DDoS mitigation techniques in IoT : A Survey

Dhanya M Rajan
Department of Computer Science and Engineering
Hindustan Institute of Technology and Science
Chennai, India
dhanyamrajan83@gmail.com

Sathya Priya S
Department of Computer Science and Engineering
Hindustan Institute of Technology and Science
Chennai, India
sathyap@hindustanuniv.ac.in

2022 International Conference on IoT and Blockchain Technology (ICIBT) | 978-1-6654-2416-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICIBT52874.2022.9807799

***Abstract*— Cities are becoming increasingly smart as the Internet of Things (IoT) proliferates. With IoT devices interconnected, smart cities can offer novel and ubiquitous services as well as automate many of our daily lives (e.g., smart health, smart home). The abundance in the number of IoT devices leads to divergent types of security threats as well. One of such important attacks is the Distributed Denial of Service attack(DDoS). DDoS attacks have become increasingly common in the internet of things because of the rapid growth of insecure devices. These attacks slow down legitimate network requests. Although DDoS attacks were first reported in 1996, the sophistication of these attacks has increased significantly. In mid-August 2020, a 2 Terabytes per second(TBps) attack targeting critical infrastructure, such as finance, was reported. In the next two years, it is predicted that this number will double to 15 million attacks. Blockchain technology, whose development dates back to the advent of the internet, has become one of the most important advancements to come along since that time. Several applications can use this technology to secure exchanges. Using blockchain to mitigate DDoS attacks is discussed in this survey paper in diverse domains to date. Its purpose is to expose the strengths, weaknesses, and limitations of the different approaches to DDoS mitigation. As a research and development platform for DDoS mitigation, this paper will act as a central hub for a more comprehensive understanding of these approaches.**

Keywords*— *Blockchain Internet of Things(IoT), Distributed Denial of Service (DDoS) attack, DDoS mitigation.

I. Introduction

Internet-connected devices as well as new technologies like the IoT, which provide anytime-anywhere capabilities, will add to the number of devices getting connected, as they become more popular. An IoT system integrates physical devices that can react, communicate, and operate autonomously [1]. This allows for new services to be optimized and enabled across a broad array of applications. A major security concern with IoT systems is the threat posed by the DDoS attacks. In DDoS attacks, internet-connected devices overwhelm networks and computers with excessive traffic. Typical targets include financial institutions, broadcasting networks and Internet-based services. Many of the DDoS attacks have exploited the Simple Service Discovery Protocol (SSDP). These protocols put Internet-connected devices at risk (such as CCTV cameras, wireless routers, and IP-based devices). DDoS attacks against Dyn′s DNS servers in October 2016 relied heavily on IoT devices.

In DDoS, malicious traffic is used to overwhelm the target system and infrastructure. Malware is typically distributed through botnets, which are networks of computers and other devices controlled by an attacker that is infected with malware. The availability of systems in the network one of the major aspects which is adversely affected by many DDoS attacks. Business and industry are not the only ones affected, as government agencies and infrastructures, as well as the networks used by the national defense forces in each country, also face the same problem. Media and political websites are often targeted by hacktivists, who use DDoS attacks to attack them. The social and political consequences of these attacks go beyond just financial losses. As a result of DDoS attacks carried out against US banks [2], network operators and ISPs worldwide are suffering from very destructive and stealthy attacks that are becoming more powerful, destructive, and stealthy [3]. Small numbers of nodes launching malicious attacks make them easier to detect [4,5]. A DDoS attack consists of a large number of nodes, and their collective behavior impedes the ability to serve requests that are not malicious. By sending a large number of packets over the network without interrupting them, the attacker can lead the victim to believe they are legitimate. This means that the host communicates simultaneously with multiple devices and with multiple types of packets [5].

The most common type of DDoS attack is flooding, which disables network bandwidth and blocks all legitimate requests. Other attacks include brute-force, spoofing, and flooding, which are currently designed for single victims. Current survival methods rely on the victims′ ability to detect and react to attacks. Network-wide flooding, however, necessitates mitigation measures before the flood hits the victims, which makes it an attractive strategy for multi-targeted attacks [6, 7].

978-1-6654-2416-5/22/$31.00 ©2022 IEEE

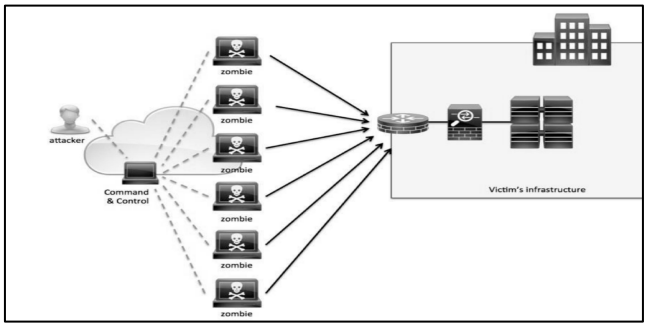

Figure 1: Distributed Denial of Service (DDoS) attack [6]

During a DDoS attack, attackers use infected devices to overload target resources (such as the network bandwidth and the computer CPU) with undesired traffic. To launch DDoS attacks, attackers typically use thousands of compromised devices (referred to as zombies). Fig. 1 shows how zombies attempt to disrupt legitimate users by sending large amounts of traffic (see DDoS attacks). DDoS attacks fall into two distinct categories: IP-based real-source attacks and denial-of-service attacks using distributed reflections. DRDoS attacks employ botmasters, zombies, and reflectors. It is normal for a botmaster to send zombies to flood a target as part of a DDoS attack. It is the botmaster who instructs each zombie to send multiple packets to other devices called reflectors, which are based on the victims IP address instead of the source IP address.

Many organizations ignore DDoS protection. It is very expensive and requires a large human and financial resource, and that is the major reason why most of them do not pay any attention to it.

II. DDoS ATTACK TYPES

The DDoS attacks are intended to temporarily stop or interrupt a server′s service to prevent legitimate users from logging in to an online service. Multiple compromised computers are incorporated in DDoS attacks which act as attack traffic sources. DDoS attacks use networks of Internet-connected machines to carry out their attacks. Computers and IoT devices can be exploited. By using malware, cyber-attackers can remotely control computers and other devices (such as Internet-connected devices). Bots (or zombies) are devices that communicate remotely, and a botnet is a network of bots. An attacker can send instructions via the network to the bots within the network to direct an attack. Botnets attack targeted servers and networks by sending requests to every address in the target′s IP address, which can overload the servers and degrade network performance.

Attacks that are based on volume are classified as 1) volume-based attacks, 2) protocol-based attacks and 3) application-layer attacks. Volumetric attacks are designed to overburden targets′ bandwidths. The number of bits transmitted per second (Bps) measures the intensity of an attack, while packets sent per second (Pps) determine the number of servers′ or equipment′s resources devoted to the attack.

A .*VOLUME-BASED ATTACKS*

An amplification engine and other methods, such as botnets, may be used in tampering attacks to send large amounts of data to the target. This causes the target to be overwhelmed, causing congestion. There are two kinds of flooding attacks: UDP floods and ICMP floods. The goal of the attack is to overload the website with traffic, measured in bits per second (Bps).

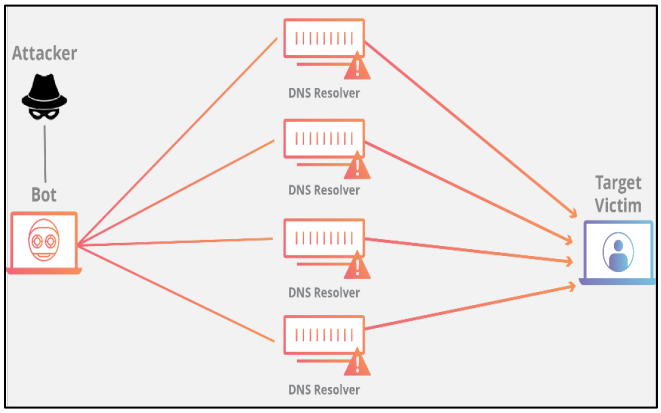

Figure 2: Volume-based attack model [6]

a. UDP Flood

DDoS attacking and flooding random ports on remote hosts using User Datagram Protocol (UDP) packets are called UDP floods. The host is responsible for periodically looking for applications on that port and responding with ICMP 'Destination Unreachable' packets if the application cannot be reached. This consumes the host′s resources and makes the host inoperable.

b. ICMP Flood

ICMP flood attacks are similar to UDP flood attacks in the sense that packets are automatically sent rapidly without waiting for a reply. A system can be significantly slowed down by this type of attack as inbound and outbound bandwidth is consumed. Furthermore, the victim′s servers receive requests for ICMP echo replies, further slowing down the system.

B. *PROTOCOL ATTACKS*

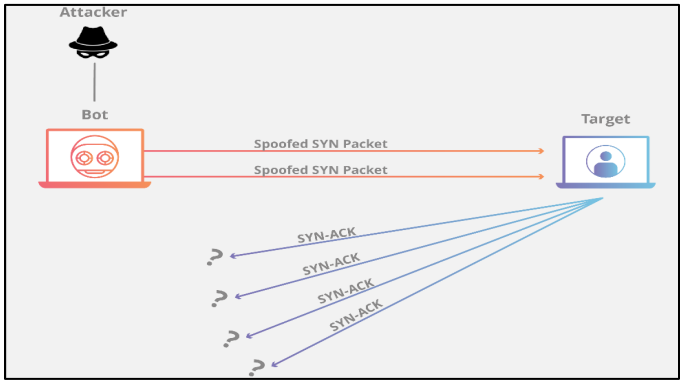

Figure 3: Protocol attack model [7]

A protocol attack also called a state-exhaustion attack, disrupts services when servers or network equipment are overloaded. Protocol attacks leverage weaknesses at layer 3 and layer 4, such as SYN floods and fragmented packet attacks. Smurf DDoS is another example of a protocol attack utilizing these weaknesses. Each of these processes consumes server resources or equipment in the communications chain, such as firewalls.

a. SYN Flood

The floods of SSYN function like workers in the supply rooms that receive requests from the front. After a request is received by the worker, he or she retrieves the package and waits for confirmation before handing it over. However, as the worker continues to receive more requests for packages without confirmation, he or she eventually becomes overwhelmed, cannot answer any more and the requests stop getting answered.

b. Ping of Death

Ping of Death attacks involves sending a large amount of malformed or malicious pings, each of which may be 65,535 bytes long. However, Data Link Layer settings restrict the frame size, such as 1500 bytes on an Ethernet network. In the case of IP packets of this size, each packet is typically split into multiple packets (called fragments), and each fragment is reassembled by the recipient host.

C. *APPLICATION LAYER ATTACK*

Often referred to as the 7th layer of the OSI model (since it reaches the point when a target′s resources are exhausted), an attacker targets the layer of web pages that are generated by a server and served through HTTP requests. Clients make HTTP requests at a very low cost, but Web servers often have to load multiple files and query databases to create a page, so they are costly. Getting infected by Layer 7 traffic, which is impossible to distinguish between malicious and legitimate, can be very difficult. You may see the low-and-slow attack, GET/POST flood, or attacks exploiting Windows, Apache, and OpenBSD security vulnerabilities. Typically, Requests per second (Rps) is used to assess the scale of these attacks, because they are composed of seemingly innocent requests being sent to a webserver to crash it. These legitimate requests are measured as legitimate requests.

a. HTTP Flood

The denial-of-service attack is essentially the simultaneous refreshing of several web browsers, which results in a flood of HTTP requests. This category of attack can be manageable or complicated. Depending upon the IP address, referrer, and user agent, these may be simple or complex versions. In simple versions, URL targets and user agents may be randomly selected from a pool of IP addresses. Complex versions use several IP addresses and URL targets may be randomly chosen.

III. BLOCKCHAIN

The concept of blockchain, which uses public-key cryptography and digital signatures, is an interesting and innovative one that has many applications, including cryptocurrencies, health records, and other fields. The goal of a secure network is to meet the most crucial requirements of information security, such as maintaining the integrity of transactions, preventing fraud, providing effective authentication, being immutable, and being reliable. In addition to the decentralized infrastructure provided by the blockchain, the technology had been initially designed for peer-to-peer transactions between users, which eliminated the need for some sort of third-party intermediary [30]. Blockchains, such as the Bitcoin blockchain, are types of new technology. Ethereum is also a type of blockchain, along with other blockchains. Bitcoin was created by Satoshi Nakamoto as a peer-to-peer electronic cash system described in a white paper. As a solution to double-spending of digital currency or bitcoins created by Satoshi Nakamoto, the bitcoin blockchain eliminates the duplication and retransmission of a currency or bitcoin resulting in financial irregularities. Vitalik Buterin first introduced Ethereum as a white paper in 2013. Later, the Ethereum software was developed by the company Ethereum Switzerland GmbH. As opposed to Bitcoin, Ethereum seeks to decentralize computer systems based on client-server models, which currently rule the industry [10].

There is nothing more than a blockchain as a distributed ledger, which is maintained in a database and records transactions chronologically. As such, a blockchain is typically a series of data structures that are linked together that store multiple transactions in a chain. Blockchains differ significantly in size and generation duration. Bitcoin blockchains have larger block sizes (*1 MB) than Ethereum blockchains (*2 KB). The Bitcoin blockchain generates a block every 10 minutes, while the Ethereum blockchain generates a block every 12-14 seconds [10]. A block of 1 MB size has been generated on the Bitcoin blockchain within the first 10 minutes. As a result, huge processing and energy resources are required for the generation of blocks.

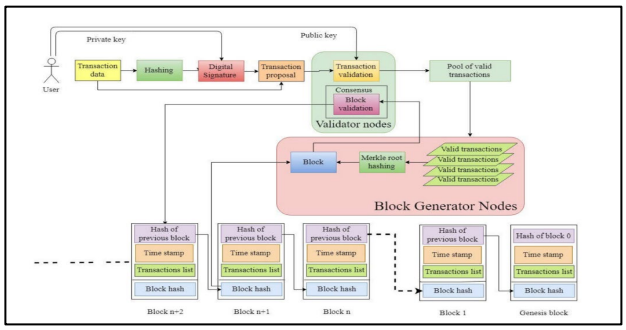

Figure 5: Transaction execution flow in a blockchain [11]

The nodes who make a block on the Bitcoin blockchain are rewarded with bitcoins (cryptocurrencies) for solving complicated problems. Therefore, the blockchain keeps growing in size since each node maintains its copy of the chain, meaning each new block is added to the chain in the same way

a new block is generated and verified. Transactions between parties are stored within blocks of the blockchain network for safe, tamper-proof storage. Now-a-days, the blockchain network is used to strengthen the operations in supply chain, processing logistics, identity and access management, diverse types of security procedures, financial tasks, and other online activities [11].

IV. MITIGATING DDOS ATTACKS USING BLOCKCHAIN

The use of blockchains in peer-to-peer networks is becoming more widespread. Blockchains store records and transactions separately from banks and authentication servers. Only authorized users can view the records and transactions to validate the change [24]. Researchers consider Blockchain to be a DDoS mitigation solution due to its independently accessible properties of being independent of any network and its cryptographic significance. The paper reviews major DDoS mitigation techniques that utilize recent blockchain technologies.

Among the applications of Blockchain technology, cryptocurrency is the most widely used. In general, Blockchain is divided into two types: Bitcoin Blockchain and Ethereum Blockchain. Bitcoin Blockchain is primarily used to transact digital assets, while Ethereum Blockchain is used to execute smart contracts. These smart contracts run on sandboxed Ethereum Virtual Machines that execute, verify and enforce them on their own. Smart contracts are software that performs agreements [26]. DDoS researchers mainly use the Ethereum blockchain and smart contracts as part of the DDoS mitigation process (in terms of gas). DDoS attacks are prevented by smart contracts, and the transactions are based on gas (in terms of cost).

Using the blockchain-based Co-IoT approach [13], Zakaria et al. [13] provide effective mitigation along existing attacks′ paths as well as efficient mitigation close to the source of attacks. Using Ethereum official test network Ropsten[14], Co-IoT implements its infrastructure on an open blockchain platform. In the course of this project, contributions have been made regarding the design of a decentralized, efficient, and secure DDoS collaboration scheme (Co-IoT) built on blockchain technology leveraging smart contracts. An Ethereum smart contract-based scheme was developed to establish low-cost, decentralized, secure and flexible DDoS collaboration among multiple SDN domains, to mitigate against DDoS attacks.

The paper by Shivansh and Ruhul (15) proposes a collaborative approach to DDoS mitigation through the use of SDN and Blockchain. This paper discusses DDOS mitigation by considering an emerging technology, the Blockchain. In addition to its application in large to small organizations, this network architecture can also be used in multiple domains as a comprehensive DDoS mitigation security mechanism. It utilizes a very flexible design that will assist in reducing intrusion attacks in a variety of domains. By using an SDN controller that can authenticate users and filter their traffic, validating legitimate users can be achieved. Then, the ABS that we introduce can increase the scalability of the trust list by providing multiple nodes. Lastly, Distributed Ledger provides an impenetrable way of mitigating DDoS attacks.

According to Rodrigues et al [12], a blockchain-based architecture for collaborative DoS mitigation is presented, which is suitable for protecting users across multiple networks under the control of autonomous systems. This architecture consists of three components: ASes, customers, and a blockchain/smart contract. Both ASes and customers are capable of publishing transactions into the blockchain. The associated ASes will receive the addresses that are to be blocked or authorized from the blockchain as soon as possible

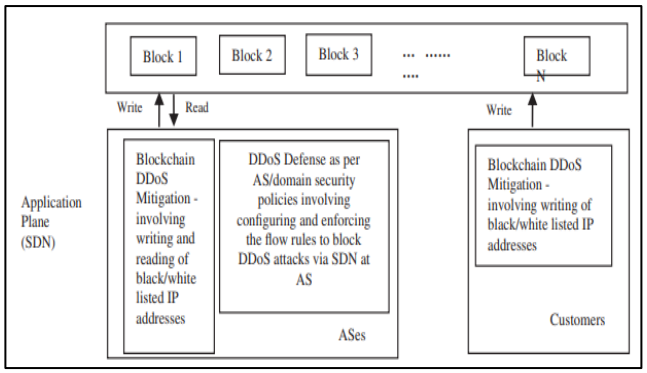

Figure 6: Architecture for collaborative DDoS mitigation based on Blockchain proposed by Rodrigues [12]

Researchers need to put a lot of effort into developing blockchain-based DDoS protective measures, as they should travel a long way to achieve integrity, immutability, and reliability. Blockchain-based DDoS protective measures provide a distributed ledger management system that ensures transaction integrity.

The paper by Rajeev et al. (16) describes how the use of blockchain technology. It is one of the newest and most promising innovations for fighting distributed denial-of-service attacks. Due to the decentralized, secure, and stable architecture of the blockchain platform, blockchain applications have been applied to numerous industries, including financial services and gaming. The paper also compares existing blockchain-based technologies with DDoS attacks. Blockchain nodes can also be authenticated among themselves. A smart contract implementing a DDoS mitigation architecture is deployed in a private blockchain by Nupur et al. [17]. Blockchain technology enables the sharing of protection across network domains, thereby enhancing network security by facilitating collaborative DDoS mitigation. Through smart contracts, one can distribute rules across all host devices, and SDN can be used to enable dynamic services and security policies. This proposal would allow autonomous systems to establish their DPS (DDoS Prevention Service) without giving up control over their networks. The author discusses how hybrid enterprises can protect themselves from the widespread

and rapidly evolving threat of Distributed Denial of Service (DDoS) attacks.

The authors of Bruno et al. [18] hypothesize that Distributed Denial-of-Service (DDoS) in defence systems cannot implement a comprehensive strategy to counter large-scale attacks. Coordinating protection efforts offer a solution to this problem. However, current DDoS signaling protocols stand in the way of delivering a fully integrated and distributed defensive system. This is a novel approach to signaling DDoS attacks using hardware to produce a cooperative network defence system, known as the Blockchain Signaling System (BLOSS).

According to [19] Zacharia et al. (paraphrase), BrainChain is the solution for protecting permitted blockchain nodes from DDoS attacks, the largest ever experienced in software-defined networks (SDNets). BrainChain comprises four schemes: (1) Flow statistics collection scheme (FS) to gather flow statistics efficiently using sFlow; (2) Entropy-based scheme (ES) to quantify the chaos in network features; (3) Bayes Network-Based Filtering scheme for differentiation of illegitimate DNS requests based on entropy values (4) DNS Mitigation scheme to mitigate the illegitimate flows (i.e., illegitimate DNS requests) effectively. In experiments, Brain Chain has demonstrated a high degree of detection and mitigation of attacks (DNS amplification attacks) rapidly and with a low false-positive rate, which makes it excellent for protecting blockchain applications from DNS amplification attacks. We propose a scalable collection mechanism (FS) that reduces data plane-control plane exchanges by leveraging the sFlow protocol. This reduces the amount of data plane-control plane exchanges.

This paper attempts to propose an alternative approach to detecting and mitigating DNS amplification attacks in the context of software-defined networks (SDN). WisdomSDN performs both DNS amplification detection and mitigation. Our proposal involves the following: We propose (1) a proactive and stateful DNS mapping scheme (PAS) operating proactively by excluding amplified DNS responses, and (2) a machine learning sensor to detect DDoS attacks intended to identify, in real-time, illegitimate DNS requests. This module includes (a) Scheme for Flow statistics collection (FSC), which gather the features of flows in a coherent and scalable way using sFlow protocol; (b) Scheme for Entropy calculation (ECS) to measure the randomness in the network traffic; and (c) Bayes Network-based Filtering scheme (BNF) to classify, based on entropy values, illegitimate DNS requests; and (3) The DNS Mitigation Scheme (DM) mitigates illegitimate DNS requests effectively.
A review, or survey, is presented by Darshi [8] of DDoS attack mitigation solutions for non-IoT domains, systems, or domains based on blockchain technology. It also describes the similarities and differences between DDoS attacks and blockchain technology under an emerging domain called DDoS attacks.

In Cochain-SC, Zakaria et al. propose both intra-domain and inter-domain DDoS mitigation. There is also an intra-domain mitigation method that relies on software-defined networks (SDNs); it has three parts: (1) Internal Entropy-based Scheme (I-ES), which employs sFlow to measure the randomness of data inside the domain; (2) Intra Bayesian (I-BS) scheme to identify illegitimate flows based on entropy values; and (3) Intra-domain Mitigation scheme to mitigate illegitimate flows within the domain. Their inter-domain DDoS mitigation scheme uses blockchain to facilitate collaborative DDoS mitigation. It uses smart contracts (i.e., Ethereum′s smart contracts) to support DDoS mitigation among SDN-based domains.

Using the private blockchain technology, Kim, You, Park [22] provide a scheme for decentralized CDNs that are as robust as conventional CDN networks. The paper explains how DDoS can be mitigated by applying decentralized CDNs and a network with participants whose participation is trusted by a government or military agency. A model for a scale-free network was created and applied to a graph of the most decentralized network based on the developed schema. Private blockchains provide a higher amount of bandwidth than CDNs currently provide, and they can be used to protect the integrity of the blockchain as well as create reliable blocks for nodes. Table 1 depict the overall comparison of the review works.

Table 1. Overall Summary of various methods

Authors	Methodology	Remarks
Zakaria et al. [13]	Blockchain based Co-IoT	Ropsten helps in mitigation, low-cost, secure and flexible.
Shivansh and Rahul [15]	SDN-Blockchain	Flexibility, increase scalability, authentication for security.
Rodrigues et al. [12]	SDN-Blockchain	Integrity, reliability, immutable.
Nupur et al. [17]	Blockchain	DDoS PS protection.
Bruno et al. [18]	BLOSS	Reduce cost and cooperation.
Zacharia et al. [19]	SDN-Blockchain	Less FPR and more TPR and thereby secure.

V. OPEN CHALLENGES AND OPPORTUNITIES

According to research, mitigation strategies in today′s climate are limited to specific scenarios or architectures. Some concepts appear promising, but lack experimental proof and require further investigation to be proven to be effective. In addition, some of the learning approaches rely on outdated data, which makes it difficult for them to maintain their effectiveness. The implementation of approaches like this in a real-world setting endure few open queries as well. The application of such

approaches in a real-world setting also remains an open question. To evaluate any current or future solutions that address DDoS attacks, realistic scenarios should be considered in addition to considering the complexity and volume of DDoS attacks over time. Predefined rules are not tailored to new attacks, but rather to reportable attacks already in the past. Simulating real-world or near real-world traffic and infrastructure conditions, as well as systematic updating of dynamic learning approaches at short intervals, is necessary.

VI. CONCLUSION

This survey examines different approaches to mitigate DDoS attacks using blockchain technology, which is currently considered one of the most important technological advances since the advent of the internet. A large volume of work needs to be done to develop blockchain-based DDoS protective measures, and the researchers need to travel a long road ahead. The purpose of this paper is to highlight the specific details, strengths, weaknesses, and challenges of different approaches. In addition to providing an effective mechanism for securing transactions, blockchain also maintains integrity, immutability, and reliability. The majority of DDoS protection schemes utilize intelligent contracts to maintain and record transactions through the use of blockchain.

References

[1] Britton, K., 2016. Handling Privacy and Security in the Internet of Things. *Journal of Internet Law,* p. 6.

[2] DDoS Attacks Against U.S. Banks. (2019). Available: https://www.computerworld.com/article/2493861/ddosattacks-against-u-s–banks-peaked-at-60-gbps.html

[3] J. Zheng, Q. Li, G. Gu, J. Cao, D. K. Y. Yau, and J. Wu,(2018), Realtime DDoS defence using COTS SDN switches via adaptive correlation analysis, IEEE Trans. Inf. Forensics Security, vol. 13, no. 7, pp. 1838–1853, Jul. 2018.

[4] Denial-of-Service. https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/. Accessed April 9, 2019.

[5] Denial of Service Attack. https://en.wikipedia.org/wiki/Denial_of_Service_attack. Accessed April 9, 2019.

[6] Cheng, J.; Li, J.; Tang, X.; Sheng, V.S.; Zhang, C.; Li, M. A novel DDoS attack detection method using optimized generalized multiple kernel learning. Comput. Mater. Contin. 2020, 62, 1423–1443.

[7] Mirchev, M.J.; Mirtchev, S.T. System for DDoS attack mitigation by discovering the attack vectors through statistical traffic analysis. Int. J. Inf. Comput. Security. 2020, 13, 309–321.

[8] Darshi Patel(2020), Blockchain Technology towards the Mitigation of Distributed Denial of Service Attacks, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-6, March 2020

[9] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/en/bitcoin-paper. Accessed April 10, 2019.

[10] Buterin V. Ethereum: a next-generation smart contract and decentralized application platform 2014. https://github.com/ethereum/wiki/wiki/ White-Paper. Accessed January 8, 2019

[11] Gupta R. Hands-on Cybersecurity with Blockchain. Birmingham, England: Packt Publishing; 2018.

[12] Rodrigues B, Bocek T, Lareida A, Hausheer D, Rafati S, Stiller B. A blockchain-based architecture for collaborative DDoS mitigation it smart contracts. IFIP Int Conf Auton Infrastructure Management Security. 2017;10356:16-29.

[13] Zakaria Abou El Houda, Abdelhakim Hafid, Lyes Khoukhi. Co-IoT: A Collaborative DDoS mitigation scheme in IoT environment based on the blockchain using SDN, 978-1-7281-0962-6/19/$31.00 ©2019 IEEE

[14] Etherscan. The Ethereum Block Explorer: ROPSTEN (Revival) TESTNET. Accessed: May. 1, 2019. [Online]. Available: https://ropsten.etherscan.io.

[15] Shivansh Kumar, Ruhul Amin(2021), Mitigating distributed denial of service attack: Blockchain and software-defined networking based approach, network model with future research challenge, Wiley, Published on: 27 April 2021

[16] Rajeev Singh, Sudeep Tanwar, Teek Parval Sharma (2019), Utilization of blockchain for mitigating the distributed denial of service attacks, Wiley, October 2019

[17] Nupur Giri, Rahul Jaisinghani, Rohit Kriplani, Tarun Ramrakhyani, Vinay Bhatia (2019). Distributed Denial Of Service(DDoS) Mitigation in Software Defined Network using Blockchain, Proceedings of the Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2019) IEEE Xplore Part Number: CFP19OSV-ART; ISBN:978-1-7281-4365-1

[18] Bruno Rodrigues, Thomas Bocek, Burkhard Stiller, Enabling a Cooperative, Multi-domain DDoS Defense by a Blockchain Signalling System (Bloss), University of Zurich (UZH), 2017.

[19] Zakaria Abou El Houda, Abdelhakim Hafid, Lyes Khoukhi (2020). BrainChain - A Machine-learning Approach for protecting Blockchain applications using SDN. 978-1-7281-5089-5/20/$31.00 ©2020 IEEE

[20] Zakaria Abou El Houda, Lyes Khoukhi, Abdelhakim Senhaji Hafid (2020), Bringing Intelligence to Software Defined Networks: Mitigating DDoS Attacks, IEEE Transactions on Networks and Service Management

[21] Zakaria Abou El Houda, Abdelhakim Senhaji Hafid, Lyes Khoukhi, (2019), Cochain-SC: An Intra- and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract, IEEE Access, Volume7 July 24, 2019,

[22] Kyoungmin Kim, Youngin You, Mookyu Park, Kyungho Lee (2018), DDoS Mitigation: Decentralized CDN Using Private Blockchain, ICUFN, 978-1-5386-4646-5/18/$31.00 ©2018 IEEE.

[23] Chaganti, R., Bhushan, B., & Ravi, V. (2022). The role of Blockchain in DDoS attacks mitigation: techniques, open challenges and future directions. *arXiv preprint arXiv:2202.03617*.

[24] Khader, R., & Eleyan, D. (2021). Survey of DoS/DDoS attacks in IoT. *Sustainable Engineering and Innovation*, *3*(1), 23-28.

[25] Shah, Z., Ullah, I., Li, H., Levula, A., & 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.

[26] Alhijawi, B., Almajali, S., Elgala, H., Salameh, H. B., & Ayyash, M. (2022). A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets. *Computers & Electrical Engineering*, *99*, 107706.

[27] Saravanan, L., Sharma, H., Sreenivasulu, K. N., & Deivakani, M. (2021). Detection of software intrusion based on machine learning techniques for IOT systems. *Materials Today: Proceedings*.

[28] Zhou, Y., Cheng, G., & Yu, S. (2021). An SDN-enabled Proactive Defense Framework for DDoS Mitigation in IoT Networks. *IEEE Transactions on Information Forensics and Security*, *16*, 5366-5380.

[29] Pandey, N., & Mishra, P. K. (2021, December). A Survey on DDoS Attacks on Network and Application Layer in IoT. In *International Conference on Advanced Network Technologies and Intelligent Computing* (pp. 240-250). Springer, Cham.

[30] Tsiknas, K., Taketzis, D., Demertzis, K., & Skianis, C. (2021). Cyber threats to industrial IoT: a survey on attacks and countermeasures. *IoT*, *2*(1), 163-188.