. Flooding attacks are caused by way of sending massive volume of packets of TCP, UDP, ICMP traffic and HTTP Posts. The legitimate volume of traffic is suppressed and lost in traffic flooding traffics. Early detection of such attacks helps in minimization of the unauthorized utilization of resources on the target machine. Various inbuilt load balancing and scalability options to absorb flooding attacks are in use by cloud service providers up to ample extent still to maintain QoS at the same time by cloud service providers is a challenge. In this proposed technique. Change Point detection approach is proposed here to detect flooding DDOS attacks in cloud which are based on the continuous variant pattern of voluminous (flooding) traffic and is calculated by using various traffic data based metrics that are primary and computed in nature. Golden ration is used to compute the threshold and this threshold is further used along with the computed metric values of normal and malicious traffic for flooding attack detection. Traffic of websites is observed by using remote java script.

Keywords: *Flooding Attacks; HTTP(S); DDOS Attack; Threshold; Cloud.*

1. Introduction

Flooding attack is a type of distributed denial of service (DDOS) attack that exhausts the resources and services of target machine or network by way of sending a huge volume of packets with fake and randomized source addresses. The packets sent belongs to TCP, UDP, ICMP traffic and HTTP Posts. Flooding traffic is originated by either a single source machine (DOS attack) or multiple machines (DDOS attacks). The genuine traffic is suppressed and lost in spurious flooding traffics. Bandwidth attacks are also caused by flooding due to immense number of malicious traffic due to which network bandwidth of legitimate traffic is exhausted and is unable to reach at the destination system. Flooding attacks are commonly network-layer attacks and application layer DDOS attacks. Application-layer DDOS attacks [1] exhaust the resources in the application layer that makes the destination machine unavailable to the authentic users.

Cloud computing has gained immense response because of which the communication between machines to machine has increased immensely. HTTP(S) protocols primarily play role for communication many fold. Today, it is easy to interface with the hardware devices based on HTTP API calls. HTTP protocol is an application protocol that functions as a request-response protocol in the process of client-server communication. This application layer protocol is used along with the TCP-IP framework. Various methods defined by HTTP [1], [3] are GET, HEAD, POST, PUT, DELETE, TRACE, CONNECT etc. These methods are used for request/response purpose. In HTTPS, the "S" refers to secure hence HTTPS [1] is the secure version of HTTP that makes communication between browser and website in an encrypted manner. HTTPS pages mainly use one of the two different secure protocols (SSL and TLS) for encryption of communication between source and destination. PKI or public key-private key combination is used for cryptography. As these protocols are mainly used in web communication [2], [14], [15] hence these two protocols have come under attack from illegitimate stake holders.

The main intention of the attacker is to saturate the network by way of using different types of flooding attacks. The flooding either severely slows down the system or crashes the system to the saturation point.

Table 1: Internet Growth Indicator [34]

Internet Traffic Growth indicator	Growth Rate values
Annual global IP traffic	3.3 ZB in 2021 from 1.2 Zb in 2016 (per year)
Global IP traffic (GipT)	Threefold increase from 2016 to 2021
Compound Annual Growth Rate (CAGR) of GipT	24 percent from 2016 to 2021
Number of devices connected to IP networks	Expected 3-times higher than global population in 2021
Live Internet video	Expected growth 15-fold from 2016 to 2021
Virtual reality and augmented reality traffic	Expected 20-fold from 2016 and 2021 (CAGR of 82 percent.)
Global mobile data traffic	Expected growth twice to fixed IP traffic from 2016 to 2021
Business IP traffic will	Expected growth 21% at a from 2016 to 2021

The table-1 shows the Internet growth indicators which signifies that as the traffic is increases over the Internet. It is general observation that more is the traffic over cloud or Internet more are the chances of attacks over it. It is also estimated that nearly two thirds of all workloads will be processed in the cloud [30] which have interfacing with billions of machines, sensors and web applications. These statistics clearly shows that cloud encompasses all kinds of communication including sensor to sensor communication, sensor to cloud over Ethernet, sensor to mobile phone network to cloud, sensor to long range radio to cloud, sensor to wi-fi router to cloud [13].

