Volume 6, Issue 10, October 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Approach for Detecting DOS Attacks using Polymorphic Behavior in Cloud

E. Susmitha
M-Tech Student, Department of CSE, JNTUA College of Engineering,
Anantapuramu, Andhra Pradesh, India

Abstract*— *Cloud computing is popular because it's on-demand, shared pool resources and self service. Cloud services allow single and businesses to use software and also hardware managed by third parties at remote locations. Social networking is the example for cloud computing. It is the delivery of services in the internet. According to this, impact of denial of service (DoS) attacks involves quality and maintenance costs. So, particular attention has to be paid for stealthy attacks. Stealthy attacks undetected by the client. It shows invisible to the user and also it's harmful as the brute force attacks. In recent years, DoS attacks use low-rate traffic because of their invisibility. DoS attacks are increasing threat to the internetworking. The main aim of this proposed system to arrange stealthy patterns which leads to slowly increasing intensity trend this cause to maximum cost. Describe both into the proposed strategy and also deployed the target system in the cloud. Here service visible to the user instead of invisible by using mosaic framework and slowly increasing polymorphic DoS attack strategy (SIPDAS)agent algorithm. SIPDAS agent blocks the attacker by using resources.

Indexed Terms- SIPDAS, DoS, XML, Intrusion Detection.

I. INTRODUCTION

Cloud computing allows customers to services and cloud resources according to its demand, shared pool resources and self service. Cloud computing is nothing but sharing of resources by splitting the data [1]. Similar to electricity supply, won't worry about from where the electricity comes or transported. Every month user pay for what they consumed. Cloud computing is permanently stored in the servers and cached memory on clients include laptops, computers, sensors etc. service unavailable attacks common in cloud because of its adopted pay by use nature. It leads to services cost in cloud. DoS attack is side effect in the cloud computing , it is prone to distributed DoS (DDoS), which leads to reducing the availability and performance by the resources of the host service system (processing resources, including memory, bandwidth network [2]. This type of attacks special in the cloud due to adopted pay-by-use nature model. Cloud computing is a partial degradation service due to direct effect on costs, performance and also availability by the customer. The delay of provider to analysis the impact of degradation service i.e., due to attack or an overload it can be considered as a vulnerability [3].

The past decade, efforts have been dedicated to the detection of DDoS attacks in distributed. Prevention security mechanisms use the approaches based on time window, worst case threshold, rate controlling and pattern matching methods to differentiate between the normal system and malicious behaviors [4]. But now attackers are known that type of protection mechanisms. They try to perform activities in a "Stealthy" fashion in order to escape the mechanisms. DDos mechanisms for detection, and extend the attack response time, i.e., time of the ongoing system attack has been noticed.

This paper presents an advanced strategy to organize stealthy pattern attacks versus application running in cloud. Instead of service unavailable, the proposed work aim to make visible to that services. Based on this paradigm reduce the service cost in cloud . The pattern attack organizes in order to escape, or delay the techniques offered in the literature to detect low-rate attacks. It doesn't expose a periodic waveform distinctive of low-rate consuming attacks [5], [6], [7], [8], [9]. In direct contrast with them, it is a reiterative and incremental process. SIPDAS can be applied several attack models, that purchase known application vulnerabilities, in order to demean the service allowed by the target server application running in the cloud computing. The condition polymorphic is animated to polymorphic attacks which change message sequence at every successive transmission in order to put off signature detection mechanisms. This paper concentrates on serious terrors to cloud, which comes from XML-based DoS (XDoS) attacks to the web [10]. The data-based test bed on the mOSAIC framework that acts as purveying system damaged resources from confederation of providers.

The rest of this paper is orchestrated as follows. Related-work is exhibited in section II. Section III illustrates proposed work to anatomy the stealthy attacks, and presents the pattern attack, detailed implementation is described. Section IV shows the results and section V. Describe the Conclusion and future work.

II. RELATED WORK

DDoS attacks are determined as that class of attacks, which are cut a weak point in target design, in order to put down the performance in DoS [12]. The stealthy has been used in to describe twisted attacks that are designed to

continue the malicious behaviors invisible to the detection mechanisms. These attacks can be harder to find compared with traditional attacks [6]. The methods of establishing twisted attacks can be two classes: job-content-based and job arrival pattern-based. In universal, such attacks are performed by sending low rate traffic in order to unnoticed by the DDoS detection mechanisms [15]. The stealthy Dos refer to shrew attacks first introduced in, specifically timeout mechanisms (RTO) [12]. RoQ attacks resources to decrease the overall performance [12].

In particular, SIPDAS is a low-rate attach pattern that purchase the both LoRDAS and RoQ. One hand, it is common vulnerability in implementation. On the other side, it is dynamic operation of the adaptation mechanisms to ensure performance. Finally, works proposed in stealthy doesn't work against in the cloud environment. Cloud providers offer services to rent and storage, here transparent possible of unlimited availability. These resources are not free. Customers can pay only for usage of resources. Cloud providers offer the load balancing service, apart from auto scaling service also enabling consumers to closely follow the curve demand for their applications. Reduce the costs, when average CPU exceeds a fixed threshold. Remove that by using auto scaling.

mOSAIC framework aimed at simple way to manage applications in multi cloud environment [12]. Two main framework components use, the cloud agency and the software platform. The first component the cloud agency acts as brokering resources from confederation of cloud providers. It is small Linux distribution. File blocked in two ways either attacker block or the user or cloud can block that particular user. Cloud not block for particular file only the chance to block is attacker. so, realize user also don't know what really happens there. The mOSAIC framework checks whether the user present in the cloud or not, if cloud is present then check the files, again activate the particular user instead of deactivate by using this framework. It tells to the admin because of this reason the file was blocked [10]. Finally, load balancing mechanism automatically balances the application. In existing only the files was blocked don't login again so, here implement the user friendly security [13]. Release that file in proposed work.

III. PROPOSED WORK

This paper describes a sophisticated planning to trim stealthy patterns against applications running in the cloud. Instead of aiming service unavailable, proposed work aims to use something safe way that helps the application flexibility, and also reduce the financial cost by the service available. DDoS attacks those effort application vulnerabilities [10], [11], [12], admitting: the oversize payload attack that efforts the high memory consumption of XML processing. Deeply-nested XML is a resource debilitation attack, which efforts the XML message format by inserting a large number of nested XML tags in the message body.

Stealthy DoS: DDoS attack versus an application running server in cloud should have stealth. Regarding quality, the performance under a DDoS attack is more degenerate. Stealthy is an event it applies to computer viruses, like invisible to hacking programs. It can cause damage to networks. Stealthy is nothing but invisible. Denial of service (DoS) [15] is an authorized user's access to a computer network, it leads to malicious intent. Unusually slow network performance. DoS, DDOS are the special effects in the cloud.

***Load balancing Mechanism*:** DoS attacks are slow to detect that's why the traffic is more in cloud, the load balancing mechanism optimize the resources use, maximize the throughput and minimize the response time [6] . By using some parameters the service requests automatically up or down according to their situations, example for this is used memory and number of active users. It optimizes the resource use; here the cost is more to the customer.

***Attack approach*:** The attack pattern delays the techniques it detects low-rate attacks. In counterpoint, it is an iterative and incremental process. Attack potency is slowly increases by a patient attacker; it leads to service financial losses, even if the attack pattern is performed in accord to the maximum job size and arrival rate of request service allowed. Using experiment designed; derive an expression for increasing attack, to ensure SLA with the customer [14]. This type of attacks leads to minimize attack visibility, creating service degradation. Two attacks namely normal attack and XML attack, in XML attack, particular tag exists in different users profile, this is called polymorphic behavior but only one user tag blocked.

***SIPDAS*:** Present a strategy to implement attack patterns that decreases the problem, it is an incremental and iterative process. In first iteration limited number of flows detected [11]. Service degradation is achieved. Algorithm 1 follows the approach to perform a stealthy degradation service in the cloud. Based on the requests and resources, the requests greater than resources, then the file was blocked by the admin or master.

Algorithm 1: **Algorithm of SIPDAS Agent**

Require: Integer time Window = T {Burst period.}
Require: Integer $n_T = 0$ {Nested tags within each message.}
Require: Integer tag Threshold = N_T {Nested tags threshold.}
Require: Integer $C_{R=} I_0$ {Initial attack intensity.}

```
Repeat
  t = 0;
  While t <= T do
    n_T = pick random Tags (tag Threshold);
    t_I = compute Inter arrival Time (C_R, n_T);
    send Message(n_T, t_I);
    t = t + t_I;
  end While
```


if! (Attack Successful) **then**
$C_R = (C_R +$ attack Increment);
{Attack intensification}
else
While! (attack-detected) and attack Successful do
{
Service degradation achieved;
Attack intensity is fixed}
until Request < Resource **and** !(attack-detected)
if attack detected **then**
{
Notify to the admin that the attack has been detected**}**
Print 'Attack detected';
Else
{
Notify to the admin the attack has reached the threshold and achieved the intensity.
Print 'threshold-reached';
{
Continue the attack by using the previous C_R value
}
$C_R = C_R -$ attack increment;
Loop
N_T = pick Random tags (tag Threshold);
T_I = Compute Inter arrival Time (C_R, n_T);
Send message (n_T, t_I);
end loop
end if;

Implementation of SIPDAS attack can be done in several ways. Here, use the same framework assumed for building up the target application server SUA. when the attack is activated by the web, a parameters is sent to the Master, including the URL. The master acquires periodically information from the store and sends messages to agents in order to update their actions, according to attack strategy [13].

IV. RESULTS

Even if a person harmed , the attack process can be begin by working a different application polymorphism in the form, overtime in order to visit a action continuing for a long time. The performance degradation is achieved through SIPDAS agent, and also service visible instead of invisible by using mOSAIC framework. User has so many problems, implement the user-friendly security, and reduce the cost.

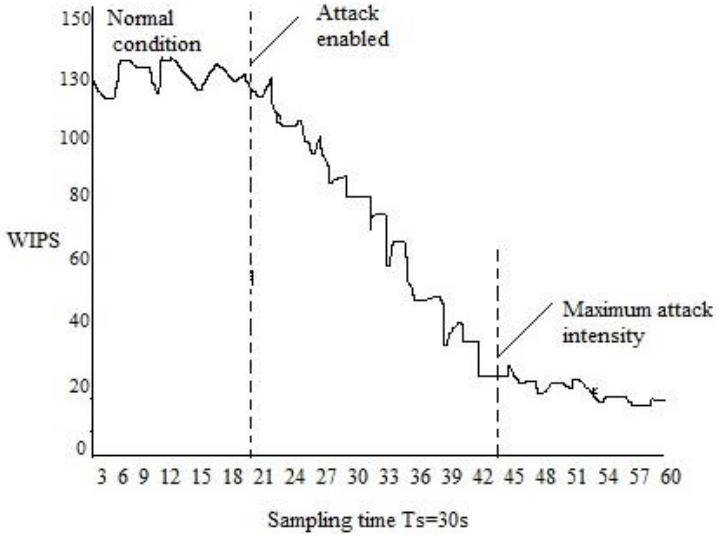

Fig.1. SIPDAS effect on the mOSAIC based application

Fig.1 shows the performance degradation by using SIPDAS agent algorithm, the attack intensity increased, the attack successful is true and attack is detected, the admin that maximum average message rate is reached and continue to inject messages formatted. The current agents reached threshold, the master replaces them with new agents, maximum level of intensity achieved by the previous agents. The attack starts with a limited number of agents. (i.e., Single Agent). Auto scaling mechanisms is enabled by the mOSAIC framework.

V. CONCLUSION AND FUTURE WORK

In this paper, propose a plan to implement attack patterns, these exposes a SIPDAS behavior that can elude, delay the techniques aimed in the literature to detect low-rate attacks. Working a vulnerability of the target application, a user and attacker can organize sophisticated flows of messages, identical from legitimate requests of service. In the proposed pattern of attacks, instead of aiming service unavailable, it aims cloud flexibility, rescale and down more resources than needed, its effects on cost than the service availability. SIPDAS attack agent take care of services available instead of unavailable by using mOSAIC framework.

In future work, carrying the approach to large set application level exposure, apart from this fixing a sophisticated method capable to detect SIPDAS attacks in cloud environment.

REFERENCES

[1] Ficco, Massimo, and Massimiliano Rak. "Stealthy denial of service strategy in cloud computing." Cloud Computing, IEEE Transactions on 3.1 (2015): 80-94.

[2] Dr. S. Vasundra et.al, CSE, JNTUACEA, "Study of Cloud Based Mobile Learning Approaches" published a paper on i-manager's Journal on Cloud Computing, Vol.2 No. 1 November 2014-January 2015.

[3] F.Cheng and C. Meinel, İntrusion detection in the cloud," in proc. IEEE Int.Conf. Dependable, Autonom. Secure Comput., Dec.2009,pp. 729-734.

[4] C. Metz. (2009, Oct.). DDoS attack rains down on Amazon Cloud [Online]. Available: http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/S

[5] K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, "Robust and efficient detection of DDoS attacks for large-scale internet," Comput. Netw., vol. 51, no. 18, pp. 5036–5056, 2007.

[6] H.Sun, J.C.Lui, and D. k. Yau,"Defending against low rate TCP attacks: Dynamic detection and protection, "in proc.12th IEEE Int. Conf, Netw. Protocol.,2004, pp. 196-205.

[7] M. Hossian and S. Bridges, "A framework for an adaptive intrusion Detection system with data mining," inProc.13thAnnu.CITSS Jun.2001.

[8] Vincent Shi-Ming Huang Hsinchu, Taiwan and Ming Chiang" A DDoS Mitigation System with Multi-Stage Detection and Text-Based Turing Testing in Cloud Computing".

[9] R. L. Carter and M. E. Crovella. Measuring bottleneck link speed in packet-switched networks. *Performence Evaluation*,27(28):297–318, 1996.

[10] A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defense to protect cloud computing against HTTP-DOS and XML DoS attacks," J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1097–1107,Jul. 2011.

[11] Dr.S. Vasundra et.al, CSE, JNTUACEA, Distributed Intrusion Detection System for Resource Constrained devices in Networks, International Journal of Compute Science and Mobile Applications, Vol 3 Issue 7 Pg 8-15.

[12] U. Ben-Porat, A. Bremler-Barr, and H. Levy, "Evaluating the vulnerability of network mechanisms to sophisticated DDoS attacks," in Proc. IEEE Int. Conf. Comput. Commun., 2008, pp. 2297–2305.

[13] S. Antonatos, M. Locasto, S. Sidiroglou, A. D. Keromytis, and E. Markatos, "Defending against next generation through network/ endpoint collaboration and interaction," in Proc. IEEE 3rd Eur. Int. Conf. Comput. Netw. Defense, 2008, vol. 30, pp. 131–141

[14] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks and counter strategies," IEEE/ACM Trans. Netw., vol. 14, no. 4, pp. 683–696, Aug. 2006.

[15] G. Macia-Fernandez, J. E. Diaz-Verdejo, and P. Garcia-Teodoro, "Mathematical model for low-rate DoS attacks against application server," IEEE Trans. Inf. Forensics Security, vol. 4, no.3, pp. 519–529, Sep. 2009.

AUTHORS PROFILE

E.SUSMITHA, received B.Tech degree in Computer Science and Engineering from Sri Venkateswara engineering college, tirupati affiliated to JNTUA University, Anantapuramu, A.P, India, during 2010 to 2014. Currently pursuing M.Tech in Computer Science(Software Engineering) from JNTUA College of Engineering, Anantapuramu, A.p, India, during 2014 to 2016. Her area of interests is Cloud Computing.

