Cloud Shield: Effective Solution for DDoS in Cloud

Rajat Saxena(✉) and Somnath Dey

Cloud Computing Lab, Department of Computer Science and Engineering,
Indian Institute of Technology Indore, Indore, India
{rajat.saxena,somnathd}@iiti.ac.in

Abstract. Distributed Denial of Service (DDoS) attack is a complex security challenge for growth of Cloud Computing. DDoS attack is very easy to apply, difficult to prevent and hard to identify because attacker can spoof the IP address of itself for hiding the identity of himself.

In this paper, we present a Third Party Auditor (TPA) based efficient DDoS detection and prevention technique which has the strong identification factor based on these weaknesses. It has less overhead at the user end. Thus, we target various aspects of prevention of DDoS attack in the Cloud environment.

Keywords: Cloud computing · DoS attack · DDoS attack · Third party auditor (TPA) · Dempster shafer theory (DST)

1 Introduction

Cloud computing [1,2] is defined as services and applications that are enforced on a distributed network using virtual resources and accessed by common networking standards and Internet protocols. It is distinguished from the traditional system in the conditions that resources are virtual and limitless and implementation details of the physical systems, on which software runs, are abstracted from the user.

However, Denial-of-service(DoS) and Distributed Denial of Service (DDoS) attacks are two major security restrictions for functionality and availability of Cloud services. In DoS attack, an intruder tries to prevent authorized users from retrieving the information or services. DDoS is an advance version of DoS attack. DDoS is a collaborative attack on functionality and availability of a victim cloud through multiple corrupted systems. In DDoS attack, multiple corrupted systems are utilized for targeting and corrupting a victim cloud to produce a DoS attack. The approach of attack is "distributed" because multiple systems are used by the intruder to launch DoS attack. In the process of DDoS attack, victims are all, victim cloud as well as multiple compromised systems. The main objective of DDoS attack is debacle damage on a victim cloud. Commonly, the undisclosed intension behind this attack is to restrict the available resources and dissolute the service which is highly demanded by the victim cloud.

G. Di Fatta et al. (Eds.): IDCS 2015, LNCS 9258, pp. 3–10, 2015.
DOI: 10.1007/978-3-319-23237-9_1

Thus, it commits harassment of the victim due to huge financial loss. The attacker also malfunctions the confidentiality of the victim and uses their valuable data for own malicious purpose. Apart from all these, acquires the popularity in the hacker‘s community is also an ambitious reason for these attacks.

In current situations, all the malicious attackers which are affected by the intruders, are send a large number of malicious packets directly to the victim cloud servers. As a result whole network is flooded with attack messages instead of legitimate packets. Thus, availability of cloud storage servers for the legitimate users would be null, because Cloud storage server have been crashed out from attack packets. It is also possible that attackers can manipulate the content of the legitimate packets. This would damage the services of victim Cloud server.

Some examples of DDoS attacks are following. A massive DDoS attack [3,4] occurred on website of yahoo.com at February 7, 2000. In this attack, even though yahoo.com have much extensive computing and bandwidth resources than any of the attackers, yet yahoo.com server collapse for 1.5 h. In 2008 [5], BBC, eBay and Amazon.com are suffered from DDoS attack. In 2010, transactions through PayPal.com are suspended by WikiLeaks website. In 2012 [5], Sony, US, Canadian and UK government websites knocked down by anonymous. In 2013 [8], Czech financial sector, stock exchange and national bank websites are destructed by enormous DDoS attack.

Recent analysis observes a giant amount of financial losses due to DDoS attack every year. According to the Computer Crime and Security Survey [6], the Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) survey [7], annual loss of financial corporations are increases day by day. A survey by Arber network [8] exposed the fact that approximately 1,200 DDoS attacks occurred per day. It is also disclose this interesting fact that the scale of DDoS attacks have been growing drastically since 2001. In year 2013, the largest recorded DDoS attack against a single target reached 150 gigabits per second, as against 40 gigabits per second in the year 2008 and 24 gigabits per second in year 2007.

Key elements that motivated us for providing a solution to DDoS attacks are revenue loss, slow network performance, service unavailability and loss of customer trust in service providers. Thus, we require a powerful and efficient technique to detect and prevent DDoS attack in cloud environment. For this purpose, we need to find out which type of tools are required to implement this attack and what are the weakness of these tools.

2 Proposed Scheme

We propose an effective approach to detect and prevent the victim cloud servers from any type of attack. First, we take a workstation as a TPA for observation of the all packets reached to cloud servers. It is an independent and trustworthy entity which logs all legitimate as well as malicious packets on the behalf of all cloud servers. We called this entity as “Cloud Shield”. Figure 1 shows the architecture of proposed Cloud Shield.

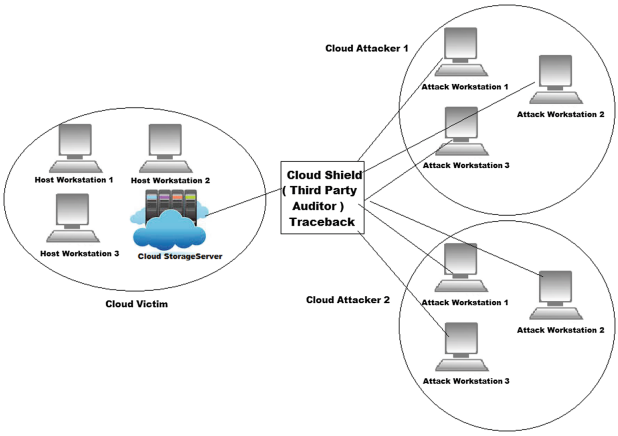

Fig. 1. Our proposed scheme

Cloud Shield is able to traceback the origin of the attack based on Dempster Shafer Theory (DST) to analyze all packets. This DST analysis is depended on 3-valued logic.

2.1 Dempster Shafer Theory (DST)

DST [9] is powerful method for mathematical diagnostics, statistical inference, decision analysis and risk analysis. For DST, probabilities are assigned on mutually exclusive elements of the power sets of state space (Ω) (all possible states). The assignment procedure of probabilities is called basic probability assignment *(bpa)*.

According to DST method [10] for a given state space (Ω) the probability (called mass) is allocated for t set of all 2^{Ω} elements, which are all possible subsets of (Ω). The DST operations with 3-valued logic provides Fault Tree Analysis (FTA) [11]. For example, if a standard state space (Ω) is (True, False), then 2^{Ω} should have 4 elements: Φ, True, False, (True, False). The (True, False) element describes the imprecision component, which is introduced by DST. This elements refers the value either true or false, but not both.

We have the following relation for DST as the [sum of all probabilities] = 1 and P(Φ) = 0:

$$P(True) + P(False) + P(True, False) = 1 \tag{1}$$

Thus, for analyzing each VM corresponding to the victim, we use FTA, which is perceived by boolean OR gate.If we choose set A = $\{a_1, a_2, a_3\}$ as an input set and B = $\{b_1, b_2, b_3\}$ as output set. Then Table 1 describes the Boolean truth table for the OR gate. From Table 1 we get:

$$P(A) = (a_1, a_2, a_3) = \{P(True), P(False), P(True, False)\} \tag{2}$$

$$P(B) = (b_1, b_2, b_3) = \{P(True), P(False), P(True, False)\} \tag{3}$$

$$P(A \vee B) = \{a_1b_1 + a_1b_2 + a_1b_3 + a_2b_1 + a_3b_1; a_2b_2; a_2b_3 + a_3b_2 + a_3b_3\} \tag{4}$$

Table 1. Boolean truth table for the OR gate

		b_1	b_2	b_3
	$\vee$	T	F	(T, F)
a_1	T	T	T	T
a_2	F	T	F	(T, F)
a_3	(T, F)	(T, F)	T	(T, F)

