iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XII **Month of publication:** December 2022

DOI: https://doi.org/10.22214/ijraset.2022.48374

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XII Dec 2022- Available at www.ijraset.com

A Study on DDOS Attacks, Danger and Its Prevention

Dhairya Patel
CSE Batch (2017-2021) Gujarat Technological University, Ahmedabad, Gujarat

Abstract: ***The present era is completely dependent on Internet which serves as a global information source for all users. Therefore the availability of internet is very important. Distributed denial-of-service is one kind of the most highlighted and most important attacks of today's cyber world. This paper mainly focuses on the DDoS attack which obstruct the network availability by overflowing the victim with high volume of illegal traffic usurping its bandwidth, overburdening it to prevent valid traffic to get through. We have also described the various types of DoS attack techniques that are inflicted upon the ISPs. The study of this research is to find out the various techniques to prevent these attacks along with their mitigation techniques and to find out any possible solution.***
Index Terms: Denial of Service, DDOS attack, overflowing attacks, mitigation techniques

I. INTRODUCTION

The Internet is defined as an interconnected system of computer networks. The scope of internet in day to day life is very vast. It provides a wide range of information, services, resources which allows all the sectors to be well linked As the need of internet is growing faster with time, various issues are related to its security. The reason for internet insecurity is basically concerned with its design because the foremost concern was its functionality rather than its security. Hence several types of attacks and threats are reason for apprehension towards security of internet.

The issues related to internet security are authentication, integrity, availability, confidentiality and non-repudiation. Among all the attacks DDoS (Distributed Denial of service) attacks are those which hinder clients, users to access all the advantages of services available to them from server side. The number of DoS and DDoS attacks on the Internet Service Providers has risen sharply in the last several years. Service providers are under tremendous pressure to prevent, monitor and mitigate DDoS attacks directed toward their customers and their infrastructure.

II. INTERNET SERVICE PROVIDER (ISP)

An Internet Service Provider (ISP) provides services for accessing and using the Internet. ISP providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.

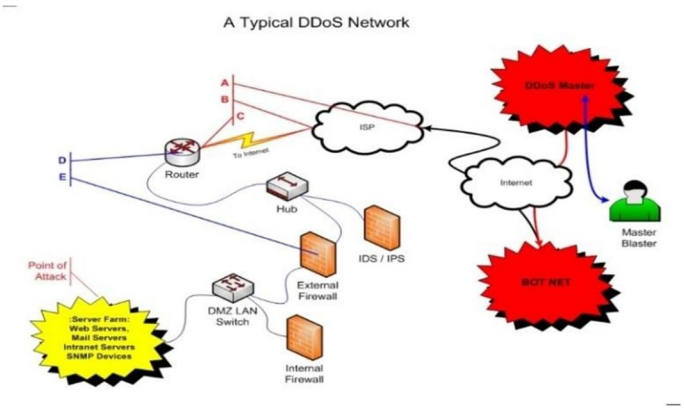
The services provided by ISP are as follows:

1) *Internet Access:* Internet access provided by ISP is the process that enables individuals and organizations to connect to the Internet by using computer terminals, computers, mobile devices, sometimes via computer networks so that the users can access Internet services, such as email and the World Wide Web.
2) *Internet Transit:* It is the service of allowing network traffic to cross or "transit" a computer network, usually used to connect a smaller ISP to the larger internet.
3) *Domain Name Registration:* A domain name is an identification string that defines a realm of administrative autonomy, authority or control within the Internet.
4) *Web Hosting:* It is a type of Internet hosting service that allows individuals and organizations to make their website so that it can be accessible via the World Wide Web.
5) *USENET Service:* It is a worldwide distributed discussion system which is available on the computers. It resembles a bulletin board system (BBS) and is the antecedent cursor to Internet forums that are widely used today.
6) *Co-location:* A co-location center is a type of data centre where equipment, space, and bandwidth are available for rental purpose to the retail customers.

