Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# An Efficient Threshold Vector Based Model for Detecting DDOS in Cloud Environment

**Dhanya D C**
M.tech CSE,
Nitte Meenakshi Institute of Technology,
Bangalore, India

**Afroz Pasha**
Asst. Prof. Dept of CSE (UG),
Nitte Meenakshi Institute of Technology
Bangalore, India

***Abstract: Cloud computing is been the interesting topic in recent time. It provides and offers various services to end user or clients. Cloud provides a storage services which is stored in it data center but user always feel insecure of their virtualized storage data. So security is always an issue specially security risk like including Distributed Denial of Service (DDOS) attack.Many cloud providers like amazon, drop box provide service based on http protocol.So here we propose efficient DDOS mitigation system for cloud environment. Here we design an algorithm which is based on threshold vector to detect DDOS for cloud. We tested our approach on different http data set and found that our system improves the detection accuracy of DDOS in Cloud. We also provide a security for DDOS by designing an image text fusion turing which improves the security of our system. We designed and implemented our system and also evaluated the performance which shows that our system works efficiently to mitigate the DDOS traffic from the Internet.***

***Keyword: - DDOS, CAPTCHA, Turing Test, cloud computing, Text-image fusion.***

## I. INTRODUCTION

Cloud computing is becoming the term that describes the delivery of any and all information technology. u computing basically refers to large number of computers that are connected through a real-time communication network such as the Internet. Cloud computing is an emerging style of computing where applications, data and resources are provided to users as a service over the web. By using cloud dynamically scalable resources such as CPU, storage, or bandwidth are provided as a service over the internet. Cloud services today provides user-friendly manner and it offers an wide variety of services. Nowadays adoption of cloud is being increasing as it is massive, web-scale abstracted infrastructure.

### *A. Service models*

The several fundamental models of cloud computing provides the variety of services like Infrastructure as a service (IaaS), platform as a service (PaaS),and software as a service (SaaS). IaaS is treated as most basic model. Other services are like XaaS, Desktop as a service (Daas),Strategy-as-a-Service, Collaboration-as-a-Service, Business Process-as-a-Service, Database-as-a-Service, etc.

### *B. Infrastructure as a Service (IaaS):*

Iaas makes available of hardware or virtual computers where the organization can control over the OS, thereby it can allow execution of software. IaaSoffers additional resources such as a virtual-machine disk image library, file-based storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and many software bundles. IaaS-cloud can supply these resources on-demand from pools of data centers. Examples of IaaS are Amazon web service, Google compute engine.

### *C. Platform as a Service (PaaS):*

The PaaSmodel, makes available of hardware and OS, framework and database, for these developers write the custom applications. Application developers can develop and run their software on a cloud platform in a cost effective manner by managing the underlying hardware and software layers. With somePaaS offers, on demand service to match application demands. Examples of PaaS are Google App Engine, Microsoft Azure Services.

### *D. Software as a Service (SaaS):*

SaaSmodel makes available of hardware, OS, and special purpose software made available through internet. SaaSusers are provided with access to application software and databases.SaaS is sometimes referred to as "on-demand software" and it is based on pay-per-use policy. Examples of SaaS are Google Gmail, Microsoft 365.

### *E. DDOS*

A distributed denial-of-service (DDOS) attack is one which makes the resources unavailable for the deliberate user. In cloud the resources are concentrated at a single place and it will be easy for the attackers to attack and capture the

information. So it is very essential to provide the security for the cloud. There are two types of DDOS attack : newtwork-centric attack, deals with bandwidth by overloading of services and application-layer attackwhere services are being overloaded with application calls. Other types of DDOS attacks are UDP flood, SYN flood, permanent DDOS attack etc. DDOS attack can be carried out in number of ways by Consumption of computational resources, such as bandwidth, memory, disk space, or processortime. Disturbing of configuration information, such as routing information. Confusion in state information, such as unsolicited resetting of TCP sessions. Disordering of physical network components. Preventing the communication media between the intended users and the victim so that they can no longer communicate adequate.

### *F. Turing Testing*

The Turing test is a test of a machine's ability to exhibit whether it is capable of thinking or acting like a human. The Turing Testing model will be able to detect the packets that are being malicious and hence by this Turing Testingmethod the possible DDOS attack can be identified.

### *G. CAPTCHA*

A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a challenge response system test where it is designed such that the machine generates a random text and the user should able to reproduce it properly so that it can be treated as a valid one. CAPTCHA can be of text and image based. The differentiation between human and bot can be done by using CAPTCHA by setting some task which can be easily performed by most of the humans and it will be little more difficult and time consuming for bots to complete. Many automated programs and bots can be stopped by CAPTCHA.

## II. LITTERATURE SURVEY

| Author | Title of the paper | Concept | Year of publication | Conference/Journal Name |
|---|---|---|---|---|
| A. Pinar Saygin, I. Cicekli, and V. Akman | The turing test : 50 years past | This paper is review of the past 50 years of the Turing Test review is done in this paper Here turing test ideas are been presented and implemented | 2000 | Minds and Machines. |
| L. V. Ahn M. Blum, N. J. Hopper, and J. Langford | Using Hard AI Problems For Security | Here they introduce captcha, an automated test which can be passed by humans, but computer programs can't pass | 2003 | 22nd international conference on Theory and applications of cryptographic techniques |
| J. B. Gizzard V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon | Peer-to-peer botnets: overview and case study | Peer botnets communicates with many different peers. Here different peer-peer botnets are mentioned and text based security of captcha is analysed Peer-to-peer botnets have the same basic goals of centralized C&C botnets. | 2007 | First Workshop on Hot Topics in Understanding Botnets, and HotBots. |

## III. PROPOSED SYSTEM

Here we propose an efficient algorithm which can detect DDOS attack on cloud environment. We design an algorithm which is capable of detecting HTTP based DDOS attack on cloud. We developed kernel vector model which is based on threshold computing. Here first we load the HTTP based dataset which consist of 41 attributes for training. Then we divide these attribute by generating rule and based on these rule we start training our algorithm. We then load the dataset again for testing our algorithm and we have found that our algorithm gives better result. We also test our algorithm by capturing data live data and tested our algorithm. The following diagrams shows how the DDOS packets are been identified through fig1, fig2, fig3.

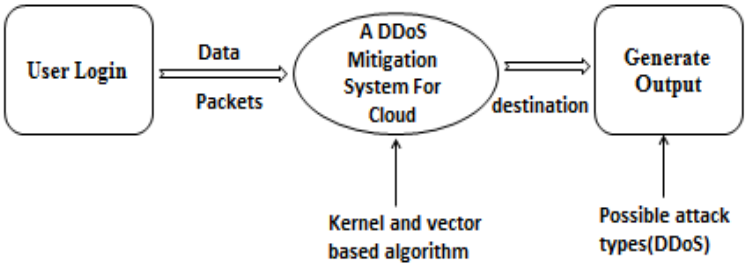



Figure 1: Login using authenticated user

In Fig 1 system the whole system is presented as a flow of data. Here the Sever gets started first and then logs in the user after authentication, detects the intrusion and generates the output.

Here in figure 2 user uploads the committee database and then adds fields to the process in order to mine the dataset. Then it classifies the filters and classification is performed by the server and all the specified classifiers are then displayed.

