The Security Testing and Analysis of DDoS Attacks In Cloud Computing Environment

Krishnaveni S,Dr.Prabakaran, Sivamohan S,Kanngi Mahajan VijayChaitanya

Abstract— Distributed Denial of Service attacks becoming a most serious security issues in cloud computing environment. In DDoS attack model Large number of compromised host are accumulated to send useless service requests, packets at the same time .DoS and DDoS attacks initiates the service degradation, availability and cost problems under cloud service providers. This proposed approach unified between HTTP GET flooding among DDOS attacks and Stealthy attack patterns are raised against applications running in the cloud. for a fast attack detection in cloud computing environment Slowly Increasing Polymorphic DDoS Attack Strategy (SIPDAS) can be used to detect the application vulnerabilities in the cloud. SIPDAS changes the message sequence at every successive infection to avoid signature detection process. This proposed approach enable to increase the high accuracy of the system, improve the performance and detection of HTTP GET flooding. In experiments, the processing time for performance evaluation compares with SIPDAS Detection method and Snort Detection method. According to the experiment result proved that the proposed SIPDAS Detection method is better than Snort detection method because processing time of proposed method is lower with increasing congestion. Moreover our approach can test and evaluate "cloud-to-end user" workflows and generate the vulnerability analysis report, it helps to eliminate vulnerability risk in cloud environment.

Index Terms—Cloud computing, DDoS attack, low-rate attacks,Security Testing, intrusion detection, stealthy increasing polymorphic detection approach.

1 INTRODUCTION

Distributed Denial of Service attacks becoming a most serious security issues in cloud computing environment. Cloud Computing allows customers to access cloud resources and services. On-demand, self service and pay-by-use business model are adapted for the cloud resource sharing process. Service level agreements (SLA) regulate the cost for the services that are provided for the customers. Cloud data centers are employed to share data values to the users[1]. Denial-of-Service (DoS) attack is an try by attacker to prevent legitimate users from using resources. Distributed Denial of Service (DDoS) Attacks are produced in a distributed environment. In DDoS attack model Large number of compromised host are accumulated to send useless service requests, packets at the same time[2] .DDoS attacks ensure the service degradation, availability and cost problems for cloud service providers. Brute-force attacks are raised against through specific periodic, pulsing and low-rate traffic patterns. Rate-controlling, time-window, worst-case threshold and pattern-matching are adapted to discriminate the legitimate and attacker activities[3][4]. Stealthy attack patterns are raised against applications running in the cloud. This proposed approach unified between HTTP GET flooding among DDOS attacks and Stealthy attack patterns are raised against applications running in the cloud. we propose a Slowly Increasing Polymorphic DDoS Attack Strategy can be used to detect the application vulnerabilities in the cloud. SIPDAS changes the message sequence at every successive infection to avoid signature detection process. This proposed approach enable to increase the high accuracy of the system, improve the performance and detection of HTTP GET flooding[5][6]. The flood attack name can be determined by the specific protocol that attack is made on. Due to its high similarity to legitimate network traffic and much lower launching overhead than classic DDoS attack, this new strike type cannot be efficiently detected or prevented by existing network-based solutions. They make an assumption that the target server has a finite service queue, where the incoming service requests are not permanently stored to be served by the similar application process or thread. The attack takes advantage of the capacity to forecast the time at which the answers to incoming requests for a given service occur [7] [8]. This capability is used to plan an intelligent pattern in such a way that the server that has been attacked becomes busy the most time in processing of the fake requests instead of those from true users. No such work has been proposed in the literature focus on stealthy attacks against application that run in the cloud environment.

2.BACKGROUND

2.1.CLOUD COMPUTING

Cloud service providers provide services to lease computation and storage capacity, in a way as transparent as possible, providing the effect of non-limited resources. Such resources are not free. Therefore, cloud service providers grant users to access and configure suitably the system capacity, as well as to quickly agree such capacity as their requirements change, in such a way that the user can pay only for resources what they actually use as pay as you go model. Several cloud service providers grant the unlimited services for automatically distributing the application service requests across multiple tenants, as well as the automatic scaling service for enabling user to follow the demand for their applications. In order to reduce the user costs, the auto scaling ensures that the number of the application instances increases endlessly during the demand make fast and decreases automatically during the demand lulls. For example, by using Amazon EC2 cloud services, the consumers can set a condition to add new computational instances when the average CPU utilization exceeds a fixed threshold. Moreover, they can configure a cool-down period in order to allow

the application workload to stabilize before the auto scaling adds or removes the instances. In the following, we will show how this feature can be maliciously exploited by a stealthy attack, which may slowly exhaust the resources provided by the cloud provider for ensuring the SLA, and enhance the costs incurred by the cloud customer.

2.2.DENIAL OF SERVICE ATTACK

DoS attacks have become a major threat to current computer networks .To have a better understanding on DoS attacks. This statistics involves an outline of existing DoS, DDOS attacks and major defense techniques over the internet. In this observation we describe host based and networks based DoS attack methods.DOS attacks are categorized according to the major attack types. Current available techniques are also reviewed, including variety of defense products in deployment and representative defense approaches in research survey. The different DoS attacks and defenses in 802.11 protocol based wireless networks are explored physical ,network layers and MAC. Some of the major attack names keywords are Denial of Service (DoS), Distributed Denial of Service (DDoS), Internet Security, Wireless Security, Scanner, Spoofing. DOS attack history and incidents DoS attacks started at around early '90s. At the first stage they were quite "primitive", involving only one attacker exploiting maximum bandwidth from the victim, denying others the ability to be served[1]. This was done by using different flooding attack methods. These attacks had to be "manually" synchronized by a lot of attackers in order to cause an effective damage.

2.3.CLOUD SECURITY TESTING

The Testing, validation, and process analysis of technologies and infrastructure security related to cloud-based service environments. A cloud platformexists outside your operations center location and utilizes paid hosting servers acting as your Software-as-a-Service (SaaS) platform. Shared services, virtualization, and pooled resources that are managed by you and your hosting vendor. DoS attacks can come from a single source or possibly vast numbers of malicious groups coordinating a focused assault on your infrastructure. We test and evaluate "cloud-to-client" workflows and provide a Vulnerability GAP analysis report to you and your cloud security providers to help fortify and correct this vulnerability[2].

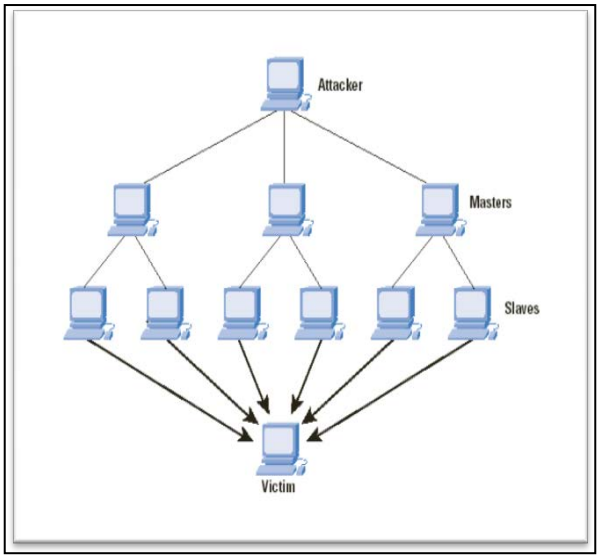

Figure 1:A taxonomy of DDoS flooding attacks.

3.SYSTEM OVERVIEW

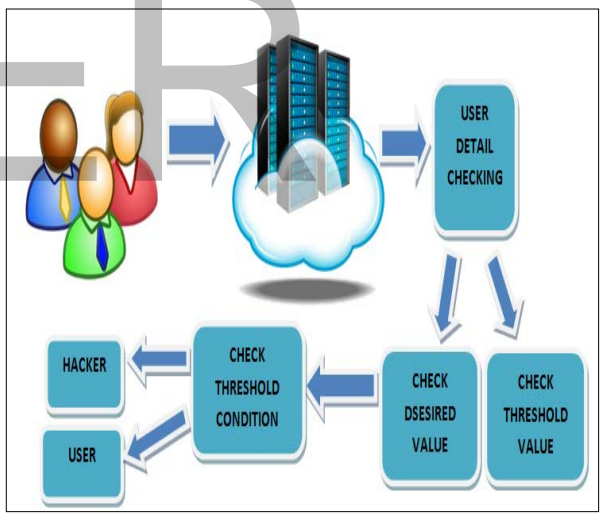

Figure 2: System Flow Diagram

System overview contain system methodology as well as system requirement for developing system as shown in figure 2 the current systems and network protocols are developed without applying security engineering that results in providing attackers many inhibited machines over the Internet. System Overview shows all description about the work done under the system.In system firstly user has to login to system then it request to the server for validation of user. After that desired value and threshold value are checked by server for checking or measuring threshold value and then decided that user is valid or not. If user is hacker then access will be denied for that and if not then he is given permission to proceed. If user is valid but he enters wrong information then after checking validity again the permission for access is given to him. System outline also contains what is the requirement for the system for development it may contain software, hardware. Software requirement contain the software use to develop system and the software use to store database of system and its feature. These inhibited and unable to match machines are used by DDS attackers as their army to launch attack. An attacker gradually inserts attack programs on these inhibited machines. Depending upon the complexity in logic of the inserted programs these compromised machines are called Masters/Handlers or Zombies and are in combination known as bots and their network is known as bonnet in attacker's community. Attackers send commanding instructions to masters, which are transferred to zombies for producing attack. In system the very first thing is user sends the request to the server then server checks the client's profile details so that it does not processes a fake request. Then final result gives a decision that if request has to be denied or accepted.

User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server.

Cloud owner Module

This module is used to help the cloud server to view details the file, if the key is correct means file will be download oth erwise we can't download the file.This paper provides a strategy to control stealthy attack patterns against applications working in the cloud. Instead of making the service not available, the proposed strategy works on the cloud flexibility, forcing the application to consume some more resources than needed, affecting the cloud customer more on monetary aspects than on the service availability.

The attack pattern is recognized in order to evade or take time to detect low-rate at tacks. It does not display a periodic waveform of such attacks. In distinction with them, it is an iterative and incrementing process. In particular, the attack potency is slowly enhanced by a patient attacker, in order to impose financial losses, even if the attack pattern is performed in accordance to the maximum job size and arrival rate of the service requests allowed in the system. The proposed attack strategy, namely Slowly-Increasing-Polymorphic DDoS Attack Strategy (SIPDAS) can be applied to such attacks, that leverage known application vulnerabilities, in order to degrade the service provided by the target application server running in the cloud. The proposed strategy of slowly-expanding polymorphic behavior persuades enough overload on the target system and avoids, or however, delays g the detection methods.

4.EXPERIMENT RESULT AND EVALUATION

This study proposes a method of integration between HTTP GET flooding attack among DDOS attacks detection in cloud computing environment. The proposed system was evaluated on two aspects: impact and performance.The performance evaluation of proposed method were tested accuracy, reliability and rapid detection of HTTP GET flooding attack. We use the NetBot attack tool for experiment and table 1 is the probability result of attack detection the environment of evaluation was measured according to the normal environment and network congestion. Finally, The comparison experiment of detection time according to the network congestion compares the average detection time by attack of 50 times between proposed method and Snort detection method The table 1 is comparison Evaluation between Previous Method and Proposed Method. Firstly, detection method based on signature cannot detect new patterns and varietal but proposed method can detect them using analysis of normal CPU usage, packet information, protocol distribution and so on. Secondly, DDoS detection method based on a threshold simply detects to use only threshold/second but proposed method shows a low error rate by threshold checking based on HTTP Response analysis .Finally, detection method based on user behavior needs definition of browsing model and analysis of all web site structure but proposed method has the advantage of simple algorithm because our method can detect a attack except analysis of web site.

Table 1
Comparison between SIPDAS Detection method and Snort Detection method

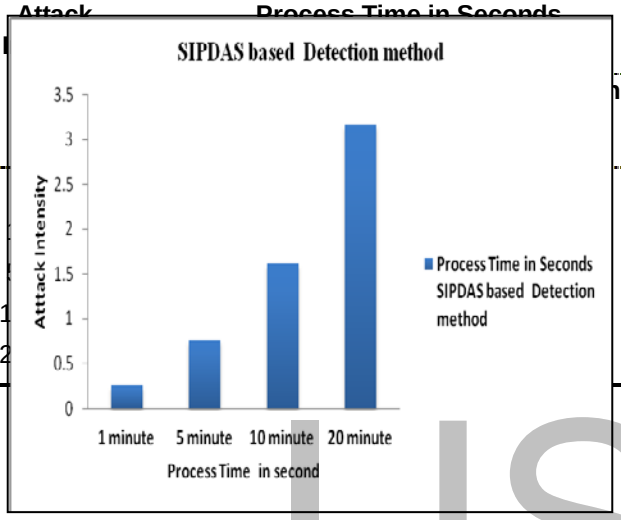

Figure 3: Process Time in Seconds in SIPDAS based Detection method

Figure 4: Process Time in Seconds in Snort based Detection method

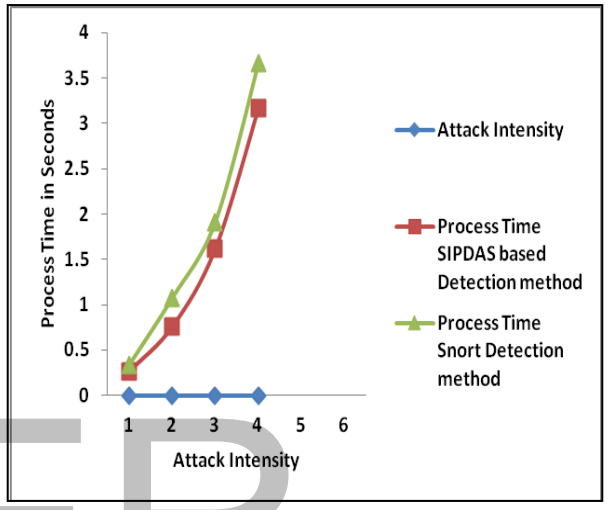

Figure 5: Comparison between SIPDAS Detection method and Snort Detection method

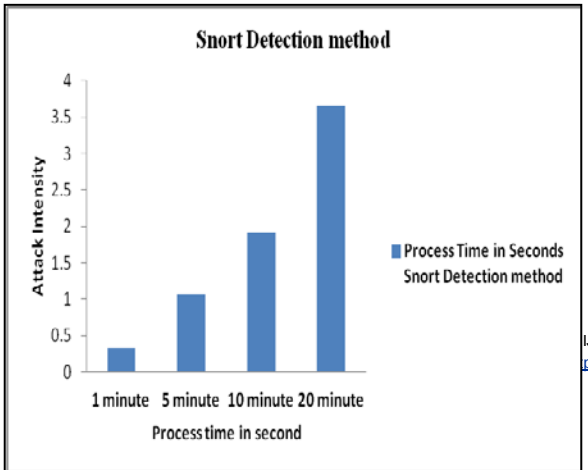

Table 2
Analysis of Different Technique against DDoS Flooding Attacks in the Cloud

Techniques	Advantage	Disadvantage	Effective Detection Parameters			
			Accuracy	Scalability	System Perfor-mance	Implementa-tion Complexity
Cooperative IDS	Increasing confidence in Proportion to an ordinary IDS	Consuming more computing time in proportion to an ordinary IDS	High	Medium	Low	low
Cloud Trace back Model	Overcoming direct DDoS Attacks, Identifying the attacker in a successful attack	Collecting the dataset is difficult for the neural net	Low	Medium	Low	High
Confidence based Filtering	Low storage capacity High speed filtering attack Packets Reducing the overhead of the server	The accuracy of the model is less than the other models	Medium	Medium	High	Low
CLASSIE	Reducing false positive rates of attacks Reducing the overhead of the server	Detecting the attacks at application level	Medium	Low	High	Medium
Filtering Tree	Filtering the attacks at different levels	Detecting the attacks at application level	Low	Medium	Low	High
Information theory based metrics	Easy deployment and decreases of negative rate	Probability of information loss due to entropy compression	Medium	Medium	High	Low

5.RELATED WORK

Sophisticated DDoS attacks are defined as that category of attacks, which are tailored to hurt a specific weak point in the target system design, in order to conduct denial of service or just to significantly degrade the performance. The term stealthy has been used to identify sophisticated attacks that are specifically designed to keep the malicious behaviors virtually invisible to the detection mechanisms. These attacks can be significantly harder to detect compared with more traditional brute-force and flooding style attacks. The methods of launching sophisticated attacks can be categorized into two classes: job-content-based and jobs arrival pattern-based[9][10][11][12][13]. In recent years, variants of DoS attacks that use low-rate traffic have been proposed, including Shrew attacks (LDoS), Reduction of Quality attacks (RoQ), and Low-Rate DoS attacks against applica tion servers (LoRDAS).

6.CONCLUSION

This study proposes a method of integration between HTTP GET flooding among DDOS attacks for a fast attack detection in cloud computing environment. This method is possible to

ensure the availability of the target system for accurate and reliable detection based on HTTP GET flooding. In experiments, the processing time for performance evaluation compares a patten detection of attack features with the Snort detection. The proposed method is better than Snort detection method in experiment results because processing time of proposed method is shorter with increasing congestion. Moreover our approach can test and evaluate "cloud-to-end user" workflows and generate the vulnerability analysis report, it helps to eliminate vulnerability risk in cloud environment Future work needs the study of various pattern recognition for DDoS attack detection in cloud computing environment.Cloud resources are shared with mutual and commercial models. Slowly-Increasing Polymorphic DDoS Attack Strategy (SIPDAS) is adapted to initiate DDoS attacks on the clouds. Cloud Intrusion Detection System (CIDS) is constructed to discover the SIPDAS attacks with flow correlation analysis. Polymorphic behavior identification and cost analysis methods are integrated with the CIDS. Cloud Intrusion Detection System (CIDS) is build to discover slowlyIncreasing- Polymorphic DDoS Attack Strategy (SIPDAS). The CIDS controls the resource consumption and cost factors. The system minimizes the application level vulnerabilities. Attack behavioral changes are automatically detected by the system.

REFERENCES

[1] M. C. Mont, K. McCorry, N. Papanikolaou, and S. Pearson, "Security and privacy governance in cloud computing via SLAS and a policy orchestration service," in Proc. 2nd Int. Conf. Cloud Comput. Serv. Sci., 2012, pp. 670–674.

[2]Cybersec Aegis Cyber security:Available at: "http://cybersec.org/cyber-security-services/penetration-testing/cloud-security-testing"

[3] S. Malek and S. Salvatore, "Detecting masqueraders: A comparison of one-class bag-ofwords user behavior modeling techniques," in Proc. 2nd Int. Workshop Managing Insider Security Threats, Morioka, Iwate, Japan. Jun. 2010, pp. 3–13.

[4] A. S. Sodiya, O. Folorunso, S. A. Onashoga, and P. O. Ogundeyi, "An improved semi-global alignment algorithm for masquerade detection," Int. J. Netw. Security, vo1. 12, no. 3, pp. 211– 220, May 2011.

[5] Yongdong Wu, Zhigang Zhao, Feng Bao and Robert H. Deng, "Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 1, January 2015

[6] Hisham A. Kholidy, Fabrizio Baiardi and Salim Hariri, "DDSGA: A Data-Driven SemiGlobal Alignment Approach for Detecting Masquerade Attacks", IEEE Transactions On Dependable And Secure Computing, Vol. 12, No. 2, March/April 2015

[7] Subrat Kumar Dash, K. S. Reddy, and K. A. Pujari, "Adaptive Naive Bayes method for masquerade detection", Security Commun. Netw., vol. 4, no. 4, pp. 410–417, 2011.

[8] Guojun Wang, Felix Musau, Song Guo and Muhammad Bashir Abdullahi, "Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce", IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 3, March 2015

[9] X. Xu, X. Guo, and S. Zhu, "A queuing analysis for low-rate DoS attacks against application servers," in Proc. IEEE Int. Conf. Wireless Commun., Netw. Inf. Security, 2010, pp. 500–504.

[10] Shui Yu, Wanlei Zhou, Robin Doss, & Weijia Jia, (2011) "Traceback of DDoS ttacks using EntropyVariations", IEEE Transactions on Parallel and Distributed Systems.

[11] Supranamaya Ranjan, Ram waminathan, Mustafa Uysal, Antonio Nucci, & Edward Knightly, (2009) "DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer attacks", IEEE/ACM Transactions on Networking,

[12] Huey-Ing Liu & Kuo-Chao Chang, 2011) "Defending systems Against Tilt DDoS attacks", 6th International Conference on Telecommunication Systems, Services, and Applications.

[13] Jin Wang, Xiaolong Yang & Keping Long, (2010) "A New Relative Entropy Based App-DDoS Detection Method", IEEE Symposium On Computers And Communications (Iscc).

[14] S. Yu, W. Zhou & R. Doss, (2008) "Information theory based detection against network behavior mimicking DDoS attack," IEEE Communications Letters, vol. 12, no. 4, pp. 319–321.