Blockchain Technology towards the Mitigation of Distributed Denial of Service Attacks

Darshi Patel

Abstract: ***The Distributed Denial of Service attack become one of the most adverse effects among all Cyber-attack due to the high availability of the internet and unprotected internet-connected communication devices. There are many mitigation solutions available to reduce the risk of DDoS attacks, and the researcher represents many techniques to get rid of the DDoS attacks. The main challenge to identify and mitigate the attack is that attack traffic mixes with the legitimate system user traffic so it becomes very important to block the attack traffic because it costs in terms of money and system reputation. Blockchain technology presents the ideology of decentralized distributed database and transaction without the need of any central authority. But utilization of blockchain is not only limited to the financial sector but supply chain, IoT, hospitality sector used blockchain most. The most attractive features of the blockchain like immutability, distributed makes the use of blockchain for mitigation of various Cyber-attacks, and one of them is DDoS Attacks. The solution of DDoS attacks that utilize the blockchain is still in the infancy phase. In this paper, we propose the review or survey of DDoS attacks solutions based on blockchain. And also present the comparative study of Blockchain-based DDoS mitigation solutions for non-IOT domain or system. This paper also gives brief about the features of this interconnection of two emerging domain named DDoS Attacks and Blockchain Technology.***

Keywords : ***Blockchain, Denial of Service Attacks, Ethereum blockchain, Mitigation, Security, Smart contract.***

I. INTRODUCTION

Distributed Denial of Service Attacks is a threat related to the availability of systems or services. Denial of service is generally performed by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled [1]. The DDoS attack is the Distributed form of the DoS Attacks. In DoS Attack, the Attack traffic source is one particular system or network whereas DDoS Attack is distributed in nature. The flooding or resource consumption in terms of Bandwidth, processing power and memory. The adverse effects of DDoS Attacks are not limited to the financial losses and reduce the reputation of the system; it becomes one of the major sources to spread malware and malicious code in the network or system. Intensity and magnitude are another points of difference between the two categories. The DDoS attack can reach high magnitude and intensity as compared to DoS Attack.

Block the malicious IP which is the origin of the excessive traffic is one of the solutions of the DDoS attack. And as a result, legitimate users get the service on time without any delay. The DDoS attacks are varying in types and solution of this deferent types of attacks are also varies in themselves.

The DDoS attacks are mainly divided into three main categories: 1). Volume-based Attacks 2). Protocol Attacks 3). Application Layer Attacks. The volume-based or volumetric attack's main goal is to saturate the bandwidth of the target. And the magnitude of the attack is measured in bits per second (Bps). Consumption of server resources or communication equipment happens in Protocol Attacks which is measured in packets per second (Pps). Whereas Application Layer Attacks mainly targets the web server by sending the legitimate requests and measurement unit to map the intensity of this type of attack is Requests per second (Rps). Another classification of the DDoS attacks is based on which the network layer is targeted for performing the DDoS attacks.

But when talking about the solution to these different types of attacks, various techniques and types of solutions are present in the market. The main goal is to identify the attack traffic and block the illegitimate traffic. Several Hardware or mitigation equipment are used to detect and manage the traffic flow whereas some mitigation service providers give the DDoS attacks mitigation services on-demand bases or full time. However, some organizations use the hybrid approach to get rid of the attacks. These techniques and solutions mainly fall majorly into collaborative or non-collaborative (individual). In a collaborative approach, the collaboration between the networks is used during the DDoS attacks in terms of detection, defense, and Solutions.

DDoS attacks are the simplest and common type of cyber-attacks but it is very difficult to deal with when magnitude and intensity of attacks are very high. A very large-scale attack on GitHub, a popular online code management website was detected in February 2018 with 1.7 Tbps. Along with that, the 2016 Dyn attacks (also called Mirai botnet), The 2013 Spamhaus attack, the 2000 Mafiaboy attack, the 2007 Estonia attack are some of the famous examples of the DDoS Attacks. The DDoS attacks frequency and magnitude are increasing day by day along with attackers are come with a novel strategy to perform the DDoS attacks. So, this paper presents a review of some of the DDoS mitigation solutions through one of the most leading network technologies named Blockchain Technology [1]-[3].

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author

Darshi Patel*, Research Scholar, Gujarat Vidyapith, Ahmedabad, India. Email: pdarshi94@gmail.com

II. BACKGROUND

A. Blockchain Technology

Blockchain is the inventive concept of managing the distributed ledger in the untrusted environment without the help of any central party. In other words, it simply replaces the client-server architecture which is the core element of the network services.

The cryptography and digital signature are the core element of blockchain technology. It provides the immutability, cryptographically secured, reliability, integrity to the ledger. At the same time, it prevents the ledger from a single point of failure because of distributed in nature. Blockchain originally designed for transferring the tokens in the decentralized peer to peer network. Transferring process does not need any third party to act as a trust manager but it is directly performed between the peers with the help of consensus protocols. Proof of Work, Proof of Stake, Proof of concept and Practical Byzantine Fault Tolerance (PBFT) are some of the consensus protocols.

The crypto-currency is one of the famous applications of Blockchain Technology. But its use cases are not limited to it. Supply chain, asset management, health care, voting is some of the areas which utilize the blockchain technology. The blockchain is mainly categorized in public and private blockchain based on the participation and privileges of the user in the system.

The most well-known application of the Blockchain is Bitcoin and Ethereum. The Bitcoin provides the secure transfer of payment without any third party in a completely decentralized manner. Whereas the Ethereum protocol provides a distributed computing platform with programmability on the blockchain. One of the most attractive features of Ethereum blockchain is smart contracts, which are code that can automatically enforce the terms of the contract without any third party [4][5].

B . Existing DDoS Mitigation Technique

The DDoS mitigation approach is mainly divided into two categories: Collaborative DDoS Mitigation approach and Non-Collaborative DDoS Mitigation approach. Mainly all the solutions used for DDoS mitigations majorly fall into these categories.

In the Collaborative DDoS Mitigation approach, the collaborative networks provide the supports in the detection, defense, and prevention. The advantage of this approach is attack traffic is blocked very close to the origin of the attack. As well as the attack is also signalized so that others are being alert about the attack.

On the contrary, the Non-Collaborative DDoS Mitigation approach is implementing all the possible strategies for own network without being part of the collaboration of networks. In this scenario, the web-servers rely on their own mechanism so as a result several domains are overloaded with the traffic because attacks may not be blocked close to the origin.

The protocol named DOTS specially designed by the Internet Engineering Task force (IETF) includes Intra and Inter organizations communication mechanism. DOTS is protocol provides the sharing or advertising of the white-listed and blacklisted IP addresses to organizations. For that purpose, it requires client-server architecture in both centralized as well as distributed domains. The architectural complexity is the significant reason behind less implementation and adoption as a solution [12].

DDoS mitigation typically involved analyzing the internet traffic through detection algorithms; after that filtering process is performed through the filter then it sends to the network. When organization is not performing this work, then third party organizations or services are required. Common techniques used by a third party for DDoS mitigation includes:1). DNS-based routing; 2). BGP prefix announcements; 3). In-line filtering; 4). A hybrid that consists of a local appliance and a third-party component based on either DNS or BGP.

The DNS-based routing all the visitors who requested to visit the website are first redirected to the scrubbing center then based on the filtering and validation, the legitimate user may further route to the original website. And malicious traffic will be dropped during the filtration. In-line filtering the traffic is not routed to the third party such as scrubbing center but it is processed on-premise. It is especially done through the special mitigation equipment or hardware that place in between the internet and the organization's network.

The BGP based and hybrid technique focus on the idea that when the attack traffic is not handled by the customer network then it diverted to the scrubbing center, where traffic is filtered then clean traffic is redirected to the customer. A hybrid technique consists of a local appliance and a third-party component based on either DNS or BGP.

In these days, DDoS mitigation service providers and CDNs are giving the mitigation service on demand and full-time bases [6].

III.BLOCKCHAIN BASED MITIGATION OF DDOS ATTACKS

Blockchain is the distributed ledger secured using the cryptography. All the transactions hashed then included in the block, which is further linked to the lastly added block of the blockchain. So, when compromised with the single data of blockchain, the whole chain is changed as a result it is impossible to hack or compromised. As well as the blockchain is immutable, cryptographically secured and integrity added value for any system. The significance of blockchain is such that it runs in any infrastructure without having additional requirements and providing the securing data in the un-trusted environment. In collaborative DDoS mitigation, the secure networking infrastructure is a prerequisite for signalized the DDoS attack in a various domain so the researchers consider them as a solution for mitigating the DDoS attacks.

A. Multi-domain DDoS Mitigation Based on Blockchains

Bruno Rodrigues proposed Multi-domain DDoS mitigation using Blockchain. This architecture provides the DDoS mitigation of multiple Domains through the Blockchain and novel networking concept named software defined networking (SDN).

The blockchain technology has become a medium of sharing the attack information across the multiple domains whereas the SDN and Network Function virtualization (NFV) is utilized as scale the defense capabilities in a single network. The reason behind using the blockchain as signalizing the attack to inter-domain is that it reduces the complexity of distributed protocol as well as broadcasts the attack information in a secure way.

Additionally, to develop the customized security policies and management to services is very efficiently handled by the SDN.

Ryu SDN controller is used which is open-source and supported a range of application management APIs. The role of NFV is to enforce the security policies through the virtual functions of generic hardware. The NFV is implemented through the VNF-BC which is the virtual appliance work with a network management system and flow-records.

The Ethereum blockchain is used to build this infrastructure for signalized the attack to the cooperative domains. The reason behind the utilization of Ethereum blockchain is that a new block is published in every 14 seconds timeframe so that a new address reporting task is performed very faster and secure way. Additionally, the Smart contracts are used for reporting the whitelisted and blacklisted IP address and sharing the characteristics of attacks and reporting entities. The participant's node of Ethereum blockchain can report the addresses by simply running the solidity based smart contract. But the authenticity of the reporting entity is checked before addresses are included in the new block. The certificate issuing entity is required for issue the certificate to the reporting entity. For that, the certificate issuing entity and additional public key infrastructure are the additional requirements of this infrastructure [7].

B. Cochain-C: An Intra- and Inter-Domain DDoS Mitigation Scheme Based on Blockchain Using SDN and Smart Contract

Cochain-SC presented the DDoS mitigation approach which includes Intra and inter-domain mitigation solution through the blockchain technology (Figure-1). The Intra and inter-domain mitigation are integrated so it serves a nearly complete solution for the DDoS attacks. The intra-domain mitigation scheme implements various methods with the help of software defined networking (SDN) for detecting and blocking the attack traffic within the domain. The collaborative approach is deployed in inter-domain through the blockchain.

Intra-domain mitigation scheme consists of three methods in the context of the SDN. 1). Intra Entropy-based scheme (I-ES) which keep track of the randomness of data inside the domain using the popular network monitoring tools named SFlow. 2). Intra Bayes-based scheme (I-BS), mainly classify the traffic based on the illegitimate flows and entropy values. And 3). Intra-domain Mitigation (I-DM) scheme for mitigating or blocking the malicious traffic inside the domain.

For implementing the solution in Inter-domain, blockchain-based architecture is used for collaborate between the various domain. It uses the Ethereum blockchain as a collaboration platform and Ethereum smart contracts providing the collaboration or interconnection between all SDN based domains. Especially, blockchain is used for signalized the DDoS attack to all collaborative domains in a decentralized and secure manner. The Cochain-SC integrates the Intra and Inter-domain mitigation scheme so that the mitigation solution works very effectively during the attack and block the attack traffic near the origin of the attack. So, packet forwarding cost is decreased and get relief from the amplification types of attacks [8].

C. Enabling a Cooperative, Multi-domain DDoS Defense by a Blockchain Signaling System (BloSS)

BloSS presents the solution which used the blockchain to reduce the complexity of the existing DDoS signalling solution with incentive policy for the cooperation between the domains. The operation cost of the existing infrastructure is reduced due to use of blockchain as a medium to distribute attack information along with incentive policy motivates the cooperators. A deployment of hardware which helps in reduces the complexity of DDoS attack signaling, as a part of a cooperative network defense system.

The gossip-based protocol is used by the existing approaches to mitigate the DDoS attacks in multiple domains. The combination of Blockchain and Smart contracts gives a very effective solution for signaling the attack information to multiple domains without requirements of additional infrastructure and deploy independently from the existing infrastructure. For that purpose, the smart contracts work as information exchanger among the Autonomous System. The Dapps pay attention on the Autonomous Systems' interaction for the cooperative defense. The consortium-based blockchain is work as the intermediate trust agent among unregistered and untrusted Autonomous Systems. The incentive mechanism is mainly demotivating the peers from free-riding (consuming resources without contributing). The peers get rewarded as per the security policy for routing a minimal number of IP addresses. The Ryu SDN controller is used to monitor/enforce rules in the OpenFlow switches. The BloSS also implement the system through actual hardware and test the performance of the system. As a result, the security of the data and the whole system is increased through the utilization of the consortium-based blockchain. While the performance of the system mainly depended upon the latency due to block creation and retrieval data from the off-chain storage [9].

D. A Reputation Scheme for a Blockchain-based Network Cooperative Defense

A Reputation Scheme for a Blockchain-based Network Cooperative Defense is presented by Andreas Gruhler et al. This paper presents the incentive scheme for the participants of the distributed infrastructure. Because when the participants of the cooperative multi-domain DDoS mitigation scheme leave the network because of a lack of incentive and reputation. Then it becomes disadvantageous for DDoS system as well as participants who give an active contribution towards maintaining the system.

So, this scheme serves the reputation management to the blockchain Signaling system (BloSS).

DDoS attacks might be originated in remote networks without a close relationship between the governing Internet Service Providers (ISP). Thus, a reputation system is to encourage truth-telling and discourage free-riding between providers without a trust relationship.

This Reputation scheme does not mitigate the DDoS attack directly but it prevents the attack target from free riding and mitigators from the false reporting the Ip Address.

A mitigation task index is created in a MongoDB database, using this data as an input Reputation API develops the reputation matrix. Then identity smart contracts hold the identity of all the participating domains. The real identity of the domain is preserved in pseudonyms ID. For a particular reputation claim, the interaction between the claim owner and customers is traceable through the blockchain. Reputation contracts, reputation score and historic data about the behavior of peer forms the foundation of trust and visible to all peers. Public Blockchain is used to share the malicious IP addresses to potential mitigators. Based on all information, both contract parties take a decision about participating in a contractual relationship or not. Then this reputation data is further shared with the interested peers. This system demotivates the attack targets and mitigators from the system because of the incentive mechanism [10].

E. Decentralized CDN and DDoS Protection on the Blockchain

The start-up named Gladius established recently in 2017 by Niebylski and his friends at the University of Maryland developed an innovative way of utilizing blockchain for mitigating DDoS attacks. Now a day, the majority of DDoS solution provider companies use Content Delivery Network (CDN) in their solution as well as CDN to improve the user experience and speed of the website. Gladius use Ethereum blockchain for user's transaction and peer to peer network is set up on top of the blockchain. The company presents the instant bandwidth sharing mechanism for defense against the DDoS attack. The unused bandwidth of individual and companies are collected and shared to the system which is under attack so that the website becomes stable against the attack. This distributed solution is used by the Gladius to overcome the problem of shortage of bandwidth during the DDoS attack. The user of unused bandwidth is an incentive according to the predefined standards. Along with that, Rate limiting, Intelligent Geo Matching, and CDN services offered which helps to prevent the site from the DDoS attacks [11].

IV. DISCUSSION AND ANALYSIS

Based on the comparison between the five alternatives to mitigate DDoS attacks using the blockchain have some benefits as well as limitations. Main Comparison Parameters: Type of Blockchain, Intra/Inter-domain solution, attack detection, and mitigation and Implementation are mainly taken into consideration for the comparative study.

TABLE - 1: Comparison among various Blockchain oriented DDoS Mitigation Systems

NO	Solutions	Blockchain Type	Intra/Inter Domain solution	Detection/ Mitigation	Implementation
1	Multi-domain DDoS Mitigation Based on Blockchains	Public	Inter		NO
2	Cochain-C: An Intra- and Inter-Domain DDoS Mitigation Scheme Based on Blockchain Using SDN and Smart Contract	Public	Both	YES	YES
3	Enabling a Cooperative, Multi-domain DDoS Defense by a Blockchain Signaling System (BloSS)	Consortium based	Both	NO (use existing modules)	YES
4	A Reputation Scheme for a Blockchain-based Network Cooperative Defense	Public	Inter		YES
5	Decentralized CDN and DDoS Protection on the Blockchain	Private		YES	YES

A. The Advantages

The Blockchain oriented DDoS mitigation solutions basically use the blockchain as part of their solution. So mainly the inheritance features of the blockchain technology are also present in the existing solutions which utilize the blockchain as a solution. When implemented the solution of DDoS attacks across multiple domains, the first questions are that managing the trust across multiple domains. The blockchain has operating power to run between the untrusted domains and manage the trust through the system without having any central authority. This become one of the reasons to utilize blockchain for mitigate DDoS attacks.

In cooperative DDoS attacks mitigation, the signalization of attack information among the various cooperators becomes the key solution. Additional infrastructure and protocols become prerequisites for advertising the attack information in a secure manner. Blockchain has an inbuilt feature like cryptographically secured and broadcasting information to the public. So blockchain becomes adventitious to share the attacks information without having any special network infrastructure. The blockchain is very simple to deploy in any networking system and store and transfer data in a secure manner.

All the data which secured in the blockchain also immutable. So that hacking and data modification is not possible in existing solutions.

Concerning security, the comparative study of five solutions shows that the blockchain proposes a secured, immutable, and trusted environment for the data and system.

In summary, the blockchain provides features like distributed, cryptographically secured, immutable, trust management, which become the key requirement to construct any full-fledged DDoS solution.

B. Problem still remains

Due to the distributed nature of the DDoS attacks, single-ended solutions are not appropriate. And blockchain has many interesting features in one system that catches the attention of the researcher towards developing a solution through blockchain. But some problems remain still unsolved after implementation of blockchain as a solution.

Blockchain becomes the suitable medium of advertise the attacks information across the various domains. For sharing the attack information, the blacklisting IP addresses are stored into the block, and it has limited storage. So, storage becomes one of the major concerns when implementing the blockchain as a solution.

In terms of performance, the block latency time (especially block creation, and retrieval information from the block) is very high. And in Ethereum a new block is added into the chain after 14s. So, it may affect the performance of the system. Additionally, the scalability problem of blockchain also influences the system in the long term [5].

V. CONCLUSION

Revering blockchain-oriented DDoS mitigation solutions, blockchain technology provides an innovative way to mitigate DDoS attacks, especially the collaborative attacks. The DDoS attacks are distributed and blockchain serves for the ledger management solutions in the distributed world. Blockchain has stronger features like immutability, cryptographically secured, reliability and distributed nature based on which blockchain performs as a powerful tool in any network infrastructure as a solution of DDoS attacks. In many exiting solutions, the blockchain is used as the attacks information sharing system. But blockchain is not limited to advertise attacks information but it has capability to serve as a mitigation solution in many aspects like detection, prevention and much more. While overcome from some of the limitations like the storage and scalability problem, which have to be addressed by the research community before the blockchain-based DDoS solutions can be implemented in practice.

REFERENCES

1. Imperva. “Distributed denial of service attack (DDoS) definition.” imperva.com. https://www.imperva.com/learn/application-security/ddos-attacks/ (accessed Jan. 20, 2020).
2. Denial-of-service attack. “Denial of Service Attack.” Wikipedia.org. https://en.wikipedia.org/wiki/Denial-of-service_attack (accessed Jan. 20, 2020).
3. CISA. “Understanding Denial-of-Service Attacks.” Us-cent.gov. https://www.us-cert.gov/ncas/tips/ST04-015 (accessed Jan. 20, 2020).
4. S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” White Paper, 2009. [Online]. Available: https://bitcoin.org/en/bitcoin-paper.
5. V. Buterin, “Ethereum: a next-generation smart contract and decentralized application platform,” White Paper,2014. [Online]. Available:https://github.com/ethereum/wiki/wiki/.
6. C.J.T.M. Schutijser, “Comparing DDoS Mitigation Techniques,” Semantic scholar, 2016.
7. B. Rodrigues,T. Bocek, B Stiller, “Multi-domain DDoS Mitigation Based on Blockchains,” presented at Security of Networks and Services in an All-Connected World. 2017, 185-190, 2017.
8. Z. Houda, A. Hafid, L. Khoukhi, “Cochain-SC: An Intra- and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract,” IEEE Access: Advanced Software and Data Engineering for Secure Societies., Vol. 7, pp. 98893-98907, Jul. 2019, doi:10.1109.
9. B. Rodrigues , T. Bocek, B. Stiller, “Enabling a Cooperative, Multi-domain DDoS Defense by a Blockchain Signaling System (BloSS)”. Published in 42nd IEEE Conference on Local Computer Networks 2017 (LCN 2017), Oct. 2017, pp.185-190.
10. A. Gruhler, B. Rodrigues, B. Stiller, “A Reputation Scheme for a Blockchain-based Network Cooperative Defense,” 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), May 2019.
11. Gladius, “Gladius Network Project,” White paper, 2017 [Online]. Available: https://static2.coinpaprika.com/storage/cdn/whitepapers/17499.pdf
12. Nishizuka, K. Xia, L. Xia, J. Zhang, D. Fang, L. Gray. “Inter-organization cooperative DDoS protection mechanism.” Tools.ietf.org. https://tools.ietf.org/ html/draft-nishizuka-dots-inter-domain-mechanism-02 (accessed Jan. 20, 2020).

AUTHOR PROFILE

Ms. Darshi Patel, has completed her post-graduation in computer science and information technology from Gujarat University, Gujarat. And she is pursuing her Ph.D. in computer science from Gujarat Vidyapith, Gujarat. Her research interests include Distributed ledger technologies, Blockchain Technology and Cyber security.