National College of Ireland

MSc Research Project
Programme Name

Forename Asad Ali Khan
Student ID: x21168342@student.ncirl.ie

School of Computing
National College of Ireland

Supervisor: Michael Pantridge

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……Asad Ali Khan ……

Student ID: …… x21168342@student.ncirl.ie……..……

Programme: MSc- Cybersecurity Evening **Year:** 2022-24…..

Module: ……Final Thesis…….……

Supervisor: ……Michael Pantridge…….……

Submission Due Date: ……28th April 2024…….……

Project Title: ……..……

Word Count: ……7642…… **Page Count**……23 with references ……..……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……

Date: ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

DDoS Prevention in Home IoT Devices Using Hyperledger Blockchain.

Asad Ali Khan
Student ID: x21168342@student.ncirl.ie

Abstract

IoT devices have significantly altered our daily lives, experiencing rapid growth in recent years. However, this proliferation has also brought about considerable security challenges, often exploited by malicious actors. In response, this study seeks to investigate the potential for mitigating Distributed Denial of Service (DDoS) attacks on IoT devices through the application of innovative technologies like blockchain and fog computing. Through a comprehensive review of existing literature, the research aims to assess the feasibility of simulating DDoS attacks in controlled laboratory environments and subsequently thwarting them using Hyperledger blockchain technology. It is assumed that foundational security measures such as firewalls, intrusion detection systems, and updated operating systems are already in place. Furthermore, this study aims to identify avenues for future research, particularly exploring the integration of decentralized private blockchain technology at the level of low-performance IoT devices, leveraging various available platforms for simulating such attacks.

Keywords: IoT, Hyperledger Framework, Blockchain, Fog Nodes, Home IoT

1 Introduction

Research background.

The proliferation of Internet of Things (IoT) devices has ushered in a new era of connectivity and convenience, revolutionizing various industries and enhancing everyday life. However, with this widespread adoption comes a myriad of security challenges, chief among them being the vulnerability of IoT devices to Distributed Denial of Service (DDoS) attacks. DDoS attacks pose a significant threat to the integrity, availability, and security of IoT networks, potentially disrupting critical services and compromising sensitive data.

Addressing the pressing need for robust security measures to safeguard IoT devices against DDoS attacks, this research focuses to develop and implement effective prevention strategies within the Hyperledger Fabric (HLF) framework. HLF, a leading blockchain platform renowned for its scalability, security, and flexibility, presents a promising avenue for enhancing the resilience of IoT networks and fortifying them against malicious attacks.

Drawing upon insights from existing literature on IoT security, blockchain integration, network security, and DDoS mitigation techniques, this research seeks to establish a comprehensive framework for DDoS attack prevention tailored to the unique challenges and requirements of IoT environments. Central to this framework is the collection and analysis of device health

metrics, including CPU utilization, memory usage, and network bandwidth, as key indicators of potential DDoS attack activity.

By leveraging the capabilities of HLF and integrating device health monitoring mechanisms into the blockchain network, this research aims to enable real-time detection, analysis, and mitigation of DDoS attacks targeting IoT devices. Exploring different experimentation, options then evaluation, and validation, the effectiveness and feasibility of the proposed solution will be assessed, paving the way for enhanced security and resilience in IoT ecosystems.

In summary, this research endeavors to contribute to the advancement of IoT security by leveraging blockchain technology and comparing existing and new methods to carry out simulations of DDoS attacks and their prevention by HLF BC. By addressing this critical challenge, the research aims to bolster the confidence of researchers in testing of IoT devices for security in new ways. This will allow for IoT device adoption and foster a safer and more secure digital future.

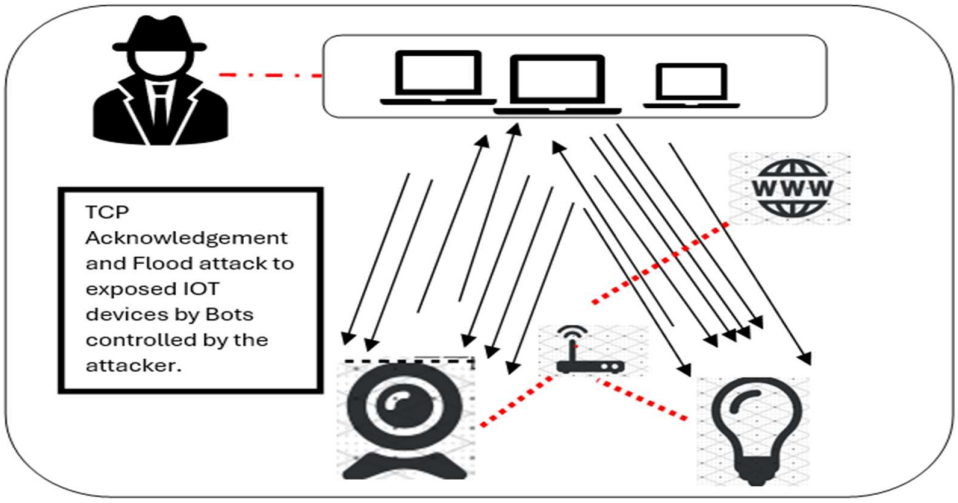


Figure 1. Representation of DDoS Sync Acknoldege Flood attack when victim IoT devices are overwhelmed by flood of TCP packets coming towards them.

