iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** IX **Month of publication:** September 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue IX, September 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Approaches in DOS Attacks

MR Seshan Ram[1]
[1]Assistant professor, Dept. of Computer science, Shri Krishnaa College of engineering, Pondicherry-605501

Abstract*— Application DoS attack,has emerged as a larger threat to network services, compared to the classic DoS attack. To identify application DoS attack, we propose a novel group testing (GT)-based approach deployed on back-end servers. These approaches not only obtain short detection delay and low false positive/negative rate, but also defend against general network attacks. Here we first extend classic GT model with size constraints, then redistribute the client service requests to multiple virtual servers. Here we propose a detection mechanism using some dynamic thresholds to efficiently identify the attackers.

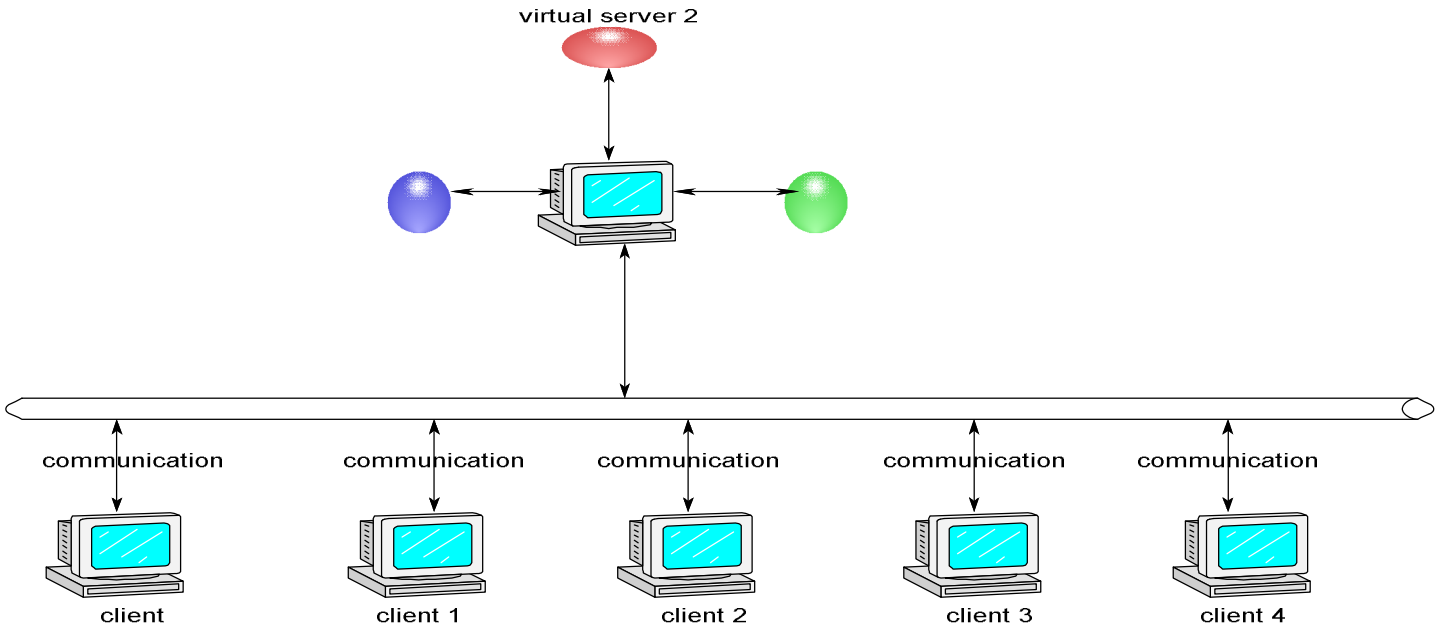
Keywords—*DOS, GT, CAPTCHA, SERVER, IP*

I. INTRODUCTION

DENIAL-OF-SERVICE (DoS) attack, which aims to make a service unavailable to legitimate clients, has become a severe threat to the Internet security. Traditional DoS attacks mainly abuse the network bandwidth around the Internet subsystems and degrade the quality of service by generating congestions at the network .Consequently, several network-based defense methods have tried to detect these attacks by controlling traffic volume or differentiating traffic patterns at the intermediate routers . However, with the boost in network bandwidth and application service types, recently, the target of DoS attacks has shifted from network to server resources and application procedures themselves, forming a new application DoS attack . The DENIAL-OF-SERVICE(DoS) attack, has become a severe threat to the network security. Traditional DoS attacks mainly abuse the network bandwidth and degrade the QOS by generating congestions at the network.With the