iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VI **Month of publication:** June 2024

DOI: https://doi.org/10.22214/ijraset.2024.63392

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 12 Issue VI June 2024- Available at www.ijraset.com

A Systematic Review of the Rise of DDoS Attacks as a Service (DDoSaaS)

Afra Pathan[1], Rutika Patil[2], Prof. Pavan Mitragotri[3]
[1, 2]*Post Graduate Student, Department of Master of Computer Applications, KLS Gogte Institute of Technology, Belagavi, India*
[3]*Professor, Department of Master of Computer Applications, KLS Gogte Institute of Technology, Belagavi, India*

Abstract: ***The emergence of DDoS-as-a-Service (DDoSaaS) platforms has changed the landscape of cyber threats, leading to a substantial evolution in the propagation of Distributed Denial of Service (DDoS) assaults. In order to better understand the emergence of DDoSaaS, this systematic review looks at its evolution, working processes, and driving forces. We combine information from technical papers, peer-reviewed articles, and cybersecurity threat assessments that were released until now.***
Keywords: DDoS-as-a-Service (DDoSaaS), Cyber threats, Cybersecurity, DDoSaaS Mitigation, DoS, Cloud computing

I. INTRODUCTION

In recent years, cyber threats have changed a lot, with Distributed Denial of Service (DDoS) attacks becoming very common and disruptive. In the past, carrying out a DDoS attack required a lot of technical knowledge and resources, which meant only skilled hackers could do it. Advances in the processing technologies have helped attackers in increasing the attacks too, for instance, the development of Denial of Service (DoS) attacks to distributed DoS (DDoS) attacks which are seldom identified by conventional firewalls [1]. However, the rise of DDoS-as-a-Service (DDoSaaS) has changed this, making it easy for almost anyone to launch powerful DDoS attacks, even if they have little technical skill. In recent years, cyber threats have changed a lot, with Distributed Denial of Service (DDoS) attacks becoming very common and disruptive. In the past, carrying out a DDoS attack required a lot of technical knowledge and resources, which meant only skilled hackers could do it [1]. However, the rise of DDoS-as-a-Service (DDoSaaS) has changed this, making it easy for almost anyone to launch powerful DDoS attacks, even if they have little technical skill. DDoSaaS works like regular online services, offering attack capabilities to anyone who can pay. These services provide easy-to-use interfaces, customer support, and different pricing options, making it much easier for people to perform DDoS attacks. This has led to a significant increase in the number, size, and complexity of DDoS attacks, creating big challenges for cybersecurity experts and organizations By reviewing a range of sources like academic papers, technical reports, and cybersecurity assessments, this study provides a detailed look at DDoSaaS. It describes the different types of services available, how they are marketed, and the technology behind them. The review also looks at the impact of DDoSaaS on various industries, showing how it has made DDoS attacks more accessible and increased cyber threat. The rise of DDoS-as-a-Service has democratized cyber-attacks, allowing even those with little to no technical expertise to launch sophisticated and large-scale DDoS attacks with ease. These services, often found on the dark web, offer a variety of attack options, customer support, and competitive pricing, making them accessible to a wide range of individuals, from disgruntled employees to cybercriminals looking to extort money from businesses. The proliferation of DDoSaaS has resulted in a significant uptick in the frequency, scale, and complexity of DDoS attacks, overwhelming traditional defense mechanisms and necessitating more advanced cybersecurity strategies. The impact of these services is far-reaching, affecting industries from finance to healthcare, where the downtime and disruption caused by DDoS attacks can lead to substantial financial losses and compromise sensitive data. As a result, cybersecurity professionals are increasingly focusing on developing more robust, adaptive defenses and emphasizing the importance of proactive threat intelligence and incident response planning. This shift underscores the urgent need for continued research and innovation in cybersecurity to combat the evolving threat posed by DDoSaaS.

II. OBJECTIVE

The objective of the systematic review is to comprehensively understand the emergence, evolution, working processes, and driving forces behind DDoS-as-a-Service (DDoSaaS) platforms. The review aims to analyze information gathered from technical papers, peer-reviewed articles, and cybersecurity threat assessments spanning from 2000 to 2023. Specifically, the objective is to investigate how DDoSaaS has transformed the cyber threat landscape by democratizing access to DDoS attack capabilities, thereby making it easier for individuals with minimal technical skills to launch powerful and disruptive attacks.

