Double-Ended Prevention Mechanism For DDOS Attack In The Application Layer of Cloud Environment

Sreekanth D[1], Gladston Raj S [2]
[1]Dept of Computer Science
[2]Assistant Professor, Dept of Computer Science
[1]Bharathiar University, Coimbatore, India
[2]Govt. College- Nedumangad, Trivandrum, India

Abstract*- The enriched features of cloud computing brought a wide acceptance to the cloud technology among the customers. Cloud computing became famous nowadays because of its great features like pay per use, 99.99% of uptime, reliability, less hardware and software costs etc. Even though based on the demand of service, the environment provides the facility to assure the high availability of services, but nowadays Distributed Denial of Service (DDoS) attack is one of the major problems affected badly to extend such services of cloud computing. In this work, we have deployed a double ended prevention mechanism to prevent DDoS attack in the application layer of cloud environment through the statistical analysis of the system logs generated. The system proposes a model which can prevent the DDoS attack by analyzing the web logs and application logs.*

Keywords- Access Log, Application Log, DDoS, Layer-7, Cloud computing

I. INTRODUCTION

The Denial of Service (DDoS) [1] Attack is one of the major attacks affected to cloud environment nowadays. DDoS attack will lead to the full acquisition of bandwidth. Running multiple jobs for a long time taking processes is also one of the DDoS attacks. The system proposes a double ended security mechanism to prevent Distributed Denial of Service (DDoS) attack. All the existing major models are points to prevent DDoS attack by availing high processing time. The proposed model wouldn’t affect the performance of the system because it will be run through analysing the system and application logs. One of the major attacks in this area is Layer 7[4] attack. The attacks affect to the Application layer is the Layer-7 attack. Most of the time, these automated attacks usually maintain the same pattern. The attacker will find out a heavy URL to the site and will start requesting it frequently. Sometimes they will make the requests more than a dozen time or more than hundreds of time per second [3]. Today we can see hundreds of Application Layer attack’s and there is no scientific mechanism to handle such type of attacks without compromising the cloud performance.

II. ACCESS LOG

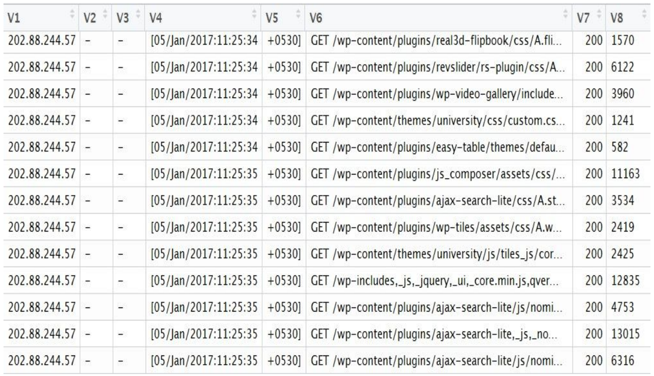
Initially, the system will be running a crawl job in the Access logs of the web server. Access logs will be updated whenever a client accesses the application with relevant details. The log contains all relevant information like accessed IP address [5], date and time, type of request (GET), status codes, and the size of the object returned to the client. In the provided access log,

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
```

- 127.0.0.1: is the IP address
- Hyphen (-): indicates that the requested information is not available
- Frank: Is the user id of the person
- [10/Oct/2000:13:55:36 -0700]: The date, time with the zone of the server when completed the request.
- "GET /apache_pb.gif HTTP/1.0”: Request from the client
- 200: the status of the code
- 2326: The size of the object.

By running a crawl job in the access log, we can easily identify, what type of access have requested by the client and what is the response of the server for the request. The status code in every snippet is highly useful to identify the type of the requests. The code begins with ‘2’ points that the request was handled successfully. Codes begin with ‘3’ says it is a redirection, an error caused by the client will start with ‘4’ and ‘5’ is for the error in the server [5].

Analyzing the access logs will be helpful to create meaningful information out of it. We have used the highly capable analytical tool R for the analysis. We can read the access logs directly into R and can be easily classified. The uploaded data will be available for the process. (Fig. 1 shows an example).



V1	V2	V3	V4	V5	V6	V7	V8
202.88.244.57	-	-	[05/Jan/2017:11:25:34	+0530]	GET /wp-content/plugins/real3d-flipbook/css/A.fli...	200	1570
202.88.244.57	-	-	[05/Jan/2017:11:25:34	+0530]	GET /wp-content/plugins/revslider/rs-plugin/css/A...	200	6122
202.88.244.57	-	-	[05/Jan/2017:11:25:34	+0530]	GET /wp-content/plugins/wp-video-gallery/include...	200	3960
202.88.244.57	-	-	[05/Jan/2017:11:25:34	+0530]	GET /wp-content/themes/university/css/custom.cs...	200	1241
202.88.244.57	-	-	[05/Jan/2017:11:25:34	+0530]	GET /wp-content/plugins/easy-table/themes/defau...	200	582
202.88.244.57	-	-	[05/Jan/2017:11:25:35	+0530]	GET /wp-content/plugins/js_composer/assets/css/...	200	11163
202.88.244.57	-	-	[05/Jan/2017:11:25:35	+0530]	GET /wp-content/plugins/ajax-search-lite/css/A.st...	200	3534
202.88.244.57	-	-	[05/Jan/2017:11:25:35	+0530]	GET /wp-content/plugins/wp-tiles/assets/css/A.w...	200	2419
202.88.244.57	-	-	[05/Jan/2017:11:25:35	+0530]	GET /wp-content/themes/university/js/tiles_js/cor...	200	2425
202.88.244.57	-	-	[05/Jan/2017:11:25:35	+0530]	GET /wp-includes,_js,_jquery,_ui,_core.min.js,qver...	200	12835
202.88.244.57	-	-	[05/Jan/2017:11:25:35	+0530]	GET /wp-content/plugins/ajax-search-lite/js/nomi...	200	4753
202.88.244.57	-	-	[05/Jan/2017:11:25:35	+0530]	GET /wp-content/plugins/ajax-search-lite,_js,_no...	200	13015
202.88.244.57	-	-	[05/Jan/2017:11:25:35	+0530]	GET /wp-content/plugins/ajax-search-lite/js/nomi...	200	6316

Fig. 1. Access Logs

Once the Access logs are available, we can make the analysis of every column. Using the available log data, we can calculate the total number of access counts to the application as shown in the Figure 1 column V8. Generating a report on the analysis hour wise traffic as generated shown Fig.2 will be helpful to track in the case of any anomalies takes place.

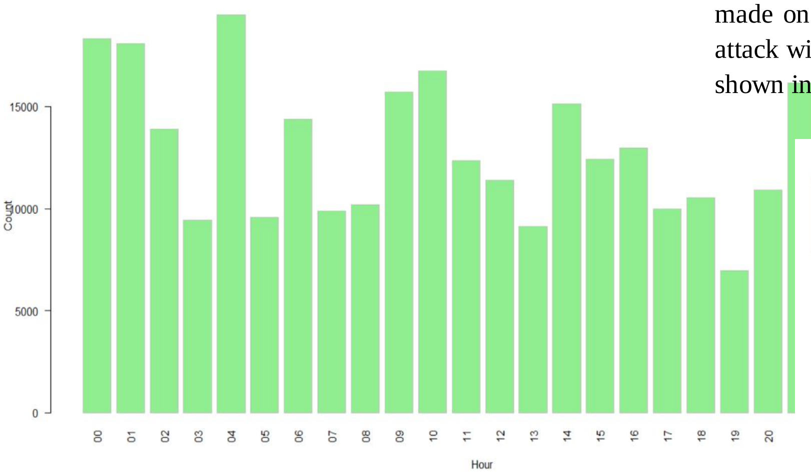
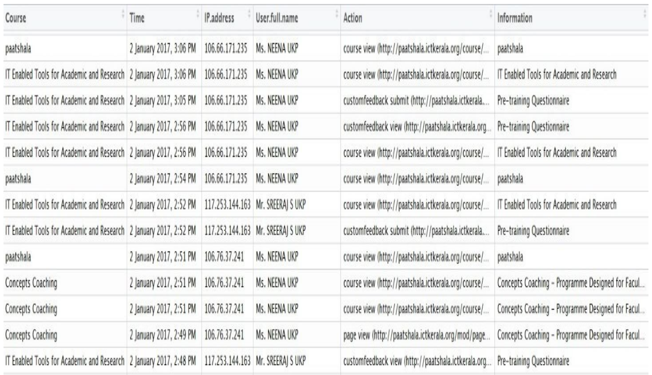


Fig. 2: Hourly Visits to the Application

III. APPLICATION LOGS

Application log is created from a by the application software. It is purely a customized format, depends upon the requirement of the application. Any transactions take place in the application software can be logged. Writing logs for every transaction is a good method to assure the software quality. Here we have used a log file generated by MOODLE, an open source learning management system for the application log analysis [2]. The application log loaded into the system is shown in the below Fig.3



Course	Time	IP.address	User.full.name	Action	Information
paatshala	2 January 2017, 3:06 PM	106.66.171.235	Ms. NEENA UKP	course view (http://paatshala.ictkerala.org/course/...	paatshala
IT Enabled Tools for Academic and Research	2 January 2017, 3:06 PM	106.66.171.235	Ms. NEENA UKP	course view (http://paatshala.ictkerala.org/course/...	IT Enabled Tools for Academic and Research
IT Enabled Tools for Academic and Research	2 January 2017, 3:05 PM	106.66.171.235	Ms. NEENA UKP	customfeedback submit (http://paatshala.ictkerala...	Pre-training Questionnaire
IT Enabled Tools for Academic and Research	2 January 2017, 2:56 PM	106.66.171.235	Ms. NEENA UKP	customfeedback view (http://paatshala.ictkerala.org...	Pre-training Questionnaire
IT Enabled Tools for Academic and Research	2 January 2017, 2:56 PM	106.66.171.235	Ms. NEENA UKP	course view (http://paatshala.ictkerala.org/course/...	IT Enabled Tools for Academic and Research
paatshala	2 January 2017, 2:54 PM	106.66.171.235	Ms. NEENA UKP	course view (http://paatshala.ictkerala.org/course/...	paatshala
IT Enabled Tools for Academic and Research	2 January 2017, 2:52 PM	117.253.144.163	Mr. SREERAJ S UKP	course view (http://paatshala.ictkerala.org/course/...	IT Enabled Tools for Academic and Research
IT Enabled Tools for Academic and Research	2 January 2017, 2:52 PM	117.253.144.163	Mr. SREERAJ S UKP	customfeedback submit (http://paatshala.ictkerala...	Pre-training Questionnaire
paatshala	2 January 2017, 2:51 PM	106.76.37.241	Ms. NEENA UKP	course view (http://paatshala.ictkerala.org/course/...	paatshala
Concepts Coaching	2 January 2017, 2:51 PM	106.76.37.241	Ms. NEENA UKP	course view (http://paatshala.ictkerala.org/course/...	Concepts Coaching - Programme Designed for Facul...
Concepts Coaching	2 January 2017, 2:51 PM	106.76.37.241	Ms. NEENA UKP	course view (http://paatshala.ictkerala.org/course/...	Concepts Coaching - Programme Designed for Facul...
Concepts Coaching	2 January 2017, 2:49 PM	106.76.37.241	Ms. NEENA UKP	page view (http://paatshala.ictkerala.org/mod/page...	Concepts Coaching - Programme Designed for Facul...
IT Enabled Tools for Academic and Research	2 January 2017, 2:48 PM	117.253.144.163	Mr. SREERAJ S UKP	customfeedback view (http://paatshala.ictkerala.org...	Pre-training Questionnaire

Fig. 3: Application Log

Here the application log consists, the course name, Time, IP Address, User's Full Name, Action performed and information. This differs depends upon applications, even though the IP Address is an essential component in every log.

IV. DOUBLE ENDED PREVENTION TECHNIQUE

The work proposes a double ended prevention mechanism to prevent the DDoS attack in the cloud environment without compromising its major advantages like availability and scalability. The prevention technique will be applied based on analysis, classification, and comparison made on Web Logs and Application Logs. Here the Layer-7 attack will be prevented through the following process flow as shown in the Fig.4

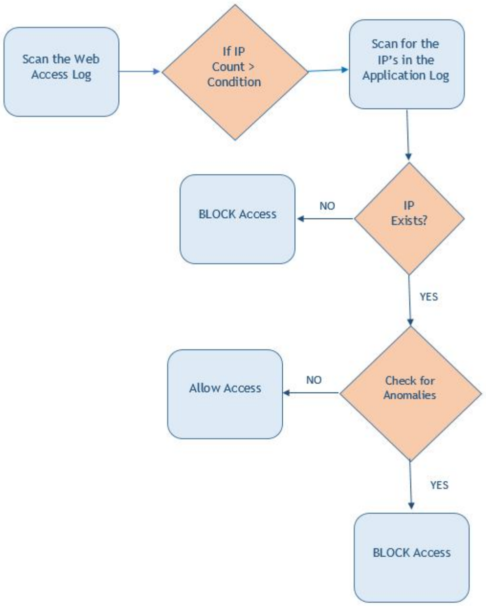


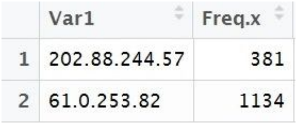
Fig. 4: Process Flow

- Run the crawl job in the Web Access Log
- Identify the IP address with maximum counts

- Perform the Search in the Application Log for the IP Address identified with maximum count in Web Log
- Check the action/status of the IP address in the Application Log.
- Block the IP, if it is:
  - o Not present in the Application Log
  - o Not performing any of the actions with the Application
  - o Connected only with a single process
  - o Accessed from a single username.

V. RESULTS AND DISCUSSIONS

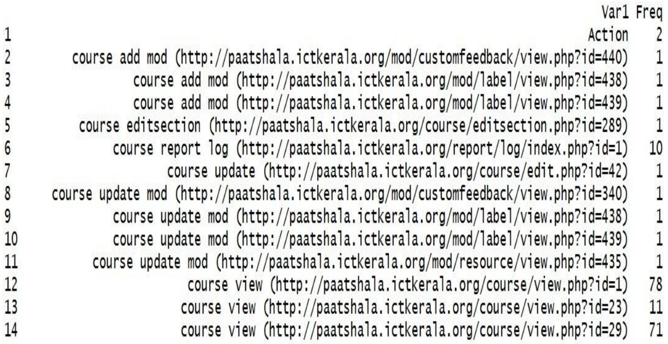
After performing the search in the application log for the highly-occupied IP's over the condition set, the output can be generated as shown in the Fig.5



	Var1	Freq.x
1	202.88.244.57	381
2	61.0.253.82	1134

Fig 5: Merged Log with Frequency

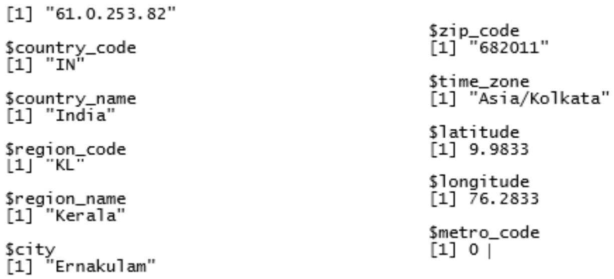
The system will scan for the respective actions performed in the application log and we will get the output as in the Fig. 6



```
                                                                                Var1 Freq
1                                                                             Action    2
2       course add mod (http://paatshala.ictkerala.org/mod/customfeedback/view.php?id=440)    1
3                course add mod (http://paatshala.ictkerala.org/mod/label/view.php?id=438)    1
4                course add mod (http://paatshala.ictkerala.org/mod/label/view.php?id=439)    1
5         course editsection (http://paatshala.ictkerala.org/course/editsection.php?id=289)    1
6             course report log (http://paatshala.ictkerala.org/report/log/index.php?id=1)   10
7                    course update (http://paatshala.ictkerala.org/course/edit.php?id=42)    1
8    course update mod (http://paatshala.ictkerala.org/mod/customfeedback/view.php?id=340)    1
9             course update mod (http://paatshala.ictkerala.org/mod/label/view.php?id=438)    1
10            course update mod (http://paatshala.ictkerala.org/mod/label/view.php?id=439)    1
11         course update mod (http://paatshala.ictkerala.org/mod/resource/view.php?id=435)    1
12                        course view (http://paatshala.ictkerala.org/course/view.php?id=1)   78
13                       course view (http://paatshala.ictkerala.org/course/view.php?id=23)   11
14                       course view (http://paatshala.ictkerala.org/course/view.php?id=29)   71
```

Fig 6: Action Log

By analyzing the action log, we can easily identify that the server request is genuine or not. Another advantage for the applications running in the private cloud is, can easily restrict the access to the application by analyzing the geographical location of the IP. The geographical location and other relevant credentials can be pulled using IP as shown in the Fig. 7.



```
[1] "61.0.253.82"
                                        $zip_code
$country_code                           [1] "682011"
[1] "IN"
                                        $time_zone
$country_name                           [1] "Asia/Kolkata"
[1] "India"
                                        $latitude
$region_code                            [1] 9.9833
[1] "KL"
                                        $longitude
$region_name                            [1] 76.2833
[1] "Kerala"
                                        $metro_code
$city                                   [1] 0 |
[1] "Ernakulam"
```

Fig 7: Geographical Location Details

The log data we have used for the process is from an Apache Webserver. A MOODLE application is running here and the application log for the analysis have also taken from here. We have used R as the analytical tool to analyze the data, because of the high capacity of the tool to process the huge amount of data we can easily prevent the DDoS attack.

VI. CONCLUSION

The work provides a mechanism to prevent the DDoS attack in the cloud environment without affecting the performance of the application running on the cloud server. The system is capable to analyse the huge amount of data generated as system logs and application logs using the statistical analysis. The analysis performed without affecting the performance of the cloud facilities will be able to identify the threat before establishing the full-fledged attack. The system will block any of the unauthorized access to the application in a scientific manner.

REFERENCES

[1] Rashmi V. Deshmukh, Kailas K. Devadkar.: Understanding DDoS Attack & Its Effect In Cloud Environment, 1877-0509, Elsevier B.V. (2015)

[2] Anteneh Girma, Moses Garuba, Jiang Li, Chunmei Liu.: A Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment,978-1-4799-8828-0, IEEE (2015)

[3] David Holmes.: DDoS ATTACK TRENDS-2016, F5 Networks, Inc. (2016)

[4] Amazon Web Services, AWS Best Practices for DDoS Resiliency, https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf

[5] Apache, HTTP Server Project https://httpd.apache.org/docs/1.3/logs.html

[6] Jonathan Trostle ASK Consulting and Research, Inc., Protecting Against Distributed Denial of Service (DDoS)

Attacks Using Distributed Filtering, 1-4244-0423-1/106/©2006 IEEE

[7] Aman Bakshi, Yogesh B ,Securing cloud from DDOS Attacks using Intrusion Detection System in Virtual Machine, -2010 Second International Conference on Communication Software and Networks, 978-0-7695-3961-4/10© 2010 IEEE.

[8] Mr. Vince Paul, Dr. K . Prasadh, Mr. Sankaranarayanan, APPLICATION - DDOS ATTACKS RESISTANCE SCHEME USING POLYNOMIAL DISTRIBUTION MODEL, 2013 Third International Conference on Advances in Computing and Communications, 978-0-7695-5033-6/13 © 2013 IEEE

[9] Anteneh Girma, Moses Garuba, Jiang Li, Chunmei Liu - A Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment, 2015 12th International Conference on Information Technology - New Generations, 978-1-4799-8828-0/15 © 2015 IEEE

[10] Qiao Yan, F. Richard Yu, Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges, IEEE, Qingxiang Gong, and Jianqiang Li, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 1, FIRST QUARTER

[11] Mohammed Khudhur Hussein, Ir.Dr. Nasharuddin Bin Zainal,Aws Naser Jaber, Data Security Analysis for DDoS Defense of Cloud Based Networks, 2015 IEEE Student Conference on Research and Development (SCOReD), 978-1-4673-9572-4/15/©2015 IEEE