International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 10 | Oct 2018 www.irjet.net p-ISSN: 2395-0072

# EEDE- Extenuating EDOS for DDOS and Eluding HTTP Web based attacks in Cloud using MapReduce

**S.Ezhilarasi[1]**

[1]*Assistant Professor, Department of CSE, Velammal college of Engineering and Technology, Madurai, TamilNadu, India*

---

**Abstract -** *Security assurance in the Cloud Service is a major challenge for the Providers. The Security can be administered in the Cloud at various levels and for several types of attacks. This study proposes a method of integration between HTTP GET flooding among DDOS attacks and MapReduce processing for a fast attack detection in cloud computing environment. This method is possible to ensure the availability of the target system for accurate and reliable detection based on HTTP GET flooding. This paper deals about the threats and the counter measures of the prevailing DDoS attacks on the Cloud Environment as well as the Cloud Specific Vulnerabilities to these attacks. In specific, HTTP and XMLbased DDoS attacks on the cloud service are experimented under proposed security framework for EDoS Protection. A Cloud Service was hosted on Amazon EC2. The Service was targeted by HTTP, XML DDoS attacks from several nodes, which lead to the scaling of the service by consuming more Amazon EC2 resources, which in turn lead to Economic Denial of Sustainability to the Cloud Service under attack. Thus this paper explores the transformation of traditional Distributed denial-of-service (DDoS) attack into cloud specific Economic Denial of Sustainability (EDoS) attack*

***Key Words***: *DDoS attack, EDoS attack, HTTP GET Flooding Attack, Web Security, MapReduce*

## 1.INTRODUCTION

"Cloud Computing", a new wave in the Internet revolution, transforms the kind of services provided over the Internet. The Cloud Services can be viewed from two perspectives, one as Cloud Service Provider and the other as Cloud Service Consumer. The Security can be administered in the Cloud at various levels and for several types of attacks. The threats and the attacks on the Cloud service can be common prevailing attacks in the internet or can be cloud specific. Cloud Computing is a heterogeneously distributed environment, which provides highly scalable, elastic and always available resources as service through Internet. The cloud computing provides everything as a service. In cloud computing, large pools of resources are available and it is allocated dynamically to the applications. The cloud infrastructure is fully virtualized to utilize the hardware effectively. The cloud infrastructure supports all hardware architectures [1].The cloud middleware provides an abstraction to the underlying physical cloud resources. Thus providing security to cloud is a complicated issue. The papers [3][4][5][6] give an clear idea about the security issues related to cloud computing. Further Cloud Security Alliance (CSA) give us the areas for security needed in cloud computing [7]. DDos attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet [8] [9] [2].

Web applications attacks are difficult to distinguish between normal traffic and DDoS. Also, the Target system can be affected regardless of hardware performance because target server can be damaged by small connections and traffics. This study proposes a method of integration between HTTP GET flooding among DDOS attacks and MapReduce processing [6] [2] for a fast attack detection in cloud computing environment. This method is possible to ensure the availability of the target system for accurate and reliable detection based on HTTP GET flooding.

### 1.1 Distributed denial of service (DDoS) attacks

DDoS attack is a distributed, large scale coordinated attempt of flooding the network with an enormous amount of packets which is difficult for victim network to han-dle, and hence the victim becomes unable to provide the services to its legitimate user and also the network performance is greatly deteriorated. This attack exhausts the resources of the victim network such as bandwidth, memory, computing power etc. The system which suffers from attacked or whose services are attacked is called as "primary victim" and on other hand "secondary victims" is the system that is used to originate the attack. These secondary victims provide the attacker, the ability to wage a more powerful DDoS attack as it is difficult to track down the real attacker. Denial of Service (DoS) attacks is used to consume all the resources of the target machine (victim's services) Distributed denial of service (DDoS) attack is some sort of malicious activity or a typical behavior, which cooperate the availability of the server's resources and prevents the legitimate users from using the service. DDOS attacks are not meant to alter data contents or achieve illegal access, but in that place they target to crash the servers, generally by temporarily interrupting or suspending the services of a host connected to the Internet. DOS attacks can occur from either a single source or multiple sources. Multiple source DOS attacks are called distributed denial-of service (DDOS) attacks.

