SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V11I3P125

Volume 11 Issue 3, 299-307, March 2024
© 2024 Seventh Sense Research Group®

*Original Article*

# Harnessing Blockchain for Collective Defense: A Strategy for Detecting and Combating DDoS Attacks

Kriti Patidar[1], Swapnil Jain[2]

[1,2]*Department of Electrical and Electronics Engineering, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Madhya Pradesh, India.*

[1]*Corresponding Author : kritipatidar1@gmail.com*

Received: 17 January 2024 Revised: 12 February 2024 Accepted: 15 March 2024 Published: 25 March 2024

***Abstract -*** *Among the current security challenges faced by the Internet, Distributed Denial of Service (DDoS) attacks loom as a significant threat. DDoS attacks represent potent cyber threats designed to incapacitate services by overwhelming servers, thereby hindering their responsiveness to users. These attacks can swiftly deplete the processing and communication capabilities of the targeted entity. The previous few years have seen a noticeable surge in the frequency and duration of DDoS attacks, rendering them more impactful and perilous. The surge in insecure mobile device usage and escalating traffic volumes contribute to the heightened risk posed by DDoS attacks on various services. This paper proposes a collaborative approach for identifying and mitigating DDoS flooding attacks. The utilization of smart contracts can play a crucial role in identifying malicious actors, subsequently enabling their inclusion in blocklists. Leveraging blockchain technology simplifies the complexity of the DDoS signaling system, offering an effective means for numerous independent and distributed systems to collaborate. Through resource and defense characteristic sharing, blockchain facilitates a robust defense strategy against DDoS attacks.*

***Keywords -*** *Blockchain, Denial of Service, DDoS attacks, DDoS mitigation, IP spoofing, TCP SYN flooding*.

## 1. Introduction

The use of portable and stationary devices has seen an unprecedented increase in the past few years, resulting in an increase in cyber-attacks. DDoS attacks, also known as distributed denial of service attacks, are a particular sort of Denial of Service (DoS) where the server is overwhelmed by attackers with a tremendous amount of traffic. Among the most potent hazardous attacks is DDoS, aimed at making services unreachable or preventing their use over the Internet [1]. Cloud ecosystems suffer the greatest losses as a consequence of DoS attacks, resulting in service deterioration [2]. The targeted victims range from low-key public networks to organizations, including banks, hospitals, and government offices [3].

Over time, DDoS attacks have swiftly advanced and become extremely sophisticated. DDoS attacks have a significant negative impact on an organization's infrastructure, finances, and computer resources [4]. In the past few years, DDoS attacks have shown exponential growth, affecting even well-known servers [5]. GitHub was reportedly subject to an attack of 1.3TBps. After the attack on GitHub, a 1.7TBps attack was also recorded [6, 7]. When a DDoS attack peaked at 160Gbps [8], certain reputable banks were seriously impacted. In just 2014, there were recorded monetary losses of roughly $491 billion [5]. A global DDoS extortion attack totaling 2TBps that targeted the financial and tourism sectors was also reported by NetScout [9]. In DDoS attacks, attackers are geographically dispersed and can spoof MAC and IP addresses, making detection difficult. During the attack, the impacted service is fully inaccessible. In addition to the immediate cash consequences, this service interruption harms the company's reputation, which may have a considerably more detrimental long-term impact. Numerous ways to mitigate the effects of these attacks have been proposed.

A successful defense requires a dispersed and coordinated defense. Cooperative defenses provide many advantages; for instance, they permit combining the ability for mitigation and detection, lowering overhead and load on single devices, and blocking harmful traffic close to its source. However, because of their inefficiency and difficult installation, there is yet to be a wide-scale deployment of these systems.

Due to its decentralized network and ability to cut out intermediaries, its usage has grown recently. The advantage of using blockchain is that it may be used to create a decentralized system for maintaining blocklisted IPs and blocking them [10]. A fully distributed and automated method of sharing attack information is made possible by blockchain technology and smart contracts. The primary benefit of such architectures is the efficient promotion of the blocklisted IP addresses, and the use of such a foundation adds an extra layer of safety to the DDoS defensive systems already in place.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

This paper addresses TCP SYN flood, a pronounced category of DoS attack. The TCP SYN flood overwhelms the server, denying legitimate request attempts. This paper proposes a technique for detecting and mitigating DDoS attacks by efficiently distributing blocklisted IP address lists.

## 2. Background

### *2.1. Blockchain*

Blockchain is a trustworthy technology that enables nodes in a distributed network to share data reliably without the requirement of a centralized body or server. Nodes in a blockchain system have a common shared database maintained at each node. As a result, rather than being restricted to electronic payment transactions, this technology has been employed in a number of industries needing data trust and integrity.

Blockchain employs a peer-to-peer mechanism known as flooding. Flooding is when a node transmits data to a node that is directly connected to it rather than the entire network, and the nodes that have already conveyed the data then transmit it again to other related nodes. Figure 1 represents a typical blockchain architecture.

