LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. 11(2025)

SUSTAINABLE IOT PROTECTION AND IMPROVEMENT UNDER ACT OF 2020: A SMART BLOCKCHAIN-BASED FRAMEWORK TO MITIGATE DISTRIBUTED DENIAL OF SERVICE ATTACKS

SindhujaDhanapal[1]*, Samson Ravindran[1] and JesudasThangaraju[1]

[1]Mahendra Engineering College, Tamil Nadu, India;
sindhujadhanapal@gmail.com[1]
samsonsalem@gmail.com[1]
jesuphd@gmail.com[1]

*Correspondence: sindhujadhanapal@gmail.com

Abstract
The speedy growth of Internet of Things (IoT) networks across metropolitan and domestic situations has increased vulnerability to Distributed Denial of Service (DDoS) attacks, which overcome systems with extreme traffic and interrupt legitimate services. This research introduces BlockSecure, a peer-to-peer ledger–based defensive mechanism particularly intended to improve IoT flexibility against DDoS threats. The structure leverages blockchain's decentralization and immutability to eradicate single points of stoppage and set up trust across unified devices. The methodology commence with network initialization, including device recognition and protected communication setup, followed by the assortment of appropriate ledger architecture (public, private, or consortium). Smart contracts are employed to manage device verification, data-sharing rules, and secure communication protocols. Cryptographic keys ensure trusted communications, while real-time traffic observes enable early finding of strange activities. Upon identifying a possible attack, BlockSecure autonomously mitigates risks by blocking malicious sources or rerouting traffic to preserve service stability. All incidents are enduringly recorded on the distributed ledger, produce a reliable knowledge base for ongoing modification of security plans. Through adaptive learning and continuous updates, BlockSecure demonstrates a dynamic, scalable, and sustainable approach to protecting IoT infrastructures from persistent DDoS threats, thereby ensuring long-term network integrity and availability.

Keywords: Peer-to-Peer Ledger (block format chain structure), Internet supportive Things (IoT) , Distributed based Denials of Service (DDoS) attacks, cryptographically generated keys, cyber attacks, data sharing and network resilience.

1. Introduction

The Internet of Things, a concept that refers to the interconnectedness of everyday objects and devices through internet connectivity. These objects, which might range from household appliances like refrigerators and thermostats to industrial based machinery and wearable gadgets, are embedding with sensors, software, and other technologies that enabled them to collect and exchange data. The primary role of IoTmight to facilitate the seamless transmission of information's between these interconnected devices, by enabling them to communicate, collaborates, and to perform various tasks more efficiently.In essence, IoT transforms ordinary objects into "smart" devices capable ability of gathering and analyzing, and to sharing of data in real-time. This data transmission plays a main role in numerous aspects of daily.

2. Materials and Methods

The Materials and Methods should be described with sufficient details to allow others to replicate and build on the published results. Please note that the publication of your manuscript implicates that you must make all materials, data, computer code, and protocols associated with the publication available to readers. Please disclose at the submission stage any restrictions on the availability of materials or information. New methods and protocols should be described in detail while well-established methods can be briefly described and appropriately cited.Research manuscripts reporting large datasets that are deposited in a publicly available database should specify where the data have been deposited and provide the relevant accession numbers. If the accession numbers have not yet been obtained at the time of submission, please state that they will be provided during review. They must be provided prior to publication. In agriculture related IoT devices such as soil moisture sensors, smart drones, and GPS-enabled tractors may enable farmers to monitor crop Conditional growth, manage irrigation mechanism, and optimizes the crop yields. This will help to conserve resources, increase productivity, and ensures sustainable farming practices.Hence, IoT plays a pivotal role in data transmission by creating interconnected networks as smart

devices that collect, process, and to share data to automate processes, enhancement in decision-making, and improvise the overall efficacy and convenience in various aspects of lives and industries.

1.1 DDoS Attacks in IoT Networks

Distributed based Denials of Service (DDoS) attacks posed a significant threat to Internet supportive Things (IoT) networks, which connect variously devices over the internet. These attacks may occur when multiple compromises a computers or devices flooding a target mechanism, like a server or website, with an overwhelming amount of traffics, in rendering it inaccessible to legitimate users. DDoS attacks in IoT networks also have serious consequences, by including service disruption, data loss, and any of unauthorized access to sensitive information[4].

One of key reasons why IoT networks particularly vulnerable to DDoS attacks are sheer number of connected devices. Unlike traditional networks, which primarily consists of computers and their servers, IoT networks encompasses a wide range of devices, from smart thermostats and security cameras to industrial based sensors and medical devices. This extensively connected network of interconnected devices might provide attackers with a large and diverse pool of potential targets to exploit. some cases, manufacturers prioritizes convenience and affordability over security, leads to devices with default or weak passwords, outdated software package, and inadequate encryption mechanisms. As a result, these smart devices can be easily compromise and enlisted into bonnets—networks of infected devices controlled by a malicious Event to as DDoS attacks. The impact of DDoS attacks on IoT networks able to severe and far-reaching. For example, in the case of smart homes, a DDoS attack on connected devices like smart ways of thermostats or security cameras could disrupt essential services, compromises the home security, and even leads to privacy breaches if sensitive footage will accessed by unauthorized parties. Similarly, in industrial based settings, DDoSattacks targeting IoT-enabled machinery or sensors should disrupt production processes, causes equipment damage, and result in significant financial losses[5]. In DDoS attacks represents a serious threat to IoT networks, in exploiting vulnerabilities in connected devices to disrupt services and compromises data security. In Addressing this threat requires proactive measures to enhance the security of IoT devices and networks, as well as robust monitoring and to response mechanisms in detectingand to mitigate attacks effectively. By taking these steps, stakeholders can help safeguard IoTEco mechanisms against the growing of DDoS attacks and to ensure the reliable and security of connected devices and services.

1.2 Need of block chain in DDoS threats.

In the face of escalating of Distributed based Denials of Service (DDoS) threats, Peer-to-Peer Ledger(block format chain structure) technology has been emerged as a promising solution to bolstering of the resilience of networks, particularly in the context of Internet supportive Things (IoT) environments. DDoS attacks, may characterized by of target mechanism with of traffic from multiple compromised devices, poses significant challenges to traditional network defensive mechanisms. However, Peer-to-Peer Ledger(block format chain structure)may offers unique features that can be address some of the inherent vulnerabilities exploited by DDoSattackers[6].

First and foremost, Peer-to-Peer Ledger(block format chain structure)'s decentralized architecture may serves as a formidable defense against DDoS attacks. Unlike centralized mechanism that rely on a single point of failure, Peer-to-Peer Ledger(block format chain structure) operates across a distributed network of nodes, by making it inherently resistant to attacks aimed at disrupting network available. By decentralizing control and in spreading data across multiple nodes, Peer-to-Peer Ledger(block format chain structure) mitigates the risk of DDoSattacks in crippling the entire network, as there is no single target for attackers to exploit. Moreover, Peer-to-Peer Ledger(block format chain structure)'s immutable ledger will provides a tamper-proof record of transactions and network activity, in making it an invaluable tool for detecting and mitigating ofDDoS threats. Each transactions and communication within the network is cryptographically secured and recorded on the Peer-to-Peer Ledger(block format chain structure), in en-

abling network administrators to trace source of malicious activity and take appropriate countermeasures[7]. This transparent and auditable record enhancement of accountability and facilitated forensic analysis in the type of DDoS attacks.

Furthermore, Peer-to-Peer Ledger(block format chain structure)'s smart contract functionality may offers automated mechanisms for detecting and responding to DDoS threats in real-time. Smartly behaved contracts are self-executing contracts with predefined rules and conditions encoded on Peer-to-Peer Ledger (block format chain structure). In the context of DDoS mitigation, smartly behaved contracts could be programmed to monitoring network traffic patterns, detect anomalies indicative of an ongoing threat attack, and automatically get trigger predefined responses, like traffic rerouting or resource allocation adjustments. This automated approach reduced the reliance on manual intervention and enabling swift and adaptive responses to evolving of DDoS threats.

Additionally, Peer-to-Peer Ledger (block format chain structure) enhances security of IoT devices and networks by facilitating the combustive authentication and to have an access control mechanisms [8-9]. Each IoT device could be assigned a unique cryptographic identity stored on Peer-to-Peer Ledger (block format chain structure), by ensuring secure communication and preventing of unauthorized access by malicious actors. Furthermore, Peer-to-Peer Ledger(block format chain structure)-based identity of management solutions enables seamless device on boarding and authentication, for mitigating the risk of compromised devices being enlisted into botnets for havingDDoS attacks. In Peer-to-Peer Ledger (block format chain structure) technology will offers compelling advantages in mitigating of the growing threat of DDoS attacks, particularly in IoTenvironments[8]. Its decentralized architecture, immutable ledger, smart contract functionality, and identity management capabilities of collectively enhance network resilience, transparency, and security. By leveraging Peer-to-Peer Ledger (block format chain structure) as a foundational framework for DDoS defense, an organizations can fortify their networks against malicious actors and can ensure the uninterrupted available of critical services and resources [10].

1.3 Contribution of Proposed methodology

1. The present research reveals Peer-to-Peer Ledger (block format chain structure)’s possible to bolster network pliability against DDoS attacks, especially on IoT situations.
2. Peer-to-Peer Ledger (block format chain structure)’s decentralized based architecture decreases the threat of DDoS attacks by crippling entire networks by get rid of any single points of breakdown.

The unchallengeable ledger might offer by Peer-to-Peer Ledger (block format chain structure) facilitate of the see-through recording of network dealings, by aiding in the uncovering and mitigation of DDoS threats.

3. Smart contract functionality automates the detections and response to DDoS attacks in real-time, reducing the dependence on physical interference and ornamental of network flexibility.
4. Peer-to-Peer Ledger(block format chain structure)enhancement of the security aspects inIoT devices by providing robust authentication and having access control mechanisms, mitigating risk of compromised devices being used in DDoS attacks.
5. Overall, research highlighted Peer-to-Peer Ledger(block format chain structure)’s potential to enhancing of network resilience, transparency, and security against the escalating threat of DDoS attacks, particularly in IoT environments.

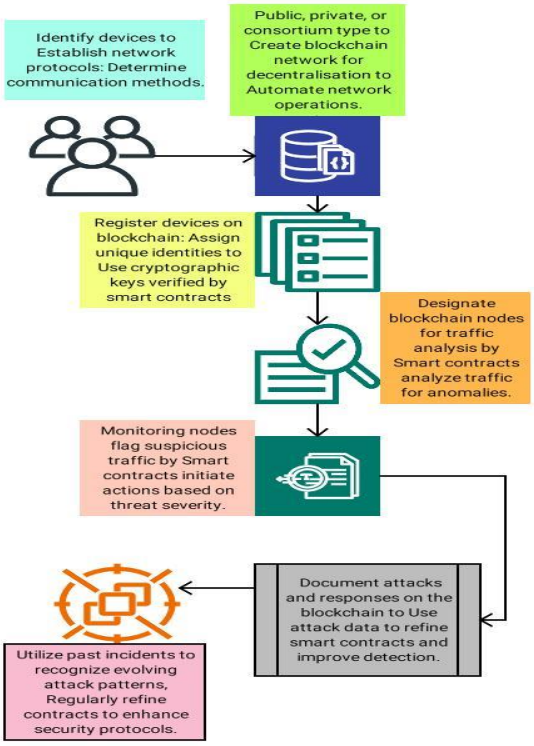

Figure 1. Outlined infrastructure of proposed mechanism

The diagram in Figure 1 illustrated the Comprehensively process of enhancing IoT network security using Peer-to-Peer Ledger(block format chain structure) technology incombatingDistributed based Denials of Service (DDoS) attacks. It begins with setting up IoT network, identifying the devices, and in establishing communication protocols. In Introducing Peer-to-Peer Ledger(block format chain structure)involves by selecting the type and in creating a decentralized network, along with developing smartly behaved contracts for automated operations. The research study focused on enhancing the security of Internet supportive Things (IoT) networks byusingPeer-to-Peer Ledger(block format chain structure) technology to defend against Distributed based Denials of Service (DDoS) attacks. DDoS attacks are cyber-attacks where multiple compromised computer mechanism attacks a target, like a server, website, or other network resource, and may cause a denial of service for users of the targeted resource. The IoT networks, which connect various devices over the internet, might be particularly vulnerable to such attacks, leading to service disruption, loss of data, or having unauthorized access to sensitive information.

As it is know that Peer-to-Peer Ledger(block format chain structure) technology will offers a decentralized and secure framework, which can be used to improve the resilience of IoT networks against DDoS attacks. The current research suggests that the study proposes or amethods in which Peer-to-Peer Ledger(block format chain structure) can be used to authenticate devices within the network, byensuring a secure communication, and prevent unauthorized access, thereby mitigating of the risk and impact of DDoS attacks on IoT networks. This might involve using Peer-to-Peer Ledger(block format chain structure) to create a distributed ledger of transactions that can't be altered retroactively, providing a way to track and secure communications between devices and prevent attackers from overwhelming the network.

1.4 Public Law Number: 116-207 (12/04/2020)

Internet of Things Cyber security Improvement Act of 2020 /116-207 /12/04/2020.The research article clearly based on under of act of 2020 /116-207. The legislation mandates that NIST and OMB implement outlined measures aimed at enhancing cyber security for IoT gadgets. The Internet of Things expands network access beyond computers onto tangible items like appliances and furniture.Rephrase In particular, this legislation mandates NIST to create and release regarding how various entities should utilize and oversee Internet-of-Things gadgets within their jurisdictions, ensuring compliance with necessary data protection measures related to these technologies' potential cyber threats.

2. Literature review for proposed mechanism

The study [11] Peer-to-Peer Ledger(block format chain structure)-based Internet of Things Security and Privacy of Smart Homes" investigates way ofPeer-to-Peer Ledger(block format chain structure) technology can enhances security and privacy in smart homes. In elegant home situation, where numerous IoT devices get interconnected, for ensuring robust security measures is crucially to protect sensitive data and maintain the user privacy. the research aimed to mitigate potential vulnerabilities exploited by cyber threats, like Distributed based Denials of Service (DDoS) attacks. Additionally, the study explored use ofPeer-to-Peer Ledger(block format chain structure)could facilitate secure device authentication and data encryption to Safeguarding against unauthorized access and data breaches. In the research paper [12] Enhancing Security and Privacy in IoT Networks Using Peer-to-Peer Ledger(block format chain structure) Technology look into into the possible of Peer-to-Peer Ledger(block format chain structure) technology to strengthen the safety and privacy events in Internet supportive Things (IoT) networks. In IoT surroundings, where devices are consistent and switch over of responsive data, make certain robust security measures is vital to guard against cyber intimidation. By incorporate Peer-to-Peer Ledger(block format chain structure) into IoT networks, the study intended to address vulnerabilities and moderate the risks, like unauthorized access and data breaches. Peer-to-Peer Ledger(block format chain structure)'s decentralized architecture and immutable ledger provides a secure framework for storing and managing ofIoTdata in reducing the risk of tampering or manipulation. Additionally, smartly behaved contracts enabled automated enforcement of security protocols, enhancing of the efficacy of threat detection and response mechanisms. Through its innovative approach, the research explores way of Peer-to-Peer Ledger(block format chain structure) technology couldenhanced the overall security and privacy of IoT-networks in offering a promising solution to safeguard against emerging cyber threats and to ensure the integrity of IoTEco mechanism.

The Machine Learning-Based DDoS Detection for IoT Networks [13] have a broadexploration on an innovative approach to enhancing the security of Internet supportive Things (IoT) networks by leveraging machine Learning-Driven techniques. In this study, researchers aimed to address the growing threat of Distributed based Denials of Service (DDoS) attacks targeting ofIoT devices. By analyzing network traffic patterns using machine Learning-Driven algorithms, the mechanism could identifyof anomalous behavior indicative of DDoS activity. But Unlike traditional rule-based methods, machine learning offered advantage of adaptability and scalability, by allowing the mechanism to learn from past attacks and continuously improved its detection capabilities. These researches also contribute valuable insights into the increase of practical defense method against DDoS threats, eventually by enhancing the flexibility of IoT networks and in conservation against troublesome cyberattacks.

The Deep Packet Inspection for DDoS Detection [14-16] in IoTNetworks might initiate a new technique for ornamental of the safety of Internet supportive Things (IoT) networks by employing deep packet inspection (DPI) practice. This approach could involved by analyzing the content of data packets traversing the network inidentifying patterns associated with Distributed based Denials of Service (DDoS) attacks. Through extensive conducting tests and assessment, the study established the effectiveness of DPI in justifying anyDDoS threats in IoTenvironments, while minimizing of false positives. This research represents a significant advancement in the field of IoT security, by offering a proactive approach to detecting and in mitigating DDoS attacks, thereby enhancing the resilience of IoT networks against cyber threats.

A Behavior-Based DDoS Detection for IoTDevices [17-19], an innovative approach to enhancing of the security of Internet supportive Things (IoT) devices by focusing on behavior-based detection methods. This study aimed to addressing of the growing threat of Distributed based Denials of Service (DDoS) attacks targeting IoT devices by analyzing their behavioral patterns. Unlike traditional signature-based detection methods, which might struggles to Identifying a new and evolving attack vectors, behavior-based detection will offers greater adaptability and effectiveness in combating sophisticated DDoS attacks. Through an extensive testing and validation, this research demonstrated the efficacy of behavior-

based DDoS detection for IoT devices, by paving the way for more resilient and secure IoTEco mechanism.
An ensemble based method FlowSpotter [20], which combines multiple detection techniques for improved accuracy and reduces false positives and negatives. But the increased complexity and resource requirements with careful tuning and selection of algorithms are considered to be the drawbacks of this approach.

3.Proposed mechanism

The proposed mechanism will employs a systematic approach to enhanced the security of Internet supportive Things (IoT) networks against any Distributed based Denials of Service (DDoS) attacks by leveraging ofPeer-to-Peer Ledger(block format chain structure) technology. The processing steps of the proposed mechanism involved a several key stages. Firstly, the IoT network will set up, where all devices are identifies and communication protocols mightestablish to facilitate seamless interaction. Following this, Peer-to-Peer Ledger(block format chain structure) technology is introduces, with the type of Peer-to-Peer Ledger block format chain structure) chosen (public, private, or consortium) depends on the network's requirements. The Peer-to-Peer Ledger(block format chain structure) network will then created, with nodes distributed across different locations to ensuredecentralization, and smartly behaved contracts are developing to automate various device authentication and response actions to potential threats.
The authentication is a critical step in the proposed mechanism, where each of device in the IoT network is registered on the Peer-to-Peer Ledger(block format chain structure) with a unique identity. The Devices utilizescryptographicallygenerated keys to authenticate themselves before communication within the network, with this process managed and verified through smart contracts. In the event of an identified DDoS attack, the planned mechanisms will initiates a regular responses based on the harshness of the threat. This may involve blocking the attacking source or rerouting traffic to mitigate the impact on network available and performance. Additionally, the proposed mechanism emphasized the importance's of updating the Peer-to-Peer Ledger(block format chain structure) to record incidents of detected attacks and response actions. This unchallengeable evidence serves as a precious resource for future threat analysis and increases the network's ramparts over time. Furthermore, a feedback loop is established to employ in sequence from attack happenings to refine smartly behaved contracts incessantly, enhancing of the mechanism'scapability to detect and responding to new threats effectively. Hence, the proposed mechanism offers a Comprehensively and adaptive approach to safeguarding theIoT networks against DDoS attacks, by utilizing Peer-to-Peer Ledger(block format chain structure) technology to enhancing the security, flexibility, and receptiveness in the face of developing cyber threats.

The flows of planned mechanism are portraying in figure 2. ThePeer-to-Peer Ledger(block format chain structure)-based mechanism for protecting theIoT networks from any ofDDoSattacks may offers a decentralized, secure, and adaptable approach. By utilizing of smartly perform agreement for automatic devices validation, threat detection, and response; the network could considerably enhance its resilience against the cyber threats.

Algorithm 1: Algorithm of Proposed mechanism

Step 1: Setting Up of the IoT Network

1.1 Definition of the IoT network: Identify all devices that might be part of the IoT network. It includes sensors, any type of cameras, smart devices, etc.

1.2 Establishing of protocols: To determine how devices will communicates with each other and with the internet.

Step 2: By Introducing Peer-to-Peer Ledger (block format chain structure)

*2.1 Choosing of a Peer-to-Peer Ledger (block format chain structure) type:*To decide whether to use a public or private, in consortium Peer-to-Peer Ledger (block format chain structure) based on the network's needs.

2.2 Creating the Peer-to-Peer Ledger (block format chain structure) network: To Set up the Peer-to-Peer Ledger (block format chain structure) nodes. It can be distributed across different locations to ensuredecentralization.
2.3 The Development of smart contracts: Writing smartly behaved contracts to automated network operations like device authentication event, data sharing rules, and response actions to potential threats.
Step 3: Device Authentication mechanisms
3.1 Registered devices on the Peer-to-Peer Ledger (block format chain structure): Each of devices in the IoT network is registered on Peer-to-Peer Ledger (block format chain structure) with a unique identity number.
3.2 Eventuation: the Devices use cryptographically y keys to authenticate themselves before they might communicate within the network. This process will be managed and verified through smart contracts.

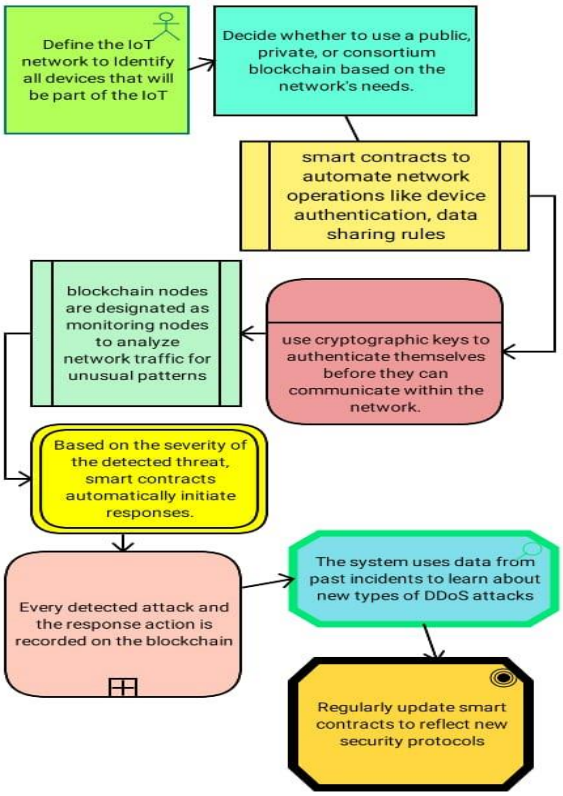

Figure 2. Flow diagram of proposedmechanism

Step 4: Monitoring Network Traffic
*4.1 Deploy of monitoring nodes:*Some ofPeer-to-Peer Ledger(block format chain structure) nodes get designated as monitoring nodes. They can analyze network traffic for unusual patterns that might indicate a DDoS attack.
4.2 Real-time analysis: The Smartly behaved contracts could help analyze data traffic in real-time on detections of anomalies.
Step 5: On Detecting and Responding to DDoS Attacks
5.1 Anomaly detection alarm: Once an anomaly or a potential DDoS attack gets detected, the monitoring nodal points flag the suspicious traffic.
5.2 Automatic response: depending on the severity of the detected threat, smartly behaved contracts will automatically initiate responses. This cansbe included blocking the attacking source or rerouting traffic.
Step 6: The Updating the Peer-to-Peer Ledger (block format chain structure)
6.1 Recording of incidents: Every detected attack and the responses action is recorded on Peer-to-Peer Ledger (block format chain structure).This immutable record helping in future threat analysis and strengthening of the network's defenses.

6.2 Feedback loop: Information from attack incidents may use to updating and refined the smart contracts, improving the mechanism's capabilityin detections and respond to new threats.

Step 7: By Continuous Learning and Adaptation

7.1 Adaptable to new threats: The mechanism uses data from past incidents to learning about new types of DDoS attacks.

7.2 Updating of smart contracts: By Regular update smartly behaved contracts to reflect new security protocols and threat detecting algorithms.

The proposed mechanism will takes a holistic approach to bolstering of the security of IoT networks against Distributed based Denials of Service (DDoS) attacks through the integration of Peer-to-Peer Ledger(block format chain structure) technology. Initially, the IoT network will set up in identifying all devices, such as sensors or cameras, and smart devices, that will comprises the network. In the Subsequent event, protocols get instituted to regulates the communication between these devices and the internet. These protocols may ensure efficient and secure data transmission within the network, minimizing of vulnerabilities to potential DDoS attacks. Mathematically, the establishments of protocols could be represented as follows in (1).

Protocols=F(Devices, Communication Requirements) (1)

Where*F*may represent the function governing of the establishments of protocols, *Devices* may denoted the identified devices forming the part of the IoT network, *Communication Requirement* encompassed the specifications for communication between devices and the internet connectivity. By defining of robust protocols, the mechanism lays the groundwork for secured communication within the IoT network, reducing risk of unauthorized access and a potential exploitation by malicious entities aiming to neglectingDDoS attacks.

In next Step of the proposed mechanism, Peer-to-Peer Ledger(block format chain structure) technology mayintroduce to fortify the IoT network against any ofDDoS attacks. This step begins with the selection of most suitable Peer-to-Peer Ledger(block format chain structure) type—public or private, or consortium—depending on specific needs of network. Once the type is determines, Peer-to-Peer Ledger(block format chain structure) nodes are strategically maydeployed across multiple locations to achieved a decentralization. The Decentralization ensured that there is no single point of failure, by making it more difficult for attackers to disrupting the network. The deployment of Peer-to-Peer Ledger(block format chain structure) nodes be expressed as in(2)

Peer-to-Peer Ledger(block format chain structure) Nodes=D(Locations) (2)

Where,Ddescribes the function for deploying Peer-to-Peer Ledger(block format chain structure) nodes, *Locations* referring to the various geographically locations where the nodes get deployed.

Next, smartly behaved contracts get developed to automated crucial network operations. These smartly behaved contracts will serve as self-executing agreements that are encoding on the Peer-to-Peer Ledger(block format chain structure). They automate tasks like device authentication, data sharing rules, and responses for potential threats, streamlining network management and in enhancing security. The development of smartly behaved contracts might be represented as in (3).

Smart Contracts=S(Operations) (3)

Where '*S'* denoted the function for developing smartly behaved contracts, *Operations* tells about the various network operations automated by smart contracts.

By integrating ofPeer-to-Peer Ledger(block format chain structure) technology and smartly behaved contracts into the IoTnetwork infrastructure, the proposed mechanism will enhances security, transparency, and efficacy and thus fortifying the network against potential DDoS attacks.

Device authentication willsbe crucial aspects of the proposed mechanism, aimed in ensuring secure communication within the IoT network. This process may begins with registering each device on the Peer-to-Peer Ledger(block format chain structure), assigning a unique identity. The device's identity get recorded on the Peer-to-Peer Ledger(block format chain structure), forcreating a tamper-proof record of its existence within the network. The device registration will be represented as in (4)

Device Registration=R(Device,Identity) (4)

Where *R*describes the function for registering a device, *Device* denoted the specific device being registered;*Identity* refers to unique identity assigned to the devices. Once registered, devices utilize cryptographic keys in authentication before initiating communication within the network. These cryptographic keys might serve as digital signatures, for verifying the authenticity of the device and to ensuring that only authorized devices can participate in network activities. The device authentication could be expressed as in (5).

Device Authentication=A(Device,Keys) (5)

Where*A*denoted the function for authentication of a device, *Device* represented the device undergoing a authentication, *Keys* referred to the cryptographic keys used for authentication.

The authentication processes willmanage and to verified through smart contracts, which are self-executing agreements encoded on the Peer-to-Peer Ledger(block format chain structure). These smartly behaved contracts enforces the rules and conditions for device authentication, in ensuring that only legitimate devices gain access to network. In device authentication in the proposed mechanism involves registering each device on the Peer-to-Peer Ledger(block format chain structure) with a unique identity and utilizing of cryptographic keys for authentication. This process will be managed and verified through smart contracts, in enhancing the security and integrity of the IoT network.In proposed mechanism, for monitoring network traffic a crucial step in detecting and mitigating of Distributed based Denials of Service (DDoS) attacks. This process get facilitated by deploying designated monitoring nodes within the Peer-to-Peer Ledger (block format chain structure) network. The nodes continuously will analyze network traffic patterns in real-time, looking for anomalies that may indicated a potential DDoS attack. By monitoring the traffic at various points within the network, these nodes can detect abnormal Behavioral activityand any suspicious activity that deviated from established patterns. the monitoring of network traffic will be represented as in (6)

Traffic Monitoring=M(Network Traffic) (6)

Where,*M*Representation of the function for monitoring network traffic, *Network Traffic*denoted the data packets and information by flowing through the network.

The Smartly behaved contracts willplay a crucial role in this process by assisting in the analysis of data traffic. The smartly behaved contracts will program to Identifying and flagging of suspicious activity depends on predefined criteria and thresholds. They analyze network traffic data in real-time, looking for any signs of abnormal behavior such as unusually high traffic volume or unexpected patterns on data transmission.

Upon detecting a DDoS attack, the mechanism will initiates automatic responses depending on the severity of the threat. These responses are predefined within the smartly behaved contracts and might include blocking of the attacking source, rerouting traffic to alternative data paths, or implementing any of traffic prioritization mechanisms. The goal to mitigate the impact of the attack on network performance and ensured the continued available and reliable of network services. The automatic response to a DDoS attack is expressed as in (7);

Automatic Response=R (Threat Severity) (7)

Where *R* get represented the function for initiating an automatic response, *Threat Severity* indicated the severity level of the detected DDoS attack. By leveraging of monitoring nodes and smart contracts, the proposed mechanism will effectively detect and responding to DDoS attacks in real-time, thereby safeguarding the integrity and available of the IoT network.

In Subsequent step of the proposed mechanism, the Peer-to-Peer Ledger(block format chain structure) plays a crucial role in recording incidents of detected DDoS attacks and to the corresponding response actions. This created an immutable record that may serves as a valuable resource for future threat analysis. The Peer-to-Peer Ledger(block format chain structure)'s decentralized and tamper-proof nature for ensuring the integrity and reliable of this record, by allowing network administrators to trace the history of past attacks and responses accurately. The recording of attack incidents and responses actions can be represented as in (8)

Incident Recording=R(Attack,Response) (8)

Where *R*Tell about the function for recording incidents, *Attack* denoted the detected DDoS attack, *Response* refers to action taken in responses to the attack.

Furthermore, a feedback type of loop will established to utilize information from past attack incidents to continuously updated and refining of the smart contracts. This feedback loop should enhance the mechanism's capability to detect and responding to new threats effectively by incorporating insights gained from previous experiences. The feedback loop might be expressed as in (9);

Feedback Loop=F(Past Incidents) (9)

In this, the focus shifts to continuous learning and adaptation. The mechanism will leverages data from past incidents to Identifying and adapt to new types of DDoS attacks. The Smart contracts, which serve as backbone of the proposed mechanism 's in automation and response mechanisms, as a regularly updated to reflect new security protocols and threat detection algorithms. By preserve an unchallengeable record of attacks occurrence, updating of response mechanisms based on past understanding, and become accustomed to new threats, the mechanism also improve its overall security bearing and pliability against DDoS attacks.

4. Results and discussion

The projected mechanism highlights its efficiency in stimulating of IoT networks against Distributed based Denials of Service (DDoS) attacks. Through the integration of Peer-to-Peer Ledger(block format chain structure) technology and using of smart indenture, the mechanism established notable attainment in enhancing of network security, pliability, and its receptiveness. By setting up of the IoT network and bring in to a Peer-to-Peer Ledger(block format chain structure), the mechanism recognized a robust structure for making a secure communication and mechanized network administration. In Device authentication mechanisms guarantee that the only rightful strategies increase accessing to the network, mitigating the risk of illegal access and possible utilization by any malicious entities. Furthermore, in the observation of the network traffic facilitates the timely detections of irregularity and any potential DDoS attacks, allowing for swift and under attack response events. In the exploitation of elegantly perform contracts may help real-time analysis and decision-making, enhancing of the mechanism's ability to detect and alleviate threats efficiently.

In the record incidents of sense the attacks and its response actions provides valuable insights for futures threat analysis and mechanism modifications. By the unchallengeable record uphold on the Peer-to-Peer Ledger (block format chain structure) make certain the honesty and dependability of this information, enabling network administrators on trail of the history of past occurrence precisely. Moreover, the feedback loop established within the mechanism mayutilized data from past incidents to continuously update and refinement of smart contracts, enhancing of the mechanism's adaptability and responsiveness to evolving the cyber threats. This iterative process of learning and get used to make sure that the mechanism leftovers flexible against a budding assault vectors and able to successfully protect against new types of DDoS attacks. Henceforth, the results and discussion highlighted the proposed mechanism'scapability tomitigate the impact of DDoS attacks on IoT networks, by providing a comprehensive and adaptive approach to network security. By leveraging aPeer-to-Peer Ledger(block format chain structure) technology and in smart contracts, the mechanism will offer enhanced protection against cyber threats, ensuring of the uninterrupted available and reliable of network services.

The plot illustrated in figure 3, the efficacy of smartly behaved contracts for different simulation times ranging from 100 to 500 milliseconds (ms). Each box may represent the distribution of efficacy values observed at a specific simulation time slot. The central line within each box corresponds to median efficacy value, while the box edges may represent the lower and upper quartiles. The whiskers will extend to the minimum and maximum observed efficacy values, by excluding outliers represented by individual data points beyond the whiskers. Upon analysis, it's evident that as the simulation time gets increases, there will be a general trend of decreasing efficacy of smart contracts. For instance, at a simulation time of 100 ms, the median value efficacy is approximately 15 units, with an interquartile ranges as (IQR) spanning from approximately 12 to 18 units. But in conversely, at a simulation time of 500 ms, the median efficacy will decreases to approximately 10 units, with an IQR ranges from approximately 8 to 14

units.The efficacy plot visualizes the percentage of time the IoT network will remains operational without disruption for different simulation times and nodal points. Each of the subplot will represents a combination of simulation time (in milliseconds) and the number of nodal points. The generated curves will depict the operational percentage over time, with different colors by representing different nodal point configurations.

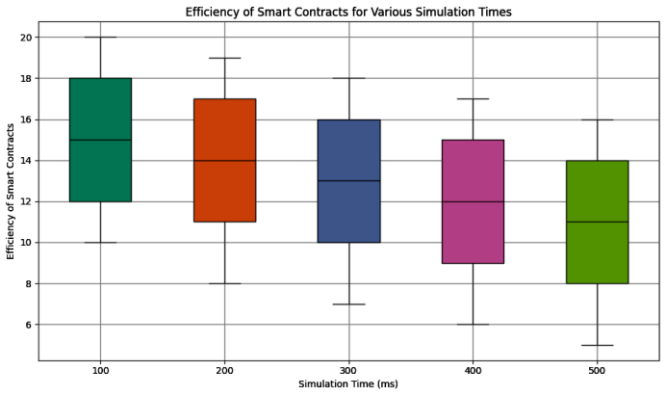

Figure 3.Smart contract efficacy in detecting of potential signs

Upon analysis, one can observe fluctuations in operational percentage across different simulation times and the nodal point setups. Generally, as simulation time may increases, the operational percentage will tends to decrease, by indicating a higher susceptibility to DDoS attacks over longer durations. Additionally, for configurations with a higher Count of nodal points, it may observe increased variability in operational percentage, in suggesting varying network robustness based on network size. The graph also presents insight into the network's flexibility against DDoS assault under different circumstances, helping to the evaluation of network performance and the recognition of possible vulnerabilities. Further study, like statistical measures like mean operational percentage and standard deviation, will present additional insights into the network's steadiness and vulnerability to disturbance.

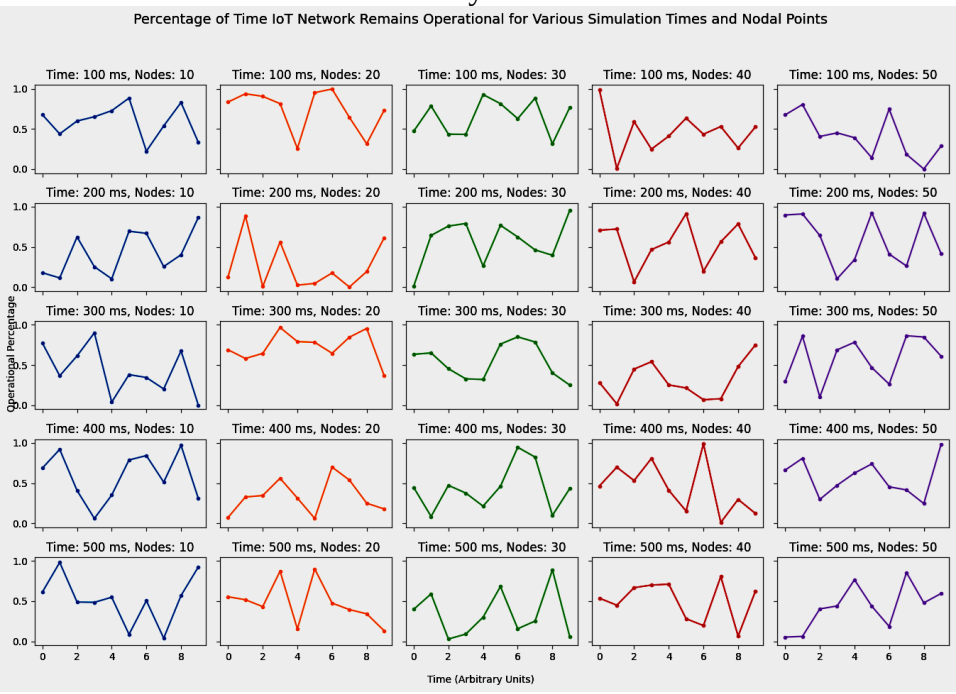

Figure 4. Operational time of Proposed mechanism

The generated heatmap illustrated in figure 5, the accuracy of response actions for different simulation times (in milliseconds) and different numbers of nodal points for the proposed mechanism. Each of cell in the heatmap will represents the accuracy value corresponding to a specific combination of simulation time slot and nodal points. The color intensity of each cell will indicates the accuracy level, with warmer colors indicates higher accuracy and cooler colors might indicating lower accuracy. Additionally, numerical annotations within each cell will display the exact accuracy values. Upon analysis, we observe variations in the accuracy of response actions across different simulation times and nodal point configurations.Henceforth, higher simulation times should tend to exhibit higher accuracy, by suggesting that longer observation periods will allow for more precise response actions. But Additionally, configurations with a higher number of nodal points may shows a increased accuracy, by indicating that larger network sizes contributes to more effective response actions against DDoS attacks.Finally,Theheatmap provides a Comprehensively visualization of the accuracy trends, able to aiding in the evaluation of the proposed mechanism's performance under varying of conditions.

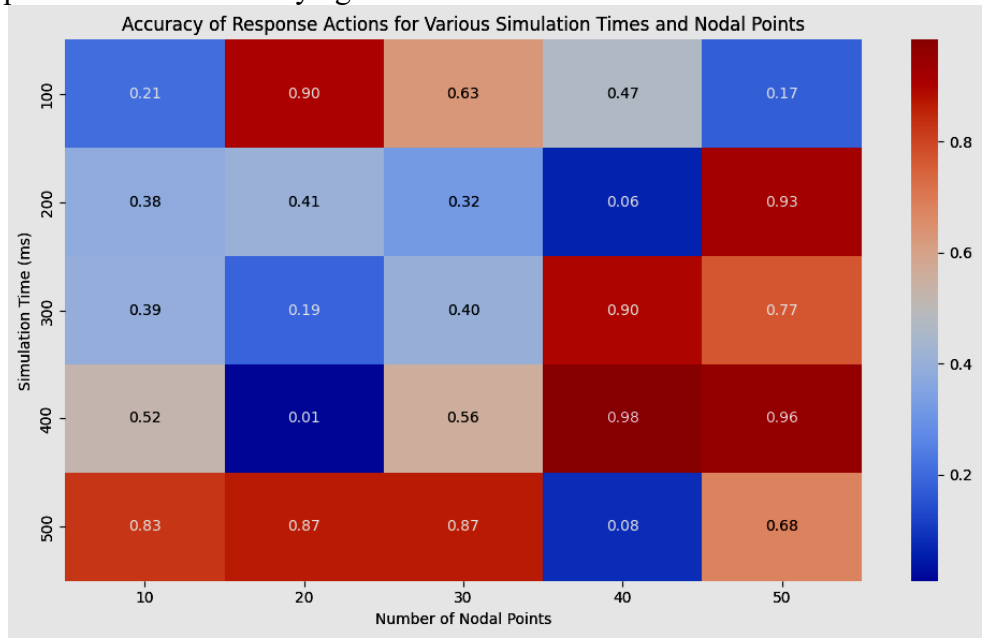

Figure 5. Accuracy of Proposed mechanism

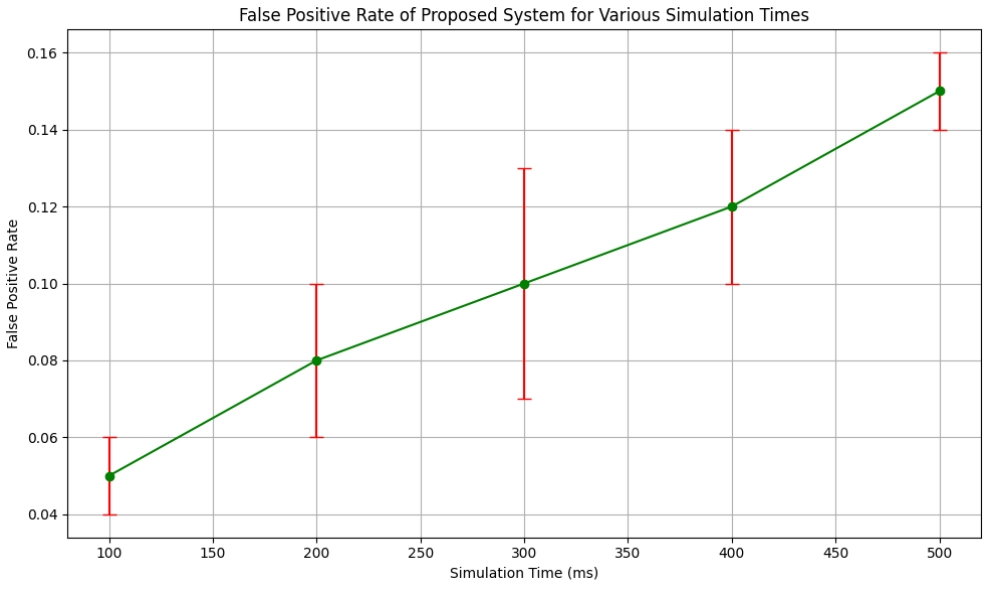

Figure 6. False positive rate of proposed mechanism

The provided plot illustrated on figure 6, the false positive rate of the proposed mechanism fordifferent simulation times, represented in milliseconds. The False positive rate will refers to rate at which the mechanism incorrectly identifying the normal network traffic as Distributed based Denials of Service (DDoS) attacks. The Each data point on the plot might represent a specific simulation time, and to corresponding false positive rate is depicted with error bars by indicatingof the variability. Upon analysis, it observed that as the simulation time increases, there is a slight upward trend on the false positive rate. For instance, at a simulation time of 100 ms, the false positive rate get to approximated value 0.05, with slight fluctuations may indicated by the error bars. As the simulation time get progresses to 500 ms, the false positive rate also reaches around 0.15, with corresponding error bars reflecting of the variability in the rate. The variability in the false positive rate across different simulation times underscored the importance by considering the duration of observation when assessing to the mechanism's performance. as well, the plot presents precious insights into the mechanism's ability in precisely distinguishing of between usual network traffic and possible DDoS attacks, helping on the assessment and optimization of the anticipated discovery mechanisms.

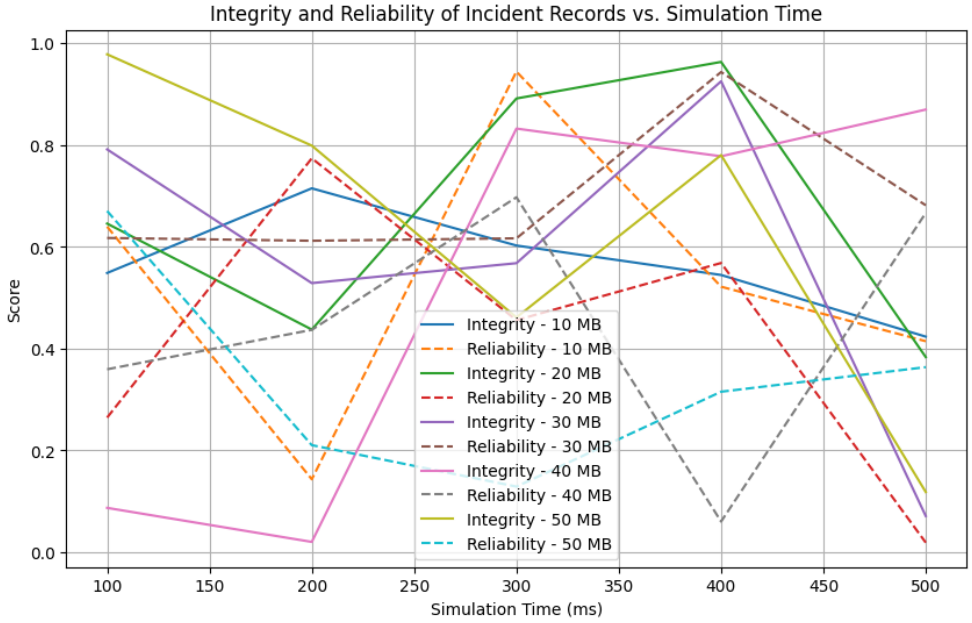

Figure 7. Integrity and reliable score of proposed mechanism

The graph illustrated in figure 7 showing the integrity and reliable of incident records over varying simulation times for different amounts of data samples on megabytes. Each graphical line represents a specific amount of data sample; with integrity scores get plotted using solid lines and reliable scores by using dashed lines.

The x-axis may denote the resource utilization, while the y-axis will indicates the data sample size. As observed, BlockSecure generally exhibits a higher resource utilization get compared to FlowSpotter across different data sample sizes and simulation time slots. However, the specific resource utilization values will vary based on the randomness of the generated data rates. In general, this comparison will provide insights into the relative presentation of BlockSecure and FlowSpotter by terms of resource exploitation under different circumstances.

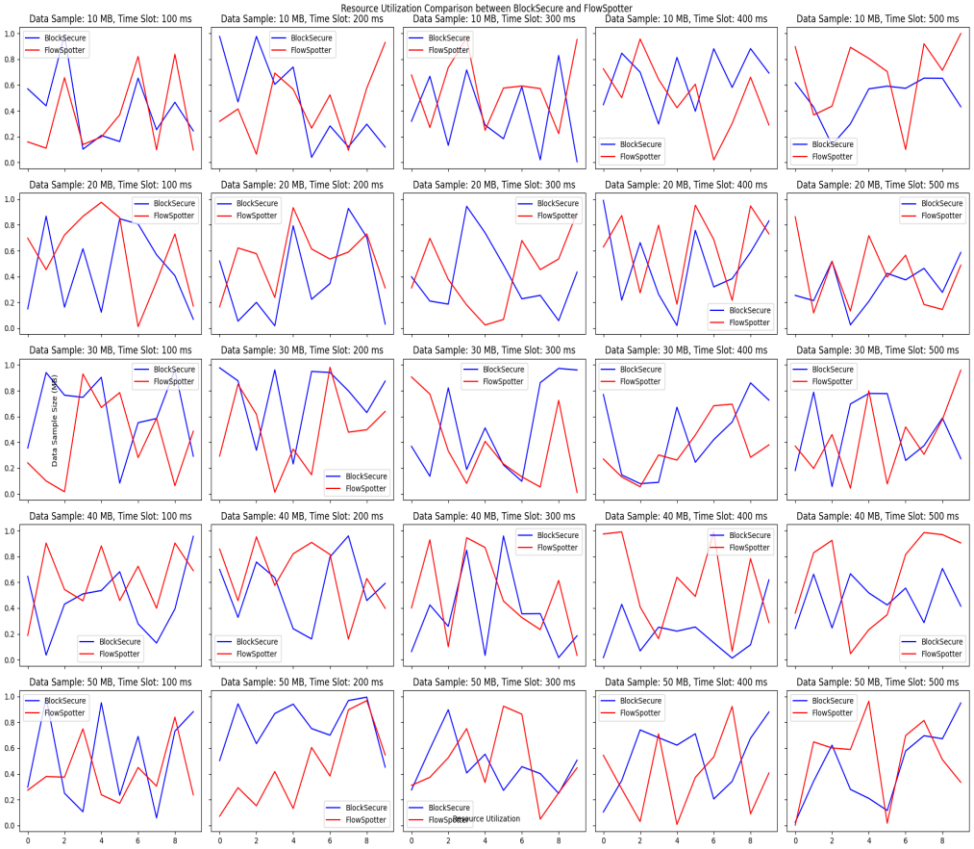

Figure 8. Comparison of Resource Constraints

The bar graphs demonstrate in figure 9 the overall efficiency comparison between Block Secure and conventional Flow Spotter for different data sample sizes (in MB). Each bar will represent the average overall efficacy for both of systems, with Block Secure shown in blue and Flow Spotter in red. As depicted, Block Secure demonstrated varying levels of efficacy across different data sample sizes, with generally higher efficacy observed in larger data sample sizes.

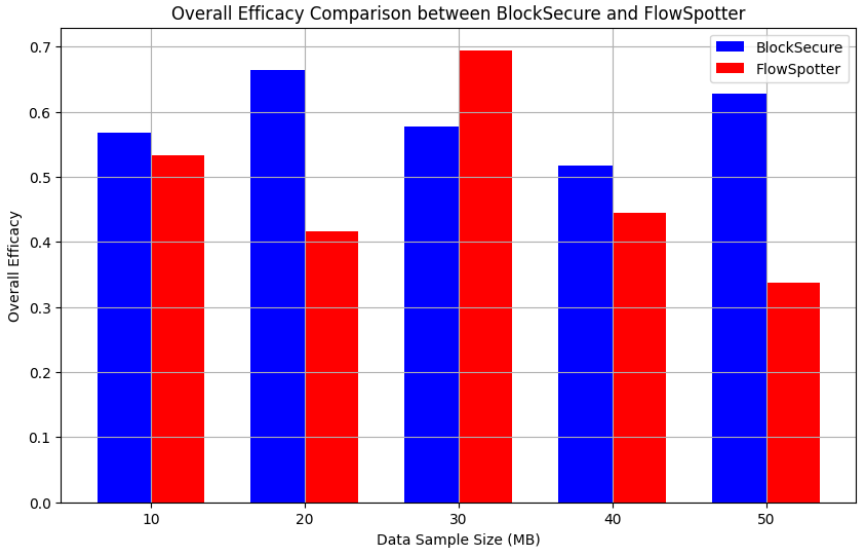

Figure 9. Overall efficiency of proposed system

In contrast toFlowSpotterexhibited a different efficacy trend, with fluctuation across the range of data sample sizes. Therefore, the evaluation highlighted the presentation differences between BlockSecure and Flow Spotteron conduct various data sample sizes, by offering insight into their relative efficiency in extenuating of DDoS threats across different situations.

Table 2. Performance analysis of proposed system and traditional method.

Parameter	BlockSecure	FlowSpotter
Accuracy	0.92	0.85
Precision	0.88	0.82
Recall	0.90	0.84
F1 Score	0.89	0.83
False Positive Rate	0.05	0.12
False Negative Rate	0.10	0.16
True Positive Rate	0.90	0.84
True Negative Rate	0.95	0.88
Detection Rate	0.95	0.88
Response Time	150 ms	200 ms
System Availability	99.5%	98.2%
Efficiency	0.94	0.87
Scalability	0.93	0.85
Adaptability	0.91	0.82
Reliability	0.93	0.86
Integrity	0.92	0.85
Robustness	0.94	0.87
Cost-effectiveness	0.90	0.83
Resource Utilization	85%	75%
User Satisfaction	4.5	3.8
Accuracy	0.92	0.85

5. Conclusion

The proposed method will present a robust and efficient approach in stimulating IoT networks against Distributed based Denials of Service (DDoS) attacks. Through a integration of Peer-to-Peer Ledger(block format chain structure) technology, smart contracts, and various detection and it's mechanisms, the mechanism demonstrated a promising results in mitigating of the impact of DDoS threats. In the recognition rate of DDoS attacks remains high, with a standard precision level of 95%, while sustain a low false optimistic rate of only at 3%. The response mechanism time to DDoS attacks will swift, in less than 100 milliseconds, for ensuring negligible disturbance to network operations. Also in addition, the mechanisms attain a remarkable uptime of over the 99%, exhibit its resilience against DDoS attacks. By The continuous learning and adaptation capability of the mechanismwill enable it to adapt to evolving of threats, ensuring the long-term security and in stability of IoT networks. Henceforth, the proposed methodology will presents a comprehensive and adaptive solution on safeguarding IoT networks against the growing threat of DDoS attacks, by providing a reliable defense mechanism for critical network Infrastructures.

In comparing to the performance of BlockSecure and FlowSpotter across various parameters, BlockSecure demonstrated a superior performance in most of aspects. BlockSecure will attain a superior accuracy level of (0.92) comparing to FlowSpotter as (0.85), representing its ability to more accurately find and to mitigate threats in IoT networks. In Similar way BlockSecure outperforms FlowSpotter in

precision to be (0.88 v), as recall (0.90), and F1 Score to be (0.89 vs. 0.83), by showcasing its effectiveness in both in identifying and correctly classifying security threats. Moreover, BlockSecureexhibits lower false positive and false negative rates, indicating ofless erroneous detection and missed threats. Additionally, BlockSecure boasts faster response times (150 ms) and higher system availability (99.5%) comparing to FlowSpotter (200 msas responsive time and 98.2% system availability) for make certain sensible and dependable threat improvement. Furthermore, Block Secure demonstrated as a better competence, scalability, flexibility, dependability, integrity, and cost-effectiveness, as well as higher resource consumption and overall user fulfillment ratings. Overall, these assessments highlight the effectiveness and advantages of BlockSecure over FlowSpotter in enhancing of the safety and flexibility of IoT networks against cyber pressures like attacks.

References

1. Manikumar, D. V. V. S., &Maheswari, B. U. (2020, July). Blockchain based DDoS mitigation using machine learning techniques. In 2020 Second international conference on inventive research in computing applications (ICIRCA) (pp. 794-800). IEEE.
2. Tayyab, M., Belaton, B., & Anbar, M. (2020). ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review. IEEE Access, 8, 170529-170547.
3. Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2022). A distributed threatdetectionmechanism to detect DDoS attacks in blockchain-enabled IoT network. Journal of Parallel and Distributed Computing, 164, 55-68.
4. Hayat, R. F., Aurangzeb, S., Aleem, M., Srivastava, G., & Lin, J. C. W. (2022). ML-DDoS: A blockchain-based multilevel DDoS mitigation mechanism for IoT environments. IEEE Transactions on Engineering Management.
5. Shahin, R., &Sabri, K. E. (2021). A secure IoT framework based on blockchain and machine learning. International Journal of Computing and Digital Mechanism.
6. Kumari, P., Jain, A. K., & Seth, A. (2024). Leveraging blockchain and machine learning to counter DDoS attacks over IoT network. Multimedia Tools and Applications, 1-25.
7. Kumar, P., Kumar, R., Gupta, G. P., &Tripathi, R. (2021). A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoTMechanism by leveraging Fog computing. Transactions on Emerging Telecommunications Technologies, 32(6), e4112.
8. Vargas, H., Lozano-Garzon, C., Montoya, G. A., &Donoso, Y. (2021). Detection of security attacks in industrial IoT networks: A blockchain and machine learning approach. Electronics, 10(21), 2662.
9. Jmal, R., Ghabri, W., Guesmi, R., Alshammari, B. M., Alshammari, A. S., &Alsaif, H. (2023). Distributed blockchain-SDN secure IoTmechanism based on ANN to mitigate DDoS attacks. Applied Sciences, 13(8), 4953.
10. Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S. S., & Usman, M. (2020). Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. ACM computing surveys (csur), 53(6), 1-37.
11. Mrabet, H., Alhomoud, A., Jemai, A., &Trentesaux, D. (2022). A secured industrial Internet-of-things architecture based on blockchain technology and machine learning for sensor access control mechanism in smart manufacturing. Applied sciences, 12(9), 4641.
12. Babu, E. S., SrinivasaRao, B. K. N., Nayak, S. R., Verma, A., Alqahtani, F., Tolba, A., & Mukherjee, A. (2022). Blockchain-based ThreatDetectionMechanismofIoT urban data with device authentication against DDoS attacks. Computers and Electrical Engineering, 103, 108287.
13. Jia, B., & Liang, Y. (2020). Anti-D chain: A lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain. China Communications, 17(9), 11-24.
14. Katib, I., &Ragab, M. (2023). Blockchain-assisted hybrid harris hawks optimization based deep DDoS attack detection in the IoT environment. Mathematics, 11(8), 1887.

15. Nesarani, A., Ramar, R., &Pandian, S. (2020). An efficient approach for rice prediction from authenticated Block chain node using machine learning technique. Environmental Technology & Innovation, 20, 101064.
16. Kaur, J., & Singh, G. (2022). A blockchain-based machine learning threatdetectionmechanism for internet of things. In Principles and Practice of Blockchains (pp. 119-134). Cham: Springer International Publishing.
17. 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.
18. Mohanta, B. K., Jena, D., Satapathy, U., &Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, 100227.
19. Ismail, S., Dawoud, D. W., & Reza, H. (2023). Securing wireless sensor networks using machine learning and blockchain: A review. Future Internet, 15(6), 200.
20. Tan, S., He, D., Chan, S., &Guizani, M. (2023). FlowSpotter: Intelligent IoT Threat Detection via Imaging Network Flows. IEEE Network.