III. DOS: A MAJOR THREAT TO THE ISPS

The impact of a successful DDoS attack on an ISP is widespread. Site performance is severely compromised, resulting in frustrated customers and other users. Service-level agreements (SLAs) are violated, resulting in costly service credits. The growing dependence on the Internet makes the impact of successful DDoS attacks. DDoS on ISPs results in the following:-

1) Lost revenue
2) Lost productivity
3) Increased IT expenses
4) Mitigation costs
5) Loss of customers



The figure given shows how DDoS attack is carried over on ISP.

a) *Point A:* This is the entry point of ISP
b) *Point B:* This is the exit point of ISP
c) *Point C:* This is the entry point to your network
d) *Point D & E:* This is the area where Anti DDoS or Firewalls or your IPS/IDS systems reside.

From the above diagram it is quite evident that DDoS may attack a single point in your infrastructure but the repercussions are felt from Point B Onwards and can be thwarted at Point B itself.

IV. UNDERSTANDING THE DDOS ATTACK

The interconnectivity among computers on which the World Wide Web relies, renders it an easy target for launch Denial-of-Service (DoS) attacks against them. A DoS attack is an attempt to make a machine or network resource unavailable to its future users, by indefinitely interrupting or suspending services of a host connected to the Internet. According to B. B. Gupta et. al (2008) CERT defines the term "Denial of Service" as "Occupancy of limited resource or difficult to renew such as network bandwidth, data structure or memory of a system".

When many hosts coordinate to flood the victim with an abundance of attack packets, and the attack takes place simultaneously from multiple points it is called a Distributed DoS (DDoS) attack. Another form of DoS attack known as DRDoS (Distributed Reflector DDos**).** A DRDoS attack is more damaging than a typical DDoS attack.

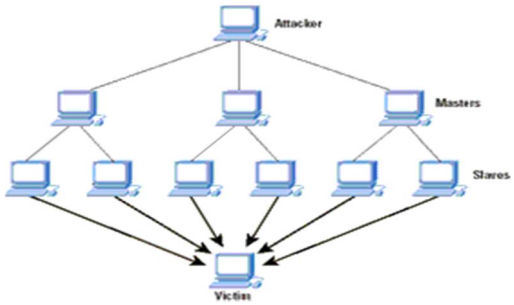


Fig: 2 DDoS Attack

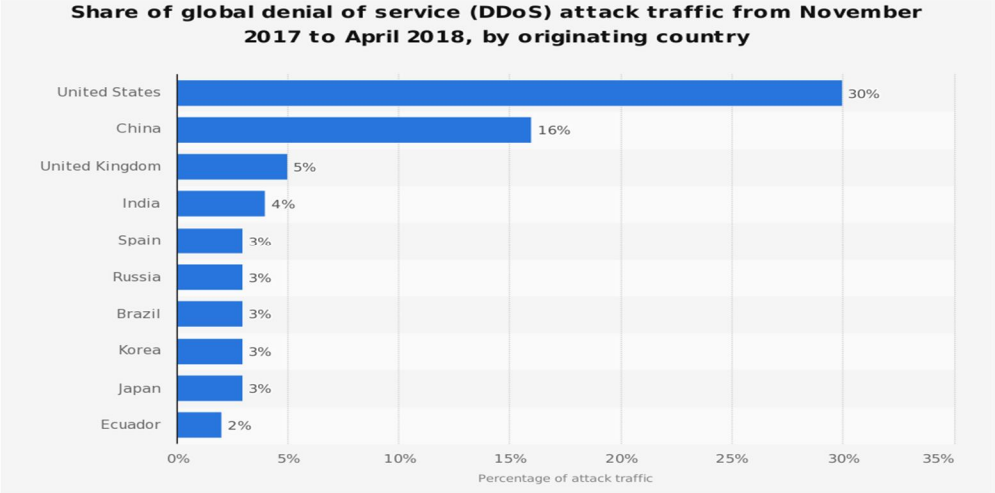


Fig: 3 Source Country for DDoS Attack
https://www.statista.com/statistics/440582/ddos-attack-traffic-by-originating-country/

From the Graph in Figure: 3 shows the percentage of worldwide DoS attack traffic between November 2017 and April 2018, sorted by originating countries. It is shown that during that period, 30% of DDoS attack traffic originated from the United States.

