A Layered Approach towards Securing Cloud against DDoS Attack

Neha Sharma
Department of Computer Science & Engineering
Lovely Professional University, Phagwara, India

Abstract- *Today cloud is the most attractive place for the researchers. Everyone is trying hard to make cloud as secure service so as to confirm to CIA triad. Among various issues the security issue is of the huge importance. This study focuses on the security aspects of cloud computing so the vendors of cloud can provide security guaranteed storage service. The study focuses on availability, confidentiality and authentication procedures. Availability factor is most frequently targeted in clouds. Cloud is vulnerable to DDoS attack, hence the availability of the services are reduced. This study stresses upon the encryption and managing encryption keys by using any famous algorithm or by designing an improved one. Managing cloud data is one of the major challenges in cloud. Most of the Organizations consider security as their primary need for any web service. All sensitive information must be properly located in cloud environment.*

Keywords: Cloud, Security, CTB, Layered Model, DDoS, Encryption

1. INTRODUCTION

1.1 Overview

Cloud is a challenging term now-a-days. Cloud has gained importance as a major computing platform. Today companies are moving from the physical servers to virtual cloud environment so as to have unlimited storage and easy accessibility of data for the users. Majority of the organizations are shifting to cloud for greater availability but the same cloud is daunting for many as it is prone to various threats. One of the most notorious and abusive threat is Distributed Denial of Service attack.

1.2 Types of Service Models

A cloud computing comprises of three different layers namely Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) as shown in Figure 1. Physical resources, bandwidth and storage are provided by IaaS layer. PaaS deals with providing the interface, the operating system or the platform to develop new applications. SaaS provides software and applications to the users.

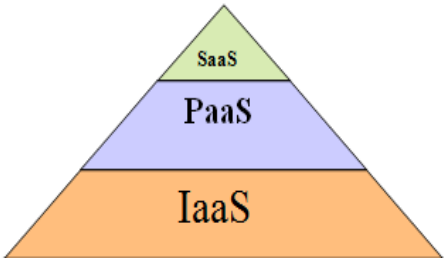

Figure 1 Services of Cloud Computing

1.3 Issues in cloud computing

Cloud computing is challenging as there are many security issues because users store their data on servers which do not have any fixed and known locations. Today the demands and concerns for confidentiality, availability and authentication are increasing day by day.

- **Availability**

  The most challenging task for cloud is to provide data when required as this availability can be or is usually targeted by the DDoS attack. Spamhaus.org faced the largest DDoS attack in March, 2013 with the estimation of 300 Gbps [1] while mitigation techniques were provided by CloudFare against this attack.

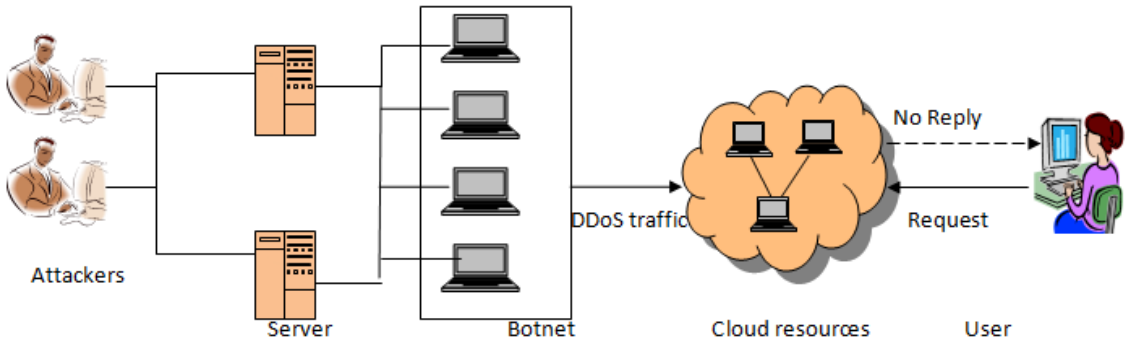

Figure 2 Scenario for DDoS attack in cloud

DDoS attack intakes resources, network bandwidth, processing space and makes server unavailable for some time. DDoS attacks are performed by the botnet as shown in Figure 2. But the previous researches have proved that intruder cannot compromise as many nodes he wants but only a few or thousands of bot commands can be there

- **Authentication**

  Authentication can be provided in passwords or login name or any kind of personal identification number (PIN). Another way can be authentication using message so that the source can be determined. One of the paper introduced Group Key Authentication [2]. It produces a composed group key which replaces the traditional authentication keys used till date. Multifactor Authentication [3] is also proposed by a paper which is an effective method to defend the cloud from unauthorized access. The basic model for this is shown in Figure 3.

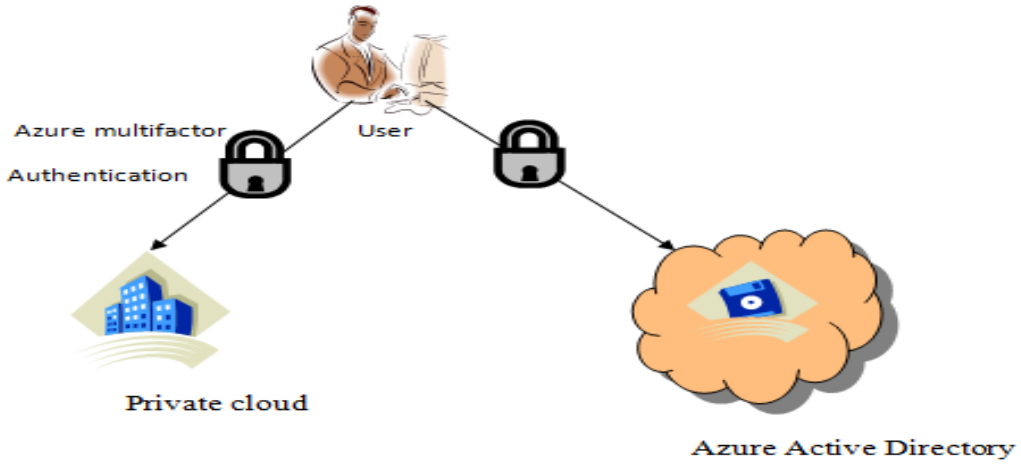

Figure 3 Authentication model to prevent unauthorized access

- **Confidentiality** is another issue in cloud computing which needs to be taken care of. To ensure data confidentiality, there is a need to change the way the distributed systems like cloud are designed. CSP needs to ensure that the data of the customers are not compromised and accessed by the unauthorized parties.
- **Integrity** is also one of the issues of cloud computing. Users need a promise that their data are secured and are not exposed to some changes by the intruders. Identity Management is proposed by [7] to ensure all these issues.

2. LITERATURE REVIEW

Cloud is a sensitive service which needs security at every moment.

2.1 Availability

Availability is targeted frequently by i.e. DDoS attack. Many types of Layer 3 DDoS are flooding the cloud and making resources unavailable to the users. These are discussed below.

2.1.1 Attacks

- **IP Spoofing Attack:** In this attack headers of the IP packet is changed and legitimate IP source address or fake IP address which is not reachable is forged and the packets are sent to that legitimate user by the server or will not be able to complete the transaction to the unreachable address [4] as shown in Figure 4. This will negatively affect the network resources and bandwidth. Hop count filtering (HCF) is used, which counts number of hops in between the source and destination which is dependent on TTL field in IP packet, IP to hop count routing or mapping is made which can be used to detect illegitimate packet.

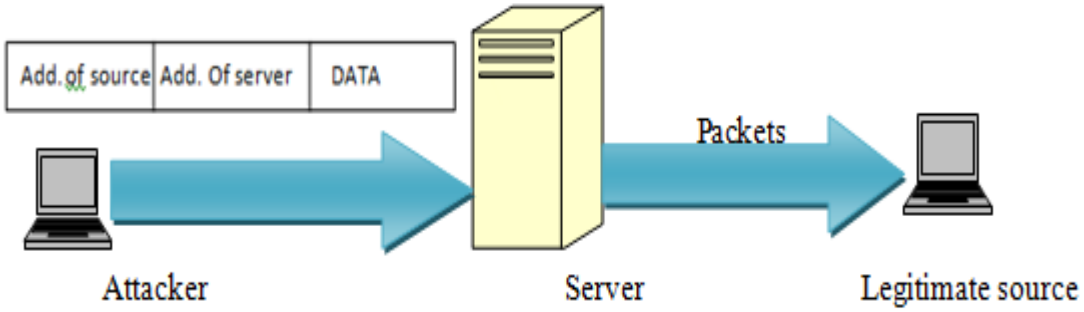

Figure 4 IP Spoofing Attack

- **Smurf Attack:** This type of attack deals with sending ICMP echo requests by forging source address in IP packet with the legitimate or victim's address and destination address with the broadcast address. Thus the packets will get flooded on victim's computer which will prevent the victim to access any of the resources as shown in Figure 5. Marwan Darwish has proposed in his paper [4] two methods to prevent this kind of situation. First is configuring the routers so that broadcast requests are denied.

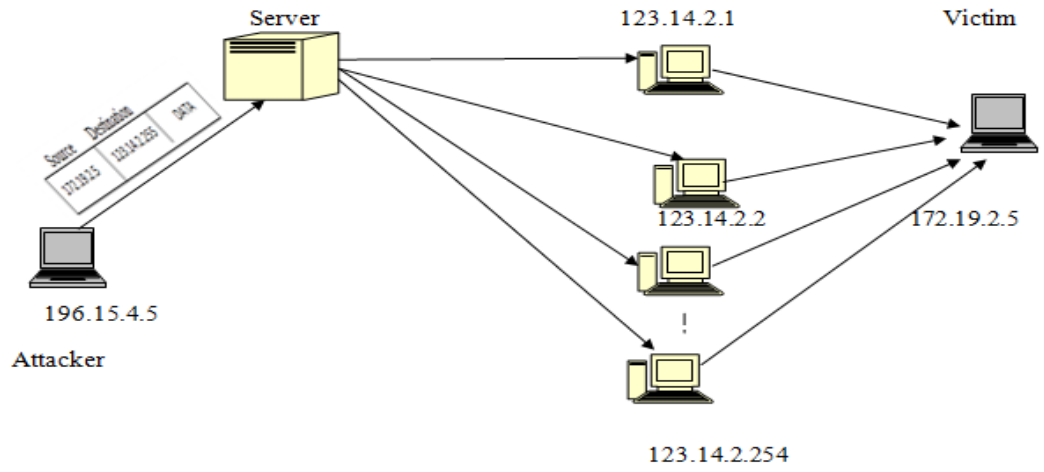

Figure 5 Smurf Attack

- **Buffer overflow attack:** In this attack, attacker attacks the victim's computer by sending a malicious executable code which once being hit in victim's computer can cause damage to it. Methods for escaping or preventing from such an attack [4] can be either perform some bounds checking of the arrays or estimate it during the run time.
- **Land Attack:** This kind of attack uses a land.c file and sends it to the victim's computer with the source and destination address as victim's address and hence request are sent to the victim by victim itself, hence crashing the system [4]. This has no effect on cloud now but can be developed in future. All the packets having same source and destination addresses are discarded thus protecting within all layers of cloud.
- **Teardrop attack:** In this, attacker sends teardrop.c file which overlaps the values of IP fragments in header [4]. This attack has also been prevented, so it cannot affect the resources in cloud.

- **DNS Reflection Attack:** In this attacker sends a request to DNS resolver with the source address as the victim's address [5]. DNS server sends the response in a large size as compared to the request to the source i.e. victim. Attacker can amplify the response size and can produce flood of traffic as shown in Figure 6.

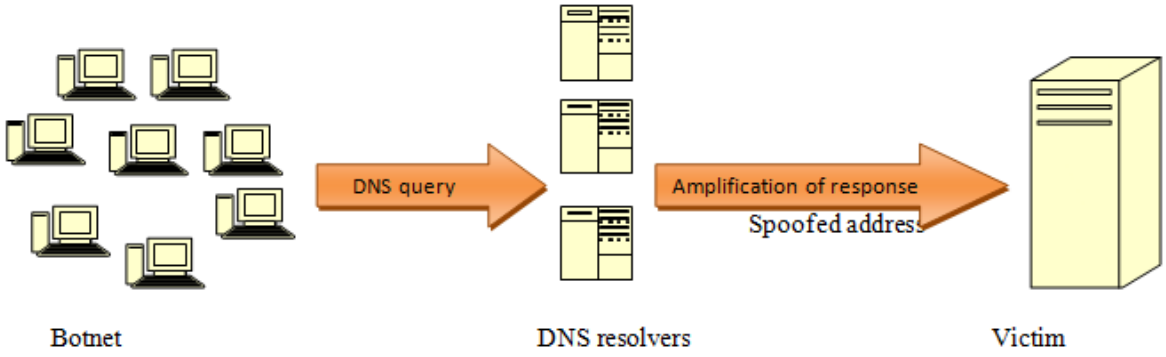

Figure 6 DNS Reflection Attack

2.2 Authentication

Independent of the application, when it runs on cloud it needs to know some of the information of its users prior to its use.

- Authentication may include login interfaces, key creation, firewall configuration, remote access and accessing multiple accounts [7].
- OTP can be used if high assurance is required for IDM (Identity Management) [7] and for low assurance usernames and passwords can be used.

Figure 7 shows the access of data over cloud which has many security issues. Data owner keep his data on cloud provided by cloud service provider which is in encrypted format. Whenever user requires data, he authenticates and access data. But authentication and key management between the data owner and CSP is difficult. So [8] provides a framework to ensure valid users have rights to access data.

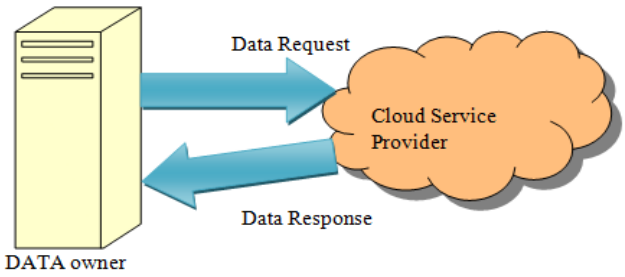

Figure 7 Data Access (Unsecure)

Today two-way authentication is being used to prevent forgery and attacks. Two-way authentication [8] involves user who is registered on cloud and is given a onetime password (OTP) to their numbers which they entered at the time of registration. This uses Diffie-Hellman Key Exchange Algorithm for key exchange and symmetric encryption for data encryption.

2.3 Confidentiality

Confidentiality can be obtained through encryption of data, third party authentication and access control. [10] proposed a three-tier Confidentiality Framework for securing cloud data. It gave three algorithms i.e.

- Algorithm for storing files
- Algorithm for downloading files
- Algorithm for TPA-integrity check

Algorithm for storing files

The paper proposed that when new user signs up, access is granted to the user by the admin. If the user wants to upload some data on cloud then the auto encryption method gets executed which uses Triple DES and MD5

Algorithm to download files

This algorithm provides user his files that are stored on cloud after getting authenticated. If he/she tries to access files that do not belong to him/her actually algorithm for TPA-integrity is executed. After getting the file, it is decrypted using the key mailed to the user.

Algorithm for TPA-integrity check

If an illegitimate user tries to access the files then binary format of the file is changed and thus this unauthorized access is informed to admin of the system with the information of previous attempts and illegitimate IP. Hence the illegitimate user is blocked.

It has showed results in favour of cloud and has improvement over the traditionally used techniques.

3. DDoS Mitigation Techniques with Cloud

Currently, several DDoS mitigation techniques are proposed by many researchers in recent years and are used by large and famous organizations like CloudFlare, Arbor, Cisco, and Akamai are discussed below:

- **Ingress Filtering:** It checks the IP of each outgoing packets that belong to a network and is written down in Best Common Practices. When the traffic is reflected, it is dropped with the help of this filtering [5].
- **HTTP Flood Attacks Mitigation:** HTTP protocol is used to generate HTTP flood attack at application layer. It is detected by Intrusion Detection System (IDS) or Web Application Firewall (WAF). It can also be detected by TCP connection counts which are required for HTTP responses at different layers.

  Five layers are there to detect this flood [5] as shown in Figure 8.

