**IJCTA,** 9(22), 2016, pp. 67-74


# Performance Analysis of Web Services Under HTTP Attack Using GENI Testbed

**Ajitpal Kaur* Daljeet Kaur** Krishan Kumar*** SunnyBehal******

***Abstract :*** Internet has gained popularity at amazing rate in order to share the ideas between people and have reduced the communication barriers among people. Regrettably, the usage of Internet has bring sharp rise of DDoS attacks. DDoS attacks are getting more sophisticated and intense every year. A number of techniques are proposed in literature to combat DDoS attacks but they are very hard to detect. It is very difficult to distinguish legitimate user traffic from attack traffic which spread across so many points of origin. In this paper, we have measure the performance of DDoS attacks on HTTP service. Global Environment for Network Innovations (GENI) tesbed is used to generate legitimate and attack traffic. The DDoS attack is launched at varying strengths and impact is measured in terms of metrics such as, Throughput (Goodput, Badput), Average Response time and Round Trip time metrics.

***Keywords :*** DDoS, GENI, Metrics, Measurement.

## 1. INTRODUCTION

The Internet is a global system of interconnecting computer networks that use the inter protocol suite (TCP/IP) to link several billion devices worldwide. It is a Network of Networks that consists of millions of private, public, academic, business and government networks of a local to global scope, linked by a broad array of electronic, wireless and optical networking technologies [20].

When you are using internet Resources, hardware and software, components are the target of malicious attempts to gain unauthorized control to cause interruptions or access private information. A computer user can be tricked into downloading software onto a computer that is of malicious intent. Such as software comes in many forms, such as viruses, Trojan horses, spyware and worms. There are various attacks on the internet resources such as: Passive attacks, Active attacks, and Distributed attacks.

In GENI platform the experimenters perform own works on the DDoS (Distributed Denial of service) attacks. Distributed Denial of Service (DDoS) is defined as an attack in which multiple compromised and vulnerable systems are used to attack a single target or victim machine to make the service unavailable to the intended users. DDoS attacks are launched from botnets large clusters of connected devices (*e.g.*, cellphones, PCs or routers) infected with malware that allows remote control by attackers. DDoS attacks are amplified from of DDoS attacks where attackers direct hundreds or even thousands of compromised hosts called zombies against a single target. The widely used World Wide Web environment is also prone to DDoS attacks. This has been demonstrated by the large number of exploits against web services, browsers and application. Traditionally, DDoS attacks are carried

* Department of Computer and Science Engineering SBS State Technical Campus, Ferozepur, Punjab, India Email- jeetpal.ajitAK@gmail.com

** Department of Computer and Science Engineering SBS State Technical Campus, Ferozepur, Punjab, India Email- daljeetkaur617@gmail.com

*** Department of Computer and Science Engineering SBS State Technical Campus, Ferozepur, Punjab, India Email- k.salujasbs@rediffmail.com

**** Department of Computer and Science Engineering SBS State Technical Campus, Ferozepur, Punjab, India Email-sunnybehal@rediffmail.com

out at the network layer, such as ICMP flooding, SYN flooding, and UDP flooding, which are called Flooding DDoS attacks [9]. The intent of these attacks is to consume the network bandwidth and deny service to legitimate users of the victim systems. Since many studies have noticed this type of attack and have proposed different schemes (*e.g.*, network measure) to protect the network and equipment from bandwidth attacks, it is not as easy as in the past for attackers to launch the DDoS attacks based on network layer [17]. When the simple flooding-DDoS attacks fail, attackers shift their offensive strategies to application-layer attacks and establish a more sophisticated type of DDoS attacks [7]. To circumvent detection, they attack the victim Web servers by HTTP GET requests (*e.g.*, HTTP Flooding) and pulling large image files from the victim server in overwhelming numbers [6]. In another instance, attackers run a massive number of queries through the victim search engine or database query to bring the server down. We call such attacks application-layer DDoS attacks.The goal of DDoS attacks to overloads the server with unwanted traffic and Second goal is to acquire the bandwidth by generating the large volume of unwanted traffic[13].As shown in figure1.

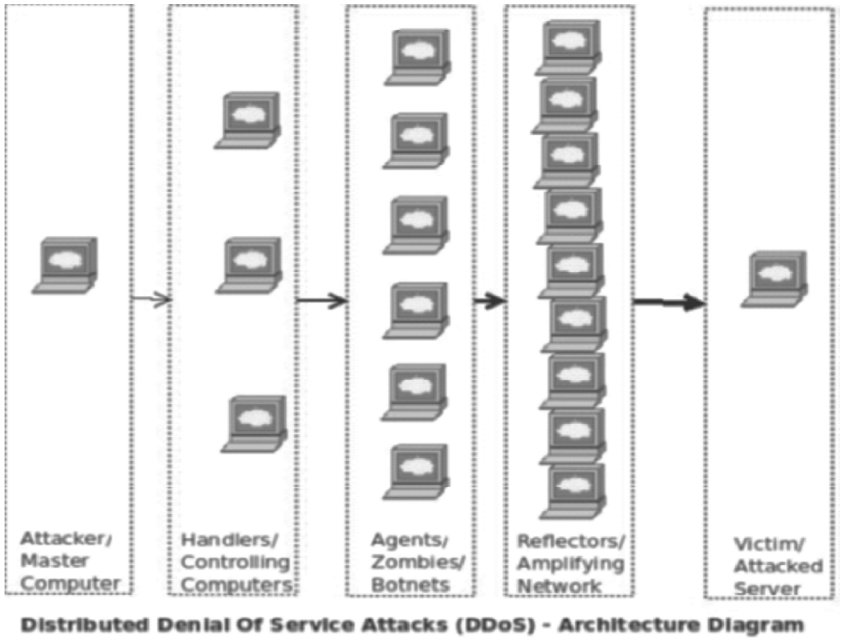


**Fig. 1. Architecture of DDoS Attacks.**

In order to devise a comprehensive DDoS solution, there is need to study and measure the performance of DDoS attack against web server. In this paper we measure the performance of DDoS attacks in various attack scenarios in term of following metrics: Throughput, Response time and Round trip time [19].

In this paper, we have investigated various Network Research Validation Techniques like Simulation, Emulation and Real-Time Experiments used for the validation of various DDoS detection methods. Out of these Validation Techniques, GENI is extremely used in Network Related Research based on real time experiments [1].

## GENI TESBED

The GENI (Global Environment for Networking Innovation) is a suit of research infrastructure rapidly taking shape in prototype from across the United States. It is sponsored by the national science foundation, with the goal of providing a laboratory environment for networking and distributed systems research and education [3].

## GENI AND ITS ARCHITECTURE

GENI is a new network testbed, nationwide suite of infrastructure supporting research in networking, distributed systems, security and novel application. Global Environment For Network Innovation is a distributed virtual laboratory sponsored by the U.S NSF (National Science Foundation) and available without charge for research and classroom use. It is well suited for exploring networks at large scale, thereby promoting innovation in network science and services [5]. GENI allows experimenters to:

1. Obtain compute resources from location around the United States.
2. Connect resources using Layer 2 topologies in network best suited to their experiments.
3. Install custom operating systems and software on these compute resources.
4. Control network switches in their experiment handle traffic flows.
5. Run layer 3 and above protocols by installing protocols software in their compute resources and providing flow controllers for their switches. As shown in figure 2[5].