boost in network bandwidth,recently the target of DoS attacks has shifted from network to server resources and application procedures. Application DoS attack , which aims at disrupting application service rather than depleting the network resource,has emerged as a larger threat to network services.This new assault type cannot be effficientiy detected or prevented by existing detection solutions.

II. DESCRIPTION

We propose a novel group testing (GT)-based approach deployed on back-end servers. Here we first extend classic GT model with size constraints,then redistribute the client service requests to multiple virtual servers.Based on this framework, we propose a two-mode detection mechanism using some dynamic thresholds to efficiently identify the attackers. DDoS shield and CAPTCHA-based defense are the representatives of the two major techniques of system-based approaches.DDoS shield can provide efficient session schedulers for defending possible DDoS attacks. CAPTCHA-defence introduce additional service delays for legitimate clients.



Volume 4 Issue IX, September 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

III.RESOURCES

First node get registered to network topology, by specifying the node IP address, Port Number and status.Only after user authentication by the server system it allows the node into the transmission Node can send the packets to the destination or otherwise it can send to server system. Node can add or relive to and from the network easily and the status is monitored by the sever system.

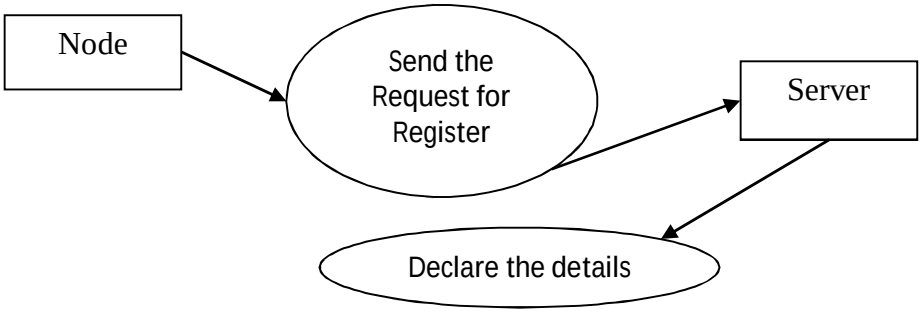


Fig1: Node Details Declaration

A. Server Creation

1) In this module first the centralized server system will be designed for whole network.
2) It has one centralized database and collect the details of each node. And store it into the centralized database.
3) Server maintains these details, which is very useful for node calculation and node details identification.
4) Server can receive the request from all clients and the provide the corresponding response

