International Journal of Multidisciplinary Research and Growth Evaluation

International Journal of Multidisciplinary Research and Growth Evaluation
ISSN: 2582-7138
Received: 28-06-2021; Accepted: 21-07-2021
www.allmultidisciplinaryjournal.com
Volume 2; Issue 4; July-August 2021; Page No. 897-903

Mitigating DDoS Attacks in Cloud Networks

Abhishek Singh
Independent Researcher, USA

Corresponding Author: **Abhishek Singh**

DOI: https://doi.org/10.54660/.IJMRGE.2021.2.4.897-903

Abstract

Distributed Denial of Service (DDoS) attacks represent a significant and growing threat to cloud networks, capable of causing extensive service disruptions and substantial financial and reputational damage. These attacks leverage multiple compromised devices to flood a target with malicious traffic, overwhelming its resources and rendering services unavailable to legitimate users. As cloud computing becomes increasingly integral to business operations, the need for effective DDoS mitigation strategies has never been more critical.

This paper delves into the multifaceted nature of DDoS attacks, categorizing them into volumetric, protocol, and application layer attacks, each with distinct characteristics and impacts. It examines the specific vulnerabilities of cloud networks to these attacks, highlighting the unique challenges posed by their distributed and scalable nature.

To combat these threats, a multi-layered approach to DDoS mitigation is essential. This includes traffic filtering and rate limiting to control the flow of traffic, anomaly detection and machine learning algorithms to identify and respond to attacks in real-time and leveraging the inherent scalability of cloud infrastructure to absorb and distribute attack traffic. Additionally, the use of Content Delivery Networks (CDNs) and specialized DDoS protection services can provide robust defenses against these attacks.

Looking ahead, the paper explores future advancements in DDoS mitigation, emphasizing the potential of AI-driven mitigation tools, blockchain technology for creating decentralized and tamper-proof networks, advanced threat intelligence for proactive defense, and enhanced collaboration between cloud service providers, security vendors, and organizations.

By providing a comprehensive understanding of DDoS attacks and the strategies to mitigate them, this research aims to equip organizations with the knowledge and tools necessary to protect their cloud networks. As DDoS attacks continue to evolve, staying ahead of these threats will require continuous innovation and adaptation in mitigation techniques.

Keywords: DDoS, cloud networks, mitigation, traffic filtering, anomaly detection, AI, Blockchain

Introduction

The rapid adoption of cloud computing has revolutionized the way businesses operate, offering unparalleled scalability, flexibility, and cost-efficiency. Cloud networks enable organizations to deploy and manage applications and services with ease, providing the foundation for digital transformation across various industries [4]. However, this shift to cloud-based infrastructure has also introduced new security challenges, with Distributed Denial of Service (DDoS) attacks emerging as one of the most significant threats.

DDoS attacks are designed to overwhelm a target's network, server, or application with a flood of malicious traffic, rendering it inaccessible to legitimate users. These attacks can cause severe disruptions, leading to service outages, financial losses, and damage to an organization's reputation. The distributed nature of cloud networks, while offering numerous advantages, also makes them particularly vulnerable to DDoS attacks. Attackers can exploit multiple entry points and leverage the scalability of cloud resources to amplify their attacks, making mitigation efforts more complex [2].

The impact of DDoS attacks on cloud networks can be devastating. Service outages can result in significant revenue loss, especially for businesses that rely on continuous online availability. Additionally, the reputational damage caused by prolonged downtime can erode customer trust and loyalty. The operational costs associated with mitigating and recovering from DDoS attacks can also be substantial, further highlighting the need for effective defense mechanisms [5].

To address these challenges, organizations must adopt a multi-layered approach to DDoS mitigation. This involves implementing a combination of strategies and technologies to detect, prevent, and respond to attacks. Traffic filtering and rate limiting can help control the flow of traffic and block malicious requests. Anomaly detection and machine learning algorithms can identify unusual traffic patterns and trigger automated responses to mitigate attacks in real-time. Leveraging the scalability of cloud infrastructure allows organizations to absorb and distribute attack traffic, maintaining service availability even during an attack. [6]

Content Delivery Networks (CDNs) play a crucial role in DDoS mitigation by distributing content across multiple servers, reducing the load on any single server and enhancing resilience against attacks. [7] Specialized DDoS protection services offer advanced mitigation techniques, such as traffic scrubbing and real-time monitoring, providing robust protection against sophisticated attacks.

