ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ACCESS CAP AND ATTESTATION TO PREVENT D.D.o.S ATTACKS IN CLOUD COMPUTING

Virender Kumar*, Hiresh Kumar Gupta, Sunil Kumar Sharma
*Associate Professor- FIMT Bareilly, India
Assistant Professor- Invertis University- Bareilly, India
Assistant Professor- Sikkim Manipal University Campus, LOME-Togo

ABSTRACT

Since the inception of computer networks D.D.o.S attacks are very much prevalent. Distributed Denial-of-Service (DDoS) attacks originate from exploited clients controlled by a remote attacker. No matter, whether it is the case of Cloud Computing, Grid Computing, or any other computing paradigm, this DDoS attack is having its impression every where. Scientists and researchers have designed various strategies to mitigate these attacks, but in none of the case cent percent success has achieved. In this research paper we present an exclusive fool proof method for enhancing service availability. In this approach every I.P is given an access cap, to access particular resources. If the client machine is looking for more attempts than the request is send for remote attestation, thereby server grants further access.

.

KEYWORDS: Cloud Computing, DDoS attacks in cloud, Access Cap, DDoS attacks.

INTRODUCTION

A distributed denial of service attack is a special type of denial of service attack. The principle involves bombarding an I.P address with large amounts of traffic from multiple sources (although orchestrated from one central point). If the I.P address points to a Web server, then it may be overwhelmed. Legitimate traffic heading for the Web server will be unable to contact it, and the site becomes unavailable. Service is denied. The fact that the traffic sources are distributed - often throughout the world - makes a DDoS attack much harder to block than one originating from a single IP address.

In this study we present a mechanism where every resource located on server is accessed a fixed number of time by a specific I.P. Once that fixed number is exhausted, resource can not be accessed by that I.P. This fixed access number is decided, by service provider. This fixed number (access cap)[5] can be high for those resources which are rarely accessed and average/low for those which are highly accessed. In cases where fixed access number is exhausted and further resource access is required than such request is send for remotely attestation by a third party (trusted computing), thereby granting further access (to a fixed number).

What is Access Cap?

Each client can access server resources any number of time, every time client requests for services, in turn server responses. Server is not aware about the fact whether the request is generated from computer or human. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) test proved to be a good step in this direction, but again advances in digital image processing made holes in CAPTCHA techniques as well . Now in this paper we are proposing **Fixed Access Number** [5]technique, this technique states that any resources located on server can be accessed a fixed number of time by a specific I.P(of Client). After consuming that Fixed Access number, resources can not be further accessed, making server un available. Now, if an I.P wants to access resources further, it has to get attestation certificate thereby making that server available. In absence of attestation certificate that IP is blocked [2] and it can not access services further. Beside this at server location a blacklist of IP address is also generated and all such IP addresses are added to its stack. Unlike, other approaches this approach is best suited where sophisticated data is needed to be accessed. And, also where the frequency of access is comparatively less.

What is remote Attestation?

Remote attestation is a method by which a client authenticates it's hardware and software configuration to a server. The goal of remote attestation is to enable a remote system (challenger) to determine the level of trust in the integrity of platform of another system (attestator)

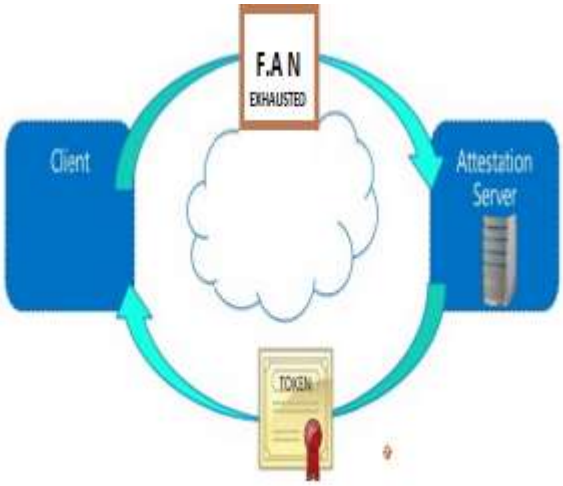

Fig 1-Role of FAN

ASSUMPTIONS IN THIS MODEL

This model is based on the fact, that DDoS attacks can only be minimized, and various techniques are available for that. One such technique is fixing a quota for accessing such resources, and when such resources are exhausted a request can be made for re allocation of quota. This seems to be a fool proof technique as; client which accesses the resources is authenticated (attested) by another party. After attestation certificate being received at servers end a quota is re allocated else not.