Putting the value from Eq. (1) into Eq. (4)

$$P(A \vee B) = \{a_1 + a_2b_1 + a_3b_1; a_2b_2; a_2b_3 + a_3b_2 + a_3b_3\} \tag{5}$$

In last, our solution uses Dempsters combination rule, which fuse evidences from multiple independent sources using a conjunctive operation (AND) between two *bpa's* P_1 and P_2, called the joint P_{12}

$$P_{12}(A) = \frac{\sum_{B \cap C = A} P(B)P(C)}{1 - K} \tag{6}$$

The factor $1 - K$ is called normalization factor and it is constructive for entirely avoiding the conflict evidence, When A $\neq \Phi$; $P_{12}(\Phi) = 0$ and $K = \sum_{B \cap C = \Phi} P(B)P(C)$.

Thus, by Eq. (6) we can easily analyze the DDoS flood attack from any topology or any type of resources the attacker have.

2.2 Our Implementation

Cloud Shield is a private cloud which is configured with front end server and three nodes (or VMs). The first step in our implementation involves deployment of a private cloud using Cloudera CDH 5.3.0-0 [12]. The other three nodes are selected and managed in "networking mode" of Citrix Xen Server 6.2.0 [13], because it provides the advanced features of virtualization. The depiction of Cloud Shield is given in Fig. 2.

We divide whole working of Cloud shield in three parts.

1. **Detection Phase:** This phase is handled by three nodes in which we assume that snort based on DST is installed and configured. It detects the packet floods and stores in the MySQL database. It also stores the attack alerts gathered from VM based IDS.
2. **Conversion Phase:** In this phase, front server convert alerts into basic probabilities assignments (bpas) based on the attack alerts. In our work, we utilizes 3-valued logic {True, False, (True, False)} in DST operations for successful detection of TCP-flood, UDP-flood and ICMP-flood attacks. Thus, we analysis of TCP, UDP and ICMP packets. Algorithm 1 provides conversion of alerts received from VM's into bpas.

Table 2. Boolean truth table for Dempster's combination rule

	$P_{V_1}(T)$	$P_{V_1}(F)$	$P_{V_1}(T,F)$
$P_{V_2}(T)$	$P_{V_1}(T)\ P_{V_2}(T)$	$P_{V_1}(F)\ P_{V_2}(T)$	$P_{V_1}(T,F)\ P_{V_2}(T)$
$P_{V_2}(F)$	$P_{V_1}(T)\ P_{V_2}(F)$	$P_{V_1}(F)\ P_{V_2}(F)$	$P_{V_1}(T,F)\ P_{V_2}(F)$
$P_{V_2}(T,F)$	$P_{V_1}(T)\ P_{V_2}(T,F)$	$P_{V_1}(F)\ P_{V_2}(T,F)$	$P_{V_1}(T,F)\ P_{V_2}(T,F)$

3. **Attack Assessment Phase:** This Phase is conducted inside the front-end server and it resides in the Cloud Fusion Unit (CFU). It fuses the converted *bpa's* and based on normalized factor it assess the attack. Thus, it uses Dempsters combination rule for obtaining combined results of VMs for observing the impact of DDoS flood attack. This is used for maximizing the DDoS true positive rates and minimizing the false positive alarm rate. P_{V_1,V_2} is calculated from the Eq. (6) and Truth Table presented on Table 2.

2.3 Service Model of Cloud Shield

We have identified the basic symptoms of a DoS or DDoS attacks. These symptoms are system speed gets reduced and programs run very slowly, large number of connection requests from a large number of users and less number of available resources.

We have also resolved the IP spoofing issue. In case of IP spoofing, an attacker tries to spoof the users that the packets are coming from reliable sources. Thus, the attacker takes control over the client's data or system showing himself as the trusted party. Spoofing attacks can be checked by using encryption techniques and performing user authentication based on key exchange technique. Technique like IPSec helps in mitigating the risks of spoofing. We have analyzed this and implemented multi factor authentication, which reduces the possibility of IP spoofing.