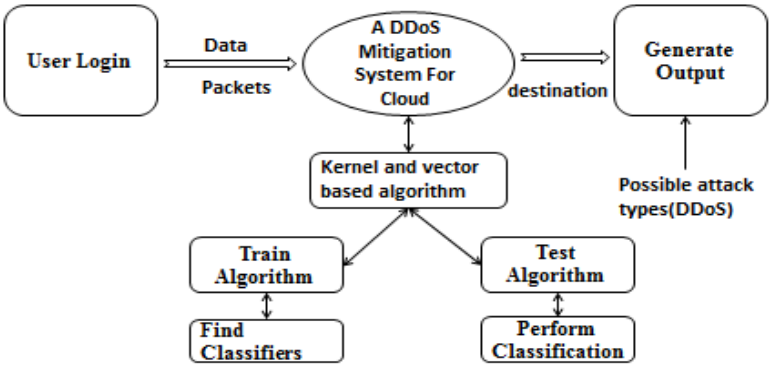



Figure 2: Training and testing of dataset

Here in figure 3 user send the classified data to the testing phase for detecting attack using Kernel and vector based algorithm and generate graph for analysis.

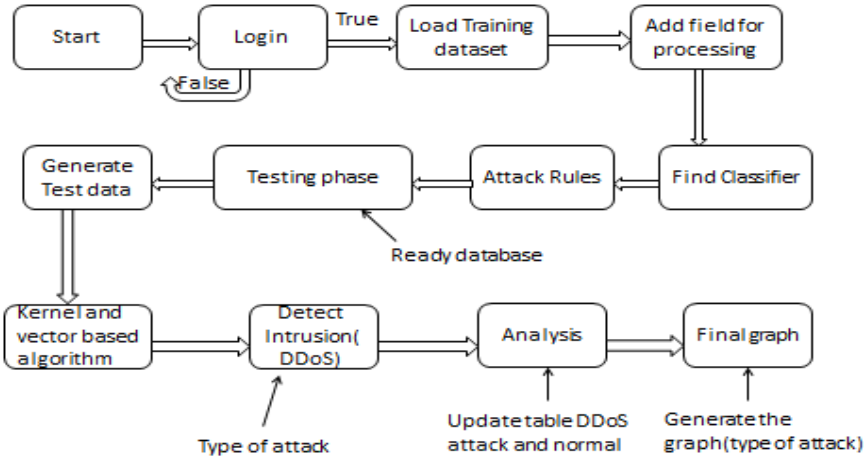
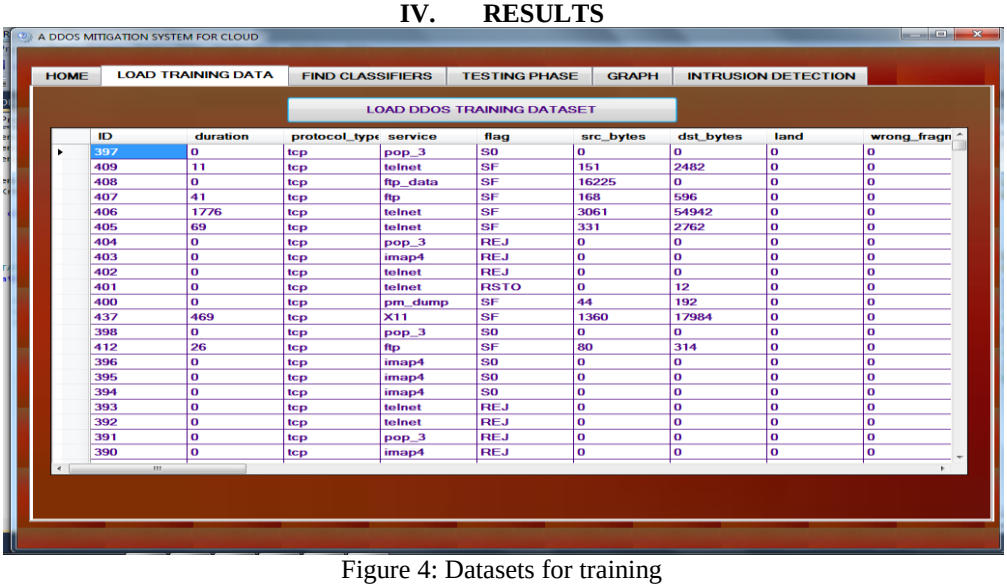



Figure 3: DDOS detecting phase

### *A. Text and image -Based fusion Module*

It is nothing but the Testing phase. The main task of this module is to randomly select an image and question from the Database and send the text and image -based question to the requester. It then checks the following answer from the requester is correct or not. The user will not be able to reach its original destination until it gives the right answer corresponding to image to the following questionit is challenged.

## IV. RESULTS




| ID | duration | protocol_type | service | flag | src_bytes | dst_bytes | land | wrong_fragn |
|---|---|---|---|---|---|---|---|---|
| 397 | 0 | tcp | pop_3 | S0 | 0 | 0 | 0 | 0 |
| 409 | 11 | tcp | telnet | SF | 151 | 2482 | 0 | 0 |
| 408 | 0 | tcp | ftp_data | SF | 16225 | 0 | 0 | 0 |
| 407 | 41 | tcp | ftp | SF | 168 | 596 | 0 | 0 |
| 406 | 1776 | tcp | telnet | SF | 3061 | 54942 | 0 | 0 |
| 405 | 69 | tcp | telnet | SF | 331 | 2762 | 0 | 0 |
| 404 | 0 | tcp | pop_3 | REJ | 0 | 0 | 0 | 0 |
| 403 | 0 | tcp | imap4 | REJ | 0 | 0 | 0 | 0 |
| 402 | 0 | tcp | telnet | REJ | 0 | 0 | 0 | 0 |
| 401 | 0 | tcp | telnet | RSTO | 0 | 12 | 0 | 0 |
| 400 | 0 | tcp | pm_dump | SF | 44 | 192 | 0 | 0 |
| 437 | 469 | tcp | X11 | SF | 1360 | 17984 | 0 | 0 |
| 398 | 0 | tcp | pop_3 | S0 | 0 | 0 | 0 | 0 |
| 412 | 26 | tcp | ftp | SF | 80 | 314 | 0 | 0 |
| 396 | 0 | tcp | imap4 | S0 | 0 | 0 | 0 | 0 |
| 395 | 0 | tcp | imap4 | S0 | 0 | 0 | 0 | 0 |
| 394 | 0 | tcp | imap4 | S0 | 0 | 0 | 0 | 0 |
| 393 | 0 | tcp | telnet | REJ | 0 | 0 | 0 | 0 |
| 392 | 0 | tcp | telnet | REJ | 0 | 0 | 0 | 0 |
| 391 | 0 | tcp | pop_3 | REJ | 0 | 0 | 0 | 0 |
| 390 | 0 | tcp | imap4 | REJ | 0 | 0 | 0 | 0 |

Figure 4: Datasets for training

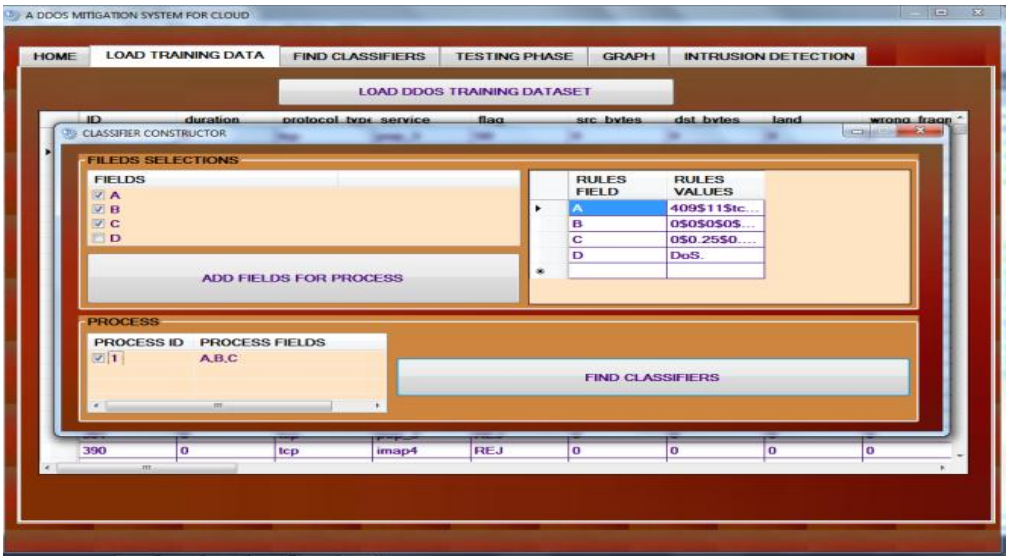



Figure5: Finding classifiers for datasets


Figure 6: Classifiers for selected datasets

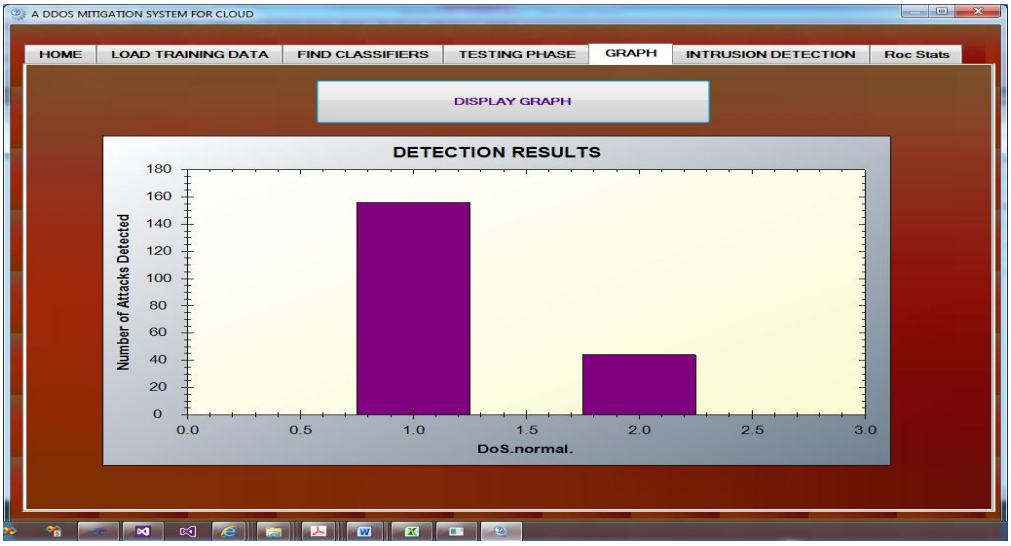



Figure 7: Detection Result for 200 packets

## V. CONCLUSION

Here we discussed about how DDOS attack affects the cloud performance. Many scheme is been proposed to solve the security issue but still it lacks the ability to detect and remove completely. Here we analyzed various existing model and identified it drawback and proposed a new algorithm which can detect DDOS attack efficiently. We proposed

a threshold vector based model which detect DDOS attack efficiently and improve the detection accuracy of our cloud DDOS detection model. We also provide security by using image and text fusion turing which not only reduces bandwidth overhead but also improves the security of the cloud model. The experimental analysis shows that our proposed model performs better interm of detecting DDOS in cloud environment. In future we would test our model with some real time cloud environment.

**REFERENCES**

[1] G. Goth, "Fast-moving zombies: Botnets stay a step ahead of the fixes," IEEE Internet Computing, vol. 11, pp. 7–9, 2007.

[2] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon, "Peer-to-peer botnets: overview and case study," in Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, ser. HotBots'07. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–1.

[3] P. Salvador, A. Nogueira, U. Franca, and R. Valadas, "Framework for zombie detection using neural networks," in Internet Monitoring and Protection, 2009. ICIMP'09.Fourth International Conference on, May 2009, pp. 14 – 20.

[4] F. Giroire, J. Chandrashekar, N. Taft, E. Schooler, and D. Papagiannaki, "Exploiting temporal persistence to detect covert botnet channels," in Recent Advances in Intrusion Detection, ser. Lecture Notes in Computer Science. Springer Berlin /Heidelberg, 2009, vol. 5758, pp. 326–345.

[5] W. Chun-dong, L. Ting, and W. Huai-bin, "Botnet detection based on analysis of mail flow," in Biomedical Engineering and Informatics, 2009. BMEI '09.2nd International Conference on, Oct. 2009, pp. 1 –4.

[6] A. Pinar Saygin, I. Cicekli, and V. Akman, "Turing test: 50 years later," Minds and Machines, vol. 10, pp. 463–518, 2000.

[7] A. P. Saygin and I. Cicekli, "Pragmatics in human-computer conversations," Journal of Pragmatics, vol. 34, no. 3, pp. 227 – 258, 2002.

[8] L. V. Ahn, M. Blum, N. J. Hopper, and J. Langford, "Captcha: problems for security," in Proceedings of the 22nd international conference on Theory and applications of cryptographic techniques, ser. EUROCRYPT'03. Berlin, Heidelberg: Springer-Verlag, 2003, pp. 294–311.

[9] J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft captcha," in Proceedings of the 15th ACM conference on Computer and communications security, ser. CCS '08. New York, NY, USA: ACM, 2008, pp. 543–554.

[10] R. Datta, J. Li, and J. Z. Wang, "Imagination: a robust image based captcha generation system," in Proceedings of the 13th annual ACM international conference on Multimedia, ser.MULTIMEDIA '05. New York, NY, USA: ACM, 2005, pp. 331–334.

[11] A. Gupta, A. Jain, A. Raj, and A. Jain, "Sequenced tagged captcha: Generation and its analysis," in Advance Computing Conference, 2009. IACC 2009. IEEE International, march 2009, pp. 1286 –1291.

[12] R. Thomas, B. Mark, T. Johnson, and J. Croall, "Netbouncer: client-legitimacy-based high-performance ddos filtering," in DARPA Information Survivability Conference and Exposition, 2003. Proceedings, vol. 1, April 2003, pp. 14 – 25 vol.1.

[13] "The World's First "All-in-One" Cloud Computing System," http://www.itri.org.tw/eng/econtent/about/about0902.aspx?sid=5&PageID=1, 2011, [Online; accessed 05-Dec-2011].

[14] J. Yan and A. S. El Ahmad, "Usability of captchas or usability issues in captcha design," in Proceedings of the 4th symposium on Usable privacy and security, ser. SOUPS '08.New York, NY, USA: ACM, 2008, pp. 44–52.

15] L. von Ahn, M. Blum, and J. Langford, "Telling humans and computers apart automatically," Commun. ACM, vol. 47, no. 2, pp. 56–60, Feb. 2004.

[16] M. Chew and J. Tygar, "Image recognition captchas," in Information Security. Springer Berlin / Heidelberg, 2004, vol. 3225, pp. 268–279.

[17] Y. Rui and Z. Liu, "Artificial: Automated reverse Turing test using facial features," Multimedia Systems, vol. 9, pp. 493–502, 2004.

[18] M. Shirali-Shahreza and S. Shirali-Shahreza, "Question-based captcha," in Conference on Computational Intelligence and Multimedia Applications, 2007.International Conference on, vol. 4, Dec. 2007, pp. 54 –58.

[19] S . Kandula, D. Katabi, M. Jacob, and A. Berger, "Botz- 4-sale: surviving organized ddos attacks that mimic flash crowds," in Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation - Volume 2, ser. NSDI'05. Berkeley, CA, USA: USENIX Association, 2005, pp. 287–300.

[20] R. Buyya, R. Ranjan, and R. Calheiros, "Intercloud: Utilityoriented federation of cloud computing environments for scaling of application services," in Algorithms and Architectures for Parallel Processing, ser. Lecture Notes in Computer Science, C.-H. Hsu, L. Yang, J. Park, and S.-S. Yeo, Eds. Springer Berlin / Heidelberg, 2010, vol. 6081, pp. 13–31.