A Study on Security Methods and its Counter measurements against DXDoS attack in Cloud Computing Environment

J. Vijayalakshmi and Dr. C. R. Rene Robin

Received 28 January 2017; Accepted 14 May 2017; Available online 25 May 2017

Address For Correspondence:
Mrs. J. Vijayalakshmi, Research Scholar, Anna University, Associate Professor, Sri Sai Ram Engineering College, West Tambaram, Chennai 44.
E-mail: jr_viji@hotmail.com

ABSTRACT
Cloud Computing facilitates IT related resources to the required people based on, on-demand and pay per usage basis. The key characteristics of Cloud are multi-tenancy, elasticity, resource provisioning, and metered services. In the enterprise world, medium scale and small scale companies started to migrate towards Cloud Computing, as they need to complete huge computational task within low budget. Therefore the security to Cloud is very important. Cloud Computing finds its root in SOA, which is an architectural paradigm and provides IT resources as services to the internet world. Webservice is a technology used to implement SOA. Cloud computing supports two kinds of webservices, REST based services and XML based services. Making these XML based webservices available to all required users is important. Huge amount of illegitimate traffics target at cloud webservers and tamper the Cloud resources like bandwidth and connectivity. This research paper provides an in-depth study on Distributed XML Denial of service attack (DXDoS) against XML webservices and their counter measurement in the cloud environment.

KEYWORDS: Cloud Computing, Webservice, REST, SOA, DXDoS

INTRODUCTION

Cloud Computing is a delivery model for IT services. In Cloud computing rather than a direct connection to the server, resources are retrieved through the usage of web applications and web-based tools. Software packages and data are stored in servers.[16]

No longer Cloud computing is on its horizon, it started to move to its next step in the IT world. Cloud computing is a new de facto standard in every division of society as well as become the new strategic tool in enterprise computing. As Cloud offers efficient use of IT software and hardware investments, scalability, agility, metered service, on-demand service, elasticity it is beneficiary if we move storage and application capabilities, infrastructure, application development environments, and even security capabilities to the Cloud.[16]

1.1 Importance and benefits of Cloud Computing:

In Cloud environment Low Cost and scalability are the main benefits. We need not purchase any hardware and software to lobat business automation problems. In this environment, we can provision a cloud computing
platform, and scale up to any level we need which is directly in line with the money we’re spending. Thus, we pay for just what we leverage, and can scale on demand. In Cloud environment risks and costs go way down, and speed-to-deployment and efficiency become a main benefit of leveraging cloud computing.[16]

For the past few years, organizations around the world making tremendous effort to address the challenges in Cloud Computing environment, it has transformed how governments function and how different companies do their business. Enterprises are now leveraging the cloud for cost benefits, operational benefits, and flexibility. In the first half of 2016, 274 DDoS attacks have been observed. On Oct 2016 DYN – one of world’s largest Internet Service Provider (DNS Service provider), there was a big DDoS attack due to which organizations couldn’t perform the important business operations & access critical business applications. As Dyn went offline, large number of DNS were down. Especially SaaS users came to stand still.[13]. Enterprises which are doing their business successfully — are currently moving all their services to the Cloud environment and depend on it, to help manage software and hardware — will soon have no IT infrastructure or headquarters.[17]

2. DoS attacks in cloud environment:

The Denial of Service attack is against the availability objective of secured cloud. There are different denial of service attacks exist, even though the target of all of the attack is the same i.e. unavailability of service. Different DoS attack adopt different execution mechanism and produce different impact on a server and the network, so they need different defense mechanism to protect against them. [17]

2.1 Generic Types of DoS attacks:

Different types of Denial of Service attacks are as follows:

1. **Bandwidth exhaustion:**
   In this attack, the hacker exhaust the bandwidth of the victim by sending a huge volume of data chunks, which the victim is unable to handle and thereby its service is not available to the outside world. Ex. ICMP flooding[7]

2. **Flow in protocol specification:**
   The basis of this kind of attack is, finding the vulnerability that exist in the specification of various protocols such as ICMP, SNMP etc. and overload the resources of the victim. Ex. Smurf attack, SYN flood [7]

3. **Application Layer Orientation:**
   This type of attack concentrate on specific webservice/webapplication and sends the HTTP request beyond the limit, what the victim could handle. Ex. XDoS attack, HDoS attack [1]

2.2 Specific types of DoS attack:

The following table summarizes the different Denial of Service attacks and their impacts

<table>
<thead>
<tr>
<th>S.No</th>
<th>Name of DoS</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ICMP Flood</td>
<td>The victim will be saturated by the ICMP Echo packet by the attacker, for which the victim sends back the ICMP reply. The bandwidth utilization is maximized [8][6]</td>
</tr>
<tr>
<td>2</td>
<td>Ping of Death</td>
<td>Attacker sends a flood of pings to the intended victim. The ping packets will saturate the victim’s bandwidth.[8]</td>
</tr>
<tr>
<td>3</td>
<td>Smurf</td>
<td>A variation of a ping attack. It uses the same vehicle, a ping packet with two extra twists 1. The attacker changes the source address in the ping packet so that it appears as if it come from the victim. 2. The attacker sends this request to the network in broadcast mode, broadcast mode packets are distributed to all hosts on the network. [8]</td>
</tr>
<tr>
<td>4</td>
<td>SYN Flood</td>
<td>This attack uses the TCP protocol suite, making use of its basic session-oriented nature and work against the victim. In this attack the attacker sends many SYN requests to the victim server and never sends back the response with ACKs, thereby saturating the victim’s SYN_RECV queue.[8]</td>
</tr>
<tr>
<td>5</td>
<td>DNS attack</td>
<td>By overtaking a name server or causing it to cache unauthentic entries (called DNS cache poisoning), an attacker can redirect the routing of any traffic, with an implication for denial of service.[8]</td>
</tr>
<tr>
<td>6</td>
<td>HDoS</td>
<td>Attacker uses HTTP Get and HTTP Post request messages to flood the victim. If the web server is overloaded with many HTTP Get request, CPU and Memory exhaustion of server will happen. The HTTP POST request is more complex as it involves input data from forms, which requires more computation from the server side. So HTTP POST DDoS attack is</td>
</tr>
</tbody>
</table>
5. **DXDoS attacks in cloud environment:**

   XML denial of service attack is a content-borne type and its purpose is to shut down the web service or the web server which is running that web service. In this Denial of Service attack, the aspiration of attacker’s is to reveal information that he can use for crashing the Web application process, thereby the entire cloud. DoS may disable the users’ computer or network where the attack can, for example, prevent data exchanging between two sites. XDOS attack dealt with compromising many clients called zombies to attack the victim system simultaneously using SOAP messages. [18]

3.1 **Types of XDoS attack:**

   - **Attribute Blowup attack:**
     Under this attack XML elements with large number of attributes is created, which will monopolize the victim processor for a long period of time.
   
   - **Billion Laughs attack:**
     Which is nothing but nesting entities within other entity.

   - **Quadratic Blowup attack:**
     In this attack one very large entity is defined and refers to it many times.

   - **External Entity Attacks:**
     
     (i) It is due to the external entity functionality, in which the parser is engaged to a resource long period of time; i.e. sending the parser into an infinite wait loop.
     
     (ii) Write an unlimited number of a character (one million at a time) to the response stream and eat up a huge amount of memory in a very short amount of time.
     
     (iii) The external entity is pointing to a very big resource on a third-party Web site.
     
   In this external entity the victim server is spending its own resources (memory, processor time and bandwidth) to attack itself or the other servers on the same network.

4. **Challenges:**

   Due to the availability of advance attack tools, DXDoS attack is prevailing in Cloud environment. The challenges that are faced, due to DXDoS are given below: [13][14][18]

4.1 **Webserver Resources:**
When DDoS happened the resources that are affected at webserver side are CPU, Bandwidth and Memory. As illegitimate request are processed, the legitimate access to legitimate resources are denied to legitimate users.

4.2 Traffic flow classification:
When the intensity of attack packet is high, without any classification method, it is difficult to separate the legitimate traffic flow and malicious traffic flow.

4.3 Speed:
In the high speed network the number of nodes, protocol, attack intensity and other attack parameters are unpredictable. As a consequence, the defense method should be highly reactive in high speed network.

4.4 Real Datasets:
Non availability of standard datasets and testing platforms are the real challenge in DDoS solution environment.

4.5 Attack Signature:
Maintaining a comprehensive list of all DDoS attack signature is very difficult in real time environment.

4.6 Open Architecture:
The openness and collaborative nature of internet is exploited to pollute the machines and networked devices. Polluted nodes should be traced and removed quickly, to prevent the infection to other nodes.

5. Counter Methods for DDoS Attack:
5.1 Filter tree approach:
In this approach client request is framed in XML format and embedded in SOAP packet which is doubly signed along with client IP address, client puzzle and client puzzle solution. IP traceback packets which are not matching, to Cloud defender. Cloud defender filters the attack packet with the aid of 5 filters namely hop-count filter, sensor filter, Puzzle resolver filter, IP Frequency Divergent filter and Double signature filter. It is not detecting the attack in network layer and transport layer and failed miserably. [1][14]

5.2 Decision Tree:
ENDER – pre-decision, advanced Decision, learning System. ENDER applies two decision theory methods (implemented using CLASSIE and RAD) to detect attack traffic and marks the attack message. Detection rate is not up to the mark. Detects the attack only in application layer [3]

5.3 Service Oriented Traceback Architecture:
As the attacker tries to hide his identity, Service Oriented Trace Back- SOTA’s main objective is to identify the true identity of bogus messages, in which to avoid current defense systems and escape prosecution. To accomplish the main objective, SOTA should be attached as close to the source of the attack. When an incoming SOAP message comes into the router, it is tagged with user defined SOAP header. The header can be used to traverse the network back to the true source of the attack. Initial stage authentication part is missing and it was not tested in Grid and Cloud environment. [4][15]

5.4 Metrics based on Information theory:
This method works in two phases, behaviour monitoring and behaviour detection. In the first phase, normal web user behaviour is identified during non-attack period and an entropy value for requests per session is calculated and a trust score is assigned to each user. During behaviour detection phase, the entropy value for each request is calculated and compared with a threshold value. If it exceeds the threshold value, then the request packets are considered malicious and dropped immediately. If calculated entropy is less than threshold, and then based on the trust score of the user and difference in entropy value, the rate delimiter restricts the user access. [10].

5.5 SOA based:
approach – In this approach, the ingress router is acting as the repository for WSDL file and protect the web server from outside world’s sling and slang. Packet Marking is used to mark the sender’s IPAddress. Later using Cloud protector traced back. The ingress router works in attack mode/normal mode under demand. The solution concentrates only the application layer. [11]

5.6 Against SIPDAS approach:
Stealthy attack patterns are prevalent and increasing in Cloud environment. To avoid signature detection process, polymorphic patterns of attack are induced by the attacker. Slowly Increasing polymorphic behavior increases the load of the victim system. Heap Space Monitoring algorithm is used to find the number of request given by the user who belongs to an appropriate IP address. In the mentioned approach stealth attack patterns are rewritten to detect and eliminate it. Cloud management system is overburdened due to this approach.[20][21]

**Table 2:** Summary of approaches against DXDoS attacks in cloud

<table>
<thead>
<tr>
<th>SL.No</th>
<th>Approaches</th>
<th>Characteristics</th>
<th>Downsides</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Filter tree Approach</td>
<td>1. For detecting and resolving uses five filters</td>
<td>It can detect only application layer attack[1][12]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Uses client puzzles to detect HDoS attack.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Usage of Metrics oriented to</td>
<td>1. entropy concept is used</td>
<td>Information loss may happen due to aggregation in entropy. [10]</td>
</tr>
<tr>
<td></td>
<td>Information Theory</td>
<td>2. Low false packet rejection</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Decision Tree Approach</td>
<td>1. ENDER – pre-Decision, advaNceDecision, IEaRning System. ENDER applies two</td>
<td>Here user authentication is performed in the initial stage but overhead is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>decision theory methods (implemented using CLASSE and RAD) to detect attack</td>
<td>high in terms of computational difficulties. Detection rate of only 91% is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>traffic and marks the attack message.</td>
<td>achieved.[3][9][19]</td>
</tr>
<tr>
<td>4</td>
<td>SOTA</td>
<td>1. User IP Address is marked as a tag in the header part of the SOAP packet.</td>
<td>Initial stage authentication is missing and it was not tested in Cloud</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Retrived by Cloud Protector under attack</td>
<td>environment.[4][5][15]</td>
</tr>
<tr>
<td>5</td>
<td>SOA based Module</td>
<td>Detects application layer Denial of Service attack</td>
<td>Fails to detect service denial of service.[11]</td>
</tr>
<tr>
<td>6</td>
<td>Against SIPRAS approach</td>
<td>1. Slowly Increasing Polymorphic DDoS Attack Strategy (SIPDAS) attackers attack</td>
<td>Cloud management system is overburdened due to this approach [20][21]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the victim.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Heap space management algorithm is used to overcome the same.</td>
<td></td>
</tr>
</tbody>
</table>

**Conclusion:**

The base for cloud is SOA, which is implemented using web services. Especially XML web services are exposed to DoS. In this paper, we have taken only the XML based services and discussed the different protected mechanisms against DXDoS attack. An ideal DXDoS defense mechanism should include Low False Positive Rate, Low Negative Rate, Low Detection Time, High Normal Packet Survival ratio. A defense approach that precisely recognizes the attack and reduces its effect is the future direction of this research paper.

**REFERENCES**