As DDoS attacks continue to evolve in complexity and scale, future advancements in mitigation strategies will be essential. Integrating artificial intelligence (AI) and machine learning (ML) into DDoS mitigation tools can enhance the ability to detect and respond to attacks more effectively. Blockchain technology holds promise for creating decentralized and tamper-proof networks, improving the resilience of cloud infrastructure. Advanced threat intelligence can provide proactive defense by predicting and preventing attacks before they occur. Enhanced collaboration between cloud service providers, security vendors, and organizations can lead to the development of more comprehensive and effective DDoS mitigation strategies [8].

This paper aims to provide a comprehensive overview of DDoS attacks in cloud networks, exploring their nature, impact, and the strategies and technologies used for mitigation. By examining current methodologies and future advancements, this research seeks to equip organizations with the knowledge and tools necessary to protect their cloud infrastructure from DDoS threats. As cloud computing continues to play a pivotal role in modern business operations, ensuring the security and availability of cloud services will be critical to maintaining competitive advantage and driving innovation.

Nature of DDoS Attacks

Distributed Denial of Service (DDoS) attacks are a type of cyberattack where multiple compromised devices, often part of a botnet, are used to flood a target with an overwhelming volume of traffic. The primary goal of a DDoS attack is to disrupt the normal functioning of a network, service, or application, rendering it inaccessible to legitimate users. Understanding the nature of DDoS attacks involves examining their types, mechanisms, and the tactics used by attackers. [9]

Types of DDoS Attacks

DDoS attacks can be broadly categorized into three main types, each targeting different aspects of a network or service:

a) **Volumetric Attacks** Volumetric attacks aim to consume the target's bandwidth by generating a massive amount of traffic. These attacks are often measured in gigabits per second (Gbps) or packets per second (PPS). Common volumetric attacks include: [6]

- **UDP Floods**: Attackers send a large number of User Datagram Protocol (UDP) packets to random ports on the target, overwhelming its ability to process the traffic.
- **ICMP Floods**: Also known as Ping Floods, these attacks involve sending a high volume of Internet Control Message Protocol (ICMP) Echo Request packets to the target, consuming its bandwidth and processing power. [1]
- **DNS Amplification:** Attackers exploit misconfigured Domain Name System (DNS) servers to send amplified traffic to the target, significantly increasing the volume of the attack.

b) **Protocol Attacks** Protocol attacks exploit weaknesses in network protocols to exhaust server resources, such as CPU, memory, or connection tables. These attacks target the infrastructure layer and can disrupt the normal operation of network devices [10]. Common protocol attacks include:

- **SYN Floods:** Attackers send a large number of TCP/SYN packets to the target, initiating connections but never completing the handshake. This exhausts the target's connection table, preventing legitimate connections.
- **Ping of Death:** Attackers send malformed or oversized ICMP packets to the target, causing it to crash or become unresponsive.
- **Smurf Attack:** Attackers send ICMP Echo Request packets with the target's IP address as the source address to a network's broadcast address. The network's devices respond to the target, overwhelming it with traffic.

c) **Application Layer Attacks** Application layer attacks target specific applications or services, aiming to disrupt their functionality. These attacks are often more sophisticated and harder to detect, as they mimic legitimate user behavior. Common application layer attacks include:

- **HTTP Floods:** Attackers send a high volume of HTTP requests to a web server, overwhelming its ability to process the requests and causing it to become unresponsive. [35]
- **Slowloris:** Attackers open multiple connections to the target web server and send partial HTTP requests, keeping the connections open for as long as possible. This exhausts the server's resources and prevents it from handling legitimate requests [11].
- **DNS query floods:** Attackers send a large number of DNS queries to the target DNS server, overwhelming its capacity to respond and causing service disruption.

Mechanisms of DDoS Attacks

DDoS attacks typically involve the use of botnets, which are networks of compromised devices controlled by the attacker. These devices, often referred to as "zombies," can include computers, IoT devices, and other internet-connected devices. The attacker uses command and control (C&C) servers to coordinate the botnet and launch the attack [12].

The attack process generally follows these steps:

- **Recruitment:** The attacker infects devices with malware, turning them into bots that can be controlled remotely.
- **Coordination:** The attacker uses C&C servers to issue commands to the botnet, specifying the target and the type of attack.
- **Execution:** The bots simultaneously send traffic to the target, overwhelming its resources and causing a denial of service.

Tactics used by attackers

Attackers employ various tactics to maximize the impact of DDoS attacks and evade detection**:**

- **Reflection and Amplification:** Attackers use reflection techniques to hide the source of the attack and amplification techniques to increase the volume of traffic. For example, in a DNS amplification attack, the attacker sends small DNS queries with a spoofed source IP address (the target's IP) to open DNS resolvers, which then send large responses to the target. [13]
- **Multi-Vector Attacks:** Attackers combine multiple types of DDoS attacks to target different layers of the network simultaneously. This makes mitigation more challenging, as defenders must address multiple attack vectors at once.
- **Stealth and Evasion:** Attackers use techniques to evade detection and prolong the attack. For example, they may use low-and-slow attacks that generate low traffic volumes over an extended period, making it harder to detect the attack [14].

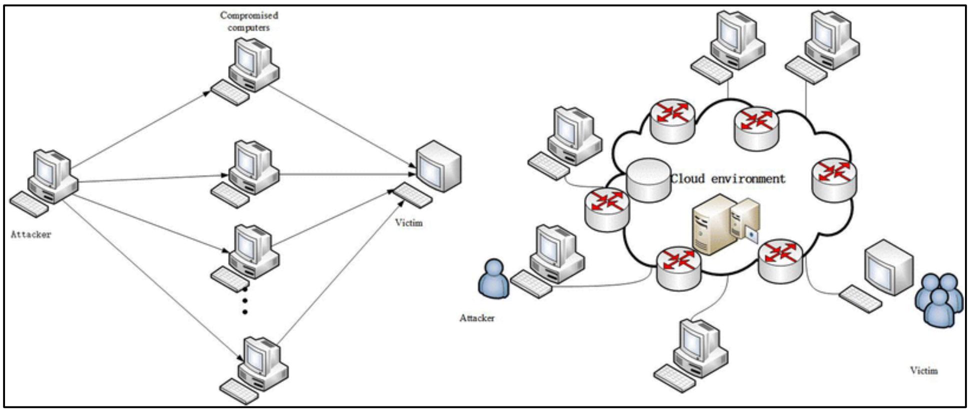

Fig 1: Traditional DDoS attack the DDoS attack in cloud environment [32]

Impact on cloud networks

Distributed Denial of Service (DDoS) attacks can have a profound and multifaceted impact on cloud networks. These attacks not only disrupt services but also lead to significant financial, operational, and reputational consequences. Understanding the specific impacts of DDoS attacks on cloud networks is crucial for developing effective mitigation strategies. [15]

a) Service disruptions and downtime

The most immediate and visible impact of a DDoS attack is the disruption of services. By overwhelming the target's network, server, or application with a flood of malicious traffic, DDoS attacks can render services unavailable to legitimate users. This downtime can be particularly damaging for businesses that rely on continuous online availability, such as e-commerce platforms, financial services, and online gaming providers. Prolonged service outages can lead to significant revenue loss and customer dissatisfaction. [16].

b) Financial Losses

DDoS attacks can result in substantial financial losses for affected organizations. These losses can stem from several sources:

- **Lost Revenue**: For businesses that generate revenue through online transactions, service outages can lead to lost sales and missed opportunities.
- **Mitigation Costs**: Implementing DDoS mitigation measures, such as traffic filtering, rate limiting, and employing specialized DDoS protection services, can incur significant costs. [17]
- **Recovery Costs**: After an attack, organizations may need to invest in additional resources to restore services, investigate the incident, and implement measures to prevent future attacks.
- **Operational Costs**: The increased workload on IT and security teams to manage and mitigate the attack can lead to higher operational expenses.

c) Reputational Damage

The reputational impact of a DDoS attack can be long-lasting and difficult to quantify. Customers and clients expect reliable and secure services, and a DDoS attack that results in prolonged downtime can erode trust and confidence. Negative publicity and media coverage of the attack can further damage an organization's reputation, leading to a loss of customers and potential business opportunities. Rebuilding trust and restoring a positive reputation can take considerable time and effort. [18]

d) Increased operational complexity

DDoS attacks add a layer of complexity to the operation and management of cloud networks. During an attack, IT and security teams must quickly identify the source and nature of the attack, implement mitigation measures, and monitor the network for any signs of ongoing or secondary attacks. This increased complexity can strain resources and divert attention from other critical tasks and projects.

e) Performance Degradation

Even if a DDoS attack does not completely disrupt services, it can still cause significant performance degradation. The increased traffic load can slow down response times, reduce the quality of service, and lead to a poor user experience. For applications that require high performance and low latency, such as real-time communication tools and online gaming, performance degradation can be particularly detrimental.

f) Security Vulnerabilities

DDoS attacks can expose underlying security vulnerabilities in cloud networks. Attackers may use DDoS attacks as a smokescreen to distract security teams while they attempt to exploit other vulnerabilities or gain unauthorized access to sensitive data. [19]The increased traffic and activity during an attack can also make it more challenging to detect and respond to other types of cyber threats.

g) Impact on cloud service providers

Cloud service providers (CSPs) are also affected by DDoS attacks on their customers. A large-scale attack on one customer can impact the shared infrastructure and affect other customers hosted on the same platform. CSPs must invest in robust DDoS mitigation measures to protect their infrastructure and ensure the availability and performance of their services. Failure to do so can lead to customer dissatisfaction and loss of business. [20]

h) Regulatory and compliance issues

In some industries, regulatory and compliance requirements mandate the availability and security of services. A DDoS attack that results in prolonged downtime or data breaches can lead to non-compliance with these regulations, resulting in fines, legal action, and increased scrutiny from regulatory bodies. Organizations must ensure that their DDoS mitigation strategies align with regulatory requirements to avoid potential penalties. [21]

i) Long-term strategic impact

The long-term strategic impact of DDoS attacks can influence an organization's approach to cybersecurity and risk management. Organizations may need to reassess their security posture, invest in additional resources and technologies, and develop more comprehensive incident response plans. The experience of a DDoS attack can also drive changes in organizational culture, emphasizing the importance of cybersecurity awareness and preparedness. [22]

Mitigation Strategies

Mitigating Distributed Denial of Service (DDoS) attacks in cloud networks requires a comprehensive, multi-layered approach that combines various strategies and technologies. [15] [34] Here are some key mitigation strategies:

a) Traffic filtering and rate limiting

- **Traffic Filtering:** Implementing traffic filtering mechanisms helps to block malicious traffic before it reaches the target. This can be achieved using firewalls, intrusion prevention systems (IPS), and access control lists (ACLs). These tools can filter traffic based on IP addresses, protocols, and other criteria to block known malicious sources.
- **Rate Limiting:** Rate limiting controls the flow of traffic by setting thresholds on the number of requests a server can handle within a specific time frame. This helps to prevent overwhelming the server with excessive requests. Rate limiting can be applied at various levels, including the network, application, and API levels.

b) Anomaly detection and machine learning

- **Anomaly Detection:** Anomaly detection systems monitor network traffic for unusual patterns that may indicate a DDoS attack. These systems use statistical analysis and behavioral modeling to identify deviations from normal traffic behavior. [23]
- **Machine Learning:** Machine learning algorithms can enhance anomaly detection by continuously learning from network traffic patterns and improving their ability to detect and respond to DDoS attacks in real-time. These algorithms can identify subtle changes in traffic that may be missed by traditional detection methods.

c) Scalable Infrastructure

- **Elastic Scaling:** Leveraging the scalability of cloud infrastructure allows organizations to absorb and distribute attack traffic. Cloud providers offer auto-scaling capabilities that automatically adjust the number of resources based on traffic load. This helps to maintain service availability during an attack by dynamically allocating additional resources to handle the increased traffic.
- **Load Balancing:** Load balancers distribute incoming traffic across multiple servers, preventing any single server from becoming overwhelmed. This helps to ensure that legitimate traffic can still access the service even during a DDoS attack.

d) Content Delivery Networks (CDNs)

CDNs distribute content across multiple geographically dispersed servers, reducing the load on any single server and enhancing resilience against DDoS attacks. By caching content closer to end-users, CDNs can absorb and mitigate the impact of volumetric attacks. Additionally, CDNs can provide built-in DDoS protection services that filter out malicious traffic before it reaches the origin server [7, 36].

e) DDoS Protection Services

Specialized DDoS protection services offer advanced mitigation techniques and real-time monitoring to protect against DDoS attacks. These services typically include:

- **Traffic Scrubbing:** Redirecting traffic through scrubbing centers that filter out malicious traffic and allow only legitimate traffic to reach the target.
- **Real-Time Monitoring:** Continuous monitoring of network traffic to detect and respond to DDoS attacks as they occur.
- **Threat Intelligence:** Leveraging global threat intelligence to identify and block known attack sources and patterns.

f) Redundancy and Failover

Implementing redundancy and failover mechanisms ensures that services remain available even if one component fails. This includes:

- **Geographic Redundancy:** Distributing resources across multiple geographic locations to prevent a single point of failure.
- **Failover Systems:** Automatically switching to backup systems or servers in the event of a failure, ensuring continuous service availability.

g) Network architecture design

Designing a resilient network architecture can help mitigate the impact of DDoS attacks. Key considerations include:

- **Segmentation:** Dividing the network into smaller segments to contain the impact of an attack and prevent it from spreading.
- **Defense in Depth:** Implementing multiple layers of security controls to protect against different types of attacks.
- **Zero Trust Model:** Adopting a zero-trust security model that requires verification for every request, regardless of its origin. [24].

h) Regular testing and drills

Regularly testing DDoS mitigation strategies and conducting drills can help organizations prepare for real-world attacks. This includes:

- **Simulated Attacks:** Conducting simulated DDoS attacks to test the effectiveness of mitigation measures and identify areas for improvement. [25]
- **Incident response drills:** Practicing incident response procedures to ensure that teams are prepared to respond quickly and effectively during an actual attack.

i) Collaboration and information sharing

Collaboration between cloud service providers, security vendors, and organizations can enhance DDoS mitigation efforts. Sharing information about attack patterns, threat intelligence, and best practices can help organizations stay ahead of evolving threats.

j) Advanced threat intelligence

Leveraging advanced threat intelligence can provide proactive defense against DDoS attacks. This includes:

- **Predictive Analytics:** Using predictive analytics to identify potential attack vectors and take preventive measures.
- **Threat Hunting:** Actively searching for signs of potential threats within the network to identify and mitigate attacks before they occur.

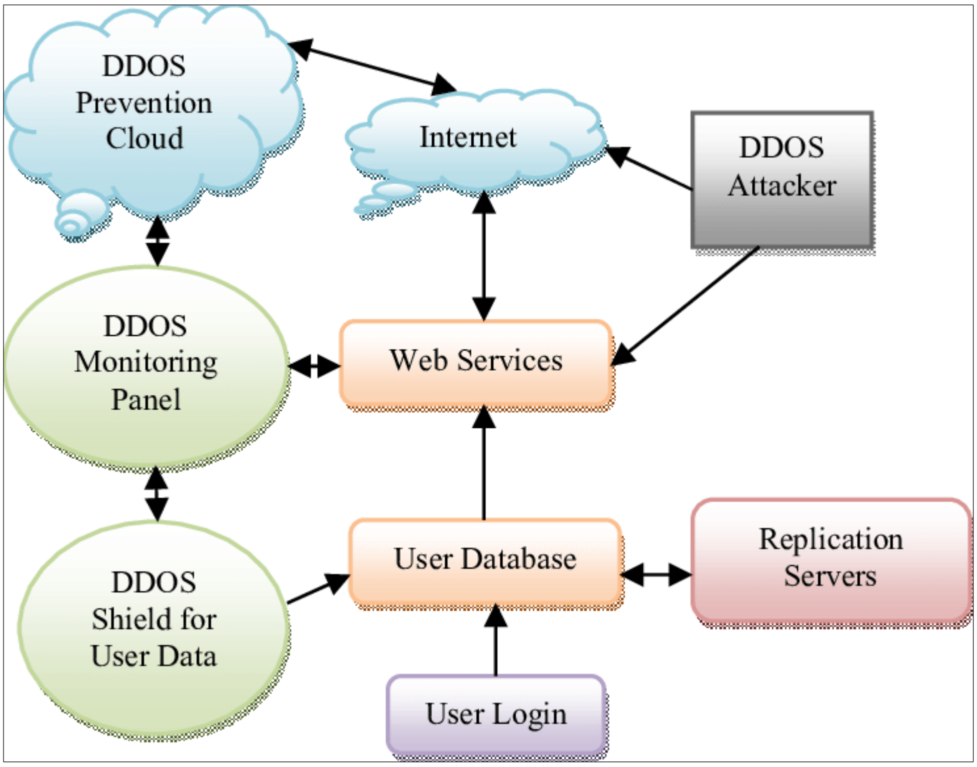

Fig 2: Model for Controlling DDOS Attack on Cloud Computing [33]

Future Advancements

As DDoS attacks continue to evolve in complexity and scale, future advancements in mitigation strategies will be essential to stay ahead of these threats. [15] Some potential areas of development include:

AI-Driven Mitigation

Integrating artificial intelligence (AI) and machine learning (ML) into DDoS mitigation tools can significantly enhance the ability to detect and respond to attacks in real-time. AI and ML algorithms can analyze vast amounts of network traffic data to identify patterns and anomalies that may indicate a DDoS attack. These technologies can also adapt and improve over time, learning from past attacks to better predict and mitigate future threats. By automating the detection and response process, AI-driven mitigation can reduce the time it takes to identify and neutralize DDoS attacks, minimizing their impact on cloud networks [26].

Blockchain Technology

Using blockchain technology to create decentralized and tamper-proof networks can help improve the resilience of cloud networks against DDoS attacks. Blockchain's distributed ledger system can enhance security by eliminating single points of failure and making it more difficult for attackers to disrupt network operations. Additionally, blockchain can be used to verify the authenticity of network traffic, ensuring that only legitimate requests are processed. This decentralized approach can provide a robust defense against DDoS attacks, making it harder for attackers to achieve their objectives [27].

Advanced threat intelligence

Leveraging advanced threat intelligence to predict and prevent DDoS attacks before they occur can provide a proactive approach to mitigation. Threat intelligence platforms can collect and analyze data from various sources, including global threat databases, to identify emerging threats and attack patterns. By integrating this intelligence into DDoS mitigation strategies, organizations can anticipate potential attacks and take preventive measures to protect their cloud networks. Advanced threat intelligence can also help organizations stay informed about the latest attack techniques and trends, enabling them to continuously update and improve their defenses [28].

Enhanced Collaboration

Promoting collaboration between cloud service providers, security vendors, and organizations can help develop more effective and comprehensive DDoS mitigation strategies. By sharing information about attack patterns, threat intelligence, and best practices, stakeholders can work together to enhance their collective defenses. Collaborative efforts can also lead to the development of industry standards and guidelines for DDoS mitigation, ensuring a consistent and coordinated response to attacks. Enhanced collaboration can foster a more resilient and secure cloud ecosystem, where organizations can benefit from shared knowledge and resources.

Conclusion

Mitigating Distributed Denial of Service (DDoS) attacks in cloud networks is a critical and ongoing challenge that requires a comprehensive, multi-layered approach. As cloud computing continues to play an integral role in modern business operations, the need for robust DDoS mitigation strategies has never been more urgent. [29]

This paper has explored the nature of DDoS attacks, highlighted their various types and mechanisms, and examined the significant impact these attacks can have on cloud networks. From service disruptions and financial losses to reputational damage and increased operational complexity, the consequences of DDoS attacks are far-reaching and multifaceted.

To effectively combat these threats, organizations must implement a combination of mitigation strategies, including traffic filtering, rate limiting, anomaly detection, machine learning, scalable infrastructure, content delivery networks (CDNs), specialized DDoS protection services, redundancy, resilient network architecture, regular testing, and enhanced collaboration. Each of these strategies plays a vital role in ensuring the security, availability, and performance of cloud services [30].

Looking ahead, future advancements in DDoS mitigation will be essential to stay ahead of evolving threats. Integrating artificial intelligence (AI) and machine learning (ML) into mitigation tools, leveraging blockchain technology for decentralized and tamper-proof networks, utilizing advanced threat intelligence for proactive defense, and promoting enhanced collaboration between stakeholders are key areas of development that hold promise for the future [31].

References

1. Chang RKC. Defending against flooding-based distributed denial-of-service attacks: a tutorial. IEEE; 2002 Oct 01. doi: 10.1109/mcom.2002.1039856.
2. Somani G, Gaur MS, Sanghi D, Conti M, Rajarajan M, Buyya R. Combating DDoS attacks in the cloud: requirements, trends, and future directions. IEEE; 2017 Jan 01. doi: 10.1109/mcc.2017.14.
3. Swami R, Dave M, Ranga V. Software-defined networking-based DDoS defense mechanisms. ACM Comput Surv. 2019 Apr 09;52(2):1. doi: 10.1145/3301614.
4. Khan S, Almogren A, Alajmi MF. Using cloud computing to improve network operations and management. IEEE; 2015 Feb 01. doi: 10.1109/nsitnsw.2015.7176418.
5. Gupta BB, Joshi RC, Misra M. Distributed denial of service prevention techniques. Cornell University; 2012 Jan 01. doi: 10.48550/arXiv.1208.
6. Huyn J. A scalable real-time framework for DDoS traffic monitoring and characterization. ACM; 2017 Dec 01. doi: 10.1145/3148055.3149205.
7. Wang D, Chen D, Guo R. DDoS mitigation in content distribution networks. Inderscience Publishers; 2013 Jan 01. doi: 10.1504/ijwmc.2013.057397.
8. Somani G, Gaur MS, Sanghi D, Conti M, Buyya R. DDoS attacks in cloud computing: issues, taxonomy, and future directions. Comput Commun. 2017 Mar 31;107:30–50. doi: 10.1016/j.comcom.2017.03.010.
9. Bhuyan MH, Kashyap HJ, Bhattacharyya DK, Kalita J. Detecting distributed denial of service attacks: methods, tools, and future directions. Comput J. 2013 Mar 28;56(1):13–29. doi: 10.1093/comjnl/bxt031.
10. Tariq U, Hong M, Lhee K. A comprehensive categorization of DDoS attack and DDoS defense techniques. Lect Notes Comput Sci. 2006;4060:1025–34. doi: 10.1007/11811305_112.
11. Mitigating Slowloris. 2009 Jul. Available from: https://insights.sei.cmu.edu/blog/mitigating-slowloris/
12. Vormayr G, Zseby T, Fabini J. Botnet communication patterns. IEEE Commun Surv Tutor. 2017 Jan 01;19(1):1–16. doi: 10.1109/comst.2017.2749442.
13. MacFarland DC, Shue CA, Kalafut AJ. The best bang for the byte: characterizing the potential of DNS amplification attacks. Comput Netw. 2017 Feb 16;116:83–97. doi: 10.1016/j.comnet.2017.02.007.
14. Rudd EM, Rozsa A, Günther M, Boult TE. A survey of stealth malware attacks, mitigation measures, and steps toward autonomous open world solutions. IEEE Commun Surv Tutor. 2016 Dec 08;18(4):2627–42. doi: 10.1109/comst.2016.2636078.
15. Darwish M, Ouda A, Capretz LF. Cloud-based DDoS attacks and defenses. Cornell University; 2015 Jan 01. doi: 10.48550/arXiv.1511.
16. Matsukawa T, Hiroyuki F, Koshiji K. Evaluating downtime and maintenance time in communication networks. IEEE; 2011 Jan 01. doi: 10.1109/rams.2011.5754491.
17. Verisign Inc. DDoS cost analysis. 2012 May. Available from: https://verisigninc.com/assets/whitepaper-ddos-costanalysis.pdf
18. Horn IS, et al. Business reputation and social media: a primer on threats and responses. Springer Science+Business Media; 2015 Jan 01. doi: 10.1057/dddmp.2015.1.
19. Devi BSK, Subbulakshmi T. DDoS attack detection and mitigation techniques in cloud computing environment. IEEE; 2017 Dec 01. doi: 10.1109/iss1.2017.8389464.
20. Ku C, Chen TC. The risk management strategy of applying cloud computing. Int J Adv Comput Sci Appl. 2012 Jan 01;3(9):38–45. doi: 10.14569/ijacsa.2012.030903.
21. Duncan B, Zhao Y. Risk management for cloud compliance with the EU General Data Protection Regulation. 2018 Jul 01. doi: 10.1109/hpcs.2018.00109.
22. Zeb K, Baig O, Asif M. DDoS attacks and countermeasures in cyberspace. IEEE; 2015 Mar 01. doi: 10.1109/wswan.2015.7210322.
23. Cha B, Kim J. Study of multistage anomaly detection for secured cloud computing resources in future internet. In: DASC; 2011 Dec 01. p. 1–6. doi: 10.1109/dasc.2011.171.
24. Rose S, Borchert O, Mitchell S, Connelly S. Zero Trust

Architecture. NIST Special Publication 800-207; 2020 Aug. doi: 10.6028/nist.sp.800-207.

25. Mirković J, et al. Testing a collaborative DDoS defense in a red team/blue team exercise. IEEE; 2008 Jun 24. doi: 10.1109/tc.2008.42.
26. Atasever S, Özçelik İ, Sağıroğlu Ş. An overview of machine learning based approaches in DDoS detection. IEEE; 2020 Oct 05. doi: 10.1109/siu49456.2020.9302121.
27. Park J, Park JH. Blockchain security in cloud computing: use cases, challenges, and solutions. Symmetry. 2017 Aug 18;9(8):164. doi: 10.3390/sym9080164.
28. One in five firms hit by APTs. 2014 Jul 01. Elsevier BV. doi: 10.1016/s1353-4858(14)70065-0.
29. Carlin AP, Hammoudeh M, Aldabbas O. Defence for distributed denial of service attacks in cloud computing. Comput Sci. 2015 Jan 01;56:42–8. doi: 10.1016/j.procs.2015.12.037.
30. Albugmi A, Alassafi MO, Walters RJ, Wills G. Data security in cloud computing. IEEE; 2016 Aug 01. doi: 10.1109/fgct.2016.7605062.
31. Fraley JB, Cannady J. The promise of machine learning in cybersecurity. IEEE; 2017 Mar 01. doi: 10.1109/secon.2017.7925283.
32. Wang C, Yao H, Liu Z. An efficient DDoS detection based on SU-Genetic feature selection. Cluster Comput. 2019;22:2505–15. doi: 10.1007/s10586-018-2275-z.
33. Ahmed A, Ahmed H. A proposed model for controlling distributed denial of service attack on cloud computing. In: 2019 Int Conf Eng Emerg Sci Technol. 2019;1–4.
34. Yu S, Tian Y, Guo S, Wu D. Can we beat DDoS attacks in clouds? IEEE Trans Parallel Distrib Syst. 2014 Sep;25(9):2245–54. doi: 10.1109/TPDS.2013.291.
35. Zargar ST, Joshi J, Tipper D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun Surv Tutor. 2013;15(4):2046–69. doi: 10.1109/SURV.2013.031413.00127.
36. Almusawi AA, Al-Kadhemy MA, Al-Husseini AA. A survey of DDoS attacks and defenses in cloud systems. In: 2018 Int Conf Adv Sci Eng (ICOASE); Duhok, Iraq; 2018. p. 1–6. doi: 10.1109/ICOASE.2018.8548919.