PROPOSED ALGORITHM

Fixed parameters
Client IP=a:b:c:d
Server IP= u:v:w:x
MaxR= Maximum request Client Can make=100
If= MaxR<=100
u:v:w:x = access
Else
u:v:w:x = Deny
If
u:v:w:x =Deny
Goto –Attestation Certificate
If
Certificate=Granted
Than
u:v:w:x =access
Else
u:v:w:x = Deny

ALGORITHM EXPLAINED

The CITFA[1] has certain shortcomings which are eliminated in this model. In this model we have provided an access cap and followed by remote attestation (if needed). In this algorithm we have chosen a server whose IP is for example u:v:w:x this server can be accessed by any number of machines, but at server level we have fixed rights to access to any fixed number of times(IN 24 Hrs). If that fixed number of time is exhausted, and the client is again requesting the server access, than that requested has to produce remote attestation certificate. Once this remote attestation certificate is received to server, a top-up of fixed number access is granted. Likewise we can prevent any big loss.

SIMULATION

We have used the above algorithm, server I.P which is denoted by u:v:w:x is taken as 64.233.161.83, client IP are multiple, which are accessing server resources, when simulated in cloud sim following results were obtained

S No	Client IP	Server I.P	Access Cap	Server Accessed	Remote Attestation	Action
1	192.168.1.1	64.233.161.83	100	80	Not Required	No action needed
2	192.168.1.2	64.233.161.83	100	50	Not Required	No action needed
3	192.168.1.3	64.233.161.83	100	70	Not Required	No action needed
4	192.168.1.4	64.233.161.83	100	10	Not Required	No action needed
5	192.168.1.5	64.233.161.83	100	3	Not Required	No action needed
6	192.168.1.6	64.233.161.83	100	60	Not Required	No action needed
7	192.168.1.7	64.233.161.83	100	10	Not Required	No action needed
8	192.168.1.8	64.233.161.83	100	40	Not Required	No action needed
9	192.168.1.9	64.233.161.83	100	50	Not Required	No action needed
10	192.168.1.10	64.233.161.83	100	00	Not Required	No action needed
11	192.168.1.11	64.233.161.83	100	40	Not Required	No action needed
12	**192.168.1.12**	**64.233.161.83**	**100**	**100**	**Required**	**Remote Attestation**
13	192.168.1.13	64.233.161.83	100	40	Not Required	No action needed
14	192.168.1.14	64.233.161.83	100	50	Not Required	No action needed
15	192.168.1.15	64.233.161.83	100	60	Not Required	No action needed
16	192.168.1.16	64.233.161.83	100	20	Not Required	No action needed
17	192.168.1.17	64.233.161.83	100	30	Not Required	No action needed
18	**192.168.1.18**	**64.233.161.83**	**100**	**100**	**Required**	**Remote Attestation**
19	192.168.1.19	64.233.161.83	100	50	Not Required	No action needed
20	192.168.1.20	64.233.161.83	100	50	Not Required	No action needed
21	**192.168.1.21**	**64.233.161.83**	**100**	**100**	**Required**	**Remote Attestation**
22	192.168.1.22	64.233.161.83	100	80	Not Required	No action needed
23	192.168.1.23	64.233.161.83	100	50	Not Required	No action needed
24	**192.168.1.24**	**64.233.161.83**	**100**	**100**	**Required**	**Remote Attestation**
25	192.168.1.25	64.233.161.83	100	50	Not Required	No action needed

Fig 2. Simulation result on CloudSim

It is evident from simulation result that in four cases out of random 25 IP taken from LAN, remote attestation is needed. After exhausting FAN which apparently is 100, the resources are blocked. This is done as it is suspected to be an activity of Bots, after attestation the services can be revoked.

CONCLUSION

In this paper we have designed a model for enhancing server availability or server uptime. As we have fixed the access number so any IP looking to access more than her fair share shall have to be pass attestation , after attesting it can access the resources further, else it will be blocked. This will block bot activities permanently, as bots may not be able to pass attestation. This will successfully prevent DDoS attacks, how ever it may take a small amount of time to re connect services while the attestation process is completed. This algorithm is not applicable for all the services where login expires after a fixed time, as attestation and re establishing services may take some time. How ever in such cases , user can re login and continue his session again. This model provides a major solution to CITFA [1] as every request having high frequency can not have the robotic origin.

ACKNOWLEDGEMENT

I acknowledge the sincere support provided to me by my institute authorities. I especially acknowledge the support given to me by Mr. Mukesh Gupta Chairman Future Group of Institutions – Bareilly , Mr. Pramod Rana, MD- Future Group of Institutions- Bareilly, and Dr Manish Sharma Director General Future Group of Institutions, Bareilly. I also acknowledge the intellectual support given to me by my co-authors, I also acknowledge, the support given by my colleagues MrRohit Singh, Mr Sunil Sharma,. I must not forget to acknowledge my family, my kids and at last almighty, without whose grace nothing is possible.

REFERENCES

1. Virender Kumar, Hiresh Gupta, Sunil Kumar, DDoS Mitigation in Cloud by Using C.I.T.F.A
2. Virender Kumar, Hiresh Gupta, Sunil Kumar, Neutralizing the Impact of Account or Service Traffic Hijacking in Cloud Computing International Journal of Electronics Communication and Computer Engineering ISSN 2249-071X Volume 5 Issue 1, Jan. 2014.
3. M.V.R Jyothisree V.Ramakrishna,Dr.A.V.Krishna Prasad, Internet Routing With Lightweight Route Attestation International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume2 Issue 8 August,2013
4. Angelos D. Keromytis, Vishal Misra, Dan Rubenstein, SOS:An Architecture For Mitigating DDoS Attacks published in Journal on Selected Areas in Communications Volume 21 No XXX,XXX20031
5. Kailash Patidar, Ravindra Gupta, Gajendra Singh, Megha Jain and Priyanka Shrivastava, "Integrating the Trusted Computing Platform into the Security of Cloud Computing System," International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 2, February 2012.
6. Gurudatt Kulkarni, Ramesh Sutar and Jayant Gambhir, "Cloud Computing-Storage as Service," International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, Vol. 2, Issue 1, Jan-Feb 2012, pp.945-950.

7. S.Sajithabanu and E.George Prakash Raj, "Data Storage Security in Cloud," International Journal of Computer Science and Technology, ISSN: 0976-8491 (Online)| ISSN: 2229-4333 (Print), IJCST Vol. 2, Issue 4, Oct. -Dec. 2011.
8. Hari Baaskar R and Gomathi A, "A Framework for Security Based Cloud by using Trusted Computing," International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 12, December 2012.
9. Nashaat el-Khameesy and Hossam Abdel Rahman, "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems," Journal of Emerging Trends in Computing and Information Sciences, ISSN 2079-8407, Vol. 3, Nn. 6, June 2012.
10. Cong Wang, Qian Wang, KuiRen, Ning Cao and Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," Services Computing, IEEE Transactions on , vol.5, no.2, pp.220,232, April-June 2012.
11. Mehdi Hojabr, "Ensuring data storage security in cloud computing with effect of kerberos," International Journal of Engineering Research & Technology (IJERT),ISSN-2278- 0181, Vol. 1, issue 5, July - 2012.