**Fig.2. Resource available to GENI experiments includes GENI Racks, regional and national backbone networks and WIMAX base station.**

**Use of GENI**

**GENI might be right for you if your experiment requires.**

1. GENI has large scale experiment infrastructure. GENI can potentially provide you more resources than is typically found in any one laboratory. GENI gives you access to hundreds of widely distributed resources such as virtual machine and bare machines and network resources such as link switches and Wimax base stations.
2. GENI has Non-IP connectivity across resources. GENI allows you to set up layer 2 connection between resources and run own layer 3.
3. In GENI has Deep programmability. With GENI you can program not only the end hosts of your experimental network but also the switches in core of your Network.
4. You can get exclusive access to certain GENI resources including CPU resources and network resources by using Reproducibility.
5. GENI has two instrumentation and measurement systems that you can use to instrument your experiments. These provide active and passive measurements, data storage and tools for visualizing and analyzing measurement data [21].

**GENI Key Concepts**

GENI key concepts introduces various terms you will need to know before you use GENI.GENI experimenter workflow that ties together these concepts and terms.

1. **GENI Project :** In GENI a project organizes research both people and their experiments. GENI provide a portal for an individual's researcher. The project is created by a single responsible individual. The individual lead the project. Projects have many experimenters as its members and experimenter may be a member of various projects. In GENI has provided a unique account for the researcher. The researcher

must have project leader and privileges to create projects but only any senior Professor of any organization can leads only. For examples: Students cannot be project leads.

2. **Slice :** GENI is a shared testbed in which multiple experimenters may be running multiple experiments at the same time. A slice is a container in which you perform multiple experiments such as make topologies. The project head is automatically member of the slice. The experimenter only uses those resources they will provide by GPO (GENI project office). GENI use the concept of slicsebility from the planetlab testbed. GENI supports multiple models of visualization even for a single resource type.
3. **GENI Aggregates :** The Global Environment for Networking Innovation has provided aggregates resources to GENI experimenters. In which Experimenters may request to the resources from this GPO aggregate and then add to slice. GENI has multiple aggregates. Each aggregate provides its own resources. Some aggregates provide Virtual Machines or bare machines for compute resources and some provide networking resources that experimenters can used to compute resources. There are multiple aggregates in GENI [2]. As shown in Figure 3[5].


**Fig 3. GENI Aggregates.**

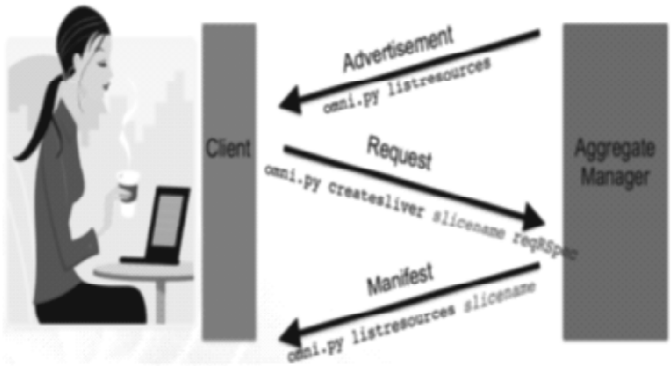


**Fig 4. GENI RSpec and AM API.**

4. **GENI RSpecs and GENI AM API :** GENI RSpecs is Resource specification document that is used to request the resources from aggreates and AM API is Aggregate Manger that provides the available aggregates to the experimenter [10]. As shown in figure 4[1].

## 2. RELATED WORK

DDoS attack's impact metrics are closely related with measuring the effectiveness of DDoS defense approaches. At present, there are no benchmarks in terms of effective metrics for evaluating DDoS attack impact and defense strategies [16]. Most of the researchers measure the Performance of a DDoS attack on network traffic. Most of existing strategies measure the impact metrics with attack and without attack scenarios. Daljeet et.al [8] designed a dumb-bell topology and generated FTP traffic and measures the various performance metrics. Kaur et.al [14] characterize and compare the popular DDoS attack tools used by the attackers in recent times, their modus operandi and types of attacks, they launch. Sachdeva et.al [18] measure the impacts of DDoS attacks using DETER testbed. Behal et.al [4] compare the various validation techniques used for network based experiments. They propose a new paradigm of real datasets and gives direction to the researcher community to use real experiments for better results.

In this paper, we have explored a new real experimentation testbed named as GENI which is based on using the real systems for the network based experiments. We have used this testbed to generate HTTP DDoS attacks and their impact on web server is measured in terms of various performance metrics.

## 3. PERFORMANE METRICS

In the internet growing number of DDoS attacks that bring down the internet sites worldwide continually. DDoS attacks goal is to make an entire website unavailable to its regular visitors or customers. A few minutes of downtime can be expensive for all users [15]. DDoS attacks cripple websites, interrupt business operations,

interfere with customer support, and inflict brand damage the targeted organizations. The DDoS attacks study surveyed 450 companies in North America across multiple sectors, including financial services, technology, retail, government/public sector, health care, energy, telecommunications, e-commerce, Internet services and media industries. When DDoS attacks are launched, the various performance metrics are affected. In recent work, our focus is on measuring these performance metrics and comparing them without and with attacks [12].

### 3.1. Throughput (α)

Throughput can be classified as the volume or amount of data or traffic that can flow through a network at a given time. Throughput can be used to measure network efficiency and performance in the sense that a low throughput offers low network performance and vice versa. Throughput is measured in terms of good-put and bad-put respectively. Good-put is defined as no. of bytes per second of legitimate traffic that are received at the server and bad-put is defined as no. of bytes per second of attack traffic that are received at the server.

$\alpha = (bl + ba)/\Delta$, *bl*, *ba* and Δ represents no. of legitimate bytes, no. of attack bytes and time window for analysis respectively

### 3.2 Response Time (α)

Response time is a measure of the amount of time required for a packets to travel across a network path from a sender to a receiver.

$$\alpha = tc + td + ts$$

For example, The time taken for a packet to travel from client to server (*tc*) + server delay (*td*) + Time required for packet to reach to client from server(*ts*).

### 3.3. Round Trip Time (RTT) (μ)

Round-trip time (RTT) is the time required for a signal pulse or packets to travel from a specific source to a specific destination and back again.

$$\mu = x + y$$

*x* is time to travel from source to destination and *y* is time to travel from destination back to source

**Table 1. All performance metrics are show in**

| ***Metric*** | ***Description*** |
|---|---|
| Throughput α | Vα = (*bl* + *ba*)/Δ, *bl*,*ba* and represents no. of legitimate bytes, no. of attack bytes and time window for analysis respectively. |
| Response Time β | β = *tc* + *td* + *ts*, the timetaken for a packet to travel from client to server (*tc*) + server delay (*td*) + Time required for packet to reach to client from server(*ts*). |
| Round Trip Time μ | μ = X + Y, X is time to travel fromsource to destination and Y is time to travel from destination back to source |

All the metrics are measured with and without attacks. The experiments are conducted in GENI Desktop tool that is a performing Experiment tool.

## 4. EXPERIMENTAL SETUP

We have used GENI testbed to evaluate our metrics in experiments using with GENI Desktop. The GENI Desktop is a tool that supports multiple ways to visualize a slice, and makes it easy to apply an operation to a subset of resources within a slice [11]. GENI Desktop supports extensible functionality we called Modules that perform commonly used operations like ssh, Downloads Log and Pcap files, Upload software's, running a command, rebooting nodes etc. GENI Desktop is familiarity with the Unix Command line.

### 4.1. Experimental Topology

To show the experimental topology in Fig. 5 and in which the Node-0 is a server and Node-1 to Node-6 is clients. These clients are used to send legitimate traffic to server (node-0). The attacks nodes are Node-7 to Node 10 that sends attack traffic to server. In which add a global node that is an extra node (VM) that is automatically added to your slice when you select the GENI Desktop tool. The purpose of the Global node is to the collect point for all instrumentation and measurement data collected by the slivers. As shown in figure 5.

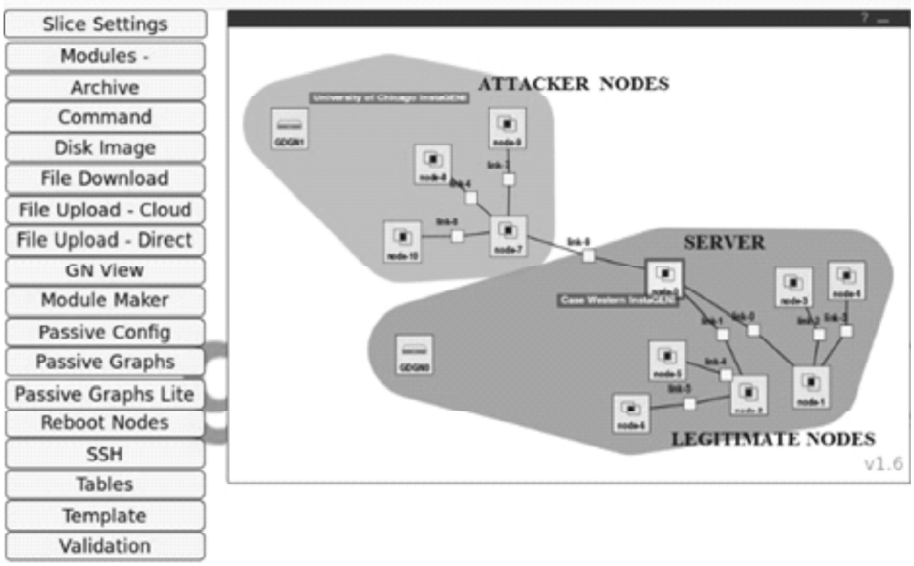


**Fig. 5. Experimental Topology.**

### 4.2. Legitimate Traffic

We have used HTTP traffic in our experiment and the legitimate nodes send the legitimate traffic to the server for 240 secs.

### 4.3. Attack Traffic

We have used to generate the HTTP attacks. In our experiment we are launches two time attacks. In first attack we are used only one node and in second attack we are used two nodes. The starts and stop time is same both of attacks traffic to the server for 80th sec to 160th sec. So, Then we measure the performance of DDoS attacks on HTTP service.

During Perform experiments we are using various tools as shown in Table 2.

**Table 2. Tools used in experiments**

| ***Metric*** | ***Description*** |
|---|---|
| GENI Desktop | This tool is used for performing Experiment |
| HTTperf | This is used for launching Legitimate traffic to the server |
| GoldenEye | This is used for generating Attack traffic to the server |
| Tcpdump | This is a package analyzer toolwhich is used to capture or filter packets. |

## 5. RESULTS AND DISCUSSION

### 5.1 Throughput

Throughput is the amount of data moved successfully from source to destination at the given period of time. In Fig. 6 and Fig. 7, we have measured throughput in term of goodput and badput. Good-put is defined as no. of bytes per second of legitimate traffic that are received at the server and bad-put is defined as no. of bytes per second of attack traffic that are received at the server.

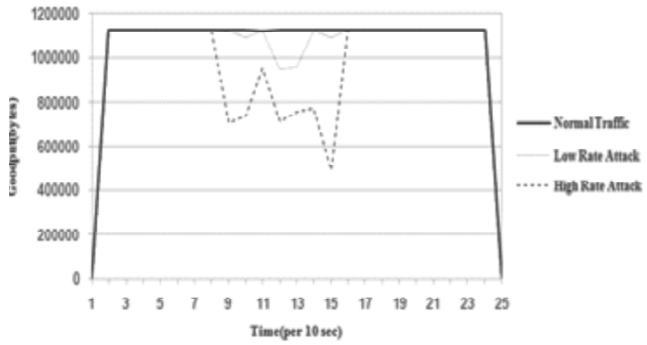


**Fig. 6. Variation of Goodput.**

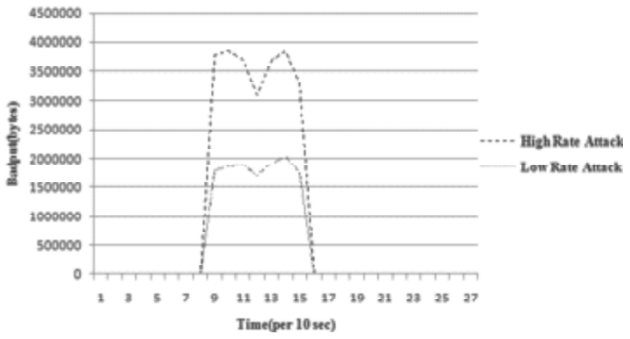


**Fig. 7. Variation of Badput.**

## 5.2. Response Time

The very important metric to be measure in an attack would be server response time. The server performance is changing during the attack and could be measured by using commands. when the attack is launched at that time, response time start to increasing. We have showed the response time with and without attack in Fig. 8.

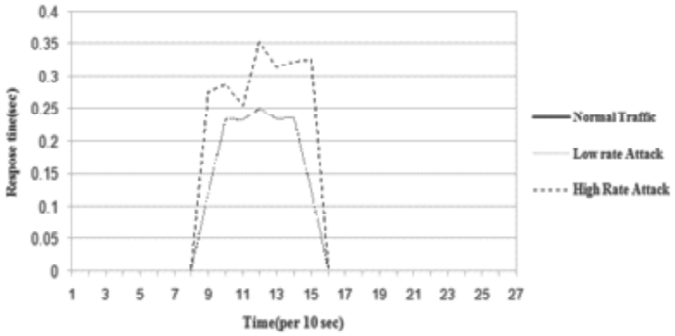


**Fig. 8. Variation of Average Response Time.**

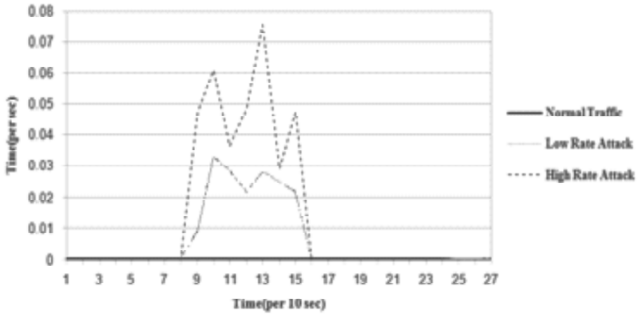


**Fig. 9. Variation of Average Round Trip Time**

## 5.3. Round Trip Time

The time taken by a packet to reach the destination and return is called the Round trip time. This RTT is an important metric for establishing a connection. When the attack is initiated, the RTT increases up to 10 microseconds which stays almost constant till the end of the attack. We have showed the RTT during attack period in Fig. 9 and Round trip Time (RTT). In this paper, we measure the impact of DDOS attack numbers of metrics.

# 6. CONCLUSION

After analyzing all the experiments we concluded the DDoS attack incidents increasing day by day. But to measure the performance of these attacks various techniques also attaining new heights. We evaluated our performance measurement on the GENI testbed. The GENI testbed allows carrying out the DDoS experimental in a secure environment. There are Network Research Validation Techniques evaluating like Simulation, Emulation and Real-Time but out of these summery GENI is very promising distributed testbed. We launched several of DDoS attacks on GENI testbed and measure the performance of attacks. We have measured the performance of generated attacks with the help of various metrics such as Throughput, Response Time.