A Denial of Service (DoS) attack is an attempt to make a computer resource unavailable to normal users. The Dos attacks are becoming more powerful due to bot behavior. Attack that leverages multiple sources to create the denial-of-service condition is known as The Distributed Denial of Service (DDoS) attack. DDoS attacks are big threats to

internet services. HTTP flooding attack is one of the typical DDos attack, in that hosts are sending large amount of request to target website to exhaust its resources. Now a day there is massive growth in internet traffic. Due to this many DDoS attack detection systems facing a problem. A Distributed Denial of service (DDos) attack can employ hundreds or even thousands of computers that have been previously flooded by HTTP GET packet.

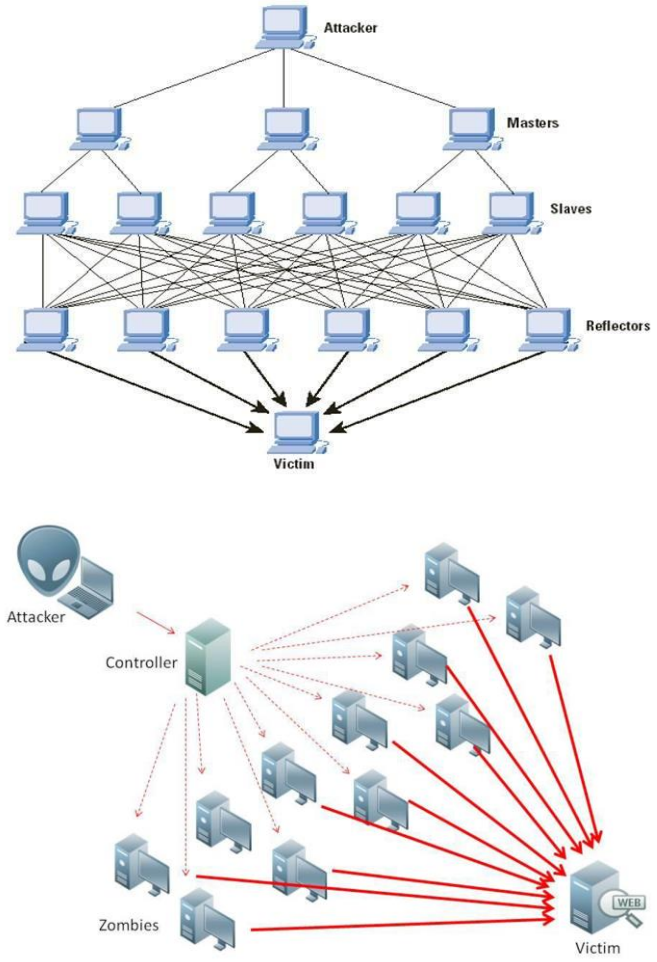


**Fig -1**: Architecture of DDOS

### 1.2 Economic Denial of Sustainability (EDOS) Attack

Many organizations move their business into cloud for the following reasons. They no need to buy the entire infrastructure. The maintenance cost is nill.There by the organization can reduce the purchasing and operational costs. They need to pay for only the resources used [1].Cloud services are provided in the form of service level agreements (SLA).The SLA defines the level of service required by the user. Some SLA will restrict the use of cloud resources to the customers. Some SLA provides infinite amount of resources to customers for QoS. The Cloud services are provided as Pay-per-Use. Therefore the resource utilization and the processing power are charged to the customer by the provider. The DDoS attack aims to utilize the cloud resources there by denying the service to the legitimate users. In the absence of any proper mechanisms to counter DDoS attack the resources can be allocated to the DDoS requests. As mentioned earlier identifying the attack traffic from the legitimate traffic is a difficult one and also there is no one technique which will completely eliminate the DDoS attacks. Therefore the DDoS attack may deplete the cloud resources rapidly. To provide 100% availability the provider may allocate more and more resources to the attack itself. More instances of the services may be launched according to the customers SLA. Finally the resource utilization and the processing power are charged to the customer. Thus a traditional DDoS attack can be transformed into an Economic Denial of Sustainability attack (EDoS) in the cloud Environment. If vulnerability is prevalent in the state-of-theart cloud offerings, it must be regarded as cloud-specific. Thus the cloud is vulnerable to EDoS attack, the EDoS attack can be cloud specific.