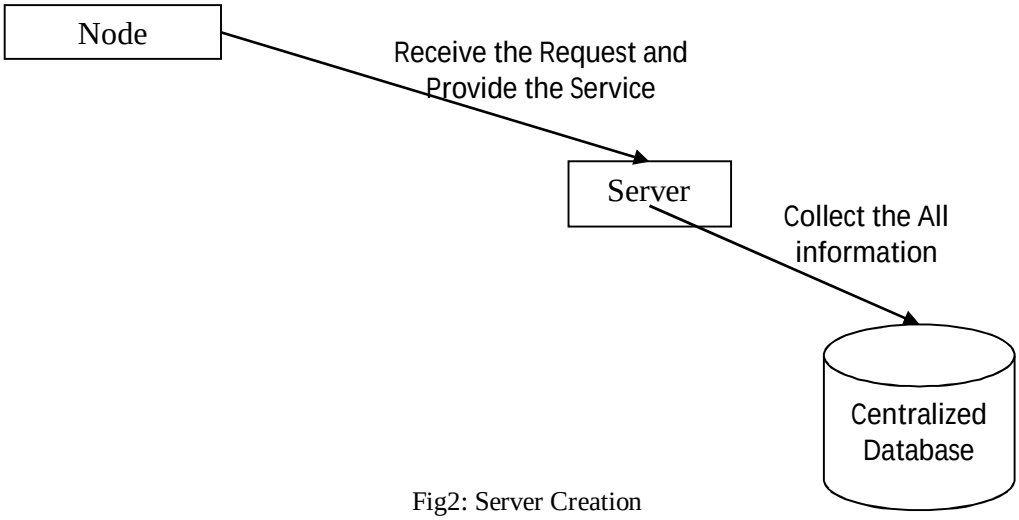


Fig2: Server Creation

B. Server Monitoring

1) In this module if we have any problem in the network topology, server will take the necessary action.
2) The action is to not only discard the particular packet, but also server will collect the details about that particular node from the database and remove it from the network.
3) Server system can identify the attacker node by using the **captcha** mechanism.
4) This process also detect the attacker node in the whole network. And the monitoring result is stored at the server side.

Volume 4 Issue IX, September 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

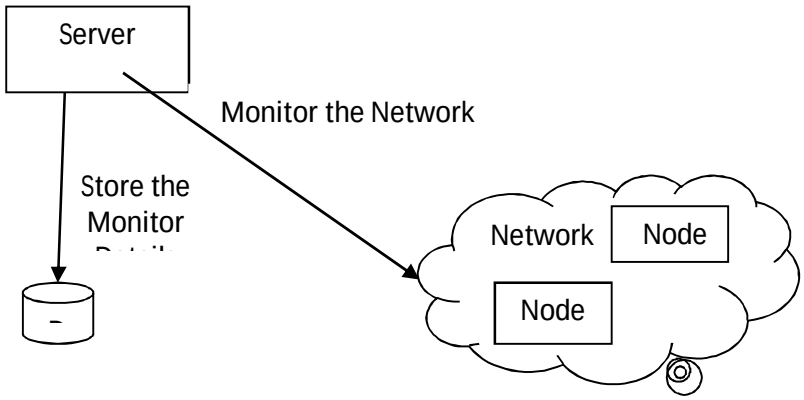


Fig3: Server Monitoring

C. Captcha Generation

1) In Captcha generation, each request is notified by server using this unique captcha. This captcha is unique for all system.
2) Captcha has two parts one is node id and another one is process id.
3) Each node id has node name and port number combination. And each Process id started from the process name and combine with process count.
4) Both are used to identify the node and type of process from DOS attacking node.