Countries	US	China	UK	India	Spain	Russia	Brazil	Korea	Japan	Ecuador
Total (100%)	30%	16%	5%	4%	3%	3%	3%	3%	3%	2%

Table: 1

A. Types of DDoS Attack

1) *Flooding:* Available bandwidth is one of the "goods" that attackers try to consume by flooding the network with useless packets.

2) *Protocol Violation Attacks:* It Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS etce. This type of attack consumes actual server resources, or intermediate communication equipment, such as firewalls and load balancers, and is measured in packets per second (Pps).

3) *CPU Power and Service:* By generating several thousands of useless processes on the victim's system, attackers managed to fully occupy memory and process tables. In this way the victim's computer breaks down. Attackers can try to occupy victims' services so that no one else can access them.

B. Based on Q2 2018 DDoS Trends Report: 52 Percent of Attacks Employed Multiple Attack Types

Following are the DDoS Trends and Observations:

1) 56% of DDoS attacks were UDP floods.

2) It is seen that TCP-based attacks were the second most common attack vector, making up 26% of attack types in the quarter.

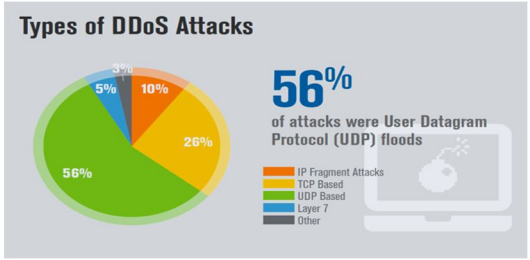


Fig : 4 Types of DDoS Attacks

3) 52 % of DDoS attacks curbed by Verisign in Q2 2018 employed multiple attack types.

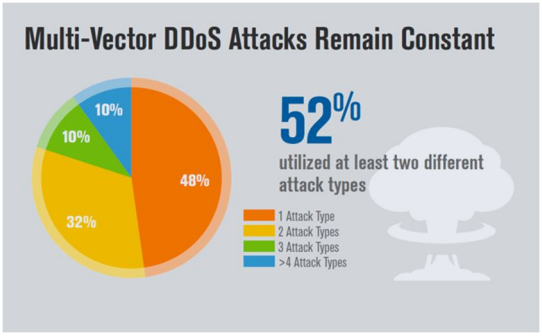


Fig: 5 Multi-Vector DDoS Attacks Remain Contant

4) 43% of mitigation activity of the Financial Services industry, represents the most frequently targeted industry for Q2 2018. The second highest number of DDoS attacks were acknowledged by the IT Services/Cloud/SaaS industry, representing 37% of mitigation activity, which is followed by the Media and Entertainment industry, representing 20 % of mitigation activity.

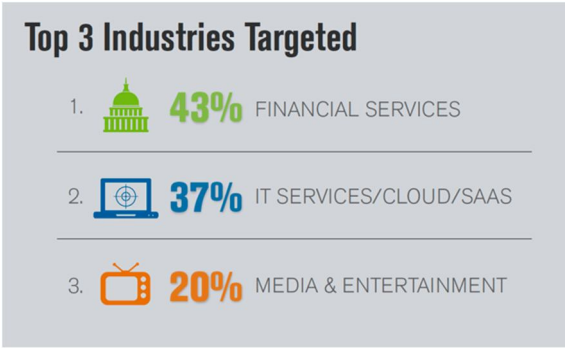


Fig: 6 Top 3 Industries Targeted

C. Popular DDoS Attack Trends on ISP Network

The major DDoS attacks on ISP network are the Network Infrastructure attacks. These have a serious impact on the overall operation of the ISP. These attacks can create regional or global network outages. These includes:-

1) *Control Plane Attacks:* Direct DDoS attacks against the routing protocols and lead to regional outages. Attacks are usually directed at dynamic routing protocols such as BGP, OSPF, and EIGRP

2) *Management Plane Attacks:* The management plane allows network operators the ability to configure the network elements. This includes protocols such as telnet, SSH, HTTP, HTTPS, SNMP, NTP etc.

3) *Network Services Attacks:* It aims the basic services provided by and needed by the ISP. DNS is a critical network service for operation of the ISP as well as a service provided by the ISP. As a public service, DNS in a service provider's environment is the most targeted service.

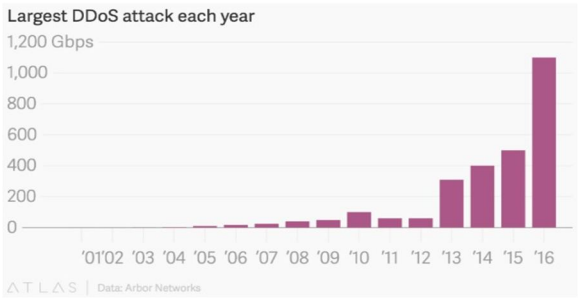


Fig: 7 DDoS Attack >100 Gbps

4) The following figure shows that there is 50% increase in the DDoS Attack between the year 2015-2016

V. DEFENSE CHALLENGES

In spite of the tremendous efforts by researchers and experts to address the denial of service, it still remains an unsolved problem. The various technical and non-technical challenges underlying the inability to mitigate these attacks includes:

A. Internet Architecture Related Challenges

1) *On-demand Resource Sharing:* Inter-user dependency is a fundamental factor that enables DoS to occur. The fundamental structure of the Internet is a packet switched communications facility which allocates link use on demand. The link capacity will be shared among the users. In such environment, a mischievous user can disrupt service for other users by occupying most of the shared resources.
2) *Decentralized Management:* Current Internet can be seen as interconnection of many Autonomous Systems (AS). Each AS has its own set of operating policy and security policy. The implementation of a global security policy or mechanisms is enormously difficult, which makes solutions that require cross-domain cooperation unattractive.
3) *Accountability:* Accountability ensures that the actions of an entity may be uniquely traced back to that entity. The indifference to accountability issue is now difficult to ignore.
4) *Variation in link Capacity:* The provisioning of link bandwidth in modern Internet varies significantly from core networks to edge network *(Bush and Meyer 2002)*. Traffic from the high-bandwidth core link can overwhelm the low-bandwidth edge link.

B. Miscellaneous Challenges

1) *Difficulty of Distinguishing Malicious Requests:* It is difficult to distinguish between malicious requests and legitimate ones.
2) *Asymmetry of Request and Response Overhead:* Asymmetry of request and response overhead refers to the asymmetry in the amount of consumed resources for generating a request at the client and creating response at the server. In most cases, a client spends trivial amount of CPU and memory resources to generate a requests, and the operations carried out by the server to produce the corresponding response incurs significantly more resource overhead in comparison.
3) *Research Challenges:* Very limited information about DoS incidents are publicly available due to organizations' unwillingness to disclose the occurrence of an attack, for fear of damaging the business reputation of the victim. It becomes very difficult to compare the performance of various solutions. Moreover, the testing of DoS solutions in a realistic environment is immensely challenging, due to the lack of large-scale test beds or detailed and realistic simulation tools.
4) *Lack of core Competency:* ISP's are in the business of selling bandwidth and don't always invest in the required capital and resources to stay ahead of the latest DDoS threats. According to some ISPs lack of ROI (Return of Investments) is a major discouraging factor.

VI. DEFENCE MECHANISMS

DDoS attacks have become more sophisticated in the last several years as the level of attack automation has increased. Organizations are now increasingly targeted by application-layer DDoS attacks. Fully functional attack software and ready to use programs is readily available on the Internet allowing novice users to launch large scale attacks with little knowledge.

1) *Monitoring:* Developed by Cisco monitoring traffic patterns and DoS/DDoS attacks is a very popular tool used by ISPs. A flow is defined as having some unique attributes like sourceIP, Destination IP, Source port, Destination port etc. To monitor traffic in both directions all router interfaces must be monitored, including uplinks to the core routers.
2) *Ingress/Egress Filtering:* The purpose of ingress/egress filtering is to allow traffic to enter or leave the network only if its source addresses are within the expected IP address range.
3) *Drawback:* It is difficult to deploy ingress /egress filtering universally. If the attacker carefully chooses a network without ingress/egress filtering to launched spoofed dos attack, the attack can go undetected. Hence ingress/egress filtering are ineffective to stop DDoS attack. The possibility of multi-path routing diminishes routers' ability to determine spoofed source, since a router may receive an unexpected packet due to route changes [Clark 1988].
4) *Black Holing:* ISP's use RTBH (remotely triggered blackholing), by which they can ask their upstream networks to discard the traffic, so it won't even reach the destination network.
5) *Drawback:* The biggest the target IP address (and thus the services running on it) is put offline exactly what the attackers want.
6) *Scrubbing:* The scrubbing centre has equipment to filter unwanted traffic, leaving a stream of (mostly) clean traffic which gets routed back to the ISP. Drawback: Most scrubbing centers are commercial, and can cost quite a lot. Also, scrubbing is not always easy.

VII. PROPOSED SOLUTION AND METHODOLOGY

Based on our findings recommended some measures to local ISPs to strengthen security against DDoS attack in an economical manner. These include:

1) Every single user who accesses your router should be given a username and password.
2) Make sure you have RPF (ingress and egress filtering) on the interface of every static connection.
3) Disable Telnet on vtys and allow only SSH based connections.
4) Use Vtys filters to prevent public routers from getting response from your router.
5) Use TACACS (Terminal Access Controller Access Control System) for password verification.
6) Set up security labs if not possible set aside at least one spare router and server to try a new service instead of implementing it directly on live network.
7) Minimizing the number of transit providers possibly one
8) Team up with other local ISPs for benefits like leasing a scrubbing centre, out of band management and possibly setting up better security labs.

