I.J. Wireless and Microwave Technologies, **2018, 1, 42-49**
Published Online January 2018 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2018.01.05

***Available online at** http://www.mecs-press.net/ijwmt*

Energy Aware Supervised Pattern Attack Recognition Technique for Mitigation of EDoS Attacks in Cloud Platform

Preeti Daffu[a], Amanpreet Kaur[b]

[a]*Research Scholar, #341/6, Morinda and 140101, India*
[b]*Assistant Professor, Khrar and 140301, India*

Received: 29 May 2017; Accepted: 30 June 2017; Published: 08 January 2018

Abstract

Cloud computing is a rapidly growing technology in this new era. Cloud is a platform where users get charged on the basis of the services and resources they have used. It enables its users to access the cloud resources from the remote locations i.e. from anywhere at any time. It needs only a working internet connection to access the cloud services. Cloud users have always been victim to the security issues and attacks which leads to the data loss. The data is not saved on the hard disk of the computer so it is highly prone to security risks. Identifying the attacks on cloud platform is a difficult task because everything on cloud is in virtual form. EDoS (Economic Denial of Sustainability) attack is a form of DDoS attacks; carried out for a long span of time and intended to put a financial burden and cause economical loss to the users of cloud. Such attacks do not exhaust the bandwidth of the user; their main aim is to put a huge financial loss or burden on the user. A technique named as SPART (Supervised Pattern Attack Recognition Technique) implemented to mitigate the EDoS attacks in cloud computing which consumes lesser energy as compared to the existing models. The experimental results have shown the less energy consumption in proposed model.

Index Terms: SPART (Supervised Pattern Attack Recognition Technique), EDoS (Economic Denial of Sustainability), DDoS (Distributed Denial of Service).

1. Introduction

* Corresponding author. Tel:
E-mail address:

Cloud computing is a platform where users get charged on the basis of the services they have retrieved and taken access to. It has provided its users to use the data resources with the minimal data overhead. Cloud computing has three service models, four deployment models and five main characteristics [5]. These five characteristics have been shown in Fig. 1.

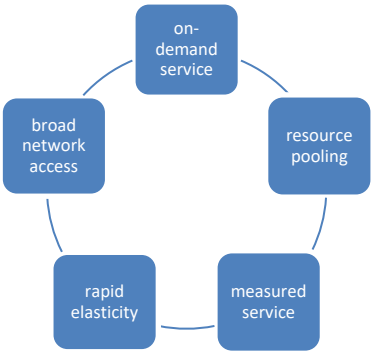

Fig.1.Five main characteristics of cloud computing.

Cloud platform has provided its users to gain access to resources from shared pool whenever they need i.e. at anytime and at any location. It needs only a working internet connection to retrieve resources from cloud. In cloud environment large pool of resources are available and these are allocated dynamically among its users. An immense popularity has been gained in the cloud platform by allowing the cloud users to lease he computer resources when they run out of them, a pay-based usage of resources and this is known as "pay-as-you-use". It allows its users to run the applications directly from the cloud [7]. Today protecting the stored data on the cloud platform is an important issue that cannot be understated. Securing the cloud users from various cloud attacks and their effects becomes a major issue today and it has been the reason that many users still don't shift their data to cloud.

The cloud infrastructure is fully virtualized and it supports all type of hardware architectures. Thus providing security to cloud is an important issue these days. The papers [3][6][7] give a brief idea about the concerns related to the security and attacks on the cloud platform. Cloud is prone to a variety of attacks such as malware injection attack, Spoofing attack, flooding attack, wrapping attack, DoS, DDoS and EDoS attack. Detecting and filtering the attack packets is a difficult job. Denial of service (DoS) attack is an intended attempt to exhaust the computing resources and the network bandwidth of the target user. Distributed Denial of Service (DDoS) attack is attempted to multiple users by flooding the packets. Economic Denial of Sustainability (EDoS) attack can be taken as a new form of the DDoS attack. The only difference is that these attacks are taken over long span and put a huge financial burden on the cloud users and hurt them economically.

Security Issues in Cloud Environment: Security concerns have played a major role in the issues related to the cloud. Cloud users have always compromised with the security of their data when they need to achieve the better performance. Transmission of the sensitive data over cloud is highly prone to the risks. Cloud is a platform where multiple users share the same data resources from the shared pool of resources. Data is not saved on the hard disk and saved on the network [6]. This cause major security issues and to remove such security issues some of the best aspects are required to provide authentication and authorization to the cloud users.

Energy Consumption: The energy consumption is the parameter to estimate the power consumed by the cloud nodes in performing the operations on the cloud nodes to send, receive to route the data from one node or one path to another path. Also the nodes consume the energy while performing the sensing operations. The proposed model has been evaluated for the energy consumption against the energy consumption of the existing

models in performing the similar operations over the similar amounts of data for the similar length of periods in the both of the simulations.

The energy consumption is the parameter to estimate the power consumed by the cloud nodes in performing the operations on the cloud nodes to send, receive to route the data from one node or one path to another path. Also the nodes consume the energy while performing the sensing operations.

The remainder of this paper is organized as follows: Section 2 gives an overview of the existing and the previous researches done in the same area. Section 3 has discussed the design and the implementation of the model that has been proposed. Section 4 has discussed the result analysis. Conclusion and future work are given in the final section.

2. Related Works

Morein, William G. et al. (2003) has proposed the method to counter the ddos attacks using graphic turing tests against web servers. The authors have implemented an overlay based model to provide guaranteed access to web servers that have been made the target for the DoS attacks. This model has explained two main features of the web environment. The first feature us the design of the model which was implemented around a human centric interface and other is its extensibility in various browsers through downloaded "applets." Khor and Nakao have implemented architecture to assure cloud users to retrieve the data resources when they need by solving crypto puzzles. The access to resources was granted only to those genuine users who pay for the cloud resources they have retained. Clients first need to define the difficulty level k of the crypto puzzles and then request for the resources they need to utilize. If the initial request of the client is not accepted in the given interval of time due to resource constraint then user may ask for the more complex crypto puzzle to solve. After the users solve the complex crypto puzzle a more secure communication link gets established between the cloud users (client) and the server so that they can exchange the messages. This secure channel is established by the server always. This proposed technique has several shortcomings such as the correlation between puzzle difficulties, problem of asymmetric power consumption, and solving the puzzle accumulation.

Zunnurhain, Kazi. et. al. [20] has analyzed the security attacks and their effects on the cloud. The authors have also proposed the solutions to such attacks. Cloud platform offers great potential and minimize the expenses but at the same time it is vulnerable to various threats and security risks. The authors have identified the possible security attacks on clouds including wrapping attacks, Flooding attacks, Browser attacks, malware injection attacks and also accountability checking problems. The authors have identified and proposed the required solutions to remove the root cause behind these attacks. In [19] Sqalli, Mohammed H. et. al. has implemented two step mitigation technique i.e. EDoS-shield against EDoS attacks on cloud platform. In this paper, the authors have extended the previous approach and named it as EDoS Shield, for mitigation of EDoS attacks that have been originated from spoofed IP addresses. The authors have evaluated the performance to mitigate the EDoS attacks that have been generated from the spoofed IP address. In this technique a virtual firewall and a verifier node does the mitigation of the EDoS attacks. The incoming requests from the users are filtered by the firewall and the filtration is done on the basis of two lists: white list and black list. White list contains the genuine users while black list contains the attacker nodes. If a client request to retrieve the cloud services then the verifier node use the turing test to check the legitimate users. If it is from the genuine user and it passes the turing test then the IP address of the user is held in the white list and if it fails the test then verifier node held its IP address in black list. The requests from black listed IP will be blocked. The shortcomings of this technique include its susceptibility to spoofed IP. The attack that used a spoofed IP address belonging to white list of verifier node will remain undetected. Secondly, it has high number of false positives identified. Many legitimate users are identified as attackers and get blocked.

Al-Haidari, Fahd et. al. [2] has discussed the EDoS shield architecture which was further enhanced and the model was named as Enhanced EDoS shield. EDoS attack is generated by transforming DDoS attack into an EDoS to target the financial component of the users. The authors have proposed the discrete simulation

technique for the mitigation of EDoS attack. This technique has a drawback that it do not include the auto-scaling feature of the cloud.

In [9] the author has conducted a survey on the detection and the defence approaches related to the DDoS attacks. Nowadays DDoS attacks have become a serious threat to the cloud users and the buzzing technology. Distributed Denial-of-Service (DDoS) attack is a major concern today because such an attack is difficult to detect and there is not an appropriate solution to mitigate such attacks. Such attack can shut down whole business of an organization from the internet. The main goal is to deny the access to the resources the user need and to cause the congestion on the network. The authors have reviewed the various defence and detection techniques for DoS and DDoS attacks.

In [11] authors have discussed about the services on a cloud and these services can be categorized into two categories: one is cloud service provider and other is cloud service consumer. As the security in the cloud service is the biggest concern; the control measures for the threats and the attacks prevailing the cloud services have been used. A framework is used to experiment the XML based and HTTP based DDoS attacks for the protection of EDoS attacks. The transformation of DDoS attacks into EDoS attacks is also explored.

Baig, Zubair A. et. al. [6] has analyzed the controlled virtual resources access to mitigate the EDoS attacks against cloud infrastructure. Through this analysis the authors classified the incoming requests into two categories: normal list and suspect list. It ensures that only the legitimate end users get the priority to access the cloud services and the suspected users get the less priority for retrieving the cloud services. Until a user is present in suspect list, user cannot take advantage of the cloud services.

Al-Haidari, F. et. al. (2015) has evaluated the impact of EDoS attacks against cloud computing services. A cloud introduces resource-rich computing platforms, where adopters are charged based on the usage of the cloud's resources or utility computing. However, traditional Distributed Denial-of-Service (DDoS) attacks on server consume the resources of the users and make the resources unavailable for them. The authors have developed a simulation model to evaluate the impact of the EDoS attacks. This analytical model is based upon the queuing model that captures the cloud services. Baig, Zubair A. et. al. [7] has proposed a novel approach based upon the rate limit technique and data with low overhead for the detection and mitigation of the EDoS attacks. It is a model which relies upon the incoming request rate from one source (a client of cloud network) based upon the fixed threshold value. The duration factor also lies as the major factor while evaluating the nodes sending the request rate more than threshold. It is unable to detect the pattern-based controlled EDoS attacks where the attacker nodes work in the group. Multiple nodes might attack the target cloud by beating the threshold for request rate and duration. It is not capable of analysing the proposed scheme to optimize the overall performance while looking at the service provider and network-level variations.

3. Design and Implementation

3.1 SPART Algorithm

In the first phase, data is received at Cloud ingress point. The Cloud ingress point is defined as the entry point of the user data in the Cloud environment and act as the gateway. The user data is received at the ingress point and analysed using the traffic analytic phase to evaluate the abnormalities in the ingress traffic data. The

Algorithm: SPART Algorithm
Step1. Initialize the simulation.
Step2. Scan the ingress traffic.
Step3. Apply pattern detection module.
Step4. Compute the Resource Usage (R_U)
Step5. Compute the Response Time (R_T)
Step6. Apply key management on the possible attackers.
Step7. Mark the unauthorized and unauthenticated violating nodes.
Step8. Apply the packet filtering module.

abnormalities in the ingress data is found in the form of individual user at the first step of the ingress data analysis. Then the data patterns are evaluated to determine the abnormalities on the basis of multiple node based pattern attacks. Then the legitimacy of all of the individual users sending the data to the Cloud is evaluated and updated in the pattern analytical record.

4. Result Analysis

The proposed model has been designed to reduce the energy consumption in cloud environment. Energy consumption is a biggest concern in the cloud platform today. While mitigating attacks on the cloud energy parameters should also be concerned.

The proposed algorithm has been implemented over the Greencloud simulator installed over the Debian Linux operating system. The Greencloud simulator is based upon the network simulator 2 and has been specifically designed for the performance evaluation of the cloud environment under the real time data transmission based emulation.

Energy Consumption: It is calculated by subtracting the present energy of a path from the Initial energy of path. When data is transferred between the networks nodes, energy is consumed during the packet receive event, packet transmit event, during the idle or sleep state of the cloud nodes. The energy is calculated after each interval of 0.5s in the given simulation scenario. Energy consumption is plotted across Y-axis and the simulation time on the X-axis and this has been shown in fig.2 .

The energy consumption is the key parameter in the case of cloud nodes. The lifetime of cloud nodes entirely depends upon the battery life which is directly proportional of the volume of data and amount of local processes on the node. The heavy data volumes are the key factor behind the energy consumption of the cloud nodes. The cloud node's energy consumption can be reduced by mitigating the heavy traffic volume by filtering the overflowing attack data from the ingress ports of the network nodes. The energy consumption reduction directly affects the network lifetime and elongates the network lifetime in the direct manner.

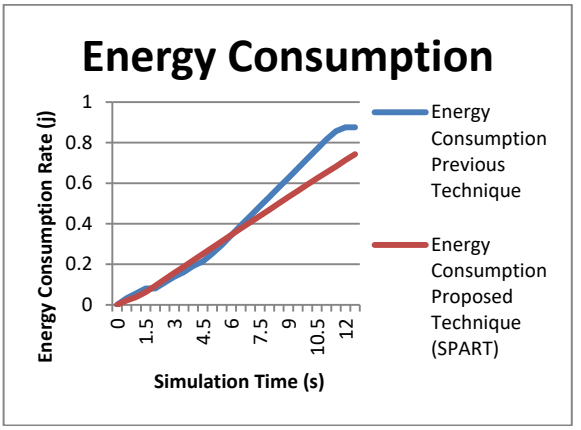

Fig.2. Energy Consumption

The energy consumption is the parameter to estimate the power consumed by the cloud nodes in performing the operations on the cloud nodes to send, receive to route the data from one node or one path to another path. Also the nodes consume the energy while performing the sensing operations. The proposed model has been evaluated for the energy consumption against the energy consumption of the existing models in performing the similar operations over the similar amounts of data for the similar length of periods in the both of the simulations. The proposed model has been found more energy efficient than the existing model. The proposed

model has been found consuming very low amount of energy in comparison with the existing models. The proposed results with the comparison to existing models haves been shown in Table 1.

Table 1. The comparison between the numbers of neighbors in the existing v/s proposed models

Number of Hops	Before Detection	Proposed (After Prevention)	During Detection
0	0	0	0
2	240000	110	242000
4	250000	190	250000
6	250000	280	246000
8	257000	400	260000
10	246000	520	255000
12	300000	1000	320000

Table 1 illustrates the comparison of energy consumption between the previous model and the proposed model. Energy consumption has shown a great fall after preventing the EDoS attacks using the SPART technique.

A graph is plotted in Fig. 3 for the energy consumption before detection of an attack and after preventing the attack. Energy consumption has visibly shown a great fall after the attack has been prevented or mitigated. The graph is plotted across y axis (energy consumption) and x axis for no. of hops.

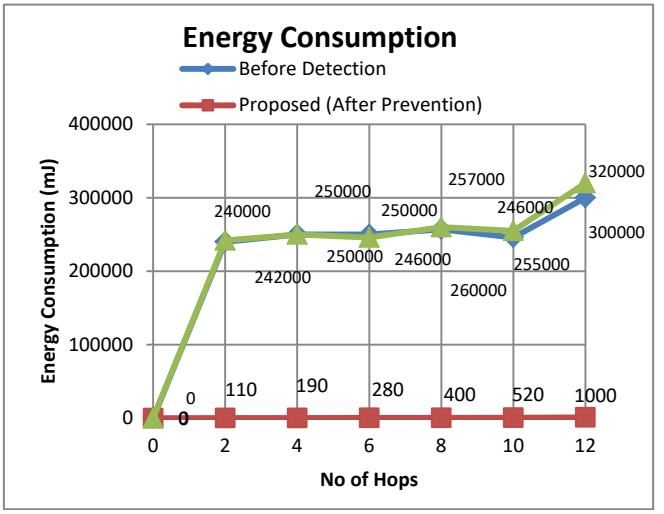

Fig.3. The count of neighbors in the existing v/s proposed models

5. Conclusions

In the proposed model energy consumption has been recorded in the form of residual energy. The overall energy consumption has been drastically improved in the case of proposed model. The overall energy of the cloud nodes has been consumed to 0.5 percent with 99.5 % residual energy remaining with the nodes to run for the hours. The simulation time of 10 seconds which includes the heavier traffic count during the attack simulation, the energy consumption has been reduced to the drastically low level, as per expected from the proposed defense model against the service unavailability attacks.

6. Acknowledgement

I acknowledge with deep feel of obligation and most trustworthy recognition, the helpful guidance and bottomless assistance rendered to me by “Er. Amanpreet Kaur” Assistant Professor for her experienced and concerned guidance, useful assistance and enormous help. It have been deep sense of praise for her convict goodness and infinite passion. The proposed work will be finished under the guidance of official guide and other experts at the campus of the Chandigarh Group of Colleges, Landran and Mohali.

References

[1] Al-Haidari, F., M. Sqalli, and K. Salah. 2015 "Evaluation of the Impact of EDoS Attacks Against Cloud Computing Services." Arabian Journal for Science and Engineering, 40(3): 773-785.
[2] Al-Haidari, F., Sqalli, M.H. and Salah, K., 2012, June. Enhanced edos-shield for mitigating edos attacks originating from spoofed ip addresses. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on : 1167-1174. IEEE.
[3] Alzamil, Ibrahim. "Simulation of Cloud Computing Eco-Efficient Data Centre."
[4] Bala, A., Bansal, M. and Singh, J., 2009, December. Performance analysis of MANET under blackhole attack. In Networks and Communications, 2009. NETCOM'09. First International Conference on 1:141-145 IEEE.
[5] Baig, Zubair A., and Binbeshr Farid 2013. "Controlled Virtual Resource Access to Mitigate Economic Denial of Sustainability (EDoS) Attacks against Cloud Infrastructures." Cloud Computing and Big Data (CloudCom-Asia), International Conference: 346-353, IEEE.
[6] Baig, Zubair A., Sait S.M. and Binbeshr F. 2016. "Controlled Access to Cloud Resources for Mitigating Economic Denial of Sustainability (EDoS) Attacks." Computer Networks. 97: 31-47.
[7] Bakshi, A. and Yogesh, B., 2010, February. "Securing cloud from ddos attacks using intrusion detection system in virtual machine." In Communication Software and Networks, ICCSN'10. Second International Conference on : 260-264, IEEE.
[8] Bhandari, N.H. 2013. "Survey on DDoS Attacks and its Detection & Defence Approaches." International Journal of Science and Modern Engineering (IJISME) ISSN, 2(7): 2319-6386.
[9] Booth, G., Soknacki, A. and Somayaji, A., 2013, June. "Cloud Security: Attacks and Current Defenses." 8th Annual Symposium on Information Assurance (ASIA’13): 56.
[10] Chaudhary, A., Kumar, A. and Tiwari, V.N., 2014, February. A reliable solution against Packet dropping attack due to malicious nodes using fuzzy Logic in MANETs. In Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference on :178-181. IEEE.
[11] Chonka, A., Xiang, Y., Zhou, W. and Bonti, A., 2011. "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks." Journal of Network and Computer Applications, 34(4): 1097-1107.
[12] Gupta, G.K. and Singh, M.J., 2010. Truth of D-DoS Attacks in MANET. Global Journal of Computer Science and Technology, 10(15): 15-22.
[13] Harb, L.M., Tantawy, M. and Elsoudani, M., 2013, January. Performance of mobile ad hoc networks under attack. In Computer Applications Technology (ICCAT), 2013 International Conference on IEEE, 27(12): 1201-1206.
[14] Liu, H., 2010, October. A new form of DOS attack in a cloud and its avoidance mechanism. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop:65-76, ACM.
[15] Lo, C.C., Huang, C.C. and Ku, J., 2010, September. A cooperative intrusion detection system framework for cloud computing networks. In Parallel processing workshops (ICPPW), 2010 39th international

conference on : 280-284. IEEE.
[16] Morein, W.G., Stavrou, A., Cook, D.L., Keromytis, A.D., Misra, V. and Rubenstein, D., 2003, October. Using graphic turing tests to counter automated ddos attacks against web servers. In Proceedings of the 10th ACM conference on Computer and communications security: 8-19. ACM.
[17] Naresh Kumar, M., Sujatha, P., Kalva, V., Nagori, R., Katukojwala, A.K. and Kumar, M., 2012, November. Mitigating economic denial of sustainability (edos) in cloud computing using in-cloud scrubber service. In Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on: 535-539. IEEE.
[18] Shakshuki, E.M., Kang, N. and Sheltami, T.R., 2013. EAACK—a secure intrusion-detection system for MANETs. Industrial Electronics, IEEE Transactions on, 60(3): 1089-1098.
[19] Sqalli, M.H., Al-Haidari, F. and Salah, K., 2011, December. Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing. In Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on: 49-56. IEEE.
[20] Zunnurhain, K. and Vrbsky, S.V., 2010, December. Security attacks and solutions in clouds. In Proceedings of the 1st international conference on cloud computing : 145-156.

Authors' Profiles

Preeti Daffu Morinda, September 18, 2017. She holds the degree of B.tech in Information Technology from Rayat and Bahra Engineering College Mohali, Punjab, India, 2013, M.tech from Chandigarh Engineering College, landran, Mohali, Punjab, India. She is an Active Researcher who has contributed 3 research papers in international conferences. She has also contributed 4 research papers in international journals. Her area of interest is Cloud Computing.

The lists of publications are: Low Cost Robust Inter-Server Authentication for Cloud Environments (Noida, U.P, and IEEE Conference 2016 pp. 537-541). Mitigation of DDoS Attacks in Cloud Computing (Rajpura, Punjab, IEEE Conference ID: 38683X, 2016). Mitigation of EDoS Attacks in Cloud: A Review: (Gurgaon, Haryana, Taylor and Francis, pp. 533-538, 2016). Pattern Analytical Module for EDoS Attacker Recogniton (IOSR-JCE pp. 14-20).

Amanpreet Kaur is an Assistant Professor in Chandigarh Engineering College, Landran, Mohali. She completed her B.Tech in Computer Science and Engineering from Guru Nanak Dev University, Amritsar in year 2000 with distinction and honours. She received her M.Tech degree in Information Technology from Guru Nanak Dev University, Amritsar in year 2005 and topped in the University. She has been in teaching profession for the last 14 years and pursuing Ph.D. in Computer Engineering from IK Gujral Punjab Technical University, Jalandhar in the area of Cloud Computing. Her interests are in areas of cloud computing, wireless networks and Image Processing.

How to cite this paper: Preeti Daffu, Amanpreet Kaur," Energy Aware Supervised Pattern Attack Recognition Technique for Mitigation of EDoS Attacks in Cloud Platform", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.8, No.1, pp. 42-49, 2018.DOI: 10.5815/ijwmt.2018.01.05