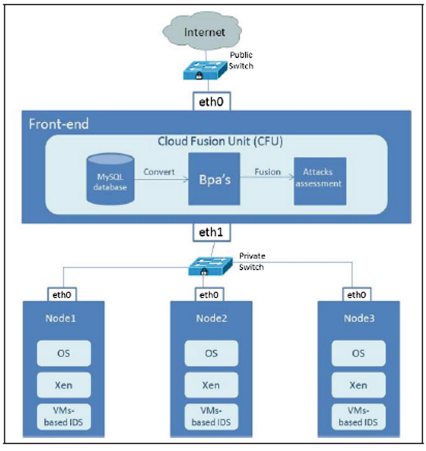

Fig. 2. Cloud shield

Algorithm 1. Conversion of Alerts into BPA's

Input: Alerts received from VM's .
Output: Probabilities.
$\{P_{UDP}(T), P_{UDP}(F), P_{UDP}(T,F)\}$.
$\{P_{TCP}(T), P_{TCP}(F), P_{TCP}(T,F)\}$.
$\{P_{ICMP}(T), P_{ICMP}(F), P_{ICMP}(T,F)\}$.

1: **for** each VM node **do**
2: Capture {UDP; TCP; ICMP } packets.
3: **for** each packet X ∈ {UDP; TCP; ICMP } **do**
4: Query the alerts from the database when a X attack occurs for the specified VM node.
5: Query the total number of possible X alerts for each VM node.
6: Query the alerts from the database when X attack is unknown.
7: Calculate the Probability (True) for X, by dividing the result obtained at step 1 with the result obtained at step 2.
8: Calculate the Probability (True, False) for X, by dividing the result obtained at step 3 with the result obtained at step 2.
9: Calculates probability (False) for X: 1- {Probability (True) + Probability(True, False)}
10: **end for**
11: Calculate the probabilities for each VM by the FTA given in Fig. 3. Figure 3 only shows the calculation of the probabilities (i.e. P_{V_1}(T),P_{V_1}(F),P_{V_1}(T, F)) for the first VM node.
12: With the help of FTA the values of belief (Bel) and plausibility (PL) for each VM is calculated as follows :
13: Bel(V_1) = P_{V_1}(T)
14: PL(V_1) = P_{V_1}(T)+ P_{V_1}(T, F))
15: This Calculation is done also for VM node V_2 and V_3.
16: **end for**

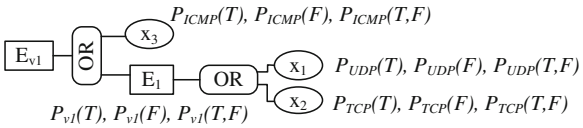

Fig. 3. Fault tree analysis for one VM

Our service model provides secure connection and convenient exposed Open APIs to the user for accessing to the cloud service. We have consider cloud orchestration environments and Single Sign-On Token to provide seamless experience to user. Furthermore, we provide possible technologies for cloud collaboration. The details of each component of service model are shown in Fig. 4.

1. **Client:** Client can retrieve the resources with the help of web browser enabled devices like PDA, laptop or mobile phone which require multi factor

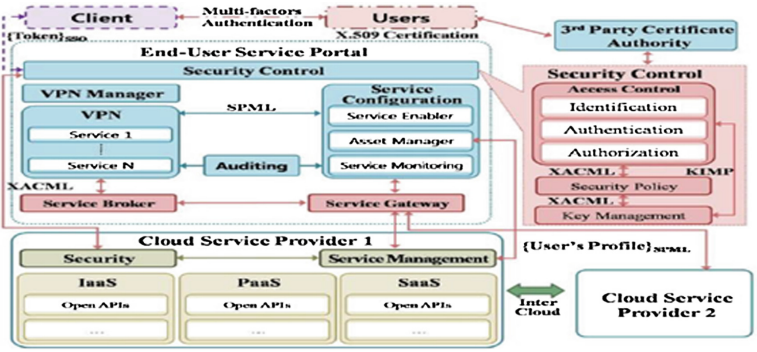

Fig. 4. Service model of cloud shield

authentication. Multi-factors authentication is done based on the certificate issued by Cloud Shield.