# 7. REFERENCES

1. A. Kaur, K. Kumar, S. Behal and D. Kaur, "Network research validation using geni platform", Proceedings of 2015 National Conference on Communication, Computing and System(NCCCS), 24-25 August 2015.
2. I. Baldine, Y. Xin, A. Mandal, P. Ruth, C. Heerman, and J. Chase, "Exogeni: A multi-domain infrastructure-as-a-service testbed," in *International Conference on Testbeds and Research Infrastructures*. Springer, 2012, pp. 97–113.

3. L. L. Baldine, "Exo-geni: A multi-domain infrastructure as a testbed," *IEEE*, 2012
4. S. Behal and K. Kumar, "Trends in validation of ddos research," *Procedia Computer Science*, vol. 85, pp. 7–15, 2016
5. M. Berman, J. S. Chase, L. Landweber, A. Nakao, M. Ott, D. Raychaudhuri, R. Ricci, and I. Seskar, "Geni: A federated testbed for innovative network experiments," *Computer Networks*, vol. 61, pp. 5–23, 2014.
6. R. K. Chang, "Defending against flooding-based distributed denial-of-service attacks: a tutorial," *IEEE Communications Magazine*, vol.40, no. 10, pp.42–51, 2002.
7. K. D and S. M, "Impact analysis of ddos attacks on ftp services," *Associatison of Computer Electronics and Electrical Engineers*, 2014.
8. M. S. D kaur and K. Kumar, "Study of ddos attacks and defense evalution approaches," *International Journal of Computing and Business Research*, vol. 3, May 2012.
9. K. Daljeet and S. Monika, "Study of flooding based ddos attacks and their effect using deter testbed," *International Journal of Research in Engineering and Technology*, May 2013.
10. J. Duerig, R. Ricci, L. Stoller, M. Strum, G. Wong, C. Carpenter, Z. Fei, J. Griffioen, H. Nasir, J. Reed *et al.*, "Getting started with geni: a user tutorial,"*ACM SIGCOMM Computer Communication Review*, vol. 42, no. 1, pp. 72–77, 2012.
11. S. Huang, J. Griffioen, and K. L. Calvert, "fast-tracking geni experiments using hypernets," in *Research and Educational Experiment Workshop (GREE), 2013 Second GENI*. IEEE, 2013, pp. 1–8.
12. S. F. P. R. J Mirkovic and A. Hussain, "Measuring impact of ddos attacks," *in Proceeding of DETER Community Workshop on Cyber Security Experimentation*, June 2006.
13. D. Kaur and M. Sachdeva, "Study of recent ddos attacks and defense evaluation approaches," *the International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 1, pp. 332–336, 2013.
14. H. Kaur, S. Behal, and K. Kumar, "Characterization and comparison of distributed denial of service attack tools," in *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on*. IEEE, 2015, pp. 1139–1145.
15. K. Kumar, "Protection from distributed denial of service (ddos) attacks in isp domain," Ph.D. dissertation, Ph. D. Thesis, Indian Institute of Technology, Roorkee, India, 2007.
16. J. Mirkovic, E. Arikan, S. Wei, R. Thomas, S. Fahmy, and P. Reiher, "Benchmarks for ddos defense evaluation," in *MILCOM 2006-2006 IEEE Military Communications conference*. IEEE, 2006, pp. 1–10.
17. J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.
18. M. Sachdeva, K. Kumar, G. Singh, and K. Singh, "Performance analysis of web service under ddos attacks," in *Advance Computing Conference, 2009.IACC 2009. IEEE International*. IEEE, 2009, pp. 1002–1007.
19. M. Sachdeva, G. Singh, K. Kumar, and K. Singh, "Measuring impact of ddos attacks on web services," *Journal of Information Assurance and Security*, 2010.
20. H. F. Tipton and M. Krause, *Information security management handbook*. CRC Press, 2003.
21. Z. Yu, X. Liu, M. Li, K. Liu, and X. Li, "Exoapp: Performance evaluation of data-intensive applications on exogeni," in *Research and Educational Experiment Workshop (GREE), 2013 Second GENI*. IEEE, 2013, pp. 25–28.