Webproxy, DNS Hijacking, Layer Seven Level Security Approach: To Protect SAAS From Web based DDOS and Web Service Based DDOS Attacks In Cloud

S.Tamilselvi[1], Dr.S.Tamilarasi[2],S.Loganathan3

1. M. tech , ISCF, Dr.mgr educational and research institute, chennai

2. Associate Professor, CSE, Dr.mgr educational and research institute, chennai

3.Assistant Professor, ECE, Paavai Engineering College , Namakkal, Tamil Nadu

ABSTRACT

Cloud computing is an emerging trend in business world. Provide services to its customers on demand, services like Infrastructure services , Platform services , Software services , Network services so on. Resources are maintained in the virtual datacenters for both private and public clouds. Saas contains web application services, windows application services, tools services, console application services, third party software services so on. In web application services web based distributed denial and web services based distributed denial of attack is easily implemented hacker because web application transmitted through hypertext transfer protocol and web services through XML, WSDL .In this paper we introduce DNS hijacking security, Web proxy implementation, application level security to resolve web based and web services based distributed denial of service attacks.

KEYWORDS: web application security, web service security, ddos attacks, DNS hijaking security, web proxy implementation, cgi security.

1.INTRODUCTION

Cloud services offers platform services, software services, infrastructure services via web services. these type of services increases vulnerability which invite attackers. common vulnerabilities are

Security level attacks:

1. Dictionary attacks
2. Brute force attacks
3. Spoofing
4. Credential theft
5. Password cracking

Management level attacks:

1. Credential theft
2. Elevation of privileges
3. luring

Infrastructure layer security attacks:

1. Side channel attacks
2. Tampering
3. Eves dropping
4. Privilege elevation
5. Physical access

Platform layer attacks:

1. Buffer overflow attacks
2. canonicalization
3. Encryption
4. Tampering
5. Confidential data disclosure
6. SQL injection

Application layer attacks:

1. Connection pooling
2. Privilege elevation
3. Open redirect
4. CSRF
5. SQL Injection
6. Buffer over flow attacks
7. Encryption

Client Level attacks:

1. Session modification
2. Cookie manipulation
3. Privilege elevation
4. Buffer overflow attacks
5. Key loggers
6. Device theft

Service delivery level attacks:

1. Cookie replay
2. Ip spoofing
3. Dos attacks
4. Encryption

web based and web service based ddos attack is very dangerous when compare to other attacks.

1.1 Software services in cloud

Delivers application to its clients. all the back office details of application provided as service.

websites accessed in the internet considered as software services. for example gmail or yahoo mail provides email services. Share point as software service online via web browser.

1.2 cloud service

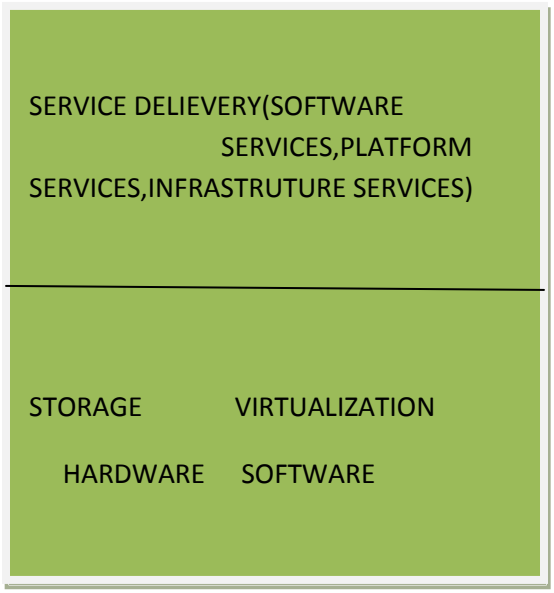

Fig 1.Cloud service

1.3 cloud service providers

Software services includes web application,SCMsoftware,CRM.software.serviceproviders Google apps, Microsoft dynamics, sales force soon. Plat form services includes Application Dev, Middleware, Enterprise portals. Plat form service providers are windows azure, Google App engine, Force.com. infra structure service includes networking, servers, storage. Infra structure service includes Amazon web service, Verizon, backspace so on.

2. RELATED WORK

Day to day cloud faces new attacks. This paper is mainly focusing on web based and web service based DDOS attacks.

commonly cloud security focuses on API ,service hacking, attack on firewall, attack on browser, confidentiality sign on, authentication problems and integrity, risk profile, data leakage, shared technology vulnerabilities so on. We analyze DDOS attacks and mitigation techniques through online, international journals, corporate solution white papers, international conference papers. According to the literature survey web application crashes under DDOS attacks in few minutes. Private and public

clouds are affected by Denial attacks in few minutes.

3.SYSTEM ARCHITECTURE

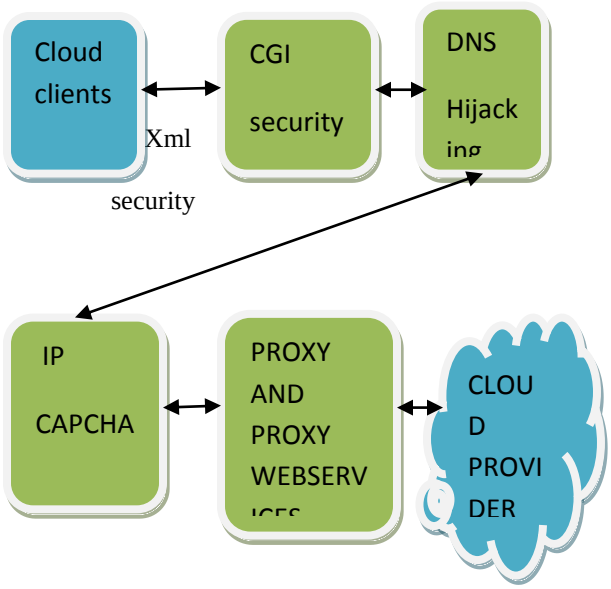

Fig 2.System Architecture

4.XML VALIDATORS AND EMBEDDING SOAP MESSAGE WITH DOUBLESIGNATURE

a) Now a days web services via XML and WSDL .REST web services uses HTTP and representational state transfer protocol principles. To avoid XML INJECTION and XML DDOS we using XMLVALIDATORS.

<!DOCTYPE transaction

<!DOCTYPE Transaction system "file">

b)parameter double signature

protection against XML rewriting by making some SOAP parameters signed again and kept with SOAP header.

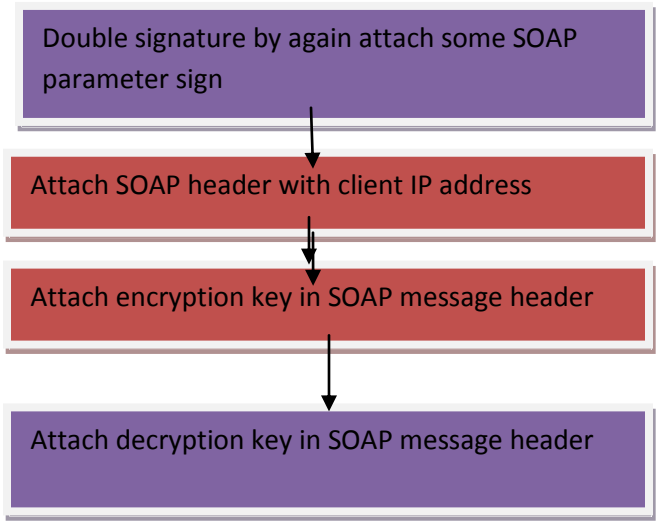

Fig 3.Attaching double signature and security keys in soap and wsdl

C)security key attachments

Encryption and decryption key attached in WSDL and SOAP request message

<wsp:Policy Xmlns: wsp=policy link

Xmlns: wsu=""

Fig4.Encrption key attached in WSDL

<wssp: decryption <wssp : message>

Wsp: Body/wssp: msg>

Fig 5.Decrption key attached in SOAP

5.CLOUD SPACE CREATION

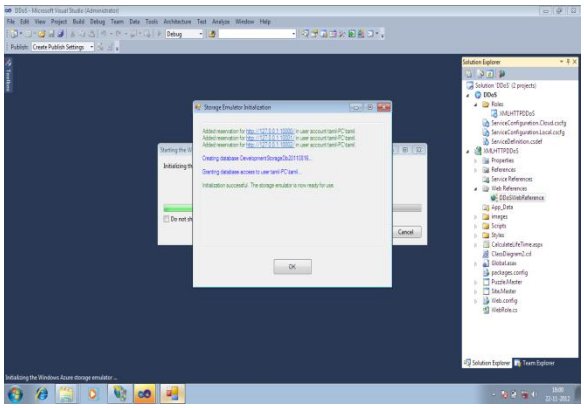

Fig 6.cloud space creation

5)CGI security

a)In private and public clouds we introduce cgi security byMD5 hash authentication ,Locking normal hypertext transfer and secure hypertext transfer. This is a infrastructure security.

b)CGI security on IIS by

- Web service extension for IIS6.0
- role service for IIS7.0

6)DNS hijacking analyzer

Analyze and scan the tcp dump of the victim. Commonly used hijacking tools are Hjsuite.

7)IP CAPCHA

Capture the suspected IP by means of

Increase no of Ip, same domain name request,. ip spoofing verified with hardware address, unique frequency.

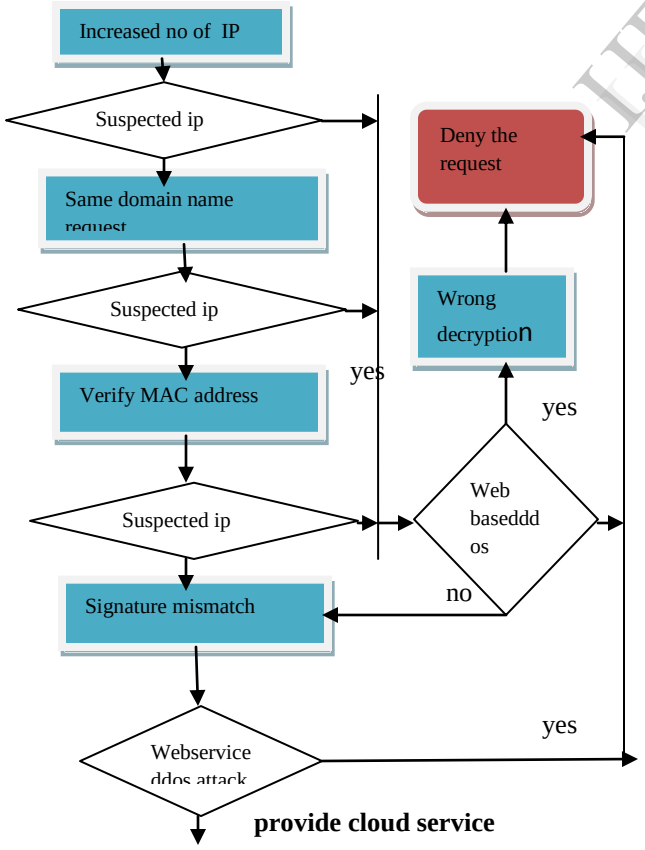

Fig 7.workflow of system

8)PROXY IMPLEMENTATION

It works as middleware between cloud server and browser. It detects system name, IP address, request URL, time which is invoked by client.

9)PROXY WEBSERVICE IMPLEMENTATION

- To scan the request.

CGI SECURITY authenticates transport and socket level transactions. If any unauthorized action takes place means lock the http and https. Dns hijacking analyzer detect the ip spoofing. If any suspected ip means deny the request.

Ip capcha responsible for monitoring suspected ip by help of MAC address verification, unique frequency of IP soon.

proxy web service responsible for detect the IP, time request, system name so on.

10)OTHER SECURITY ACTS

10.1) **A**udit log

The audit log file must be encrypted and stored in network segments.

10.2) Attach providers information

10.3) Reduce of risk patches

- Use isv to reduce risk.

10.4) Several factor authentication

More than password to prove identity . must for admin who are unable to onsite but access the production.

11)CONCLUSION

Now a days cloud DDOS attacks are challenge for medical and banking domain. Enterprises also attacked by web based and web service based ddos attacks.

To avoid this we introduce CGI authentication, DNS hijacking analyzer, IP CAPCHA , proxy web services for web based DDOS attacks.

security key and double signature to avoid web service DDOS attacks. IPCACHA uses MAC address verification , frequency verification, same domain name request.

These techniques will helpful to avoid the web based and web service based DDOS attacks.

12)REFERENCES

1.Security Manager's Journal: First task is to tighten up SaaS security By Mathias Thurman

2.Security Manager's Journal: Plugging a SaaS access hole By Mathias Thurman

3.On deterministic packet marking byAndreyBelenky, NirwanAnsari available online at science direct website

4..Asurveyonsecurityissues in service delivery models of cloud computing S. Subashini n, V.Kavitha,journal homepage: Elsevier website Journal of Network and Computer Applications

5.Availability challenge of cloud system under DDOS attackAboosaleh Mohammad Sharifi1, Saeed K. Amirgholipour1, Mehdi Alirezanejad2,Baharak Shakeri Aski1 and Mohammad Ghiami, Indian Journal of Science and Technology .

6.A Survey on Network Security Issues in Cloud Computing)International Journal of Computing Science and Information Technology, 2013, Vol. 01 (01), 29-32 ISSN: 2278-9669, January 2013 ijcsit org website. T.JohnJeya Singh,V. Praveen Kumar, A.Janet Mary,C.Menaka.

7.New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment Mohdna zriismail, International Journal of Computer Science and Security , Volume (6) : Issue (4) .

8.Securing Web 2.0 and Social Networking for Enterprise IT online web content.

9.Cloud -DoS and XML-DoS attacks by Ashley Chonka, YangXiangn, WanleiZhou, AlessioBonti. Contents lists available at Science Direct journal homepage..

10.Guidelines on Security and Privacy in Public Cloud Computing by Wayne Jansen, Timothy Grance.NSI U.S department of commerce.

11. HTTP DDoS Attack Mitigation Using Tarpitting by Joe Stewart available on web.

12.Tracing Sources of DDoS Attacks in IP Networks Using Machine Learning Automatic Defence System**,** k. subhashini , g.subbalakshmi, International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X.

13.Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud by Salvatore J. Stolfo.

15.An Efficient Way Of IP Trace back Of DDOS Attacks Based On Entropy International Journal of Communications and Engineering Volume 02– No.2, Issue: 04 March2012 Variation.

16.Time-limited black box protecting mobile agent approach for distributed secure intrusion detection system against ddos attacks ,International Journal of Communications and Engineering .