Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (96-100), Month: January-April 2016, Available at: www.noveltyjournals.com

# Multi-Channel DDOS Attack Detection & Prevention for Effective Resource Sharing in Cloud

[1]J. JANCYRANI, [2]B. NITHIA

[1]PG scholar, Department Of Computer Science and Engineering, Surya school of engineering and technology, India
[2]Assistant Professor, Department of Computer Science and Engineering, Surya school of engineering and technology, India

***Abstract:*** **The DDOS Attack in a Client Server Environment would Collapse the Entire System, but as far as Cloud is concern it is not that Effective but still it will try to Disturb the Regular Activity of the System. The proposed system, User's Request could also increase the CPU Load of the Cloud Server. Filters the Request based on the behavior and forwards to the corresponding Servers through Cloud Server. Every Server would have allocated Certain Space in Cloud Server. Our system monitors the Activity of the Users to Avoid DDOS Attacks. We Deploy once data owner upload their data along with their keyword data stored in separate server. We implement seven types of attacks. 1. Continuous & same request from single user in a point of time. 2. Different query from the same user within a period of time. 3. Different queries from different users but from same IP. 4. Request of huge sized file beyond the permitted. 5. Wrong user name & password for more than 4 times. 6. IP address of the registered user. 7. CPU utilization of the user's request. Based on these pattern user behavior is monitored DDOS attack is avoided in cloud. Mango lab is also implemented.**

***Keywords:*** **Cloud computing, sophisticated attacks strategy, low-rate attacks, intrusion detection.**

## 1. INTRODUCTION

CLOUD Computing is an emerging paradigm that allows customers to obtain cloud resources and services according to an on-demand, self-service, and pay-by-use business model. Service level agreements (SLA) regulate the costs that the cloud customers have to pay for the provided quality of service (QoS). A side effect of such a model is that, it is prone to Denial of Service (DoS) and Distributed DoS(DDoS), which aim at reducing the service availability and performance by exhausting the resources of the service's host system (including memory, processing resources, and network bandwidth). Such attacks have special effects in the cloud due to the adopted pay-by-use business model. Specifically, in cloud computing also a partial service degradation due to an attack has direct effect on the service costs, and not only on the performance and availability perceived by the customer. The delay of the cloud service provider to diagnose the causes of the service degradation (i.e., if it is due to either an attack or an overload) can be considered as a security vulnerability. It can be exploited by attackers that aim at exhausting the cloud resources (allocated to satisfy the negotiated QoS), and seriously degrading the QoS, as happened to the Bit Bucket Cloud, which went down for 19h. Therefore, the cloud management system has to implement specific countermeasures in order to avoid paying credits in case of accidental or deliberate intrusion that cause violations of QoS guarantees. Over the past decade, many efforts have been devoted to the

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (96-100), Month: January-April 2016, Available at: www.noveltyjournals.com

detection of DDoS attacks in distributed systems. Security prevention mechanisms usually use approaches based on rate-controlling, time-window, worst-case threshold, and pattern-matching methods to discriminate between the nominal system operation and malicious behaviors. On the other hand, the attackers are aware of the presence of such protection mechanisms. They attempt to perform their activities in a "stealthy" fashion in order to elude the security mechanisms, by orchestrating and timing attack patterns that leverage specific weaknesses of target systems.

They are carried out by directing flows of legitimate service requests against a specific system at such a low-rate that would evade the DDoS detection mechanisms, and prolong the attack latency, i.e., the amount of time that the ongoing attack to the system has been undetected. This paper presents a sophisticated strategy to orchestrate stealthy attack patterns against applications running in the cloud. Instead of aiming at making the service unavailable, the proposed strategy aims at exploiting the cloud flexibility, forcing the application to consume more resources than needed, affecting the cloud customer more on financial aspects than on the service availability. The attack pattern is orchestrated in order to evade, or however, greatly delay the techniques proposed in the literature to detect low-rate attacks. It does not exhibit a periodic waveform typical of low-rate exhausting attacks. In contrast with them, it is an iterative and incremental process. In particular, the attack potency (in terms of service requests rate and concurrent attack sources) is slowly enhanced by a patient attacker, in order to inflict significant 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. Using a simplified model empirically designed, we derive an expression for gradually increasing the potency of the attack, as a function of the reached service degradation (without knowing in advance the target system capability). We show that the features offered by the cloud provider, to ensure the SLA negotiated with the customer (including the load balancing and auto-scaling mechanisms), can be maliciously exploited by the proposed stealthy attack, which slowly exhausts the resources provided by the cloud provider, and increases the costs incurred by the customer. The proposed attack strategy, namely Slowly Increasing-Polymorphic DDoS Attack Strategy (SIPDAS) can be applied to several kind of attacks, that leverage known application vulnerabilities, in order to degrade the service provided by the target application server running in the cloud. The term polymorphic is inspired to polymorphic attacks which change message sequence at every successive infection in order to evade signature detection mechanisms. Even if the victim detects the SIPDAS attack, the attack strategy can be re-initiate by using a different application vulnerability (polymorphism in the form), or a different timing (polymorphism over time).

## 2. ATTACK SYSTEM

DDOS Attack in a Client Server Environment would Collapse the Entire System, but as far as Cloud is concern it is not that Effective but still it will try to Disturb the Regular Activity of the System.

**DISADVAN TAGES:**

- Increase CPU load
- Congestion occurring
- Time consuming process
- Less effective
- Less security

**ATTACK IDENTIFICATION SYSTEM:**

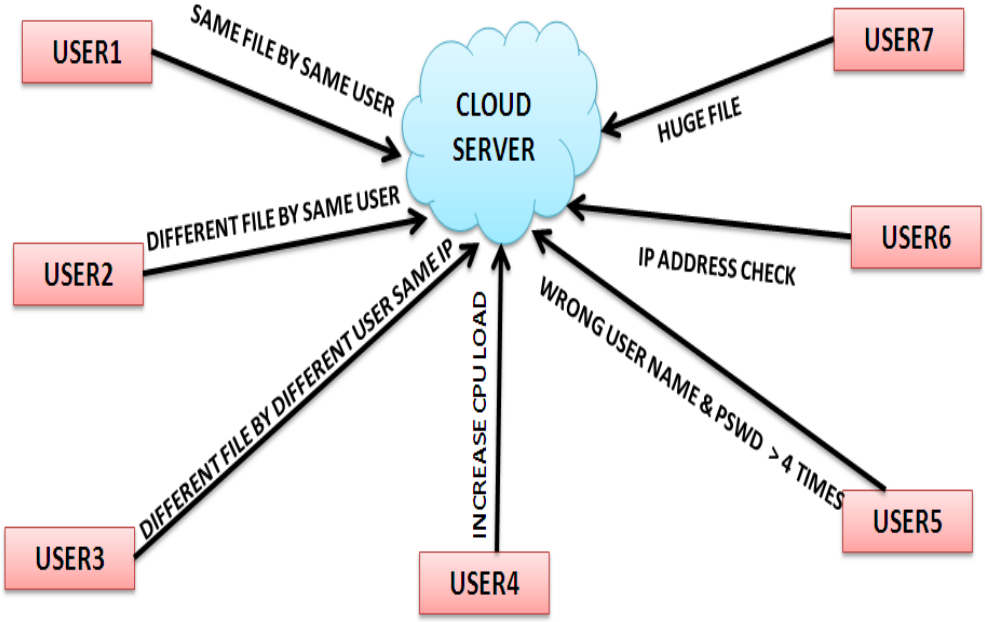
We Deploy User's Request could also increase the CPU Load of the Cloud Server. Filters the Request based on the behavior and forwards to the corresponding Servers through Cloud Server. Every Server would have allocated Certain Space in Cloud Server. Our system monitors the Activity of the Users to Avoid DDOS Attacks.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (96-100), Month: January-April 2016, Available at: www.noveltyjournals.com

**ARCHITECTURE DIAGRAM:**




## 3. AVOIDING PROCESS

Once data owner upload their data along with their keyword data stored in separate server. We implement seven types of attacks. 1. Continuous & same request from single user in a point of time. 2. Different query from the same user within a period of time. 3. Different queries from different users but from same IP. 4. Request of huge sized file beyond the permitted. 5. Wrong user name & password for more than 4 times. 6. IP address of the registered user. 7. CPU utilization of the user's request. Based on these pattern user behavior is monitored DDOS attack is avoided in cloud. Mango lab is also implemented.

**ADVANTAGES:**

- Congestion occurring
- Less Time consuming process
- Less effective
- Provide security
- CPU utilization

## 4. MODULES

1. Cloud Server Deployment
2. Space Allocation
3. User Mustering
4. Deployment of Multiple IPS
5. DDOS from Single User
6. DDOS from Multiple User from same IP
7. Attacks Filtering Model

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (96-100), Month: January-April 2016, Available at: www.noveltyjournals.com

**CLOUD SERVER DEPLOYMENT:**

Cloud Service Provider will contain the large amount of data in their Data Storage. Also the Cloud Service provider will maintain the all the User information to authenticate the User when are login into their account. The User information will be stored in the Database of the Cloud Service Provider. Also the Cloud Server will redirect the User requested job to the Resource Assigning Module to process the User requested Job. The Request of all the Users will process by the Resource Assigning Module. To communicate with the Client and the with the other modules of the Cloud Network, the Cloud Server will establish connection between them. For this Purpose we are going to create an User Interface Frame. Also the Cloud Service Provider will send the User Job request to the Resource Assign Module in Fist In First Out (FIFO) manner.

**SPACE ALLOCATION:**

**Cloud Servers** is a cloud infrastructure service that allows users to deploy "one to hundreds of cloud servers instantly" and create "advanced, high availability architectures" .The "cloud servers are virtual machines running on the hypervisor for Linux-based instances, and Xen Server for Windows and Linux instances. Each quad core hardware node has between 16 and 32 GB of RAM, allowing for allocations between 256 MB and 30 GB. Disk and CPU allocations scale up with memory, with disk sizes ranging from 10 GB to 620 GB. Various distributions of Linux are supported, and each user space allocation with different band width is allocated so they utilizes within the bandwidth

**USER MUSTERING:**

In this module we tell about the user mustering in we can

1. Track Users during an Emergency

2. Ensure nobody is left in danger zone

3. Reduce Paperwork / Human Error during

4. Data collection and reporting.

5. Get workers back into facility in a safe and timely manner.

**DEPLOYMENT OF MULTIPLE IPS:**

In this module we implement multiple IPS ie intrusion protection system that used to protect the user form the attacks .in existing they were using single to scan the query of a cloud user. but in this proposed module we multiple IPS is deployed to monitor the user query so that it easily find the denial of attack .

**DDOS FROM SINGLE USER:**

DDOS is a type of DOS attack where multiple compromised systems -- which are usually infected with virus are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. in a DDoS attack, the incoming traffic flooding the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

**DDOS FROM MULTIPLE USER FROM SAME IP:**

To launch a **DDoS** attack, malicious **users** first build a network of computers that a large **number of** compromised hosts to probe and check the **same** addresses in period of time, the spreading rate reduces because the **number of** the new **IP** .in this multiple will be login in the same ip address and send query so it will see the account and it will lead to overload on the sever. in out proposed we monitor the query coming from multiple user form the same ip .And we analysis ip address to find the DDOS attack

**ATTACKS FILTERING MODEL:**

We present a probabilistic packet **filtering** (PPF) mechanism to defend the Web server against Distributed Denial-of-Service (DDoS) **attacks**. In the attack filtering model we implement the requested huge sized file beyond the permitted. Based on these patterns user behavior is monitored DDOS attack is avoided in cloud.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (96-100), Month: January-April 2016, Available at: www.noveltyjournals.com

## 5. CONCLUSION

In this paper, we propose a strategy to implement stealthy attack patterns, which exhibit a slowly-increasing polymorphic behavior that can evade, or however, greatly delay the techniques proposed in the literature to detect low-rate attacks. Exploiting a vulnerability of the target application, a patient and intelligent attacker can orchestrate sophisticated flows of messages, indistinguishable from legitimate service requests. In particular, the proposed attack pattern, instead of aiming at making the service unavailable, it aims at exploiting the cloud flexibility, forcing the services to scale up and consume more resources than needed, affecting the cloud customer more on financial aspects than on the service availability.

## 6. FUTURE ENHANCEMENT

In the future work, we aim at extending the approach to a larger set of application level vulnerabilities, as well as defining a sophisticated method able to detect SIPDAS based attacks in the cloud computing environment.

## 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] F. Cheng and C. Meinel, "Intrusion Detection in the Cloud," in Proc. IEEE Int. Conf. Dependable, Autonom. Secure Comput., Dec. 2009, pp. 729–734.

[3] 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

[4] 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.

[5] H. Sun, J. C. S. 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.

[6] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-Targeted denial of service attacks: The shrew vs. the mice and elephants," in Proc. Int. Conf. Appl., Technol., Archit., Protocols Comput. Commun., 2003, pp. 75–86.

[7] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of quality (RoQ) attacks on internet end-systems," in Proc. IEEE Int. Conf. Comput. Commun., Mar. 2005, pp. 1362–1372.

[8] 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.

[9] L. Wang, Z. Li, Y. Chen, Z. Fu, and X. Li, "Thwarting zero-day polymorphic worms with network-level length-based signature generation," IEEE/ACM Trans. Netw., vol. 18, no. 1, pp. 53–66, Feb. 2010.