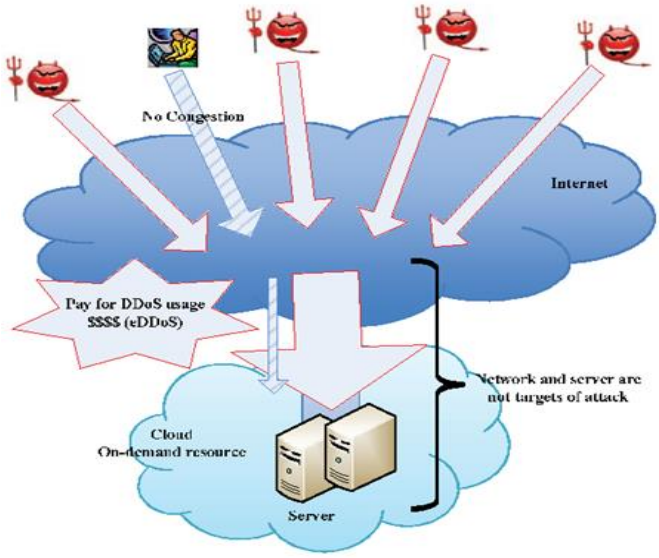


**Fig -2**: Architecture of EDOS

### 1.3 Literature Survey

Firstly, detection method based on signature can identify an attack if the monitored traffic matches known characteristics of malicious activity. In practice, bandwidth attacks do not need to exploit software vulnerabilities in order to be effective. It is relatively easy for attackers to vary the type and content of attack traffic, which makes it difficult to design accurate signatures for DoS attacks. While signature based detection can be used to detect communication between attackers and their "zombie" computers for known attack tools, in many cases this communication is encrypted, rendering signature-based detection ineffective. This limits the effectiveness of signature based detection for DoS attacks [10].

The next is DDoS detection method based on a threshold for HTTP GET Request. The HTTP Get Flooding attack is the most critical and frequently attempted attacks and the threshold is generated from the characteristics of HTTP GET Request behaviors [11]. DDoS detection method based on a threshold for HTTP GET Request is short of accurateness since the threshold is bound to be high. Especially, the

conventional method is vulnerable to up-to date DDoS attack that paralyzes the system with small amount of HTTP requests.

Finally, detection method based on user behavior is a methodology for disadvantage between the above methods. The main research contents of this method are a classification method through applying user pattern from web page, a method applying Markov model through web browsing pattern analysis, a detection method of falsification HTTP message attack through monitoring HTTP Request and so on.

## 2. HTTP GET Flooding attack

An HTTP flood is an attack method used by hackers to attack web servers and applications. It consists of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a target web server. These requests are specifically designed to consume a significant amount of the server's resources, and therefore can result in a denial-of-service condition (without necessarily requiring a high rate of network traffic). Such requests are often sent en masse by means of a botnet, increasing the attack's overall power [8].

Fig 3 illustrates the packet flow of HTTP GET request attack after single TCP connection. This case is from a Single TCP connection to processing of HTTP GET request and attack Victims get damaged by less attack bandwidth. This attack can not detect using SYN rate limit detection method. Also, it can request to change the number of pages for avoiding detection. This process is for giving a heavy load to same page or database server through multipe HTTP GET request in single connection. HTTP flood attacks may be one of the most advanced non-vulnerability threats facing web servers today. It is very hard for network security devices to distinguish between legitimate HTTP traffic and malicious HTTP traffic, and if not handled correctly, it could cause a high number of false-positive detections. Rate-based detection engines are also not successful at detecting HTTP flood attacks, as the traffic volume of HTTP floods may be under detection thresholds. Because of this, it is necessary to use several parameters detection including rate-based and rate-invariant [12].

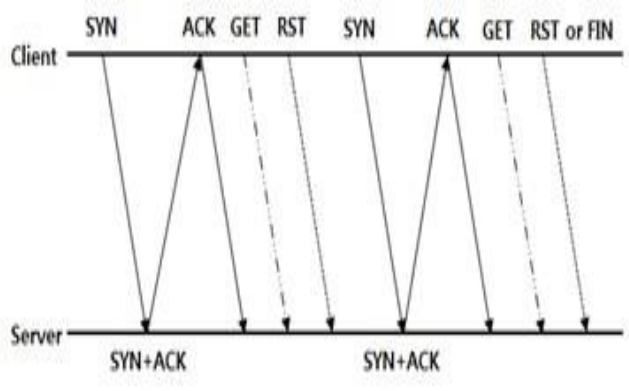


**Fig -3**: Packet Flow of HTTP GET Request attack

### 2.1 Analysis for DDOS Attack detection

DDos threats can be classified as an attack of Zombie Cloud Client, DDoS attack for user VM(Virtual Machine) attack between VM through partial domination of cloud server, Hypervisor attack of VM through most domination of cloud server and so on [13] [14]. Among them, hypervisor attack performs the service and data loss through authorization. Fig 4 illustrates flooding DDoS attack in cloud computing environment. DDos attack is occured the resource imbalance between victim client and internet through packet transmission from infected zombie cloud client to victim client system. Also, transmitted huge traffics from infected host interrupt to connect victim clients. DDoS attacks have occurred, the source address is widely distributed. However the port can be changed by attack packets and attack tool. As a result, the distribution of destination address converges on small point.

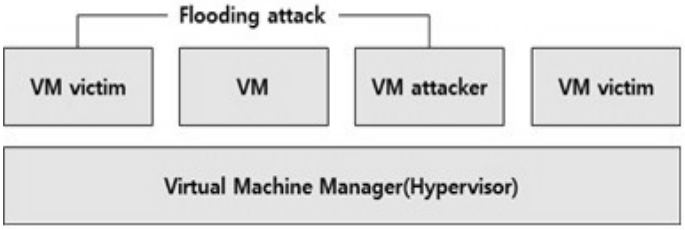


**Fig-4**:Flooding DDoS attack in cloud computing environment.

## 3. Proposed Model

The most typical response method of HTTP GET flooding is the analysis of request value based on packet checking. And then, it performs detection and blocking by threshold. Policy based on threshold performs a web server protection and traffic blocking using threshold through monitoring of HTTP GET Request by source terminal and destination. Detection of DDoS attack analyzes to check the normal state of each network.

### 3.1. Eluding HTTP Web based attacks in Cloud using MapReduce

In this paper, confrontation method of HTTP GET flooding attack is as following:

1. The suspected IP by DDoS attack is sent challenge values.

2. The IP by normal response is allowed the connection but another IP is filtered over a period of time.

3. The depletion of TCP connection are checked and huge HTTP Request are confirmed. (Creation of HTTP Request such as, image, jsp, html and so on.)

4. The detection method of DDoS attack by packet analysis is used input values of MapReduce for strange detection rule analysis using a statistical analysis and threshold

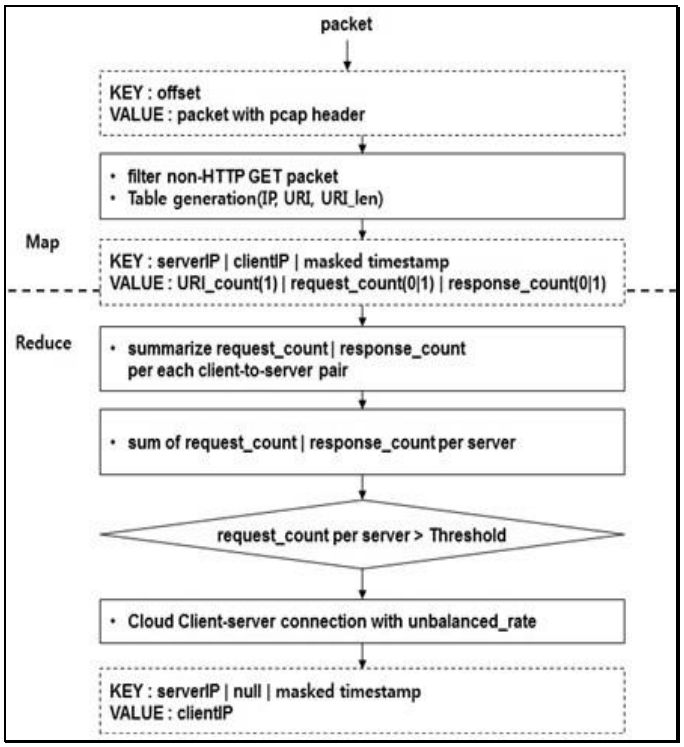


**Fig -5**: MapReduce for HTTP GET flooding DDoS detection

In fig. 5, Get count of Map region table is increased after 3 ways hand shake if incomplete GET or POST has been entered. Finally, Get count value of excess threshold is indicated that this case is a malicious packet. Also, Get packet is continually used a same URI. The Get packet is continually used a same URI in HTTP GET flooding attack. Therefore, malicious packet can be divided using threshold of IP, Port, URI and so on.

### 3.2. Extenuating EDOS for DDOS

The major focus of this paper is to find a cloud specific vulnerability.

The EDoS attack is identified as a Cloud Specific DDoS attack. Various techniques that are prevalent today are not up to the mark to protect the cloud from the EDoS attack. The counter mechanisms which are implemented only in the target machine are not efficient to defend against the DDoS attack. The approach should be a distributed one. On demand mitigation techniques will be well suited for the cloud environment. The mechanism which is fully based on trust might not be a good choice. The cloud computing is not yet standardized, so the vendors uses their proprietary security mechanisms. The Cloud Computing should be standardized soon, so that a solid solution can be proposed and implemented. The mechanism should be interoperable between different cloud providers. The mechanisms focusing on the identity of the user is a better solution to avoid the EDoS attack. Distributed traceback approach can be used to eliminate the attack traffic in the network itself. More intelligent traffic monitoring techniques are needed.

### 3.3. Security Framework for EDOS Atteack Protection

Considering the requirements that are necessary for the countermeasure, new security architecture is proposed. This frame work can be implemented to protect the cloud services from the EDoS attacks. The proposed framework consists of firewall which is the entry point for the cloud and Client puzzle server, which is a well-known technique used in mitigating the DDoS attack. The working of the EDoS Protection framework is explained with two scenarios, one with a legitimate user and another with an attacker accessing the service.

#### 3.3.1. Legitimate User

The legitimate user access the cloud services

The solution uses the public key cryptography. Here the solution is based on the trust. The trusted third party will provide certificates to all the layers such as hardware, virtual, user and network layers of the cloud architecture. Here the certificate based authentication is used .Each layer will use the other layer certificate for authentication.

1: The user request to access cloud service is first intercepted by the firewall
2: The firewall then redirects the request to the puzzle server which is an on demand cloud service
3: Puzzle server sends the client a puzzle to solve.
4: The user solves the puzzle and sends the result to the puzzle server
5: The puzzle server verifies the result if correct, sends positive acknowledgement to the firewall
6: The fire wall adds the client's IP to its white list
7: The firewall redirects the user to access the cloud services
8: The service is offered to client by the provider

#### 3.3.2. Attacker

Attacker access the cloud services
1: The attacker request to access the cloud services is first intercepted by the firewall.

2: The firewall then redirects the request to the puzzle server which is an on demand cloud service

3: Puzzle server sends the client a puzzle to solve.

4: The user solves the puzzle and sends the result to the puzzle server

5: The puzzle server verifies the result, if wrong, sends the negative acknowledgement to the firewall

6: The firewall adds the client's IP to its black list The packets identified as the attack can be dropped by the firewall. The requests fail to satisfy the puzzle can be considered as an attack .The source address of the attacker can be stored in the black list. Hence the future packets from the blacklisted IP can be dropped by the firewall.

### 4. EEDE Framework Evaluation

The experiment was conducted in the amazon EC2 cloud to demonstrate the EDoS. The Fig 6 gives the experimental setup. The high end instances such as the large and extra-large instances are used for creating the experimental setup. Four extra-large EC2 instances are clustered together using a load balancer to form a Server Cluster. The Web service applications are loaded in the Server Cluster. A group of four large EC2 instances are used as the AttackerNetwork, and a large instance is used as the legitimate user. To simulate the attack, HTTP requests to the web service are continuously given to the server cluster in a large scale.The experiment results were taken from the AWS monitoring system, and the incoming packets are monitored trough the packet capturing application wireshark. The number of HTTP requests and response are tracked. The SOAP messages are also tracked.

The average response time for each request to be processed by the server is also calculated. The graph drawn from the data obtained from the experiments shows the occurrence of Economic Denial of Sustainability for the DDoS Victim. When the numbers of attacks increase, the load balancer distributes the load to more instances, hence incurring cost for the extra instances.An increase in the attack, increases deployment of instances to meet the SLA and hence the cost also increases. Thus the traditional DDoS attack in the cloud can be transformed into an EDoS attack. The Fig 6 shows the cost escalation of the service for one day.

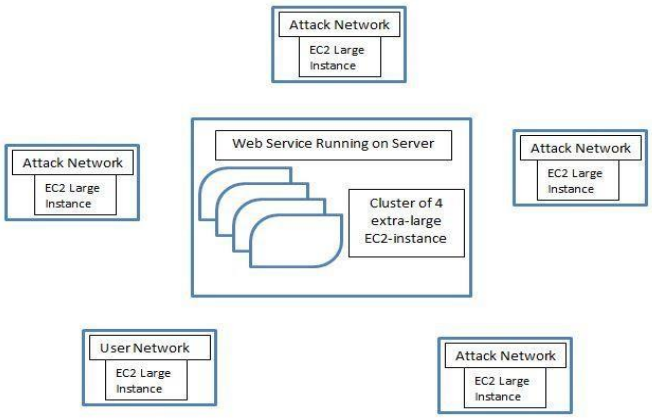


**Fig -6: Experiment Setup**

**Table -1: Comparison of existing with proposed systems**

| Comparison Item | Existing model | EEDE Framework |
|---|---|---|
| Detection of varietal attack | Not Detected | Detectable |
| Error rate | High | Low |
| The learning process of all site | Complex algorithm | Simple algorithm |

### 5. CONCLUSION

Cloud Computing provides a wide range of services. Existing Security mechanisms are not up to the mark .New approaches are needed which should be a distributed and scalable approach. New form of attacks is possible in the cloud. One such kind of attack is EDoS attack which is a new breed of DDoS attack. The EDoS attack exists only in the cloud so it can be termed as one of the cloud specific attack. A new security EDoS protection frame work is proposed. Also, an experiment is conducted to demonstrate the EDoS attack.The existing approaches are not capable of completely eliminating the EDoS attack. This method is possible to ensure the availability of the target system for accurate and reliable detection based on HTTP GET flooding. a method of integration between HTTP GET flooding among DDOS attacks and MapReduce processing for a fast attack detection in cloud computing environment. processing time of proposed method is shorter with increasing congestion. Future work needs the study of various pattern recognition for DDoS attack detection in cloud computing environment. Research is still needed to provide a better mechanism to protect the cloud from EDoS attack.

### REFERENCES

[1] Xue Jing, Jens Nimis, Zhang Jian-jun,"A Brief Survey on the Security Model of Cloud Computing" 2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science.

[2] Bernd Grobauer, Tobias Walloschek, and ElmarStöcker "Understanding Cloud Computing Vulnerabilities" Cloud Computing, Copublished By The IEEE Computer And Reliability Societies

[3] KrešimirPopović, ŽeljkoHocenski "Cloud computing security issues and challenges", MIPRO 2010, May 24- 28, 2010, Opatija, Croatia

[4] Paul Wooley ,Tyco Electronics ,"Identifying Cloud Computing Security Risks"University of Oregon ,Applied Information Management Program, Feb 2011

[5] V VenkateswaraRao , G. Suresh Kumar, Azam Khan, S SanthiPriya,"Threats and Remedies in Cloud"Journal of Current Computer Science and Technology, Vol. 1 Issue 4[2011]101-106

[6] A Survey on Cloud Computing Security,Challenges and Threats", Journal of Current Computer Science and Technology Vol. 1 Issue 4[2011]101-106

[7] Cloud Security Alliance,"Critical Areas of Focus in Cloud Computing" ,Prepared by the Cloud Security Alliance ,December 2009

[8] B. s. Sumit kar. An anomaly detection system for ddos attack in grid computing. International Journal of Computer Applications in Engineering, Technology and Sciences (IJ-CA-ETS), 1(2):553–557, AprilSeptember 2009.

[9]t. f. e. Wikipedia. Denial-of-service attack. http://en.wikipedia.org/wiki/Denial-of-service_ attack, 2013.

[10] T. Peng, C. Leckie, and K. Ramamohanarao. Survey of network-based defense mechanisms countering the dos and ddos problems. Journal of ACM Computing Surveys (CSUR), 39(1):1–42, April 2007.

[11] Y. seo Choi, I.-K. Kim, J.-T. Oh, and J.-S. Jang. Aigg threshold based http get flooding attack detection. In Proc. of The 13th International Workshop on Information Security Applications (WISA'12), Jeju Island, Korea, LNCS, volume 7690, pages 270–284. Springer-Verlag, August 2012.

[12]R. Ltd. DDoSPedia - HTTP Flood. http://security.radware.com/knowledge-center/DDoSPedia/ http-flood/, 2013.

[13] M. Zakarya and A. A. Khan. Cloud qos, high availability and service security issues with solutions. International Journal of Computer Science and Network Security (IJCSNS), 12(7):71–79, July 2012.

[14] R. N. C. Rajkumar Buyya, Rajiv Ranjan. Modeling and simulation of scalable cloud computing environments and the cloudsim toolkit: Challenges and opportunities. In Proc. of the 7th High Performance Computing and Simulation (HPCS'09), Leipzig, Germany, pages 1–11. IEEE, June 2009.

[15] R. Lammel. Google's mapreduce programming model — revisited. ¨ Science of Computer Programming, 70(1):1–30, January 2008.

[16] J. CHOI, C. CHOI, K. YIM, J. KIM, and P. KIM. Intelligent reconfigurable method of cloud computing resources for multimedia data delivery. Informatica, 24(3):381–394, 2013.

**BIOGRAPHY**

She received B.E(CSE) from Raja College of Engineering and Technology, Madurai, M.E(CCE) from Pavendar Bharathidasan College of Engineering and Technology, Trichy, M.B.A(ISM) form Bharathiyar University, Coimbatore and PGDB from Bharathiyar University, Coimbatore. She is currently working as Assistant Professor in department of CSE in Velammal College of Engineering and Technology, Madurai. She has published various papers in six different International journals and published papers at nine International conferences and sixteen National conferences.