An Intrusion Detection System for Detecting Denial-of-Service Attack in Cloud Using Artificial Bee Colony

Shalki Sharma, Anshul Gupta and Sanjay Agrawal

Abstract Cloud computing is a technology which allows users to share resources and data over the Internet. Cloud computing represents the maturing of technology and is a pliable, cost-effective platform which provides business/IT services over the Internet. Although there are various benefits of adopting this technology, there are some significant barriers to it and one of them is security. Cloud computing is still growing and there is still uncertainty about how security is achieved, at all levels (network, host, application, and data), in cloud. In computing environment like cloud where whole infrastructure is shared by millions of users, attacks like denial-of-service are likely to have a much greater footprint than other attacks. The main aim of denial-of-service attack is the disruption of services by attempting to limit access to a machine or service instead of subverting the service itself. This paper tested the efficiency of artificial bee colony, a swarm approach, for finding denial-of-service attack in a cloud environment and finds that it is useful in tackling denial-of-service attacks.

Keywords Cloud computing · Denial-of-service · Artificial bee colony

1 Introduction

As the field of cloud computing is growing so are the security issues pertaining to it. The world cloud is very appealing as it provides the user with a lot of resources at one place without much of effort. Cloud provides its user with (1) on demand

Shalki Sharma (✉) · Sanjay Agrawal
NITTTR, Bhopal, India
e-mail: shalkisharma27@gmail.com

Sanjay Agrawal
e-mail: sagrawal@nitttrbpl.ac.in

Anshul Gupta
MPSTME, NMIMS, Mumbai, India
e-mail: anshul.gupta@niims.edu

S.C. Satapathy et al. (eds.), *Proceedings of the International Congress on Information and Communication Technology*, Advances in Intelligent Systems and Computing 438, DOI 10.1007/978-981-10-0767-5_16

self-service (2) broader network access (3) resource pooling (4) rapid elasticity (5) measured services [1]. There are various benefits of using cloud over a traditional approach such as cloud helps to reduce the cost; it provides global access, unlimited storage capacity, improved performance, and many more. But with this attraction comes a severe issue of the security in cloud. Threats like man-in-the-middle attack, denial-of-service attack are always present and attackers have become more prominent and active in using these kinds of attacks for disrupting the services of cloud and making them unavailable to the intended users. Cloud Security Alliance [2] has defined (1) data breaches (2) data loss (3) account hijacking (4) insecure APIs (5) denial-of-service (6) malicious insiders (7) abuse of cloud services (8) insufficient due diligence (9) shared technology issues as "Notorious Nine," nine critical threats to cloud computing. Hackers in the past have tried to attack and some have been successful also. On August 6, 2009, twitter went down abruptly for 2 h and the reason for this shut down was denial-of-service attack [3, 4].

With the advancement made in cloud, security has become an important aspect both with respect to the user and as well as to the CSP. In our proposed work, we are using artificial bee colony (ABC) technique for the detection of denial-of-service attack in a cloud environment. The rest of the paper is sub partitioned into four sections. In Sect. 2, a brief definition of DoS attack and its detection approaches are provided. In Sect. 3, proposed methodology is summarized. Section 4, discusses the results and we conclude the paper with Sect. 5.

2 Denial-of-Service Attack

Denial-of-service is an attack that attempts to make the resources or services unavailable to the users for infinite amount of time by flooding it with useless traffic [5, 6]. Numerous approaches have been proposed in the past for detecting these kinds of attacks. Some of the techniques and related work are mentioned below.

2.1 Related Work

2.1.1 Malicious Detection

Mahajan Pushback approach [7] uses two techniques; aggregate congestion control (ACC) and pushback. Local ACC uses identification algorithm for finding the cause of congestion and control algorithm for reducing its effect. Second mechanism, Pushback, allows router to request their adjacent upstream router to rate limit the specified aggregate. Crowding at router level is detected by Local ACC and devices a congestion signature and translates into router filter. Network traffic and high bandwidth aggregate are defined by signature and local ACC defines a rate limit for

this aggregate. This rate limit is propagated to the intermediate upstream neighbors, by Pushback that contributes to the largest amount of traffic.

Lo et al. [8] proposed the use of distributed IDS and of cooperative defense for each of the cloud by the IDS. Each cloud is provided with its own IDS and alerts are generated by the IDS who are under the attack. Trustworthiness of the alert is defined by judgment criteria. Block tables are used to keep track of all the alerts generated and if any new alert is found, it is added in the table, thus helping in an early detection. Alerts so generated are categorized among serious, moderate, and slight; depending upon the type of the attack. The overall benefit is that it forestalls the entire system from a single point failure.

Approach proposed by Lua et al. [9] aims to detect DoS attack using intelligent fast flux swarm network. Fast flux technique maintains connectivity among swarm nodes, clients, and servers. To maintain parallel and distributed optimization IWD was used. Swarm network was built on two concepts: fast flux technique in DNS and organization of swarm. Client reaches the server via fully qualified domain name and the request is forwarded to the designated server via community exit node. Results are reverted back to the client through the swarm network. Swarm network reconfigures itself constantly using IWD as it is highly resistant to sudden changes in network. The proposed approach is highly robust in nature.

Anitha et al. [10] proposed the use of packet marking approach for the detection of DoS attack. CLASSIE, rule set-based detection, was used to discriminate between legitimate and illegitimate attacks. The proposed method was checked by HX-DOS attacks cloud web services. CLASSIE is situated one hop away from the host. Whenever an HX-DOS attack is detected, CLASSIE drops the packets and they are subjected to marking, done both on edge and core routers. RAD method allows incoming messages to pass or to drop and is situated one hop away from the victim. RAD also avoids spoofing. The technique reduces the false positive rate.

Joshi et al. [5] uses cloud trace back (CTB) for detecting DoS attacks. CTB uses SOA for tracing back the true source of the attack and is based on deterministic packet marking algorithm. CTB uses FDPM by integrating a cloud trace back mark (CTM) within the header of CTB. Back propagation neural network is used as Cloud Protector, to train and filter out the traffic. CTB removes the service provider's address by placing itself before the web server and hence all services are first sent to CTB. In case an attack has been observed, attacker will request CTB for the service and attacker will formulate a SOAP message. CTM is placed in the CTB header upon the receipt of this message and the message is forwarded to the web server. When an attack is observed mark is extracted and this will also filter out the attack traffic. If the attack was successful the victim will recover the CTM tag and thus revealing the true identity of the source.

Reddy et al. [11] proposed the use of quantum-inspired particle swarm optimization technique (QPSO) for the detection of DoS attack in a cloud. Anomaly-based detection was used for decision making. The technique was subdivided into two subphases training and testing. In training, normal traffic was trained using the quantum algorithm and in the testing phase abnormal traffic was

tested using the detection module of the algorithm. The observed were compared with QEA and the algorithm was found to be better than QEA.

3 Proposed Methodology

A lot of techniques and approaches have been proposed in the past for detection of these kinds of attacks. In our research, we are using artificial bee colony (ABC), a swarm approach [12], for detecting these kinds of attacks. In the proposed framework basic feature selection is done for each record, ABC working nature is determined and at the end we do decision making. For evaluating the accuracy of ABC, we are comparing it with QPSO and it was found that the average accuracy of ABC is better than QPSO.

3.1 Artificial Bee Colony (ABC)

ABC proposed by Karaboga, simulates the foraging behavior of honey bees [13]. The colony of honey bees consists of employed bees, onlookers, and scouts. Pseudo code of the algorithm is given below. The bee which is waiting on the dance area for making a decision to select the food source is the onlooker and the bee going to the food source, visited by it before, is the employed bee. Scouts are responsible for carrying out random search for finding new food source. The first half of the algorithm is of artificial employee bee and the second half of onlookers. Possible solutions to optimization problem are found by the position of the food source the nectar amount of a food source corresponds to the quality (fitness) of the associated solution, calculated by [13]. As the algorithm performs both global and local searches, it gives us efficient results.

$$\mathrm{Fit}_i = \frac{1}{1+f_i} \tag{1}$$

Steps of ABC Algorithm:

1. Start
2. Initialize the population
3. Employed bees finds a neighbor source for nectar and dances in hive
4. Each onlooker bee watches the dance chooses one of the neighbor sources depending on the dance.
5. Onlooker bee goes to that neighbor source and evaluate nectar amount.
6. Scouts replace abandoned food sources with new one
7. Determine best food source, so far
8. Repeat the steps from 3 to 7, until max is achieved
9. Stop

Probability, P_i, of choosing a new food source by onlooker bees is calculated by the following:

$$P_i = \frac{\text{Fit}_i}{\sum \text{Fit}_n} \tag{2}$$

where n = 1…size of population

For finding the new solution, v_{ij}, in the neighborhood of old one, x_{ij}, following formula can be used:

$$V_{ij} = x_{ij} + \Phi_{\text{ij}}\left(x_{ij} - x_{kj}\right) \tag{3}$$

where k and j are randomly chosen indexes and Φ_{ij} is random function within the range [−1,1].

3.2 Dataset for Training and Testing

The efficiency of any bio-inspired network depends on the training data. The more accurate the training data is more is the performance of the network. Thus collection of data is critical factor for training and can be done in any of the three ways: using a real traffic, using sanitized traffic, or using a simulated traffic. Using simulated traffic is the most common and feasible way for obtaining data and for creating a test bed network and also for generating background traffic on the given network [5, 14]. Background traffic can be generated by employing complex traffic generators modeling actual network statistics or by employing a more simple traffic generator by fabricating smaller number of packets at a high rate. By adopting this approach, data can be distributed freely because there is no sensitive information in it and also assures that the generated traffic does not have any unknown attacks because simulator is producing this traffic. In our approach, on the whole we have generated the background traffic in CloudSim.

3.3 Framework

The proposed framework has been divided into three steps. First basic feature selection is done for each record. In this step basic network features are generated and traffic is recorded in a well-defined manner. The more detailed approach can be found in [15]. Second, we employ ABC algorithm and determine the working behavior of ABC and at the end we do decision making. Decision making is done using anomaly-based detection technique [16]. Anomaly-based technique

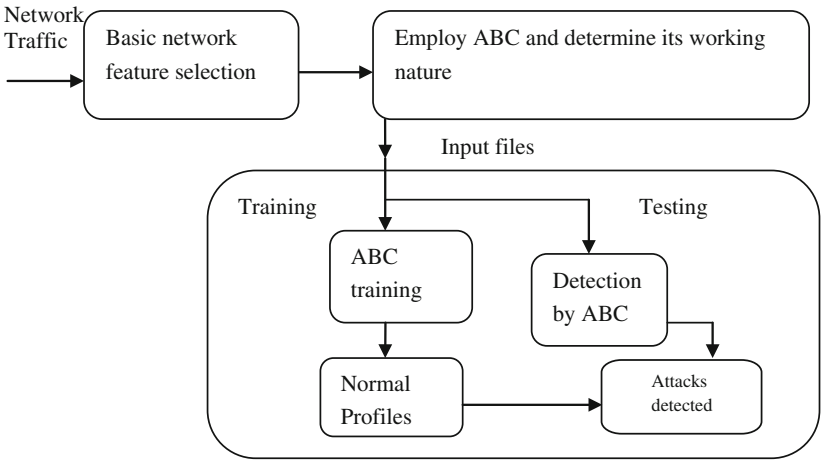

Fig. 1 Proposed framework

determines any kind of DoS attacks without having any kind of knowledge about the attacker. The technique is robust in nature as the attacker has to create a specific attack which appears as a normal traffic to the detection system and is too difficult to achieve. The decision making technique incorporates two processes: training and testing. The training phase incorporates the ABC training module for generating profiles for all types of legitimate records and for storing these generated profiles in a database. In the testing phase, ABC detection module is used for testing the traffic. Figure 1, gives a brief description about the same.

3.4 Methodology

The proposed approach was tested in a simulated environment with the help of CloudSim [17]. In order to do so, first we characterized our attackers and we generated attackers and non-attackers cloudlets and labeled both of them. After this we extracted the features and data partitioning was done where some data were reserved for training and while the other for testing. Our approach has two phases for its implementation: training and testing. While in training phase we construct a normal profile using ABC algorithm, in testing phase main focus is on detecting the DoS attacks. In order to detect the attack, we have used centroids as classifiers. Centroids are generated for both attackers as well as non-attackers and distance is calculated with both to determine the attackers and non-attackers. At the end we evaluate the performance of the system. In order to do so, we calculate the mean or average accuracy of ABC. The results so obtained are then compared to QPSO. The flowchart in Fig. 2 gives a brief description about it.

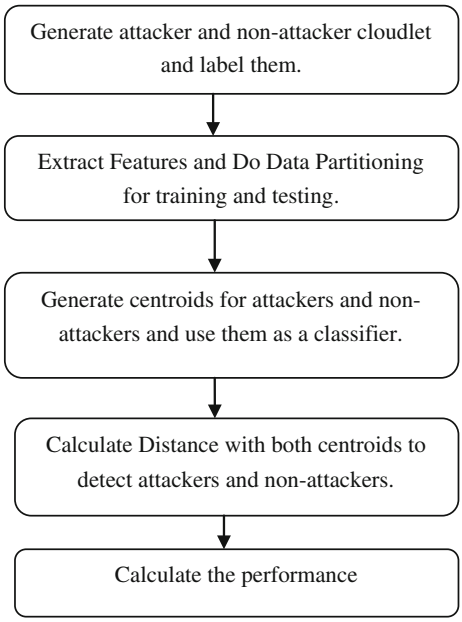

Fig. 2 Flowchart

4 Experiments and Results

In our research work, main aim was to prove the efficiency of artificial bee colony optimization approach for the detection of denial-of-service attack in a cloud environment. The results obtained shows that ABC is efficient enough to do the same.

In our research we have compared the efficiency of ABC and QPSO. Figure 3 shows that ABC is successfully detecting maximum attacks with a rate of 75–80 %. The average accuracies were found for ABC and QPSO using (3). A total of 10 readings were taken.

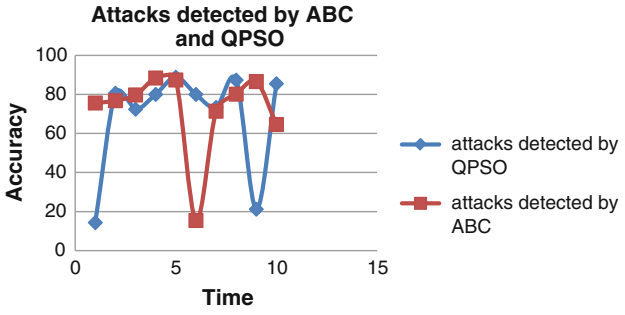

Fig. 3 Traffic detected by ABC and QPSO

$$\text{Mean} = \frac{\text{Sum of all values}}{\text{Total number of values}} \quad (4)$$

The average detection rate observed for ABC was 72.4 % while that for QPSO was 68.3 %.

Thus, from the above we can conclude that the average detection rate of ABC is far much higher than that of QPSO.

5 Conclusion and Future Work

Cloud computing provides a lot of advantages to its user to improve their conventional system. However, security should be alongside implemented to improve the performance and functionality. One of the serious threats come to cloud are from denial-of-service attack as this attack is easy to launch but difficult to stop. This research work has showed that artificial bee colony optimization, a swarm approach, is useful in detecting denial-of-service attack in a cloud environment. The proposed approach was carried out in a simulated environment using CloudSim [17]. The proposed approach also shows that it is able to detect most of the attacks in a very short period of time. This approach was further compared with quantum-inspired PSO and was found to be better. The results achieved for testing and training data sets were found to be 72.4 and 68.3 % for ABC and QPSO, respectively. In future, we will set up to work with real-world data and attacks to fine tune our system.

References

1. Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).
2. Top Threats Working Group. "The notorious nine: cloud computing top threats in 2013." Cloud Security Alliance (2013).
3. Akbarabadi, Ahad, et al. "Client To Client Attacks Protection in Cloud Computing By a Secure Virtualization Model." Journal of Next Generation Information Technology 4.8 (2013).
4. Chen, Shuo, et al. "Side-channel leaks in web applications: A reality today, a challenge tomorrow." Security and Privacy (SP), 2010 IEEE Symposium on. IEEE, 2010.
5. Joshi, Bansidhar, A. Santhana Vijayan, and Bineet Kumar Joshi. "Securing cloud computing environment against DDoS attacks." Computer Communication and Informatics (ICCCI), 2012 International Conference on. IEEE, 2012.
6. Iftikhar A., Azween B. A., Abdullah S.A., (2009), "Application ofArtificial neural Network in Detection of DoS attacks," SIN'09, Oct 6–10.
7. Mahajan, Ratul, et al. "Controlling high bandwidth aggregates in the network."ACM SIGCOMM Computer Communication Review 32.3 (2002): 62–73.
8. Lo, Chi-Chun, Chun-Chieh Huang, and Joy Ku. "A cooperative intrusion detection system framework for cloud computing networks." Parallel processing workshops (ICPPW), 2010 39th international conference on. IEEE, 2010.
9. Lua, Ruiping, and Kin Choong Yow. "Mitigating ddos attacks with transparent and intelligent fast-flux swarm network." Network, IEEE 25.4 (2011): 28–33.

10. Anitha, E., and S. Malliga. "A packet marking approach to protect cloud environment against DDoS attacks." Information Communication and Embedded Systems (ICICES), 2013 International Conference on. IEEE, 2013.
11. Reddy, Pallavali Radha Krishna, and Samia Bouzefrane. "Analysis and Detection of DoS Attacks in Cloud Computing by Using QSE Algorithm." High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC, CSS, ICESS), 2014 IEEE Intl Conf on. IEEE, 2014.
12. Binitha, S., and S. Siva Sathya. "A survey of bio inspired optimization algorithms." International Journal of Soft Computing and Engineering 2.2 (2012): 137–151.
13. Karaboga, Dervis, and Celal Ozturk. "A novel clustering approach: Artificial Bee Colony (ABC) algorithm." Applied soft computing 11.1 (2011): 652–657.
14. Xiang X, Zhou W, Guo M., (2009), "Flexible deterministic packet marking: an IP Trace Back system to find the real source of attacks," IEEE Transactions on Parallel and Distributed Systems, Volume 20, No 4, pp 567–80.
15. S.J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P.K. Chan, "Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project," Proc. DARPA Information Survivability Conf. and Exposition (DISCEX '00), vol. 2, pp. 130–144, 2000.
16. D.E. Denning, "An Intrusion-Detection Model," IEEE Trans. Software Eng., vol. TSE-13, no. 2, pp. 222–232, Feb. 1987.
17. http://www.cloudbus.org/cloudsim/.