iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** I **Month of publication:** January 2023

DOI: https://doi.org/10.22214/ijraset.2023.48675

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 11 Issue I Jan 2023- Available at www.ijraset.com

Mechanism, Tools and Techniques to Mitigate Distributed Denial of Service Attacks

Shankar Kumar[1], Dr. Nandeshwar Pd Singh[2], Dr. Narendra Kumar[3]
[1]*Research Scholar, Magadh University, Bodh-Gaya*
[2]*Associate Prof, Dept. of Mathematics, S.M.S.G. College, Sherghati, Gaya.*
[3]*Dept. of Computer Science, UMC, Raigarh (C.G.)*

Abstract: ***Attacks such as Distributed Denial of Service (DDoS) continue to menace the Internet. Attackers are able to use larger bandwidths because they concentrate on application layers. In order to create novel prevention strategies, it is crucial to understand the nature of distributed denial of service assaults. One of the most upsetting types of attacks on the Internet today is the distributed denial of service (DDoS) attack. When fundamental Internet infrastructure and services, such as the Domain Name System, are targeted or misused, such attacks become far more powerful and deadly (DNS). The DNS is a key component of the Internet's core infrastructure, and it plays a significant role in supporting many popular Internet applications like e-mail, VoIP, etc. in addition to translating human-readable names into IP addresses. Attacks such as Distributed Denial of Service (DDoS) continue to menace the Internet. Attackers are able to use larger bandwidths because they concentrate on application layers. In order to create novel prevention strategies, it is crucial to understand the nature of distributed denial of service assaults. The development of proactive preventative techniques is a crucial area of study, just like in other security-related fields. This essay examines recently released preventative measures. Additionally, it emphasizes the cloud era and how its systems are safeguarded against DDoS assaults.***
Keywords: DDoS Attacks, Cloud Attack, DDoS Preventions, Botnets, Cloud Security.

I. INTRODUCTION

DDoS (Distributed Denial of Service) assaults are a type of malicious cyber-attacks that are used by hackers or cybercriminals to block access to a host system, network resource, or online service by its intended users. DDoS attacks overwhelm the target computer and its supporting resources by flooding it with hundreds or millions of unnecessary requests. Because DDoS attacks come from dispersed or numerous sources or IP addresses, they differ from traditional Denial of Service situations. By using numerous compromised computer systems as sources of attack traffic, DDoS attacks are made effective. Computers and other networked resources, like as IoT devices, can be exploited machines.

When viewed from a distance, a DDoS assault resembles an unexpected traffic congestion that blocks the roadway and keeps ordinary traffic from reaching its destination **[1]**.

The reasons for a DDoS vary greatly, as do the kinds of people and organizations eager to carry out this kind of cyber-attack. Some assaults are conducted by irate people and hacktivists who wish to knock down a company's servers in order to make a statement, have fun by taking advantage of cyber-weakness, or show their displeasure.

Other distributed denial-of-service attacks have a commercial motivation, such as when a rival disrupts or shuts down the online activities of another company in order to steal customers in the interim. Others involve extortion, in which attackers target a firm, install hostage-ware or ransom-ware on its servers, and then demand that they pay a substantial quantity of money in order to undo the harm.

DDoS attacks are becoming more frequent, and some of the biggest international corporations are susceptible to them. One and only Amazon Web Services (AWS) was the target of the biggest attack in history in February 2020, surpassing an earlier attack on GitHub two years earlier.

DDoS effects can result in decreased genuine traffic, lost sales, and reputational harm. The number of Internet-connected gadgets (IoT) will increase along with the number of remote workers who work from home and the Internet of Things (IoT). Each IoT device's security may not always be up to date, making the network to which it is connected vulnerable to intrusion. As a result, DDoS mitigation and prevention are quite important.

II. COMMON DDOS ATTACKS

Different DDoS attack types target various network connection components. Knowing how a network connection is established is required in order to comprehend how various DDoS assaults operate. On the Internet, a network connection is made up of numerous separate parts or "layers." Each layer in the model has a distinct role, much like constructing a house from the ground up.

A conceptual framework known as the OSI model is used to categorize network connectivity into 7 different layers. Although the majority of DDoS assaults involve flooding a target device or network with traffic, there are three different types of attacks. In response to the target's countermeasures, the attacker may employ one or more distinct attack vectors, or they may switch attack vectors.

A. Application Layer Attack

The objective of these attacks, sometimes referred to as layer 7 DDoS attacks (in reference to the 7th layer of the OSI model), is to exhaust the target's resources in order to produce a denial-of-service. The layer where web pages are created on the server and transmitted in response to HTTP requests is the focus of the assaults. The cost of processing a single HTTP request is low on the client side, but the cost of responding on the target server's end can be high because the server frequently loads several files and does database queries to generate a web page. Layer 7 assaults are challenging to protect against since it might be challenging to distinguish between malicious and valid traffic.

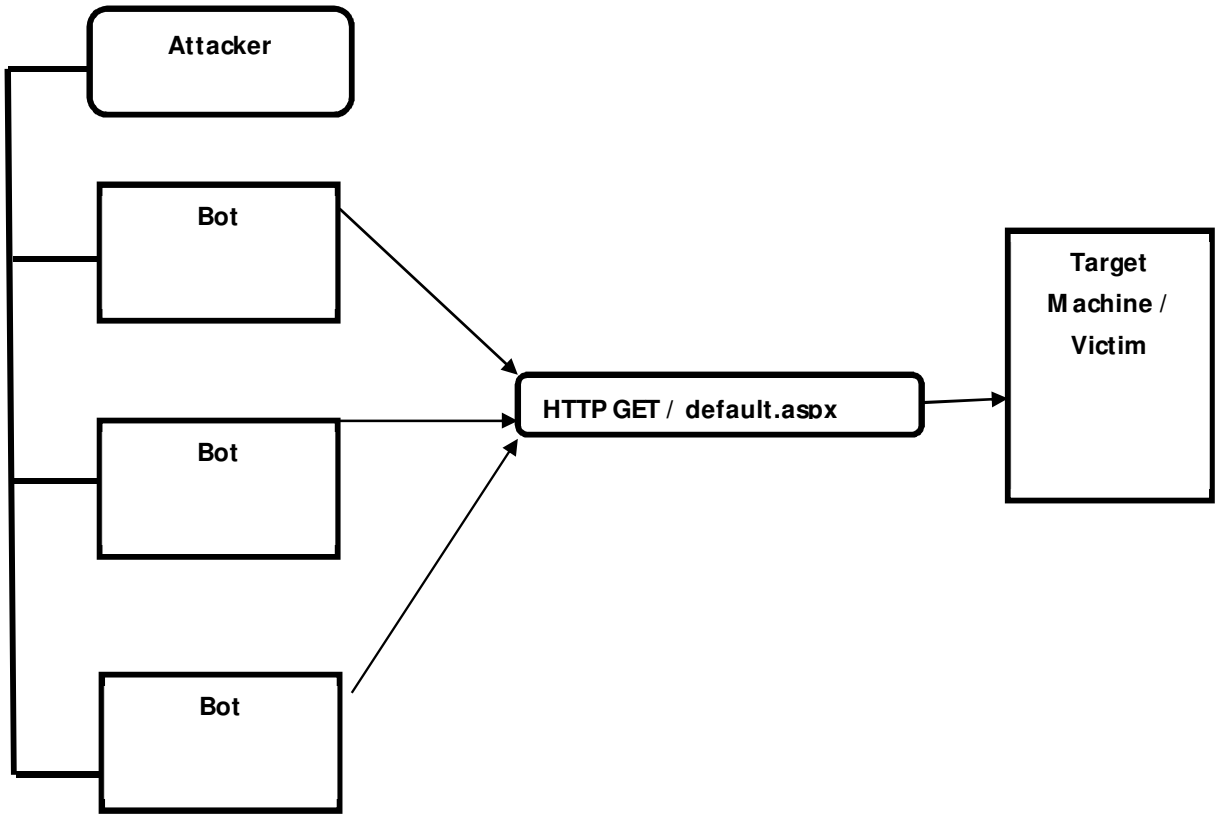


Fig. 1: Application Layer DDoS Attack

This kind of attack might be straightforward or intricate. Simpler systems might use the same set of attacker IP addresses, referrers, and user agents to access a single URL. When targeting random urls with complex versions, a huge number of attacking IP addresses, random referrers, and various user agents may be used.

B. Protocol Attack

Protocol assaults, often referred to as state-exhaustion attacks, interrupt services by using up excessive server resources as well as those of network hardware such as firewalls and load balancers. Protocol assaults make the target unreachable by taking advantage of flaws in layers 3 and 4 of the protocol stack.

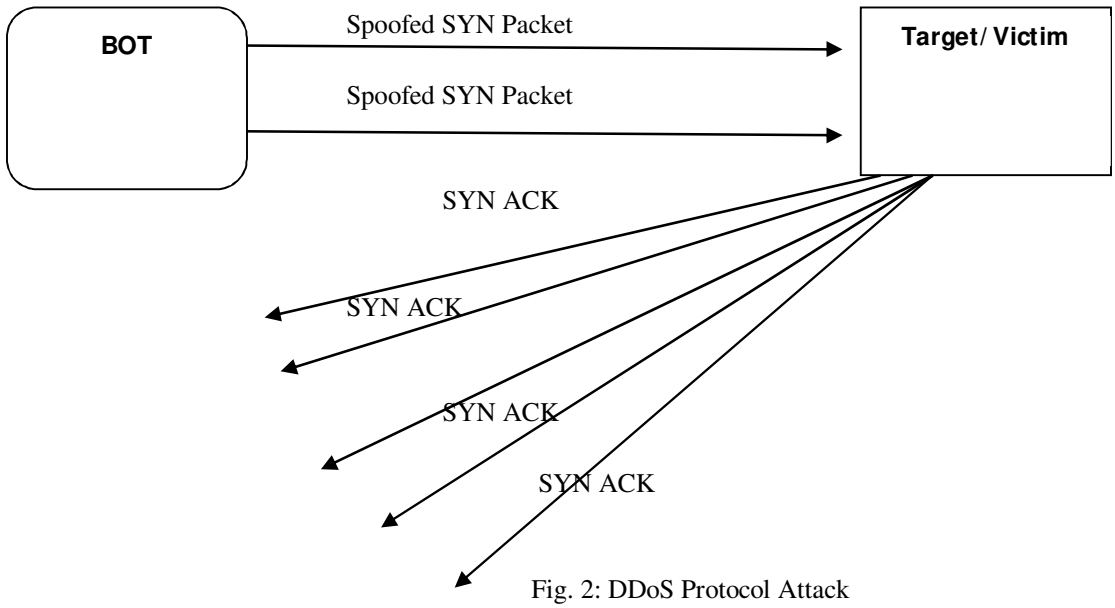


Fig. 2: DDoS Protocol Attack

After receiving a request, the employee goes to retrieve the package and waits for approval before carrying it outside. The employee then receives numerous additional shipment requests without confirmation up until they are unable to carry any more, are overburdened, and requests begin to go unanswered. This attack sends a target a lot of TCP "Initial Connection Request" SYN packets with fictitious source IP addresses in an attempt to take advantage of the TCP handshake, the series of interactions by which two computers establish a network connection.

Each connection request is answered by the target computer, which then waits for the handshake's last phase to complete itself but never does, using up all of the target's resources in the process.

C. Volumetric Attack

By utilizing all available bandwidth between the target and the greater Internet, these attacks aim to create congestion. By employing an amplification technique or another method of generating a lot of traffic, like requests from a botnet, large amounts of data are transmitted to a destination.

D. DNS Amplification

A Distributed Denial of Service (DDoS) attack known as DNS amplification uses DNS servers' weaknesses to amplify initial modest searches into much bigger payloads that are then utilized to bring down the victim's systems. DNS amplification is a form of reflection attack that tricks domain name systems that are open to the general public into bombarding a target with a lot of UDP packets **[2]**.

Attackers can "inflate" the size of these UDP packets using a variety of amplification techniques, making the attack powerful enough to bring down even the most resilient Internet infrastructure.

DNS amplification is a kind of reflection attack, as are other amplification techniques. In this instance, the reflection is obtained by asking a DNS resolver to respond to a spoof IP address.

In a DNS amplification attack, the attacker sends a DNS query to an open DNS resolver with a forged IP address (the victim's), causing it to respond to that address with a DNS response. The victim's network could rapidly get overloaded by the sheer volume of DNS responses once several fictitious queries are sent out and various DNS resolvers respond at once.

III. MECHANISM OF ATTACKS

In a DDoS assault, attackers profit from typical interactions between network devices and servers, frequently focusing on the networking devices that create an internet connection. As a result, rather targeting single servers, attackers concentrate on the edge network devices, such as, routers and switches. The bandwidth or the devices that provide that bandwidth are overloaded during a DDoS assault.

Distributed denial-of-service attacks are primarily conducted using botnets. The attacker will use hacking to get access to computers or other devices and install malware known as a bot. A botnet is the collective name for the network of compromised computers. The attacker then gives the botnet instructions to send more connection requests than the victim's servers and devices can manage.

Once a botnet has been created, the attacker can control an attack by giving each bot remote commands. Each bot in the botnet sends queries to the IP address of the victim's server or network when that server or network is being targeted by the botnet. This could overload the server or network and result in a denial-of-service attack on regular traffic. It might be challenging to distinguish attack traffic from regular traffic because each bot is an actual Internet device.

Botnets and zombie machines are the new threats in today's world. These are infected distributed devices that collaborate via master servers or distributedly to attack targets utilizing Internet Relay Chat (IRC), HTTP, Instant Messaging (IM), or Peer-to-Peer (P2P) protocols. Botnets are used for DDoS assaults as well as spamming, malware, espionage, and hosting dangerous programs and activities. Botnets are still a significant issue on the Internet **[3]**. According to **[4]**, the scattered nature of DDoS is the key issue. Even if the individual attacks of the many geographically dispersed zombie machines are modest, the total attack is very large.

IV. PREVENTION MECHANISM / TECHNIQUES

Prevention strategies have been published thus far from several angles. In Papers **[5]** and **[6]** provide classification algorithms. Paper **[5]** classifies prevention according to the activity used or the area where it was used. The measures made to defend against DDoS attacks are included in the activity deployment category. Additionally, it entails intrusion prevention tactics including turning off no-longer-used services, patching host machines, and changing the IP addresses of victims. This category also includes intrusion detection systems like anomaly or misuse detection systems. The DDoS prevention device may be placed close to the victim's network, on the attacker's side, or through an intermediary. The work demonstrated in **[6]** discussed general methods that can be used frequently.

Among them are turning off unnecessary services and IP broadcasting, applying the most recent security updates as described in **[5],** creating firewall rules, and using an IP pool to dynamically change server IP addresses. In **[7],** a different strategy is provided. This study suggests that DDoS prevention techniques can be divided into two groups based on the deployment location and the moment at which the DDoS defensive mechanism will kick in.

Some of the prominent prevention mechanisms are:

A. Prevention Mechanism Based on Source

Source-based defenses are set up as near to the attacking side as is practical. The deployment points of an Autonomous System (AS) are the edge routers at the source local network or the access routers that connect the sources' edge routers. The source that is referred to as the attacker is one of the locations where DDoS protection mechanisms are deployed. The defense is deployed more effectively the closer it is to the source. Network Egress and Ingress Filtering (NEIF), which is implemented by ISPs at the edge routers, is one security method. In addition to preventing their own network from taking part in DDoS assaults, the goal is to defend against attacks from faked IP addresses **[8].**

Ingress filtering decreases DDoS attacks brought on by IP spoofing, however it does not address the use of impersonating valid addresses. Filtering will not be applied to IP ranges that are utilized legally. Egress filtering, on the other hand, is an outbound filtering that limits just the specified IP addresses from accessing the outside network. Resources are wasted as a result of egress filtering. A certain ratio between incoming and outgoing traffic is assumed by MULTOPS. There is an attack if there is a noticeable variation in the flow of traffic coming in and going out. MULTOPS is susceptible to memory consumption since it uses a dynamic tree structure to maintain packet rates and IP addresses. Congested routers use a cooperative pushback mechanism to request rate limits from their neighbors on traffic based on the premise that the neighbors transmitting the traffic are more likely to be carrying attack traffic. A source-end defense mechanism is D-WARD. It is deployed at the end network's exit router and keeps track of both inbound and outbound traffic. Periodically, the traffic is profiled, and the flow models define the attacks. By rate limiting the outgoing traffic to the victim, DWARD responds to the attacks. The profiling uses up memory because it uses CPU resources. Attackers may act normally in the profiled flow attributes to avoid D-WARD defense.

The packet drop history at the router is used by RED-PD. Congestion causes dropped packets from flows to be mistakenly identified as high-bandwidth ones and dropped. MANAnet Reverse Firewall is yet another rate-limiter option. Although it functions similarly to a regular firewall, the prevention is directed from within outward.

DDoS assaults are prevented between the networks it divides. The goal is to stop the surrounding attacks by zombie machines. The reverse firewall requires manual direction, therefore runtime dynamic configuration changes are not possible.

B. Prevention Mechanism Based on Destination

The destination known as the victim is a different deployment location. This approach places the victim at the center of detection and prevention. IP trace-backing is one of the techniques. In cases where source IP verification is necessary, IP trace-backing is performed to find IP spoofing. Link testing or packet marking are also employed. In order for the victim to identify the source, packet marking depends on the routers passing through the victim's network. Link testing often begins at the router closest to the victim and progresses upstream routers until it reaches the source. Trace-back techniques have significant flaws. The number of routers that will participate in the trace-backing is one of them. Second, a large amount of the trace-back functionality necessitates network or administration overheads as well as high processing power.

The IP address database is necessary for history-based IP filtering (IAD). This database was created by looking at the IP addresses that appeared at the target side the most frequently. Only the IP addresses listed in the source IP database are permitted during a DDoS attack. It is reliable since it does not have to function across the entire Internet. On the other hand, it will be useless if the attacker discovers any IP address associated with the prior connections as well as the IAD.

Another suggestion is to maintain track of the source IP addresses' hops in addition to the source IP database. Hop-based IP filtering is the term used to describe this filtering method. The IPs and their hops are fetched to find the fake IP addresses when an attack is detected. Hops can be replicated using the legitimate IP addresses in the database, just like with the history-based technique, to make an attacker's connection appear real.

Path Identifier (PI) advises marking the packets with the same fingerprint rather than retaining the database at the target side. The PI method states that every packet following the same path has the same identifier. The same path identification may represent several paths because to the limited space on the packets for identification.

Another danger for the victim side is SYN flooding. Through the use of SYN Cookies, they can be avoided. One method for SYN flood attacks is this one. When the proper ACK is returned, it is a mechanism to reconstruct the three-way handshake between the client and server. If the SYN queue becomes full, the server keeps connections from being dropped. The client continues to receive SYN + ACK answers from the server, which discards the SYN entry. The server can recreate the SYN queue entry after receiving the proper ACK.

C. Prevention Mechanisms against Application Layer Attack

The application level DDoS attack preventions are a crucial category in addition to deployment location of the prevention. DNS is one of the most frequently hit targets. DNS Amplification Attacks Detector (DAAD) is suggested as a defense against DNS amplification attacks. DAAD uses the Iptraf program to analyse and preserve the collected network traffic in real time. Request and response messages are the two types of DNS messages. A request is looked for in the database for each response. It is tagged as suspicious if none are discovered. An alarm is set off when the suspicious number goes above a certain level.

Rational rate limiting is suggested for HTTP attacks. DDoS Shield detects suspicious sessions using statistical methods. Rate limiting is used by the DDoS-resilient scheduler in accordance with the suspicion assignment. For HTTP attacks as well, an anomaly-based technique is used in place of statistical methods. The entropy of the document is used with a semi-markov model to detect application layer attacks. Monitoring user behavior is another strategy for figuring out whether or not a person is malevolent. User characteristics such as request volume, immediate, and long-term habits are observed. DAT, which stands for Defense against Tilt-DDoS Attacks, offers customized services to distinct user types.

D. Prevention Mechanisms against Cloud Attack

Commercial companies are entering the cloud business and providing services to their clients on the cloud platform as a result of the cloud builders' quick development and open structure. Many companies, such as Redhat, Paypal, Dell, HP, Intel, and others, are beginning to create their own cloud architectures. Additionally, they are helping to develop open source cloud tools like OpenStack and Cloudstack. The use of cloud systems is anticipated to rise along with the amount of money being invested in cloud services.

While major investors like Google, eBay, Amazon, and IBM publish their services in the cloud, cloud systems are vulnerable to attack. In addition to Google announcing its Compute Platform and eBay collaborating with Microsoft on its Azure platform, both companies started deploying OpenStack for testing and development at the same time. IBM has been offering its own cloud solution while Amazon is well-known for its Compute Cloud (EC2) platform. Customers of these companies are also under attack from hired professionals who employ system weaknesses to bring down cloud services, in addition to actual attackers. An example situation was Bitbucket.com, which keeps its infrastructure under EC2.

The study of DDoS attacks and cloud-based security techniques is still in its early phases. Many different areas of cloud security are covered, including DDoS protection as a cloud service, attack mitigation approaches against DDoS, affordable DDoS attacks in the cloud, and security architecture against DDoS attacks.

Swarm network use is one of the mitigation strategies suggested. Using the Intelligent Water Drop (IWD) method, the Transparent and Intelligent Fast-Flux Swarm Network prevents DDoS attacks. Fast-Flux Fast-flux domain name servers and decentralized swarm nodes form the foundation of the swarm network. The attacker receives several IP addresses from a fast-flux service. The nodes that will transport messages between the client and the server are chosen using the IWD method. In the conventional method, routers route requests from the client to the server. An additional layer is introduced in the swarm network architecture so that all incoming traffic is registered with the swarm and forwarded to the server.

The response will be returned to the swarm and at the conclusion delivered to the client. It is challenging for the attacker to bring down the network because there isn't a clear bottleneck there. However, there are certain restrictions. At the swarm network, each connection is tied to a specific route for a specific client and server. It does not permit SSL connections or quick changes that leave name servers idle.

Cloud-based attack defense is a new, transparent way of prevention that is announced as a network approach (CLAD). To at least one CLAD entry point, all traffic that is directed to the protected server is redirected. A network layer assault defense is implemented at the CLAD's entrance point. Packets that are undesired or harmful are dropped utilizing firewall mechanisms. To limit the number of concurrent connections to the same server, admission control is also used.

Depending on the load on the protected server, the number of concurrent connections may vary. It is also suggested to use authentication to separate fraudulent clients from trustworthy ones. Instead of using the cloud service provider's maximum quota definition for the inappropriate charging of harmful traffic, a new challenging model is presented. The CLAD system also includes a congestion control mechanism to stop the client from using up resources. CLAD is concentrated on HTTP traffic.

Despite the availability of tools like Agobot, Mstream, and Trinoo, the most of attackers using less sophisticated equipment for extensible XML-based Markup Language Denial of Service (X-DoS) and H-DoS (Hypertext Denial of Service) attacks because of their straightforward application. Service-oriented traceback architecture (SOTA) and Cloud TraceBack (CTB) are suggested as defenses against H-DoS and X-DoS attacks. SOTA is an online security service application that uses the traceback methodology in a Service-Oriented Architecture (SOA) fashion. It is used to detect fraudulent communications and to thwart X-DoS attacks. All service requests are initially sent to CTB for marking at the edge router. In an attack scenario, the client asks CTB to transmit a request for a website to the requested server.

When SOTA responds to the attack client's Simple Object Access Protocol (SOAP) request with an answer, a mark is appended to the header. This message is tagged, and the server is instructed to extract the mark and send it to the client side, which is used to block attack traffic.

E. Prevention of DDoS using IDS/IPS

IDS is also advised for cloud environments as a defense tactic. They are useful for examining the attacker's activity for well-known attack types like SYN, Smurf, and others. They operate on a signature-based system and are effective at detecting misuse, but they shouldn't be chosen for unusual traffic or novel types of attacks. Deploying the IDS on each host machine is one suggested strategy. On each Virtual Machines (VMs), Snort is utilized as the IDS, and the Dempster-Shafer Theory (DST) is employed to evaluate the acquired data. It is a development of the Bayesian model **[10]**, a potent technique for statistical inference, diagnosis, risk assessment, and decision making It is claimed in the proposed work that IDS data can be used to find DDoS attacks.

For well-known flood attack types like SYN, the IDS method can be used. Techniques like Hop-Count Filtering (HCF) and IP-to-hopcount (IP2HC) are suggested as faked IP detection methods for spoofing attacks. Depending on the Time to Live (TTL) value, the HCF counts the number of hops. Another variant of HCF is IP2HC, which adds each IP address's hop count to a hash table between the source IP addresses. By verifying the SYN flag state and the TTL value, it is possible to establish whether a packet is tagged as dubious or not**[11]**.

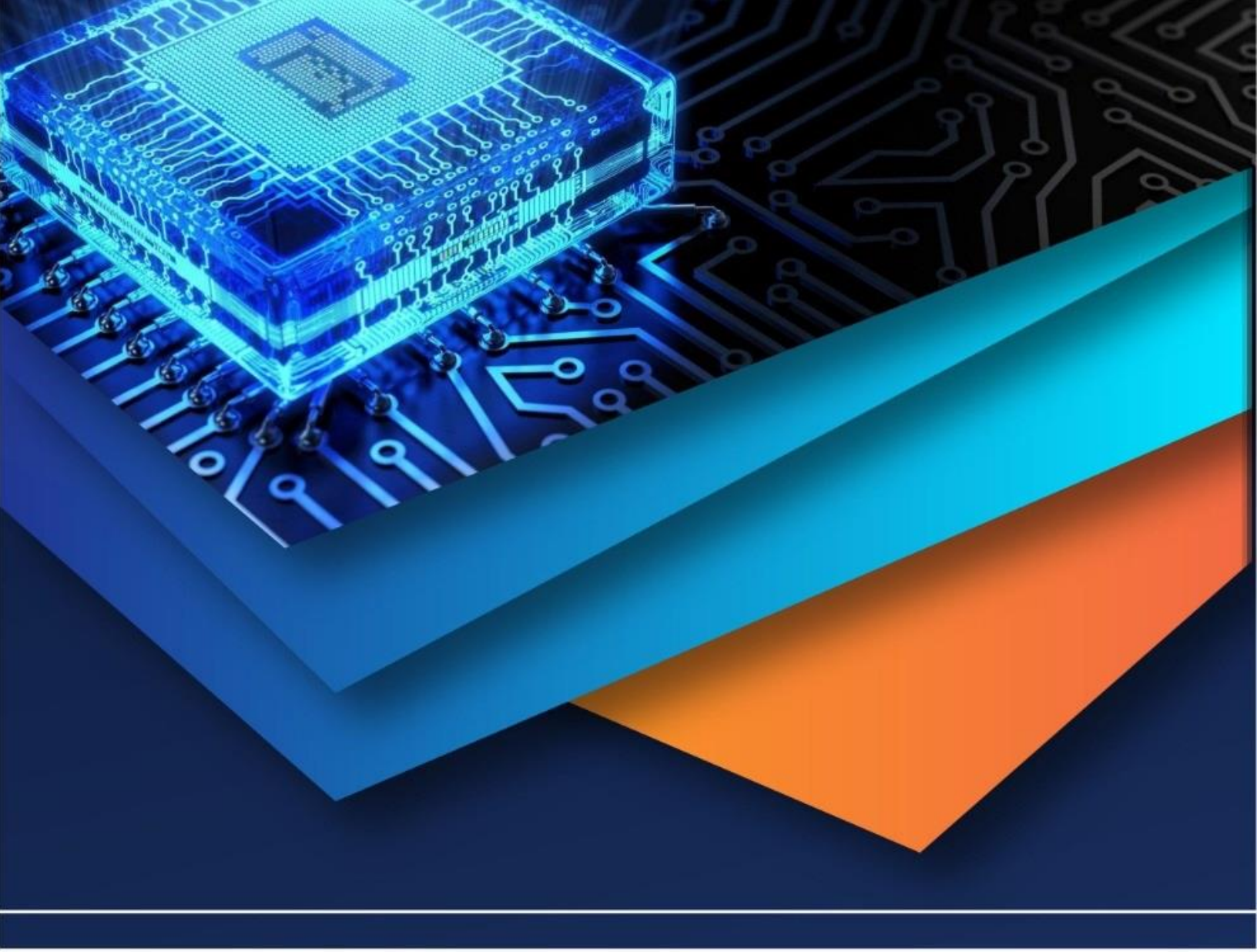
A stronger defense can be built by combining detection and prevention techniques. To stop DDoS attacks, the multilayer firewall structure is paired with DDoS detection using flow patterns. It is suggested that some flooding assaults can be identified by looking at the flow parameters, such as the average number of flows per packet, coming from the router. A firewall can also be used to filter the traffic by using the IP and port information of these flows.

V. CONCLUSION

There are anomaly-based approaches in addition to the growing number of signature-based detection and prevention techniques. Machine learning algorithms offer anomaly-based preventions for zero-day attacks. Future research will focus on both machine learning and data mining techniques in cloud computing. In particular, at the botnet detection and Data mining techniques appeared to be a working area in the area of preventive. Hybrid approaches can be made more effective by combining them with source-based, destination-based, or web-based preventative procedures that improve the cloud's performance.

REFERENCES

[1] S. Tripathi, B. Gupta, A. Almomani, A. Mishra, and S. Veluru, "Hadoop based defense solution to handle distributed denial of service ddos attacks", Journal of Information Security, vol. 4, pp. 150–164, June 2013.
[2] F. Guo, J. Chen, and T. Chiueh "Spoof detection for preventing dos attacks against dns servers," in 26th IEEE Int. Conf. on Distributed Computing Systems, 2006, pp. 38–43.
[3] N. Hachem, Y. Ben Mustapha, G. G. Granadillo, and H. Debar, "Botnets: Lifecycle and taxonomy," in Conf. on Network and Information Systems Security, pp. 1–8, 2011.
[4] D. Mahajan and M. Sachdeva, "DSoS attack prevention and mitigation techniques - a review," Int. Journal of Computer Applications, vol. 67, no.19, pp. 975–8887, April 2013.
[5] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: a classification," in 3rd IEEE Int. Symposium on Signal Processing and Information Technology, pp. 190–193, December 2003.
[6] B. B. Gupta, R. C. Joshi and M. Misra, "Distributed denial of service prevention techniques," Int. Journal of Computer and Electrical Engineering, vol. 2, pp. 1793–8163, April 2010.
[7] S. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046–2069, 2013.
[8] T. Yatagai, T. Isahora and I. Sasase, "Detection of HTTP-GET flood attack based on analysis of page access behavior," in IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, 2007, pp. 232–235.
[9] Nazrul Hoque, Dhruba K Bhatattacharya and Jugal K Kalita,: Botnet in DDoS Attacks: Trends and Challenges. In:IEEE Communications Surveys and Tutorials VOL. X(2015)
[10] Altwaijry H. and Algarny S. (2012), "Bayesian based intrusion detection system",In Journal of King Saud University – Computer and Information Sciences, pp.1-6.
[11] Kiran Bala, Narendra Kumar and Ashok Kumar Singh, "Performance Evaluation of Intrusion Detection System, pp., 10 – 15, 2018, doi: https://doi.org/10.15623/ijret.2018.0710003
[12] Hwang, Y. Kwok, S. Song, M. Cai, Y. Chen, and Y. Chen (2006), "DHT Based Security Infrastructure for Trusted Internet and Grid Computing", In Int'l J. Critical Infrastructures, vol. 2, no. 4, pp. 412- 433.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY