International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

# Shield Advanced Mitigation System of Distributed Denial of Service Attack in integration of Internet of Things and Cloud Computing Environment

**E.Helen Parimala, S. Albert Rabara, Y.Sunil Raj**

***Abstract*: Cloud services among public and business companies have become popular in recent years. For production activities, many companies rely on cloud technology. Distributed Denial of Services (DDoS) attack is an extremely damaging general and critical type of cloud attacks. Several efforts have been made in recent years to identify numerous types of DDoS attacks. This paper discusses the different types of DDoS attacks and their cloud computing consequences. Distributed Denial of Service attack (DDoS) is a malicious attempt to disrupt the normal movement of a targeted server, service or network through influx of internet traffic overwhelming the target or its infrastructure. The use of multiple affected computer systems as a source of attacks makes DDoS attacks effective. Computers and other networked tools, including IoT phones, may be included on exploited machines. A DDoS attack from a high level resembles a traffic jam that is caused by roads that prevents normal travel at their desired destination. So DDoS Attack is a major challenging problem in integrated Cloud and IoT. Hence, this paper proposes Shield Advanced Mitigation System of Distributed Denial of Service Attack in the integration of Internet of Things and Cloud Computing Environment. This secure architecture use two verification process to identify whether user is legitimate or malicious. Dynamic Captcha Testing with Equal Probability test for first verification process, moreover Zigsaw Image Puzzle Test is used for second verification process, and Intrusion Detection Prevention System is used to identify and prevent malicious user, moreover reverse proxy is used to hide server location. These functional components and flow could strengthen security in Client side network to provide cloud services furthermore to overcome distributed denial of service attack in the integration of Internet of Things and Cloud Environment.***

***Keywords* : Distributed Denial of Service, Internet of Things, Cloud Computing, Intrusion Detection and Prevention System, Firewall, Reverse Proxy.**

**Revised Manuscript Received on December 30, 2019.**
***** Correspondence Author
**Mrs. Helen Parimala***, Department of Computer Science, St. Joseph's College, Trichy, India. E-mail: helenandrew@gmail.com
**Dr. S. Albert Rabara**, Department of Computer Science, St. Joseph's College, Trichy, India. E-mail: a_rabara@yahoo.com
**Mr. Y. Sunil Raj**, Department of Computer Science, St. Joseph's College, Trichy, India. E-mail: ysrsjccs@gmail.com



## I. INTRODUCTION

The "IoT" model provides models and systems that enable "smart things" to be networked on an expansive scale using technologies such as RFID,

wireless sensors and actuator networks, which disperse embedded devices within the smart environment. The ongoing development of ICTs suggests to people that towns and environment itself are protected by awareness and practice, which in turn lead to an intelligent society [1]. At the moment, these devices are widely accepted in our daily facilities, such as vehicles, mobile phones, home appliances, etc., and provide an atmosphere, where a great number of things spread over an enormous area. However, with such huge sensor and actuator development, different challenges arise in fields of scalability, heterogeneity, versatility and inter-operability. Resource reflection has opened IoT to a wide range of potential applications [2]. It is currently moving to World Wide Web and its partner, in particular Web Services, which can be utilized as an intelligent platform and is useful to enhance interoperability between heterogeneous devices through an interface for outside world communications. These networks are proposed as Web-based next generation services and are referred to as Internet of Services (IoS) [3].

In Cloud, data is stored, managed and processed via a network of remote servers hosted on Internet ("Cloud") in data centers of third parties located at a remoteness from a city to all over the globe rather than on a pc or local server. The grid and virtualization software combines and evolves Cloud Computing. It allows end users to allow all-round shared computer resource storage and information applications to be shared on request by computers and by other devices. This can be done with the lowest leadership commitment.

According to NIST, Cloud Computing may be characterized as "the model for allowing rapid provisioning of and publication of management efforts or service provider interactions on request, accessible and on claim network access to shared pools of configurable computing assets (e.g., networks, databases, storage devices, applications and services). CC is more viable and available for its customers through certain products and models [4].

The Deployment and Service Systems are two working models for the cloud. Cloud provides its customers primarily three kinds of product types. They are PaaS, SaaS and IaaS. Four types of cloud deployment models are available. Such clouds are public, private, hybrid and community [5]. Such working models allow CC more versatile for SMEs to use large configurable and low-cost computer services.

The combination of IoT and cloud was not intended to be used in much of the applications because of their security issues and remains in the comprehensive written study. Some challenges to cloud environment are lack of protection, confidentiality, DDoS, QoS, trustworthiness, etc [6].

CC relies primarily on distribution of resources in the midst of third parties, which are the most important safety threats concern. The denial of services (DoS) are the major security threat to integrated CloudIoT [7]. During DoS, the attacker sends a large number of fake data packets from a zombie machine to the same network to access bandwidth or victims networks resources [8]. DDoS attack is like a DoS attack, but is carried out using multiple network botnet networks that go anywhere else in the world to hit single system, with more than one zombie system.

Intrusion detection prevention systems (IDPS) and conventional firewall framework use cloud providers (CSPs) to protect server from these attacks. IDPS is the mixture of Intrusion Detection Systems and Intrusion Prevention Systems (IPS). The IDS typically detects safety measures risks, but does not stop them from entering the data center by detecting samples and assaults. IDS is a little misleading since they do not detect intrusions but show proof of interruption [9] according to Deshmukh et.al.

Safety, confidentiality, on request availability of data, quality and latency are the major challenges of cloud computing. "Privacy is also seen as being the cloud's biggest concern" [10]. Security problems such as information protection, network security, access to resources etc. occur in cloud service layers respectively. To do this, hackers such as DoS attacks, cross-site scripting attacks, buffer overflow attacks etc. are responsible for numerous security attacks. Out of which DDoS attacks are put as the nine highest intimidation to CC [11].

According to the number of requests, the cloud servers increase their computational power. But the processing of queries by unit time is limited. When there are such queries to the client, further queries are prevented. This is the breakpoint that draws attention to DoS and DDoS attacks by attackers.

DDoS is the biggest attack in Norwegian history, and has disrupted five banks, three airlines, two telecommunications companies and online payment systems [12]. One of the largest threats was also a DDoS assault on Amazon Elastic Cloud Computing (EC2). Because of technical errors, given digitally signed service, eaves dropped messages can be manipulated. This has made hackers implement illogical code and attack DDoS that causes EC2 to charge users.

The hacker can easily perform these DoS and DDoS attacks even with a novice hacking experience. The DDoS attack generation systems are available [13] to accomplish this. The attackers execute DDoS attacks to diminish the victim's bandwidth and network assets [14]. DDoS attacks primarily impact network resource availability by blocking their bandwidth, so that legitimate users do not access cloud services. Therefore, these attacks must be avoided and users must be equipped with secure services.

Many types of attacks can damage network resources and services in the field of network security. Service Denial [15] is one of the best-known attacks. However, consumers may have issues with removing them from cloud services. It is important to defend network from malicious attacks so that they are able to provide their users with services. A clear authentication system can be enforced to external users, resources can be dedicated for internal usage depending on their responsibilities and access control policy management.

The network [16] may be exposed to several risks, including theft of sensitive data, in the absence of the layout of such procedures. In addition, network protection is designed to prevent misuse of the data and to prevent damage to the network. In the cloud environment, network security is growing throughout importance based on the role it can play in cloud security. On the basis of the above, a network safety approach for counteracting DDoS attacks on the network of a cloud user is suggested. It is a proactive system, which at the end of network access verifies user's legitimacy.

This paper therefore introduces a novel framework called Shield Advanced Mitigation System of Distributed Denial of Service which can be used to checking the packet of origins of applications (legitimate or malicious) to legitimize the origin using a Dynamic Captcha with Equal Probability Test. When DDoS attempts were malicious, the program retards requests from suspicious users using ZigSaw Image Puzzle test. The MSOFDDOS framework therefore carries out different actions against various types of attackers attempting to damage the device being secured. In this proposed architecture, Firewall is used for conducting Two Verification Process to identify Malicious user, and IDPS used for detecting and preventing Malicious users, Moreover Reverse Proxy is used for hide the server location. The Aim of the proposed architecture is providing uninterrupted cloud services to legitimate client and avoid Distributed Denial of Service Attack.

The following section provides an overview of work literature in this particular area that encourages us to carry out the work. In Section 3, denial of the type of service attacks was discussed. Section 4 explains the proposed architecture. Section 5 gives Experiment and Result Analysis. Section 6 gives Conclusion.

## II. REVIEW OF LITERATURE

A variety of research studies in DDOS flood attack detection performed, are available in several articles. In this section few of the related works are stated in the form of review. In [17] author F.Guenane et.al projected a new cloud-based firewall approaches that consists primarily of three key elements. This architecture contains frontage gateway, instances of digital firewalls and a back gateway. The Front-entry is a router that authenticates and distributes incoming traffic to various virtual firewall instances.

