https://doi.org/10.51483/IJCCR.2.1.2022.1-6 ISSN: 2790-1386

SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Cryptocurrency Research

Publisher's Home Page: https: / / www.svedbergopen.com /

Research Paper Open Access

Protecting Cloud Infrastructure from DDOS Assaults the use of Blockchain to Achieve Cloud Security

Salwa. H. Alghmadi[1] and Mohammed. I. Alghamdi[2*]

[1]College of Computer Science and Information Technology, Department of Engineering and Computer Sciences, Al-Baha University, Saudi Arabia. E-mail: 442021118@stu.bu.edu.sa

[2]College of Computer Science and Information Technology, Department of Engineering and Computer Sciences, Al-Baha University, Saudi Arabia. E-mail: mialmushilah@bu.edu.sa

Article Info

Volume 2, Issue 1, June 2022
Received : 12 March 2022
Accepted : 17 May 2022
Published : 05 June 2022
doi: 10.51483/IJCCR.2.1.2022.1-6

Abstract

Cloud Infrastructure has become the need of the hour which has resulted in increasing interest of attackers. The most prominent attack on the cloud in recent years is DDoS. DDoS attack results in service unavailability due to a botnet that overflood the network with service requests. The blockchain technology used to diminish DDoS has not yet been completely researched and arranged. This project will survey, and position cutting-edge DDoS decrease arrangements in light of blockchain technology. Considering our research, we will likewise talk about the research difficulties and future headings for executing a blockchain-based DDoS moderation arrangement. We expect this project will fill in as a beginning stage and reference for future researchers attempting to recognize and moderate denial of service attacks utilizing blockchain technology.

Keywords: *Cloud Technology, Blockchain, DDoS, IoT*

1. Introduction

Cloud computing is a model to deliver on demand computing resources with the minimal effort and management. It is the sharing of computer resources over the internet. These shared resources can be in the form of software, development interface, virtual hardware or storage. The essential components of a cloud computing are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). These resources are dynamic and can be configured according to the needs.

The attacks of Distributed Denial of Service (DDoS) on cloud computing services are greater than before in recent years and are constantly increasing (Akamai, 2017).

DDoS attacks have the basic purpose of disrupting or suspending Internet services, and their motivations range from personal grudges to blackmail to political motivations (Mansfield-Devine, 2015). In October 2016, Spotify (The Associated Press, 2017) released a Blockchain-Based Architecture for Collaborative DDoS Mitigation. As a result, many US users were unable to use such services for several hours. DDoS attacks are becoming more efficient and harmful as their frequency, severity, and duration increase. The availability of many reflectors, i.e., poorly secured or configured Internet of Things (IoT) devices or home gateways is one cause for the growing magnitude of attacks (The Associated Press, 2017) .

* *Corresponding author: Mohammed. I. Alghamdi, College of Computer Science and Information Technology, Department of Engineering and Computer Sciences, Al-Baha University, Saudi Arabia. E-mail: mialmushilah@bu.edu.sa*

Increased use of cloud technology due to telework and the Covid-19 pandemic in the first quarter of 2020 increased the volume and intensity of DDoS attacks in 2020. For example, various amplifications and basic attacks through UDP are increasing the initiation of flooding of the target network up to 570% (Sharma *et al.*, 2020). In comparison to the same quarter last year, the second quarter of 2020 is the same. Existing threshold-based mitigation methods are inadequate to detect these attacks, and machine learning models can accurately detect whether an attack pattern follows a trained data pattern, creating new attack patterns. The attacks used may deviate slightly from these models. DDoS attack vectors have been around for years (Wang *et al.*, 2019).

By exploiting legal services on those clouds, the power of a DDoS attack is amplified, and the problem of defense is made more complicated. Thus, the impact of DDoS varies from minor inconvenience to severe financial losses for enterprises that rely on their online availability (Peng *etal.*, 2007). Various mitigation techniques have been proposed. However, only a few have been considered for widespread deployment because of their effectiveness and implementation complexities (Sattar *et al.*, 2015). DDoS protection services, such as those provided by Akamai (2017) and CloudFlare (Yue *et al.*, 2018), are becoming more popular (Jonker *et al.*, 2016).

By exporting the responsibility of detection away from the device under attack, these cloud-based solutions can absorb DDoS attacks by expanding capacity and transferring the weight of detection away from the device under attack. Flow records from edge routers and switches. Additional analysis is done in the cloud, and traffic is balanced, rerouted, or dropped via packet filtering inside the cloud. However, those solutions require a third-party DDoS Protection. Service (DPS) provider, which is implying additional costs and a decrease In-service performance. In this paper, we will discuss the impact of the use of blockchain technology in improving the efficiency of cloud infrastructures by mitigating DDoS attacks in a decentralized manner.

2. Background

The attacks of DDoS intend to consume the bandwidth and assets and keep appropriate clients as of getting to facilities. Numerous researchers talk about these attacks at three layers of design of the cloud (Sharma *et al.*, 2020). At the perceptual level, many malicious attacks, kill commands, and asynchronous attacks forestall RFID data sniffing. At the network level, Layer 3 attacks mean to deplete casualty assets in various ways, including flood attacks, reflection-based flood attacks, amplification-based flood attacks, and amplification-based attacks. Application (Layer 7) attacks of the DDoS are more perplexing than Layer 3 attacks and challenging to distinguish through channels (Wang *et al.*, 2019). Applications vulnerable to attack incorporate DNS, HTTP, and VoIP (Yue *et al.*, 2018).

3. Problem Statement

New innovations, for example, cloud computing, IoT, and SDN these technologies are exchanging the design of the Internet, furnishing attackers with new chances to observe weaknesses and send off denial attacks. The test of huge scope DDoS attacks is to moderate them in a brief timeframe and keep away from the deficiency of business and notoriety of the organizations engaged with the attack. So, to overcome these issues we will present the blockchain solution (Yue *et al.*, 2018).

4. Research Goals and Objectives

The goals and objectives of this research include:

- How an attacker could utilize a cloud network, for example, a botnet to launch a DDoS attack focusing on a legitimate client, and the gamble of an attack of DDoS in cloud space.
- How is the blockchain turning into an applicant technology to lessen the attacks of the DDoS?
- Current recommendations for blockchain-based answers for relieving the attacks of the DDoS in the cloud, particularly DDoS working standards and guard components (like avoidance, recognition, reaction)?
- What is the extent of research and difficulties in proposing the networks of cloud that are based on the blockchain (and proposing utilization of additional supportive innovations) to lessen the attacks of the DDoS?

5. Literature Review

As cloud computing provide large number of resources online, so it is facing with several security problems like secrecy, authenticity, confidentiality and DDoS attack. The most major threat to Cloud security is DDoS Attack. It greatly affect the services of simple network and there are different techniques for its detection and prevention, this attack also affect the new emerging cloud computing technology, so to improve resource availability of resources in cloud computing environment, it is essential to provide a mechanism to prevent DDoS attacks (Sattar *et al.*, 2015).

In this section different DDoS attack detection and prevention techniques with blockchain for cloud computing environment proposed by different authors has been collected and discussed.

The combination of Blockchain and IoT has attracted a lot of attention and recently many surveys and review papers are published in this area. Some of the surveys discussed these two technologies in terms of the importance of usage of blockchain for the security of IoT, challenges and future directions of applying blockchain in IoT. However, these surveys did not discuss how blockchain can be used to detect and mitigate DDoS attacks in IoT. In the surveys conducted by the authors reviewed and compared several case studies that utilize blockchain in IoT to provide security and privacy in different scenarios, such as, access control, economic scenarios, smart homes, etc. However, authors did not provide any discussion on mitigating DDoS attacks in IoT. Some researchers analyzed the requirements of deploying blockchain in IoT and explained how blockchain is used in IoT but without consideration of DDoS attacks. The history of DDoS attacks can be traced back to 1998 and, therefore, there is a lot of literature that reviews types of DDoS attacks and various defense mechanisms. However, these surveys are only for traditional networks and do not discuss IoT-based networks. For surveys in the IoT environment, Spathoulas *et al.* (2019) discussed on DDoS attacks in three layers of the IoT architecture. However, they did not explain and critically analyze different solutions for mitigating DDoS attacks in IoT. Some researchers reviewed the effects of DDoS attacks on IoT, prevention mechanisms and solutions to mitigate DDoS attacks in IoT. In the focus of authors is on the DDoS attacks at the network layer; however, Chaganti *et al.* (2022) discussed technologies on an IoT protocol stack to mitigate DDoS attacks, such as IPv6, IEEE 802.15.4, 6LoWPAN, etc. However, Shah *et al.* (2022) did not mention blockchain-based solutions that mitigate DDoS attacks.

Tayyab *et al.* (2020) take the approach that each IDS in the network acts as a blockchain node and collaborate with other blockchain IDS nodes to share the attack information like correlated alarms. This decentralized correlated information sharing is used for the detection of ICMP6 based DDoS attacks. Although IDS collaboration improves DDoS attack detection capability, the practical implementation of collaboration can have difficulties. For example, the IDS vendor interoperability to support the blockchain technology is needed in enterprise environment. Denial of service attacks detection at the IDS level is too late and might already congest the edge network communication channels or the content delivery network communications (Chaganti *et al.*, 2022).

Yeh *et al.* (2020), Shafi and Basit (2019) and Hajizadeh *et al.* (2020) discussed the threat information sharing including DDoS threat data among the collaborators for secure data sharing using blockchain based smart contracts technology and decentralized data storage. The security operation centers can be uploading the threat data and ISP act as verifier to confirm the illegitimacy of the threat data prior to adding to the blockchain transaction. The Ethereum based smart contract implementation for DDoS data sharing is performed for evaluation. But, the Hyperledger caliper is used to implement the threat information sharing among the organizations. Each organization may have the SDN controller to run the blockchain application and act as a blockchain node for updating the threat information in other nodes (Chaganti *et al.*, 2022).

Pavlidis *et al.* (2020) proposed a blockchain based network provider collaboration for DDoS mitigation. The AS's are selected based on the reputation scores to participate in the DDoS mitigation plan. The programmable data planes are used to implement the mitigation mechanism for DDoS attacks, which is in contrast to most of the works using SDN OpenFlow protocol. In the machine learning algorithms such as K-Nearest Neighbors (KNN), decision tree and random forest as well as deep learning technique Long Short-Term Memory (LSTM) are applied to the network traffic to determine the DDoS attack and considered blockchain technology to whitelist/blocklist the IP addresses at the autonomous system level of the network. But the machine learning application on the network traffic requires infrastructure and computation capabilities, and ownership responsibility to allocate the resources need to be addressed. Any specific entity like ISP, security service providers will not be interested to perform data analytics unless they have any monetary benefits or business advantages (Chaganti *et al.*, 2022).

Our literature review shows that there is no study available in the existing literature that has carried out a survey to analyze the blockchain-based solutions to mitigate DDoS attacks in IoT. This paper aims to fill in this research gap by categorizing and critically evaluating various blockchain-based solutions to mitigate DDoS attacks in IoT. Another novelty of our work is to propose future work directions that can be explored by other researchers to propose better blockchain solutions to mitigate DDoS attacks in IoT (Shah *et al.*, 2022).

5.1. Blockchain and DDoS Detection

Blockchain technology promises to transform the way information and data is exchanged between untrustworthy entities. Building trust in distributed environments without the need of central authorities is a technological breakthrough

and blockchain technology can be an appropriate mechanism for securing IoT systems that are by default distributed and of limited trust. The use of both IoT and Blockchain technologies requires addressing multiple challenges before being an effective approach. Nevertheless, blockchain technology has already been successfully employed, to enhance detection system with respect to defending traditional cyber security attacks. Blockchain has also been used to improve IoT security in general, and it has been shown that it can be specifically used for authentication, data integrity, or secure communication between IoT devices (Spathoulas *et al.*, 2019).

While selecting DDoS solution many things need to be considered.

- **Functional:** The solution should be functional enough, which means it should be able to reduce impact of the attack irrespective of how powerful the attack is.
- **Transpicuous:** The solution must be easy to implement, i.e., it should not require modifying the existing network and its infrastructure.
- **Lightweight:** Most importantly the solution should not overhead the system.

6. Research Methodology

In this survey, we reviewed how the IoT networks and our subject topic cloud services are vulnerable to the DDoS attacks by showing studies that are done on the field. We discuss the DDoS attack scenario, its effect on IoT network and connected services, the layer of impact, the integration of Blockchain in cloud services and its potential use to address DDoS attacks; in addition, we further briefly discuss challenges of Blockchain implementation in cloud services. Various research directions are also proposed in this survey that will enable future researchers to propose better Blockchain-based solutions to mitigate DDoS attacks in IoT. In addition, we did not discuss the solutions that address the privacy issues. Furthermore, this paper limits its study to blockchain-based solutions, and we plan to see how the DDoS security (along with privacy) issues were addressed using Machine Learning or other technologies.

7. Relevance to the Program to the Field/ Significance and /or Impact of Proposed Research

The cloud computing model has the ability to scale computer resources on demand and give users a number of advantages to progress their conventional cluster system. In fact, the total cost of going towards cloud is almost zero when resources are not in use. Therefore, it is no wonder that academic research and industry are moving towards cloud computing. However, Security should in fact be implemented it alongside functionality and performance. One of the most serious threats to cloud computing security itself comes from DDoS attacks. These types of attacks are simple and easy to implement by the attacker, but to security experts they are twice as difficult to stop. Although there are various solutions to the DDoS attack on cloud services, we wanted to search blockchain based solutions that need to be studied more in the field. We believe that blockchain based solutions will provide successful results on defending cloud computing services.

Out of confidentiality, integrity and availability as three major issues in cloud security, availability is the area where cloud-based infrastructure appears to have had its largest challenges to date; and it is DDoS attack, a major threat to availability. In cloud computing where infrastructure is shared by potentially millions of users, DDoS attacks have the potential to have much greater impact than against single tenanted architectures (Joshi *et al.*, 2012). Since the attackers look for the crowded services since it is easier to attack to the system when it is busy. Cloud systems are one of the most private services for the users, and they are widely used all around the world. In our research we are looking for the solutions provided by variety of researchers so that it would help the readers to collaborate with the authors. The solutions are based on blockchain since it is a powerful software defense system that can detect malicious attacks on cloud computing environments. Thus, the research has the relevancy to the program of DDoS attack and its solutions.

8. Relevance to the Program

Since the attackers look for the crowded services since it is easier to attack to the system when it is busy. Cloud systems are one of the most private services for the users, and they are widely used all around the world. In our research we are looking for the solutions provided by variety of researchers, so that it would help the readers to collaborate with the authors. The solutions are based on blockchain since it is a powerful software defense system that can detect malicious attacks on cloud computing environments. Thus, the research has the relevancy to the program of DDoS attack and its solutions.

9. Research Plan and Timeline

The planning of this research has been developed by taking advantage of how the latest blockchain technologies can be used to fend off DDoS attacks that occur in cloud computing systems. A draft of the project was created by looking

at the studies and expected success rates in this field, the advantages and disadvantages encountered in these studies, and the usefulness of the use of blockchain technology in this field. The literature where this information can be obtained has been reviewed and information has been collected from relevant sources. In terms of timeline, research steps were followed, including first understanding the subject, then collecting relevant documents, investigating their relevance to the subject, underlining the necessary information, and different sources to support this information. These all were followed accordingly, and the data was collected and gathered together in our research.

10. Conclusion

In conclusion, we made research on DDoS attacks on cloud services, and we demonstrated the literature review for the existing solutions to avoid those attack with a brand-new technology blockchain. With this research we conclude that with blockchain technologies, it would be easier to detect the DDoS attack on cloud computing services. Since security is a very important issue for almost everyone, we think that more future research should be some in this field.

References

Akamai. (2016). How to Protect Against DDoS Attacks - Stop Denial of Service. https://www.akamai.com/us/en/resources/protect-against-ddos-attacks.JSP. Accessed on January 10, 2017.

Chaganti, Rajasekhar., Bhushan, Bharat. and Ravi, Vinayakumar. (2022). The Role of Blockchain in DDoS Attacks Mitigation: Techniques, Open Challenges and Future Directions. https://doi.org/10.48550/arXiv.2202.03617

Hajizadeh, M., Afraz, N., Ruffini, M. and Bauschert, T. (2020). Collaborative Cyber Attack Defense in SDN Networks using Blockchain Technology. 6th IEEE International Conference on Network Softwarization (NetSoft). DOI:10.1109/NetSoft48620.2020.9165396

Jonker, M., Sperotto, A., van Rijswijk-Deij, R., Sadre, R., Pras, A. (2016). Measuring the Adoption of DDoS Protection Services. In: Proceedings of the 2016 ACM on Internet Measurement Conference, IMC 2016, Santa Monica, California, USA.

Joshi, B., Vijayan, A. S. and Joshi, B.K. (2012). Securing Cloud Computing Environment Against DDoS Attacks. In 2012 International Conference on Computer Communication and Informatics, January, 1-5. *IEEE*.

Mansfield-Devine, S. (2015). The Growth and Evolution of DDoS. *Netw. Secure*., 10, 13-20.

Pavlidis, A., Dimolianis, M., Giotis, K. and Anagnostou, L. (2020). Orchestrating DDoS mitigation via blockchain-based network provider collaborations. *The Knowledge Engineering Review.*,35. DOI:10.1017/S0269888920000259

Peng, T., Leckie, C., Ramamohanarao, K. (2007). Survey of Network-Based Defense Mechanisms Countering the DoS and DDOS Problems. *ACM Compute. Suvv.* (CSUR). 39(1), 3.

Sattar, Iqra., Shahid, Muhammad. and Abbas, Younis. (2015). A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment. *International Journal of Computer Applications*. 115, 23-27. 10.5120/20173-2370.

Shafi, Q. and Basit, A. (2019). DDoS Botnet Prevention using Blockchain in Software Defined Internet of Things. In Proceedings of 2019 16th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2019, 624-628.

Shah, Z., Ullah, I., Li, H., Levula, A. and Khurshid, K. (2022). Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. *Sensors*, 22(3):1094. https://doi.org/10.3390/s22031094

Sharma, P., Jindal, R. and Borah, M.D. (2020). Blockchain Technology for Cloud Storage: A Systematic Literature Review. *ACM Comput. Surv*, 4, 32.

Spathoulas, G., Giachoudis, N., Damiris, G.P. and Theodoridis, G. (2019). Collaborative Blockchain-Based Detection of Distributed Denial of Service Attacks Based on Internet of Things Botnets. *Future Internet*, 11(11), 226.

Tayyab, M., Belaton, B. and Anbar, M. (2020). ICMPv6-Based DoS and DDoS Attacks Detection Using Machine Learning Techniques, Open Challenges, and Blockchain Applicability: A Review. *IEEE Access*, 8, 1-19. DOI:10.1109/ACCESS.2020.3022963.

The Associated Press: Hackers Used 'Internet of Things' Devices to Cause Friday's Massive DDoS Cyberattack. http://www.cbc.ca/news/technology/ hackers-DDoS attacks-1.3817392. Accessed on January 10, 2017.

Wang, S., Wang, X. and Zhang, Y. (2019). A Secure Cloud Storage Framework with Access Control based on Blockchain. in *IEEE ACCESS.*

Yeh, L.Y., Huang, J.L., Yen, T.Y. and Hu, J.W. (2019). A Collaborative DDoS Defense Platform Based on Blockchain Technology. Twelfth International Conference on Ubi-Media Computing (Ubi-Media). DOI:10.1109/Ubi-Media.2019.00010

Yue, D., Li, R., Zhang,Y., Tian, W. and Peng, C. (2018). Blockchain-Based Data Integrity Verification in P2P Cloud Storage. *in EEE 24th International Conference on Parallel and Distributed Systems (ICPADS).*

Cite this article as: Salwa. H. Alghmadi and Mohammed. I. Alghamdi (2022). Protecting Cloud Infrastructure from DDOS Assaults the use of Blockchain to Achieve Cloud Security. *International Journal of Cryptocurrency Research,* 2(1), 1-6. doi: 10.51483 / IJCCR.2.1.2022.1-6.