VIII. CONCLUSION

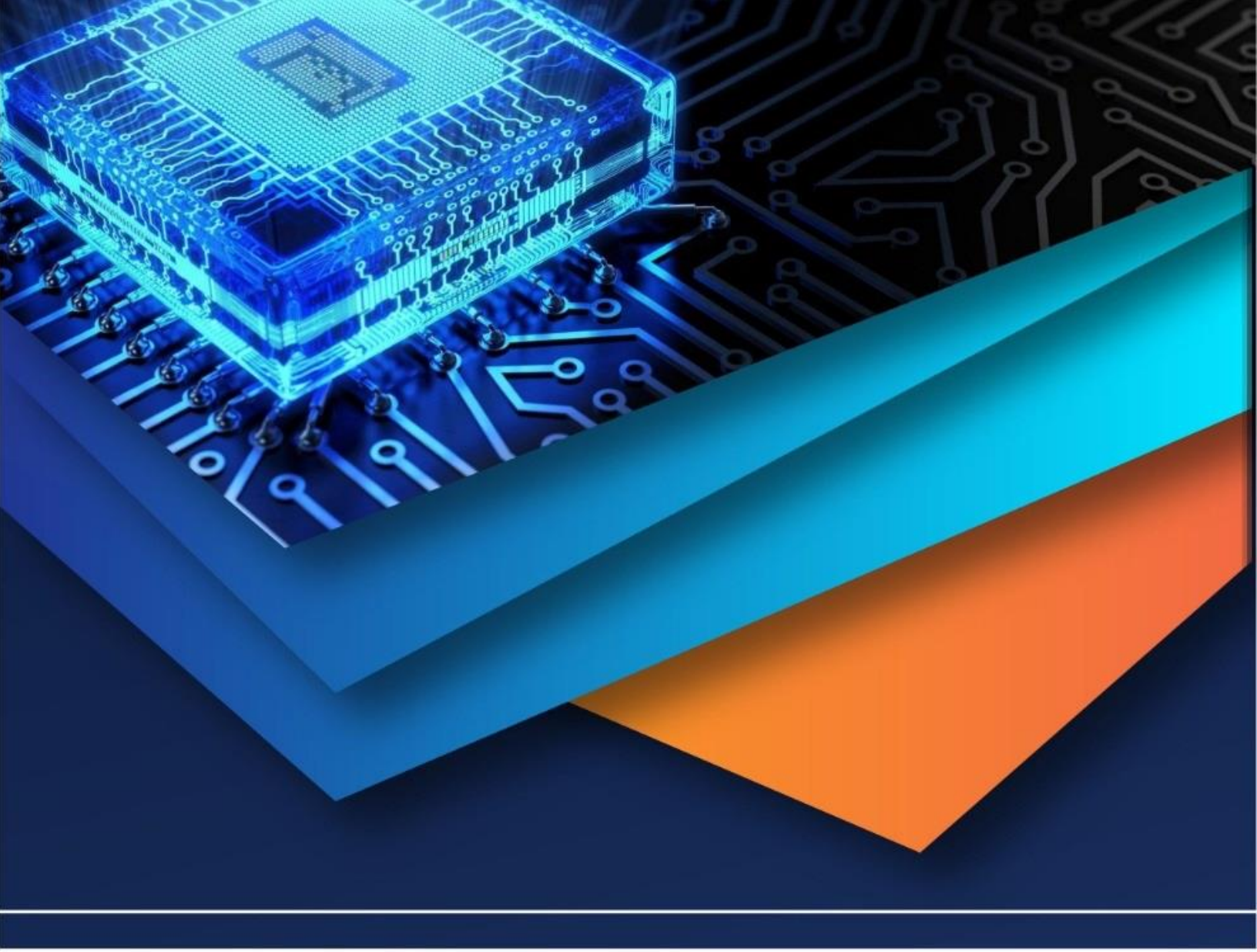
DDoS is becoming a major component of a long term threat campaign and the level of attack automation has escalated. Several efforts are being taken by ISPs to combat it but they are still not able to overcome the problem completely, instead they are likely to pose a bigger danger in future. Several weaknesses like the distributed and non-uniform architecture of the Internet infrastructure, business policies, privacy policies and return on investment has lowered the interest of ISPs in eradicating DDoS completely. Instead DDoS protection is itself growing as a new market. Under such circumstances it seems impossible to completely eradicate DDoS from society. By following the recommendations given in paper local ISPs will be able to cope with DDoS attacks more effectively.

IX. FUTURE SCOPE

While all tiers of network providers are taking individual precautions there is a need of unification of the efforts. Distributed nature of the DDoS attacks can be mitigated by a united effort where the local ISPs provide DDoS protection to Customers while Connection Providers (Transit Providers) avail DDoS protection to local ISPs. This hierarchical defence structure will cover security loopholes at all levels and will successfully give DDoSers a hard time.

REFERENCES & WEBLINKS

[1] https://journals.sagepub.com/doi/full/10.1177/1550147717741463
[2] International journal of Distributed Sensor Network
[3] https://blog.eccouncil.org/types-of-ddos-attacks-and-their-prevention-and-mitigation-strategy/
[4] http://users.eecs.northwestern.edu/~khh575/pub/pub/Report-DDoS-1.pdf
[5] International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013 https://www.researchgate.net/publication/258790077_DDoS_Attack_Prevention_and_Mitigation_Techniques_-_A_Review



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY