IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 5, Ver. III (Sep. - Oct. 2016), PP 80-86
www.iosrjournals.org

Pattern Analytical Module for EDOS Attacker Recognition

Preeti Daffu[1], Amanpreet Kaur[2]
[1]*Research Scholar Morinda, India*
[2]*Assistant Professor Mohali, India*

Abstract: *Cloud computing has provided a platform to its users where they are charged on the basis of usage of the cloud resources; this is known as "pay-as-you-use". Today, Cloud computing is the most hyped technology arenas and it has became one of the rapidly rising sections of IT. It has permitted us to measure our servers in better and availability to provide the services to greater number of the end users. . In cloud environment it is very difficult to detect and filter the attack packets because everything is virtualized there. Issues of protecting the cloud from the attackers and hackers cannot be underestimated. EDOS attacks are the cloud specific attacks and such attack causes the financial loss to the end users. The cloud service model automatically balances the resources according to their request of the consumers. The technique used in proposed model will detect and mitigate the EDoS attack through few strategic attacker/s, group of the attackers or zombie machine network (BOTNET), it indirectly or directly decreased profits and reduce the cost for the cloud operators. In this paper, an approach have been proposed, named Pattern Attack Recognition, to detect and mitigate the Economic Denial of Sustainability (EDoS) attack in cloud computing. The model is designed to assess its response time and the outcomes show that it is a capable solution to mitigate the EDOS. computing is generally based upon the most usage of internet. Cloud computing offers high computing platforms which utilize the resources on basis of 'pay-per-as-use' model [7]. Cloud computing provide its users with five different characteristics which are broad network access to its users, on demand self service (anytime-anywhere), rapid elasticity, resource pooling (resource sharing), and measured service. There are three service models in cloud computing and these service models are Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) [4]. Cloud computing comes with benefits to its users and organizations. But there are various security issues and concerns that have come alongside the benefits it provide. There are multiple attack in cloud computing that are used to consume the bandwidth of the users and the resources too. Some of these attacks are spoofing attack, flooding attack, malware injection attack, DDoS attacks and EDoS attacks. Economic denial-of-sustainability (EDoS) is a form of DDoS attack and it is a cloud specific attack. Such attacks make use of available resources, they don't aim to consume the bandwidth of the user but there is an intention to put a huge financial burden and economical loss to the victim.*
Keywords: *Cloud Computing; EDOS-Shield; EDoS; Mitigation; Security; SLA; Pattern Recognition.*

I. Introduction

Cloud computing is a paradigm that represents the most significant moves in IT areas. The rapid growth of cloud computing brings revolt to current business models. Cloud computing technology has an ability to give multiple services to end users. The cloud computing model allows its users access to all information and computer resources from anywhere and anytime when a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computing processing power, and specialized corporate and user applications Cloud computing provide data storage, processing power and networks to user application. In simple terms, cloud computing is storing data and programs over internet rather than on computer's hard disk. Cloud

1.1 EdoS Attacks:

EDoS attack occurrs when the zombie machine transmits a very huge amount of unwanted traffic to cloud system and uses scalability of the cloud. As a result, this attack can make cloud unsustainable to charge the bill of user for their activities of attack. Mainly DDoS can attack on the cloud computing environment and an EdoS attacks is a form of a DdoS attack, where services can suggest to authorized user that never get the utilization of cloud resources are dynamically higher to fulfil the excess traffic. The following actors are involved in attempting an EDoS attack:

1. Cloud Service Provider (CSP): a user who rents its resources and performs billing
2. Cloud Service Consumer: it uses cloud resources to host its web application
3. Legitimate Client: access the services provided by cloud consumer.
4. Attacker: intentionally generates unwanted traffic to hit the economy of cloud consumer.

EDoS attacks aim to make the cloud resources unsustainable to the victim machine or the end users and DDoS attacks are attempted to block the cloud services.EDoS attacks are carried out for a long period of time unliked DDoS attacks which are short lived type of attacks [7]. The firms are chosen for the cloud that will experience overstated bills for the usage of auto scaling feature which is used address the overflow of malicious traffic to meet the necessity to clear SLA.

Figure 1. Effect of an EDoS Attack on the cloud users

A service level agreement contains the particular aspects that have been agreen between the end user and the service provider. A SLA can be defined at three different levels: customer based, service based and multilevle based sla. Service Level Agreement can contain the terms of reliability, availability, QoS, performance, service cost, billing approaches, and consequence terms. Thus the consequences are compulsory on the service providers if any of services registered in the SLA is not encounter the opportunities. Service provider can implement practical which need to be introduced by the customer inside the reply time remark as per SLA.

A service level agreement is article that can describe the connection between two parties: the receiver (end-user) and the service provider. This is a significant element of the certification for both parties. If used correctly it must:

- Describe and classify the customer's requirements.
- Provide a framework for understanding.
- Shorten composite matters.
- Decrease parts of struggle.
- Inspire discussion in the event of arguments.
- Remove impractical prospects.

In cloud computing security concerns and issues have played an important role in postponing the Cloud Computing reception.

Many of the organizations don't run their business on cloud due to the security issues related to it. Without doubt, tap your data, install the software on hard disk while using someone else's CPU seems unsatisfactory to many. Popular security matters like as botnet, data thrashing and data thrashing carriage to consider the threats to administration's software and data. Moreover, multi-tenancy model and combined computing properties in the cloud computing which has obtained the newest security tasks which essential novel methods to face with. For example, hackers may use Cloud to establish the botnet as because cloud offers consistent infrastructure which facilities to compact value for them to begin an attack.

Current computing methods provide to facilitate the multiple operators and require capability to classify the operator on making demand. In outdated methods, the operator's identity can confirm by examination and typed password through the login; the organization can record identification and use to regulate what processes have been executed. The process can confirm the operator's identity, which is called authentication. In this, Password-based authentication cannot appropriate for use on the computer networks. Password can transmit across networks has been interrupted and next used by the listeners to imitate the operator. In adding to security problem, password based authentication can be difficult; operator do not require to enter the password at every time they admission the network service. To control these difficulties, essential authentication approaches that have based upon cryptography are important. Once using authentication founded

on cryptography, an attacker's entry to the network needs information that will stop it from incorrectly claiming another's uniqueness.

The rest of paper is organized as follows: section II provides an extensive analysis of the existing work that have been done to reduce and mitigate such attacks. Section III describes the design and proposed model. Section IV describes the implementation and results. Section V describes the conclusion and future work.

II. Literature Survey

In 2016 Baig, Zubair A. et. al. [7] has proposed an approach which is based upon the rate limit technique and low overhead data for the mitigation of the EDoS attacks. This model relies upon the incoming request rate from one source (a client of cloud network) based upon the fixed threshold value. The duration factor also lies as the major factor while evaluating the nodes sending the request rate more than threshold. It is unable to detect the pattern-based controlled EDoS attacks i.e. it is unable to detect the attacks based upon their behaviour, where the attacker nodes work in the group. Multiple nodes might attack the target cloud by beating the threshold for request rate and duration. It is not capable of analyzing the proposed scheme to optimize the overall performance while looking at the service provider and network-level variations.

In 2014 [] F. Al-Haidari. M. Sqalli.K. Salah proposed the EDoS attacks on cloud computing services which is seen only a lone class of service. It has established the analytical model which is confirmed by the simulation model to study such influence of the EDoS attacks on cloud computing. The analytical model have faith on line up model which imprisonments cloud services and reflected the cost metrics counting and various performance end-to-end response time, throughput, usage of computing resources, and experienced cost resultant from attack. Meanwhile EDoS attack aims to cloud adopter, they have assessed the cost connected by the computing resources and bandwidth distributions at cloud service side. Additionally, results are exposed that there was slight or no obvious influence of attack on throughput of legitimate requests which is predictable due to availability and scalability of cloud services.

In 2013 [] W.Alosaimi and K.Al-Brgain presented the Outline to meet EDoS with testing of first packet from source of request to recognized legitimacy of source place using the Graphical Turing Test is proposed. In this method source of first packet receive at firewall which has check against at current list to authenticate source node. If source IP does not originate in list then that packet has been advanced to the verifier node. Furthermore, verifier node transmits the GGT test to user. If user will permit to test a positive greeting is sent to firewall and packet is confirmed as legitimate. Else a negative greeting can be received at the firewall and packet is declined. Also IP address of the source will be added to blacklist seeing it as a malicious packet. This scenario can be implemented with well-organized filtering system against of the DDoS that replaced the place hiding of the protected servers by reverse proxy method. This function can help in other tasks such as load balancing.

In 2013[] Z.A. Baig, F.Binbeshr proposed an approach for selective regulatory user requirements for service, applied at the service provider's end. This system mitigate the effects of imminent EDoS attack against serious cloud resources. The incoming requests from the users have been categorized into two categories i.e. genuine users and suspicious. Subsequently, further examination is lead to guarantee that precedence to cloud service admission is given to those end-users marked as being legitimate, whereas, doubtful users are given smaller importance to service admission, till they are finally removed from doubtful list. Simulations were lead to study the presentation of the scheme with results display promise. The system can be included of various components, specifically, vFirewall, VM Observer, and VM Investigator operating hand in hand, to regulate the admission to end-users, for mitigating their effects of an EDoS attack. To examine their results which are founded from simulation of proposed system, it is obvious that the consequences causing the EDoS attack is mitigated when the access to cloud resources is controlled over the bounce of time.

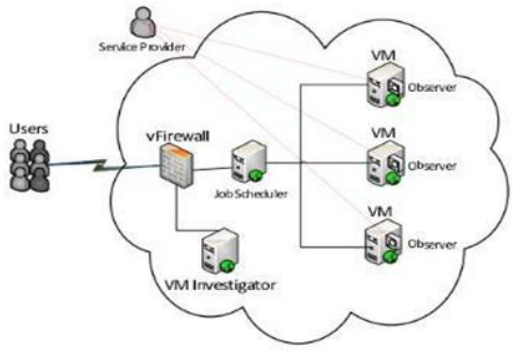

Figure 2. The proposed architecture of EDoS mitigation technique

In 2012 [] Al, F., Sqalli, M., AND Salah, K proposed EDoS-shield to mitigate their EDoS attacks to create from spoofed IP addresses. They have assessed four different circumstances while using discrete event simulation model. In first situation of attacks it signifies the worst case of scenario. In second situation used the real EDoS-Shield mitigation technique. In third scenario proposed enhanced EDoS-Shield mitigation method to defend their cloud service. The last situation is base situation which they are assuming there is no attack at all, and so it defines the best solution. They use time to live (TTL) parameter of IP packet header field to calculate their life time of packet inside network value of TTL is decremented each time when packet has permitted through any router. The packet can be rejected whenever TTL value has become zero. It avoids infinite loop of packet in their network. Results are founded from discrete event simulation

In 2012[] M.Naresh Kumar, EL. AL proposed their work that will stress on in-cloud eDDoS mitigation web service which is used on-demand. In-Cloud Scrubber Service functionality is authenticate and to produce the crypto puzzle. The produced crypto puzzle is used to resolve by the Service Consumer/ User with brute force method in order to display their legitimacy to locate Service. The proposed model can be displayed in figure 3. As the result of Puzzle generation and confirmation has done by Scrubber Service, load on the Service Provider servers has been succeeded. There are dropping cloud-based bills to service provider and availability of service can be guaranteed.

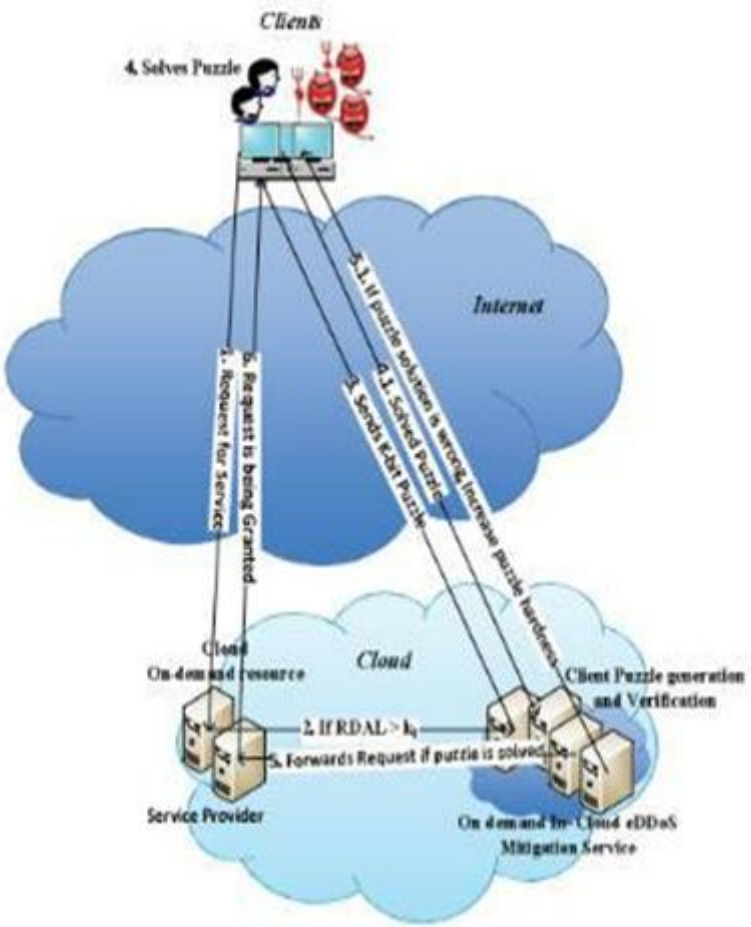

Figure 3. In-cloud eDDoS mitigation web service (Scrubber Service)

In 2011[] H.Sqalli. F.Al.Haidari. K.Salah proposed novel mitigation technique against their EDoS attack in the Cloud Computing, which is namely EDoS-Shield. The main idea is to verify whether requests are coming from users are from a legitimate user or obtain by bots. This is obtained by advance first demand to verifier node in the proposed construction. This verifier node has answerable for verification process and for apprised black and white lists based upon their results of verification process. The succeed requests are coming from bots that will be jammed by virtual firewall since the IP addresses can be originated in black list. On other side, the succeeding requests are coming from legitimate clients will be advanced straight to target cloud service since their IP addresses will be originate in white list. As result only requests from the legitimate clients will reach target cloud service and thus mitigating the EDoS attack.

III. Design And Proposed Model

This section displays the proposed model which mitigates EDoS attack in the cloud security. Pattern recognition technique has been used in the proposed model. The pattern recognition technique refers to the behavior of the packets that have been sent to the user. The delivery of packets from several nodes at frequency of 400-800 displays the nature of attack detected. The proposed model can detect the attacks in range as severe attacks. The proposed model provides pre-shared security mechanism which is used to ensure their access of legitimate users on cloud services. It performs pattern analysis to detect EDoS caused by the BOTNET mechanism and include key-sharing and post-setup authentication method to preserve from the replication of attacks. The proposed technique is used to include existing security scheme to add their attack detection functionality to the security method to detect single user attacks.

The pattern recognition has done in following manner:

Algorithm 1: Pattern Attack Recognition

Step1. Scan the traffic flow.
Step2. Find the anomalies and peaks in traffic flow.
Step3. Apply pattern recognition on network flow.
Step4. Evaluate the impact of pattern based EDoS attack.

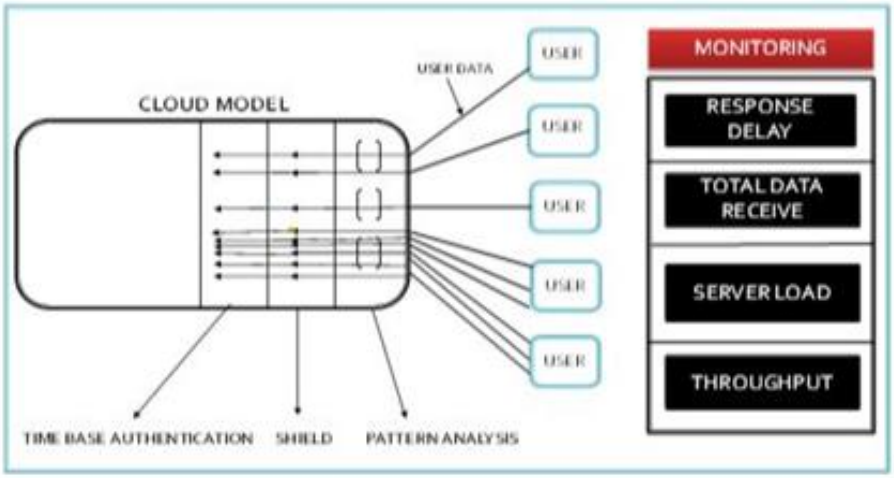

Figure 4: The proposed model for pattern recognition.

Figure 4 displays the proposed model in which displays five different user that are sending data to the cloud. The traffic has based upon the data that is coming for user. First three users send the data in normal flow. Where, data is passing through the cloud normally. In next two user data is transmitting to cloud in suitable manner. In which lots of data is sends from a particular node and therefore traffic causes.

The monitoring process displays four different terms that will provide reading for simulation In the future.

- Response delay displays the total time taken by a packet to reply the sender.
- Total data receive will tells the data which receive at the receiver end.
- Server load will display how much load is on resources.
- Throughput displays the amount of packets passing through a particular system.

4. 4. IMPLEMENTATION AND RESULTS

The Implementation consists of three main components:

- Per user Attack with Proposed security model.
- Multiple users Pattern Attack under the permitted traffic limit.
- Pattern Recognition.

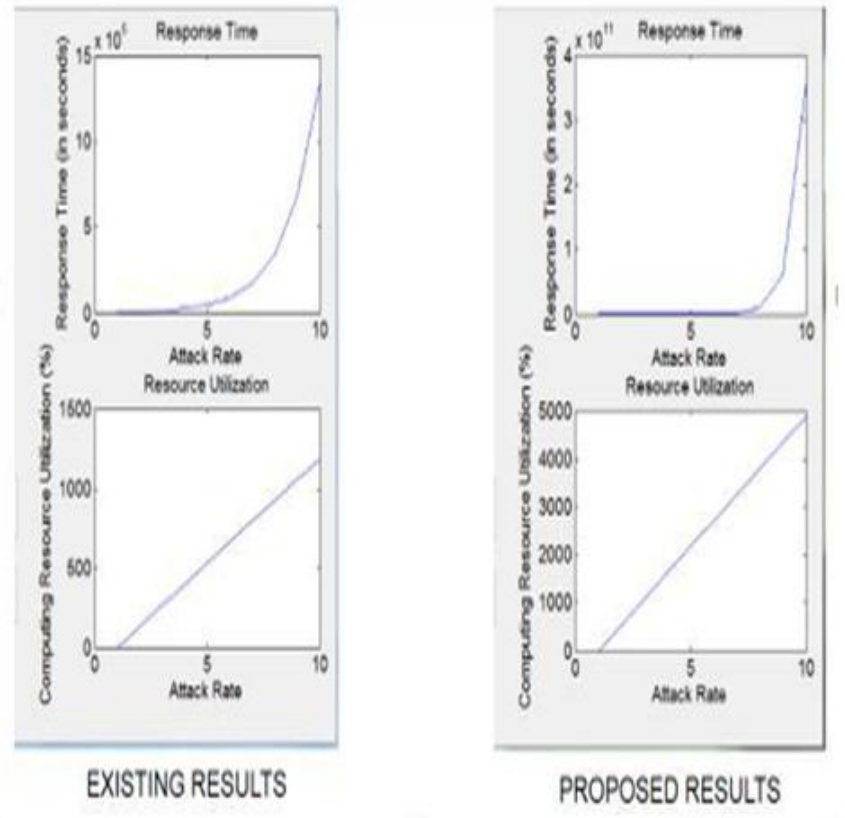

Figure 5 Implementation results.

The implementation scenario includes cloud based service level setup. Scenario can be simulated with several legitimate and attacker users. The module to simulate EDoS attacks and attacks effect the monitoring on basis of throughput, request delay, etc. implementation scenario will further include the use of existing security mechanism to evaluate real-time performance of the existing system in simulated environment. The setup will include setup of proposed model based on the basic simulation setup. It considers several attack situations in their cloud simulations to evaluate their performance of proposed model in detail. The implementation includes their existing work. The existing model can be effective in the detection and prevention of per user attacks. Existing solution can protect effectively, if few user violate the traffic laws by sending heavy amount of traffic. But existing solution is not able to save from the pattern attack, where attackers works same as legitimate users and transmit under their limit traffic from several nodes in overload the cloud processing.

The existing model is detected effectively the attack from individual users, but failed to track the pattern attack, where as attacker nodes are sending under permitted limit data to the cloud platform. Existing system are permitted all the attacker links that collectively lowers performance of cloud platform. As shown in figure 5, performance lag can be clearly looking from the high response time. The pattern attack is being detected as Minor Attack or No Attack in case of existing system. The proposed model implementation for pattern recognition is capable of detecting the severity of pattern attack. The proposed model has efficient in detecting the impact of pattern attack and classify it as moderate or severe attack, where existing model fails to detect severity of attack. The Proposed model displays more resource utilization as compared to the existing model because attack prevention has not completed yet. Both, existing and proposed model rely on node/user verification to ensure the legitimacy of the user.

V. Conclusion And Future Work

In this paper, proposed model has designed for the pattern attack recognition and detection and traffic pattern analysis. The proposed model has been designed for the purpose of original impact detection for pattern attacks on the cloud platforms. The existing system is lacking in their reading real impact of pattern based EDoS attacks. The proposed model is performed significantly well for their calculating impact of pattern based upon EDoS attack. The results are recorded in form of response time and resource usage. The proposed model has been performed well on basis of given parameters. In the future, the proposed model will be enhanced for attack prevention technique once the pattern attack in detected. The attack prevention model will use node and traffic filtering in order to keep the resource usage and response time under their limits during attack periods.

Acknowledgments

I acknowledge with deep sense of gratitude and most sincere appreciation, the valuable guidance and unfailing encouragement rendered to me by "Mrs. Amanpreet Kaur" Assistant Professor for their proficient and enthusiastic guidance, useful encouragement and immense help. I have been deep sense of admiration for them inmate goodness and inexhaustible enthusiasm. The proposed work will be completed under the guidance of the official guide and other experts at the campus of the Chandigarh group of Colleges, Landran, and Mohali.

References

[1]. Al-Haidari, F., M. Sqalli, and K. Salah. 2015 "Evaluation of the Impact of EDoS Attacks Against Cloud Computing Services." Arabian Journal for Science and Engineering, 40(3): 773-785.

[2]. Al-Haidari, F., Sqalli, M.H. and Salah, K., 2012, June. Enhanced edos-shield for mitigating edos attacks originating from spoofed ip addresses. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on : 1167-1174. IEEE.

[3]. Bakshi, A. and Yogesh, B., 2010, February. "Securing cloud from ddos attacks using intrusion detection system in virtual machine." In Communication Software and Networks, ICCSN'10. Second International Conference on : 260-264, IEEE.

[4]. Baig, Zubair A., Sait S.M. and Binbeshr F. 2016. "Controlled Access to Cloud Resources for Mitigating Economic Denial of Sustainability (EDoS) Attacks." Computer Networks. 97: 31-47

[5]. Baig, Zubair A., and Binbeshr Farid 2013. "Controlled Virtual Resource Access to Mitigate Economic Denial of Sustainability (EDoS) Attacks against Cloud Infrastructures." Cloud Computing and Big Data (CloudCom-Asia), International Conference: 346-353, IEEE.

[6]. DA. Levine, IF.Akyildiz, M.Naghshineh. "A resource estimation and call admission algorithm for wireless multimedia networks using the shadow cluster concept"in IEEE/ACM Trans Netw , pp. 1–12, 1997.

[7]. EA Kaur, D Singh "Exploring Data Security Issues and Scrutinizing then in Cloud Environment"

[8]. K.Yang, A.Liotta "An adaptive multi-constraint partitioning algorithm for offloading in pervasive ystems,"In:Proceedings of the fourth annual IEEE international conference on pervasive computing and communications (PerCom'06),Pisa, Italy, pp. 116–25,2006.

[9]. Liu, H., 2010, October. A new form of DOS attack in a cloud and its avoidance mechanism. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop:65-76, ACM.

[10]. Naresh Kumar, M., Sujatha, P., Kalva, V., Nagori, R., Katukojwala, A.K. and Kumar, M., 2012, November. Mitigating economic denial of sustainability (edos) in cloud computing using in-cloud scrubber service. In Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on: 535-539. IEEE.

[11]. Morein, W.G., Stavrou, A., Cook, D.L., Keromytis, A.D., Misra, V. and Rubenstein, D., 2003, October. Using graphic turing tests to counter automated ddos attacks against web servers. In Proceedings of the 10th ACM conference on Computer and communications security: 8-19. ACM.

[12]. MV. Barbera, S.Kosta, A.Mei, VC. Perta,and J.Stefa, "Mobile Offloading in the Wild: Findings and Lessons

[13]. Learned Through a Real –life Experiment with a New Cloud-aware System,"in IEEE INFOCOM, pp 2355-2363, Toronto,ON, 27April- 2 May 2014.

[14]. R.Balan , J.Flinn , M.Satyanarayanan , S.Sinnamohideen and HI, Yang , "The case for foraging,"in Proceedings of the 10th workshop on ACM SOGOPS European workshop (EW 02), Saint-Emilion, France,pp 87-92, 2002.

[15]. Sqalli, M.H., Al-Haidari, F. and Salah, K., 2011, December. Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing. In Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on: 49-56. IEEE.

[16]. Y.Wen,W.Zhang and H,Luo, "Energy-optimal mobile application execution: Taming resource –poor mobile devices with cloud clones,"in INFOCOM,pp. 2716-2720,Orlando,FL,25-30 March. 2012.

[17]. Zunnurhain, K. and Vrbsky, S.V., 2010, December. Security attacks and solutions in clouds. In Proceedings of the 1st international conference on cloud computing: 145-156.