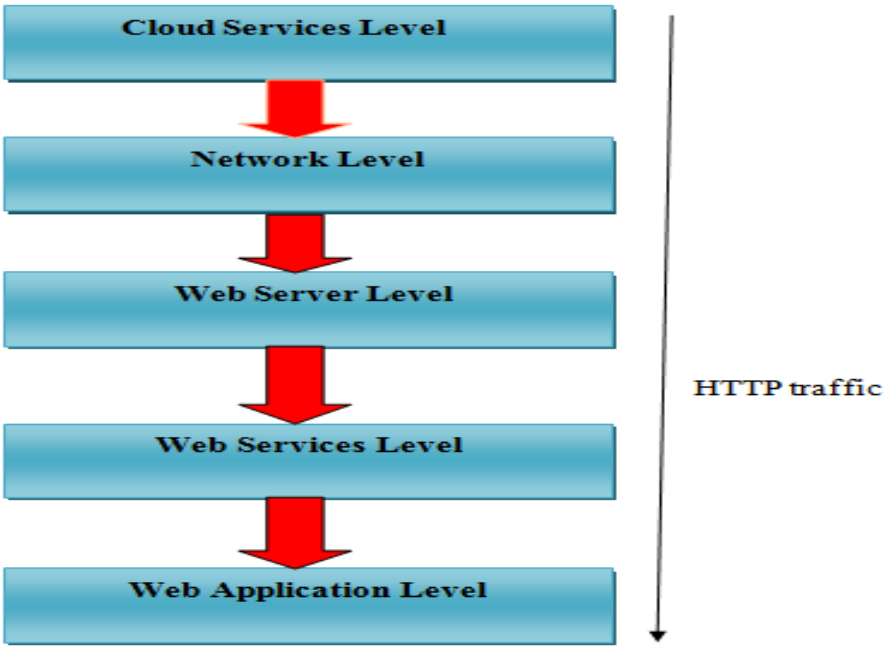

Figure 8 Levels of Mitigation of HTTP Flooding Attack

4. **Defence mechanism and models: Step towards mitigating DDoS Attacks**

In [6] the cloud is protected against DDoS attack with the help of Cloud trace back model. This model uses some mechanism which traces back the source of the attack. It checks the efficiency of the CTB (Cloud Trace Back model) by providing a fresh data set. It uses Flexible Deterministic Packet Marking (FDPM) rather than Deterministic Packet Marking (DPM). Cloud Trace Back model and Cloud Protector [6] are explained as below:

- **Cloud Trace Back Model:** CTB uses the concept of Deterministic Packet Marking which marks reserved flag and id of the packet. When the packet enters the network router, it is marked and it is not allowed to change in that network. [6] Proposed a new framework for CTB which uses FDPM and uses Cloud Trace Back Mark (CTM). The packet is marked with the CTM and CTB is placed before the web server so it is as close to the source as possible and it becomes easy to trace back the source. If no security is there at the edge servers, then the system is vulnerable to the attack. However this is protected by placing CTM in the CTB header as shown in Figure 9.

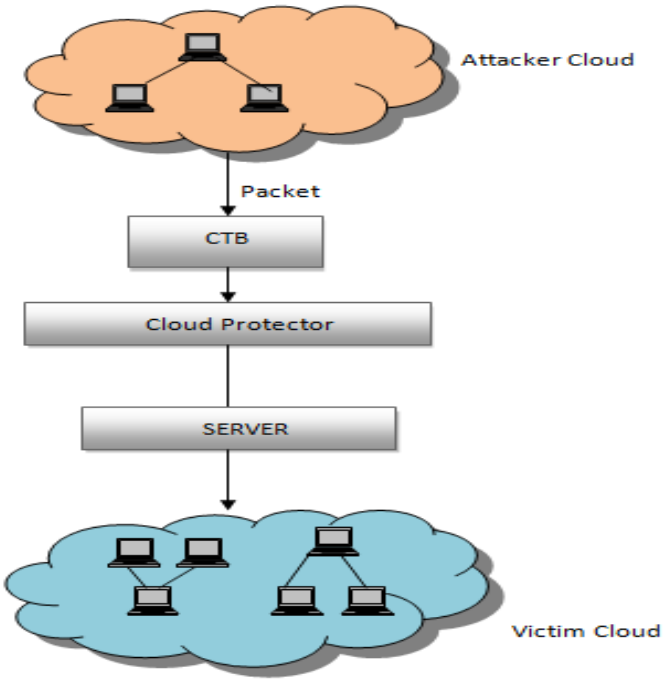

Figure 9 New Framework of CTB

The client will first request for the services from CTB and then places a SOAP request message. Upon receiving SOAP message CTB will place the CTM in the header. After that it will go to the server and if the attacker somehow wins to bring down the whole server then victim (spoofed IP address) will extract the mark and get the information of the source node. This reconstruction process will start filtering out the malicious traffic.

Cloud protector as shown in Figure 9 is a filtering system. CTB alone cannot detect DDoS attack. A trained back propagation neural network (NN) i.e. Cloud Protector, detects and filters the DDoS attack traffic. It uses a TLU (Threshold Logic Unit) which calculates the sum of the weights and checks if it greater than the threshold.

FDPM generation is shown in Figure 10.

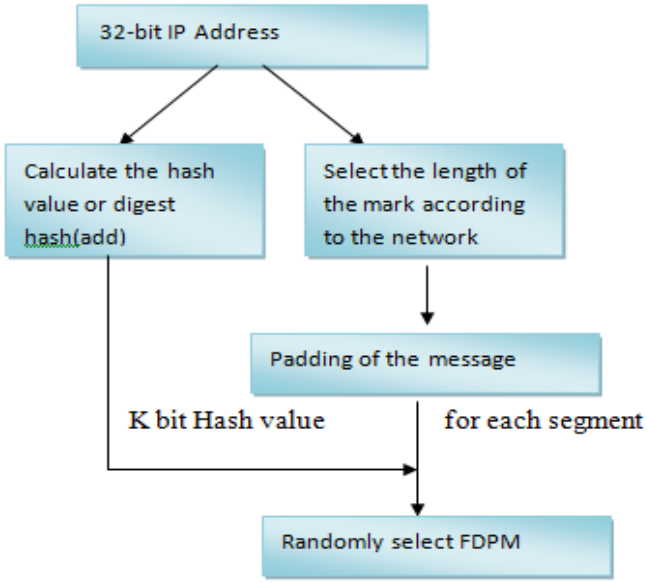

Figure 10 FDPM Generation Procedure

Cloud Filter proposed by [9] is used to filter most of the traffic and reduces the work of the victim so that he can concentrate more on the reconstruction of path. When there is no attack the server keeps in it the attributes <Cloud trace back mark, IP address> and when attack is encountered then it uses this attributes to filter the spoofed packets. It checks IP of the packet with IPs stored in the database at server.

5. PROPOSED WORK PLAN

This study deals with cloud and its security issues under various aspects. The study ensures that growing demand for cloud makes it feasible to propose a model that will confirm all the security factors required in cloud environment. Work plan can be described in context of security in cloud.

The paper will put light on the issues with authentication, confidentiality and availability. Then more existing models will be studied and be worked upon them to propose the specific problem definition. During the literature review more focus was put on the availability part and layered model for prevention from DDoS attack was proposed as shown in Figure 11. It can be explained as under.

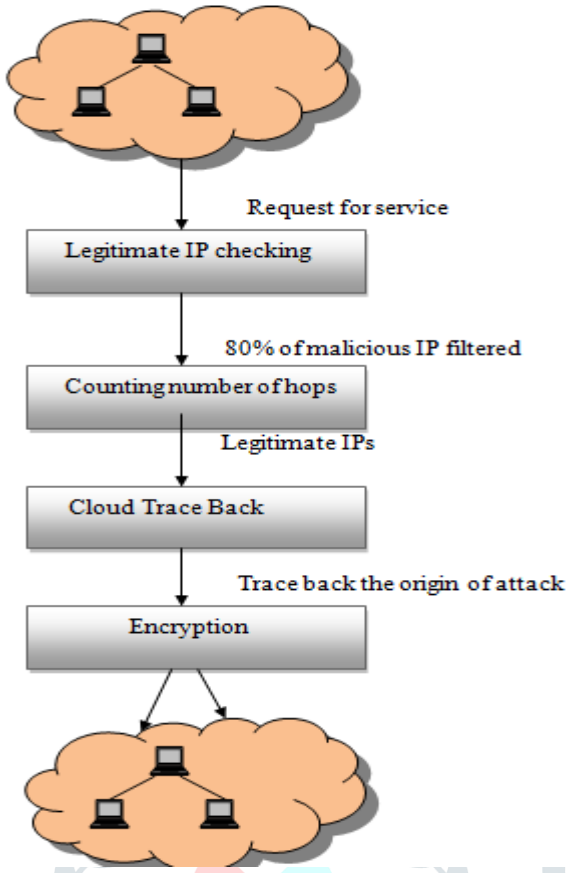

Figure 11 Proposed Layered Model for DDoS Mitigation

In this model different layers function as a technique which filter the false traffic and allow only legitimate IPs to pass through. This model has been proposed by considering in mind different techniques in different papers. Techniques are combined to provide a layered model to filter the illegitimate packets.

Still there is a need to do a lot of work regarding security. The work proposed is to promise confidentiality or authentication in clouds. Many IT industries and organizations are still reluctant to choose Cloud as their service just because of security. Thus one can realize that security matters. Without it not even a single network application is feasible or popular and is not used.

6. CONCLUSION AND FUTURE SCOPE

Cloud is the need of today's scenario as the demand for the users are getting more and more day by day. The more data user needs, the more is the issue of storing the data. Cloud has solved the problem. Besides the benefits of cloud, there are certain challenges that must be highlighted in order to account for flexibility. Consumers should trust but verify the service providers as ultimately at last consumer needs to provide security to his data on cloud. DDoS attack is the most prominent attack and this paper proposes a layered model to mitigate the attack thus keeping cloud secure. Future scope can include some more layers to enhance the security. Moreover, encryption procedure can be enhanced by advanced techniques.

RFERENCES

[1] M. Prince, (2013)"The Ddos That Knocked Spamhaus Offline(And How We Miotigated It)," in *Vol. 2013*,

Ed:CloudFare, P.Web Log Post.

[2] W. S. C. and K. Y. S. W. S. T. M.L. Chiang, (2011) "A New Group Key authentication Protocol in an Insecure Cloud Computing Environment," in *International Conference on Advanced Information Technologies*.

[3] P. H. Deepa Panse, (2014)"Multi-factor Authentication in Cloud Computimg for Data Storage Security," *Interational Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 8, p. 6.

[4] Marwan Darwish, Abdelkader Ouda, Luiz Fernando Capretz, (2013)"Cloud-Based DDoS Attacks and Defenses," in *IEEE*.

[5] FuiFui Wong, Cheng Xiang Tan, (2014) "A Survey Of Trends in Massive DDOS Attacks And Cloud-Based Mitigations," *International Journal of Network & Its Applications (IJNSA)*, vol. 6, no. 3.

[6] Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi, (2012)"Securing Cloud Computing Environment Against DDoS Attacks," in *International Conference on Computer Communication And Informatics(ICCCI-2012)*, Coimbatore,India.

[7] Safiriyu Eludiora, Olatunde Abiona,Ayodeji Oluwatope, Adeniran Oluwaranti, Clement Onime, Lawerence Kehinde, (2011), "A User Identity Management Protocol for Cloud Computing Paradigm," *International Journal of Communications, Networks and System sciences (IJCNS)*, no. 4, p. 8.

[8] D.H. Patil, Rakesh R. Bhavsar, Akshay, S. Thorve, (2012), "Data Security over Cloud," *International Journal of Computer applications*, p. 4.

[9] Lanjuan Yang, Tao Zhang, Jinyu Song, Jinshaung Wang, Ping Chen, (2012), "Defense of DDoS Attack for Cloud Computing," in *IEEE*.

[10] Gurjot Kaur, Naveen Kumari (2013) "Three tier Confidrkentiality Framework for Cloud Data Security and Integrity," *International Journal of Advanced Reasearch in Computer science and Software Engineering*, vol. 3, no. 9, pp. 339-343.

[11] Shui Yu, Yonghong Tian, Song Guo, Dapeng Oliver Wu, (2013) "Can We Beat DDoS Attacks in Clouds?," in *IEEE*.