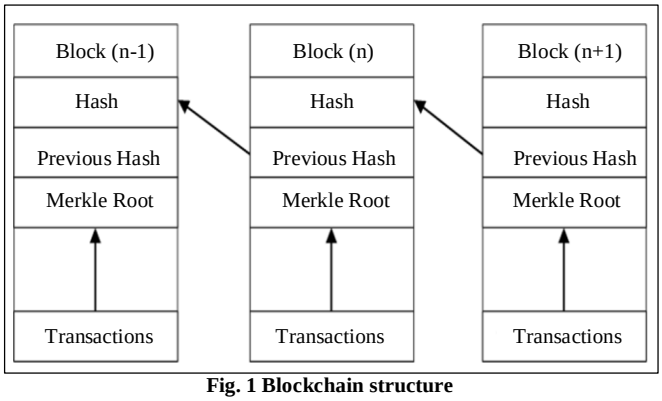


**Fig. 1 Blockchain structure**

Ethereum is an open-source Blockchain system that was modeled after Bitcoin. It offers a scripting language, Solidity, that enables anybody to create Ethereum blockchain applications. It is used to run scripts via a network of open nodes. Ether can be used to move money between accounts and to pay participating mining nodes for work they have done.

Smart contracts are contracts that are written in code and can support any type of transaction without the influence of any third party. The storing of binary data is made feasible by Ethereum smart contracts, which also let users send transactions that change the storage. The smart contract developers can regulate the user permissions as well as the conditions and behaviors of the mutations by writing the appropriate code [11]. Ethereum allows for Turing-complete programming on the blockchain, which opens up a vast range of potential applications.

### *2.2. DDOS*

Attacks that affect the accessibility of systems or services are DoS attacks. Disrupting the victim system services and preventing fulfilling requests from valid users often involves flooding the resource or the targeted machine with unnecessary requests [12]. Flooding or resource consumption refers to the use of memory, computational power, and bandwidth. They mainly target critical resources like bank servers and financial institutions, creating a significant barrier to the accessibility of critical information. DDoS attacks also serve as a key source of malware and harmful code in the network or system.

DDoS belongs to a category of DoS attacks that exploit numerous sources used to generate requests. By spreading out the requests, a Denial of Service attack can generate far more traffic and become much more difficult to manage. Typically, an attacker infects as many internet-connected devices as they can with malware, seizes control of them, and then instructs them to attack the victim, as illustrated in Figure 2 [13]. By blocking the attacker's traffic, a DDoS attack can be prevented. Each traffic packet includes details about the source, such as an Internet Protocol (IP) address, which serves as a source identifier. The attack can be reduced by filtering the incoming packets based on the sender's IP address.

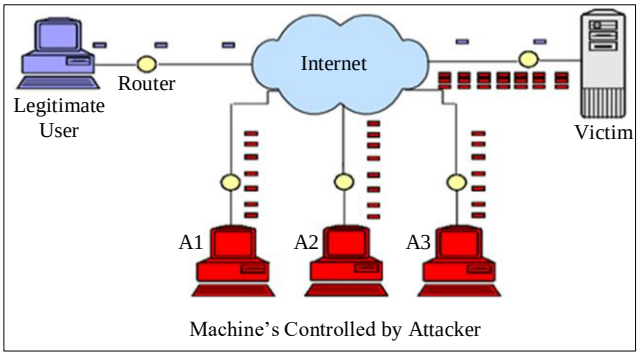


**Fig. 2 Illustration of DDoS attack**

### *2.3. TCP SYN Flood Attack*

TCP protocol stack is vulnerable to TCP SYN flood attacks owing to the process of 3 way handshake shown in Figure 3, used to establish a connection between parties. Before data transmission in a TCP connection, the client and server connections need to be established. A client begins to communicate first by sending a SYN request. In return, the server sends SYN-ACK. With this response, the server also allocates space in a buffer for the connection with the client. The client then sends a response with an ACK packet, completing the connection [15].

This 3-way handshake gets converted into a TCP SYN flood if the client uses the wrong IP addresses for sending SYN requests so that the server response of ACK is never received. This can be done by IP spoofing. For imitating an attack numerous SYN requests are sent, exchanging SYN and

SYN ACK packets as usual, but never responding with the final ACK message to the server [16]. A SYN flood attack operates by not sending the response of ACK back to the server. This can be done in two main ways, i.e., either just not sending the ACK or sending SYN with a spoofed IP address so that the ACK from the server is never received.

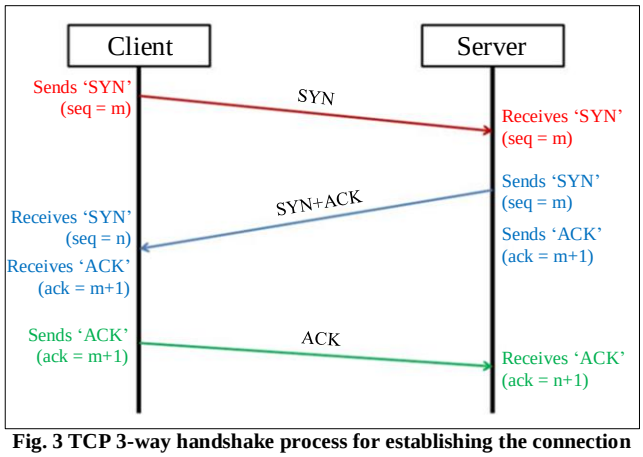


**Fig. 3 TCP 3-way handshake process for establishing the connection**

The server waits for ACK packets for a while because a missing ACK could simply be the result of normal network congestion. The server creates a backlog queue in its system memory to keep track of the incoming requests. Every new connection request made by a client is rejected by the server once the backlog queue limit is reached.

As the server does not receive ACK packets, the connections are left incomplete, as seen in Figure 4. These incomplete connections occupy the complete buffer space in the server and thus, the server starts refusing new connections to legitimate users because of these open connection requests. This can cause the server to even crash because of the starvation of resources. Thus these half-open connections on SYN flood causes denial of service to legitimate users [17].

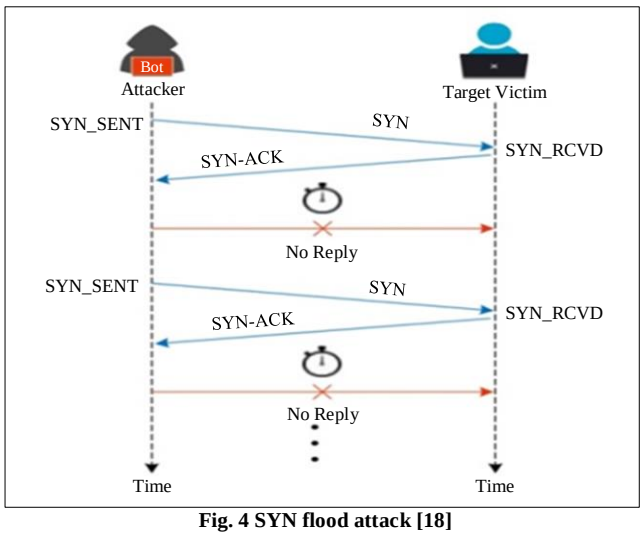


**Fig. 4 SYN flood attack [18]**

The mitigation techniques require nodes to recognize the attack on them and are centered on single-target victims [19]. Appliance deployment and software patching cannot completely prevent or mitigate DDoS [20]. As a result, Internet service providers either overprovision their networks or deploy scrubbing services [21]. Both approaches are not financially viable [22].

## 3. Related Work

### *3.1. Existing Solutions to Mitigate DDoS Attacks*

At present, there are two primary methodologies for detecting DDoS attacks: statistical approaches and machine learning techniques. Statistical detection methods operate by analyzing traffic datasets at the end nodes of a blockchain network in specified time intervals. These methods categorize the traffic based on statistical metrics such as network congestion levels, effectively distinguishing DDoS attack traffic from normal network activity [23].

However, these methods possess several limitations. For example, DDoS attack traffic can be disguised amidst Peer-to-Peer (P2P) traffic through flooding techniques. Since the fundamental characteristics of this type of attack data closely resemble legitimate data packets, these types of detection techniques mostly exhibit lower accuracy [24]. Secondly, different consensus mechanisms process network information and transactions differently, enabling attackers to send rumour-based DDoS attack data packets as disguised network traffic. Due to the similarity in attack data and normal traffic data, detection methods frequently misidentify these attacks, resulting in a high rate of false positives [25].

Rodrigues et al. [26] introduced a blockchain architecture and smart contract to combat DDoS attacks. This enables decentralized information sharing, automating attack data distribution. Their approach employs smart contracts within blockchain for efficient DDoS mitigation, utilizing existing decentralized infrastructure to share IP addresses. This enhances DDoS defense security without requiring specialized registries or distribution mechanisms. Zhou et al. proposed a smart home framework based on blockchain that is designed to detect and prevent DDoS security threats and linkage attacks, which pose risks to user privacy [27].

DDoS detection methods employing machine learning operate by capturing traffic data at end nodes within the blockchain network. Subsequently, a machine-learning algorithm is employed to analyze and extract the fundamental characteristics of DDoS attack traffic. Following a training phase, it becomes capable of categorizing the network traffic and determining DDoS attack traffic [28]. Despite their utility, these methods exhibit several limitations. Firstly, the existence of different consensus within the blockchain network layer environment presents a challenge. This diversity complicates the underlying traffic protocols [29].

Secondly, the similarity between the features of normal network data packets and rumour-based attack data poses a challenge for machine-learning methods. The core characteristics of mixed data packets are difficult to detect by machine learning techniques, resulting in reduced accuracy in the detection of such attacks.

### *3.2. Research Gap*

Traditional defense mechanisms are often insufficient to handle the scale and diversity of modern DDoS attacks. These approaches often rely on centralized solutions, making them susceptible to single points of failure. Attackers exploit these vulnerabilities, leading to service disruptions and downtime for targeted organizations. The collaborative nature of DDoS attacks, often originating from multiple sources, necessitates a collaborative defense mechanism.

The decentralized architecture of blockchain enhances the resilience of the defense mechanism. By distributing the responsibility for attack detection and mitigation across a network of nodes, the system becomes less susceptible to a single point of failure. Information sharing is crucial for a robust DDoS defense strategy. However, organizations are often hesitant to share sensitive threat intelligence due to concerns about trust. Blockchain's decentralized and immutable ledger can address these trust issues, fostering a secure and transparent collaborative environment.

The inadequacy of current DDoS defense strategies underscores the pressing need for innovative approaches that can adapt to the evolving nature of these attacks. Various intrusion detection systems and other schemes of traffic filtering have been employed to counter DDoS threats; however, they often lack the agility and scalability required to withstand sophisticated attack vectors. Moreover, the centralized nature of existing defense mechanisms renders them susceptible to single points of failure, allowing attackers to exploit vulnerabilities with relative ease.

In light of these challenges, this paper proposes a novel strategy for detecting and combating DDoS attacks by harnessing the potential of blockchain technology. Blockchain, renowned for its decentralized and immutable nature, offers a promising avenue for enhancing the resilience and effectiveness of collective defense mechanisms against DDoS threats. By distributing trust and consensus across a network of nodes, blockchain can mitigate the risks associated with centralized points of failure while facilitating real-time threat intelligence sharing and collaborative defense efforts among stakeholders.

The research paper seeks to address the pressing need for advanced, collaborative, and resilient mechanisms for DDoS attack detection and mitigation in the face of increasing cyber threats. By harnessing the capabilities of blockchain, the proposed system provides a secure, transparent, and decentralized platform for collective defense against DDoS attacks.

### *3.3. Major Contributions*

The major contributions of a research paper are:

1. The research proposes a collaborative approach to addressing DDoS attacks that involves cooperation among various independent and distributed systems, emphasizing the importance of multiple entities working together.
2. The proposed method uses smart contracts to automate response mechanisms against DDoS attacks, reducing the response time to attacks.
3. The paper proposes the inclusion of identified malicious actors in blocklists, which are used to restrict or deny access to known threats.
4. Blocklisted IP addresses are stored in the blockchain. This uniform accessibility enhances security by a level, ensuring that all relevant components can access and utilize the same tamper-resistant list of blocked IP addresses.
5. Immutability and Transparency is achieved with the use of blockchain. This contributes to the integrity of the DDoS mitigation process, preventing unauthorized modifications to the list of blocked IP addresses.
6. Blockchain technology simplifies the DDoS Signaling System involved in detecting and responding to DDoS attacks. This simplification could lead to more efficient and reliable defense mechanisms.
7. Blockchain approach also enables the seamless exchange of information related to resources and defense strategies.
8. The paper also includes a thorough evaluation of the performance and scalability of the proposed mechanism. This involves assessing how well the system handles large-scale DDoS attacks, the efficiency of information sharing, and the overall responsiveness of the collaborative defense network.

## 4. Materials and Methods

### *4.1. Proposed Work*

Blockchain has the potential to revolutionize how data and information are transferred between unreliable parties. Blockchain technology can be a suitable solution for safeguarding distributed systems. It has formerly been efficiently used to improve the detection mechanism for countering conventional cyber security attacks.

To be able to counteract DDoS attacks, this paper suggests a decentralized system that uses blockchain technology for notifying blocklisted IP addresses. A decentralized nature, in contrast to a multi-server distributed approach, prevents attackers from illegally accessing one of the nodes and changing the list. The server that is being attacked routes incoming TCP requests to various other nodes in the Blockchain network when they reach a particular

threshold amount. To determine if a DDoS attack is happening, these particular nodes analyze the incoming requests.

If the node really discovers an attack, the associated IP address will be logged on the blockchain. As the Blockchain ledger is available to all networked devices, the system under attack can block this specific IP address. The following process is employed to detect and mitigate DDoS when any server is being targeted.

1. The target machine shares all requests with nearby machines or servers. This way, all types of legitimate and illegitimate requests are shared on the network among all nodes.
2. The neighboring nodes then inspect the incoming requests and distinguish them as legit or malicious.
3. In case neighboring node discovers the request as malicious, then the source IP address is blocklisted and recorded in the blockchain ledger.
4. The blocklisted IP is stored in a distributed ledger along with a timestamp in order to block the IP only for a certain amount of time so that fake IP addresses used in DDoS attacks cannot be blocked forever.

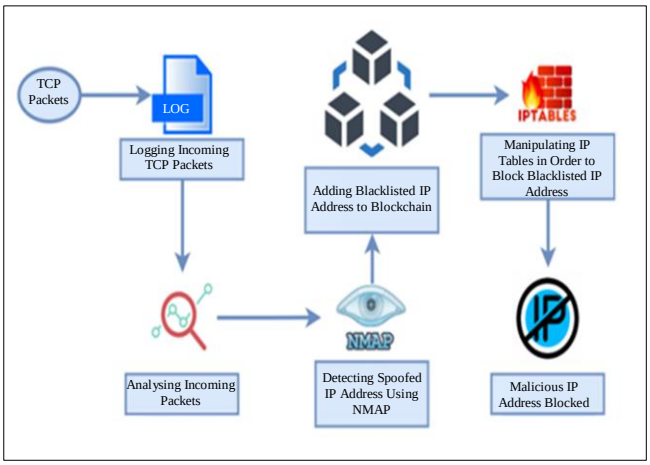


**Fig. 5 Proposed methodology for blocklisting IP address for DDoS mitigation**

### *4.2. Experiment Setup*

The following are the steps for modeling a DDoS attack and detecting and mitigating DDoS attacks using the proposed algorithm.

#### *4.2.1. Modelling a DDoS Attack*

The Hping3 tool is used to model a DDoS attack scenario. Using the hping3 tool, the target server is flooded with SYN requests by spoofing IP addresses. In real-time, botnets are utilized for this purpose. The command for simulating the DDoS attack using the hping3 tool is,

sudo hping3-S--flood--Interface $interfaceName--rand -source--destport $ destinationPort $ destinationIP

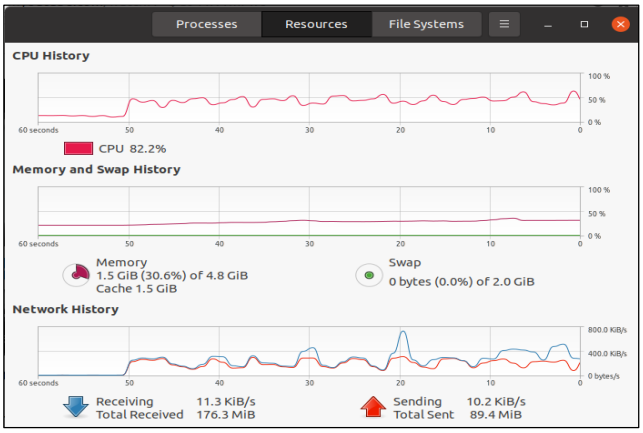


**Fig. 6 CPU and network usage during a DDOS attack on the server**

#### *4.2.2. Redirecting Incoming Requests*

Packet rerouting is accomplished by configuring the server's IP tables. The packets, along with legitimate requests, are routed to peer nodes and logged to a file called x.txt for further processing.

