Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Defense Mechanism to Protect Cloud Comuputing Against Distributed Denial of Service Attacks

K.Santhi
School of Information technology,
VIT University,India.

Abstract— Cloud computing is an internet based pay as use service which provides three layered services (Software as a Service, Platform as a Service and Infrastructure as a Service) to its consumers on demand. These on demand service facilities provide to its consumers in multitenant environment but as facility increases complexity and security problems also increase. Here all the resources are at one place in data centers. Cloud uses public and private APIs (Application Programming Interface) to provide services to its consumers in multitenant environment. In this environment Distributed Denial of Service attack (DDOS), especially HTTP, XML or REST based DDOS attacks may be very dangerous and may provide very harmful effects for availability of services and all consumers will get affected at the same time. One other reason is that because the cloud computing users make their request in XML then send this request using HTTP protocol. So the threaten coming from distributed attacks are more and easy to implement by the attacker, but to security expert very difficult to resolve. So to resolve these attacks this paper introduces an approach for security services called filtering. The filter is used to detect and resolve XML and HTTP DDOS attack.

Keywords— filtering,DDOS,REST,HTTP,XML

I. INTRODUCTION

The emerged Cloud computing technology changed the current trend of business over internet and visualized as next generation architecture of IT Enterprise which moves application software and databases to large data center. The complexity of direct hardware management is reduced by moving data onto the cloud and this computing platform eliminates the responsibility of local machines for data maintenance. Business services are provided in flexible, cost-effective and delivery platform to the users by dynamically shared, scalable resources over the internet on demand. It avoids upfront fixed costs by providing users with pay for use tactic where users pays only for the service units they consume. End users are allowed to access cloud based applications through a light weight desktop or a web browser without knowing about the location and other details of computing infrastructure. Cloud providers strive to render services and performance as if the programs were installed locally on the end user's system. Despite of volume and magnitude of the cloud, the maneuver IT virtualization strategy responds to Denial of Service Attack which is most serious threat capable of crashing applications that stored centrally on cloud. XML based and HTTP based DOS is the new form which is much simpler in implementing and devastating these attacks the web services.

1.1 DENIAL OF SERVICE ATTACK

As denial of service (DoS[1]) attack has become an increasingly prevalent security threat, people realize that protecting systems against DoS attack is also one of the key security issues. Although DoS attack is becoming a fast-growing concern, most research has focused on only one type of DoS attack, where an attacker exploits a design flaw or system bug to exhaust a resource of a victim system, and thus prevent users from accessing the system service, or degrade the service quality that they can get. For example, the early work of DoS in operating systems was about this type of resource exhaustion attack. So was the later work on network DoS attacks and the latest on the distributed DoS attack. If a service is supposed to be available but it is not, then this service is said to have been denied. , a DoS attack occurs whenever access to a computer or network resource, e.g. a user account or network connection, is intentionally prevented or degraded as a result of a malicious action. The attack intentionally compromises the availability of the resource, and it is typically against the will of affected users. Resource exhaustion has been the most popular method to materialize a DoS attack, but it is not necessarily the unique one.

1.2 DISTRIBUTED DENIAL OF SERVICE ATTACK

A distributed denial-of-service (DDoS[2]) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. A hacker begins by exploiting vulnerability in one computer system and making it the DDoS master. It is from the master system that the

intruder identifies and communicates with other systems by loading cracking tools available on the Internet on multiple compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The flood of packets to the target causes a denial of service.

The owners of co-opted computers are typically unaware that their computers have been compromised; they are nevertheless likely to suffer degradation of service and malfunction. A computer under the control of an intruder is known as a zombie or bot. A group of co-opted computers is known as a botnet or a zombie army. Both Kaspersky Labs and Symantec have identified botnets -- not spam, viruses, or worms -- as the biggest threat to Internet security. The proposed work focuses on new type of DDoS attack namely XML[3] and HTTP[4] or REST based DDoS attack may provide very destructive attacks for service availability.

1.2.1 XML BASED DDOS ATTACK

The vast majority of IT professionals and business people agree that security is the leading concern for SOA and XML messages, and most quickly realize that Secure Sockets Layer (SSL) is limited by its lack of content security, auditability, and reliability. Use of XML-based Web services removes the network safety net because messages will transit ports that are open for internet access (ports 80 and 443). Existing network defences are mostly oblivious to XML and cannot deliver perimeter protection that has the necessary application understanding to be useful.

XML DoS attacks are extremely asymmetric: to deliver the attack payload, an attacker needs to spend only a fraction of the processing power or bandwidth that the victim needs to spend to handle the payload. Worse still, DoS vulnerabilities in code that processes XML are also extremely widespread. Even if you're using thoroughly tested parsers like those found in the Microsoft .NET Framework System.Xml classes, your code can still be vulnerable unless taking explicit steps to protect it.

1.2.2 HTTP BASED DDOS ATTACK

When an HTTP client (say, a Web browser) talks to an HTTP server (a Web server), it sends requests which can be of several types, the two main being GET and POST. A GET request is what is used for "normal links", including images; such requests are meant to retrieve a static piece of data, the URL pointing to that piece of data. When you enter a URL in the URL bar, a GET is also done.

POST requests are used with forms. A POST request includes parameters, which are usually taken from the input fields on the same page. When flooding, the attacker wants to submerge the target server under many requests, so as to saturate its computing resources. Flooding works best when the server allocates a lot of resources in response to a single request. Since POST requests include parameters, they usually trigger relatively complex processing on the server (e.g. database accesses), which are more expensive for the server than serving a much simpler GET.

II. RELATED WORK

[3] Chu-Hsing Lin, Chen-Yu Lee, Jung-Chun Liu, Ching-Ru Chen , "A Detection scheme for flooding attack on application layer based on semantic concept". Flooding attack is a Malicious browsing behaviour which causes resource wastage such as bandwidth, CPU time, and memory, on the cloud results in extra and unnecessary cost. Flooding attack on cloud application layer doesn't cause complete denial of service to a Web server. In this paper semantic concept is used to identify malicious browsing behaviour to improve performance and cut down the cost.

[10] Aman Bakshi, Yogesh B, "Securing cloud from DDOS attacks using intrusion detection system in virtual machine". In this paper nevertheless of company size or volume and magnitude of the cloud the tactics of IT virtualization strategy could be used in responding to denial of service attack. When there is abnormal point in inbound traffic, the targeted application is immediately transferred to virtual machine hosted in another data center.

[4] Suriadi Suriadi , Douglas Stebila, Andrew Clark, Hua Lin, "Defending Web services against denial of service attacks using client puzzle".The effectiveness of defending web services from DOS attacks using client puzzles a cryptographic counter measure which provides a form of gradual authentication by requiring the client to solve some computationally difficult problem before access is granted. Hash based puzzle is integrated into existing web service framework. Client puzzles are an effective defense against flooding and DDOS attacks.

[5] Palvinder Singh Mann, Dinesh Kumar, "Improving network performances and mitigate DDOS attack using Analytical approach under collaborative SAAS cloud computing environment". A novel algorithm which is based on an analytical approach to mitigate DDOS attacks on cloud.

[6] Andrey Belenky, Nirwan Ansari, "Tracing multiple attackers with deterministic packet marking (DPM)". A novel approach to IP trace back (DPM) is capable of tracing thousands of simultaneously attackers during DDOS attack. DPM

performs the trace back without revealing the internet topology of the provider's network which is desirable quality of a trace back scheme.

III. SYSTEM ARCHITECTURE

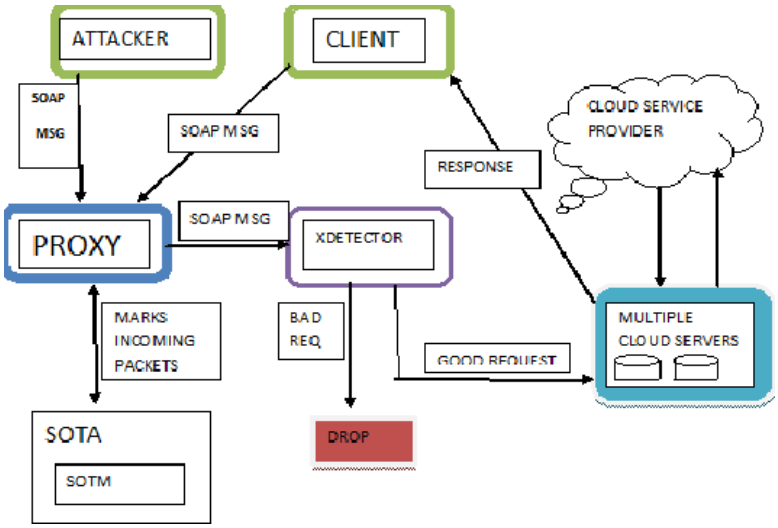

Fig 1 Architecture Diagram

IV. IMPLEMENTATION OF THE SYSTEM

In this paper, we follow Service-Oriented Trace back Architecture (SOTA), by applying our framework to OGSA. We further add to our work by introducing a defense filter called XDetector [XML Detector], in which it is distributed throughout the grid, in order to properly defend it. Our system is one of the first defense systems to attempt to defend against these new attacks. DPM methodology is applied to our SOTA framework, by placing the Service-Oriented Traceback Mark (SOTM) within web service messages. If any other web security services (WS-Security for example) are already being employed, SOTM would replace the 'token' that contains the client identification. Real source message identification are stored within SOTM, and placed inside the SOAP message. SOTM, as in DPM tag, will not change as it traverses through the network. The composition of SOTM is made up of one XML tag, so not to weigh down the message, and stored within a SOAP header. Upon discovery of an XDos or DXDoS attack, SOTM can be used to identify the true source of forged messages.

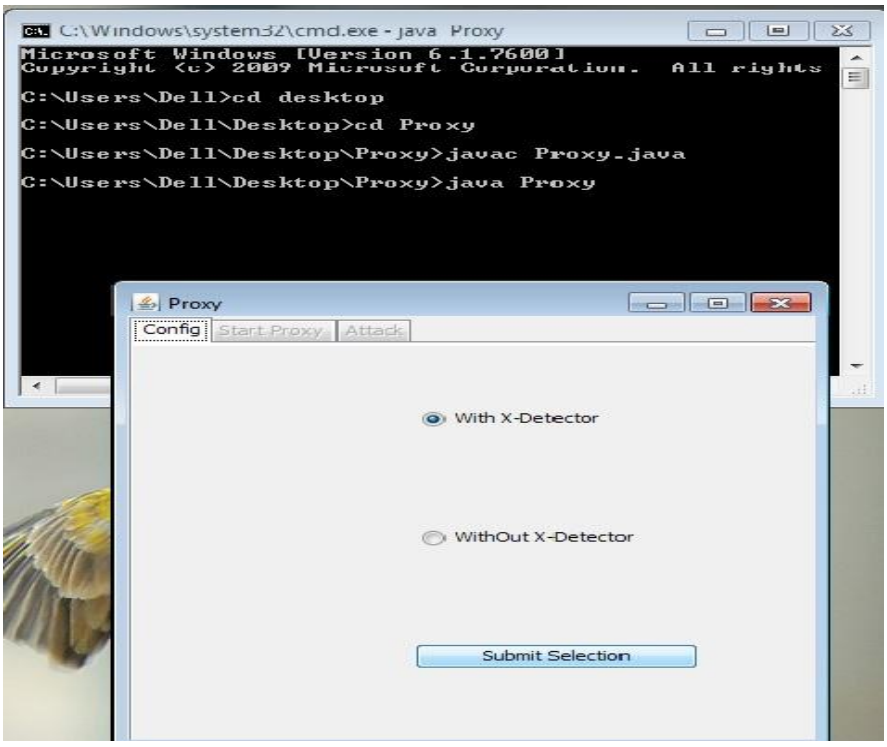

Fig 2 Proxy module

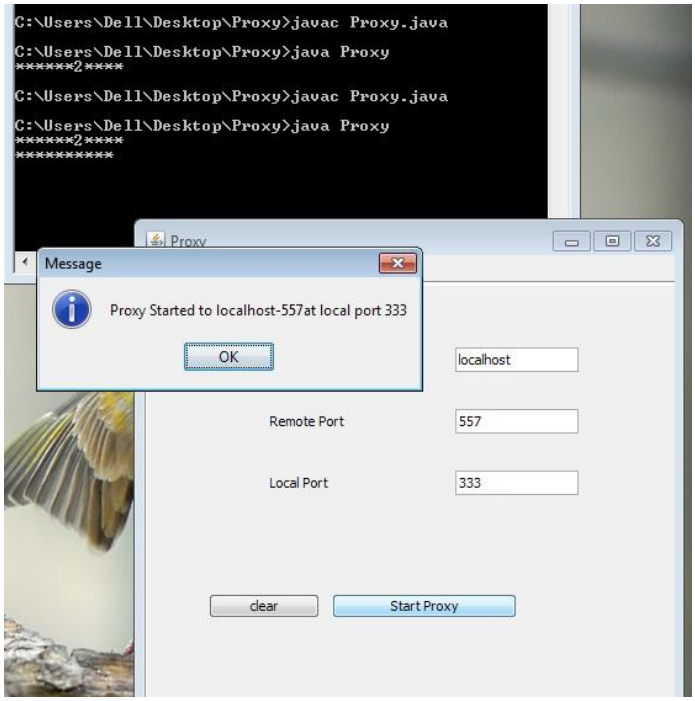

Fig 3 proxy started

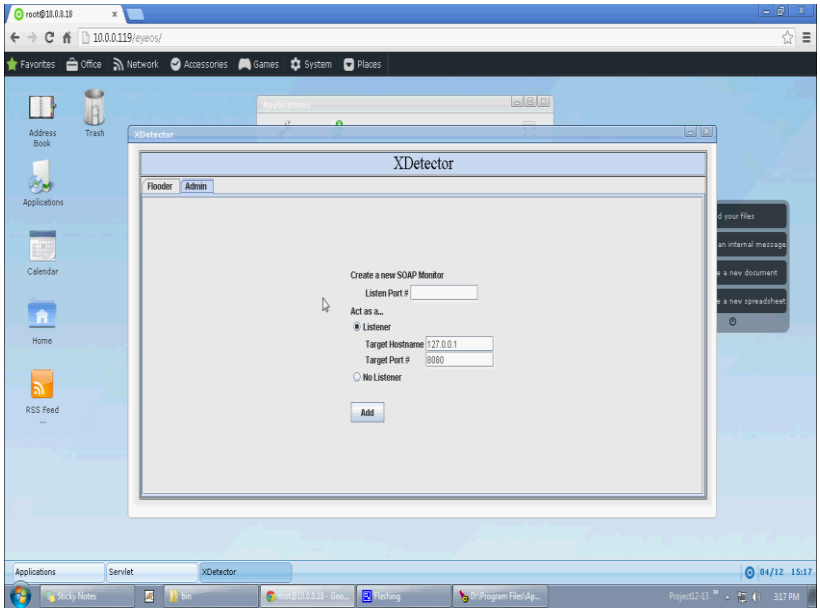

Fig 4 Xdetector

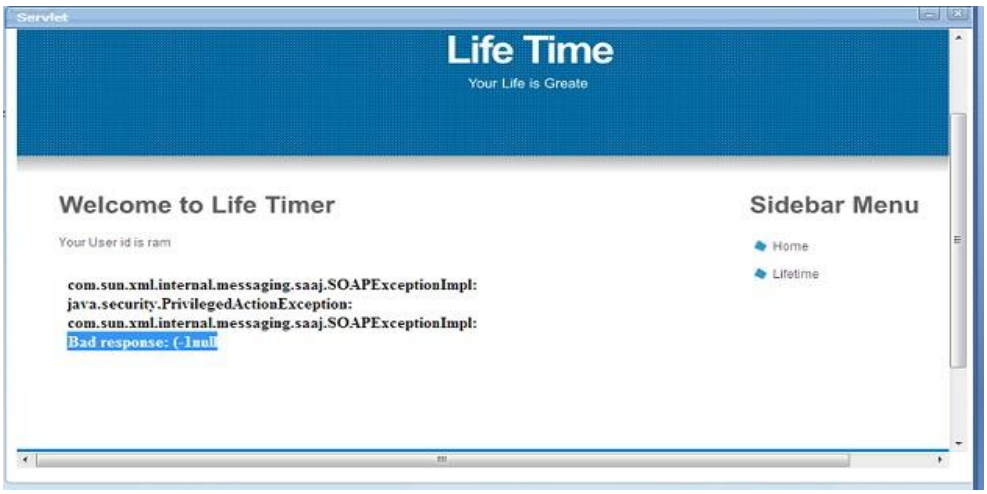

Fig 5 Bad response

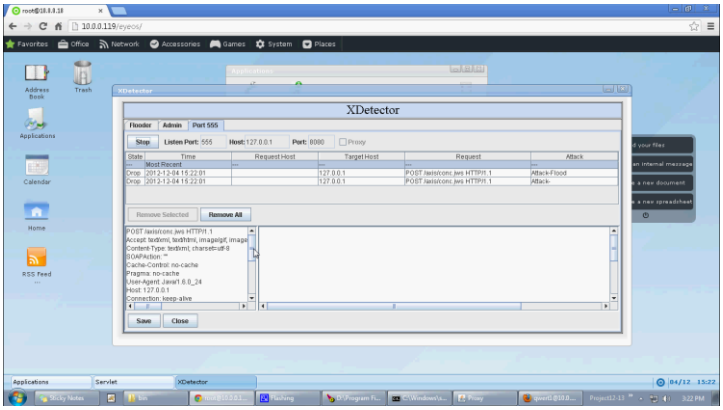

Fig 6 Xdetector sample output

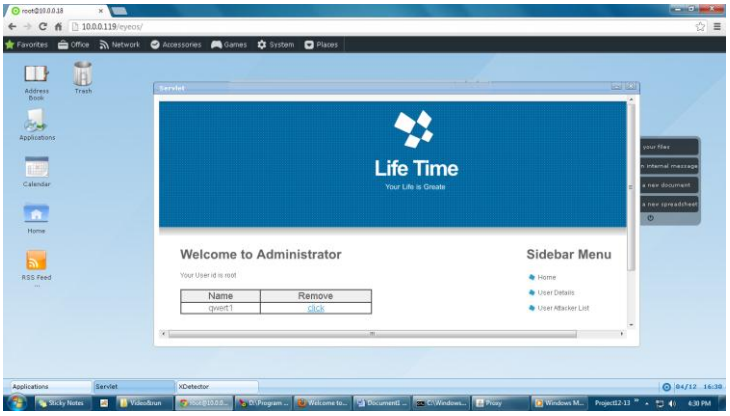

Fig 6 Attackers list

V. CONCLUSION AND FUTURE WORK

Distributed Denial of Service attack is destructive attack in the cloud since all the resources resides in single place rather than distributed. The attacker concentrates on single place to crash all the applications and the other resources since the attacks are easy to implement on the cloud and hard to resolve. Defense filter is used in this paper to detect suspicious messages and attacks. If attack is found, the corresponding request is dropped before forwarding it to server. The request is transferred to the server only when no attack is found and consequent service reply for the request would be obtained. In future, the data can be duplicated and placed in virtualized server in order to avoid the data loss.

REFERENCES

[1] [1]. Lin Fan et. al. “A Group Tracing and Filtering Tree for REST DDoS in Cloud Computing”, International Journal of Digital Content Technology and its Applications vol 4, Number 9, Dec. 2010.

[2] [2]. Dinesh Kumar and Palvinder Singh Mann, “Improving Network Performance and Mitigate Attacks using Analytical Approach under Collaborative Software as a Service(SAAS) Cloud Computing Environment”, IJCST, vol. 2, Issue 1, ISSN: 0976 - 8491, March 2011.

[3] [3]. Chen-Yu Lee, Ching-Ru Chen , Hsing Lin, Jung-Chun Liu, “A Detection scheme for flooding attack on application layer based on semantic concept”, IEEE Trans. on Software Eng., Vol.24 (5):376-390, May 2011.

[4] [4]. Andrew Clark, Douglas Stebila, Hua Lin, Suriadi Suriadi , “Defending Web services against denial of service attacks using client puzzle”, IEEE Trans. on Cloud Security, Vol.35:400-411, May 2012.

[5] [5]. Luigi Lo Iacono, Nils Gruschka, “SOAP message security validation revisited”, IEEE Trans. on Cloud Computing, Vol.26 :276-290, November 2012.

[6] [6]. Ansari and A. Belenky, "Tracing multiple attackers with deterministic packet marking (DPM)", Communications, Computers and signal Processing, 2003. PACRIM. 2003 IEEE Pacific Rim Conference on, vol.1, no., pp. 49- 52 vol.1, 28-30 Aug. 2003.

[7] [7]. F. Sabahi, "Cloud computing security threats and responses", Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.245-249, 27-29 May 2011.

[8] [8]. F.B. Shaikh and S. Haider, "Security threats in cloud computing", Internet Technology and Secured Transactions (ICITST), 2011 International Conference for , vol., no., pp.214- 219, 11-14 Dec. 2011.

[9] [9] Rajkumar Bhuya, Rajiv Ranjan and Rodrigo N. Calheiros, “Modeling and Siulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities”, Proceedings of the 7th High Performance Computing and Simulation Conference, Leipzig, Germany, June 21-24, 2009.

[10] [10]. A. Bakshi and B. Yogesh, "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine", Communication Software and Networks, 2010. ICCSN '10. Second International Conference on, vol., no., pp.260-264, 26- 28 Feb. 2010.

