



A Review of DDOS Attack Mitigation Technique Using BlockChain

Thesis

Submitted By

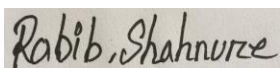
17-35298-2	Rabib, Shahnure
17-33155-1	Fatema Tasnim
16-32941-3	Tanvir Ahmmed
17-33152-1	Rukaiya Khandoker

**Department of Computer Science Faculty of Science & IT
American International University Bangladesh**

August, 29

Declaration

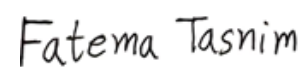
We declare that this thesis is our original work and has not been submitted in any form for another degree or diploma at any university or other institute of tertiary education. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given.



Rabib, Shahnure

17-35298-2

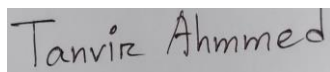
Faculty of Science & Technology



Fatema Tasnim

17-33155-1

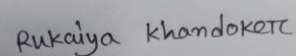
Faculty of Science & Technology



Tanvir Ahmmed

16-32941-3

Faculty of Science & Technology



Rukaiya Khandoker

17-33152-1

Faculty of Science & Technology

Approval

The thesis titled “A Review Of DDOS Attack Mitigation Technique Using BlockChain” has been submitted to the following respected members of the board of examiners of the department of computer science in partial fulfilment of the requirements for the degree of Bachelor of Science in Computer Science on 29th August 2020 and has been accepted as satisfactory.

Rifat Tasnim Anannya

Lecturer & Supervisor

Department of Computer Science

American International University-Bangladesh

MD. Hasibul Hasan

Assistant Professor & External

Department of Computer Science

American International University-Bangladesh

DR.MD. Mahbub Chowdhury Mishu

Assistant Professor & Head

Department of Computer Science

American International University-Bangladesh

Professor Dr. Tafazzal Hossain

Dean

Faculty of Science & Information Technology

American International University-Bangladesh

Dr. Carmen Z. Lamagna

Vice Chancellor

American International University-Bangladesh

Acknowledgement

First, we would be thankful to almighty God for this help in successfully completing our thesis on time. And also we would like to express our heartfelt thanks to the faculty of Science & Technology for keeping this thesis credit in our curriculum in our graduation program.

A lots of thanks to our beloved supervisor **RIFAT TASNIM ANANNYA**, from the bottom of our heart for this kind of encouragement, direction, inspiration us to complete our thesis. Finally, we would like to show our gratitude to our beloved parents, friends, and our beloved teacher who advice and motivate us all the time.

Abstract

Distributed Denial of Service (DDoS) attack cause devastating thread impending service to legitimate request on any network. The aim of DDoS is to exhaust a resource in the system reducing completely subverting the availability of the service provided. The DDoS attack incidence in the internet World are increasing day by day. A number of mitigation scheme have been designed are developed since it inception but the situation complexity demands advance solution based on block chain technology Against DDoS attack. The blockchain technology is rapidly finding use in various applications ranging from financial to gaming, this is because of stable, decentralized and secure architecture. This paper presents a study of different type of DDoS attack and collaborative mechanism using block chains and smart contacts. The objective is to create an automated and easy manage mechanism for DDoS mitigation.

Keyword: Distributed denial of service (DDoS), DDoS attack, DDoS mitigation, Block chain, smart contacts, Ethereum blockchains, Trust List.

Table of Contents

Chapter 1: Introduction	8
1.1 Denial Distributed of Service (DDoS)	8
1.2 BlockChain	8
Chapter 2: Types Of DDOS	10
2.1 UDP Flood Attack.	10
2.2 SYN Flood Attack.	11
2.3 Smurf Attack.	11
Chapter 3: BlockChain Technology	12
Chapter 4: Related Work	16
Chapter 5: Comparative Study and Discussion	21
Chapter 6: Conclusion and Future Work	23
Chapter 7: References	24

List of Tables

Table 1:	Recent Incidence of DDOS Attack.	9
Table 2:	Comparing Among various blockchain oriented DDOS mitigation technique.	21
Fig 1.1:	Distributed Denial of service (DDOS) Attack.	8
Fig 2.1:	Types of DDOS.	24
Fig 2.2:	UDP Flood.	39
Fig 2.3:	SYN Flood Attack	11
Fig 2.4:	Smurf Attack	11
Fig 3.1:	A basic block diagram of a block-chain	12
Fig 3.2:	A basic structure of a smart contract	13
Fig 3.3:	Ethereum basic architecture	13
Fig 3.4:	Ethereum virtual machine	14
Fig 3.5:	A general view of ethereum working procedure	15
Fig 4.1:	Propose Design Algorithm	16
Fig 4.2:	Proposed System Architecture	17
Fig 4.3:	Concept of Trust List	19
Fig 4.4:	Network Diagram for proof of concept(PoC) implementation	19

Chapter 1: Introduction

1.1 Denial Distributed of Service (DDoS)

The word DDoS attack means a form to attack on a computer system over a network. When an attacker use one device and one internet connection to execute a Denial of service (DDoS) Attack. When an attacker attempts to flood a targeted server with traffic from a large number of computers connected to the internet, this is known as Distributed Denial of Service (DDoS) Attack. The main Difference between of DDoS and DOS attack is that in a DDoS attack an attacker attempts to perform the attack by using a large number of computer or different host under the network and internet connection, and DOS attack an attacker attempt to perform the attack by using single computer and internet connection. The attacker main goal is to disrupt a target server's usual traffic rather than permanently harm it. DDoS attack is similar to a traffic jam on a road, where the ordinary traffic wants to get to their destination without being hampered. But when a huge amount of irregular traffic are added to their chosen road for a specific of time then there a jam will be occurred for that time, and the highway will be busy for some time. That is why the regular traffic for that highway will suffer. They will not arrive in their desired destination with in time. Like the regular traffic of the highway, when the DDoS attack happen on a server or a network the legitimate host or user under the network would not make transmission within time.

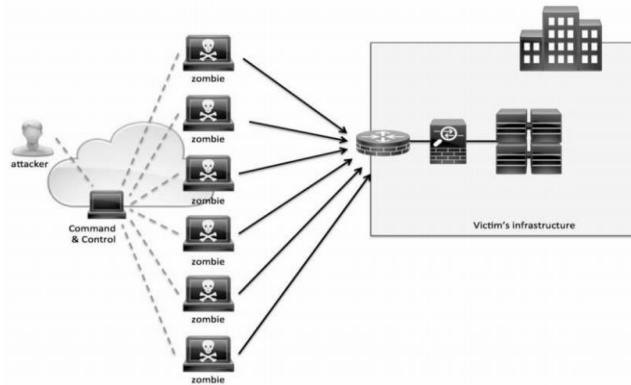


Fig 1.1: Distributed Denial of service (DDoS) Attack[1]

1.2: Blockchain

A Blockchain is a decentralized database that is made up of a series of cryptographically secure units known as Block. Each Block refers to the one before it and can not be changed without breaking the preceding block. Blockchain is no more than a distributed that is stored in a database maintaining by practicing nodes. It is only maintain a chronological sequence of transactions in a group as a block.

T A B L E 1: Recent Incidence of DDOS Attack

Attack Year	Attack Name	Attack Specifications	Victims	Attack Impact
September 2019	<i>TakeDown Attack</i>	<i>This attack Average Bandwidth Was 6.6GBPS and it was a traditional methods of attack and this attack utilized involving large volume of HTTP traffic</i>	<i>Online Encylopedia</i>	<i>The attacker Lasted almost 3Days</i>
February 2018	<i>Memcached DDOS Attack</i>	<i>The Attacker utilized extraordinary amplification and a open source of data catching tool it's name is Memcached. This attack traffic rate 1.3 terabyte/second.</i>	<i>Coding Website GitHub.</i>	<i>The Attacker Traffic wa Filtered the Akamai</i>
October 2016	<i>The Dyn DDOS Attack</i>	<i>In this attack it was a large number of IoT device targeted the victim. One day this attack utilized approx 145000 IoT device to raise the attack.</i>	<i>DNS Provider Targeted. Attack Targeted Server Of DYN client like Amazon,Netflix</i>	<i>DDOS attack on DYN Server were stopped an the all site and service were restored</i>

Chapter 2: Types Of DDOS

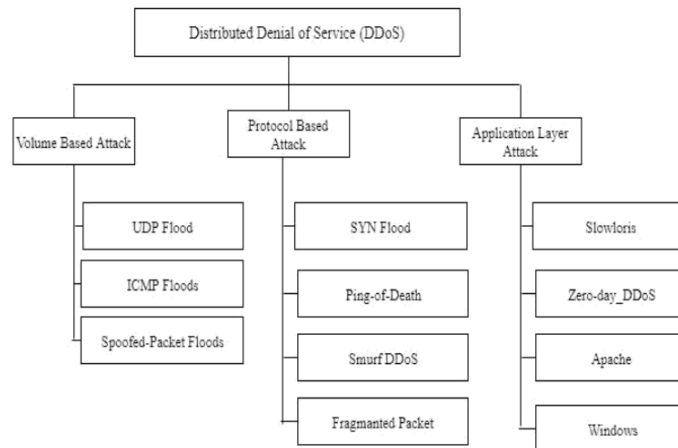


Fig 2.1: Types of DDOS

2.1 UDP Flood Attack:

One of the protocols in the internet protocols suite is the user datagram protocols (UDP). A UDP flood assault is a sort of DDOS attack that is based on Volume. An attacker perform a UDP Flood attack by sending a high number of user datagram packets to a specific server.

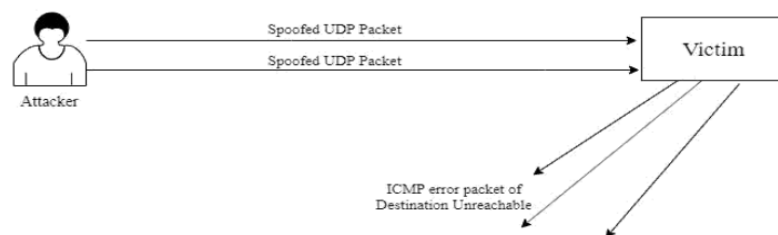


Fig 2.2: UDP Flood

2.1 SYN Flood Attack:

SYN flood is a distributed denial of service attack based on the SYN protocol. The attacker's primary goal in carrying out this attack is to render a targeted server unavailable to genuine network traffic. Attackers try to overburden the server so that genuine network users can't get service from it in a timely manner.

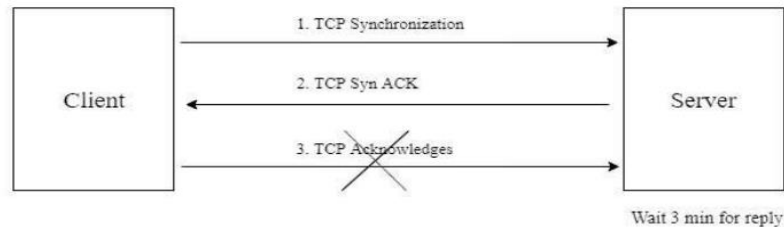


Fig 2.3: SYN Flood Attack

2.3 Smurf Attack:

One of the most well-known Distributed Denial of Service attacks in computer networks is the Smurf assault. The Smurf attack is a distributed denial of service assault based on a protocol. In a smurf attack, the attacker attempts to overload a server by sending a large amount of internet traffic to it. Actually, the attacker sends an ICMP (Internet Control Message Protocol) message to the targeted server. For sending error messages, Internet Control Messages are utilized in computer network operating systems. ICMP reply and request messages are used in the Smurf attack.

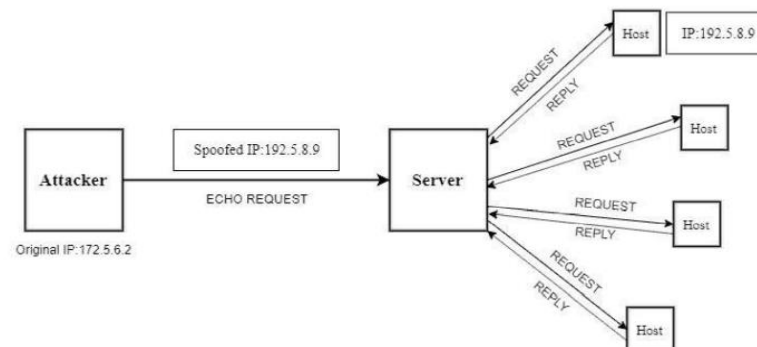


Fig 2.4: Smurf Attack

Chapter 3: BlockChain Technology

Nowadays crypto-currency transaction is more popular compared to last year. The idea of block-chain proposed in 2008 and successfully completed its implementation in 2009. Block-chain is as like as public ledger and all transactions information between one block to another block are stored in it. In block-chain, asymmetric cryptography and distributed consensus algorithms are used for user security and ledger consistency. Decentralization, persistency, anonymity and audit-ability is some main advantages of block-chain technology which makes this technology cost efficient and the improve its working power. The block-chain technology also can be used in other technological field like smart contracts, Internet of things (IoT), security systems and so on. The integration of smart contract with block-chain can make this technology more efficient for developing and designing some kind of real life problem solution without using any third party systems and moreover this is cost efficient also.

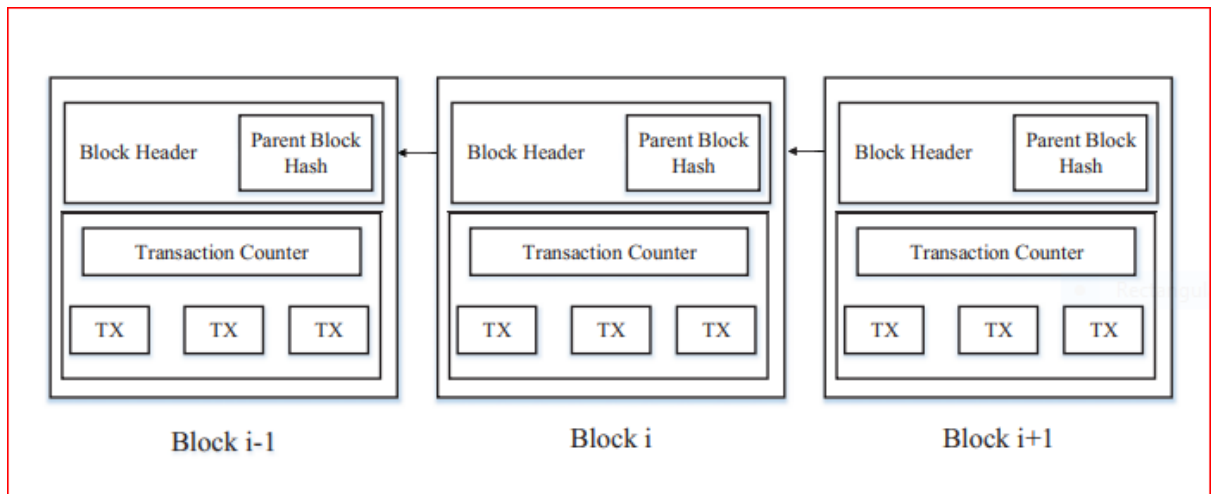


Fig 3.1: A basic block diagram of a block-chain[8]

From figure 1, everyone can easily understand the basic architecture of block-chain. In block-chain every block has three common items and these are “Data”, “Hash” and “Hash of previous block”. In “Block Header” previous block hash or parent block hash is exist. Block version, Markle tree root hash, Timestamp, nBits, Nonce are also exist in block header. In every block-chain, first block has no parent block or hash and so that this block is called “Genesis Block”.

Smart contract is a computer program which constructed by a set of rules run on the block-chain. In 1994, Nick Szabo was first proposed this concept of smart contract. Smart contracts are building up by value, address, function and state. It receives transactions as an input, executes the corresponding code and finally triggers the output. Depending on the function's logics implementation states are changes. Integrating smart contract with block-chain is most important because it gives the facilities of peer to peer transaction and databases are maintained publicly in a secure way by creating a trustful environment. For implementation of

smart contract one programming language is needed which called “Solidity”. Moreover, smart contract is a program which made up by machine readable code and run on any block-chain platform. Ethereum, ErisDB, Zeppelin and Counterparty this kind of block-chain platforms are developing using solidity programming language.

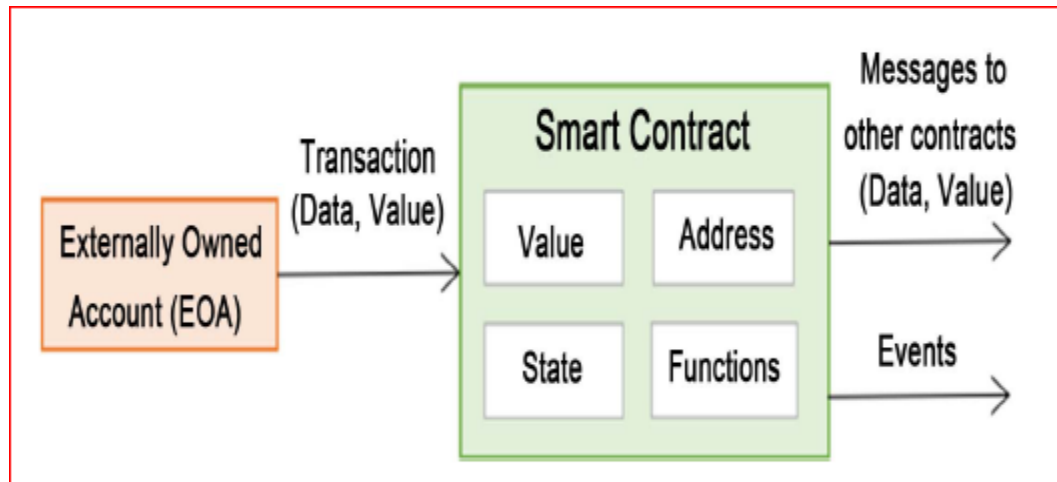


Fig 3.2: A basic structure of a smart contract[7]

Like others block-chain platform, “Ethereum” is one kind of block-chain platform which has own crypto-currency named “Ether (ETH)” and it’s also have own programming language named “Solidity”. It is open source and it has decentralized public ledger for verifying and recording transactions.

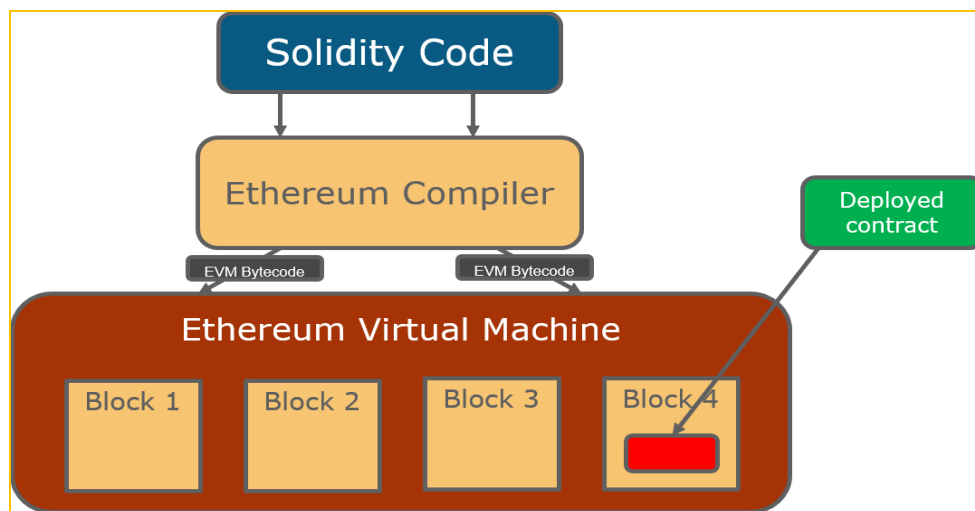


Fig 3.3: Ethereum basic architecture[11]

In July 2015, the concept of ethereum was first proposed by a small group of block-chain enthusiasts. Among them, “Joe Lubin” who is a block-chain applications developer and “Vitalik

Buterin” who is a youngest crypto billionaire were originating the first concept of “Ethereum network”. Nowadays “ETH” recognize as a second most important crypto-currency of the business world. As a result, like “Shopify”, “Overstock”, “CheapAir’s” popular e-commerce company accept the ETH for receiving their payment. At the end of May 2021, the current market value of ETH is \$2,236 that means ETH is become a most important contender in the volatile crypto-currency market. Notable information is a renowned “IT company: Microsoft” is the one of the most important partner of “ConsenSys” for developing Block-chain as a Service (EBaaS).

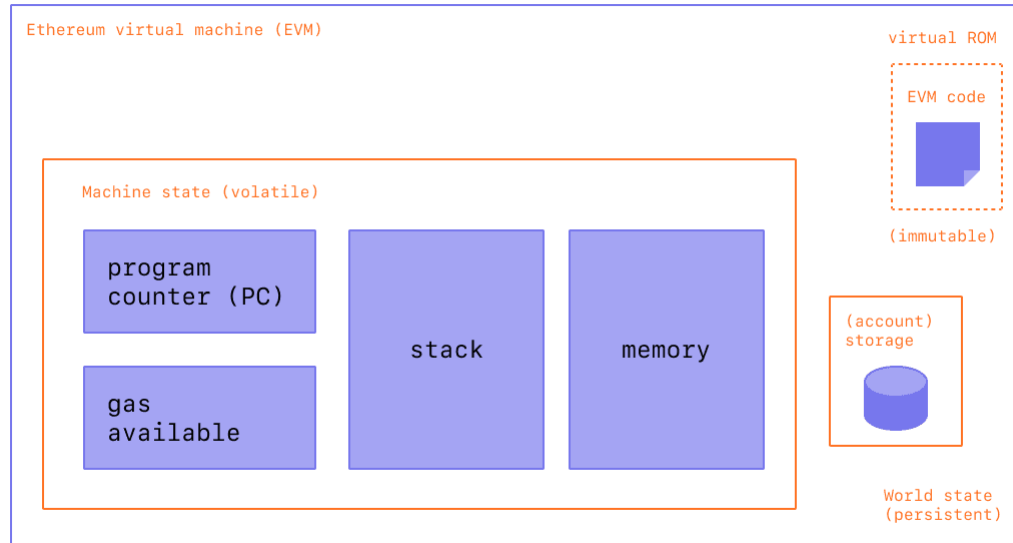


Fig 3.4: Ethereum virtual mechine[12]

The main reason for inventing “Ethereum” is to eradicate the limitations of Bitcoin. Among all the features of ethereum the most useful feature is: it gives the user’s a decentralized turing complete virtual mechine which named is “Ethereum Virtual Mechine (EVM)”. Using “EVM” technology it’s users can use it for any type of computations including all programming logic such as loops, if-else conditions and so on. That means, A built in turing complete programming language integrating with block-chain is supported by “Ethereum”. As a result, it gives a user an full abstract layer which enable anyone to create his or her own rules for ownership, transactions and state transition functions and this is only possible by integrating smart contract technology with it.

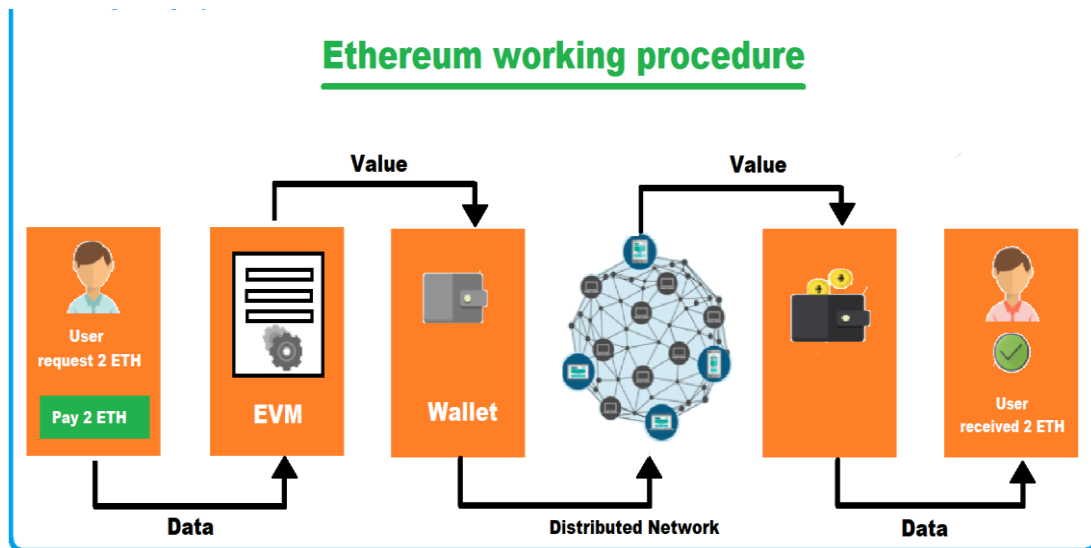


Fig 3.5: A general view of ethereum working procedure[13]

Two types of account are supported by ethereum; they are: "Externally owned" which is controlled by private key) and another is "contract accounts" which is controlled by own contract code. Every ethereum accounts have four parts. These are: Nonce, Ether balance, Contract code hash and Storage root.

Chapter 4: Related Work

Mohd Azahari Mohd Yusof, Fakariah Hani Mohd Ali, and Mohamad Yusof Darus[1] presents an overview of four types of DDoS attacks mitigation based on existing detection and defense algorithms. They also proposed a detection and defense algorithm which is evaluated using existing Intrusion detection and prevention tool to determine the proposed algorithm is the best algorithm to mitigate the DDoS attacks on a network environment. At first, they have discussed in their paper about four types of Distributed Denial of Service (DDoS) attack which are Smurf attack, TCP SYN, UDP flood, ping of death and their effects. Such as, In the Smurf attack they discussed that attacker use backdoor mechanism and for successful Smurf attack an attacker have to complete five steps. They also discussed about some current DDoS detection and defense algorithms. They even discussed seven phases in their paper for conducting this research. Then, they also proposed an algorithm for prevention of all of these four as well as detecting the specific attacker.

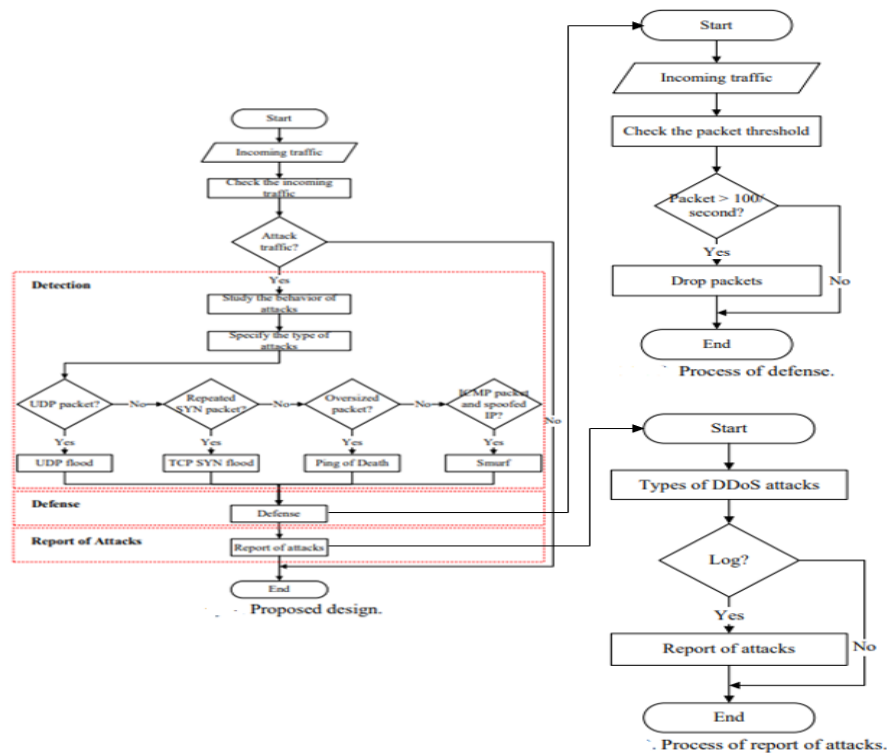


Fig 4.1: Propose Design Algorithm[1]

Mohd Azahari Mohd Yusof, Fakariah Hani Mohd Ali, and Mohamad Yusof Darus[1] proposed an algorithm, they basically focus on three important parts which are detection, defense and Report of attack. In detection part, they proposed detection algorithm to check the incoming traffic, whether it is DDoS traffic or normal traffic. If the incoming traffic is DDoS traffic, then the algorithm will specify the types of DDoS attacks based on behavior of the attack, whether it is

UDP flood, TCP SYN flood, Ping of Death or Smurf attack. Defense part which is used to block all these four attacks. For that, they proposed defense algorithms where if the number of packets received is larger than 100 packets/second, the packet will be dropped automatically. Their proposed defense algorithm also ensure clean traffic can enter into the network and protects the network even if a DDoS attack has been detected. For packet inspection, reduce the speed of incoming packets and control the use of network bandwidth, they used hybrid of Snort and Iptables. Another part is Report of attack which is used to log the types of DDoS attacks detected and produced real-time visibility into unwanted traffic.

Then, they test the proposed algorithm practically. The algorithms are implemented in the FIPS mainly. And, they measured their proposed algorithm in terms of false positive rates and detection accuracy.

J. Dheeraj, S. Gurubhara [2] proposed an infrastructure of blockchains and smart contracts which provide a mechanism without the necessity to maintain the development complexities of new protocol. They also designed an architecture combining block chain and smart contracts to introduce new opportunities for an effective DDoS mitigation as block chain and smart contracts can be used for sharing of attack information in a fully distributed and automated fashion. They also presented an architecture and designed a collaborative mechanism using blockchains and smart contracts. Firstly, they discussed the DDoS attack and how many sectors DDoS attack is detected in. And they mentioned the recent DDoS attack which occur in GITHUB website. They discussed some technologies like blockchain, smart contracts elaborately in their paper. They also mentioned that blockchain is a decentralized database consisting of block which is cryptographically secured and it grow as data enter at the end of the chain. And smart contract can control user permission by writing code inside it.

J. Dheeraj, S. Gurubhara [2] discussed about Ethereum which is kind of blockchain protocol inspired from Bitcoin and Some game applications run on it. This Ethereum create block in their system. They also used a decentralized Turing complete virtual machine known as EVM in their proposed architecture which provided by this Ethereum. Then, they did some background study related to these technologies. They even discussed some previous work related to DDoS attack mitigation. Finally, they presented their proposed system design in their paper and discussed about that proposed topic.

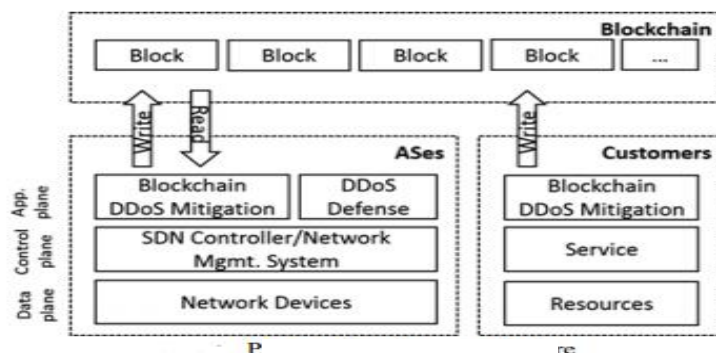


Fig 4.2: Proposed System Architecture[2]

J. Dheeraj, S. Gurubhara [2] proposed a collaborative architecture using smart contracts and blockchains to enable DDoS mitigation across multiple domains in their proposed system architecture. They used multiple domain which is AS A, AS B, AS C in their proposed system and when any of these ASes are under attack, they store IP address of the attacker in the smart contract. As Ethereum creates block every 14s, so ASes receive update IP address for blocking and confirm the attack. They further presented that when collaborative defense nodes receive information of an attack, they implement mitigation operations in agreement with the security policies. They built an architecture to mitigate DDoS attack in this paper and that architecture composed three parts which is Customer, ASes, Blockchain. In this proposed architecture customer report whitelist and blacklist IP addresses to Ethereum through smart contracts, ASes publish the whitelist and blacklist IP address and implement DDoS mitigation mechanisms, and Ethereum blockchain run the solidity smart contracts.

J. Dheeraj, S. Gurubhara's [2] proposed architecture is also based on certain principles such as DDoS detection and mitigation counter measures are provided by either the ASes or third-party services, a node need to connected to the blockchain to report and receive the information of the attack, Blockchain DDoS Mitigation modules are running on customer and ASes in this proposed architecture for reporting IP addresses and listening to the blockchain, only customer and ASes can report address to smart contract with proof of ownership and so on. In the conclusion they mentioned that this proposed architecture can be considered as an additional security to already existing techniques and it can be combined with existing solutions to reduce the DDoS attacks. So, proposed system architecture creates an automated and easy to manage mechanism for DDoS mitigation.

Kotaro Kataoka, Saurabh Gangwar, Prashanth Podili [3] proposed a Trust List that distributes trust among IoT-related stakeholders and provides an autonomous enforcement of IoT traffic management at the edge networks by integrating blockchains and Software-Defined Networking in their paper. In this paper, they argued about the prevention of unwanted traffic in a trustworthy, scalable, and distributed manner from IoT devices. They discussed about Trust List principle in their paper which automate the process of suspecting, verifying, and trusting IoT services and devices to effectively prevent attacks and abuses. They even tried to give proof of concept implementation and experiment of the Trust List using both public and private blockchains to reveal its good practice and suggest studies for realistic deployment. Then, they have discussed DDoS attacks on IoT devices, solutions and some issues that may result while developing trust on IoT devices and services. They also mentioned that this paper explores outbound traffic control at the edge networks to block unknown or malicious traffic without disturbing trusted and known communications. They discussed some related work based on IOT security, Integration of Blockchain and SDN, Blockchain for Securing Internet Transactions.

Kotaro Kataoka, Saurabh Gangwar, Prashanth Podili [3] also mentioned that the use of blockchain for networking purposes is in its early stages. Next, they discussed about trust list system design in detail and this section details the 2-step procedure of Trust List which is IoT services will be known by the edge networks, and IoT devices in each edge network gain access to their services. They also discussed about validator of IoT devices, data structures of Trust List, internet-wide delivery of Trust List, trusting an IoT service and so on, in that Trust List system design part.

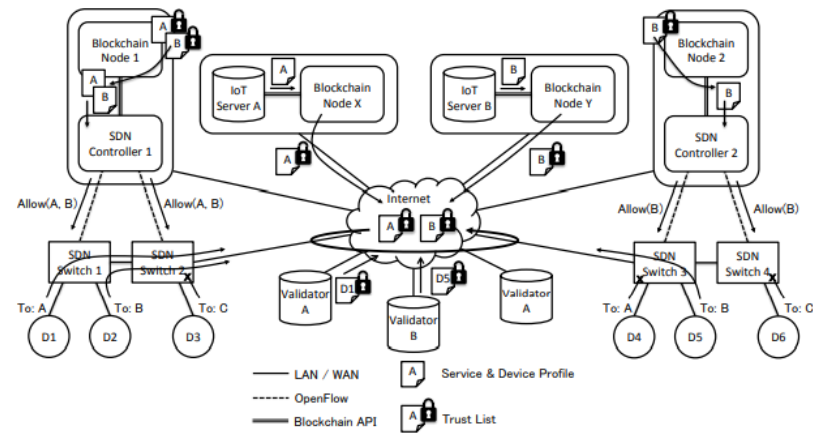


Fig 4.3: Concept of Trust List[3]

Kotaro Kataoka, Saurabh Gangwar, Prashanth Podili [3] implemented a proof of concept (PoC) system of Trust List that works in both public and private blockchain networks using the software which is Blockchain, smart contract, SDN controller, SDN switch. In this implementation part, they also discussed about Preparedness at Edge Networks, Flow Rules Implementing Trust List, Pseudo IoT Server, Device, and Validator and Flexibility of Service and Device Profiles. After implementing, they verified the implementation of Trust List using both private and public Ethereum blockchains. And, they evaluated their proposed systems by using some measurement technique such as “Difficulty of mining block”, “Time duration for delivery of trust list”, “Cost of executing transaction over block-chain” and so on.

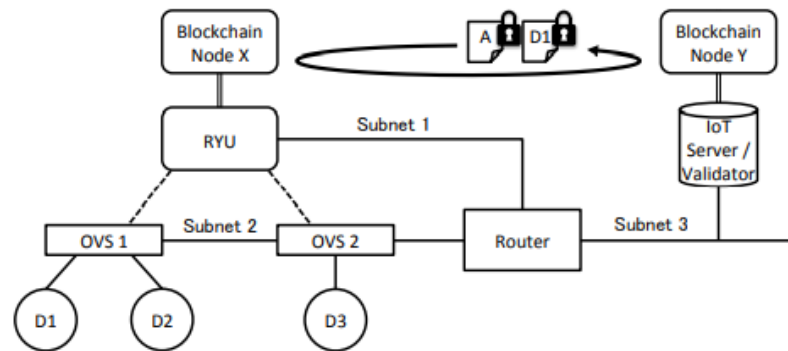


Fig 4.4: Network Diagram for proof of concept(PoC) implementation[3]

Kotaro Kataoka, Saurabh Gangwar, Prashanth Podili [3] mentioned some drawback of trusting in their paper. Finally, they said that their paper proposes a Trust List that circulates the information of trusted IoT services and devices among stakeholders, and focuses on prevention of unwanted traffic including DDoS attacks on edge networks from IOT devices. As future work, they want to standardize the core data format and establish a sustainable procedure of Trust List among a variety of stakeholders.

Jonathan Burger [4] in his paper evaluated "A Blockchain-based Architecture for Collaborative DDoS Mitigation with Smart Contracts" of Rodrigues [5]. And Rodrigues's [5] paper suggested the utilization of Ethereum blockchain as a registry for IP addresses from which attacks are originating from. His work was motivated by Solidity based smart contract which can be coded independently of the Ethereum blockchain. He also mentioned in his paper that to solve a wide variety of problems smart contracts can be programmed using the Turing-complete programming language Solidity. Firstly, he discussed about DDoS, blockchain, Ethereum and Smart Contract. He also mentioned that Ethereum blockchain is independent of web server which used for signaling the attack IP address. He also discussed some related work on this proposed topic.

Jonathan Burger [4] developed three different types of smart contract and compared them with each other. On the issue of blockchain scalability upon increase in the number of attackers, he also suggested three approaches to overcoming the Rodrigues's [5] architectural deficit. First method is similar to the original method and store blacklist or whitelist IP address in a usual array using smart contract on blockchain. In the second method, the URL is indexed to a static web resource hosted on a web server and placed in a blockchain using a smart contract. In third method, to reduce the storage cost and complexity a bloom filter is used. He used IPv6 along with IPv4 for storing the addresses on the blockchain in all the three methods. For all these three methodologies, He developed, deployed, tested, and benchmarked the smart contract based on speed, cost, and accuracy. Then, he discussed about his findings in this paper. In the first method, he found that small number of IP addresses is suitable for placing and this method faced scalability issues when IP addresses scale to few hundred. In the third method, he found that bloom filter method would give imperfect accuracy, makes it difficult to obtain the full list of stored IP addresses and increases the false positive cases. In the second method, he found that a list of IP addresses through web resources is the best method among all three methods.

Jonathan Burger [4] discussed about cost model, speed, accuracy and so on. But the result of Jonathan Burger [4] work clearly showed that among these three proposed methods none are perfect for effectively utilizing space. So, He recommended that Ethereum blockchain is not the ideal technology, Because, developed solutions using Ethereum blockchain can suffer under scalability. He further proposed to use specialized blockchains and decentralized signaling for further scalability improvements.

Chapter 5: Comparative Study and Discussion

T A B L E 2: Comparing Among various blockchain oriented DDOS mitigation technique

Solution	Prevent / Detect/ React	Upgrade Required In the method	Use of blockchain/ Smartcontract / SDN	Work across multiple domain	Build on existing network	Trust model	Implementatin
1. Mohd Azahari Mohd Yusof" Detection and Defense Algorithms of Different Types of DDoS Attacks " International Journal of Engineering and Technology	Prevent and Detect	A detecting DDOS Detecting and mitigating algorithms. Used of ddos mitigation technique	Use DDOS algorithms. algorithm to detect a Smurf attack they checked the packet type and the IP address is spoofed or not they said it a Smurf attack and make a defense against the attack	N.A	N.A	N.A	Smurf attack, TCP SYN, UDP flood and ping of death attack. To make a successful Smurf attack only Internet Control Message Protocol is used by the attacker which is a very common protocol in the network.
2. J. Dheeraj,"DDoS Mitigation Using Blockchain" International Journal of Research in Engineering, Science and Management	Prevent, Detect	Architecture can be considered as an additional security to already existing technique and it can be combined with existing solution to reduce the ddos attack.	BlockChain, Smart Contract	Y	N.A	Infrastructure of blockchain and smart contract provide mechanism without the necessity and the develop complexity of new protocol. And also Ethereum is used to create Block	Collaborative architecture Using smart contract and blockchain to enable DDOS mitigation across multiple domain in their proposed system architecture
3. Kotaro Kataoka," Trust List: Internet-wide and Distributed IoT Traffic Management using Blockchain and SDN "	Prevent and React	Standardizing primary data formats and establishment of trust list among various entities is required	BlockChain,smart Contract, SDN	N.A		IoT device and server prove trustable to each other.IoT device prove trust using 2 step and validator is used authentication purposes	Developed Trust list is available as open source software. Tools used: Ethereum BlockChain, SmartContract,Ryu Open Flow SDN Controller and open vSwitch as SDN Switch
4.Burger j.collaborative ddos mitigation based on blockchain [bachelor thesis].department of informatics university of Zurich	Prevent, Detect and React	Detecting Network Node is required for DDOS detection. Use of SDN BlockChain DDOS mitigation modules running on customer	BlockChain,smart Contract, SDN	Y	Y	Use of white or blocklist IP address. Public Ethereum blockchain is used to spread the DDOS Advertisement	Only logic of smart IP reporting function provided

In this comparative study among 4 prominent Blockchain and DDOS based mechanisms has been done in table no 2. 1) Detection and defence algorithms of different type of DDOS attack. 2) DDOS mitigation Using Blockchain 3) Trust list: Internet-wide and distributed IoT Traffic Management Using Blockchain and SDN. 4) Collaborative DDOS Mitigation based on Blockchain. All of these paper are prevent using Blockchain and DDOS mitigation Technique. It can be easily inferred about the blockchain edge network without affecting ongoing communication between trusted devices. This is provided by SDN mechanism which is Mitigation of DDOS attack relies on exception detection and significant of amount of time after the attack took place and control done. Conceptually against DDOS attack [4] basically targeted only the scalability concern in blockchain based DDOS mitigation. Jonathan Burger [4] discussed about cost model, speed, accuracy and so on. But the result of Jonathan Burger [4] work clearly showed that among these three proposed methods none are perfect for effectively utilizing space. So, He recommended that Ethereum blockchain is not the ideal technology, Because, developed solutions using Ethereum blockchain can suffer under scalability. He further proposed to use specialized blockchains and decentralized signaling for further scalability improvements.

Prashanth Podili [3] mentioned some drawback of trusting. Their system still allows traffic which matches the conditions being safe, to pass through even though it is not actually safe as with a nature of white list. This type of attack is possible when Trust List is implemented partially if a botnet is created to attack the known servers or validators in the Trust list. For inspect and verify that an apparently safe communications are legitimate, they still rely on Deep Packet Inspection (DPI). They also mentioned that the trust list must be updated when a service is victimized so that the attacking traffic can be blocked by announcing new properties of trusted services

[2]This paper also works across many domain and ASes. And it work existing network Infrastructure. They used a collaborative mechanism using blockchains, smart contracts to mitigate DDoS and presented the design and architecture of this collaborative mechanism. So, they proposed an infrastructure of blockchains and smart contracts that provide the required mechanism without the need to maintain development complexities of such a new protocol [2]. They tried to detect and prevent this DDoS attack in this paper. In the architecture they basically used Ethereum blockchain, EVM, smart contracts. This architecture work across multiple domain which is ASes. So, here different type of domains implements different security policies as well as different underlying management systems [2]. This paper didn't build on existing network. This proposed architecture can be used as an additional security to reduce DDoS attack. So, we found this second paper's solution is the best solution among all four-paper solution. Because, here they use multi domain approach and decreases the use of algorithms in the detection phase using information from other domains. And they built an architecture for mitigation, didn't work on existing work.

Chapter 6: Conclusion and Future Work

A large number of solutions to the DDoS attacks detection, mitigation and prevention using block-chain have been proposed in the papers we read. Most of those solutions are valid victimization experiments supported simulation, real time systems observance and analysis of publicly available datasets. Each approach described in the paper has its own merits and demerits. Among them, we select the journal paper named “DDoS mitigation using block-chain” for some it's remarkable qualities and these are use of collaborative mechanisms which decrease the necessity of multiple algorithms and it also uses the decentralized turing complete virtual machine called EVM. EVM has smart contract technology which can solve a real life any complex problems using its programming logic.

In future we will also use trust list concept because it is compression of trust list and reducing transection costs. We will use database, with the existing data in the database, the database can check the source of IP address of incoming traffic. It can also keep track of the IP address that is delivering an Internet Control Message Protocol message with the largest size data field. This process will be the implementation of the proposed algorithms and it will measured positive and negative false rate and detection accuracy. This saved records can be used to calculate threshold data by which we can compare the data field size.

Chapter 6: References

- [1] Mohd Azahari Mohd Yusof, Fakariah Hani Mohd Ali “Detection and Defense Algorithms of Different Types of DDoS Attacks” International Journal of Engineering and Technology, Vol. 9, No. 5, October 2017
- [2] J. Dheeraj, S. Gurubharan “DDoS Mitigation Using Blockchain” International Journal of Research in Engineering, Science and Management Volume-1, Issue-10, October-2018.
- [3] Kotaro Kataoka, Saurabh Gangwar” Trust List: Internet-wide and Distributed IoT Traffic Management using Blockchain and SDN ” 978-1-4673-9944-9/18/\$31.00 c 2018 IEEE.
- [4] Burger J. Collaborative DDoS Mitigation Based on Blockchains [bachelor thesis]. Switzerland: Department of Informatics, University of Zurich; 2017.
- [5] Rodrigues B, Bocek T, Lareida A, Hausheer D, Rafati S, Stiller B. A blockchain-based architecture for collaborative DDoS mitigation with smart contracts. *IFIP Int Conf Auton Infrastruct Manag Secur.* 2017; 10356: 16- 29
- [6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends” 2017 IEEE 6th International Congress on Big Data.
- [7] <https://www.flentas.com/ethereum-architectural-overview>, Access 21-08-2021, 10 pm.
- [8] <https://www.investopedia.com/terms/e/ethereum.asp>, Access 21-08-2021, 11 pm.
- [9] D. Vujicic, D. Jagodic, S. Randic “Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview” 17th International Symposium INFOTEH-JAHORINA, 21-23 March 2018.
- [9] B. K. Mohanta, S. S. Panda, D. Jena “An Overview of Smart Contract and Use cases in Blockchain Technology” IEEE – 43488
- [10] R. Singh, S. Tanwar and T. P. Sharma “Utilization of block-chain for mitigating the distributed denial of service attacks” 2019 John Wiley & Sons, LTD.
- [11] <https://www.imperva.com/learn/ddos/ddos-attacks/> ; Access on 1th September,2020; 12.23pm.
- [12] <https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html> ; Access on 1th September,2020; 12.24pm.
- [13] <https://www.esecurityplanet.com/networks/types-of-ddos-attacks/> ;Access on 1th September,2020; 12.25pm.

- [24] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang and K. -K. R. Choo, "An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security," in *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 625-638, 1 July-Aug. 2020, doi: 10.1109/TSC.2020.2966970.
- [15] Y. Chaba, Y. Singh, and P. Aneja, "Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET," vol. 4, no. 3, pp. 178-183, 2009.
- [16] G. Zhao, "A real-time DDoS attack detection and prevention system based on per-IP traffic behavioral analysis A Real-Time DDoS Attack Detection and Prevention System Based on per-IP Traffic Behavioral Analysis," no. August 2010, 2016.
- [17] Leila Ismail, Huned Materwala "A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions" Received: 25 July 2019; Accepted: 16 September 2019; Published: 24 September 2019.
- [18] Agrawal, N.; Tapaswi, S. Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges. *IEEE Commun. Surv. Tutorials* 2019, 21, 3769–3795.
- [19] Agrawal, N.; Tapaswi, S. Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges. *IEEE Commun. Surv. Tutorials* 2019, 21, 3769–3795.
- [20] Banitalebi Dehkordi, A.; Soltanaghaei, M.R.; Boroujeni, F.Z. The DDoS attacks detection through machine learning and statistical methods in SDN. *J. Supercomput.* 2020, 1–33.
- [21] K. Geetha and N. Sreenath, "SYN flooding attack 3/4 Identification and analysis," International Conference on Information Communication & Embedded Systems, pp. 1-7, 2014.
- [22] Denial-of Service. <https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/>. Accessed April 9, 2020.
- [23] Y. Chaba, Y. Singh, and P. Aneja, "Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET," vol. 4, no. 3, pp. 178-183, 2009.