The decision is made by decision module for the distribution of the traffic. The firewall module in the digital firewall instance authenticates the data packets based on the examination rules section containing predefined traffic regulations for assault.

Back-Gateway is responsible for assembling and sending valid packets based on packet assembly and control modules back-to-back to the server.

Authors F.Guenane et.al [18] suggested a firewall architecture based on a hybrid cloud. Physical and digital are the main components of this proposed architecture. For virtual sections, there are specific virtual machines, in which each system performs firewall programs such as evaluation, monitoring and reporting of data packets with a complex resource supply. If traffic is overwhelmed on physical servers, it is diverted to virtual servers. Transfer is carried out through Secure Forwarding Architecture (SFA) between the architectures.

Huang presented in paper [19] a low reflection migration framework that helps identify origin, detect attacks, check turns and generate question modules. It worked ahead of IaaS because it calculates the computational competence and expenses on authentic users. It is created by IP-recognizing addresses to decide whether they are a hazard to a white list, black list. These APIs are controlled by administrators however, this open up the system to potential insider manipulation. When monitoring 100,000 addresses, operational degradation of the 8.5% is seen.

N.Jeyanthi et.al suggested in [20] the three-stage authentication scheme against DDoS attacks Reputation Based Cloud User Environment System. This approach splits users into three groups. A puzzle is provided to differentiate among people and robotic programs in the initial step of filtration. The packets will be dropped instantly if the first step is failing. Using the predefined pattern signatures for the attacks in the network level, the packets are dropped in the second phase and filtered. The attackers of the service level are decreased in the third phase by observing intervals between the consequent service requests.

In [21] the author uses the' strategy for SYN-based transmission control protocols. In this approach, the author provides two security layers. Hop filtering approach and encoding series numbers technique are used to protected cloud servers from attacks by DDoS. The MAC generator distinguishes between malicious packages and legitimate packages.

The authors in [22] propose trace back filtering for the prevention of cloud DoS and DDoS attacks, which are added with tags on the SOA packets to identify route of the attacker and to filter the traffic for security purposes. In this article, spoofed IP addresses were not taken into consideration, which could yield better results.

The detection of intrusions based on destination would, according to J. Buchanan et.al [23], give best results in the dropout of malicious packages and help to protect cloud server. Author uses bandwidth, CPU charging, speed, performance and memory uses to test this proposed system.

Writer B. Khadka et.al [24] notes that the root of intrusions is the best way to remove malicious packages and helps secure the cloud. Author tests the program proposed based on the performance of CPU metrics and a decreased level of malicious packages. In filtering the malicious packets, author have used the Rate sort but not the event sort out system.

## III. TYPES OF DDOS ATTACKS

The attacker sends a large number of fabricated data packs to a single zombie device in Denial-of service [25]. In that attack, the attacker sends fake data packs across the single network. DDoS attack is related to the DoS attack, although is carried out on in excess of one robot system, which is famous as multiple network botnets, what kind of target a single system and are positioned in the same location worldwide.

According to [26], attacks by DDoS with botnets were launched. By snooping on the network of vulnerability-prone presses, the botnets are picked by the attackers. Such computers are referred to as zombie or botnet machines. Host and zombie machines use spoofed IP addresses which make identification of the intruder and its origin more difficult. This assault is mainly aimed at overloading the assets. Bandwidth, CPUs, storage etc. preserve occasionally crashes the database in the sense of CC assets.

Various types of DoS attacks and DDoS attacks exist. In CC's opinion, below are the characteristics of these attacks.

Attack UDP [27] the attacker sends messages with spoofed back addresses in the User Datagram Protocol (UDP) connection. This is filled with multiple UDP packets into the random port of the victim server, which causes the host to continue to listen to the request on the network. If no application has been found, it answers with an unattainable packet of ICMP destinations. The host's constant listening to the port saves the host's money, which results in legitimate users not being available.

Flood Attack by ICMP [28] It's like from the UDP. It sends several packets (ping) to the target resource instantly, without waiting for answers. Furthermore, the flood concept of ICMP is identical to the flutter attack of UDP and can also absorb both input and output bandwidth, as the victim's servers can decelerate the entire system by using ICMP echo response packets.

Attack IP Spoofing [29] an attacker switches the source IP headers with the valid IP address or with a fake IP address. For a non-completed application, it renders the cloud server in a loop state. This means that no further requests regarding the true user can be handled by the server.

HTTP Flood [30] which does not use malfunctioning, spoofing otherwise reflex methods although targets Web server or application with legit HTTP GET or POST requests. The attacker attempts this attack. This attack also requires less bandwidth to reach the target page or server than other attacks. The attack is more successful if the server or software reserves the maximum resource available in response to each request.

TCP Flood [31] Attacker sends messages with spoofed return addresses to transmission control protocol (TCP). This is inundated with numerous UDP packets in the random port of the victim host that constantly forces the host to listen to the request on that port.

The host's constant listening of the port saves the host's energy and results in legal user's inaccessibility.

## IV. PROPOSED FRAMEWORK

Dynamic Captcha checking with equal probability algorithm, suggested design mitigation program for the distributed denial of service. This method used toward improve security in a client-side network for the first validation process. In contrast, distributed network denial in implementation of the Internet of Things and Cloud Infrastructure can be resolved. Two checks, for example the Dynamic Captcha Test and the Puzzle Test, are used in the firewall to determine if the incoming request is by the right user or a wrong user. Using Equal Probability Algorithms to dynamically check Captcha to identify malicious users or legitimate users in the first verifying phase. This algorithm is used for user authentication in client side network using a basic Captcha check, such like object images, distorted text, numerical calculation and I am not a Robot.

Earlier Captcha-proposed methodologies to identify malicious users, limitations: first, author allows for the Captcha to be entered in additional attempts. Malicious users can thus break the test by using programs or by manually using repeated attempts. This proposed design therefore incorporates one specific feature that allows the user to enter Captcha in three efforts, and the user who enters the right Captcha in these three attempts is the legitimate user, otherwise the malignant one. Suppose the valid user answer Captcha enters the second confirmation check within these three attempts. In three trials Malicious users did not reply, control exits from the first test and attempts will no longer be provided.

In previous methodologies, the second drawback is that users are able to enter Captcha almost an hour, as malicious users can break the check by means of automation / manual approach. This proposed design therefore uses a unique function to resolve. If users enter the appropriate Captcha, they are legitimate, otherwise malicious users, to enter Captcha within 3 minutes, provided they enter it in this 3 minutes. If legitimate users have not reacted within a specified time interval (3 minutes), even if the Captcha box is null even when the user is legitimate, control can leave the first check test. Since both legitimate and malicious users did not answer the first confirmation question within 3 minutes. If a valid user is presumed to respond, Captcha must enter a second check test within assigned minutes.

Dynamic evaluation is the third unique characteristic in the proposed architecture. Assume that 1000 users send incoming requests at a time and that the author is not performing a robot experiment for every 1000 user.