Examining DDoSaaS platforms' infrastructure, user interfaces, pricing structures, and customer support systems is the goal of this review. It also looks at the different kinds of services provided by DDoSaaS platforms and how prospective users are marketed with them. In addition, the review attempts to evaluate DDoSaaS's effects on various industries, emphasizing the difficulties it presents for cybersecurity professionals and institutions. In general, the goal is to offer insights into how the spread of DDoSaaS affects cybersecurity tactics and strategies and to pinpoint possible directions for further study and the creation of countermeasures.

III. WHAT IS DDoS ATTACK AS A SERVICE?

DDoS attack as a Service (DDoSaaS) represents a disturbing trend in cybercrime where individuals or organizations can purchase DDoS attack services from criminal providers. This model operates similarly to legitimate Software-as-a-Service (SaaS) businesses, offering on-demand access to DDoS attack capabilities in exchange for a fee. Essentially, DDoSaaS providers act as intermediaries, enabling customers to launch DDoS attacks against their targets without needing to possess technical expertise or infrastructure [3]. This accessibility has democratized cybercrime, allowing a broader range of individuals, including non-technical users, to engage in malicious activities. DDoSaaS platforms typically offer various packages and services, allowing customers to customize their attacks based on parameters such as attack duration, intensity, target selection, and attack vectors. Additionally, DDoSaaS providers may offer ancillary services such as stress testing or vulnerability scanning to enhance the effectiveness of attacks. The rise of DDoSaaS has contributed to a significant increase in the frequency, scale, and sophistication of DDoS attacks, posing substantial challenges for cybersecurity professionals and organizations seeking to defend against these threats [3].

IV. THE PROLIFERATION AND MECHANISM OF DDOSAAS

DDoSaaS platforms are often marketed and sold on the dark web, mimicking legitimate service offerings with user-friendly interfaces, tiered pricing models, and customer support. These services typically leverage botnets—networks of compromised computers or IoT devices—to amplify the scale and impact of attacks. Users of DDoSaaS can specify their targets and customize the nature of the attack, selecting parameters such as duration and intensity. The ease of access to DDoSaaS has significantly expanded the pool of potential attackers. Previously, executing a DDoS attack required a certain level of technical expertise. Now, with DDoSaaS, even those with minimal technical skills can launch sophisticated attacks. In network and computer security, generally the expression denial of service is used to indicate to an attack intended to damage or saturate the computer resources or network resources, with intent of making the legitimate users no longer be able to use the provided services[2].This has led to a marked increase in the frequency and scale of DDoS incidents, affecting a wide range of targets from small businesses to large enterprises and government entities. The number of possible attackers has greatly increased due to DDoSaaS's ease of access. A DDoS attack used to take a certain amount of technological know-how and resources to carry it. DDoSaaS has made it possible for even those with little technical knowledge to launch complex attacks, democratizing cybercrime and raising the amount of attacks overall. The frequency and scope of DDoS assaults have significantly increased as a result of their democratization. These assaults have affected a wide range of targets, including small businesses, huge corporations, and governmental organizations. They frequently cause significant financial and reputational harm. Developing DDoS defense mechanisms with broad-spectrum detection capabilities, robustness against adversarial attacks, and cost-effective and collaborative DDoS defense mechanisms for establishing the Internet are future research directions in network security [17].

V. HOW CLOUD COMPUTING ENABLES DDOS ATTACKS

Cloud computing has revolutionized IT infrastructure by providing scalable and flexible resources, but it has also inadvertently facilitated the execution and amplification of Distributed Denial of Service (DDoS) attacks. DDoS attack is an attack which is targeted by multiple compromised computers called as bots or zombies focusing on a single system [1].The very characteristics that make cloud services attractive—scalability, broad network access, and resource pooling—can be exploited by malicious actors for launching DDoS attacks.

1) *Scalability and Resource Availability:* Cloud platforms offer vast amounts of computing power and bandwidth, which can be rented and used to generate significant attack traffic. Attackers can utilize multiple cloud accounts to orchestrate larger and more powerful attacks.
2) *Distributed Nature:* Cloud services are inherently distributed, allowing attackers to launch attacks from multiple geographic locations simultaneously. This makes it more challenging to mitigate the attacks as they come from numerous sources.
3) *Ease of Use:* Cloud services are designed to be user-friendly and accessible, lowering the technical barriers for launching complex attacks. This ease of use extends to setting up botnets and other malicious infrastructures within the cloud.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VI June 2024- Available at www.ijraset.com

4) *Anonymity and Abuse:* The ability to pay for cloud services using cryptocurrencies and other anonymous payment methods can make it difficult to trace the origins of an attack. Furthermore, compromised accounts and stolen credentials can be used to deploy attacks without the knowledge of the legitimate account holders.

VI. TYPES OF CLOUD-BASED DDOS ATTACKS

Cloud-based DDoS attacks can be categorized into several types based on the attack vector and the targeted layer of the network stack. These attacks exploit the scalability, resource availability, and distributed nature of cloud computing to maximize their impact. DDoS attack is separated into seven noteworthy classes which are: flood attack, amplification attack, coremelt attack, land attack, TCP SYN attack, CGI request attack, and authentication server attack [1].

1) *Volumetric Attacks:* These attacks aim to saturate the bandwidth of the target by overwhelming it with a high volume of traffic. UDP floods, ICMP floods, and amplification assaults utilizing DNS or NTP are typical instances. Attackers use the large bandwidth capacities of cloud servers to reflect and amplify traffic in cloud amplification assaults, hence boosting the attack magnitude.
2) *Protocol Attacks:* These kinds of attacks exploit some identified protocol vulnerabilities like implementation flaws or design that is used to change the information forwarded to or from a certain target and cause inappropriate behaviors [2]. These attacks exploit weaknesses in network protocols to deplete server resources. SYN floods, ACK floods, and fragmented packet attacks are a few examples. A common instance is a SYN flood, in which adversaries take advantage of the TCP handshake procedure to force the server to allot resources for partially open connections, thus depleting its ability to manage valid traffic.
3) *Application Layer Attacks:* These attacks target specific applications or services, aiming to exhaust resources at the application level. Examples include HTTP floods, Slow loris, and DNS query floods.

VII. CLOUD PROVIDERS ROLE IN MITIGATING DDOS ATTACKS

Cloud providers play a crucial role in countering DDoS attacks by utilizing their extensive infrastructure and advanced technologies. Distributed denial-of-service (DDoS) attacks have become a weapon of choice for hackers, cyber extortionists, and cyber terrorists. These attacks can swiftly incapacitate a victim, causing huge revenue losses [10] They employ strategies such as deep packet inspection (DPI) and rate limiting for traffic scrubbing and filtering, dynamically allocating resources to ensure service continuity during attacks, and offering specialized DDoS protection services like AWS Shield, Azure DDoS Protection, and Google Cloud Armor, which come with real-time monitoring and quick response capabilities. Additionally, they utilize rate limiting and load balancing to spread traffic across multiple servers and minimize the impact of attacks. These providers collaborate with cybersecurity firms and industry groups to share threat intelligence and keep abreast of emerging threats [10]. Additionally, they educate customers on best practices for securing applications and infrastructure, configuring security settings, and monitoring for suspicious activities, further strengthening defenses against DDoS attacks. More and more companies are now offering mitigation services and, typically, these are hosted in the cloud – as far upstream as possible [11].

A. Amplification Techniques

Amplification techniques are employed to increase the volume of attack traffic, making DDoS attacks more destructive:

1) *DNS Amplification:* Using a spoof IP address (the target's IP), attackers send brief requests to open DNS resolvers. Large responses are sent by the resolvers to the target, which multiplies the attack traffic several times.
2) *NTP Amplification:* In a manner akin to DNS amplification, attackers send little queries to NTP servers which reply to the spoof IP address with much larger replies. This has the potential to 500-fold increase traffic.
3) *Memcached Amplification:* One of the most potent DDoS tactics, attackers take advantage of weak Memcached servers by making tiny requests that result in enormous replies. This technique can generate amplification factors greater than 50,000 times.

VIII. PRICING MODELS AND PAYMENT METHODS

Distributed denial of service (DDoS) attacks exploit the acute imbalance between client and server workloads to cause devastation to the service providers[14].Due to their flexible pricing structures and assortment of payment options, DDoS-as-a-Service (DDoSaaS) platforms have become increasingly popular. These features aim to draw in a diverse clientele, encompassing both novice and expert cybercriminals.

A. Pricing Models

1) *Pay-Per-Attack:* Users are charged for each attack they carry out separately. The length, severity, and complexity of the attack vector are some of the variables that affect price. Prolonged, high-intensity attacks can cost hundreds or thousands of dollars, while short-term, low-intensity attacks might only cost a few dollars.
2) *Subscription-Based:* Under these models, users pay a monthly or yearly fee to access a certain number of attacks or a certain amount of attack bandwidth. These payment plans are recurring. Different tiers are frequently included in subscriptions; higher tiers offer more potent attacks or extra features like attack customization and customer support.
3) *Volume-Based Pricing:* The amount of traffic generated during an attack determines how much a service charges. For providers, this can be an especially profitable model because large-scale attacks that use a lot of bandwidth can fetch higher prices.
4) *Feature-Based Pricing:* The features and services offered can also affect the price. Standard volumetric attacks may be included in basic plans, while multi-vector attacks, targeted application-layer attacks, and individualized customer support may be included in premium plans.

B. Payment Methods

1) *Cryptocurrencies:* Due to their pseudonymous nature, which helps protect both the buyer and the seller's identity, cryptocurrencies like Bitcoin, Ethereum, and Monero are the most popular payment methods for DDoSaaS. International transactions can also be facilitated by cryptocurrencies without the use of conventional banking systems.
2) *Prepaid Cards and Vouchers:* You can buy prepaid cards or vouchers with cash and use them anonymously. Some services accept these. An extra degree of anonymity is offered by this method to users who would rather not use cryptocurrencies.
3) *Conventional Payment Methods:* In rare circumstances, some DDoSaaS platforms may take credit cards or PayPal as more conventional payment methods. Due to the traceability and possibility of legal action against suppliers and clients, these techniques are less popular.
4) *Dark Web Marketplaces:* DDoSaaS services are frequently included in larger dark web marketplaces that offer a range of illegal goods and services for sale. These online marketplaces usually employ escrow services to mediate transactions and guarantee confidence between buyers and sellers.

IX. IMPACT AND CONSEQUENCES OF DDOSAAS

A. Financial Losses and Downtime Costs

The financial impact of DDoS attacks facilitated by DDoS-as-a-Service (DDoSaaS) can be substantial [16]. Organizations face direct and indirect costs, including:

1) *Revenue Loss:* During downtime, e-commerce websites, financial institutions, and online services may suffer sizable revenue losses. Lack of availability for even a minute can result in missed opportunities, incomplete transactions, and unfulfilled client demands.
2) *Mitigation Expenses:* Businesses need to spend money on cybersecurity solutions to lessen the impact of attacks. These solutions include hiring cybersecurity experts, upgrading infrastructure, and acquiring DDoS protection services. These expenses may increase, particularly in the event of protracted or frequent attacks.
3) *Operational Disruptions:* When workers are unable to access vital systems and carry out their tasks, downtime has an adverse effect on productivity. As businesses race to restore services, this may result in missed deadlines, postponed projects, and higher operating costs.
4) *Post-Attack Recovery:* Following an attack, companies frequently have to pay for system maintenance, data recovery, and forensic analysis to identify and fix the vulnerabilities that were used in the attack.

B. Reputation damage and brand erosion

DDoS attacks have the potential to cause serious, long-term harm to an organization's reputation in addition to immediate financial losses. Long-term or frequent service interruptions erode consumer confidence and satisfaction. Customers in the digital age expect smooth and dependable service, and frequent setbacks may cause them to switch to competitors who provide more consistent and reliable experiences [17]. This is especially important in industries where uninterrupted service is essential, like banking, online retail, and entertainment. Media coverage is frequently affected by these disruptions; high-profile attacks often make headlines, resulting in un-favourable press that can damage an organization's reputation.

Customer's perceptions of the company may be greatly impacted by such negative press, which could weaken the brand's overall strength and value. DDoS attacks can also significantly erode stakeholder confidence. Investors, business partners, and shareholders might start to doubt the organization's capacity to protect its assets and carry on with business as usual [20]. A drop in stock prices, a decrease in investment inflows, and strained business relationships can result from this loss of confidence. Fearing possible risk spill-overs, partners may re-evaluate their alliances and investors may be reluctant to provide additional funding. Furthermore, businesses that have been the target of DDoS attacks frequently find it difficult to effectively compete. By taking advantage of the weaknesses in the impacted company, rivals who are seen as more trustworthy and secure can gain market share and improve their own brand image [15]. The company's market position and brand equity may be further eroded over time by this competitive disadvantage.

C. Legal and Regulatory Implications

Beyond the initial service interruption, DDoS attacks may have major legal and regulatory repercussions. Violations of compliance are a significant cause for concern. Organizations are required to put strong security measures in place to protect sensitive data by regulatory frameworks like the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS). Successful DDoS attacks have the potential to reveal holes in these security protocols, which could result in noncompliance. Such violations may have serious consequences, such as high fines, jail time, and heightened regulatory attention [20]. To satisfy compliance requirements, organizations might need to make significant investments in enhancing their security infrastructure, which would increase the cost. Risks associated with litigation are yet another important effect of DDoS attacks. Customers and partners may pursue legal action to recover damages if these attacks cause service disruptions that result in major operational setbacks. This may lead to expensive and time-consuming legal disputes, especially when class action lawsuits are involved. In addition to depleting organizational funds, these lawsuits take the organization's attention away from its primary business operations and toward settlement talks and legal defense. Such lawsuits can result in large financial settlements, which can have a negative effect on an organization's bottom line and even jeopardize its stability financially. After a DDoS attack, mandatory reporting requirements increase the complexity and consequences even further. Significant cyber incidents must be reported by organizations to regulatory authorities in many jurisdictions. Due to the requirement to disclose, organizations may face heightened scrutiny and audits, which will put them under pressure to prove they have improved their security procedures in order to avert similar incidents in the future. Additionally, the cost of cybersecurity insurance is frequently higher for organizations that have been subject to DDoS attacks [15]. When calculating coverage costs, insurers consider the past history of cyber incidents, and recurrent attacks can drive up the cost of insurance unnecessarily. Comprehensive cybersecurity strategies are crucial given the heightened financial burden and the requirement to invest in improved cybersecurity measures. Organizations must proactively mitigate these risks as DDoS attacks become more sophisticated and accessible to protect their operations and financial stability, and legal standing.

X. MITIGATION AND COUNTERMEASURES

A. Traditional Security Measures

1) *Intrusion Detection Systems (IDS) and Firewalls:* The first line of defense against DDoS attacks is comprised of firewalls and intrusion detection systems (IDS), which monitor and filter incoming traffic. After analyzing network traffic, firewalls use pre-established rules to either allow or block packets according to specifications like IP addresses, ports, and protocols. On the other side, intrusion detection systems (IDS) identify questionable patterns or actions that could point to a DDoS attack and send out alerts for additional research [19]. Although these defenses work well against SYN floods and other basic packet floods, they might not be able to stop sophisticated application layer attacks or large-scale volumetric attacks. Furthermore, it can be difficult to keep an updated set of guidelines and signatures because attackers are always changing their strategies to avoid detection.
2) *Load Balancers:* Load balancers are essential for spreading incoming traffic among several servers, which keeps a DDoS attack from overwhelming a single server [19]. Load balancers contribute to the optimal performance and availability of services by distributing the load evenly, even in the face of DDoS attacks or periods of high traffic. However, if the attack targets load balancers specifically, they may end up being a single point of failure. In these situations, attackers might concentrate their efforts on overloading the load balancer's capacity, which would prevent users from accessing the network as a whole. Furthermore, load balancers may add overhead and latency, which can affect the responsiveness and overall performance of the system.

3) *Limiting Traffic Rates:* To prevent servers from overloading during a DDoS attack, traffic rate limiting is implemented by placing thresholds on the rate of incoming traffic. Organizations can lessen the effects of DDoS attacks and preserve service availability for authorized users by setting limits on the volume of traffic that is permitted to reach the server. This strategy needs to be properly adjusted, though, to prevent unintentionally obstructing valid traffic and degrading user experience. Excessively strict rate-limiting policies may cause false positives, impede regular service delivery, and worsen the organization's reputation in addition to alienating clients. Thus, companies need to find a way to protect against DDoS attacks while still allowing authorized users to access systems without any problems.

B. Cloud-based DDoS Mitigation Solutions

Cloud-based DDoS mitigation systems successfully fend off DDoS attacks by utilizing the scalability and resilience of cloud infrastructure. With the goal of immediately identifying, reducing, and eliminating DDoS attacks, these solutions come with a number of features and functionalities.

1) *Content Delivery Networks (CDNs:* Content Delivery Networks (CDNs) are distributed networks of servers that are positioned strategically throughout different parts of the world. By distributing content closer to end users, CDNs reduce latency and enhance performance, absorbing and mitigating DDoS attacks [2]. At the network's edge, CDNs are able to detect and filter malicious traffic during a DDoS attack, keeping it from getting to the target servers. For instance, if a DDoS attack targets an e-commerce website, a CDN can handle the attack traffic and provide users with cached content, guaranteeing continuous access to the website's resources.
2) *Cloud Scrubbing Centers:* In order to remove malicious packets from traffic before they enter the target network, cloud providers provide specialized scrubbing centers. To locate and stop DDoS attack traffic, these scrubbing centers use advanced traffic analysis methods like anomaly detection and deep packet inspection (DPI). Cloud-based DDoS mitigation solutions can effectively mitigate large-scale attacks while allowing legitimate traffic to reach its intended destination by rerouting traffic through these scrubbing centers [12]. For example, in the event of a volumetric DDoS attack against a financial institution, the cloud scrubbing center can detect and eliminate malicious traffic, guaranteeing that clients can continue to access online banking services.
3) *DDoS Protection Services:* Numerous cloud service providers provide comprehensive defense against a variety of DDoS attacks through their specialized DDoS protection services. Real-time monitoring, automated threat detection, and quick reaction times are frequently included in these services. DDoS protection services can minimize service disruption and guarantee continuous availability for authorized users by detecting and mitigating DDoS attacks in real time through the use of sophisticated algorithms and machine learning [16]. DDoS protection services, for instance, can recognize and stop malicious traffic patterns if a sophisticated application layer DDoS attack targets a gaming platform. This way, players can keep using the platform uninterrupted.

To summarize the above points, cloud-based DDoS mitigation solutions make use of the scalability, global reach, and sophisticated capabilities of cloud infrastructure to provide enterprises with strong defense mechanisms against DDoS attacks. With the proactive protection offered by these solutions, businesses can protect their online assets and continue to provide their services even in the face of persistent DDoS attack [17].

C. Successful Mitigation Strategies

1) *Proactive Monitoring and Response:* In order to prevent possible DDoS attacks in real time, organizations can proactively monitor their network traffic for indications of unusual activity and implement automated response mechanisms [13]. Through consistent traffic pattern monitoring and utilization of threat intelligence feeds, organizations can detect and eliminate DDoS threats prior to any negative impact on service availability.
2) *Cloud-based DDoS Mitigation Services:* Through the utilization of cloud providers' resources and expertise, cloud-based DDoS mitigation services provide resilient and scalable defense against DDoS attacks. These services are able to filter out malicious traffic and guarantee continuous access to online resources by rerouting traffic through scrubbing centers. Cloud-based DDoS mitigation services offer advanced threat detection capabilities and on-demand scalability that can be advantageous to organizations.
3) *Collaboration and Information Sharing:* To successfully mitigate DDoS attacks, cooperation between organizations, trade associations, and law enforcement agencies is necessary. Organizations can enhance their ability to detect and respond to DDoS attacks by pooling their threat intelligence, attack signatures, and mitigation strategies. Partnerships with cybersecurity companies and DDoS mitigation service providers can also improve an organization's ability to defend against DDoS attacks.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VI June 2024- Available at www.ijraset.com

XI. EMERGING TECHNOLOGIES

Below are the few technologies through which the DDoS attacks are spreading rapidly

1) *Artificial Intelligence and Machine Learning:* Through the analysis of network traffic patterns and the identification of anomalies suggestive of DDoS attacks, AI and machine learning technologies can improve DDoS detection and mitigation capabilities. These technologies make it possible to respond to changing threats more quickly and accurately.
2) *Software-defined networking, or SDN:* SDN gives enterprises the ability to manage their networks more dynamically and flexibly, rerouting traffic and allocating resources in real time to counteract DDoS attacks. Organizations can scale their defenses and adjust to evolving attack vectors with the aid of SDN.
3) *Blockchain-based Solutions:* By dividing up traffic management duties among a network of nodes, blockchain technology can offer a decentralized and impervious method of thwarting DDoS attacks. Blockchain-based systems can lower the possibility of single points of failure and increase resilience.

XII. CASE STUDIES AND EXAMPLES

Below are a few notable DDoSaaS Attacks.

1) *Mirai Botnet (2016):* One of the most well-known DDoS assaults in history, the Mirai botnet, used infected Internet of Things devices to launch massive DDoS attacks against targets like Dyn DNS, KrebsOnSecurity, and OVH. Millions of users' internet services were interrupted by these attacks, which also brought attention to the IoT devices' susceptibility to DDoSaaS platform exploitation.
2) *GitHub (2018):* The largest-known DDoS attack at the time was launched against GitHub in February 2018. The attack, which took place over several days, used a method known as memcached amplification and peaked at 1.35 Tbps. Even though the attack didn't cause much downtime for GitHub's infrastructure, it did highlight the increasing sophistication and size of DDoS attacks made possible by DDoSaaS platforms.
3) *Dyn DNS (2016):* A number of DDoS attacks were launched against Dyn DNS, a significant DNS service provider, in October 2016. Numerous websites and online services, such as Twitter, Netflix, and PayPal, were inaccessible due to the attacks. The destructive potential of DDoSaaS - based attacks was demonstrated by the attackers, who created a massive volume of traffic by using a botnet made up of IoT devices infected with the Mirai malware.

XIII. PREDICTIONS FOR THE FUTURE OF DDOSAAS

Navigating a landscape characterized by developing technology, cybersecurity defenses, and criminal inventiveness is necessary to predict the trajectory of DDoSaaS. One pattern that jumps out as we look ahead is the likely increase in sophistication. It is anticipated that DDoSaaS platforms will develop, providing ever-more sophisticated attack methods and evasion strategies to elude detection and mitigation initiatives. These platforms might dynamically adjust to defensive measures in real time with the integration of artificial intelligence and machine learning, presenting previously unheard-of challenges for cybersecurity experts [17]. The proliferation of Internet of Things (IoT) devices has resulted in an expanding attack surface, which is another noteworthy trend. The increasing number of interconnected devices offers DDoSaaS operators a wide range of possible targets to attack. Future distributed denial-of-service attacks could take advantage of compromised Internet of Things devices to build more powerful botnets that can launch catastrophic attacks worldwide [16]. This pattern emphasizes how crucial it is to secure IoT devices and put strong defenses in place in order to lessen the possibility of DDoS attacks utilizing IoT.

Moreover, attack vectors for DDoSaaS may become more varied in the future, going beyond conventional volumetric attacks to target vulnerabilities in the application layer. Attacks that target APIs, web applications, and other essential online service components can be more difficult to identify and stop, which puts organizations at serious risk. In order to protect against these dynamic threats, cybersecurity professionals need to stay alert and proactive as DDoSaaS platforms innovate and adapt. In order to handle the changing nature of DDoS attacks, this calls for the ongoing development of DDoS detection and mitigation technologies as well as industry stakeholder collaboration.

XIV. CONCLUSION

In conclusion, the landscape of DDoSaaS is expected to be complex and dynamic in the future, with evolving attack vectors, expanding attack surfaces, and rising levels of sophistication. Organizations need to modify their cybersecurity strategies in response to the ever-evolving cyber threats in order to reduce the risks associated with DDoS attacks. This entails making investments in cutting-edge technologies for detection and mitigation, protecting IoT devices, and encouraging industry stakeholders to work together to exchange threat intelligence and best practices.

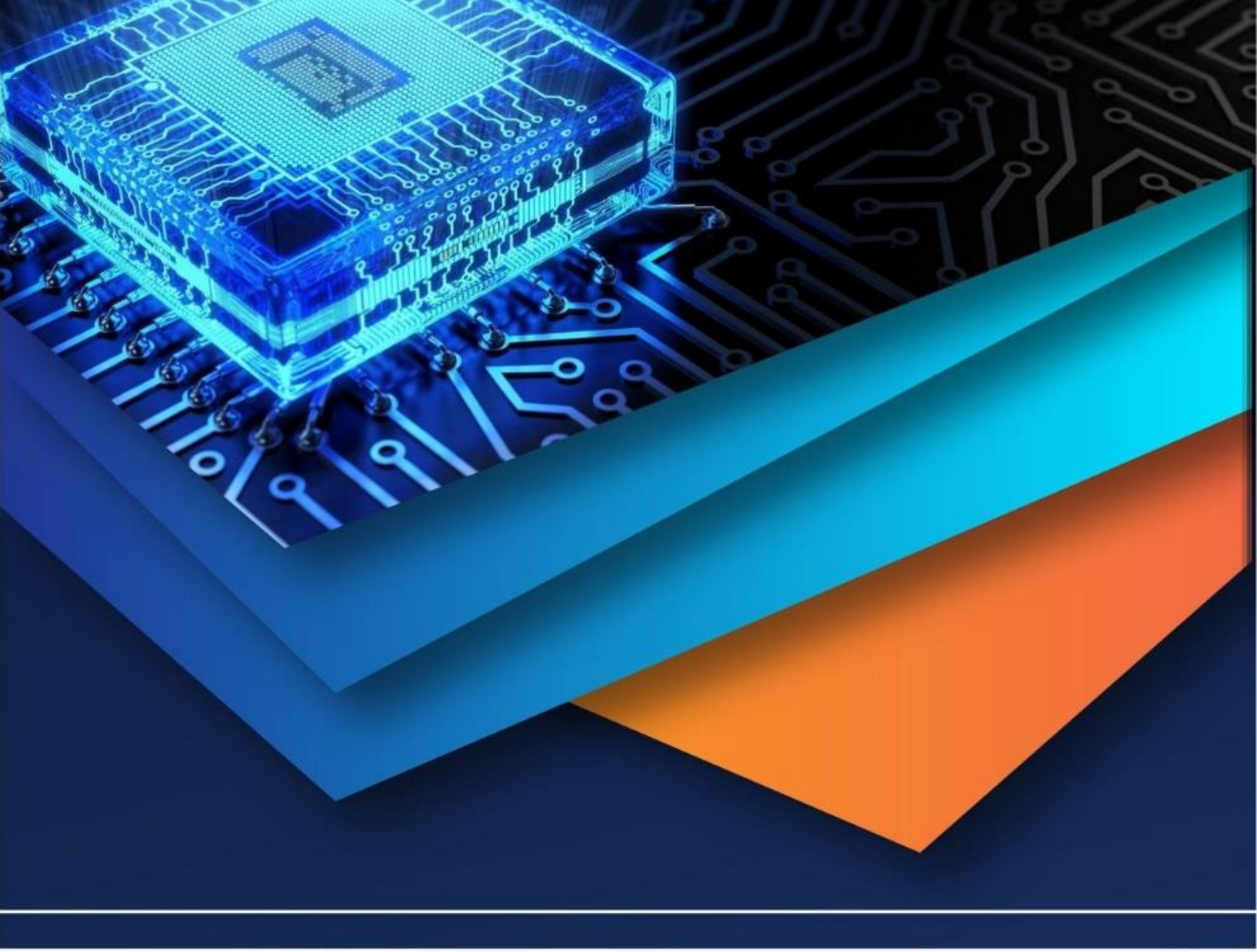
Law enforcement organizations and regulatory bodies also significantly contribute to the prevention of DDoS attacks by disrupting botnet infrastructure and enforcing stricter laws and penalties against DDoSaaS operators. In order to protect against the constantly changing threat landscape, defending against DDoS attacks ultimately necessitates a multifaceted strategy that incorporates technological innovation, proactive defense measures, and international cooperation.

XV. ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to all those who contributed to the completion of this review paper. Special thanks are due to our colleagues and classmates at Department of Master Of Computer Applications, KLS Gogte Institute of Technology, Belagavi Karnataka for their valuable insights and discussions that enriched this work.

REFERENCES

[1] Shi dong 1, Khushnood Abbas1 and Raj Jain2, (fellow, ieee), " A Survey on Distributed Denial of Service (ddos) Attacks in SDN and Cloud Computing Environments",2019
[2] Fadi SHAAR, Ahmet EFE, "DDoS Attacks and Impacts on various Cloud Computing Components", March 2018
[3] F. Lau; S.H. Rubin; M.H. Smith; L Trajkovic , "Distributed denial of service Attacks", Aug 2002
[4] Evan Cooke, Farnam Jahanian, Danny McPherson, "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets",2005
[5] Vít Bukač ,"Small scale denial of service attacks", 2015
[6] Vit Bukac, Vlasta Stavova, Lukas Nemec, Zdenek Riha & Vashek Matyas, "Service in Denial – Clouds Going with the Winds", 2015
[7] Michal Zak and J. Andrew Ware, "Cloud based Distributed Denial of Service Alleviation System",May 2020
[8] Jeroen van Kessel, Alexandros Stavroulakis, "Trusted Networks Initiative to combat DDoS attacks", April 2015
[9] Opeyemi Osanaiye a b, Kim-Kwang Raymond Choo b c, Mqhele Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework", 2016
[10] Narmeen Zakaria Bawany, Jawwad A. Shamsi & Khaled Salah, "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions", 2017
[11] Steve Mansfield-Devine (editor), "DDoS: threats and Mitigation", 2011
[12] Masoumeh Zareapoor, Pourya Shamsolmoali and M. Afshar Alam ,"Advance DDOS detection and mitigation technique for securing cloud", Jan 2018
[13] Preeti Daffu, Amanpreet Kaur, "Mitigation of DDoS attacks in cloud computing", July 2017
[14] Ashwini Khadke; Mangala Madankar; Manish Motghare "Review on mitigation of distributed Denial of Service (DDoS) attacks in cloud computing", 2016.
[15] Hardik Gulati; Aman Saxena; Neerav Pawar;Poonam Tanwar; Shweta Sharma, "Dark Web in Modern World Theoretical Perspective: A survey, 2022.
[16] Lubna Fayez Eliyan, Roberto Di Pietro "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges", 2021.
[17] Qing Li a, He Huang b a, Ruoyu Li c a, Jianhui Lv a,Zhenhui Yuan d, Lianbo Ma e, Yi Han f, Yong Jiang c a : A comprehensive survey on DDoS defense systems: New trends and challenges", Sept 2023
[18] Pankaj Sharma and Ankur Gupta "A Review of DDoS Attacks in Cloud Environment",2018.
[19] Junath Naseer Ahamed and N. Ch. S. N. Iyengar ,"A Review on Distributed Denial of Service (DDoS) Mitigation Techniques in Cloud Computing Environment", 2016
[20] R.Karthikeyani and E. Karthikeyan ,"A Review on Distributed Denial of Service Attack", Oct 2023.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY