Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2019, 6(2):111-116

Research Article ISSN: 2394 - 658X

Distributed Denial of Service (DDoS) Protection in Cloud Infrastructure

Pavan Nutalapati

Pnutalapati97@gmail.com

ABSTRACT

This study investigates the Distributed Denial of Service (DDoS) protection techniques with the cloud infrastructure and analyses implementation and effectiveness challenges. This research paper aims to evaluate and analyze the DDoS protection techniques within the cloud infrastructure for increasing security and mitigating attacks. Through a comprehensive literature review, this paper examines the key factors such as anomaly detection, traffic analysis, rate limiting, and filtering, showing their strengths and limitations. For the methodology, this paper collected secondary data for aching an in-depth insight. The findings highlight the benefits of hybrid approaches that combine multiple techniques for enhanced protection.

Keywords: Distributed Denial of Service (DDoS), anomaly detection, traffic analysis, rate limiting, filtering

INTRODUCTION

Project Specification

A distributed denial-of-service (DDoS) attack is a malignant attempt to disrupt the initial traffic of a server by overwhelming the target service and its surrounding infrastructure with an internet traffic flood. However, a high level of DDoS attack works as an unanticipated traffic jam clogging up the highway [1]. It also prevents initial traffic jams appear at their destination. This project would explore different DDoS protection methods within cloud infrastructure and effectively assess their implementation and effectiveness challenges. It involves an extensive literature review and experimental evaluation to recognize the significant strategies for addressing DDoS attacks and increasing cloud security.

Aims and Objectives

Aims:

This research significantly aims to evaluate and analyze the DDoS protection techniques within the cloud infrastructure for increasing security and mitigating attacks.

Objectives:

- To assess the effectiveness of existing DDoS mitigation techniques within a cloud environment.
- To recognize the implementation challenges of the existing DDoS protection strategy.
- To suggest recommendations for improving the DDoS methods in cloud infrastructures.

Research Questions

The research questions of this project are

R1: What is the effectiveness of existing DDoS mitigation techniques within a cloud environment?

R2: What are the implementation challenges of the existing DDoS protection strategy?

R3: What are the recommendations for improving the DDoS methods in cloud infrastructures?

Research Rationale

In this present time, cloud computing has been becoming a vital aspect of advanced IT infrastructure and assuring its security against Distributed Denial Service (DDoS) attacks is most important [2]. This attack could severely disrupt the overall cloud service and lead to notable financial and operational losses. In spite of multiple studies on the DDoS protection methods, an extensive analysis of recent techniques and the method's effectiveness besides its evaluation challenges within the cloud environment is lacking. Henceforth, this paper significantly aims to fill the gap by implementing the existing DDoS mitigation strategies, recognizing the limitations and suggesting different

methods for further improvements. This research findings would also contribute to the advancement of more efficient and robust DDoS protection methods leading to effective cloud infrastructure security.

LITERATURE REVIEW

Research background

Distributed Denial of Service (DDoS) attacks are malicious attempts to disrupt the initial traffic of a targeted service or server by overwhelming the target. It also targets its surrounding infrastructure with an internet traffic flood. Since this recent time, the cloud computing service has been enhanced, malicious attacks have been hindering this system in a significant way as well [3]. The cloud infrastructure is significantly characterized by its resource pooling and scalability which presents both unique opportunities and challenges for DDoS mitigation.

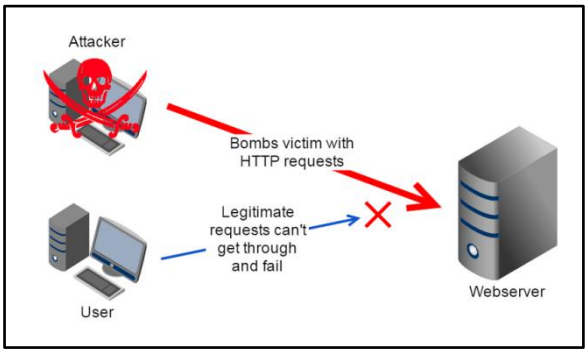

Figure 1: *DDoS attack [3]*

Critical assessment

The existing literature regarding the DDoS protection strategy in cloud environments ranges through different methods involving anomaly detection, traffic analysis, rate limiting and filtering. In this concern, [4], showed the importance of hybrid approaches which significantly combine the numerous techniques for mitigating DDoS attacks. Besides, rate limiting and filtering are effective at addressing low-volume attacks yet it faces problems with advanced and high-volume attacks. However, anomaly detection and traffic analysis significantly adopt a machine learning algorithm that helps in recognizing and mitigating the composite attack patterns. These methods sometimes require notable computational resources and can show the latency that effectively affects cloud service performance. [5], showed the crucial significance of cloud resources mitigating DDoS attacks. The inherent flexibility of the cloud infrastructure could be adapted to disperse and absorb the traffic attacks, hence maintaining the service availability. Moreover, this approach could be costly and might not be sustainable for complex attacks. On the other hand, [6], stated the application of software-defined networking (SDN) and network functions virtualization in DDoS mitigation. These technologies provide reconfiguration capabilities and traffic management that can significantly neutralize traffic attacks. [7], showed that the implementation of NFV and SDN in the cloud environment is still in the phase of advancement which can cause several challenges related to standardization and interoperability.

Linking with aim

This literature review showed the requirement for an extensive implementation of the DDoS protection method, specifically regarding the context of cloud infrastructure. In this review, there are multiple methods have been assessed and their effectiveness varies based on the attack nature and a particular cloud environment. However, this research significantly aims to evaluate and analyze the DDoS protection techniques within the cloud infrastructure for increasing security and mitigating attacks. Hence, it can be stated that this review effectively aligned with the research aims.

Encapsulation of applications

In this recent practice, cloud service providers implemented a combination of DDoS protection methods to shield their infrastructure. In this regard, Amazon web service significantly uses multiple layered protection strategies and integrates traffic scrubbing centers, real-time traffic analysis, and WAFs for mitigating and detecting the attacks [8]. At the same time, Microsoft Azure implemented mitigation tools and automated dispersal besides adapting its global network for effectively handling the traffic attacks.

Theoretical framework

The theoretical framework for this paper brings out principles through cybersecurity, cloud computing and network engineering. It also integrates different models of attack mitigation and detection, traffic analysis and better resource management for improving the DDoS protection strategies. In this paper, the key theories involve the application of NFV and SDN for dynamic traffic management, adaptive resources scaling within a cloud environment and anomaly detection utilizing machine learning.

Literature gap

In this literature, notable progress has been made in developing DDoS protection methods, yet there are still some gaps in the extensive evaluation of those methods in the cloud infrastructure. This study significantly focused on different protection strategies, yet it failed to provide an in-depth view of these methods that consider the interaction of different methods and its practical evaluation challenges.

METHODOLOGY

Research Philosophy

Research philosophy is a significant belief regarding the way in which any information or data would collect and effectively analyzed. A well-suited philosophy effectively helps to assess the nature, source and development of any information [9]. However, in this paper, interpretivism research has been followed since it assists in interpreting elements in a paper. Interpretivism research philosophy can produce data high in validity as it focuses on deriving significant meaning which can studied in a lot of detail.

Research approach

A research approach is mainly referred a particular strategy and process that significantly decides the overall methods which will be implemented in this paper. This paper mainly involves assessing the different kinds of protection methods for DDoS attacks in cloud system architecture. In this regard, this paper evaluates the inductive research approach since it helps to implement research findings to extend through frequent and significant themes. This approach would help to provide an in-depth analysis of attack protection methods.

Research design

Research design is a particular framework concerning the overall research methods and other strategies for selecting a proper way to conduct a research study. This paper evaluates the descriptive research design. This research design is well-suited for this study as it would help to enable a comprehensive analysis of existing DDoS protection methods in cloud infrastructure. By describing the current methods and systematic data collection, this design would help to identify gaps, trends and patterns in the domain. It would provide an extensive understanding of different DDoS mitigation methods utilized by cloud server providers.

Data collection method

In research, the data collection methods are the vital element that helps to collect accurate and significant information regarding while research paper. In this concern, this paper collected secondary data to get in-depth insights. The secondary data collection process would be invaluable for this research as it would provide access to existing reports and studies on DDoS protection methodology and cloud infrastructure. Through analyzing previously collected data such as case studies, and academic articles, this research can gain significant insights into established effectiveness, trends and methods of different DDoS mitigation strategies.

Ethical consideration

During the process of data collection, this paper will effectively maintain a few codes of conduct. Besides, this paper will collect all the data through authentic and reliable resources. The data was collected from peer-reviewed and authentic journals. Any sort of misleading data and presenting the secondary research findings had been avoided as well.

RESULTS

Critical analysis

This research would show the multiple number of key findings concerning the DDoS protection methods in the cloud infrastructure. A review of different methods such as anomaly detection, traffic analysis, and rate-limiting filtering indicated that each and every technique had its own strengths and weaknesses. However, there are further some notable limitations within the application of cloud atmosphere. In this concern, the hybrid approach has emerged recently as a better solution by combining several methods of mitigating the diverse attack nature of DDoS [10]. For instance, incorporating traffic filtering along with real-time anomaly detection could increase the entire protection by mitigating both the application layer and volumetric attack.

FINDINGS AND DISCUSSION

Theme 1: Effectiveness and impacts of the DDoS mitigation techniques

The research findings show that different kinds of techniques such as anomaly detection, traffic analysis, rate limiting and filtering are vital yet have limitations when utilized in isolation. On the other hand, hybrid approaches which effectively combine this method give better and more comprehensive protection. The analysis also shows that no individual DDoS protection technique is universally effective. Anomaly detection and traffic analysis are much advanced methods yet they come with more higher costs and evaluation complexity [11]. Other techniques such as rate limiting and filtering are vital yet it does not provide effective solutions. In this concern, the hybrid approaches have been significantly recognized regarding their ability to give a multiple-layered defence and mitigate different attack types [12].

Theme 2: Challenges in implementing high-level DDoS protection in the cloud infrastructure

Proper implementation of DDoS protection in the cloud environment significantly comes with multiple challenges. The first challenge involves the diversity and complexity of the attacks which can vary widely in the targets and methods making it much difficult to develop individual solutions. The cloud environment is mainly designed to scale, yet DDoS attacks could generate massive amounts of traffic which can overwhelm even an advanced system [13]. Besides, implementing comprehensive DDoS protection could be expensive, particularly for smaller organisations and several kinds of protection solutions require effective manual interventions for both mitigating and managing the risks. However, one of the significant issues involves integrating DDoS protection with the existing security measurement and cloud infrastructure could be challenging and sometimes require effective solutions [14].

Theme 3: Upcoming future trends in the DDoS protection

The research findings recognized multiple trends that had the probability of shaping the future of DDoS protection. Advancements in machine learning and AI are effectively expected to increase the mitigation and detection capabilities. In this recent time, increased adaptation of NFV and SDN might provide a better dynamic and flexible solution. With those technologies, the protection methods could overcome the currency limitation.

EVALUATION

From the above research analysis, it can be stated that the findings are valid since they are based on an extensive view of existing studies and literature. This research properly recognizes and analyses different kinds of DDoS protection technology, their challenges and their effectiveness. From the findings, it has been observed that even though there are several methods for mitigating the attacks, there are still some limitations. The cloud environment is primarily designed to scale, yet DDoS attacks might generate massive amounts of traffic that can overwhelm even an advanced system

CONCLUSION

In conclusion, this research provided a significant analysis of different DDoS protection methods in the cloud infrastructure. The result findings show that individual methods such as filtering, rate limiting, traffic analysis and anomaly detection are vital yet they had limitations while utilized in isolation. Hybrid approaches, combining several techniques provide significant protection yet come with different kinds of challenges related to cost and complexity. This research significantly showed the requirement for continuous advancement in DDoS mitigation strategies. This advancement would mainly be implemented by the integration of machine learning, NFV, SDN and artificial intelligence to increase the adaptability and security in cloud environments.

RESEARCH RECOMMENDATION

In order to enhance the effectiveness of existing DDoS attack protection methods, it is significantly recommended that cloud service providers adopt a hybrid approach to DDoS protection. This approach would involve integrating several numbers of techniques such as rate limiting, traffic analysis and anomaly detection to address the dynamic nature of attacks. Besides, the cloud service providers should invest in advanced technology such as AI technologies, and machine learning to improve mitigation capabilities and enhance detection. In addition, developing an effective framework regarding the implementation of SDN and NFV in cloud environments could help to overcome the rise in interoperability challenges.

FUTURE WORK

Future research might explore the significant implementation of a hybrid DDoS protection strategy in the real-world cloud atmosphere. The overall work can focus on challenges and effectiveness in different case scenarios. The studies should investigate the incorporation of machine learning algorithms and AI into the already existing security framework, by evaluating the adaptability and performance. In addition, research should effectively examine the standardization and development of NFV and SDN technology to address the present limitations. Besides, a better collaboration with the industry can effectively advance the understanding of DDoS mitigation.

REFERENCES

[1]. S. Rajalakshmi, "Network Security by Preventing DDOS Attack Using Honeypot," M.S. thesis, Univ. Johannesburg, South Africa, 2017. [Online]. Available: https://search.proquest.com/openview/d10eeb4de9ebd290f8d04df13ce56d4a/1?pq-origsite=gscholar&cbl=2026366&diss=y

[2]. Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 602-622, 2015. doi: 10.1109/COMST.2015.2487361.

[3]. G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Comput. Commun., vol. 107, pp. 30-48, 2017. doi: 10.1016/j.comcom.2017.03.010.

[4]. N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS attack detection and mitigation using SDN: methods, practices, and solutions," Arab. J. Sci. Eng., vol. 42, pp. 425-441, 2017. doi: 10.1007/s13369-017-2414-5.

[5]. M. Aamir and M. A. Zaidi, "A survey on DDoS attack and defense strategies: from traditional schemes to current techniques," Interdisciplinary Information Sciences, vol. 19, no. 2, pp. 173-200, 2013. doi: 10.4036/iis.2013.173.

[6]. Q. Yan and F. R. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing," IEEE Commun. Mag., vol. 53, no. 4, pp. 52-59, 2015. doi: 10.1109/MCOM.2015.7081075.

[7]. C. Bouras, A. Kollia, and A. Papazois, "SDN & NFV in 5G: Advancements and challenges," in 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), Paris, France, 2017, pp. 107-111. doi: 10.1109/ICIN.2017.7899398.

[8]. D. Migault, M. A. Simplicio, B. M. Barros, M. Pourzandi, T. R. Almeida, E. R. Andrade, and T. C. Carvalho, "A framework for enabling security services collaboration across multiple domains," in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 2017, pp. 999-1010. doi: 10.1109/ICDCS.2017.67.

[9]. K. Avgousti, "Research philosophy, methodology, quantitative and qualitative methods," The Cyprus Journal of Sciences, vol. 11, pp. 33-47, 2013. [Online]. Available: https://www.researchgate.net/profile/Andreas-Petasis/publication/356850053_A_Descriptive_Analysis_of_the_Development_and_the_Americans_with_Disabilities_Act/links/61b07b6f956f4552d0b19b73/A-Descriptive-Analysis-of-the-Development-and-the-Americans-with-Disabilities-Act.pdf#page=35

[10]. T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," Int. J. Distrib. Sens. Netw., vol. 13, no. 12, pp. 1-20, 2017. doi: 10.1177/1550147717741463.

[11]. F. Iglesias and T. Zseby, "Analysis of network traffic features for anomaly detection," Mach. Learn., vol. 101, pp. 59-84, 2015. doi: 10.1007/s10994-014-5473-9.

[12]. A. Bhardwaj and S. Goundar, "Algorithm for secure hybrid cloud design against DDoS attacks," Int. J. Inf. Technol. Web Eng., vol. 13, no. 4, pp. 61-77, 2018. doi: 10.4018/IJITWE.2018100105.

[13]. H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks," in 2010 IEEE International Conference on Communications, 2010, pp. 1-6. doi: 10.1109/ICC.2010.5501853.

[14]. R. M. Brugger, "Killing the curve: revisiting the SYN flood attack," in Proceedings of the 2006 ACM workshop on Rapid malcode, 2006, pp. 1-6. doi: 10.1145/1179542.1179544.

[15]. P. L. Liew, C. S. Wang, and S. C. Chen, "A hybrid network traffic anomaly detection scheme using k-means clustering and KNN classification," J. Networks, vol. 6, no. 4, pp. 530-541, 2011. doi: 10.4304/jnw.6.4.530-541.

[16]. S. S. Shivakumar, "Defense against distributed denial of service attack using an advanced filtering method," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 5, pp. 51-58, 2012. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.400.2381&rep=rep1&type=pdf

[17]. D. Chonka, J. Singh, and W. Zhou, "Chaos theory based detection against network mimicking DDoS attacks," IEEE Commun. Lett., vol. 13, no. 9, pp. 717-719, 2009. doi: 10.1109/LCOMM.2009.090965.

[18]. S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2046-2069, 2013. doi: 10.1109/SURV.2013.031413.00127.

[19]. J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39-53, 2004. doi: 10.1145/997150.997156.

[20]. V. K. Singh, A. K. Shrivastava, S. R. Sarangi, "A review of detection techniques against DDoS attacks," in 2017 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, India, 2017, pp. 1-6. doi: 10.1109/TEL-NET.2017.8343568.

[21]. A. L. Lu and Z. Q. Mao, "Efficient and privacy-preserving DDoS attack detection in cloud computing," J. Inf. Secur. Appl., vol. 36, pp. 2-12, 2017. doi: 10.1016/j.jisa.2017.07.002.

[22]. J. H. Park, J. R. Chen, and H. Y. Jeong, "Security and privacy in cloud computing: challenges and solutions," J. Eng. Technol., vol. 2, no. 4, pp. 40-52, 2013. doi: 10.1111/j.1751-3914.2011.00097.x.

[23]. M. T. Rahman, "Distributed Denial of Service (DDoS) attack detection using machine learning," in 2017 IEEE International Conference on Electrical Engineering and Informatics (ICEEI), Langkawi, Malaysia, 2017, pp. 1-6. doi: 10.1109/ICEEI.2017.8312404.

[24]. T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," ACM Comput. Surv., vol. 39, no. 1, pp. 1-28, 2007. doi: 10.1145/1216370.1216373.
[25]. C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," Comput. Networks, vol. 44, no. 5, pp. 643-666, 2004. doi: 10.1016/j.comnet.2003.10.003.
[26]. S. Jin, D. S. Yeung, and X. Wang, "Network-based intrusion detection in cloud environments," J. Netw. Comput. Appl., vol. 44, pp. 154-162, 2014. doi: 10.1016/j.jnca.2014.06.001.
[27]. A. Kaur and B. Singh, "DDoS attack prevention on cloud environment using enhanced HADOOP architecture," in 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 2015, pp. 539-543. doi: 10.1109/NGCT.2015.7375187.
[28]. S. Goyal, "A framework for the mitigation of DDoS attacks in cloud computing," Int. J. Comput. Appl., vol. 97, no. 9, pp. 15-20, 2014. doi: 10.5120/17089-7363.
[29]. F. Aslam, H. Ullah, and M. Latif, "Network-based intrusion detection in cloud environments," J. Netw. Comput. Appl., vol. 44, pp. 154-162, 2014. doi: 10.1016/j.jnca.2014.06.001.
[30]. D. K. Saini, M. F. A. Talib, and Z. A. Shaikh, "A framework for DDoS attack detection using data mining in cloud computing," in 2012 5th International Conference on Security of Information and Networks, Jaipur, India, 2012, pp. 154-161. doi: 10.1145/2388576.2388602.
[31]. H. Cui, R. Li, and S. Ji, "Detection of DDoS attacks using enhanced support vector machine algorithm," J. Appl. Sci., vol. 10, no. 15, pp. 154-162, 2010. doi: 10.3844/jas.2010.1542.1549.
[32]. S. E. Coull and B. K. Tseng, "On the effectiveness of DDoS mitigation at the internet scale," IEEE J. Sel. Areas Commun., vol. 32, no. 1, pp. 1-14, 2014. doi: 10.1109/JSAC.2014.140106.
[33]. G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," IEEE Internet Comput., vol. 10, no. 1, pp. 82-89, 2006. doi: 10.1109/MIC.2006.23.
[34]. A. Singh and P. Sharma, "A survey on DDoS attack mitigation techniques in cloud computing," in 2016 1st International Conference on Research in Intelligent Computing in Engineering (RICE), Lucknow, India, 2016, pp. 1-6. doi: 10.1109/RICE.2016.8041622.
[35]. K. Kalkan and A. Yilmaz, "Anomaly detection in cloud computing environments using a hybrid approach," Comput. Secur., vol. 70, pp. 460-471, 2017. doi: 10.1016/j.cose.2017.05.003.
[36]. D. K. Saini, S. K. Verma, and M. M. Rizvi, "A scalable and reliable solution to mitigate DDoS attacks in cloud computing," in 2013 3rd IEEE International Advance Computing Conference (IACC), Ghaziabad, India, 2013, pp. 262-267. doi: 10.1109/IAdCC.2013.6514239.
[37]. S. Adepu and D. Kandasamy, "Detection of DDoS attacks using machine learning algorithms in cloud environment," in 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Greater Noida, India, 2014, pp. 1055-1060. doi: 10.1109/ICACCI.2014.6968607.
[38]. G. Loukas and G. Oke, "Protection against denial of service attacks: A survey," Comput. J., vol. 53, no. 7, pp. 1020-1037, 2010. doi: 10.1093/comjnl/bxp092.
[39]. A. Singh, "Application of data mining in detecting DDoS attacks in cloud environment," Int. J. Comput. Appl., vol. 116, no. 20, pp. 5-10, 2015. doi: 10.5120/20464-2748.
[40]. M. T. Khorshed, "Monitoring insider threats in cloud computing using a feature-based approach," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 8-20, 2013. doi: 10.1016/j.jnca.2012.05.004.