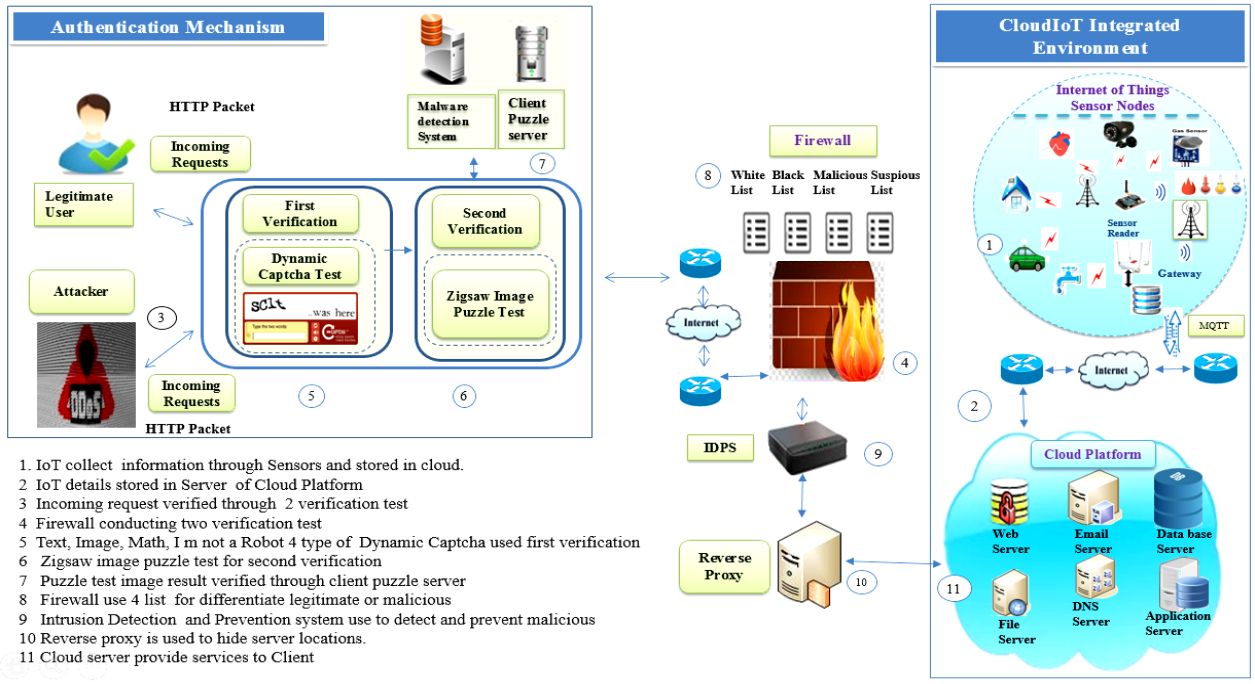


**Figure 1 Mitigation System of Distributed Denial of Service Attack**

The proposed design is therefore equally likely to present complex Captcha checks. Four types of Captcha tests are here equally allocated to 1000 users, such as object images, distorted texts, mathematical calculation and I m not a Robot, as are four randomly allocated tests for 1000 users. On this basis, malicious users can not determine which test is intended for the first testing method. Along with these new architectural features, superior architecture can be found. This is an effective method that monitors packet source at the beginning of a link by means of a dynamic Captcha test to identify bots (infected machines) that attempt to access the system.

The second check follows Zigsaw Image Puzzle analysis. The firewall manages the defense system by assigning four primary lists, Black and White list, Suspicious and Malicious list package origins, using intrusion prevention and detection systems, and monitoring packages that remain on the malware portion by using reversal proxy servers. Intrusion Detection and Prevention System is used to detect and prevent DDoS Attack. Moreover Reverse Proxy is used for hide the server location. The Aim of the proposed architecture is providing uninterrupted cloud services to legitimate client and avoid Distributed Denial of Service Attack.

## V. EXPERIMENTS AND RESULT ANALYSIS

This experiment was designed to demonstrate the firewall's positive influence in defending the database from DDoS floods with the OPNET tool. OPNET is considered to be versatile in the field of computers, communication networks, applications and protocols, among other commercial network simulators. With the correct use of the graphical editor interface, even network entities and topology are built in the physical layer of the application layer. Mapping is another feature of the graphic design of the OPNET, achieved after the object-oriented programming technique has been used to make mapping in real systems convenient. The proposed architecture focus is on this application layer protocols only, such as HTTP, Email, Telnet, ICMP, and FTP because most of the cloud applications are working in this layer.

The system design shows in Figure 2, where the server can be accessed and connected to the IP Cloud by users from the inner network. There is limited server access from IP clouds to the server and background traffic is provided for normal network access. The intruder penetrates the devices connected to Switch 1 (S1), which are compromised with all the phones. Such devices overload the network with HTTP client traffic requests and begin a large number of database applications.

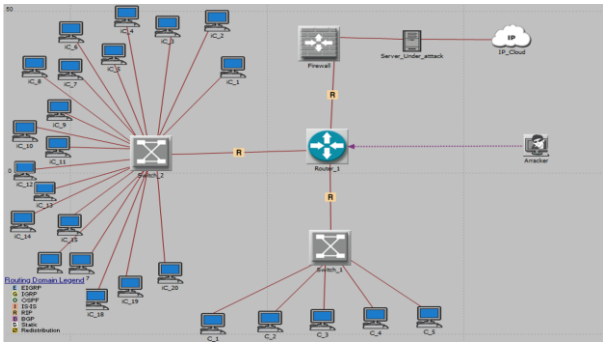

**Fig. 2. System design and implementation for a server under attack with the configured network system in OPNET**

Legitimate HTTP clients are connected via Switch 2 (S2), and the behavior of the attacker will not affect all connected users in this area. In addition, this framework considered the firewall architecture for protecting servers against DDoS attachments using a defined HTTP applications security policy which is implemented on a simulated model to safe scenarios. The enforced security policy was designed using a particular C++ script. This guarantees that the IP addresses of the compromised computers cannot be accessed, this simulates the techniques of the white and black display. In addition, only the application layer protocols are permitting access to the protected database via firewall. This is described as the blacklist that includes infected machines that are identifiable with security measures. The white list also contains all other IP addresses.

System was found to lending usual service and no delay was detected until the attack was initiated. After a serious of time delay, the attack was initiated and gradual delay was found in the response time. The results were recorded with respect to the parameters such as delay, throughput and bandwidth. Fig. 3. Displays the simulation process and response time of server with respect to the given input is recorded.

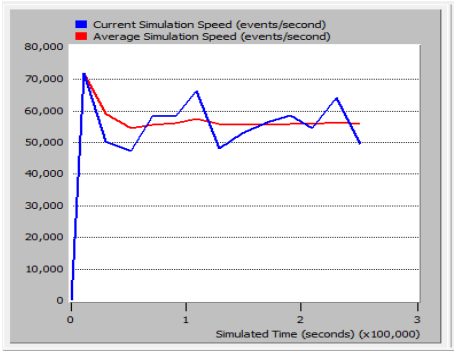


**Fig. 3. Speed of Simulation with respect to Input**

After a serious of time delay, the attack was initiated and gradual delay was found in the response time. Fig. 4. Shows the results were recorded with respect to the parameters such as delay, throughput and bandwidth. The bandwidth is assumed to be 100 Mbps. Peek time for response is increasing from 0 ms to 2592.00 ms, finally throughput of network becomes null as a result of unserviceable server which is under attack.

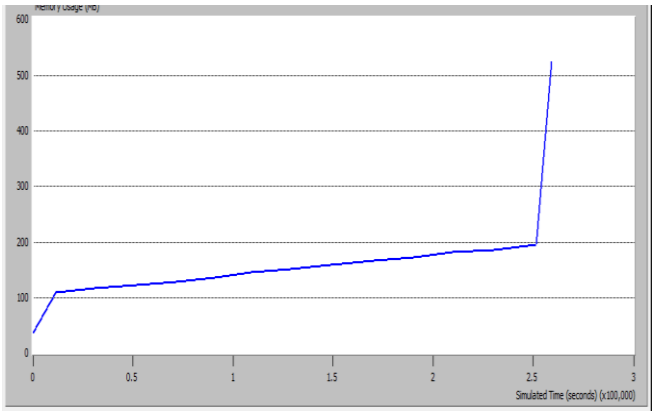


**Fig. 4. Response Time increasing during the Attack**

An ICMP packet is a packet that has been selected for the experiment because the implementation results are well known and easily obtained as the response time in the ICMP LAN environments is usually 1 or 2 ms long. In addition, ICMP was used to demonstrate the framework functionality and to improve understanding of its efficiency.

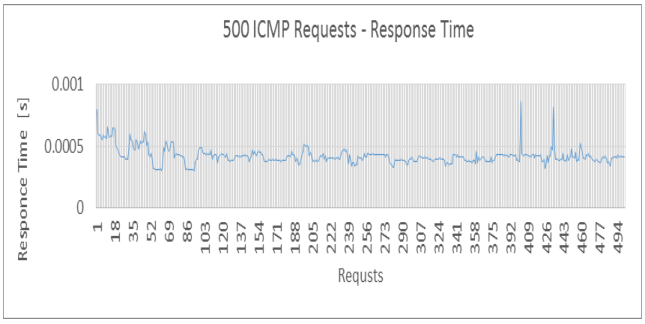


**Fig. 5. Response Time of 500 ICMP Packets.**

As typical load situation, 500 ICMP packets have been generated and sent to the protected domain via the proposed framework. The response time for 500 ICMP packets is shown in Figure (5). It is obvious that most packages were served between 0.3 and 0.5 ms entirely and that the average response time is 0.857 ms, whereas the minimum time is 0.301 ms, which is 0.419 ms.

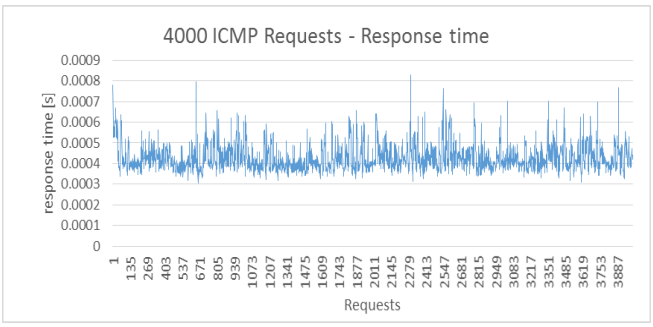


**Fig. 6. Response Time of 5000 ICMP Packets**

The response time for 500 ICMP packets is shown in Figure (6). For the entire number of test ICMP packets, the response time is therefore almost constant, even if the subset of the packets is 500 or 5000 because the average response time difference is 0.007 ms (7µs) in turn. The growing number of applications did not affect the response time. The average response time is therefore a good feature of the protection system, as the higher streams are not overwhelmed. Therefore, if attacked, it can be resilient.

## VI. CONCLUSION

In order to protect the cloud against attacks with any solution proposed, a DoS has been explained with its concept, method and specifications. Some of the most recent solutions to DDoS attacks was explored and evaluated. Dynamic Captcha Tests with an Equal Probability algorithm are used for the first experiment in authenticating customer-side networks in the Internet of Things and cloud environments to counter distributed denial of services attacks. Using the Fisrt Captcha and Zigsaw Image Puzzle Check, followed by an Intrusion Detection Prevention program and a Reversing Proxy server tracking the origin of other packages, it can be used by testing the source of requests (legitimate or malicious), to check malware components that can be found in them. Four additional keylists are added to the list of questionable and malicious firewalls (white list, black list, suspicious list and malicious list) to increase the DDoS attack reaction. The proposed model has been tested to demonstrate its validity and reliability.

## REFERENCES


1. Guinard D, V. Trifa, E. Wilde (2010). “A Resource Oriented Architecture for The Web of Things”, IEEE, Internet of Things (IoT), Tokyo, pp. 1-8, Japan.
2. Butt T, 2014, “Provision of adaptive and context-aware service discovery for the Internet of Things”, Doctoral Dissertation, Loughborough University.
3. Heuser L, Alsdorf, D. Woods, 2008, “The Web-Based Service Industry Infrastructure for Enterprise SOA 2.0”, Potential Killer Applications-Semantic Service Discovery, In International Research Forum, Potsdam, SAP Research, Evolved Technologist Press.
4. P. Yadav, S. Sujata, “Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA,” Int. J. Cloud Comput. Serv. Archit., vol. 3, no. 3, pp. 25–40, 2013.
5. K. Hwang, S. Kulkarni, Y. Hu, “Cloud security with virtualized defense and reputation-based trust management,” in 8th IEEE International Symposium on Dependable, Autonomic and Secure Computing, DASC 2009, 2009, pp. 717–722.
6. S. M. Spech, R. B. Lee, “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures,” in 17th International Conference on Parallel and Distributed Computing Systems, 2004, no. September, pp. 543–550.
7. A. Chonka, Y. Xiang, W. Zhou, A. Bonti, “Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks,” J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1097–1107, 2011.
8. M. Rahman, W. M. Cheung, “A Novel Cloud Computing Security Model to Detect and Prevent DoS and DDoS Attack,” J. Adv. Comput. Sci. Appl., vol. 5, no. 6, pp. 119–122, 2014.
9. D. Sequeira, “Types of in Intrusion Prevention Systems: Security’s Silver Bullet?”, 2003, pp. 36–41.
10. S. Piper, CISSP, SFCP, “Intrusion Prevention Systems for Dummies”, 2011.
11. K. Nagaraj, R. Dr.Sridaran, “An Overview of DDoS Attacks in Cloud Environment,” Int. J. Adv. Netw. Appl., pp. 124–127.
12. A. Harper, S. Harris, J. Ness, C. Eagle, G. Lenkey, T. Williams, “Gray Hat Hacking The Ethical Hackers Handbook,” Jan. 2011.
13. R. V. Deshmukh, K. K. Devadkar, “Understanding DDoS attack & its effect in cloud environment,” Procedia Comput. Sci., vol. 49, no. 1, pp. 202–210, 2015.
14. S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.
15. A. Carlin, M. Hammoudeh, O. Aldabbas, “Defence for Distributed Denial of Service Attacks in Cloud Computing,” in The International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015), 2015, vol. 73, no. (AWICT 2015), pp. 490–497.
16. N. Gruschka, M. Jensen, “Attack surfaces: A taxonomy for attacks on cloud services,” IEEE, 3rd Int. Conf. Cloud Comput. CLOUD 2010, pp. 276–279, 2010.
17. F. Guenane, M. Nogueira, A. Serhrouchni, “DDOS Mitigation Cloud-Based Service,” 2015 IEEE Trust., pp. 1363–1368, 2015.
18. F. Guenane, M. Nogueira, G. Pujolle, “Reducing DDoS attacks impact using a hybrid cloud-based firewalling architecture,” Glob. Inf. Infrastruct. Netw. Symp. GIIS 2014, 2014.
19. V. Huang, “A DDoS Mitigation System with Multi-stage Detection and Text-Based Turing Testing in Cloud Computing,” in 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2013.
20. N. Jeyanthi, H. Shabeeb, M. A. S. Durai, R. Thandeeswaran, “Reputation Based Service for Cloud User Environment,” Int. J. Eng, vol. 27, no. 8, pp. 1179–1184, 2014.
21. R. Aishwarya, S. Malliga, “Intrusion Detection System- An Efficient way to Thwart against Dos / DDos Attack in the Cloud Environment,” IEEE, 2014.
22. Y. Lanjuan, “Defense of DDoS attack for cloud computing,” in IEEE International Conference on Computer Science and Automation Engineering (CSAE), 2012, pp. 626–629.
23. J. Buchanan, Bill, Flandrin, Flavien,Macfarlane, Richard,Graves, “A Methodology To Evaluate Rate-Based Intrusion Prevention System Against Distributed Denial of Service,” no. August 2016, pp. 17–22, 2010.
24. B. Khadka, C. Withana, A. Alsadoon, and A. Elchouemi, “Distributed Denial of Service attack on Cloud : Detection and Prevention,” vol. 4, no. September, pp. 210–215, 2015.

25. M. Rahman, W. M. Cheung, "A Novel Cloud Computing Security Model to Detect and Prevent DoS and DDoS Attack," J. Adv. Comput. Sci. Appl, vol. 5, no. 6, pp. 119–122, 2014.
26. R. V. Deshmukh, K. K. Devadkar, "Understanding DDoS attack & its effect in cloud environment," Procedia Comput. Sci., vol. 49, no. 1, pp. 202–210, 2015.
27. P. Yadav, S. Sujata, "Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA," Int. J. Cloud Comput. Serv. Archit, vol. 3, no. 3, pp. 25–40, 2013.
28. K. Nagaraju,R. Dr.Sridaran, "An Overview of DDoS Attacks in Cloud Environment," Int. J. Adv. Netw. Appl., pp. 124–127.
29. L. Garber, "Denial-of-service attacks rip the internet," Computer (Long. Beach. Calif)., vol. 33, no. 4, pp. 12–17, 2000.
30. E. Anitha, S. Malliga, "A packet marking approach to protect cloud environment against DDoS attacks," 2013 Int. Conf. Inf. Commun. Embed. Syst. ICICES 2013, pp. 367–370, 2013.
31. J. Mirkovic,P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39–53, 2004.

## AUTHORS PROFILE

Mrs. E. Helen Parimala, is currently working as a Assistant professor in Department of Computer Science, M.V.M Arts and Science Government College, Dindigul, Tamilnadu, India. She has 8 years experience in teaching. She started her journey in academics by graduating with B.Sc Computer Science from Madurai kamaraj University with excellent academic record. She further studied at Madurai kamaraj university and holds Master degree (M.Sc) in Computer Science and also finished M.Ed in Tamilnadu Teacher Education. Further in her pursuit of education she has completed her Master of Philosophy (M.phil). She is pursuing Ph.D degree in St.Joseph's College(Autonomous), Tiruchirappalli, Tamilnadu, India. Her research interests include Computer Networks, Cloud Computing and Internet of Things. She has published various papers in the field of Internet of Things, analysis and implementation of mechanisms to optimize network performance in high speed networks and cloud environment.

**Dr. S. Albert Rabara, M.Sc, Ph.D.,** Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamilnadu, India. Having the 30 years of experience in teaching and 20 years of research experience. He is also Research Supervisor, having guided and produced a number of Ph.D's under major areas such as Network and Security, Wireless and Mobile Security, NGN Technology, Web Services Security, Internet of Things, Cloud Computing and so on. Have published 140 papers in known journals such as IEEE, ACM, Springer Science, Elsevier and Journals with high impact factors and also have 28 papers published in conferences proceedings.

**Mr. Y. Sunil Raj,** Assistant Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamilnadu, India. Having teaching experience of about seven years in Department of Computer Science, St. Joseph's College (Autonomous). He also have published papers in Cloud Computing, Big Data Analytics and Data Mining. He is also research scholar in computer science and his research interest includes Internet of Things and Cloud Computing.