Securing Cloud Networks: A Comprehensive Exploration of DDoS Threats and Proactive Countermeasures

Okoye Emeka Elvis
40274904
Montreal, Canada
emeka.okoye@mail.concordia.ca

Abstract—**With the exponential growth of cloud computing, the security of cloud networks has become a critical concern, particularly in the face of Denial of Service (DoS) attacks. These attacks can cause significant damage to cloud networks, leading to data loss, service disruption, and other negative consequences. In this paper, we explore the various DDoS threats that cloud networks face and provide proactive countermeasures to mitigate these threats. Our research is based on a comprehensive analysis of existing literature and case studies. We begin by providing an overview of cloud networks and their growing importance in today's world. We then discuss the various security threats that cloud networks face, with a particular focus on DoS attacks. We analyze the evolving nature of these attacks and their potential impact on cloud networks. Our research methodology involves a survey of existing countermeasures, and the development of novel strategies to mitigate the ever-growing sophistication of attacks. By adopting a multi-layered approach to security, cloud networks can be made more resilient to DoS attacks.**

Index Terms—**cloud computing, denial of service, attacks, countermeasures**

I. Introduction

In an era characterized by unprecedented digital transformation, the adoption of cloud computing stands as a pivotal enabler, revolutionizing the landscape of information technology. Cloud networks have emerged as the backbone of modern business operations, offering unparalleled flexibility, scalability, and accessibility [20]. This paradigm shift allows organizations to transcend the constraints of traditional on-premises infrastructures, ushering in an era where computational power and storage are commoditized resources readily available on demand. The reliance on cloud networks is testament to their transformative impact, offering a wide range of services that range from enterprise applications to data storage and processing [5]. The agility afforded by cloud infrastructures has become the linchpin for innovation, empowering businesses to rapidly deploy and scale their operations in response to dynamic market demands. Yet, as organizations increasingly rely on the cloud to streamline their operations and gain a competitive edge, the security of these virtualized environments becomes paramount. One of the biggest threats we face is Denial of Service (DoS) attacks, which can disrupt the digital ecosystem we depend on [3]. My research aims to explore the complex relationship between cloud networks and DoS threats. Cloud environments, with their shared resources and distributed architectures, present unique security challenges. Protecting these infrastructures from DoS attacks is not just an academic exercise; it's essential for the resilience and functionality of the digital services we rely on. In this study, I explored the intersection of cloud computing and DoS threats, highlighting the vulnerabilities in cloud networks. The goal is to understand these threats and develop solutions to protect the integrity and availability of cloud-based services. Remember, behind every line of code and every server, there's a community of users, businesses, and communities depending on the reliability and security of cloud networks. In the following pages, we'll delve into the complexities of DoS threats in cloud environments, looking at

Identify applicable funding agency here. If none, delete this.

past attack vectors, emerging trends, and proactive countermeasures.

II. Background of Study

The intricate dance between cloud computing and the ever-evolving threat landscape of Denial of Service (DoS) attacks has been punctuated by historical incidents that underscore the urgency of our research [3]. As cloud networks have ascended to become the backbone of contemporary IT infrastructures, they have not been immune to the disruptive forces of DoS attacks. In recent years, we've seen high-profile DoS incidents cast a shadow over the reliability of cloud-based services. These incidents, orchestrated by malicious actors, have caused widespread service disruptions and exposed the vulnerabilities inherent in shared, virtualized environments [4]. These confrontations with DoS threats have not only revealed the fragility of cloud networks but have also sparked a collective response from the cybersecurity community. The countermeasures have been as dynamic and adaptive as the attacks themselves, reflecting an ongoing battle between those seeking to disrupt and those working tirelessly to protect our digital infrastructure. In response to past DoS incidents, industry leaders and security experts have developed innovative approaches to mitigate these threats [20]. From deploying advanced intrusion detection and prevention systems to designing resilient network architectures, each countermeasure is a testament to the collaborative spirit of the cybersecurity community. Cloud service providers, aware of their shared responsibility for security, have also invested heavily in refining their infrastructure and implementing sophisticated traffic filtering mechanisms [5]. Yet, behind the technical strategies and deployments lies a human element—a collective determination to protect the digital experiences of businesses and individuals alike. The aftermath of each DoS incident serves as a stark reminder of the real-world implications, from disrupted e-commerce transactions impacting businesses to the temporary loss of vital online services affecting individuals worldwide [21]. As we navigate the historical landscape of DoS threats in the context of cloud computing, our research aims to learn from these past encounters. By scrutinizing the efficacy of previous countermeasures, we seek to understand the evolving tactics of malicious actors and to develop proactive and adaptive strategies that resonate with the human imperative to ensure the continuous, secure functioning of cloud-based services [6]. The pages ahead unfold as a synthesis of technical acumen and human resilience, charting a course towards a future where cloud networks stand resilient against the tide of DoS disruptions.

III. Common Denial of Service (DoS) Cloud Attacks

Distributed Denial of Service (DDoS) attacks on cloud computing involve malicious efforts to disrupt the availability and functionality of cloud-based services by overwhelming them with a flood of traffic. Cloud networks, with their shared resources and dynamic scalability, are particularly susceptible to DDoS threats. DDoS attacks on cloud environments can take various forms, including volumetric attacks that flood the network with traffic, protocol attacks that exploit vulnerabilities in network protocols, and application layer attacks that target specific applications or services. The motives behind these attacks range from financial extortion and hacktivism to competitive rivalry and ideological agendas. The impact of DDoS attacks on cloud services can be severe, leading to service downtime, financial losses, damage to reputation, and disruption of critical business operations.

In their research, Saman et al. [1] talks about HTTP flooding attacks and highlights 2 main modes, HTTP GET flood and HTTP POST flood attack. As explained in the paper, in HTTP GET flood, the attacker attempts to receive a large amount of data using get request from the server, the request then attempts to download large files such as images or scripts from the web server, while in HTTP post flood attack, its explained that the attacker is looking for forms in the target website, by using the form parameters, the attacker creates an HTTP post attack on the website by sending a large amount of data and a large amount of post request mimicking legitimate forms sent by legitimate users. This research provides valuable data into the mechanisms of HTTP flooding attacks, shedding light on the strategies employed by attackers and the potential vulnerabilities of the web.

In [2], Saravanan et al. describes another form of denial-of-service attack on cloud systems called the SMURF attack, Saravanan in their paper discussed the SMURF attack and states its an attack where the attacker pings on a network with the spoofed IP address of the victim as source address to flood the victim with replies. He explained that the attack takes 3 forms, first the attacker identifies a victim IP address (most likely a server), then the attacker sends an ICMP ECHO REQUEST at the broadcast address of the network. These packets have the source IP address spoofed to point towards the victim. The hosts' ICMP ECHO RESPONSE on the network will then be directed on the target's victim IP address.

A Session Initiation Protocol (SIP) flood attack is presented in [3]. The authors explained in their paper that the attack makes use of the SIP protocol which is a standard for call set-up in Voice-over IP (VoIP), the protocol often using SIP proxy servers. These servers need internet access to accept call set-up requests. To handle a lot of calls at once, SIP usually works with another protocol called UDP. Unlike some other protocols, UDP doesn't remember past interactions, which makes it faster and more scalable. The papers go into the attack by stating how the attacker can send a bunch of fake call requests, known as SIP INVITE packets, to the SIP proxy. The server gets tricked into thinking these are real calls from different sources and gets overwhelmed. The papers states that the attack hurts 2 main groups, First, the SIP proxy servers get overwhelmed and run out of resources because they're busy processing all these fake call requests and second, the people trying to receive calls have a hard time telling real calls from fake ones.

Yang Xiao et al. [4] in their paper discusses the LAND dos attack which is a layer 4 denial of service attack that plays with the source and destination details in a specific kind of message. The paper manages to go into the details of the attack stating the source and destination addresses in the crafted message points to the same computer. So, when the computer gets this confusing message, it starts replying to itself, like sending a letter to its own address. This back-and-forth goes on forever, making the computer work so hard that it gets overwhelmed and freezes up, or in some cases, crashes entirely.

The Slowloris attack as presented by [5] in their paper, outlined the basic process of the attack. The attack sends HTTP requests without the necessary termination sequence, it then tricks the web server into keeping connections open, tying up resources meant for quickly terminated connections. According to the paper, Slowloris capitalizes on this by spamming the server with countless uncompleted requests over several minutes. With no requests being terminated, it exhausts the available connection resources, leading the server to cease handling new requests and denying legitimate users access to the service.

And finally, in [6], the paper presents a well-known form of Denial of Service (DoS) attack known as amplification attacks. This form of attack allows the attacker to generate a substantial volume of traffic with minimal request (response is almost 100x the request). This attack primarily works by the attacker spoofing its IP address to the victims IP address, diverting server responses meant for the attacker to the targeted victim system. According to the paper, the type of attack exploits the broadcast address feature found in most of the routers and switches in almost every networking environment.

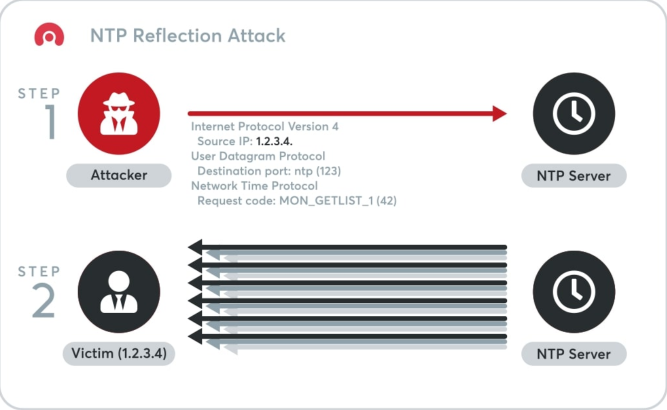


Fig. 1. Image of an NTP Reflection Attack on a victim [22]

IV. DOS MITIGATION AND PREVENTION TECHNIQUES

Cloud Denial of Service (DoS) mitigation and prevention strategies are designed to harden cloud environments against attackers seeking to overwhelm resources and compromise service availability. These mitigations cover a range of techniques outlined in

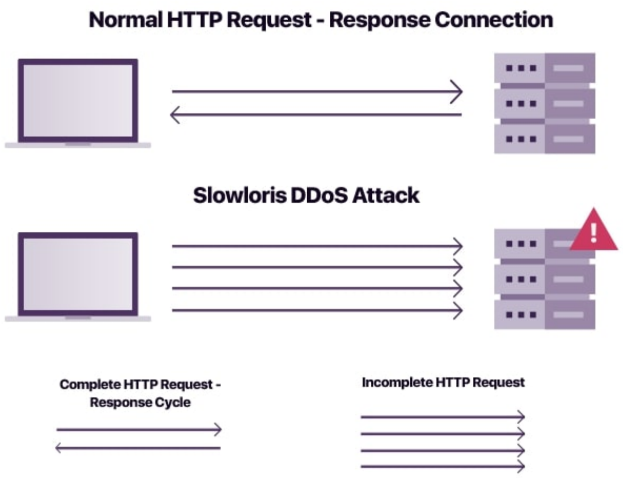

Normal HTTP Request - Response Connection
Slowloris DDoS Attack
Complete HTTP Request - Response Cycle
Incomplete HTTP Request

Fig. 2. Image of a slow loris DDOS attack [23]

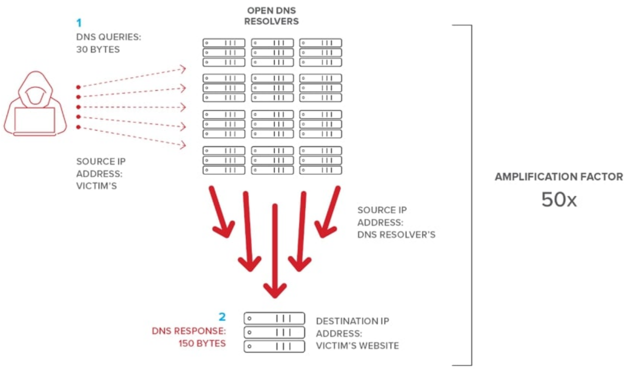

1
DNS QUERIES: 30 BYTES
OPEN DNS RESOLVERS
SOURCE IP ADDRESS: VICTIM'S
SOURCE IP ADDRESS: DNS RESOLVER'S
AMPLIFICATION FACTOR
50x
2
DNS RESPONSE: 150 BYTES
DESTINATION IP ADDRESS: VICTIM'S WEBSITE

Fig. 3. Image of a DNS Amplififcation Attack [24]

some research papers below. Together, these techniques form a proactive and adaptive approach, bolstering the resilience of cloud environments against a spectrum of Denial-of-Service threats. John et al. [7] in their paper, presented an in-depth examination of a system "Pushback" system, specifically designed for integration into core routers under FreeBSD. The paper mentioned that the systems main strength lies in its proficient management of Distributed Denial of Service attacks (DDoS) attacks, which it treats as congestion control issue. In response to these attacks, the system identifies and mitigates the traffic aggregates causing the initial congestion. The research not only underscores the efficacy of the "Pushback" system but also paves the way for its strategic implementation within real-world operational settings.

Lu Zhou et al. [8] in their paper, aimed to differentiate between two common types of low-rate Distributed Denial of Service (DDoS) attack: pulsing attacks and constant attacks. Their investigation lies in the use of a measurement called packet size expectation (ESP), which is derived from the variance in packet sizes. The research starts with experimental insights from legitimate dataset sampled at various times, revealing that the EPS of legitimate traffic remains significant and stable. The research then goes into experimentations of two typical low-rate DDoS attack on traffics, and it highlights that, when assessed against the ESP metric, the packet sizes linked to the attacks are notable small and limited.

The research [9] presents a novel anomaly detection technique for pinpointing Distributed Denial of Service attacks utilizing the Gini Coefficient. This method effectively identifies and mitigates DDoS threats by examining the variations in distributions of source IP addresses and destination port relative to destination IP address. According to the paper, the Gini Coefficient is employed as a metric to quantify the fluctuations in packet attribution distributions during attacks. The paper then builds on this with an enhanced TCM-KNN algorithm which is used to detect attacks by classifying Gini coefficient samples extracted from real-time network traffic.

In their paper, Jisa et al. [10] suggest the use of Fast Entropy method as a powerful and efficient tool for detecting Distributed Denial of Service attacks. The approach involves examining the flow count for each connection within specific time intervals. It's was discovered in the paper, that when a connection has a significantly higher flow count than others in a given time frame, the Fast Entropy value is considerably lower. The detection mechanism as found out by the paper, relies on the average entropy value within a set time interval exceeding a certain threshold. Furthermore, a DDoS attack is identified when there is a noticeable difference in entropy across individual instances of flow count.

Alan et al. [11] in their paper presents an artificial neural network detection engine, specifically designed to identify both known and unknown attacks within legitimate network traffic. Through careful pattern selection, informed by rigorous experimentation and data analysis, the system effectively distinguishes between authentic and Distributed Denial of Service (DDoS) packets. According to the paper, the evaluation process incorporates the detection of TCP, UDP, and ICMP attacks, with a meticulous consideration of accuracy, sensitivity, specificity, and precision. The learning phase involves replicating real-world scenarios by launching diverse DDoS assaults alongside regular traffic. Training datasets are meticulously pre-processed using JNNS. Rigorous testing against both known and unknown assaults illustrates the detection mechanism's seamless integration with Snort-AI.

The paper in [12], presents the Distributed Denial-of-Service Detection Mechanism (DiDDeM), an advanced system designed for early detection of denial-of-service attacks. DiDDeM utilizes a two-tier detection approach, beginning with Pre-filters (PFs) that scrutinize traffic for potential threats. This initial filtering applies routing congestion techniques to both stateful and stateless signatures. Following this, command and control (C2) servers provide a responsive strategy for containing attacks within the routing infrastructure, promoting cooperation both within and between domains. DiDDeM takes advantage of congestion techniques already used by routers to optimize traffic analysis and derive stateful information about traffic flows. It also incorporates stateless signatures into the detection process. The study highlights DiDDeM's adaptability in scenarios involving high-speed, high-volume networks, a feature validated through extensive studies focusing on TCP SYN floods.

Danlu et al. [13], in their paper proposed a user friendly and reliable method for detecting SYN flooding attacks, specifically aimed at leaf routers that connect end hosts to the internet. Unlike firewalls or servers, their approach focused on leaf routers to detect the SYN flood attacks. Their detection technique exemplifies sequential change point detections and hinges on the analysis of TCP SYN-FIN (RST) pairings. They accomplished this by utilizing a non-parametric Cumulative Sum (CUSUM) algorithm, ensuring the detection mechanism is location agnostic and adaptable to various access patterns, enhancing its broad applicability.

The authors [14], in their paper utilize the statistical discrete wavelet transform to examine the option fields of traffic stream identifiers, internet timestamps, records of data transmission routes, and the flags linked with loose and strict source routing. Some attacks are immediately recognizable, appearing as one or more packets operating within a short time span (for example, less than one second). On the other hand, some attacks last for longer periods, spanning hours, days, or even weeks, and may only be identified as attacks when examining a large collection of event records collectively

Eray et al. [15] presents an innovative approach that uses packet header information to identify backscatter Distributed Denial of Service (DDoS) traffic. The effectiveness of various learning classifiers, trained on both regular and darknet traffic traces over multiple years, is systematically evaluated. Criteria for evaluation include the rate of attack detection, false alarm rate, and computational cost. The study uses four distinct training sets and feature sets to thoroughly assess the performance of the proposed method. In addition to the decision tree classifier, two widely used feature selection algorithms, Chi-Square and Symmetrical Uncertainty, are utilized. Their paper demonstrates the feasibility of creating a robust detection system capable of adapting to the evolving behaviors of Backscatter DDoS over time.

In [16], the research presented a method aimed on the packet Inter-Arrival Time (IAT) rate, leveraging both the Cumulative Sum (CUSUM) algorithm and the Flow-Based Classifier to effectively detect cloud Distributed Denial of Service (DDoS) flooding attacks. Their strategy was put to the test using trace-driven tests, where they applied it to detect changes within traffic flows, including both legitimate and attack packets. Their approach was tested on two datasets, a normal traffic trace from Auckland-VIII and flooding attacks from the CAIDA DDoS benchmark dataset.

Ahmed et al. [17] in their paper proposed an innovative approach that combines the Consistency Subset Evaluation (CSE) and DDoS Characteristic Features (DCF) algorithms to identify and select the most significant and relevant features associated with Distributed Denial of Service (DDoS) attacks. Their method was trained and evaluated using the NSL-KDD 2009 dataset, providing a unique contrast to traditional feature selection methods such as Information Gain, Gain Ratio, Chi-squared, and Correlated Features Selection (CFS).

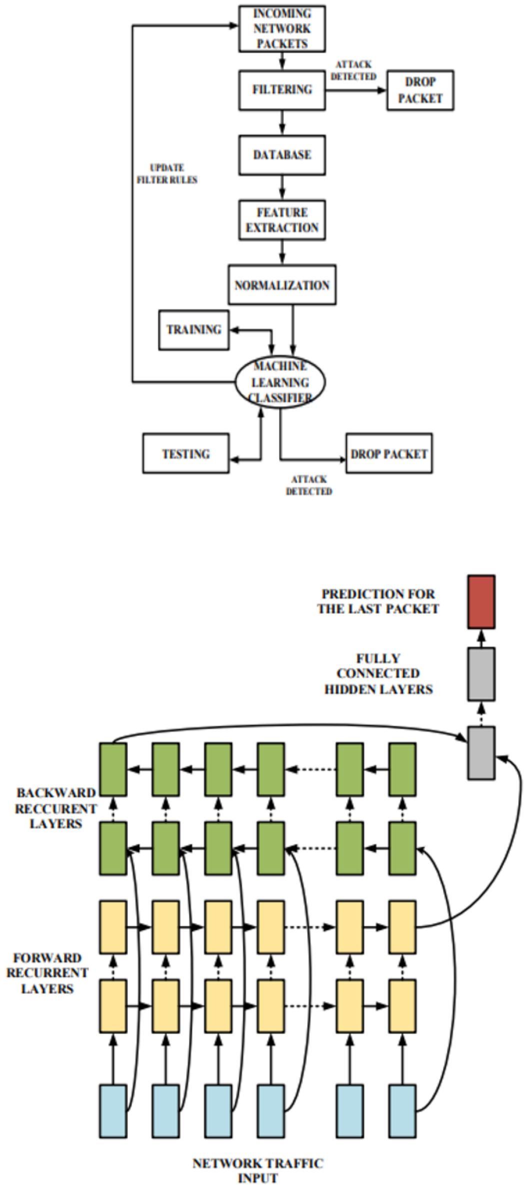
A statistical method for detecting Distributed Denial of Service attack was presented in [18], their observations were based on legitimate traffic sourced from a CAIDA data collection. The goal of their method was to minimize the calculated distances between the current observation window and a predefined reference by evaluating the consistency between received traffic volume and the number of connections per time interval. Their approach required the examination of only a few fields for each packet, enhancing its usability and practicality for real time deployment.

In their study, Jieren et al. [19] introduced an innovative method of detecting DDoS attacks in cloud computing environments using an FCD-RF framework. Their goal was to improve the accuracy of DDoS attack detection. To highlight the unique characteristics between attack flows and normal flows, they created a feature-tuple that includes statistical features from Power Spectral Density (PSD) and Spectral Domain Integral Area (SDIA). This combination captures the asymmetric and semi-directive interaction features indicative of attack functions. In their paper, the made use of the FCD feature sequence along with an optimized Random Forest (RF) derived through a genetic approach for training of the classification model. Their strategy ultimately reduces false and missed alarms, thereby improving the overall accuracy of DDoS attack detection.

In the ever-evolving field of cybersecurity, an effective defense against Distributed Denial of Service (DDoS) attacks requires a comprehensive strategy that combines state-of-the-art technologies and advanced methodologies. The power of Artificial Neural Networks (ANN), when combined with statistical methods, provides a robust framework for quick and accurate detection, serving as a strong deterrent to potential threats.

Moreover, the use of machine learning is crucial in incorporating sophisticated feature selection algorithms such as Consistency Subset Evaluation (CSE) and DDoS Characteristic Features (DCF). This strategic integration not only identifies key attack features but also enables the system to adapt to the constantly changing tactics used by cyber adversaries.

The collaborative relationship between Cumulative Sum (CUSUM) algorithms and Flow-Based Classifiers represents a forward-thinking approach in strengthening defenses against emerging DDoS behaviors. This synergy ensures a dynamic defense mechanism capable of quickly adapting to the complexities of modern cyber threats, thereby protecting network infrastructures with resilience and precision.



s

Fig. 4. Image of Anomaly based Denial of Service Prevention using Artificial Intelligence [11]

V. CONCLUSION

In conclusion, this paper emphasizes the crucial role of cloud computing in today's business and personal landscape. Cloud technology has become an essential enabler, offering scalable and flexible solutions that cater to a variety of needs. However, the widespread use of cloud networks also makes them vulnerable to malicious activities, most notably Distributed Denial of Service (DDoS) attacks [20]. DDoS threats against cloud computing infrastructures pose a significant risk, compromising the availability and reliability of vital services. Key attack vectors include HTTP flooding, SYN flooding, and Session Initiation Protocol (SIP) flood attacks, among others. These disruptions can have serious implications for businesses and individuals relying on cloud services. To strengthen cloud networks against such threats, proactive countermeasures are essential. The use of advanced technologies like Artificial Neural Networks (ANN) [11], statistical methods, and feature selection algorithms such as Consistency Subset Evaluation (CSE) and DDoS Characteristic Features (DCF) [17] becomes crucial. These mechanisms contribute to the early detection of anomalies, enabling swift responses to potential DDoS attacks. As we navigate the evolving landscape of cybersecurity, a comprehensive understanding of DDoS threats and their proactive countermeasures is indispensable. It not only safeguards the integrity of cloud computing but also ensures the continued utility and reliability of these technological marvels in our interconnected world. The ongoing development and implementation of robust defense mechanisms underscore the commitment to fostering a secure and trustworthy cloud computing environment for businesses and individuals alike

REFERENCES

REFERENCES

[1] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE Communications Surveys and Tutorials, vol. 15, no. 4, pp. 2046-2069, 2013.

[2] S. Kumarasamy and R. Asokan, "Distributed Denial of Service (DDoS) Attacks Detection Mechanism," International Journal of Computer Science, Engineering and Information Technology, vol. 1, no. 5, pp. 39-48, Dec. 2011

[3] E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah and R. Alfaris, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," International Journal of Computer Applications, vol. 49, no. 7, pp. 24-32, July 2012.

[4] Y. Xiao, T. Mahjabin, G. Sun and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," International Journal of Distributed Sensor Networks, vol. 13, no. 12, Dec. 2017, doi: 10.1177/1550147717741463.

[5] S. A. Varma and K. G. Reddy, "A Review of DDoS Attacks and Its Countermeasures in Cloud Computing," 2021 International Conference on Intelligent Sustainable Systems (ICISS), 2021, pp. 1-6, doi: 10.1109/ISCON52037.2021.

[6] R. V. Deshmukh and K. K. Devadkar, "Understanding DDoS Attack and Its Effect In Cloud Environment," in Procedia Computer Science, vol. 49, pp. 202-210, 2015.

[7] J. Ioannidis and S. M. Bellovin, "Implementing Pushback: Router-Based Defense Against DDoS Attacks," in Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 2002.

[8] L. Zhou, M. Liao, C. Yuan and H. Zhang, "Low-Rate DDoS Attack Detection Using Expectation of Packet Size," Security and Communication Networks, vol. 2017, Article ID 3691629, 14 pages, 2017.

[9] Y. Liu, S. Jiang and J. Huang, "Anomaly Detection for DDoS Attacks Based on Gini Coefficient," 2013 International Conference on Advanced Information and Communication Technology for Education (ICAICTE), 2013, pp. 649-653, doi: 10.2991/icaicte.2013.163.

[10] J. David and C. Thomas, "DDoS Attack Detection using Fast Entropy Approach on Flow-Based Network Traffic," in Procedia Computer Science, vol. 50, pp. 30-36, 2015.

[11] A. Saied, R. E. Overill and T. Radzik, "Artificial Neural Networks in the Detection of Known and Unknown DDoS Attacks: Proof-of-Concept," Communications in Computer and Information Science, vol. 438, pp. 318-332, June 2014.

[12] J. Haggerty, T. Berry, Q. Shi and M. Merabti, "DiDDeM: a system for early detection of TCP SYN flood attacks," 2004 IEEE Global Telecommunications Conference Workshops, Dallas, TX, USA, 2004, pp. 1-5, doi: [10.1109/GLOCOM.2004.1378370].

[13] H. Wang, D. Zhang and K. G. Shin, "Detecting SYN flooding attacks," Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies., Anchorage, AK, USA, 2002, pp. 1530-1539 vol.3, doi: 10.1109/INFCOM.2002.1019404.

[14] K. Saravanan, R. Asokan and K. Venkatachalam, "Detection mechanism for distributed denial of service (DDoS) attacks for anomaly detection system," Journal of Theoretical and Applied Information Technology, vol. 60, no. 1, pp. 174-178, Feb. 2014.

[15] E. Balkanli, A. N. Zincir-Heywood and M. I. Heywood, "Feature selection for robust backscatter DDoS detection,"

2015 IEEE 40th Conference on Local Computer Networks Workshops (LCN Workshops), Clearwater Beach, FL, 2015, pp. 1-8, doi: 10.1109/LCNW.2015.7365905.

[16] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, “Change-Point Cloud DDoS Detection using Packet Inter-Arrival Time,” in 2016 8th Computer Science and Electronic Engineering Conference (CEEC), University of Essex, UK, 2016, pp. 204-209, doi: [10.1109/CEEC.2016.7835910].

[17] A. R. Yusof, H. Hamdan, N. I. Udzir, M. T. Abdullah and A. Selamat, “Adaptive feature selection for denial of services (DoS) attack,” 2017 Fourth International Conference on Advances in Computing, Communication and Automation (ICACCA) (Fall), Dehradun, India, 2017, pp. 1-6, doi: 10.1109/AINS.2017.8270429.

[18] H. Rahmani, N. Sahli and F. Kammoun, “Joint Entropy Analysis Model for DDoS Attack Detection,” 2009 Fifth International Conference on Information Assurance and Security, Xi’an, 2009, pp. 267-271, doi: 10.1109/IAS.2009.298.

[19] J. Cheng, M. Li, X. Tang, V. S. Sheng, Y. Liu and W. Guo, “Flow Correlation Degree Optimization Driven Random Forest for Detecting DDoS Attacks in Cloud Computing,” Security and Communication Networks, vol. 2018, Article ID 6459326, 14 pages, 2018.

[20] A. Carlin, M. Hammoudeh and O. Aldabbas, “Defence for Distributed Denial of Service Attacks in Cloud Computing,” Procedia Computer Science, vol. 73, pp. 490-497, 2015.

[21] R. Tandon, “A Survey of Distributed Denial of Service Attacks and Defenses,” arXiv preprint arXiv:2008.01345, Aug. 2020.

[22] T. A. Nidecki, “NTP Amplification Attack,” Acunetix, 2020. [Online]. Available: https://www.acunetix.com/blog/articles/ntp-amplification-attack/. [Accessed: Dec. 3, 2023].

[23] PureVPN, ”What is a Slowloris Attack? online. Available:”https://www.purevpn.com/ddos/slowloris-attack [Accessed: Dec. 4, 2023].

[24] F5 Labs, “DNS Amplification Attack,” F5 Labs. Accessed: Dec. 4, 2023. [Online]. Available: ”https://www.f5.com/labs/learning-center/what-is-a-dns-amplification-attack”.