An Adaptive Approach to Mitigate Ddos Attacks in Cloud

Baldev Singh
Research Scholar
IKG Punjab Technical University
Jalandhar, India

S.N. Panda
Director (Research)
Chitkara University
Rajpura, India

***Abstract*—Distributed denial of service (DDOS) attack constitutes one of the prominent cyber threats and among the hardest security problems in modern cyber world. This research work focuses on reviewing DDOS detection techniques and developing a numeric stable theoretical framework used for detecting various DDOS attacks in cloud. Main sections in the paper are devoted to review and analysis of algorithms used for detection of DDOS attacks. The framework theorized here deals with the variability calculation method in conjunction with sampling, searching methods to find a current state of a particular parameter under observation for detecting DDOS attacks. This way a solution is to build that measure the performance and conduct the monitoring framework to capture adversity related to DDOS attacks. The described algorithm intends to capture the current context value of the parameters that determine the reliability of the detection algorithm and the online pass algorithm helps to maintain the variability of those collected values thus maintaining numerical stability by doing robust statistical operations at endpoints of traffic in cloud based network.**

Keywords*—DDOS attack; Intrusion detection; Threshold; Cloud; virtual machine

I. INTRODUCTION

Internet of Things (IoT) has evolved in modern times in leap and bounds. Incidents of attacks over the Internet especially DDOS attacks [1] are increasing day by day. News are dominated by successful DDOS attacks against a number of major Fortune 100 organizations in this arena. Hence, many security experts have being thinking on how does Organized Fraud Rings (OFR's) make money out by disrupting the information technology (IT) assets of a company? How can we detect and disrupt this activity? [28,29] Historically, the fragmented organizations that unwittingly constitute this "fraud supply chain" could provide no coherent indication of suspicious activity. Each step could only be observed in isolation. However, solutions are now available to correlate events across the multiple disparate systems involved to join the dots and see the complete picture.

Centralized collection of activities through every phase of the disruptive activity like DDOS attack [1] process can identify and alert on suspicious patterns and stop it in its tracks, even where evasive techniques such as geographical dispersion and Internet service provider (ISP) switching are employed. The purpose of the DDOS attack [3] is normally about breaking the business continuity. Hence, there is a need to build a mechanism on identifying the correlation of activity and transaction velocity of DDOS Attack. The existing network security mechanisms confront new challenges in the cloud [2] such as virtual machine intrusion attacks [4,5] and malicious user activities. Hence, new security methods [6] are required to increase users' level of trust in clouds. Presently, cloud service providers implement data encryption for the data centers, virtual firewalls and access control lists.

The number of threat vectors in today's cloud landscape [7] is increasing day by day that is the problem. The existing detection approaches are not foolproof. There is need to learn more about attackers and adopt an adaptive approach to defense at every stage. This can happen only if the algorithm of detections must be adaptive and numerically stable. There is need to focus on methods on how to gather threat Intelligence about our adversaries and know the motives of malicious attacker?

The cloud based networks [16] and services are prone to suffer from malicious attacks because of their inherent characteristics of being accessible globally any time and also due to the frequent changes in topology and development of IoT as well as because of landscape nature of Internet. Of particular concern, it is the denial of service attacks that makes the service unavailable to its intended cloud users. In fact, there are three major techniques which are: misuse detection, anomaly detection and specific detection like DDOS attack. Each of these detection methods has its pros and cons. These are however, reviewed in the Related Work section. But from the current incidence reports it is clear that new combinational methods need to be implemented for the proper working of cloud industry. It is known fact that both the internal and external anatomy [8] of the data-center matters, how it is structured architecturally to measure the volume of traffic is also the main critical point, if somehow the intruders are able to launch a slow attack it must be detectable or if it is a sudden flood of packets then the system must be able to mitigate the flood to have clean traffic. This is not possible unless there is continuous monitoring which includes the mapping of threats [18] cope with the understanding correlations of all the factors contributing to the adversity. Therefore, the thresholds of finding inflection points where the traffic changes to malicious is essential to successful running of data centers in cloud in thwarting the DDOS attacks.

The rest of this paper is as follows. Section II studies a couple of related works in detection and defense mechanism of DDOs attacks. In Section III, the main research gaps in the

reviewed work are highlighted. Section IV contains the threshold calculation mechanism required for DDOS attack detection. Section V summarizes the shortcomings of already contributed work. In Section VI, some concluding remarks are given and finally the future scope of study is briefed in Section VII.

II. Related Work

Due to mammoth size of network and IoT, there are various types of vulnerabilities in cloud based network. The impact of adversity on the cloud based network is not easy to estimate due the dynamic attributes of the system dynamics. These dynamics force us to think on developing various mathematical models based on which the adversity may be captured. Since, all these methods are based on mathematical model of DDOS threat detection and when they are put to test against the real life scenarios, their performance comes into question. Hence, this area of research explores many possibilities to mitigate the DDOS attacks. The Intrusion detection systems (IDS) [24, 25, 37] were first implemented as frugal, optional mitigation mechanisms but with Big Data technologies the direction of the industry to implement a permanent robust solutions at all ends of the network including ISP and customer end is now propagated. This leads to scenario where normal detection techniques using static values rendered becomes useless and as per our systematic review of related works in the field of intrusion/malicious attack detection [9,18], there are variety of mechanisms that can be used to detect anomalies or malicious behavior in the cloud based network. Each of these techniques/mechanisms discussed here are threshold basis and have their own pros and cons. A summary of some related literature that holds trade-offs in its favour, is presented in this section.

In [10] Static threshold based intrusion detection systems were proposed by Kim et al. (2004), Gates and Damon (2005), Leckie et al (2002) and Faizal et al (2009). Network IDS technique proposed by (Abdollah, Masud, Shahrin & Robiah, 2009) has used the concept of static threshold, although dynamic threshold is better solution. Threshold value is selected to take decision in identifying the DDOS attacks. It is the basic unit that differentiates between the normality and abnormality in the traffic over the cloud based network. In this static threshold method, a cutoff is fixed which decides the normal and abnormal levels. The basic features used in detection of attacks are mainly IP address of the victim machine, timestamp, time-duration of connection, protocol used, connection status flag, and source & destination services.

The threshold is used to differentiate between normal traffic and abnormal traffic [17] in the network. This threshold value is acquired by using observation and experimental technique and the verified by using statistical process control approach [13]. Although static threshold methods are easy to implement for detection as well and have low computational complexity but the main weakness of this method is that fix value range is never close to real systems and are changing with respect to time. This method does not take into account the differential or cumulative threshold which given better response to adversity in real time.

In [15] Proactive DDOS attack detection and defense mechanisms propound by Keromytis, Misra & Rubenstein 2002. It focuses on the advance detection of attacks. In reactive mechanisms, detection the attacks is by using signatures (attack pattern) or anomaly behavior. Proactive mechanisms emphasize on to improve the reliability of the global Internet infrastructure by adding additional functionality to Internet components to detect and defend various attacks as well as vulnerability exploitation. The main objective of this approach is to make the infrastructure resistant to the attacks and to provide service to normal users continually under extreme conditions.

Reactive defense approach was suggested by Ioannidis & Bellovin 2002. Third-party Intrusion Detection Systems (IDS) are deployed to obtain attack related information and then action is taken according to this information. Various strategies are used for intrusion detection purpose. If the IDS system unable to detect the DDoS attack packets, then filtering mechanisms are used, that are able to filter out the attack stream completely, even at the source network. A rate limit is imposed by the IDS on the stream to characterize that the stream is malicious.

In [13], Dynamic threshold based approach is proposed by Gupta, Sanchika, Padam Kumar, and Ajith Abraham. [13] Paper addresses to vulnerabilities responsible for known attacks on cloud and analyzed various measures to secure cloud based network from these malicious attacks both insider and outsider. A profile is created for each machine to detect and prevent various cloud attacks. In this approach, the estimation of upper and lower cutoff points are figured after some time period, after every time slot, the value may change. However, there is not much difficulty in implementation of various methods of calculations like method based on average, mode, frequency, deviation from mean. But this method cannot handle extreme high and low values statistically that may cause to wrong calculations (numerically unstable) as change point detection method may calculate wrong threshold, thereby increase the false alarm rate.

[11] B. B. Gupta, R. C. Joshi, M. Misra proposed "Dynamic and Auto Responsive Solution for Distributed Denial-of-Service Attacks Detection in ISP Network," In this paper, they presented a framework which emphasize on characterization of a wide range of flooding DDOS attacks [32] and their detection. As per [11] flooding attacks are because of high rate disruptive, diluted low rate degrading and varied rate and there should be monitoring of the propagation of abrupt traffic changes inside ISP network. [11] suggested that a profile of the traffic normally seen in the network is to be created, and then anomalies are detected whenever traffic goes out of profile. Although they claimed that the said detection system is scalable to varying network conditions and adapts itself to different attacks [19] loads but to identify threshold values detection mechanism is not free from generating false positive alarm rates and hence not foolproof for detection of malicious flows characterization.

In [37], C. Modia, D. Patela, B. Borisaniyaa, H. Patelb, A. Patelc, and M. Rajarajanc in their paper, "A survey of intrusion detection techniques in cloud," are really of the

opinion that the existing Intrusion Detection Systems and Intrusion Prevention Systems for cloud environments are short of feasible solution. The authors explained that the explored solutions of IDS are still far from the integration in the clouds. They suggested that these must be combined with security information and event management in addition to adopting additional security measures and correlation rules to identify internal attacks or to be prepared for zero-day attacks. They made stress on the necessity of the centralized view in monitoring IDS and making advancements in existing solutions with competence to examine data stream by scaling up and down.

[14] Jun-Ho Lee, Min-Woo Park, Jung-Ho Eom, and Tai-Myoung Chung in their paper "Multi-level intrusion detection system and log management in cloud computing" proposed multi-level IDS in combination with log management approach to strengthen the security in cloud based network so that anomaly behavior can be detected in cloud environments. In this approach they are of the view that more rules and patterns are proportionate to the strength of the security in cloud computing provided that proper logs are to be administered. It is based on the quantification of risk levels and assigning risk points in proportion to risk anomaly behavior. Although the approach is fully quantitative in nature which is significant in any corporate security risk program but the main thing is that more the rules and patterns, more will be the complex and slow IDS in cloud computing.

III. Research Outline

The major gaps are found on the basis of review study and its findings are as follows:

- It is difficult to judge the point of inflection or point change which can reflect the abnormal behavior due to DDOS attack.
- It is difficult to sometime identify the end points of cloud from where the DDOS attack is creating problem.
- It is hard to identify the intensity of attack, if the attack is slow in nature and has discrete events occurring based on demand cloud services.
- It is difficult to calculate accurately the thresholds of parameters that can reflect DDOS attack behavior as ranges may changing with patterns difficult to comprehend.

Pseudo code to detect DDOS attacks in Cloud based network: Following are the proposed steps to detect DDOS attacks in cloud based network:

- Measure normal traffic Volume
- Measure normal traffic Flow
- Upper bound of Threshold value for Volume
- Measure threshold value for Flow
- Measure lower bound of threshold value for Volume
- If attack pattern is detected due to flooding attacks, generate DDOS attack alert.

IV. Mechanism to Compute Threshold for Ddos Detection

An 'abnormality' may be found while observing a particular network factor. It is either the values of parameters that start touching abnormal 'lows' or 'highs' at certain 'intervals' of data series or values of parameters start scaling higher values from the normal scale. There is variance [36] which indicates the abnormality. It is more suitable to use online algorithm in cases where cost of computation is sensitive to the response time of an operation. Moreover, the method of (SEM) Structured Equation Modeling [23] which is mainly used to test conceptual/theoretical model, intends to identify an equation that defines a sequence of values between two or more parameters under observations for DDOS detection, based on time series sampling and then further sample for threshold value based methods.

(a1) *Pseudo code of Online Algorithm to compute variance for n samples:*

```
For defined timeline;
N=0; Mean=0;
M2=0;
Data=[];
For x in Data
N=N+1;
Delta=x-Mean;
Mean=Mean+ Delta/n;
M2=M2+Delta*(x-Mean)
If(n<2)
Return 0;
Variance=M2/(n-1)
End.
```

(a2) *Empirical rule:* The empirical rule [20,21] (Three Sigma rule) states that for a normal distribution, nearly all of the data will fall within three standard deviations of the mean. The empirical rule can be broken down into three parts:

- 68% of data falls within the first standard deviation from the mean.
- 95% fall within two standard deviations.
- 99.7% fall within three standard deviations.

Check 'Empirical Rules as if:

a) 68% values within the first standard deviation values
b) 95% values within two standard deviation values
c) 97% values within three standard deviation

then attack flag='true' else attack flag='false';

(a3) *Area Elimination Method*

Let there be 2 points x_1 and x_2 which lie in the interval (a,b) of the sample extracted at any given time for analysis and satisfy ($x_1<x_2$), hence the three rules:

i. If $f(x_1)>f(x_2)$ then the threshold does not lie in (a,x_1)
ii. If $f(x_1)<f(x_2)$ then the threshold does not lie in (x_2,b)
iii. If $f(x_1)=f(x_2)$ then the threshold does not lie (a,x_1) and (x_2,b).

First Rule Scenario:

If the function value at x_1 is larger than that at x_2, threshold point x cannot lie on the left side of x_1.

Second Rule Scenario:

If the function value at x_1 is less than x_2, the threshold point 'x' cannot lie in right side.

Third Rule Scenario:

When $f(x_1)==f(x_2)$, implies that there is one lowest or highest value that can be taken as threshold. Hence R_1 and R_2 areas are eliminated.

Golden Ratio method

Golden Ratio method [20], may be used as golden ratio pattern is also found in nature extensively, the 'abnormal' threshold values may be captured using golden ratio interval division method.

The sample search space (a,b) is first linearly mapped to a unit interval search space (0,1) and then two data points [22] at τ from either end of the search space are chosen so that at every iteration, the elimination region (1-τ) to that in the previous iteration is covered. This can be achieved by equaling (1-τ) with (τ x τ). This yields the golden number τ=0.618.

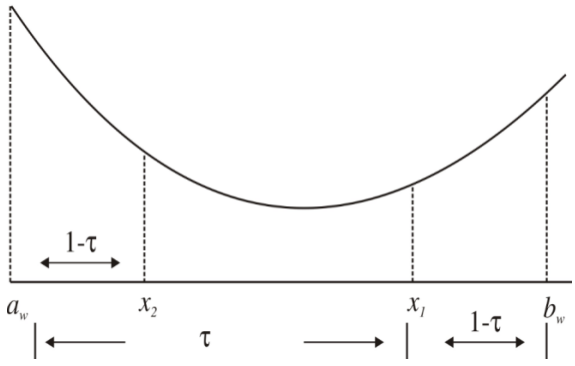

Fig. 1. Golden Ratio points (x1 and x2)

Algorithm: DDOS data under observations is divided into golden ratio parts.

Step 1:

Choose a lower bound *a* and an upper bound *b*. using Synthetic Division method [21,22]. Set small value ϵ. Normalize the variables 'x' by using the equation

ω=(x-a)/ (b-a).

Thus aω= 0, bω=1, and $\ell\ \omega$=1, set k=1.

Step 2:

Set ω1=aω+ (0.618) $\ell\omega$

ω2=bω - (0.618) $\ell\ \omega$.

Compute f(ω1) or f(ω2)

Apply the basic Area elimination method [a3].

Step3 :

Is $|\ell\omega| < \epsilon$

If no, set k=k+1, goto Step 2;

Else Terminate.

Step 4:

Online algorithm as in section [a1]

Step 5:

Check 'Empirical Rules' as in section [a2]

If large no of outlier form

Attack='true'

Else

Attack='false'

End;

The number of function evaluation 'n' required for achieving a desired accuracy, ϵ is calculated by solving the following equation

$$(0.618)^{n-1}=(b-a)< \epsilon$$

V. Discussion

There is plethora of methods to overcome the issue of rise in DDOS attacks and have understood that it affects their overall eco-system of conducting 'Business on Internet or Cloud'. These algorithms offer various degrees of stability, reliability in their working. The latest findings, occurrences, incidence reports [33] on DDOS attacks suggest that these methods still need a deeper examination as inadequate interpretations are done. Bandwidth [30] is one way to measure DDOS attacks including application layout attacks. Our solution also checks periodically the DNS TTL of all the DNS associated with our cloud endpoints. The ratio of abnormal data to the normal data will normally be imbalanced so the golden method tries to compensate this imbalance. The proposed method as discussed above is also better as real time information of deviation may not be possible every time due to inherent nature of data stream analyzed at any given time. This method is based on capturing abnormality at certain logical intervals. If a particular 'current' threshold or current value of the objective function, defined by well defined relationship, occurs above 'normal range' successively in multiple intervals during evaluation, there is high possibility that the network is going under 'adversity'. Care has been taken to evaluate the successive function evaluation values whose average does not go far away from the mean using robust online algorithm. The method has advantage in the sense that it checks the well defined mathematical relationship

between two variables that influence the performance of network under 'adversity' using structure equation modeling.

VI. Conclusion

Today we have entered a world where cyber enemy politics [31], cyber terrorism, cyber hacktivism have taken over cyber crime space or attack landscape. Now, DDOS attacks can also be launched from phone, in fact nearly any kind of device with IP address can launch DDOS attacks. Network level DDOS attacks typically require IP-threat level assessment strategy to safeguard against DDOS attacks. Reflective DDOS attacks[12] need 'state flow' awareness strategy for Outbound DDOS attacks and in case of Bi-direction flood detection [26], the strategy with algorithms having numerical stability is required. In fact, our proposed algorithm can also cover those kinds of DDOS attacks which involve 'specially crafted 'packet attacks, where protocol analysis reveals the correct situation in conjunction with threshold techniques discussed in Section-III**.** Other than the DDOS attacks that involve Recon (Scan) [26] or that involve highly advanced evasion, detection requires further advanced methods in this context. The latest Gartner report suggests that application layer level DDOS attacks account for maximum incidences (25%) which requires behavioral analysis techniques due to multifold increase in DDOS attacks[33]. It is also evident that today's service provider solutions cannot avoid analysis of protocol behaviour, volume, type of traffic for its survival. In summary, the proposed work covers following aspects to break into the anatomy of DDOS attacks. It covers the numerically stable calculations of DDOS attacks that impact network level Flow Volumetric attacks [38].

1) Proposed method covers the attacks initiated as "randomized" ,'slow' and 'low' [30,35] at application layer. The method proposed do calculations based on application's traffic end points also, where, 'payload' matching or entropy [27] based methods become useless due to high pattern variations.

2) Deploy multi stage algorithm [34] that can block spectrum of unwanted traffic as well as dynamic unwanted users. This way detection becomes more effective.

3) However, support from other components of defense mechanism shall also be solicited which include keeping an eye on application users and unwanted activities or simply enforcing usage standard, enforcement of protocol anomalies and violation by enforcing RFC and industry standards.

VII. Future Scope

The proposed solution can easily be integrated into big data analysis based solutions as it allows scalability where application of machine learning algorithms may also help. For future work, it is suggested that SEM may be used for threat modeling of DDOS attacks along with column based data mining algorithms, which use partial probability theory for detection of DDOS attacks in cloud based network.

References

[1] Bing Wang, Yao Zheng, Wenjing Lou, Y. Thomas Hou, "DDoS attack protection in the era of cloud computing and Software-Defined Networking," Computer Networks, Volume 81, 22 April 2015, pp 308-319, ISSN 1389-1286.

[2] Iankoulova, I., Daneva, M. "Cloud computing security requirements: A systematic review" in Research Challenges in Information Science (RCIS), 2012 Sixth International Conference; 2012.

[3] DDoS attacks on the rise – by criminals and spies, Network Security, Volume 2014, Issue 2, February 2014, Page 2, ISSN 1353-4858.

[4] Danny Bradbury, "The problem with Bitcoin," Computer Fraud & Security, Volume 2013, Issue 11, November 2013, Pages 5-8.

[5] Steve Mansfield-Devine, The evolution of DDoS, Computer Fraud & Security, Volume 2014, Issue 10, October 2014, Pages 15-20, ISSN 1361-3723.

[6] P. Varalakshmi, S. ThamaraiSelvi, "Thwarting DDoS attacks in grid using information divergence", Future Generation Computer Systems, Volume 29, Issue 1, January 2013.

[7] Pitropakis Nikolaos, Anastasopoulou Dimitra, Pikrakis Aggelos and Lambrinoudakis, Costas," If you want to know about a hunter, study his prey: detection of network based attacks on KVM based cloud environments", Journal of Cloud Computing,Vol 3, 2014.

[8] Ben-Porat, U.; Bremler-Barr, A.; Levy, H., "Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks," IEEE Transactions on Computers 2013, , vol.62, Issue 5.

[9] Dit-Yan Yeung, Yuxin Ding,"User Profiling for Intrusion Detection Using Dynamic and Static Behavioral Models," Springer Berlin Heidelberg, 2002.

[10] Faizal M.A., Zaki M.M., Shahrin S., Robiah Y., and Rahayu S.S., (2010) "Statistical Approach for Validating Static Threshold in Fast Attack Detection," Journal of Advanced Manufacturing Technology, Vol. 4, 2010.

[11] B. B. Gupta, R. C. Joshi, M. Misra, "Dynamic and Auto Responsive Solution for Distributed Denial-of-Service Attacks Detection in ISP Network," International Journal of Computer Theory and Engineering; pp. 71-80, 2009.

[12] WeiWei; Feng Chen; Yingjie Xia; GuangJin, "A Rank Correlation Based Detection against Distributed Reflection DoS Attacks," Communications Letters, IEEE , vol.17, no.1, pp.173,175, January 2013.

[13] Gupta, Sanchika, Padam Kumar, and Ajith Abraham. "A profile based network intrusion detection and prevention system for securing cloud environment."*International Journal of Distributed Sensor Networks* 2013 (2013).

[14] L. Jun-Ho, p. min-Woo, E. Jung-Ho, C. Tai-Myoung, " Multi-level intrusion detection system and log management in cloud computing", *Proceedings of the 13th International Conf. pp. 552–555, Feb.* 2011.

[15] Guangsen Zhang and Manish Parashar , "Cooperative Defence against DDoS Attacks" Journal of Research and Practice in Information Technology, 2006.

[16] S. Qaisar and K. Khawaja, "Cloud computing: network/security threats and countermeasures", Interdisplinary Journal of Contemporary Research In Business Volume 3, January 2012.

[17] Kollias, S.; Vlachos, V.; Papanikolaou, A.; Chatzimisios, P.; Ilioudis, C.; Metaxiotis, K., "A global-local approach for estimating the Internet's threat level," Journal of Communications and Networks, vol.16, no.4, pp.407,414, Aug. 2014.

[18] Vasanthi, S.; Chandrasekar, S. (2011), "A study on network intrusion detection and prevention system current status and challenging issues". *Advances in Recent Technologies in Communication and Computing* (ARTCom 2011), 3rd International Conference on , vol., no., pp.181,183, 14-15.

[19] Monowar H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya and J. K. Kalita (2013),"Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions", *The Computer Journal.*

[20] Deb, Kalyanmoy: Optimization for engineering design: Algorithms and examples". PHI Learning Pvt. Ltd., 2012.

[21] Aufmann, Richard, and Joanne Lockwood: *Introductory and Intermediate Algebra: An Applied Approach.* Cengage Learning, 2013.

[22] Scherer, Philipp OJ. "Roots and Extremal Points," In Computational Physics Springer International Publishing", pp. 83-111, 2013.

[23] Hoyle, Rick H.: *Handbook of structural equation modeling*. Guilford Publications, 2014.

[24] Xinya Wu; Yonghong Chen, "Validation of Chaos Hypothesis in NADA and Improved DDoS Detection Algorithm," *Communications Letters, IEEE*, vol.17, no.12, pp.2396-2399, December 2013.

[25] Chun-Jen Chung, Khatkar, P., Tianyi Xing, Jeongkeun Lee, Dijiang Huang, "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems," IEEE Transactions on Dependable and Secure Computing, vol.10, no.4, pp.198,211, July-Aug. 2013

[26] Wang Jin, Zhang Min, Yang Xiaolong, Long Keping, Xu Jie, "HTTP-sCAN: Detecting HTTP-flooding attack by modeling multi-features of web browsing behavior from noisy web-logs," China Communications, vol.12, no.2, pp.118,128, Feb. 2015

[27] Xinlei Ma; Yonghong Chen, "DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy," IEEE Communications Letters, vol.18, no.1, pp.114,117, January 2014

[28] Shui Yu; Yonghong Tian; Song Guo; Wu, D.O., "Can We Beat DDoS Attacks in Clouds?" IEEE Transactions on Parallel and Distributed Systems, vol.25, no.9, pp.2245,2254, Sept. 2014

[29] Anwar, Z.; Malik, A.W., "Can a DDoS Attack Meltdown My Data Center? A Simulation Study and Defense Strategies," IEEE Communications Letters, vol.18, no.7, pp.1175,1178, July 2014

[30] Geva, M.; Herzberg, A.; Gev, Y., "Bandwidth Distributed Denial of Service: Attacks and Defenses," Security & Privacy, IEEE , vol.12, no.1, pp.54,61, Jan.-Feb. 2014

[31] Paulo Shakarian, Jana Shakarian and Andrew Ruef, Chapter 6 - Cyber Attacks by Nonstate Hacking Groups: The Case of Anonymous and Its Affiliates, In Introduction to Cyber-warfare, edited by Paulo Shakarian, Jana Shakarian, Andrew Ruef, Syngress, Boston, 2013, Pages 67-110.

[32] Jingtang Luo, Xiaolong Yang, Jin Wang, Jie Xu, Jian Sun, Keping Long, "On a Mathematical Model for Low-Rate Shrew DDoS," IEEE Transactions on Information Forensics and Security , vol.9, no.7, pp.1069,1083, July 2014

[33] Akamai's Prolexic Security Engineering and Research Team (PLXsert)," Four-fold increase in DDoS attacks," Network Security, Volume 2014, Issue 11, November 2014, Page 2, ISSN 1353-4858, http://dx.doi.org/10.1016/S1353-4858(14)70107-2.

[34] Fei Wang, Hailong Wang, Xiaofeng Wang, Jinshu Su, "A new multistage approach to detect subtle DDoS attacks, Mathematical and Computer Modelling", Volume 55, Issues 1–2, January 2012, Pages 198-213, ISSN 0895-7177, http://dx.doi.org/10.1016/j.mcm.2011.02.025.

[35] C. Balarengadurai, S. Saraswathi, "Comparative Analysis of Detection of DDoS Attacks in IEEE 802.15.4 Low Rate Wireless Personal Area Network", Procedia Engineering, Volume 38, 2012, Pages 3855-3863, ISSN 1877-7058, http://dx.doi.org/10.1016/j.proeng.2012.06.442.

[36] "Algorithms for calculating variance"; https://en.wikipedia.org/wiki/Algorithms_for_calculating_variance

[37] C. Modia, D. Patela, B. Borisaniyaa, H. Patelb, A. Patelc, and M. Rajarajanc, "A survey of intrusion detection techniques in cloud," Journal of Network and Computer Applications, vol. 36, issue 1, pp. 42–57, 2013.

[38] Jisa David, Ciza Thomas, "DDoS Attack Detection Using Fast Entropy Approach on Flow- Based Network Traffic", Procedia Computer Science, Volume 50, 2015, Pages 30-36, ISSN 1877-0509

[39] S.N. Panda, Singh Baldev, "Defending Against DDOS Flooding Attacks- A Data Streaming Approach", International Journal of Computer & IT (Print Journal), 2015.