OUTPUT

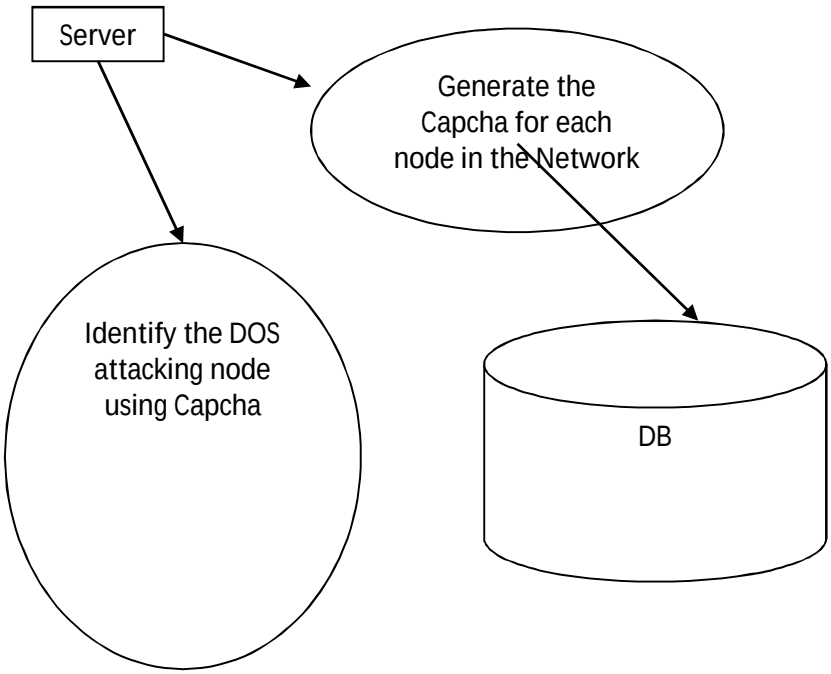
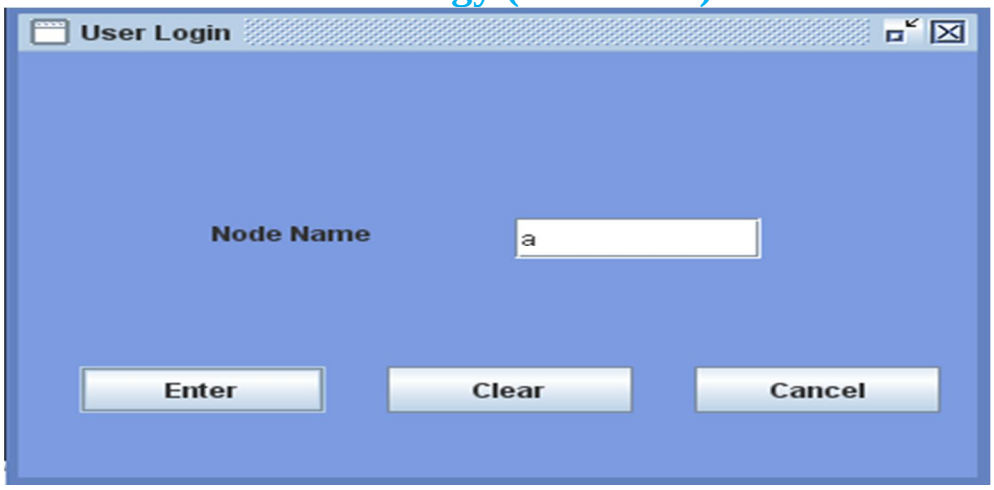
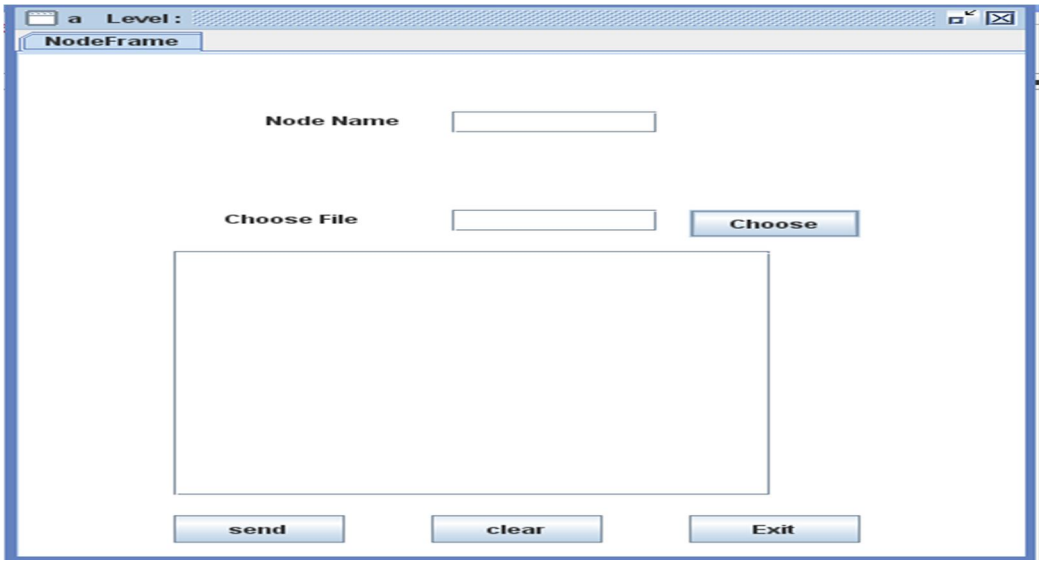


Fig4: Captcha Generation

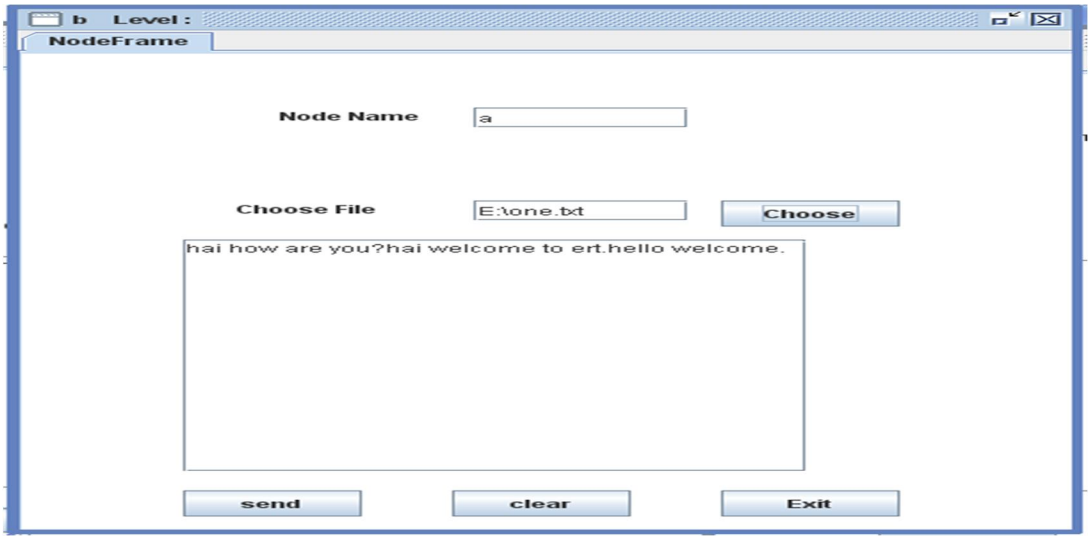
Volume 4 Issue IX, September 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



NODE FRAME

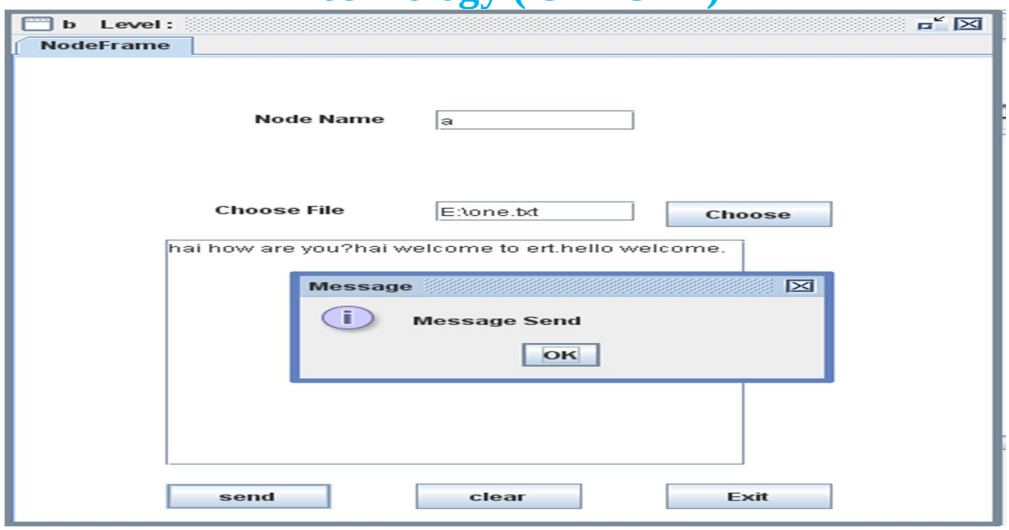


NODE FRAME-SHOWING MESSAGE SEND

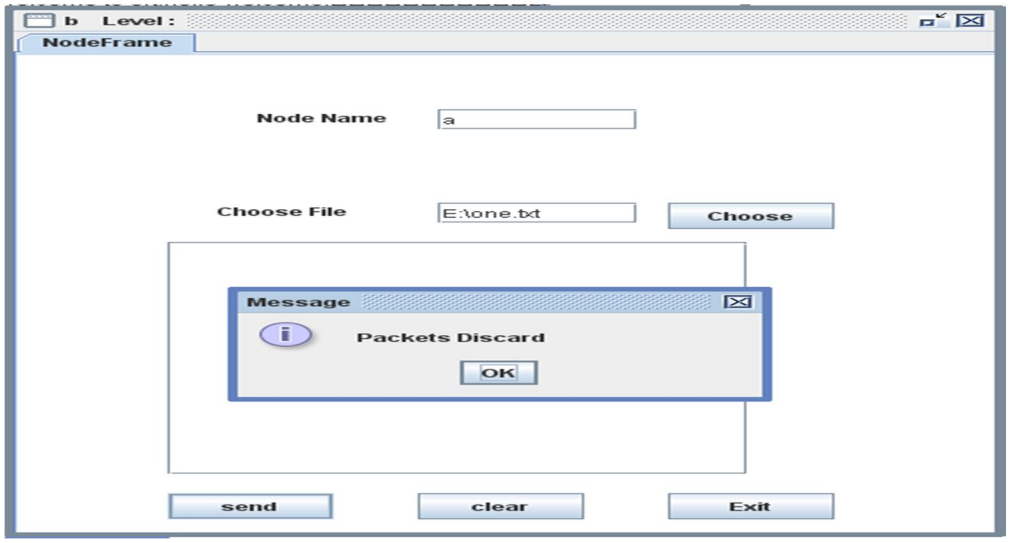


NODE FRAME AND RECEIVER FRAME

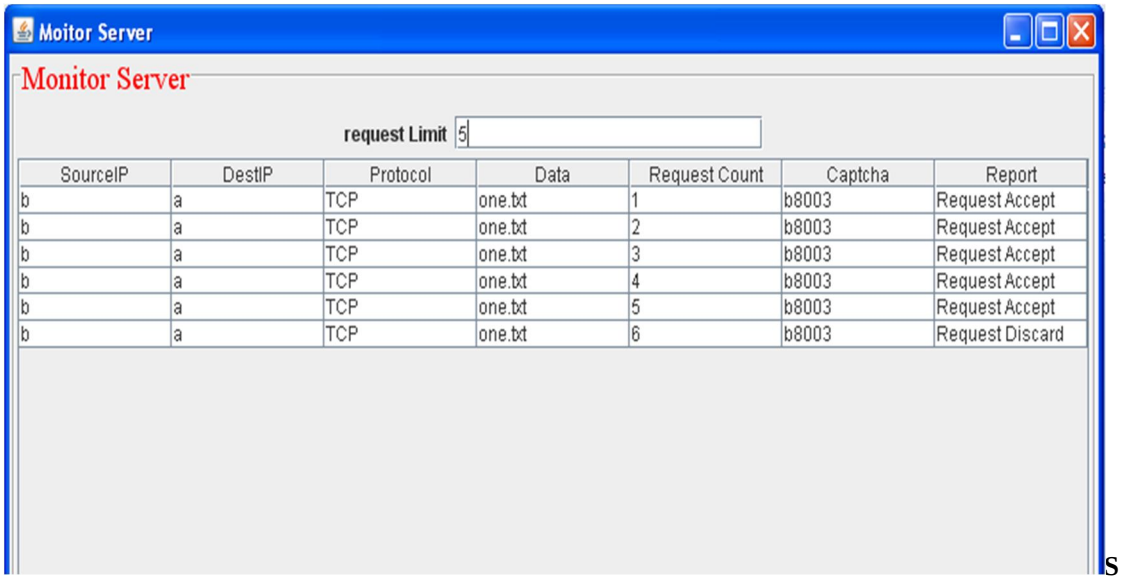
Volume 4 Issue IX, September 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



NODE FRAME - SHOWING PACKETS DISCARDED



MONITOR SERVER-FINAL STATUS



SourceIP	DestIP	Protocol	Data	Request Count	Captcha	Report
b	a	TCP	one.txt	1	b8003	Request Accept
b	a	TCP	one.txt	2	b8003	Request Accept
b	a	TCP	one.txt	3	b8003	Request Accept
b	a	TCP	one.txt	4	b8003	Request Accept
b	a	TCP	one.txt	5	b8003	Request Accept
b	a	TCP	one.txt	6	b8003	Request Discard

S

IV. CONCLUSION

This proposed a novel technique for detecting application DoS attack by means of a new constraint-based group testing model. Theoretical analysis and preliminary simulation results demonstrated the outstanding performance of this system in terms of low detection latency and false positive/negative rate. The focus of this paper is to apply group testing principles to application DoS attacks, and provide an underlying framework for the detection against a general case of network assaults, where malicious requests are indistinguishable from normal ones.

REFERENCES

[1] Ying Xuan, Incheol Shin, Thai T, Znati T." Detecting Application Denial-of-Service Attacks: A Group-Testing-Based Approach" IEEE Transactions on Parallel and Distributed Systems, Aug, 2010 , Vol : 21 , Issue:8 ,page(s): 1203 – 1216.

[2] M.T.Thai, Y.Xuan, I.Shin, and T.Znati, "On Detection of Malicious Users Using Group Testing Techniques," 28th International Conference on Distributed Computing Systems, June,2008, page(s): 206 – 213.

[3] S.Khattab, S.Gobriel, R.Melhem, and D.Mosse, "Live Baiting for Service-Level DoS Attackers" 27th International Conference on Computer Communications, Aug,2008 , Page(s): 171 - 175 .

[4] J. Mirkovic, J. Martin, and P. Reiher,"A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms," ACM journal on Computer Communication, volume 34, Issue 2, April 2004.

[5] G. Mori and J. Malik, "Recognizing Objects in Adversarial Clutter: Breaking a Visual Captcha," Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, Vol:1, 2003 , Page(s): 134 -141.

[6] D. Eppstein, M.T. Goodrich, and D. Hirschberg, "Improved Combinatorial Group Testing Algorithms for Real-World Problem Sizes," Proceedings of Workshop on Algorithms and Data Structures (WADS), page no: 86-98, 2005.

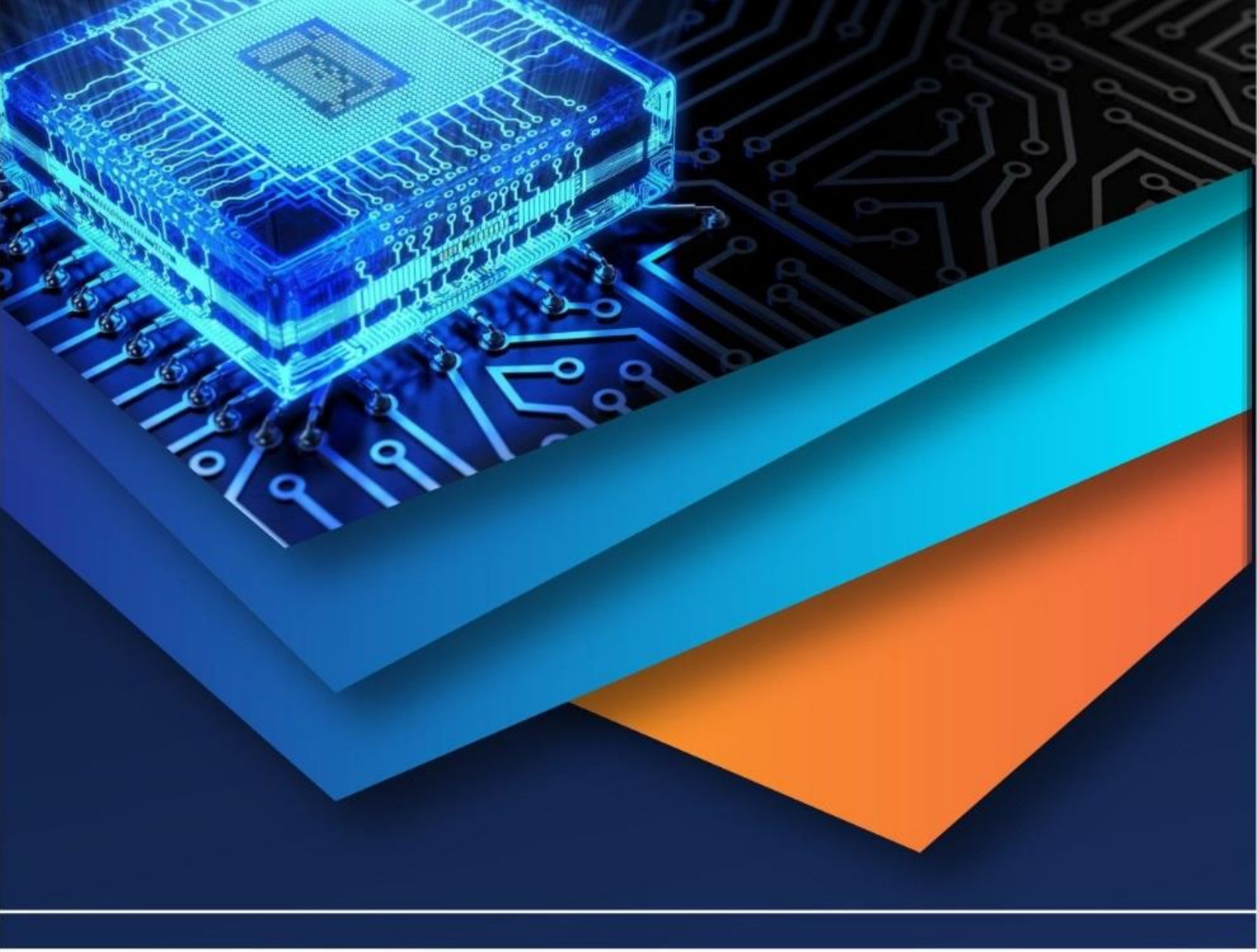
[7] V.D. Gligor, "Guaranteeing Access in spite of Distributed Service-Flooding Attacks," Proceedings of Security Protocols Workshop, 2003.

[8] G. Mori and J. Malik, "Recognizing Objects in Adversarial Clutter: Breaking a Visual Captcha," Proceedings of IEEE Conf. Computer Vision and Pattern Recognition, 2003.

[9] S.Vries, "A Corsaire White Paper: Application Denial of Service (DoS) Attacks," Author: Stephen de Vries, Document Reference : Application Level DoS Attacks, Vol : 4, April 2004.

[10] F. Kargl, J. Maier, and M. Weber, "Protecting Web Servers from Distributed Denial of Service Attacks," Proceedings of World Wide Web Conf., pp. 514-524, 2001.

[11] F.Kargl, J.Maier, and M.Weber, "Protecting Web Servers from Distributed Denial of Service Attacks," Proceedings of 10th International Conference on World Wide Web, 2001.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY