ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 4, April 2016

Cloud Computing Defense Threats and Responses against DDOS Attack

Nagendra prabhu S, Dr. D. Shanthi Saravanan

***Abstract*— Cloud computing has been developed to reduce IT expenses and to provide agile IT services to individual users as well as organizations. It moves computing and data away from desktop and portable PCs into large data centers. This technology gives the opportunity for more innovation in lightweight smart devices and it forms an innovative method of performing business. Cloud computing depends on the internet as a medium for users to access the required services at any time on pay-per-use pattern, but at the same time it possesses many security risks. These types of concerns originate from the fact that data is stored remotely from the customer's location; in fact, it can be stored at any location. One of the most serious threats to cloud computing itself comes from Denial of Service attack, especially HTTP, XML or REST based Denial of Service attacks because the cloud computing users makes their request in XML then send this request using HTTP protocol and build their system interface with REST protocol such as Amazon EC2 or Microsoft Azure. So the threaten coming from distributed REST 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 introduce a security service called filtering tree, which work like a service broker within a SOA model. It is converting the consumer request in XML tree form and use a virtual Cloud defender which will defend from these types of attacks.**

***Index Terms*— Botnet, Cloud Defender, DDOS, IP Trace back, SOA.**

I. INTRODUCTION

Cloud computing is a network-based environment that focuses on sharing computations or resources. Actually, clouds are Internet-based and it tries to disguise complexity for clients. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and software in the datacenters that provide those services. Cloud providers use virtualization technologies combined with self service abilities for computing resources via network infrastructure. In cloud environments, several kinds of virtual machines are hosted on the same physical server as infrastructure. In cloud, costumers must only pay for what they use and have not to pay for local resources which they need to such as storage or infrastructure. Nowadays, we have three types of cloud environments: Public, Private, and Hybrid clouds. A public cloud is standard model which providers make several resources, such as applications and storage, available to the public. Public cloud services may be free or not. In public clouds which they are running applications externally by large service providers and offers some benefits over private clouds. Private Cloud refers to internal services of a business that is not available for ordinary people. Essentially Private clouds are a marketing term for an architecture that provides hosted services to particular group of people behind a firewall. Hybrid cloud is an environment that a company provides and controls some resources internally and has some others for public use. Also there is combination of private and public clouds that called Hybrid cloud. In this type, cloud provider has a service that has private cloud part which only accessible by certified staff and protected by firewalls from outside accessing and a public cloud environment which external users can access to it. There are three major types of service in the cloud environment: SaaS, PaaS, and laaS [1]. In cloud, similar to every proposed technology, there are some issues which involved it and one of them is reliability, availability, and security factor. For having good and high performance, cloud provider must meet several management features to ensure improving reliability, availability, and security parameters of its service such as:

- Availability management
- Access control management
- Vulnerability and problem management
- Patch and configuration management
- Countermeasure
- Cloud system using and access monitoring

II. INFORMATION SECURITY POLICIES

In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others [I]. But the most important between them is security and how cloud provider assures it. Generally, Cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivation to move to cloud. If cloud clients are academia, security effect on performance of computing and for them cloud providers have to find a way to combine security and performance. For enterprises the most important problem is also security but with different vision. For them high performance may be not as critical as academia. Well-known Gartner's seven security

Manuscript received April, 2016.

***S.Nagendra prabhu**, Lecturer,* Information Technology Dept., *College of Computing & Informatics, Wolkite University, Ethiopia.*

***Dr.D.Shanthi**, Professor & Head,* Computer Science Dept., *PSNA College of Engineering, Dindigul, India.*

issues which cloud clients should advert as mentioned below [2]:

• Privileged user access: Sensitive data processed outside the enterprise brings with it an inherent level of risk because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs.

• Regulatory compliance: Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider [3]. Traditional service providers are subjected to external audits and security certifications.

• Data location: When clients use the cloud, they probably won't know exactly where their data are hosted. Distributed data storage is a usual manner of cloud providers that can cause lack of control and this is not good for customers who have their data in local machine before moving from local to cloud.

• Data segregation: Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cureall. Encryption and decryption is a classic way to cover security issues but heretofore it couldn't ensure to provide perfect solution for it.

• Recovery: If a cloud provider broke or some problems cause failure in cloud sever what will happen to users' data? Can cloud provider restore data completely? Moreover clients prefer don't get permission to third-party companies to control their data. This issue can cause an impasse in security.

• Investigative support: Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers.

• Long-term viability: Ideally, cloud computing provider will never go broke or get acquired by a larger company with maybe new policies. But clients must be sure their data will remain available even after such an event.

III. Cloud Reliability Availability Security Issues

Using Cloud results applications and data will move under third-party control. The cloud services delivery model will create clouds of virtual perimeters as well as a security model with responsibilities shared between the customer and the cloud service provider. This shared responsibility model will bring new security management challenges to the organization's IT operations staff [4]. Predominantly, the first question is an information security officer must answer to that whether he has adequate transparency from cloud servIces to manage the governance (shared responsibilities) and implementation of security management processes such as detection and prevention solutions to assure the costumers that the data in the cloud is appropriately protected. Actually, the answer to this question has two parts: what security controls must the customer provide over and above the controls inherent in the cloud platform, and how must an enterprise's security management tools and processes adapt to
manage security in the cloud. Both answers must be continually reevaluated based on the sensitivity of the data and the service-level changes over time [4].

A. Data Leakage

Innately, when moving to a cloud there is two changes for customer's data. First, the data will store away from the customer's local machine. Second, the data is moving from a single-tenant to a multi-tenant environment. These changes can raise an important concern that called data leakage. Because of them, Data leakage has become one of the greatest organizational risks from security standpoint [5]. Nowadays, for mitigate effects of such problem there has been interested in the use of data leakage prevention (DLP) applications to protect sensitive data. But if data stored in a public cloud because of nature of it, using DLP products is valueless to protect the confidentiality of that data in all types of cloud. Inherently, in SaaS and PaaS discovery of client's data with DLP agents is impossible except when the provider put ability of it to its service. However, it is possible embedding DLP agents into virtual. Unlike the other types of clou, machine in IaaS to achieve some control over data associated. In private clouds, Costumer has direct control over the whole infrastructure; it is not a policy issue whether DLP agents are deployed in connection with SaaS, PaaS, or IaaS services. However, it may well be a technical issue whether DLP agents interoperate with your SaaS or PaaS services as architected [6]. In hybrid cloud, if service is IaaS, client could set in DLP agents for some control over data.

B. Cloud security issues

Innately, Internet is communication infrastructure for cloud providers that use well-known TCP/IP protocol which users' IP addresses to identify them in the Internet. Similar to physical computer in the Internet that have IP address, a virtual machine in the Internet has an IP address as well. A malicious user, whether internal or external, like a legal user can find this IP addresses as well. In this case, malicious user can find out which physical servers the victim is using then by implanting a malicious virtual machine at that location to launch an attack [7]. Because all of users who use same virtual machine as infrastructure, if a hacker steals a virtual machine or take control over it, he will be able to access to all users' data within it. Therefore, The hacker can copy them into his local machine before cloud provider detect that virtual machine is in out of control then the hacker with analysis the data may be find valuable data afterward [8].

B.1 Attacks in cloud

Nowadays, there are several attacks in the IT world. Basically, as the cloud can give service to legal users it can also service to users that have malicious purposes. A hacker can use a cloud to host a malicious application for achieve his object which may be a DDoS attacks against cloud itself or arranging another user in the cloud. For example, assume an attacker knew that his victim is using typical cloud provider, now attacker by using same cloud provider can sketch an attack against his victim. This situation is similar to this scenario that both attacker and victim are in same network

but with this difference that they use virtual machines instead of physical network.

1) DDoS attacks against Cloud

Distributed Denial of Service (DDoS) attacks typically focus high quantity of IP packets at specific network entry elements; usually any form of hardware that operates on a Blacklist pattern is quickly overrun and will become in out of- service situation. In cloud computing where infrastructure is shared by large number of clients, DDoS attacks make have the potential of having much greater impact than against single tenanted architectures[9]. If cloud has not plenty resource to provide services to its costumers then this is may be cause undesirable DDoS attacks. Solution for this event is a traditional solution that is increase number of such critical resources. But serious problem is when a malicious user deliberately done a DDoS attacks using bot-net [10].

Most network countermeasures cannot protect against DDoS attacks as they cannot stop the deluge of traffic and typically cannot distinguish good traffic from bad traffic. Intrusion Prevention Systems (IPS) are effective if the attacks are identified and have pre-existing signatures but are ineffectual if there is legitimate content with bad intentions[6]. Unfortunately, similar to IPS solutions, firewalls are vulnerable and ineffective against DDoS attacks because attacker can easily bypass firewalls and also IPSs since they are designed to transmit legitimate traffic and attacks generate so much traffic from so many distinct hosts that a server, or for cloud its Internet connection, cannot handle the traffic [6].

It may be more accurate to say that DDoS protection is part of the Network Virtualization layer rather than Server Virtualization. For example, cloud systems use virtual machines can be overcome by ARP spoofing at the network layer and it is really about how to layer security across multivendor networks, firewalls and load balances.

2) Cloud against DDoS attacks

DDoS attacks are one of the powerful threats available in world, especially when launched from a botnet with huge numbers of zombie machines. When a DDoS attack is launched, it sends a heavy flood of packets to a Web server from multiple sources. In this situation, the cloud may be part of the solution. it's interesting to consider that websites experiencing DDoS attacks which have limitation in server resources, can take advantage of using cloud that provides more resource to tolerate such attacks. In the other hand, cloud technology offers the benefit of flexibility, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown.

IV. Solution for Against Cloud Security Problem

Among all the attacks, One of the most serious threats to cloud computing itself comes from Denial of Service attack, especially HTTP, XML or REST based Denial of Service attacks, when launched from a botnet with huge numbers of zombie machines, because the cloud computing users makes their request in XML then send this request using HTTP protocol and build their system interface with REST protocol [16] such as Amazon EC2 or Microsoft Azure. So this paper focus on introduce a security service called filtering tree,

which work like a service broker within a SOA model. So among these different vulnerabilities this paper focused on SaaS layer. This paper is concentrating on API security. Every Cloud will have its own APIs or adapters that need to be installed or consumed if anyone wants to use that Cloud. These adapters are publically available and this paper objective is to provide security to this Open API from HTTP, XML or REST based Denial of service attacks.

The largest DDoS [15] attacks have now grown to 40 gigabit barrier this year and may reach to 100 gigabits soon. So if someone threatens to bring down the cloud system with DDoS attack cloud may become worrisome. XML-based DDoS and HTTP-based DDoS are more destructive than the traditional DDoS because of these protocols widely used in cloud computing and lack of the real defense against them. HTTP and XML [11] are important elements of cloud computing so security become crucial to safeguard the healthy development of cloud platforms. But as a virtual environment, cloud poses new security threats that differ from attacks on physical system.

A. Hop Count Filter

Hop count filter counts the number of hopes taken by message. It works on TTL (Time to Live) value. it takes initial TTL as TTL_i and final TTL as TTL_f, then it subtract both TTL value and calculate Hop Count value

$$\text{Hop Count} = TTL_f - TTL_i$$

Now it compares this Hop Count value with the value stored in the IP to Hop Count table. If value does not match then it means the coming message is spoofed message and it will be drop otherwise send to next filter.

B. IP Packet Frequency

In flooding attack attacker send the IP packets in flood. So attacker does not create new IP packets again and again but he sends same old IP flood again and again. So these flooding packets are having same frequency.

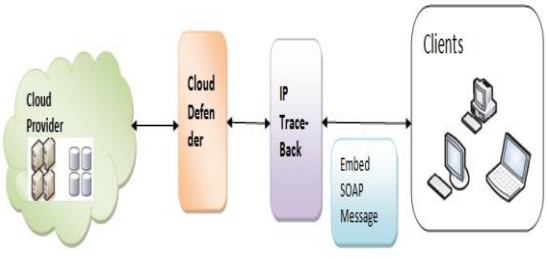

Fig. 1. System Architecture with IP Trace-back

B.1 EMBED SOAP MESSAGE

Clients or Consumers use SOAP message to request any resource from cloud providers. SOAP message used to start the communication with cloud; it works with HTTP protocol [11]. SOAP message written in XML because XML is universally accepted language and it can run on any platform.

SOAP Signature: SOAP message [12], [13] is nothing but XML tags. The process of SOAP signature as: for every message part a reference element is created and the message part is hashed and cannibalized. The resulting digest added with digest value as well as the reference of signed message is added in URI field. In last this message part and digest cannibalized and put in Signed Info part and Signature element is added in security header.

```
<Signature>
<SignedInfo>
<CanonicalizationMethod
Algorithm="..."/>
<SignatureMethod Algorithm="..."/>
<Reference URI="..." >
<DigestMethod Algorithm="...">
<DigestValue>...</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>...</SignatureValue>
</Signature>
```

Fig. 2 SOAP Message Signature

To detect coercive parsing attack using SOAP signature.

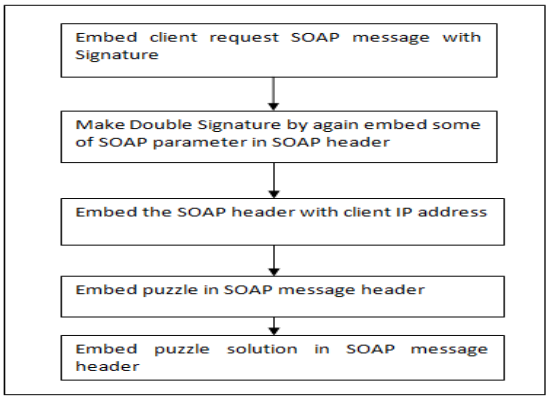

Fig. 3 Embed SOAP Message

B.2 *Double signature*

`To give the extra protection against XML rewriting attack in this paper using Double Signature by making some parameters signed again.
These parameters are as
(1) Number of children
(2) Number of header element
(3) Number of body element

Maintaining these signed parameter in SOAP Header.

B.3 IP *Marking*

At the edge router mark the IP address of client/consumer in the SOAP header.

B.4. *Client puzzle*

Client puzzle are simple type of puzzles which can be solve by any intelligent system. Client puzzle is very effective in confirming HTTP DDoS attack. Its working is very simple, Client puzzle will be part of the WSDL file and its solution is embedding in the header of SOAP Message. If any time cloud defender feels any possibility of DDoS attack, that time cloud defender simply send back the puzzle embed SOAP message to IP in doubt. If the cloud defender get back solved puzzle it means request sent by legitimate user only otherwise it will be HTTP DDoS attack.

```
<wsdl:definitions…>
<wsp:Policy wsu:Id=”clientPuzzlePolicy”>
<wsp:ExactlyOne> <wsp:All>
<wsp:clientPuzzle a:difficulty=”8” xmlns:a=”” >
abcdef</wsp:clientPuzzle>
</wsp:All></wsp:ExactlyOne></wsp:Policy>
<wsd:types…>…</wsp:types>…
</wsdl>
```

Fig. 4 Client Puzzle in a WSDL

```
<s:Envelope…><s:Header…>
<ClientPuzzleSolution xmlns=”…”…>
<timestamp>6342438044717802</timestamp>
<clientNonce>LMBfqB</clientNonce>
<puzzleSolution>abcdef….</puzzleSolution>
</ClientPuzzleSolution> …..
</s:Header></s:Body>….</s:Body></s:Envelope>
```

Fig. 5 Client Puzzle solution in SOAP request

B.5 IP TRACE-BACK

IP Trace-Back [14] is a logical file system which stores IP address in a form of list. In proposed architecture the work of IP Trace-Back is to store IP address given by Cloud Defender. When client message request pass through IP Trace-Back it matches coming message source IP address with already stored IP address. If IP matched then it discard request message otherwise it send request message to Cloud Defender.

C. CLOUD DEFENDER

Cloud defender filters the attack in five stages. These five stages are
(1) Sensor Filter
(2) Hop Count Filter
(3) IP Frequency Divergence Filter
(4) Puzzle Resolver Filter
(5) Double Signature Filter
First four filters detect HTTP DDoS attack and fifth filter detects XML DDoS attack.

C.1 Detect the suspicious message

(1) Sensor: Sensor monitors the incoming request messages. If the sensor finds that there is hypothetical increase in the number of request messages coming from any particular consumer then it marks those messages as suspicious IP otherwise send to next filter.

(2) HOP Count filter: It will calculate the Hop Count value and compare with stored Hop Count value. If no match then it marks those messages as suspicious IP otherwise send to next filter.

(3) IP Frequency Divergence: if found same frequency of IP messages then it marks those messages as suspicious IP otherwise send to next filter.

C.2 Detect HTTP DDoS Attack

All suspicious packets come to the Puzzle Resolver. It resolves the SOAP header of these suspicious messages. Firstly it finds the suspicious messages IP addresses and then send the puzzles to these IP address If the suspense IP address send the correctly solved puzzle to puzzle resolver it means it is genuine client request otherwise puzzle resolver drops the request message and send suspicious IP address to IP Trace-Back otherwise it send the request message to Double signature filter.

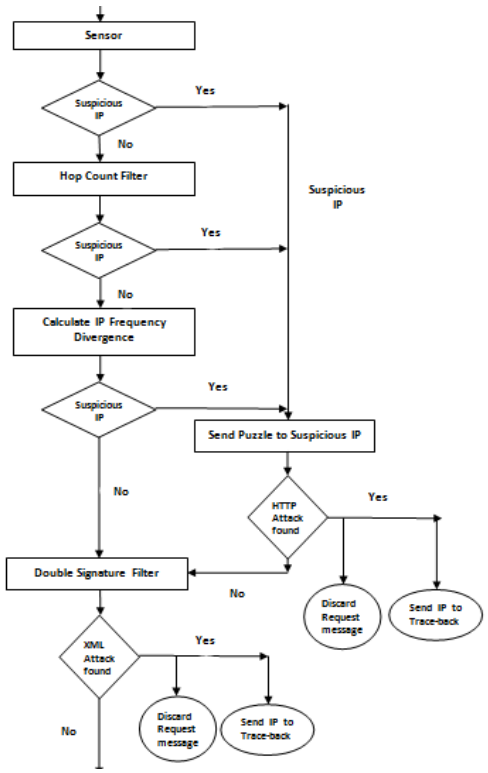

Fig. 6 Cloud Defender

C.3. Detect Coercive Parsing/XML DDoS Attack

Check the incoming request message for any open tag. If open tag found in incoming message then it discards that message otherwise send the request message to cloud provider to provide services to clients.

V. Conclusion

DDoS attack is more dangerous in cloud computing because all resources are at single place they are not distributed so attackers need to concentrate at the single place to affect all the services. As much easy to make attacks on cloud for attackers that much hard to resolve those attacks for researches so this paper filter requested message at different stages firstly matching the request client IP with previously stored suspicious IP in Trace-Back and then cloud defender is using for detecting the HTTP DDoS, Coercive parsing DDoS, XML DDoS. Cloud Defender is firstly identifying suspicious messages and then detecting attacks.

Acknowledgment

The authors wish to deeply acknowledge the College of computing & Informatics, Wolkite university, for supporting this project.

References

[I] S. Roschke, et aI., "Intrusion Detection in the Cloud," presented at the Eighth IEEE International Conference on Dependable, AutonomIc and Secure Computing, Chengdu, China, 2009.

[2] J Brodkin. (2008). Gartner Seven cloud-computing security risks. Available: http://www.networkworld.com/news/200S!07020Scloud. Html.

[3] D. L. Ponemon, "Security of Cloud Computing Users," 2010.

[4] S. K. Tim Mather, and Shahed Latif, Cloud Security and Privacy: O'Reilly Media, Inc , 2009.

[5] C. Almond, "A Practical Guide to Cloud Computing Security," 27 August 2009 2009.

[6] http://cloudsecurity.trendmicro.com/

[7] N. Mead, et ai, "Security quality requirements engineering (SQUARE) methodolgy," Carnegie Mellon Software Engineering Institute.

[8] J. W.Rittinghouse and J. F.Ransome, Cloud Computing: Taylor and Francis Group, LLC, 2010.

[9] T. Mather. (2011). Data Leakage Prevention and Cloud Computing. Available: http://www.kpmg.com/Globa1/Pages/default.aspx

[10] P. Coffee, "Cloud Computing: More Than a Virtual Stack," ed: salesforce.com.

[11] Ashley Chonka,YangXiang n, WanleiZhou, AlessioBonti(2011), "Cloud security defense to protect cloud computing against HTTP-DoS and XML-DoS attacks" *Network and Computer Applications* 34 (2011) 1097–1107.

[12] M.A. Rahaman, A. Schaad and M.Rits, "Towards secure SOAP message exchange in a SOA," in SWS'06: *Proceedings of the 3rd ACM workshop on Secure Web Services*.ACM Press, 2006, pp. 77-84

[13] N.Gruschka and L.Lo lacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," in ICWS'09: *proceedings of the IEEE International Conference on Web Services*. Los Angeles, USA: IEEE, 2009.

[14] Liming Lu et. al.; "A General Model of Probabilistic Packet Marking for IP Traceback," ASIACCS '08, ACM, Tokyo, Japan ,18-20 march 2008

[15]Bakshi, A.; Yogesh, B.; "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

[16] 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

S. Nagendra Prabhu currently working as Lecturer in Department of Information Technology, Wolkite University, Ethiopia and pursuing his PhD in Information and communication Engineering from Anna University, Chennai, India. He completed his Master of Engineering in Network Engineering from Anna University, Coimbatore and completed his Bachelor of Engineering in Computer Science and Engineering from K.C.G College of Technology, Chennai. His research interest includes Cloud computing, Botnet attack, Web based network Security. Currently the author is doing research related security issues in Cloud Computing.

.

Dr.D.Shanthi Saravanan Professor &Head in Department of Computer Science & Engineering, PSNA College of Engineering and Technology. She completed B.E. Computer Science and Engineering in 1992 from Thiagarajar College of Engineering, Madurai, Tamil Nadu and M.E. Computer science and Engineering in from Manonmaniam Sundaranar University, Tamil Nadu and PhD in Soft Computing from Birla Institute of Technology, Ranchi. She has more than 21 years of Teaching and Programming Experience. She is member of various professional societies like IEEE, CSTA, IAENG and IACSIT. Her research interests include Genetic Algorithms, Neural Networks, Intelligent Systems, Image Processing, Embedded System, M-Learning and Green Computing. She has published more than 25 papers in International Conferences and Journals and also published 5 books in computing and applications. She is the reviewer of various international journals.