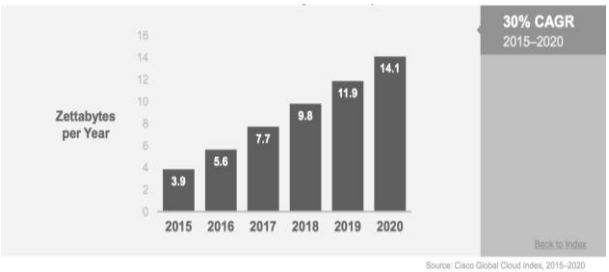

Fig. 1: Global Cloud Traffic Growth [34].

The Internet of Things (IoT) is the combination of physical objects or "things" that are embedded by using electronics, software, sensors, and network connectivity. IoT enables these objects to collect and exchange data. Objects to be sensed and controlled remotely across existing network by using the concept of IoT. It leads to the results to improve efficiency, accuracy and economic benefit. The figure-1 shows these trends. Cloud traffic will grow 3.7 fold from 2015 to 2020 as well as cloud accounts for 92% of traffic by 2020 up from 82% in 2015. All these communication are only possible because of the concept of application program interfaces (APIs). Consumer and business applications are backing to the emergent dominance of cloud service. From consumers view point, the most widespread applications includes streaming video, social networking, and Internet search. Enterprise resource planning (ERP), teamwork and collaborations, business data analytics, in addition to other digital enterprise applications are prevalent for business users. Figure-2 depicts the global IP growth trends in the coming times. It shows that the global IP traffic will increase 3 times from 2015 to 2020 which is more susceptible to attacks. CAGR of global IP traffic growth is expected 22% from 2015 to 2020 [34].

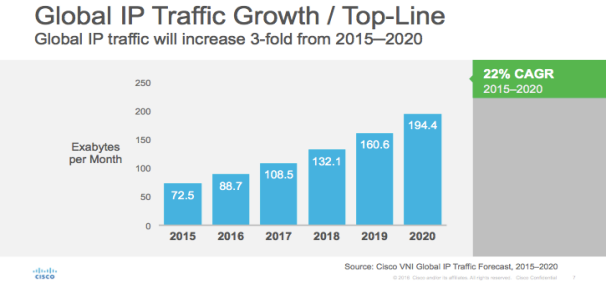

Fig. 2: Global IP Traffic Growth/Top-Line [34].

The use of application program interfaces (APIs) provide high level of interoperability between different kinds of infrastructure, platform and software components. The most popular protocols [5], [6] for data communication over the web [7], [14] are HTTP and HTTPS. There are large number of APIs available now. They are integrating the various elements of cloud. Flooding DDOS [2-5] attack is very common type of attack in the cloud environment. It has severe effect on an enterprise and its reputation hence there is dire need to ensure the security of IT resources to protect from DDOS attacks [27]. The attackers can now not only attacks websites but also attack devices like connected cameras, TVs, cars, health monitoring systems and many intelligent systems etc. The attacks may come from any geographical locations using any weakness in access vector, network vector etc. In this work, we have used different metrics [31] like bounce rate, Entry Page, Exit rate, entry to exit rate, Visits per Visitors, page views per visit and weighted bounce rate [8] to detect slow flooding DDOS attack [6], [16].

2. Review study

The impact of attacks on the cloud is not easy to evaluate due the dynamic attributes of the system dynamics. A review study about the elements of cloud [14], [17] that comes under DDOS attacks is conducted as well as the techniques to detect such attacks are reviewed.

The authors in [9] discussed that most of the application level DDOS attacks first interact with the browsers, therefore browsers need to serve inbuilt mechanisms to counter such intrusion. Failing to do these browsers becomes puppets bots in hands of DDOS attackers. The paper also analyzes the resource wastage done by puppetized browsers in terms of bandwidth, website views and size of puppet nets. The paper also discussed the role of HTTP based communication that comes under such attacks due to propagation of puppet browsers as they are bound to use HHTP protocol. The impact is on the download, upload and browsing speeds to such an extent that no service can operate. The proposed work provides an approach to overcome amplification of DDOS attack situations by safe guarding the HTML and JavaScript units rendered inside the browsers.

The authors in [10] paper discussed about success of using an improved method for the detection of DDOS attack based on the analysis of multiple factors. The factors which can help to identify the DDOS attack presence are subjected to multi variant analysis. The method computes the 'geometrical triangular' area from correlation among different features. This approach focuses on all possible combinations of correlation and hence prove an effective measure for security measuring in terms of detection of DDOS attack.

In this research paper [17], the researchers demonstrated the system of detection based on HHTP based DDOS attacks anatomy. Hence, the need for having Adaptive security appliances, firewalls and algorithms for deep inspection of such attack vectors is mandatory. The authors were able to realize the importance of HTTP deep packet inspection mechanism with the use of GNS3 simulators. The deep HTTP packet inspection policy was implemented in GNS3 experiments and showed successfully that it could prevent the network from DDOS flooding attack successfully by identification of the malicious packets.

The authors in [18], are using the basic logic of understanding the nature of data going inside or coming out from egress, the traffic is characterized based on its 'normal' and 'abnormal' behavior. Accordingly to heuristically identified methods for flooding DDOS attack detection, the benefit is security checking inside and outside the network.

The Research paper [19] is about handling DDOS attacks based on two protocols (HTTP & FTP). The paper illustrates two independent architectures for each of these protocols to design these architectures. The paper considers client puzzle protocol, ingress filtering, intrusion detection system and threshold value based systems' features and limitations to build its own system of detection of flooding DDOS attacks in cloud.

The authors in [21] discussed the issues of detecting HTTP DOS/DDOS attacks. The authors demonstrated a framework for monitoring all aspects of HTTP based DOS/DDOS attacks. Following three subsequent framework' layers viz. outer blocking (OB) layer, service trace back oriented architecture (STBOA) layer and the Entropy based (FAEB) schema layer for eliminating flash crowd and high rate DDOS attacks. The results claimed in this research paper shows that their proposed scheme suffers from low rate of false negative and hence high accuracy in detection and elimination of flooding DDOS attack by validating and tracing back technique.

The author in [25], focused on characterizing the volume of traffic, duration, speed of attack in their series of experiments for finding reliable fixes for DDOS attacks and it was found that many hackers are using Bit Torrent peer to peer file sharing/ transfer to generate flooding DDOS attack. This is done typically by four attack methods which includes (i) Report target victim as participating peer, (ii) Report the target victim as a tracker (iii) Report victim as peer in DHT and (iv) Combining all the above methods.
Many variables including number of torrents, ports under attack, throughput blocked and number of HOST involved under adversity are observed for analysis purpose. For fixing such issues in Bit torrents, the authors based on the experimental results have suggested that bit torrent clients can detect data by analyzing data about SWAM e.g. if there is malicious peer, it will hold same file(s) pieces and the state of SWAM would remain unchanged for long time indicating malicious intent of hackers.
Internet of Things (IoT) mainly consists of three layers according to the paper [26], [33], which includes perception layer, transportation layer and application layer. This has some contrast with respect to traditional networks especially in case of security domain. From this paper, we are able to understand the security architecture of IoT (s) as lot of comparative information is given in tabular form. It is apparent from these givens in this paper, there are multiple ways of integration of heterogeneous networks RIFD, sensors and electronic devices and most part of it is connected with web hence prone to DDOS attacks.

2.1. After conducting the above systematic review of the techniques used for identification of DDOS attacks over various elements of cloud [23], [24], following research gaps are identified:

1) It is identified that Website analytics, which gives statistical information about HTTP and HTTPS API calls, are not used for detection of slow DDOS attacks.
2) It is found that APIs management services and analytics are not used for detection of DDOS attacks.
3) It is observed that that the simple metrics (Table-2) like Entry Page, Bounce rate, Exit rate, Page Views per Visit, Weighted Bounce rate etc. can also help us to find correlation between the attack vectors and HTTP calls done on a cloud element like website/web services [6] cloud end points.

3. Problem statement

Impenetrable prickles in direct HTTP traffic [2], [13] at a particular endpoint in cloud may be an indication of slow flooding DDOS attack especially when there is huge bounce rate and exit rate at the same time. This may be an indication of victimization of a particular cloud endpoint by distributed unknown sources which resemble DDOS characteristics due to its flooding [12], [18] nature. Detection of such scenario is a problem to be solved in this research work. This must be done by a numerically stable algorithm so that anomaly detection [21] threshold is correctly identified for detection of adversity points during such slow HTTP based DDOS attacks in cloud environment.

4. Proposed approach

In this section various attack determinants of slow flooding DDOS attacks is illustrated. The attack determinants also encompasses various metrics on the basis of which flooding attacks are identified. These are impacting the change point detection from the normal traffic.

Table 2: Flooding DDOS Attack Determinants

Attack determinant Metrics	Adversity causes	Outcomes and Effects
Entry Page: It is calculated as Entries/Visits [8,31]	More frequent entries to a single popular page due to Flooding of traffic	Its excess value leads to degrade network
Exit Page: It is calculated as Exits/Visits [19, 31]	More frequent exit from a single popular page due to Flooding of traffic	Its excess value leads to degrade network
Bounce Rate: It is computed as Single access/entries [18], [31]	More frequent entries to a single page due to Flooding of traffic	Its excess value leads to degrade network
Weighted Bounce Rate: It is computed as Bounce rate * (Page views/Total page views) [31]	More frequent entries to a single page (more weightage to more often page) due to Flooding of traffic	Its excess value leads to degrade network
Unexpected increase in baffling Page views	DDOS bots [11], [23], DDOS attack tools	It can lead to disruption of the normal usage of cloud services as well as affect the quality of Service (QOS).
No corresponding peak or drop in other traffic sources [22]	Normal working of cloud endpoints where the adversity has no effect.	Congestion at particular end points.
Bounce rate near hundred percent	The attacker is able to send multiple HTTP requests which is authorized.	It leads to launch of more specific attacks like TCP hijacking [17].
Too much calls from geographically governing networks [19]	Typically the DDOS attack sources are coming from particular dominant sub network addresses [19], [20].	The attacker prevents the authentic packet from reaching its destination in the cloud.
Mean time spent between1 sec. to 2 secs	Since automatic bots doing calls, the time spent is <2 secs which is infect some time equal to page load/reload time.	It leads to degrade network service to cloud users or entirely make it unusable during the time it is active.
Traffic from unknown/ghost referral [9]	Spoofing type attacks	It leads to failure to detect IP Spoofing [21].
Extreme traffic from a few IPs	Usually the DDOS attacks are from a particular dominant sub network addresses.	It leads to delay in management hence fails to detect frequent communications in network.
Entry page and exit page ratio [8] close to one	This is again because of the fact that the DDOS bots doesn't traverse within the site and enter from the same source and exit from the same source having very low click depth ratio.	Undirected subverted calls.
Extreme traffic from a few user agents [9]	There are vulnerabilities in IE which has been reported to produce unexplained spikes however at the same time unknown user agents/bots also request resources leading to chocking of bandwidth.	It leads to degrade network service to cloud users or fully make it unusable during the time it is active.
DOS/ connection time out.	Typically due to flooding of traffic [22]	It can lead to disrupt the normal usage of cloud services and will affect the quality of service as well.

On the basis of research gaps identified from the review study, a novel architecture from securing cloud towards network/application based DDOS attacks is proposed. The proposed approach uses the concept of profiling [23] each cloud endpoint by using remote java script code units which would help us in identification of slow DDOS attack scenario. This research focuses on providing robust monitoring services with minimized cost and is basically a non-intrusive method of observing anomalies. The proposed approach does not require implementation of more resources like firewall, acket sniffers, and intrusion detection systems [29], [32] which require lot of resources. This approach is scalable and compatible with all technologies which use http/https calls [19] for its communication. The Change Point detection Architecture proposed for detection of flooding slow DDOS attacks is illustrated below.

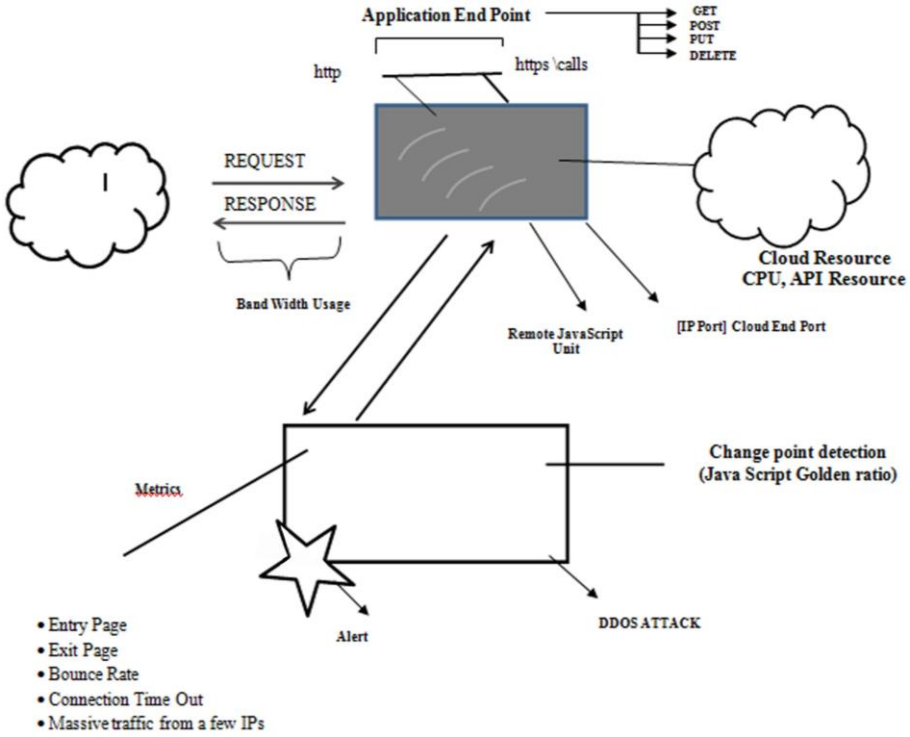

Fig. 3: Change Point Detection Architecture to Detect Slow Flooding DDOS Attack.

4.1. Proposed algorithm

Change Point Detection [31], [35] algorithmic approach for detection of flooding DDOS attacks is illustrated by using the following steps:

Step-I Remote Java Script is to be coded which includes the use of Golden ratio and embedded in the cloud application endpoint to calculate metrics (Table –2). The proposed algorithm is based on the concept of recording, the "change points" i.e. cp in cloud network which work on http(s) protocol. The "change points" are put under observation by using embedded java script code script units. The pseudo algorithm is as follows

i) Number of cloud end points is 'x'.
ii) Number of "change points" is 'cp' which are under observation for where java script is embedded.
iii) Nnumber of views of each change point 'cpi' are 'pv'. The views are created based on the http(s) request-response calls.
iv) Number of visits by cloud user to the "change point" is 'v'.
v) Let 'sae' be the number of single access entry to a 'cp' at given time't'.
vi) So, bounce ratio 'br' is defined as 'when a 'cp' is the 'entry point 'ep' and the cloud user 'cu' does not access any other 'cp'.

br= sae/ no of entries by ' (1)

However, the cloud users 'cu' may be visiting some other 'cp' more often due to navigation compulsions and popularity of the other 'cps' , therefore enhanced method would be

Weighted bounce ratio (Wbr) = (br). (pv/total pv) (2)

For better numerical stability of algorithm, second condition for verification of DDOS attack at particular cloud end point, we can use following metric also.

vii) Entry to exit ratio

Where 'entry rate' is defined as the number of entries/visits done by cloud user with respect to the entry of 'cp' and 'exit rate' is defined as the number of visits/entries by cloud users of 'cp' with respect to the exit percentage.

viii) Count Connection Time out frequency and massive frequent traffic rate from specified selected IPs.

By using above metrics, we can detect the DDOS attacks by using following algorithm:

Let 'f' be the flag (DDOS attack) = false
for each cloud end points
for each 'cp'
calculate

a) 'cp' entry rate
b) 'cp' exit rate
c) 'cp' ratio of (a)/(b)
d) Wbr 'golden ratio' [28]

g_c=0; // g='threshold', c='current'
if (wbr>= 99%) & ratio > 0.9
g_c= g_c+1
flag ='true';
else
flag='false';
end
if (g_c>= g_c previous)
DDOS Attack Alert

end
end
end

Step-II: Golden ratio [28], [31] is to be used for identification of normal and abnormal page view percentages
Step-III: Next is to calculate correlation between the values obtained from Golden ratio and bounce rate, exit rate, weighted bounce rate, connection time-out frequency and massive traffic frequency of selected specified IPs.
Step-IV: Finally, it is to find threshold 'g' ; If, Current threshold >= Previous threshold, 100% DDOS attack by using values obtained from Golden ratio with respect to flag count.

5. Discussion

There are two basic performance measures for the change point detection approach that are False alarm time and Detection time. False alarm time refers to the time duration in which no false alarm reported when there is no attack. Detection time refers to the detection delay after the attack starts. There are various Linux and windows based botnets and malware are sweltering more than 150 gbps of bandwidth which is sufficient enough as adversity to cripple and disrupt many websites in the cloud. Many of the DDOS attacks basically target "connectivity" as such flooding DDOS attacks require less effort by threat actors compared to writing full length malware and conducting long term penetration campaigns to attack a cloud point. The number of potentially bot-reflected devices on the Internet will only continue to rise.

6. Conclusion and scope for future work

Considering the explosive growth of smart phones and 'Internet of Things' (IoT), everything will be networked from small appliances to automobiles and attack susceptible. As the value of cloud connectivity for all devices increases to a greater number of organizations, the services for flooding DOS attack detection and mitigation situations will increase many folds. The proposed algorithm is a non-intrusive, low overhead technique for detection of flooding DDOS attacks occurring at application layer using HTTP protocol. Conventionally, threat actors have utilized TCP (SYN) or UDP floods to consume resources, by sending http 'GET' method requests for exhausting server resources. Hackers created significant latency by targeting 'heavy URLs' that require complex database queries. These attacks are difficult to identify especially in cloud as they rely on logic to cause application latency as per request, rather than just making fold of requests. In such situations the proposed algorithm will be very useful in detecting DDOS attacks. Although there are several software packages which help in monitoring the traffic of mobile and web assets connected to cloud based on the trend of ratio of entry and Exit points and bounce ratios etc., but the use of Change Point detection approach which encompasses composite metric based threshold along with Golden Ratio is helpful in early detection of flooding DDOS attacks mainly which are slow in nature.

References

[1] Chang, Rocky KC. "Defending against flooding-based distributed denial-of-service attacks: a tutorial." Communications Magazine, IEEE 40.10 (2002): 42-51.

[2] Suo, Hui, et al. "Security in the internet of things: a review." Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on. Vol. 3. IEEE, 2012.

[3] El Defrawy, Karim, Minas Gjoka, and Athina Markopoulou. "BotTorrent: misusing BitTorrent to launch DDOS attacks." Proceedings of the 3rd USENIX workshop on Steps to reducing unwanted traffic on the internet. USENIX Association, 2007.

[4] Ankali, Sanjay B., and D. V. Ashoka. "Detection architecture of application layer DDOS attack for internet." Int. J. Advanced Networking and Applications 3.01 (2011): 984-990.

[5] Saleh, Mohammed A., and Azizah Abdul Manaf. "A Novel Protective Framework for Defeating HTTP-Based Denial of Service and Distributed Denial of Service Attacks." The Scientific World Journal 2015 (2015).

[6] Cambiaso, Enrico, et al. "Slow DOS attacks: definition and categorisation." International Journal of Trust Management in Computing and Communications 1.3-4 (2013): 300-319.

[7] Tomar, Kuldeep, and S. S. Tyagi. "HTTP Packet Inspection Policy for Improvising Internal Network Security." International Journal of Computer Network and Information Security (IJCNIS) 6.11 (2014): 35.

[8] M. Richardson, E. Dominowska, and R. Ragno. Predicting clicks: estimating the click-through rate for new ads. In WWW, 2007.

[9] Lam, V. T., et al. "Puppetnets: misusing web browsers as a distributed attack infrastructure." Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006.

[10] Jin, Shuyuan, and Daniel S. Yeung. "A covariance analysis model for DDoS attack detection." Communications, 2004 IEEE International Conference on. Vol. 4. IEEE, 2004.

[11] Alomari, Esraa, et al. "Design, Deployment and use of HTTP-based Botnet (HBB) Testbed." Advanced Communication Technology (ICACT), 2014 16th International Conference on. IEEE, 2014.

[12] Choi, Yang-seo, et al. "Aigg threshold based http get flooding attack detection." Information Security Applications. Springer Berlin Heidelberg, 2012. 270-284.

[13] Choi, Junho, et al. "A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment." Soft Computing 18.9 (2014): 1697-1703.

[14] Genes, Raimund, Anthony Arrott, and David Sancho. "Stormy Weather: A Quantitative Assessment of the Storm Web Threat in 2007." (2011).

[15] Sachdeva, Monika, et al. "Performance analysis of web service under DDoS attacks." Advance Computing Conference, 2009. IACC 2009. IEEE International. IEEE, 2009.

[16] Yang, Jin-Seok, Min-Woo Park, and Tai-Myoung Chung. "A Study on Low-Rate DDoS Attacks in Real Networks." Information Science and Applications (ICISA), 2013 International Conference on. IEEE, 2013.

[17] Chonka, Ashley, and Jemal Abawajy. "Detecting and mitigating HX-DoS attacks against cloud web services." Network-Based Information Systems (NBiS), 2012 15th International Conference on. IEEE, 2012.

[18] Zhang Fengxiang; Abe, S., "A Heuristic DDoS Flooding Attack Detection Mechanism Analyses based on the Relationship between Input and Output Traffic Volumes," in Computer Communications and Networks, 2007. ICCCN 2007.

[19] Chao Liu; Shunyi Zhang, "A Bidirectional-Based DDoS Detection Mechanism," in Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on , vol., no., pp.1-4, 24-26 Sept. 2009

[20] Zhang Dengyin; Liu Yu; Adi, A.; Li Haibo, "Improved R/S Algorithm Based on Network Traffic Self-Similarity," in Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on , vol., no., pp.1-4, 12-14 Oct. 2008

[21] Piggott, P.; Carter, C.; Patterson, W.; Gutierrez, F.; Mujica, S.; Rojas, E.; Valenzuela, C., "Development of an indicator to distinguish DDoS attacks from other anomalous events," in Southeastcon, 2013 Proceedings of IEEE , vol., no., pp.1-5, 4-7 April 2013

[22] Ruoyu Yan; Qinghua Zheng; Guolin Niu; Sheng Gao, "A new way to detect DDoS attacks within single router," in Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on , vol., no., pp.1192-1196, 19-21 Nov. 2008

[23] Sanchika Gupta, Padam Kumar, Ajith Abraham, "A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment"; International Journal of Distributed Sensor Networks, Volume 2013.

[24] Alqahtani, S.; Gamble, R., "DDoS Attacks in Service Clouds," in System Sciences (HICSS), 2015 48th Hawaii International Conference on , vol., no., pp.5331-5340, 5-8 Jan. 2015

[25] Alomari, E.; Manickam, S.; Gupta, B.B.; Singh, P.; Anbar, M., "Design, deployment and use of HTTP-based botnet (HBB) testbed," in Advanced Communication Technology (ICACT), 2014

[26] Soejima, Y.; Chen, E.Y.; Fuji, H., "Detecting DDoS Attacks by Analyzing Client Response Patterns," in Applications and the Internet Workshops, 2005. Saint Workshops 2005. The 2005 Symposium , vol., no., pp.98-101, 31-04 Jan. 2005

[27] Singh Baldev, Panda S.N., Samra G.S., "Detecting and Countering DDOS Attacks"; IJARCSSE, Issue-11, November 2013.

[28] Rohita P. Patil, Shreyansh Daga, Singh M, Nitin L., "Gesture Recognition Engine using Golden Section Search Algorithm for Touch Tables" ; IJECCE, Vol. 5, Issue-4, 2014.
[29] Biegler, L. T. and J. E. Cuthrell, "Improved Infeasible Path Optimization for Sequential Modular Simulators-II: The Optimization Algorithm," Computers & Chemical Engineering.
[30] Cisco Global Cloud Index: Forecast and Methodology 2016-2021;
[31] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html
[32] Baldev Singh, S.N. Panda, "Weighted Bounce Threshold to Detect Slow DDOS Attacks in Cloud", IJSST, Issue-1, Vol. 2, 2014
[33] M. Khoo, Joe Pagano, A .l. Washington, M. Recker, B. Palmer, Robert D., " Using web metrics to analyze digital libraries" ; Conference: ACM/IEEE Joint Conference on Digital Libraries, JCDL 2008, Pittsburgh, PA, USA, June 16-20, 2008
[34] M. Thottan and C. Ji. Anomaly detection in IP networks. IEEE Transactions on Signal Processing, 51(8), August 2003.
[35] Cisco Visual Networking Index: Forecast and Methodolgy, 2016–2021 https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html
[36] B. Krishnamurthy, S. Sen, Y. Zhang, and Y. Chen. Sketch-based change detection: Methods, evaluation, and applications,. In Proceedings of ACM Internet Measurement Conference'2003, Miami, FL, October 2002.
[37] Muhai Li, Ming Li; " A New Approach for Detecting DDoS Attacks Based on Wavelet Analysis", 2009 2nd International Congress on Image and Signal Processing
[38] Yu Chen, Kai Hwang , Wei-Shinn Ku , "Distributed Change-Point Detection of DDoS Attacks: Experimental Results on DETER Testbed"; DETER Community Workshop on Cyber Security Experimentation and Test, in conjunction with USENIX Security Symposium, Boston, MA. August 6-7, 2007.