Volume 6, Issue 7, July 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cloud Security Issues: Counter DDOS Attack by Integrating IP Monitoring and Routing Protocol

Tanshu Gairola[1], Kulvinder Singh[2]
Mtech, Department of Computer Science, Uttarakhand Technical University, India[1]
Assistant Professor, Department of Computer Science, Doon Institute of Engineering and Technology, India[2]

Abstract— Cloud computing is the well-known services and popular in wide spread because of the services like speed, ubiquitous computing, huge storage facility provided by third party etc. However Security issues or dares are still surrounded by various complications threats .Attacks on user services associated with network communication or any data storage services are a part of each internet using customer's life. There are various types of attacks in cloud computing that deal with numerous technique and methodologies to prevent, detect or to avoid those attack. This Thesis focuses on methods to discover the denial of service or Dos and DDos attacks by performing CUSUM algorithmic that known as cumulative sum algorithm. These attack are initiated by the zombie computer sometime called botnet system, these botnet or zombie system are the infected computer over internet. these zombie system or botnet system work on DDOS attack by making a service of legitimate user inaccessible that result in availability issue of services over cloud network. Once the occurrence of attack recognize by using IP monitoring algorithm that referred the use of cusum algorithm we further studies for another attacker detection method that is use ad hoc on demand vector routing protocol to find the actual attacker and by eliminating them reduce the disturbance in communication channel to process the service of a legitimate user . By applying the first method one get the knowledge of occurrence of attack but then to find out the actual attacker or the evil nodes here we take a help of ad-hoc on demand vector protocol. By using simulations the performance of the method in several attack situations have shown, that display a better detection by sensing a much wider range of occurrences of attack.

Keywords— Cloud Computing, WSN, Counter methods, Cusum, Router, DDOS attack, Flooding.

I. INTRODUCTION

Cloud computing has turn into well-known or popular in recent years because of the services like speed, ubiquitous computing, huge storage facility provided by third party etc. However Security issues or dares are still surrounded by various complications threats. Attacks on user services associated with network communication or any data storage services are a part of each internet using customer's life. There are various types of attacks in cloud computing that deal with numerous technique and methodologies to prevent, detect or to avoid those attack. Here we focus on the attack related to the availability of service that occur in network or application level of cloud computing models that is Saas (service as service), Paas (Platform as service) and Iaas (Infrastructure as a service).This attack is well known as denial of service attack(DOS) or distributed denial service of attack(DDOS).the issue with this attack is related to the availability problem .the concern with Dos or DDOS and cloud computing is an increase in a bushiness enterpriser's risk network level due to huge usages of resources externally. Distributed DoS attacks stance an interesting trade-off to the facilities presented on cloud, self-sufficiently of the facility defense definite by the cloud provider. Botnets are being so much in used and increasingly do creative ways to deny service, which sorts it much more problematic to decide this sort of attack. Furthermore, current attackers do not want to attack all-inclusive organization. They can pick the peak resource-intensive application that are in succession on the cloud plus use low-bandwidth attacks to earnings or access to that package. Co-location poses extra exceptional threats. When cloud services belong to a cloud provider, there is necessity to worry not only about attacks on cloud resources, but on the resources of further tenants.

On the other hand, cloud computing compromises unique openings to recuperate rapidly from DDoS attacks because a provider has the capability to quickly providing resources. If the alertness of the cloud can actually derive into performance during a DDoS attack, one should escape to use changeable capacity to serve an enormous expanse of undesired traffic because it may affect a high in bill price from cloud provider, even greater than the cost of the attack itself. As the amount of linked devices increase day by day, the issue of privacy and security service also getting high. And the DDOS attack risk too.

A. Distributed Denial of Service(DDOS) attacks

A denial of service Distributed Denial of Service (DDoS) is the launched by large number of distributed attacker simultaneously disturb the services of the valid legitimate customers and disproportionately consume the target resources to make a condition of un availability that is to stops the server from replying to legitimate customers. Distributed Denial of Service attacks (DDoS) are the one of the most important attacks to avoid the uninterrupted performance of Internet service considered [5]. DDoS attack basically means sheeting down the more loads on a server that can be victim

© 2016, IJARCSSE All Rights Reserved

computer or target one and make them engaged by necessarily using of resources like bandwidth, CPU, database, memory, system bandwidth and other type of resources for serving a requesting application of user, As usual serving to the users because of the high capacity of dealing out or the so-called overkill operation of server, compromised or unavailable.

Nature of this attack includes denial numbers of packages via (DoS) or more (DDoS) car to inactivate the work out power and n/w resources or allow object car set. DDoS attacks are more influential and analysis and covenant with them is more problematic from DoS attacks. Because in these attacks, numerous machines can be incorporated in direction to set the lesser flow of traffic into the demanded machine which accomplish of the entire traffics for the objective machine is problematic. An enormous number of compromised nodes attack to similar target system that will be directed to denial of target system service in an attack DDoS. In point, this type of attacks originated by means of botnet of infested machines that inappropriately by growing the quantity of hosts at risk; don't have necessity to notice attack traffic beginning from some source of DDoS attack as independently to make a dominant attack.

II. ADDRESSING DDOS ATTACK IN CLOUD AND DETECTION METHODS

Cloud computing has developed a data-haven today. Due to its relaxed accessibility and compact price, it is one of the extensively used means to collection of data in most of the IT firms. Cloud computing, though, rest on totally on Internet connectivity, Internet scheme, tactlessly, does not have the high ranks of expected security. Distributed Denial of Service attack, broadly known as DDoS attack, is the key threat to cloud computing. DoS attacks have been everywhere for years, but they've expanded prominence once more and credit goes to cloud computing for the reason that they often affect obtainability. Systems may slow to a crawl or merely time out. And same with the DDoS attack which major distress to the obtainability. DoS and DDoS both are type of denial-of-service threats attack. The attacks evolve by demanding so many resources from a server that the server cannot answer to sincere requests. The attacker can prominently degrade the excellence or fully collapse the of victim's network connectivity. A DoS is an attack that initiates from a single device. A distributed DoS (or DDoS) contains nasty traffic from multiple devices. The DDoS attacks try to create the online data inaccessible by readdressing irresistible traffic, from numerous resources. The movement of the attacks is changing through quarters. Here we emphasis on DDOS attack. DDoS and DoS attacks are simple to implement by attacker or hacker but more difficult to prevent. In detection technique from a combination of anomaly detection algorithms to detect attacks to find out situation of attack occur and then to identified the actual attacker the ad - hoc on demand router protocol review here. DDOS or Dos attack, that creates a condition of congestion in the cloud or any network by overburdening of applications for the cloud service provider, that the reason why reorganization of DOS & DDoS attacks is crucial in reasonable conditions as dangerous ones are easily distinguishable. These are the categorized of attack launched by individual or number of infected system for the perspective of destroy the services of legitimate user by stooping the valid user from accessing any services authorized to him.

Distributed denial-of-service (DDoS) attacks a critical threat to n/w security. There have been several of methodologies and tools invented to discover DDoS attacks and decrease the harm they give. Still, many of the approaches cannot concurrently attain:

- Efficient discovery with a small number of fake alarms
- Transfer of packets in a Real-time.

III. METHODS TO COUNTER DDOS ATTACKS

Here we studies basically two type of detection approach. This detection technique first follow monitoring algorithm where the main motive is to find out that if the new IPs are the source of DDOS attack by initialize the procedure with an IP address monitoring architecture.

Overview of Steps of procedure is like:

- A trained engine that adds IP's to records.
- A trained engine that collects the IP's for a time interval Δ.
- Comparing the records with source IP's in an interval Δ, we can trace new IPs.
- First monitor the mean value of new IPs every fixed time period. Let's have Xn % of new IPs in a time interval of Δ. It is assume that mean value for any new IP sequence is negative while in normal conditions and becomes positive while changes occur. Suppose Xn (random sequence) transforms to NewXn after a change in constant β. So NewXn=Xn+β.During an attack, the major part of the values of the sequence must be negative during normal conditions. The parameter β must be adjusted according to the network conditions as a threshold for attacks detection.

The another method basically refer as mitigation technique that take place once there is knowledge of the occurrence of ddos attack; the next step that come in mind is to find out the actual attackers , there is need to take help of Ad-hoc On Demand Vector protocol. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up-to-date and to prevent routing loops.

- As transmission starts it will search for all the intermediate nodes and send data to it.
- The intermediate node failed forwarding the probe message to the next node;
- It will check the RESPONSE time for the intermediate node If (Response Time> Threshold) it says that there is a probability of a malicious node in that route. Source then sends a fake request message on the same route asking for acknowledgement, once it receives the acknowledgement, it can block that specific id tagging as malicious.

© 2016, IJARCSSE All Rights Reserved

Above methods deal with the following levels:

- Specifying the attacker and legitimate user.
- Recognized attack by cusum algorithm.
- Apply Ad-hoc On Demand Vector protocol to find out the actual attacker.

A. Review Scheme and methodology

1) Source IP Monitoring:

- Monitoring the IP address first than add all those IP address into the IP address database in time when traffic is normal .this all done by a trained engine.
- All IP should store in Δ time interval that sometime known as detection resolution.
- Analyses of traffic volume to identified if any sign of attack seem.
- Acquire the quantity of upcoming IP in Δ time interval and compare it to the previous set of IP

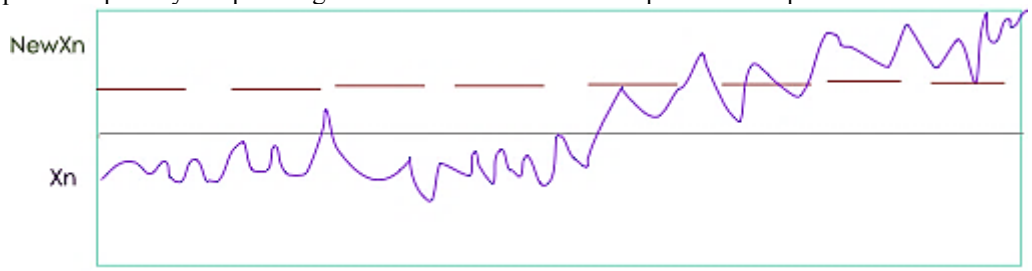

Fig 1 During an attack variation of the percentage of new IP

Commonly three traffic conditions exist here:

- With no traffic –no attack –no network congestion.
- Many legitimate users try to access the service simultaneously.
- Highly distributed denial of service attack.

The source IP monitoring referred the use of cumulative sum algorithm.

Cusum Algorithm: This Basically CUSUM deal with the fact that if there is any variation in value occurs, the probability distribution of the random sequence will modify .CUSUM is Cumulative Summation for applying cusum on N no of observations where it observe user behaviour that is user behaviour pattern to access database with previous legitimate user.[43]

- Assume initial avg av 1 -> N =0; Sum p=Sum till earlier noted =0;
- For loop n=1 -> N ,Sum p =sum p (earlier) + Present (n)
- Av (n) = (sum p/N)
- End for loop statement. Now av is the CUSUM avg and dissimilarity in two consecutive averages provides the variation.

2) Routing Algorithm:

The Ad hoc On-Demand Distance Vector (AODV) algorithm provides multi hop, dynamic, routing between contributing network nodes .AODV lets these nodes to find routes quickly for new endpoints, and does not need nodes to keep routes to endpoints that are not in live communication. Type of Message defines by AODV: Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs).Steps are [38]

- DetectDosAttack(S, D) /* Source node is S and D is the Destination Node */
- As transmission begins it will search for all the intermediate nodes and send data on to it.
- The intermediate node failed forwarding the Hello Message to the next node.
- It will check the RESPONSE time for the intermediate node.
- If (Response Time> HopTime +Threshold)
- {The Attacker Node is detected. Update Neighbour Node Table & Routing Table for the Intermediate Nodes }
- Return.

When applying Cusum algorithm the following graph presents:

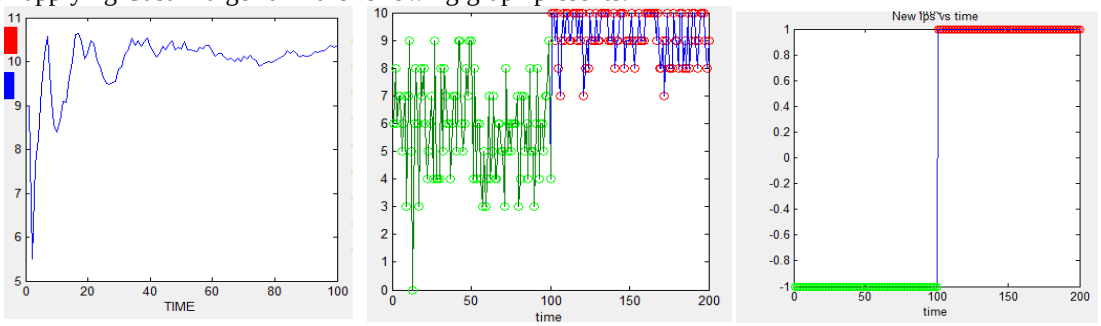

Fig 2 User behavior graph, New IP graph Hypothesis & New IP graph [43]

© 2016, IJARCSSE All Rights Reserved

- Then IP Hypothesis graph displays the Attacker& Legitimate client users, New IP graph displays that at -1 worth, there's no Attack and at 1 worth, there's associate degree of attack happens.[43]
- Now another, if we have knowledge of attack or when it DOS & DDOS identified thus, we will able to detect single source or cluster of source which might cause attack.

The next steps include the Ad-hoc vector on demand routing protocol it deal with some cases like when no attack is exists another one during attack, implementation of Ad-hoc vector on demand protocol.

- After clicking on find attacker, the output window display the next window having four case

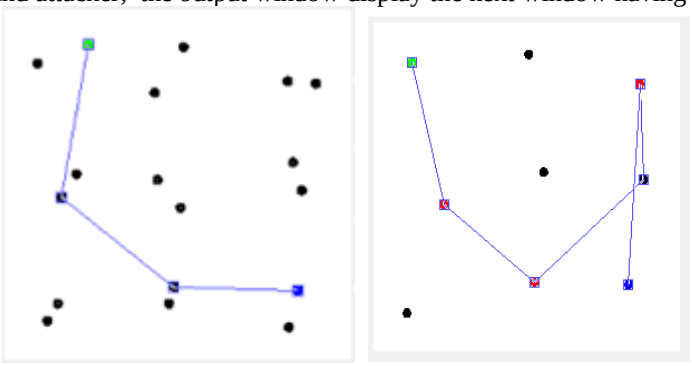

Fig 3 Ideal Case & during attack

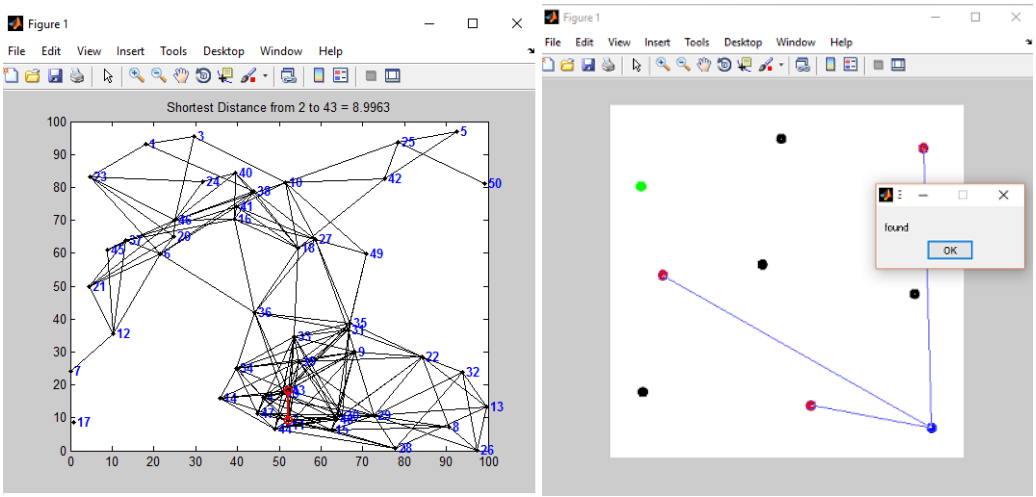

Fig 4 Implementation of AODV & Identification of actual attacker and block the invalid user's IPs

IV. CONCLUSION

Distributed denial of service attack that increased with the adoption of cloud in the network channel is easy to perform but defense to these can be complicated. By prevention or detection of those attack standards of trust sharing become effective. Here we analysis DDOS detection mechanism that based on anomaly based detection .The detection for any attack should be something like that the any abnormal change or anomaly variation can easily recognizance with the finest accuracy. When applying cusum algo, the system considers being best when it is able to recognize the pattern produced previous when the legitimate intendant user had to retrieve the file system. That why appropriate learning methodology should be delivered to the system so any conversion or variation can be easily detects and specifies the unintended user. The another ddos Defence mechanism deal with ad-hoc routing protocol to that basically take place after the identification of dos or ddos attack . Once ad-hoc vector on demand protocol find out the attacker node than it block the infected IPs source and find the shortest path to supply the request and its associated reply to the legitimate user.Market is expected to grow to $210 billion from $131 billion .Cloud computing will become more attractive for DDoS attacks in the future Both DDoS attacks and prevention against DDoS attacks will improve on self. An ideal DDoS Defence mechanism that deal with all ,must have some determined measures which includes Low False Positive Rate, Low Detection time, Low Negative rate, High Normal packet survival ratio. Exploration of precise approach for recognizing attacks and minimizing its after effect is a future research issue.

REFERENCES

[1] "National Institute of Standards and Technology." [Online]. Available: http://www.nist.gov/index.html

[2] "NIST SP 800-145, The NIST Definition of Cloud Computing - SP800-145.pdf." [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[3] A. Aissani, and M. Y. Achour, "Evaluation of the Severity of DoS Attacks on Computer Networks," Proc. of 2nd Intl' Conference On Performance, Safety and Robustness in Complex Systems and Applications (PESARO), IARIA, 2012, pp. 8-13

© 2016, IJARCSSE All Rights Reserved

[4] A. Mitrokotsa, and C. Douligeris, "Denial-of-Service Attacks," Network Security: Current Status and Future Directions (Chapter 8), Wiley Online Library, pp. 117-134, June 2006.

[5] Amit Vinayakrao Angaitkar, Narendra Shekokar, Mahesh Maurya, The Countering the XDoS Attack for Securing the Web Services, International Journal of Computer Science and Information Technologies, Vol. 5 (3) , pp.3907-3911,2014.

[6] An effective prevention of attacks using giTime frequency algorithm under ddos by Dr.K.Kuppusamy,S.Malathi, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[7] B. B. Gupta, P. K. Agrawal, R. C. Joshi, and M. Misra, "Estimating Strength of a DDoS Attack Using Multiple Regression Analysis," Communications in Computer and Information Science, Springer, 2011, vol. 133, part 3, pp. 280-289

[8] B. Prabadevi, N.Jeyanthi, Distributed Denial of service Attacks and its effects on Cloud Environment- a Survey, IEEE Explore, 2014.

[9] Berndt, A Quick Guide to AODV Routing, NIST natinal institite of standard and technology

[10] Bhuyan MH, Bhattacharyya DK, Kalita JK. An empirical evaluation of information metrics for low-rate and highrate DDoS attack detection, Pattern Recognition Letters. 2015 Jan; 51:1–7.

[11] C. Jin, H. Wang, and K. Shin. Hop-count filtering: an effective defense against spoofed ddos traffic. In Proceedings of the 10th ACM conference on Computer and communications security,October 2003

[12] chandini M Patel and Viral H Borisagar: Survey on taxonomy of DDoS attacks with impact and mitigation techniques, IJERT, ISSN: 2278-0181, Vo. 1Issue 9, NOV2012

[13] DDoS Attack. http:// www.incapsula.com/ddos/ddos-attack

[14] Debajyoti Mukhopadhyay, Byung-Jun Oh, Sang-Heon Shim, Young-Chon Kim, " A Study on Recent Approaches in Handling DDoS Attacks", Cornell University Library, 2010

[15] Foster, Ian, Yong Zhao, Ioan Raicu, et al, "Cloud Computing and Grid Computing 360-Degree Compared", In Grid Computing Environments Workshop (GCE), Austin, 2008.

[16] G. Badishi, A. Herzberg, I. Keidar, O.Romanov, and A. Yachin, "An Empirical Study of Denial of Service Mitigation Techniques," IEEE Symposium On Reliable Distributed Systems (SRDS '08), IEEE, pp. 115-124, October 2008.

[17] G.Bhatti, R.Singh and P.Singh, "A look back at Issues in the layers of TCP/IP Model," International Journal of Enhanced Research in Management & Computer Applications, Vol. 1, Issue 2, November 2012.

[18] G.Meera Gandhi, and S.K. Srivatsa, "An Entropy Architecture for defending Distributed denial-of-service attacks," International Journal of Computer Science and Information Security, Vol. 6, 2009, PP 129 – 136.

[19] H. Beitollahi, and G. Deconinck, "Denial of Service Attacks: A Tutorial,", Electrical Engineering Department (ESAT), University of Leuven, Technical Report: 08-2011-0115, August 2011

[20] http://dazeinfo.com/2015/08/28/internet-security-ddos-attacks-china-australia-us-uk-akamai/

[21] http://www.nist.gov/itl/cloud/

[22] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM SIGCOMM Computer Communications Review, Volume 34, Number 2, April 2004, pp. 39-53.

[23] K. Kumar, A. L. Sangal, and A. Bhandari, "Traceback Techniques against DDoS Attacks: A Comprehensive Review," Proc. of 2nd Intl' Conference On Computer and Communication Technology (ICCCT), IEEE, pp. 491-498, September 2011.

[24] K. Subhashini, and G. Subbalakshmi, "Tracing Sources of DDoS Attacks in IP Networks Using Machine Learning Automatic Defence System," International Journal of Electronics Communication and Computer Engineering, vol. 3, issue 1, pp. 164-169, January 2012.

[25] K.Shanti, A Defense Mechanism to Protect Cloud Computing Against Distributed Denial of Service Attacks, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, May 2013.

[26] L. Garber, "Denial-of-Service Attacks Rip the Internet," IEEE Computer, vol. 33, issue 4, pp. 12-17, April 2000.

[27] Large-scale Automated DDoS detection System by Vyas Sekar Carnegie Mellon University Nick Duffield AT&T Labs-Research Oliver Spatscheck AT&T Labs-Research-Annual Tech '06: 2006 USENIX Annual Technical Conference

[28] M. Aamir and M. Arif, "Study and Performance Evaluation on Recent DDoS Trends of Attack & Defense," International Journal of Information Technology and Computer Science, MECS Publisher, vol. 5, no. 8, pp. 54-65, July 2013.

[29] M. Zakarya, and A. Ali Khan, "Cloud QoS, High Availability & Service Security Issues with Solutions," IJCSNS International Journal of Computer Science and Network Security, Vol.12, July 2012, PP 71 – 7

[30] Madarapu Naresh Kumar, P Sujatha, Vamshi Kalva, Rohit Nagori, Anil Kumar Katukojwala and Mukesh kumar: Mitigating Economic Denial of Sustainability (EDoS) in Cloud Computing using In-Cloud Scrubber Service, 2012 Fourth International Conference on Computational Intelligence and Communication Networks

[31] Marwan Darwish, Abdelkader Ouda, Luiz Fernando Capretz: Formal Analysis of an Authentication Protocol against External Cloud-Based Denial-of-Service (DoS) Attack

[32] Mohd Nazri Ismail, Abdulaziz Aborujilah, Shahrulniza Musa, AAmir Shahzad, "Detecting Flooding based DoS Attack in Cloud Computing Environment using Covariance Matrix Approach" 2013

[33] P. Ferguson, and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2827, May 2000.

© 2016, IJARCSSE All Rights Reserved

[34] P. K. Agarwal, B. B. Gupta, S. Jain, and M. K. Pattanshetti, "Estimating Strength of a DDoS Attack in Real Time Using ANN Based Scheme," Communications in Computer and Information Science, Springer, 2011, vol. 157, part 6, pp. 301-310.

[35] Patel Ankita and Fenil Khatiwala," Survey on DDoS Attack Detection and Prevention in Cloud", International Journal of Engineering technology, Management and Applied Sciences, 3(2): February 2015.

[36] Rajkumar Buyya, Rajiv Ranjan and Rodrigo N. Calheiros," InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services", Springer 2010

[37] S. H. Kang, K. Y. Park, S. G. Yoo, and J. Kim, "DDoS avoidance strategy for service availability," Cluster Computing, Online First, Springer, DOI: 10.1007/s10586-011-0185-4, October 2010

[38] Gehlot, singh. A protocol/scheme to mitigate DDOS attacks using AODV protocol ,international journal of Scientific research development, vol. 1, issue 9,2013.

[39] S. Kent, and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, November 1998.

[40] S.S. Chopade, K.U. Pandey, D.S. Bhade, Securing Cloud Servers against Flooding Based DDOS Attacks, in Proc. International Conference on Communication Systems and Network Technologies,2013.

[41] T.Siva, E.S.Phalguna Krishna, Controlling various network based ADoS Attacks in cloud computing environment: By Using Port Hopping Technique, International Journal of Engineering Trends and Technology (IJETT), vol. 4, May 2013

[42] Toma´s Jirsk, Martin Husak, Pavel Celeda, Zdenek Eichler, "Cloud-based Security Research Testbed: A DDoS Use Case", IEEE, 2014.

[43] Jairath, Talwar. Attacks and Their Effect on security of data in cloud computing, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 3, March 2015.

[44] Trends in Denial of Service Attack Technology CERT® Coordination Center Kevin J. Houle, CERT/CC George M. Weaver, CERT/CC In collaboration with: Neil Long Rob Thomas v1.0 October 2001

[45] W. Eddy, "TCP SYN Flooding Attacks and Common Mitigations," RFC 4987, August 2007

[46] Y. Chung, "Distributed Denial of Service is a Scalability Problem," ACM SIGCOMM Computer Communication Review, vol. 42, issue 1, pp. 69-71, January 2012.

© 2016, IJARCSSE All Rights Reserved