Prevention of DDOS Attack on Data over Cloud

Vishwas Shardul[1], Yadnyik Bachchhav[2], Sayali Mahajan[3], Devyani Rakshe[4], Prof. J. A. Dandge[5]
[1, 2, 3, 4, 5] Department of Information Technology
[1, 2, 3, 4, 5] PVG's College of Engineering, Nasik, Maharashtra

Abstract- *Distributed Denial of Service (DDOS) attacks are critical threat to the organization. Recently, there are an increasing no of DDOS attacks against online services & web applications. Detecting application layer DDOS attack is not an easy task. In this system it is possible to detect DDOS attack and to stop it. The detection scheme based on the information theory based metrics. It has two phases: Behavior Monitoring and detection. In the first phase, the web user browsing behavior (HTTP Request Rate, Page Viewing Time Sequence of the requested object) is captured from the system log during not attack cases. Based on the observation, entropy of request per session and trust score for each and every user is maintained and calculated. In another second phase, the suspicious request are identified based on the variation in request and demand for data and the rate limiter is used to block services to a malicious or fraud user. A Scheduler schedule the session based on a trust score of the user and the system workload. Different security tasks provided in this system to unlock the genuine user.*

Keywords- Access Control, Authentication, Cloud Storage, Cloud Computing, Sophisticated Attack Strategy, Low Rate Attack, Intrusion Detection.

I. INTRODUCTION

In today's High Technology Environment, Organizations are becoming more and more depending on the systems. Peoples are increasingly concerned about the proper use of information, and are worried about the data and its misuse from Sophisticated Attacks. Mostly attackers want to access a valuable data of other peoples. Now days many of the peoples make use of cloud for storing and accessing data for their business needs. So, the attackers target over it and try to access data or make the cloud provider full or un-available for a while. It is vital to be concern about information security because more and more of the value of a business is concentrated in its system. Information is as way on the basis of competitive advantage. The purpose of this system:

1. Provide security on Cloud Storage and Authentication.
2. Block unauthorized user.

II. LITERATURE SURVEY

In the past few years, organizations it has been proved that growing number of incidents involving groups and organisation of attackers trying to harm commercial and institutional web apps by exhausting their services through DDOS attacks.[3] Attacker groups understand that the application which is available has an higher priority for most organizations because availability inuences application cost and therefore lets to deduction in the quality of service can reduce revenue as well as damage the organizations reputation.[5]

DDOS attacks involve in harming the particular target machine with external and other communication requests, such that it can't respond to manage traffic. Such attacks mostly leads to a server overload. DDOS attacks are generated or used purposefully to force the victims machine to reset, or to consume its resources and services such as network bandwidth, computing power, and operating system database structures so we can't longer provide its intended service.[2] To hit a Denial of service attack, the attackers firstly establishes a network of a particular affected computers that are used to generate the high volume of traffic needed to deny services and resource to appropriate users of the victim. Then the attacker installs different attack tools on the hosts computer of the affected network. The hosts or attack tools use by attackers are known as zombies, and they can be used to carry out any attack which belongs or made by an attacker. In addition, the attacker will minimize the network traffic pattern of flash event to make the detection difficult. Most of the previously used techniques cannot discriminate the DDOS attacks from the surge of legitimate accessing. In past few years, the target of Distributed Denial of service attacks has shifted from network to application-server resources and services. Different LORDAS attack models on application server have been proposed.[4] In particular, they aim to provide different service queue of the target application servers completely full of requests coming from the attacker, so that any new occurring request sent by users is discarded. Macia-Fernandez et al present an evolution of the low-rate Distributed Denial of Service attack against iterative application servers, and extends its capabilities to concurrent systems. They assume that the victim server has a finite service queue, where the incoming service requests are temporarily stored to be processed by the depending application process or thread.[2] The attacker takes advantage of the session time at which the responses made to newly incoming requests for a given service occur. This capability is

used to schedule an secure pattern in such a way that the server which is harmed by the attacker becomes busy the large time in processing the malicious requests instead of those from legitimate users.

III. SYSTEM ARCHITECTURE

The figure specified below is typically for detecting attacks.

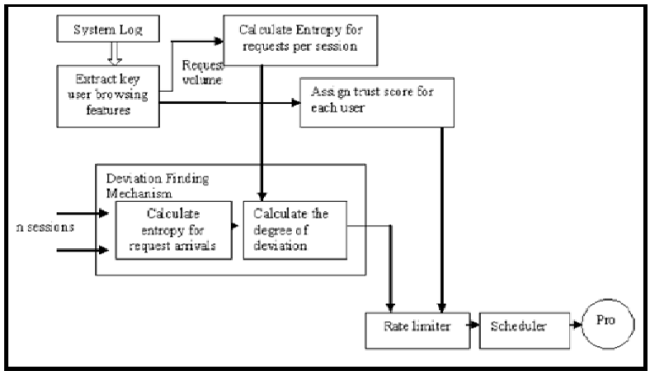

Figure 1: System Architecture

Contents of Architecture

System Log:-

System log is history information stored for reference, which is used to find bugs and errors.

Extract key user browsing features:-

This block reads the system log and selects some of information from them (like login time, number of request hit from a user etc.)

Calculate entropy:-

Calculates entropy for every user for his every logged in session, means it process user information and calculate entropy.

Assign trust score:-

This block calculates trust score for each and every user. Trust score is limited number of user's requests hit per session

Deviation finding mechanism:-

Users requests for particular current session ,will be consider and stored in this block, the request user will come here first and will be counted as well.

Calculate degree of deviation:-

Degree of deviation will be calculated here, means with comparison to trust score, how many number current requests amount is more or less.

Rate limiter:-

This block buffer the excess number of request after some different time.

Scheduler:-

This block schedules the buffered requests, means reads the requests and process them after some time interval or when load is low on server.

IV. CONCLUSION

Thus, we propose a strategy and different techniques to implement stealthy attack patterns, it will slowly detect the attacks by using different threads and assigning trust-score limit for preventing users data which is stored on cloud. In particular, the proposed attack pattern, instead of making the service or resource unavailable, it has to exploiting the cloud flexibility, forcing the services to scale up and consume or use more and more resources than needed, affecting the cloud users more on cost aspects than on the service and resource availability. In the future or propsed work, we aim to minimize vulnerabilities, as well as defining a sophisticated methods and procedure ,which are able to detect or conquer SIPDAS based attacks in the cloud computing environment.

REFERENCES

[1] "F. Cheng and C. Meinel, Intrusion Detection in the Cloud, in Proc. IEEE Int. Conf. Dependable, Autonom. Secure Comput., Dec. 2009, pp. 729734."

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

[3] "K:Lu;D:Wu; J :Fan; S:Todorovic; andA:Nucci ;Robustande_cientdetectionofDDoSattacksforlarge [[44]] " 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. "

[4] "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. 7586. "

[5] " 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. 13621372.." 26Prevention of DDOS Attack on Data over Cloud.