Assumptions: Due to limitations with the scope of our research we will assume the following. The network is protected by a firewall, intrusion detection system, firewall, segmentation, if possible, in the home environment where IoT's are connected to secondary Wi-Fi, etc. The software is up to date, software code used is based on best coding practices with good user practices of setting up strong passwords and access controls in their environment. I also assume that the devices I use should be low in processing power with limited bandwidth. In experiments, I was only able to leverage Linux and Ubuntu boxes. Abbreviations used throughout the report.

Block Chain	BC	Prb	Private Blockchain
Internet of Things	IoT	MSP	Membership service provider
Hyper Ledger Framework	HLF	HL	Hyper Ledger
Denial of Service	DoS	db	Database
Distributed Denial of Service	DDoS	VB	Virtual Box
Chain code (Smart contract)	CC	Tx /Txs	Transaction/Transactions

Table 1. Abbreviations

Internet of Things – IoT

The Internet of Things (IoT) encompasses devices, regardless of their size, equipped with components enabling internet connectivity. These devices facilitate the bidirectional transmission of data in an intelligent manner, aiding in informed decision-making processes. Examples range from temperature sensors in residential settings to various household appliances, security systems like CCTV cameras, and more. (Jay, 2020)Smart sensors generate data that can be leveraged by applications to derive meaningful insights and drive decision-making. The proliferation of IoT devices has been remarkable, extending beyond industrial settings to encompass smart homes and cities, where millions of interconnected devices contribute to a networked environment.

DDoS Attacks:

Distributed Denial of Service (DDoS) attacks, orchestrated by malicious hackers, aim to disrupt or completely deny access to services. This form of cyber assault targets a wide array of devices, including IoT devices such as smart bulbs and cameras commonly found in households. The proliferation of IoT devices is evident, with approximately 1.6 billion smart home devices shipped in 2023 (Ziv Chang, n.d.).

The ramifications of DDoS attacks extend beyond mere disruption, encompassing theft, sabotage, the incorporation of devices into crypto mining botnets, or their enlistment in botnets to perpetrate further DDoS attacks on unsuspecting victims. These attacks rely on inundating the targeted service or victim with an overwhelming volume of requests, depleting their resources or bandwidth (Chaganti et al., 2022). Such traffic is typically transmitted via protocols like TCP, UDP, HTTP, and ICMP, a technique commonly referred to as flooding. Figure1. – shows sync flood attack on IoT devices.

Despite ongoing efforts by researchers and organizations to develop detection mechanisms, DDoS attacks persist, fuelled by the rapid evolution of technology. Particularly concerning is the susceptibility of IoT devices, often connected to the internet through insecure third-party gateways. Consequently, even if a user's internet connection is fortified with router firewalls or antivirus systems, malicious actors can exploit vulnerabilities in these devices to launch attacks.(amazon, n.d.)

Traditionally, organizations have leaned on software-defined network-based approaches to mitigate the impact of DDoS attacks. (Friha et al., 2020)These strategies involve techniques such as packet dropping, port blocking, redirection, and the alteration of targeted IP addresses. However, the dynamic nature of DDoS attacks underscores the need for continual innovation in defense mechanisms to safeguard against evolving threats.

These attacks have caused companies and individuals money, and loss of data and services. Mirai botnet attacks was DDoS attacks on cameras where infected cameras were then taken over as bots to perform attacks on other cameras. (Ahmed et al., 2019). Similarly, tech giants Amazon and Google have had their share of the attacks between 2020-2023 with the largest

ever recorded DDoS attacks sending 46 million HTTP requests per second (rps) to 155 AND 398 million rps respectively. (Kobialka, 2023). They were able to keep their services up as they have invested millions in their robust cloud products.

For home users this is not the case, IoT devices used in homes are from various companies and challenges are there to have integrity and confidentiality of data. Implementing blockchain is difficult due low processing power and storage capacity of these IoT smart devices. Hence Blockchain technology comes into mind which can use data generated by the IoT devices in the form of transactions (Tx) to store it in a database called a ledger. (Almuqren et al., 2023)

Blockchain: BC is a ledger technology that is immutable and usually decentralized. The technology has been around for years and its use in IoT is increasing exponentially. (Zheng et al., 2017). It provides integrity to data transactions and helps with security, and proof of work (PoW) for any transactions that occur at the device level, data level, etc. It came to existence in 2009 as the background technology of Bitcoin the famous cryptocurrency.

The ledger maintains the record of blocks (Nakamoto, n.d.) y. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Once recorded, the data in any given block cannot be altered without altering all subsequent blocks, which requires the consensus of the network participants. The distributed ledger contains a block of transactions and the security hash of the new and previous blocks. The ledger is verified and maintained by nodes in the network of peers. Each transaction is digitally signed with cryptographic keys which cannot be changed without a consensus mechanism in the network.(Al Hwaitat et al., 2023) Blockchain can be deployed centralized, decentralized, private, or publicly depending on the security requirements. Private blockchains allow for more security as their transactions are validated by preapproved internal validators in the decentralized network. (Uddin et al., 2021)

DDOS Attack types

- Volumetric Attacks: These flood the target with massive amounts of traffic, overwhelming its bandwidth capacity. Examples include UDP floods and ICMP floods.
- Protocol Attacks: Exploit weaknesses in network protocols to consume resources on the target system. Examples include SYN floods, which flood the target with TCP connection requests, and ICMP floods, which exploit the ICMP protocol.
- Application Layer Attacks: Target vulnerabilities in specific applications or services running on the target system. Examples include HTTP floods, which overload web servers with HTTP requests, and DNS amplification attacks, which exploit DNS servers to amplify attack traffic.
- Slowloris Attack: Exploits the limited number of connections a server can handle by sending partial HTTP requests, keeping connections open until the server's resources are exhausted.

1. UDP Flood: Sends a large number of UDP packets to a target, overwhelming its ability to process and respond to legitimate requests.(amazon, n.d.; “DDoS threat report for 2023 Q1,” 2023)

For our experiment, I would use sync flood or udp attack whichever would be easy to implement.

Different Types of Blockchain

Public Blockchain: A public blockchain is open to anyone and allows anyone to participate, read, or write data to the blockchain. Examples include Ethereum, Bitcoin, and Litecoin.

Private Blockchain: A private blockchain is controlled by a single organization and is typically used for internal purposes. Participants are usually known entities, and access to the blockchain is restricted. Hyperledger Fabric is an example of a permission blockchain platform.

Hyper Ledger Framework – HLF

Everything in HLF is based on docker containers.

Docker Containers: Docker containers are used for isolated activities throughout the HLF network. Dockers help application packages that are created in isolation to run independently, what this means is that applications can run on multiple platforms without many dependencies in a standard format. The application service runs independently with its dependencies. The software is packaged in a way that it runs in multiple applications.

Chian Code: is an application code that allows us to interact with the HLF ledger. It runs in the chain code docker.

Consensus Algorithm: This means a set of rules that allow us to interact with blockchain code under certain rules. In the context of IoT devices in small setups or at home, permissionless blockchains allow anonymous participation with consensus mechanisms like "proof of work" (PoW). (Androulaki et al., 2018)Permissioned blockchains, such as Hyperledger Fabric (HLF), involve known participants and foster trust through identity verification. Unlike permissionless blockchains, permissioned ones use traditional consensus protocols like crash fault tolerance (CFT) or byzantine fault tolerance (BFT), avoiding the need for costly mining. Additionally, in permissioned environments like HLF, the risk of malicious activity is reduced due to known participants, transparent actions recorded on the blockchain, and clear governance guidelines.

Device Enrollment: The devices are enrolled to the HLF ledger. This can be done by a program written in Golang or Java using PasS (Platform as a service) such as Nodejs or Sublime text IDE.

Peer: A peer is also called a node on the network. In the case of HLF, the peers are the docker containers. The node device for our network is the fog device that hosts HLF dockers to manage transactions with the two IoT devices in our examples. The peer usually maintains a copy of the ledger and smart contracts, validates transactions, and participates in the consensus process. A peer has 2 roles, usually a committee member and an endorser. By default, each peer is a committer. Endorser is used to manage the Tx committed by the update from the IoT devices.(“Hyperledger Fabric Glossary — fabricdocs 1.0 documentation,” n.d.)

Ledger: Each transaction is maintained as an immutable block in the ledger. The database is used to keep a record of these transactions. Everything is a key and value pair in the database. For Example, the Size is 30 length is 20, and so on.

Channels: Allows the devices to communicate via transactions that are visible to the participating stakeholders on the network. The consensus agreements take place in the channels by the members of the channels. Other members of the channel are not allowed to access or see the transactions happening inside the channel. This is a crucial part of helping with the prevention of DDoS attacks by a non-member actor, program, device, or user.
The chain code is deployed in the channel and can interact with other chain code channels based on Access control lists (ACL)

Membership Server Provider (MSP): The authentication and authorization for the devices (Orderer's, peers, clients) inside the channel is managed by MSP which can be built in Fabric Certificate authority or External Certificate authority. In our case, we will use the FCA which is the internal Fabric certificate authority.
The authorization is to allow or deny the Orderer, channels, and endorsers on rules of engagement in the chain code and the ledger itself.
Fabric CA and SDKs: The certificates are provided by the MSP service for long-term and short-term transactions performed on the network. Libraries and tools for building applications that interact with a Hyperledger Fabric blockchain network.
Crypto Service Provider (CSP). Helps with the provision of private keys. X.509
Application: An application is developed to execute smart contracts. These transaction blocks constitute the blockchain within the smart contract, referred to as 'chain code' (CC) in the case of Hyperledger Fabric. The smart contract delineates rules for IoT devices to establish contracts with each other and the blockchain network. Subsequently, this information is recorded in the database as a blockchain transaction. In our scenario, we will utilize a basic application to fulfill the function of authenticating and authorizing IoT devices.

2 Related Work

(Mohapatra et al., 2022) have worked on developing a Fog-based network with blockchain technology to secure the network for IoT devices. They use two software agents, one to manage the network itself and the other software element to manage the blockchain transactions. They use AES and SHA256 for the hashing of blockchain transactions among the network of devices. They use an algorithm that gives them the best result in the performance of the network which is affected by the size of AES blocks. They don't address if the security attacks will be DDoS based and how fog networks and blockchain will help with its prevention. This provides me the opportunity to address my research question ich on how DDoS attacks can be prevented on Blockchain-enabled Fog Networks or Gateways.

(de Assis et al., 2020) have used CNN (Convolutional neural network) to detect DDoS attacks in IoT networks and have tried to explain its efficiency in restoring the network after the attack. Their research suggests areas to expand on simulated tests against different types of DDoS attacks and the impacts of using deep learning methods on SDN (Software-defined Networks). Researchers have looked at DDoS mitigation solutions for IoT based on BC.(Saha et al., 2023) The study analyzed IoT device architecture, discussed security challenges, and explored how

Blockchain can enhance security. They conclude on improving defense strategies against DDoS by highlighting gaps in IoT device deployment at the layer level in the Fog Network.

Work carried out by - (Baucas et al., 2022) present a security platform tailored for fog-based IoT networks, utilizing public-key encryption to safeguard endpoints and permissioned blockchains for traceable encryption. The researchers employ a wireless server-client architecture that protects the network against endpoint attacks using trusted authentication via BC and cryptographic techniques. They test the platform (Fred Donovan, 2021) STRIDE (Spoofing identity, tampering with data, Repudiation threats, Information disclosure, Denial of service, and Elevation of privilege) model that mitigates various threats while concerns emerge on DDoS attacks via clients on the network that need to be addressed. The permission-based blockchains and public-key encryption provide a promising foundation for securing the IoT network. I will investigate addressing the area of DDoS threat by Hyper Ledger Framework.

(Lee et al., 2020)talks about securing smart homes using blockchain-protected gateways. These gateways provide a decentralized environment for IoT devices to be secured. The data is stored at these gateways using Ethereum BC. The researchers evaluate the solution in light of security response times and accuracy, they leave room to address scalability issues with several IoT devices on the home network that can be addressed by a central BC node that can be a Fog node or Gateway. This device should provide enough processing power to complement BC's need for data processing as the transactions arise in the system.

A lot of research has been done in the IoT space which is continuously evolving, (Shahbazi et al., 2021) talks about securing home IoT devices using Deep Reinforcement learning (DRL) and BC Framework to enhance security and any possible attacks. While it does not mention DDoS attacks, the research highlights using private Ethereum BC with DRL provides security in terms of authentication, confidentiality, and integrity outperforming Artificial Neural Networks. What was interesting to see is that they point out in existing studies private Ethereum BC does not provide Integrity and scalability. (Xu et al., 2018) talks about a Decentralized IoT smart home system on Ethereum where an application Blynk stores sensor data in smart contracts on
Ethereum BC, concludes on future implementations BC which will have minimal transaction costs also called a gas fee.
(Lee et al., 2020) talks about BC-based smart gateway in a network architecture that protects data for heterogeneous IoT devices, the researchers conclude with using Fog Computing as the future work to address more processing needs for BC. (Jamader et al., 2019) talks about the BC architecture to stop DDoS attacks without mentioning what platform was used to prevent the attack using which type of BC technology. They did a fair amount of work in setting up real IoT devices in their experiments.

As IoT devices increase in numbers around the world and smart homes, their vulnerability needs to be addressed. The DDoS attacks are becoming sophisticated in nature, and developing strategies to mitigate and stop these attacks becomes critical as discussed by (Chaganti et al., 2022). They discuss deploying safe SDN architecture with the implementation of blockchain

to prevent DDoS attacks. The discussion emphasizes the importance of introducing a consensus mechanism using specialized algorithms that ensures proof of work and proof of stake through blockchain technology. Different types of DDoS attacks are discussed in terms of the source and proximity of the attacks which includes Near domain and victim attacks at the network level. They talk about different detection methods that are being used without too much detail on what the future directions to implement detection for DDoS in IoT devices.,

The paper concludes by describing blockchain as a great mitigation strategy that prevents malicious activity in an IoT environment using smart contracts and leaves room for exploring different types of prevention strategies using the Ethereum 2.0 blockchain. (Ibrahim et al., 2022) uses Ethereum BC using a command line emulator to make transactions in BC without incurring the costs of gas network charges. It was done using Eth as public BC and there was room to address this using private BC. The experiments evaluated CPU association, time per request, authentication time, and data message time for message transmission through the Eth network.

(Shah et al., 2022)The proliferation of Internet of Things (IoT) devices raises concerns about Distributed Denial of Service (DDoS) attacks. Exploiting IoT vulnerabilities, attackers can launch large-scale DDoS attacks, posing significant security threats. Blockchain emerges as a promising solution to mitigate these risks. The study examines various Blockchain-based approaches to counter DDoS attacks in IoT, categorizing solutions into four types. The focus is on Ethereum which uses gas limits as a protection mechanism, if no fee is paid by the attacker the transaction doesn't proceed. While focusing on Network layer security, this work does not explain which alternate BC can be used like HLF to save on gas costs especially if it's related to home IoT users experiencing the attack.

This article (Zheng et al., 2022) addresses the pressing need for blockchain simulators tailored to IoT environments. It reviews 18 simulators, assessing their suitability, advantages, and limitations. Notable options include Hyperledger Fabric, Ifogsim, Blocksim, NS3, and Ethereum/Ganache, each with distinct strengths. Recommendations are provided for selecting simulators based on specific needs. The study acknowledges limitations, such as the lack of detailed parameter discussions and consensus algorithm support. They discuss various simulators related to Hyperledger Fabric, such as Sawtooth, Fabric, and Iroha, along with their respective limitations. However, it's worth noting that these platforms are HLF frameworks rather than simulators.

HLF does not specifically use Proof of Work (PoW) or Proof of stake (PoS) as its consensus mechanism but it does allow flexibility to use custom pluggable consensus algorithms to your requirements. This did compel me to choose Hyperledger Fabric due to its private, permission-based structure, which aligns well with our IoT device network requirements. While their research provided insight into different simulators, it lacked practical guidance on initiating research with them. Ifogsim Simulator was used in a study to understand how internal DoS attacks can be prevented using Fog computing (Ullah et al., 2021) results of the experiment were compared by other cloud simulators, the study lacks future directing or the use of BC to be of any benefit.

3 Research Methodology

This study aims to explore the potential of Blockchain (BC) technology in mitigating Distributed Denial of Service (DDoS) attacks on home IoT devices and smaller environments, as larger corporations typically have resources to safeguard against such threats (Kobialka, 2023). Utilizing a methodological approach that involves scouring various research databases such as IEEE, ResearchGate, Springer, Science Direct, and Google Scholar, alongside scientific journals, we aim to synthesize existing research in this domain. The prevailing trend indicates a surge in research activity, mirroring the expanding use of IoT devices in offices, homes, smart cities, and utilities, necessitating enhanced security measures (Touqeer et al., 2021). Building upon a thorough literature review, our approach involves creating simulated environments to conduct DDoS attacks securely, followed by implementing BC technology in a private setting to prevent or mitigate these attacks. Given the constraints of smaller setups like home environments, where IoT devices and other peripherals often possess limited processing power, selecting the appropriate type of BC becomes pivotal, necessitating sufficient processing power at both device and network levels.

Given the inherently hazardous nature of DDoS attacks, ensuring safety within the testing environment is paramount. The low-risk solution to minimize risk with DDoS is the way forward where a simulated environment is needed to perform DDoS attacks. Experimenting with various simulations such as Netsim, Simblock, IfogSim, and Ns3, I discovered that Ns3 emerged as the most promising option.(Zheng et al., 2022) . I started with IfogSim to incorporate several IoT devices into the network and simulate a DDoS attack. I also used a Linux-based simulator called Ns3, a C++-based simulator renowned for its robust community and informational resources. (Saket, 2020).

The methodology aims to simulate HLF peers and Orderer within the Ns3 network, emphasizing the replication of IoT device behavior and the utilization of consensus mechanisms.

In my exploration with Ifogsim, I would use Eclipse as the development IDE for installing the simulator. Building on insights from prior research by (Sundareswaran and Sasirekha, 2022) I also determined that Ns3 offered greater flexibility, enabling not only DDoS attack simulation but also the implementation of blockchain (BC) protection measures. The steps would be to try all possible simulators to achieve results not only in setting up the BC but also in mitigating DDoS attacks.

The next step in the methodology involves simulating BC technology like Ethereum and HLF for comparison in testing how these respond to peers, transactions, IoT setup, and the effects of DDoS attacks. The process will be to set up nodes/peers in the Ns3 network, with a focus on replicating IoT device behavior and utilizing consensus mechanisms. This approach ensures that the simulation accurately reflects real-world scenarios, enhancing the validity of the research findings.

Upon configuring the network, I realized that Ns3 did not directly integrate with any blockchain technology. Instead, one needed to develop blockchain functionality in the form of a Docker container to simulate the operations of a smart contract-based blockchain. Given the complexity involved, I opted to explore working with Linux-based virtual machines within a VirtualBox environment. This helped me to aim for a more controlled setting with enhanced options for conducting DDoS testing in a secure and closed network of virtual machines.

Virtual Box will be set to emulate IoT devices network, Kali, Ubuntu, and lightweight Linux distribution would be used to get to real-life situations. Virtual box machines will be set up with the option of internal and external networks. An internal network will be set up to prevent any DDoS attack from going outside the network. This can be set up easily in the Virtual box provided by Oracle.("Oracle VM VirtualBox," n.d.) It allows for the configuration of different types of operating systems and allows for the ability to save your work in terms of snapshots. VMware is also another option that can be tried.

Two blockchain (BC) platforms have emerged as potential solutions to safeguard IoT devices in terms of data integrity and confidentiality: Ethereum and the Hyperledger Framework. Each platform presents its own set of challenges, and the choice between them depends on specific use cases. In the context of Distributed Denial of Service (DDoS) protection, the Hyperledger Framework stands out as the preferred option mainly because of its private BC feature and no gas costs. Ethereum Ganache was also considered as it (Ibrahim et al., 2022) command line emulator that works without incurring the gas fee of the ETH network

	Ethereum	**Hyperledger Fabric BC**
Type	Public/Private	Public/Private decentralized
Cost	Gas units – free in Ganache	minimum Cost to setup
Programming Language	Solidity	Go, Java and others
Consensus Mechanism	PoS	Raft , Kafka , Solo, chain code
BC Accessibility	Anyone can commit	Restricted to only authorized participants or peers

Table 2: Blockchain Comparison -Eth and HLF BC

My proposed methodology therefore was a combination of using different available simulation applications for DDoS testing such as iFogSim and Ns3 as well as a secure network in a virtual box setting.

4 Design Specification

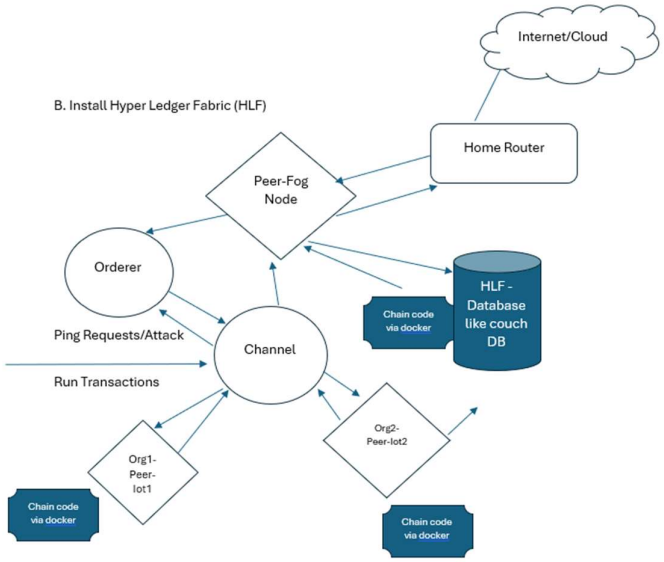


Figure 2. Hyper Leder Fabric setup with 2 nodes and 1 Orderer verifying transactions, keeping records in the couch db ledger.

Used Blocksim, IfogSim and Ns3 to test for simulation of IoT devices and blocking through BC based on a study by (Ullah et al., 2021). Despite successfully establishing a network, the simulator lacked support for HLF Blockchain (BC) integration and with no knowledgebase access available online to get the support. Block sim generated an Excel file after exhibiting blockchain behavior with different metrics, like transaction time, and BC processing time extra. (maher243, 2024) ,Ifogsim simulator on the other hand also simulated the IoT nodes environment with fog nodes, due to lack of support I had to carry out more research to switch to Ns3 simulator. Ns3 version 3.40 will be installed from nsam.org following the instructions. It requires many prerequisites like Python, SQL lite, cmake, git, tar. Carry out simulation using Ns3. Use NetAnim tool inside ns3 to display an animated DDoS Sync flood attack on 6 camera nodes by 2 x attackers.

Simulators for DDoS Attacks. Kali Linux and Windows 10 enterprise virtual machines would be utilized to carry out the DDoS attack on the victim IoT devices on the network.

Netsim Blc	**Blocksim**	**Ifogsim**	**NS3**
User friendly	BC focus	Fog computing focus	Open source
Scalable	Custom parameters	Open source	Active community
Proprietary software	Proprietary software	Integrate with other software	Extensible with performance issues
Limited flexibility	Limited scoped	Lack of features	Realistic simulations
Low support		Performance issues	Limited features lack of Gui

Table 3. Simulator for DDoS and BC testing comparison

LOCI/HOIC and HPing3 utilities were used. (*hping3 Tutorial - TCP SYN Flood Attacks*, 2022)

Disclaimer: These applications are not used outside of your test network; it is illegal and against the law to do it outside of your lab network setup for educational purposes.

Scappy Python can also be used to customize packets to the nodes, I considered this but did not use it. Any virtual box using these tools would need to block default malware protection like Windows Defender or any other AV being used. The network setup must be internal so machines on that network can communicate with each other, but no outside access is available to the internet. To check if the attacks were successful tools like *Wireshark* was used to view traffic of the attacking and victim IoT node.

Virtual Box: VirtualBox was configured with Kali 64-bit and Windows 10 virtual machines, alongside Debian boxes, virtual routers, and additional Ubuntu boxes. The network setup was tailored to the experiment's requirements, initially configured as an internal network devoid of internet access, with subsequent adjustments granting select nodes internet functionality as needed.

DDoS Attack Simulation:

HOIC setup in Windows 10 edger virtual box container. Block internet traffic from the target machine as well as from the victims. Set up an internal network using a virtual box configuration file.("Oracle VM VirtualBox," n.d.) (oetman tech media, n.d.)

Hyper Ledger- Block Chain (HLF-BC) – Configure the HLF network in Kali Linux

Configure HLF (install documentation, 2020) and configure it on the IoT Ubuntu virtual machines, which are full-scale Ubuntu machines and we are assuming here that these are IoT devices.

Hyper Ledger Fabric Pre-requisites and Setup of Network:

Define the network topology: Determine the layout of your network, including the placement of IoT devices and the node/gateway device.

Determine network protocols: Decide on the network protocols to be used for communication, such as MQTT which is used by IoT devices, or http. Determine how IoT devices will communicate with the node/gateway device and each other.

Ensure network security: Implement measures to secure communication channels and prevent unauthorized access, including DDoS protection mechanisms.

Hyper Ledger Functions and Testing:

Install Hyperledger Fabric: Set up Hyperledger Fabric on the node/gateway device according to the platform's installation instructions.

Configure the network: Define the network configuration, including channels, peers, and Orderer, using Hyperledger Fabric's configuration files.

Set up rules that are defined in the chain code to decide when a transaction occurs from the IoT devices, the endorsers that are part of the peer network will agree to a transaction. A Tx will be committed to the ledger once both of the endorsers agree on it or even if one of the endorsers agrees the Tx is committed to the ledger.

Set up membership services: Configure the membership service provider (MSP) to manage identities and permissions for devices on the network.
Develop smart contracts: Create smart contracts (chain code) that define the business logic for interacting with the ledger, including functions to handle DDoS detection and prevention. Check to see which one is easy to implement like Kafka, Solo, or Raft. Raft would be logical to implement as it is faster. Solo is for development and testing; it is not good for production and cannot recover from a crash. Kafka is complex to implement. (Spydra, 2023)
Define transaction types: Specify the types of transactions that IoT devices will perform on the network, such as data submission or querying. 2 types of Tx's are described below in the flow chart.
Test network functionality: Verify that IoT devices can communicate with the node/gateway device and perform transactions on the Hyperledger Fabric network.
Conduct integration testing: Test the integration between IoT devices and Hyperledger Fabric to ensure seamless interaction, including testing against simulated DDoS attacks.
Deploy the network: Deploy the finalized network configuration and smart contracts to the production environment.
Set up monitoring tools: Implement monitoring tools to track network performance and detect any DDoS attacks or anomalies.
Flow chart – Hyper Ledger Blockchain – How transactions will address DDoS and rogue traffic.