2. **Users:** In this component, client which enables the multi factor authentication, is able to get X-509 certificate for the user interaction.
3. **End-User Service Portal:** When clearance is granted, a Single Sign-on Access Token (SSAT) could be issued using certification of Client. Then the access control component shares the user information related with the security policy and verification. User could use services without limitation of service providers.
   - **Service Configuration:** The service enabler makes provision for Cloud Shield service using user's profile. This user's profile is provided to the service management in cloud service provider for the integration and interoperation of service provisioning requests from user. The Service Provisioning Markup Language (SPML) can be used to share user's profile. The asset manager requests user's personalized resources withuser's profile SPML to cloud service provider and configure service via VPN connection.
   - **Service Gateway, Service Broker:** A service gateway manages network resources and Virtual Private Network (VPN)on the information life-cycle of service broker.
   - **Security Control:** The security control component provides significant protection for access control, security policy and key management against security threats.
   - **VPN Manager:** An automated service monitoring systems guarantees the high level of service performance and availability.
4. **Cloud Service Providers (CSP):** This component is used to provide any type of resource as a service for an users.
5. 3^{rd} **Party Certificate Authority:** This component enables trust between user and CSP to authenticate with each other and exchanges of service with each other.

3 Conclusions and Future Work

In this paper, we have proposed a collaborative approach for DDoS detection and prevention based on third party auditors. This approach uses DST for DDoS detection and prevention. Three valued logic value of DST makes it ideally suited for cloud storage. Easy DDoS prevention in cloud environment is possible by Cloud shield. We have discussed security service model of our approach and their prevention criteria in the cloud environment. This helps to provide security with much extent. We also addressed the issue of IP spoofing. Our approach shows tremendous improvement from state-of the art work in the area of DDoS detection and prevention in cloud environment.

This technique supports to prevent the different DDoS attacks with less overhead. In future, we will able to include performance and security comparison of this technique with other techniques.

References

1. Saxena, R., Dey, S.: Collaborative approach for data integrity verification in cloud computing. In: Martínez Pérez, G., Thampi, S.M., Ko, R., Shu, L. (eds.) SNDS 2014. CCIS, vol. 420, pp. 1–15. Springer, Heidelberg (2014)
2. Ruj, S., Saxena, R.: Securing cloud data. In: Cloud Computing with e-Science Applications, pp. 41–72. CRC Press (2015). ISBN:978-1-4665-9115-8
3. Garber, L.: Denial-of-service attacks rip the Internet. IEEE Comput. **33**(4), 12–17 (2000)
4. Yahoo on trail of site hackers (2000). http://www.wired.com/techbiz/media/news/2000/02/34221
5. Powerful attack cripples Internet (2002). http://www.greenspun.com/bboard/q-and-a-fetch-msg.tclmsgid=00A7G7
6. Australian computer emergency response team, Australian Computer Crime and Security Survey (2004)
7. Gordon, L.A., Loeb, M.P., Lucyshyn, W., Richardson, R.: CSI/FBI Computer crime and security survey (2005)
8. Arbor networks, Worldwide Infrastructure Security Report, vol - IV, October 2008
9. Siaterlis, C., Maglaris, B., Roris, P.: A novel approach for a distributed denial of service detection engine. National Technical University of Athens, Athens (2003)
10. Siaterlis, C., Maglaris, B.: One step ahead to multisensor data fusion for DDoS detection. J. Comput. Secur. **13**(5), 779–806 (2005)
11. Guth, M.A.S.: A probabilistic foundation for vagueness and imprecision in fault-tree analysis. IEEE Trans. Reliab. **40**(5), 563–569 (1991)
12. Cloudera (2014). http://www.cloudera.com/content/cloudera/en/downloads.html
13. XenServer (2014). http://xenserver.org/open-source-virtualization-download.html