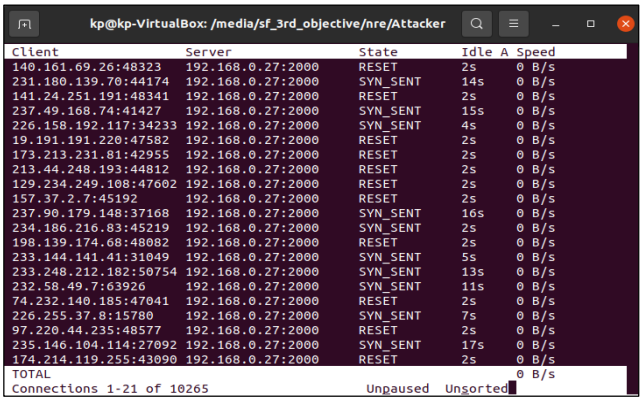


**Fig. 7 Output for analyzing the incoming packets to the server**

#### *4.2.3. Detecting Malicious IP Address*

Using Nmap, a SYN scan (TCP-based probing) is performed on all IP addresses indicated in the x.txt file. Using this, malicious/spoofed IP addresses are detected and blocklisted.

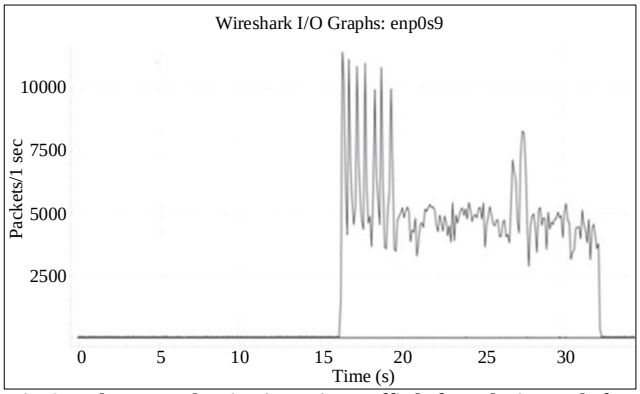


**Fig. 8 Packet trace showing incoming traffic before, during and after the attack**

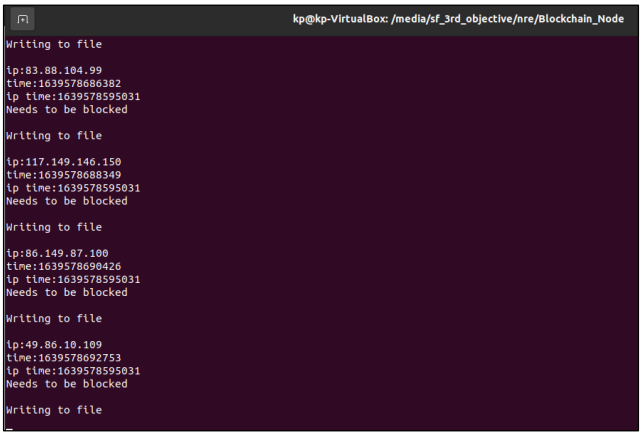


**Fig. 9 Testing of IP address to detect malicious address**

*4.2.4. Creating IP Addresses Blocklist*

Once the IP addresses are blocklisted, they are stored in the distributed ledger with a timestamp using web3.js.

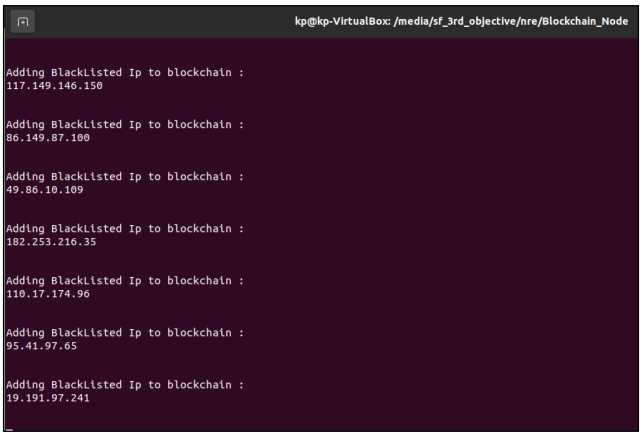


**Fig. 10 Illustration of creating IP addresses blocklist in blockchain**

*4.2.5. Blocking the Blocklisted IP Addresses*

The peers in the network then block the IP address listed in the blocklisted IP address list using iptables.

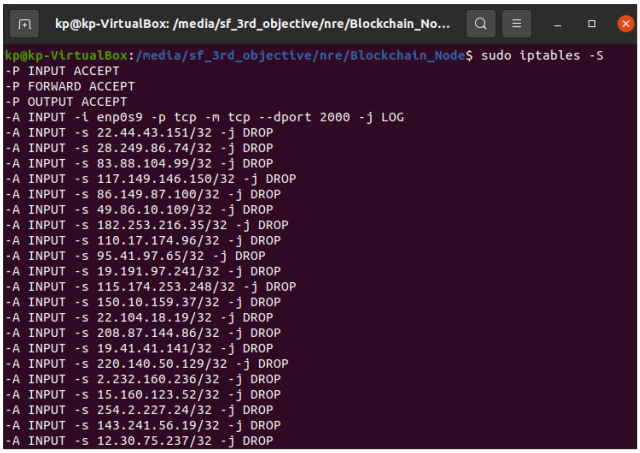


**Fig. 11 Illustration of IP-tables log showing blocked malicious IP addresses**

## 5. Results and Discussion

When a packet is classified as malicious, the decentralized network node adds the packet's information and IP address to the blockchain, where a blocklist is maintained and that IP is subsequently blocked. For comparing the effectiveness of the mechanisms for detecting and mitigating DDoS flooding attacks, the following parameters are considered:

Precision is calculated as the proportion of appropriately categorized positive predictions (malicious packets) and the total number of positive predictions (actually classified packets).

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}}$$

Accuracy is described as a measurement of the number of appropriately categorized packets.

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}}$$

False Positive Rate is measured as the proportion of inappropriately categorized positive predictions (legitimate packets) to the total number of supposed negative predictions (legitimate packets).

$$\text{FPR} = \frac{\text{FP}}{\text{FP+TN}}$$

True Positive Rate is measured as the proportion of appropriately categorized positive predictions (here malicious packets) to the total number of supposed positive predictions (malicious packets).

$$\text{TPR} = \frac{\text{TP}}{\text{TP+FN}}$$

Where TP - Count of truly categorized legitimate packets,
TN - Count of truly categorized malicious packets,
FP - Count of falsely categorized legitimate packets,
FN - Count of falsely categorized malicious packets.

**Table 1. Accuracy, precision, FPR and TPR analysis**

| | Accuracy | Precision | FPR | TPR |
|---|---|---|---|---|
| Yuan et al. | 92.09 | - | 8.45 | 88.37 |
| Yuan-H et al. | 86.13 | - | 12.26 | 86.26 |
| Pandian et al. | 89.25 | 88.16 | - | - |
| Manikumar | 95.19 | 95.1 | - | - |
| Yichen et al. | 96.33 | - | 7.63 | 96.34 |
| Choi et al. | - | - | 6.27 | 97.7 |
| Proposed | 96.65 | 95.1 | 5.1 | 98.84 |

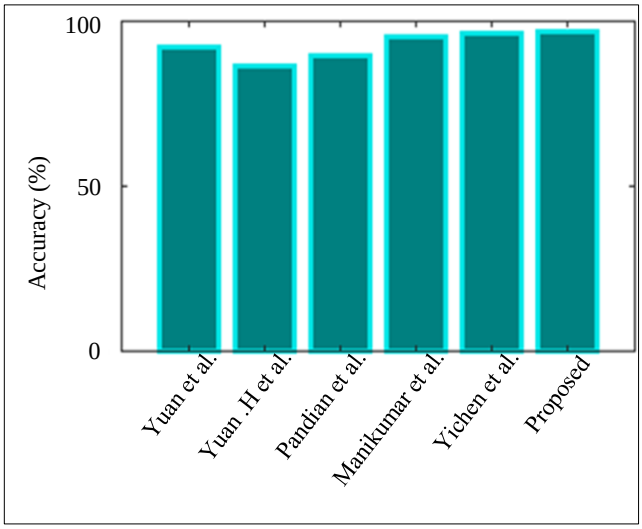


**Fig. 12 Accuracy analysis of different models**

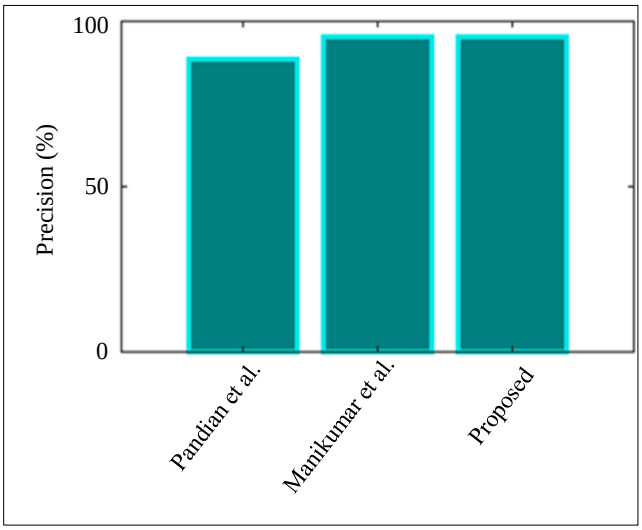


**Fig. 13 Precision analysis of different models**

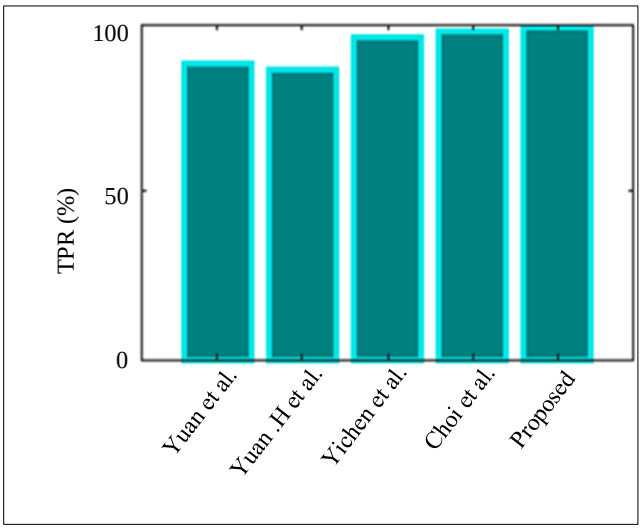


**Fig. 14 True Positive Rate analysis of different models**

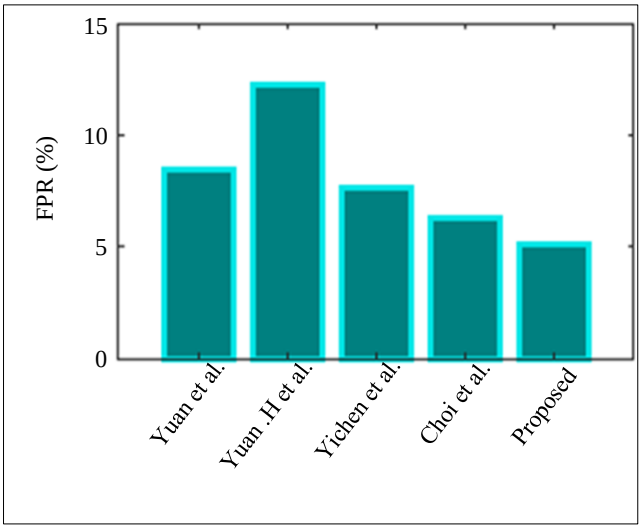


**Fig. 15 False Positive Rate analysis of different models**

**Table 2. Actual and predicted data packets**

| Actual | Predicted | |
|---|---|---|
| | **Legitimate** | **Malicious** |
| **Legitimate** | 1898 | 102 |
| **Malicious** | 32 | 1968 |

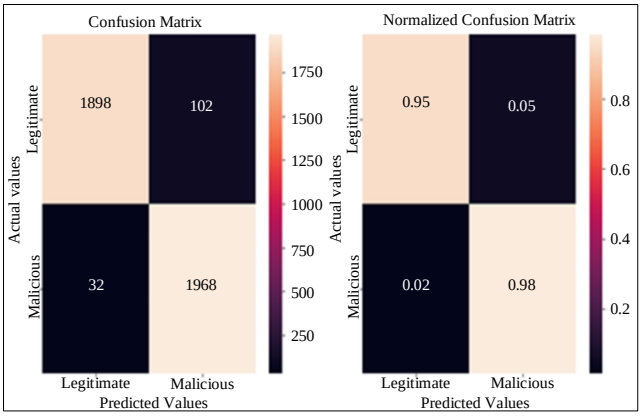


**Fig. 16 Confusion matrix result of proposed model**

The results of the different implementations compared are shown in the above graphs. The proposed mechanism provides improved detection of the DDoS, taking into account the outcomes provided in Figure 12 compared with other widely used approaches [30-34]. This approach can be employed in a distributed system to prevent service denial to legitimate clients brought on by a distributed denial service. The proposed approach gives better accuracy and a lesser misclassification rate compared to other works.

## 6. Conclusion

A collaborative approach is recommended to enhance the existing DDoS mitigation strategies. This study proposes the

utilization of blockchain and smart contracts to streamline DDoS mitigation, offering applicability across diverse domains. The primary innovation of this method lies in employing blockchain technology to establish immutability and transparency, preventing any unauthorized alteration of the blocklisted IP Addresses stored in the blockchain. The entire network, including servers and machines, can access this list, providing an additional layer of security as the information is uniformly accessible and resistant to tampering. Distributed ledger technology makes DDoS mitigation cost-effective and transparent, posing a challenge for attackers to manipulate banned IP addresses. Incorporating machine learning algorithms can further enhance the precision of identifying malicious actors.

## References


[1] Neha Agrawal, and Shashikala Tapaswi, "Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3769-3795, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] Karanbir Singh, Kanwalvir Singh Dhindsa, and Deepa Nehra, "T-CAD: A threshold Based Collaborative DDoS Attack Detection in Multiple Autonomous Systems," *Journal of Information Security and Applications*, vol. 51, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Afsaneh Banitalebi Dehkordi, MohammadReza Soltanaghaei, and Farsad Zamani Boroujeni, "The DDoS Attacks Detection through Machine Learning and Statistical Methods in SDN," *The Journal of Supercomputing*, vol. 77, pp. 2383-2415, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Elahe Fazeldehkordi, Olaf Owe, and Toktam Ramezanifarkhani, "A Language-Based Approach to Prevent DDoS Attacks in Distributed Financial Agent Systems," *International Workshop on Information and Operational Technology Security Systems, Computer Security*, pp. 258-277, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[5] An Wang et al., "A Data-Driven Study of DDoS Attacks and Their Dynamics," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 3, pp. 648-661, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Jieren Cheng et al., "A Novel DDOS Attack Detection Method Using Optimized Generalized Multiple Kernel Learning," *Computers, Materials & Continua*, vol. 62, no. 3, pp. 1423-1443, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Seth Djane Kotey, Eric Tutu Tchao, and James Dzisi Gadze, "On Distributed Denial of Service Current Defense Schemes," *Technologies*, vol. 7, no. 1, pp. 1-24, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[8] Sanghun Choi, Yichen An, and Iwao Sasase, "A Lightweight Detection Using Bloom Filter against Flooding DDoS Attack," *IEICE Transactions on Information and Systems*, vol. E103.D, no. 12, pp. 2600-2610, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] Marco Mazzoni, Antonio Corradi, and Vincenzo Di Nicola, "Performance Evaluation of Permissioned Blockchains for Financial Applications: The Consensys Quorum Case Study," *Blockchain: Research and Applications*, vol. 3, no. 1, pp. 1-12, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Tobias Guggenberger et al., "An In-Depth Investigation of the Performance Characteristics of Hyperledger Fabric," *Computers & Industrial Engineering*, vol. 173, pp. 1-20, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Ahmed Afif Monrat, Olov Schelén, and Karl Andersson, "A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities," *IEEE Access*, vol. 7, pp. 117134-117151, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[12] Bruno Rodrigues et al., "Evaluating A Blockchain-Based Cooperative Defense," *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, Arlington, USA, pp. 533-538, 2019. [Google Scholar] [Publisher Link]

[13] B.B. Gupta, R.C. Joshi, and Manoj Misra, "Distributed Denial of Service Prevention Techniques," *International Journal of Computer and Electrical Engineering*, vol. 2, no. 2, pp. 268-276, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[14] Tasnuva Mahjabi et al., "A Survey of Distributed Denial-of-Service Attack, Prevention, and Mitigation Techniques," *International Journal of Distributed Sensor Networks*, vol. 13, no. 12, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[15] Neelam Dayal, and Shashank Srivastava, "Analyzing Behavior of DDoS Attacks to Identify DDoS Detection Features in SDN," *2017 9th International Conference on Communication Systems and Networks (COMSNETS)*, Bengaluru, India, pp. 274-281, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[16] K. Geetha, and N. Sreenath, "SYN Flooding Attack - Identification and Analysis," *International Conference on Information Communication and Embedded Systems (ICICES2014)*, Chennai, India, pp. 1-7, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[17] Mitko Bogdanoski, Tomislav Shuminoski, and Aleksandar Risteski, "Analysis of the SYN Flood DoS Attack," *International Journal of Computer Network and Information Security*, vol. 5, no. 8, pp. 1-11, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[18] Xiaojun Guo, and Xuan Gao, "A SYN Flood Attack Detection Method Based on Hierarchical Multihead Self-Attention Mechanism," *Security and Communication Networks*, vol. 2022, pp. 1-13, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Omer Elsier Tayfour, and Muhammad Nadzir Marsono, "Collaborative Detection and Mitigation of Distributed Denial-of-Service Attacks on Software-Defined Network," *Mobile Networks and Applications*, vol. 25, pp. 1338-1347, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Meryam Essaid et al., "A Collaborative DDoS Mitigation Solution Based on Ethereum Smart Contract and RNN-LSTM," *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Matsue, Japan, pp. 1-6, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[21] Nguyen Ngoc Tuan et al., "A DDoS Attack Mitigation Scheme in ISP Networks Using Machine Learning Based on SDN," *Electronics*, vol. 9, no. 3, pp. 1-19, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[22] Georgios Spathoulas et al., "Collaborative Blockchain-Based Detection of Distributed Denial of Service Attacks Based on Internet of Things Botnets," *Future Internet*, vol. 11, no. 11, pp. 1-24, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[23] Weizhi Meng et al., "When Intrusion Detection Meets Blockchain Technology: A Review," *IEEE Access*, vol. 6, pp. 10179-10188, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[24] Ui-Jun Baek et al., "DDoS Attack Detection on Bitcoin Ecosystem Using Deep-Learning," *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Matsue, Japan, pp. 1-4, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[25] Tsuyoshi Idé, "Collaborative Anomaly Detection on Blockchain from Noisy Sensor Data," *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, Singapore, pp. 120-127, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[26] Bruno Rodrigues et al., "A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts," *Security of Networks and Services in an All-Connected World*, pp. 16-29, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[27] Yiyun Zhou et al., "Improving IoT Services in Smart-Home Using Blockchain Smart Contract," *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, Canada, pp. 81-87, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[28] Jose Eduardo A. Sousa et al., "Fighting Under-Price DoS Attack in Ethereum with Machine Learning Techniques," *ACM Sigmetrics - Performance Evaluation Review*, vol. 48, no. 4, pp. 24-27, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[29] Muhammad Saad, My T. Thai, and Aziz Mohaisen, "POSTER: Deterring DDoS Attacks on Blockchain-Based Cryptocurrencies through Mempool Optimization," *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pp. 809-811, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[30] D.V.V.S. Manikumar, and B. Uma Maheswari, "Blockchain Based DDoS Mitigation Using Machine Learning Techniques," 2020 *Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, pp. 794-800, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[31] A.P. Pandian, and S. Smys, "DDOS Attack Detection in Telecommunication Network Using Machine Learning," *Journal of Ubiquitous Computing and Communication Technologies*, vol. 1, no. 1, pp. 33-44, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[32] Yuan-Hsiang Su, Amir Rezapour, and Wen-Guey Tzeng, "The Forward-Backward String: A New Robust Feature for Botnet Detection," *2017 IEEE Conference on Dependable and Secure Computing*, Taipei, Taiwan, pp. 485-492, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[33] Xiaoyong Yuan, Chuanhuang Li, and Xiaolin Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, Hong Kong, China, pp. 1-8, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[34] Yichen An et al., "Traffic Feature-Based Botnet Detection Scheme Emphasizing the Importance of Long Patterns," *International Conference on Image Processing and Communications*, pp. 181-188, 2019. [CrossRef] [Google Scholar] [Publisher Link]