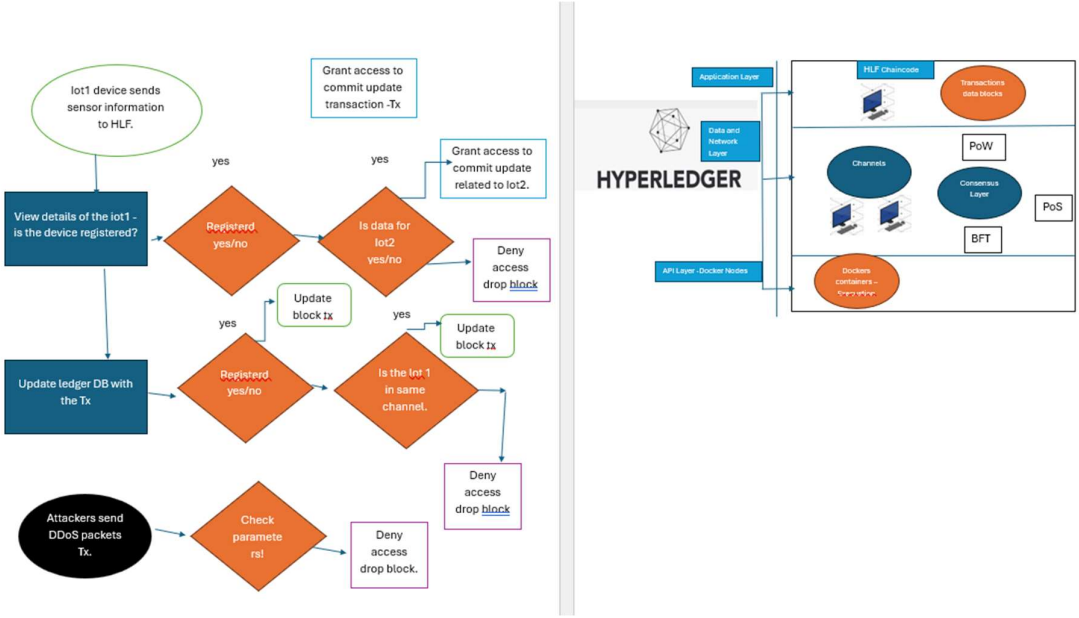


Figure 3.1 shows the flow of HLF tx (chain code transactions), packets will be dropped if DDoS traffic is detected or if IoT devices are not part of the HLF BC.
Figure 3.2 shows some additional parameters that can be in place to check what data needs to be verified from the IoT devices.
Access control will be set up for IoT devices using HLF built-in Certificate authority to manage the identities of the devices and issue certificates for authentication. X.509 certificates are issued for authentication.

Consensus Setup: Once the HLF is set up a consensus mechanism is set up using CC which is the default smart contract option available in HLF.

DDoS Detection: HLF should allow for a rate-limiting function that can help with detecting anomalous data. Monitoring tools would need to be set up to check incoming traffic. I have not been able to come to this stage yet due to the complexity of setting up the network. Smart contract -CC can be set up as shown in the figure can be set up to block incoming traffic from the rogue device.

The config files for CC need to be configured to fulfill the requirements of detection. Rate limiting needs to be set up for controlling the performance of HLF against DDoS attacks. (“Rate Controllers,” n.d.) for example, the below code in Hyper Ledger Caliper allows for 10 transactions per second. The Hyper Ledger caliper will be used for benchmarking performance.

```
{
  "type": "fixed rate",
  "opts": {
     "tps" : 10
  }
}
```

5 Implementation

Hardware deployed for this project - 11 Intel(R) Core(TM) i5-10310U CPU @ 1.70GHz 2.21 GHz with 32GB of ram and 500 GB SSD.

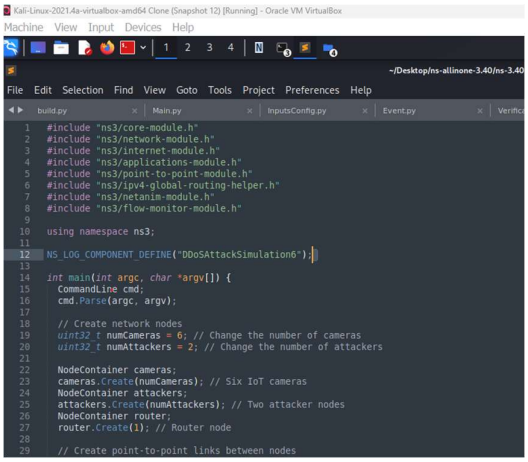
Machines Deployed: 2 x Kali machines.

2 x Ubuntu virtual Machines installed with prerequisite of HLF and with full deployment of

IfogSim Simulation: Setup Eclipse and VScode in both primary Windows and Kali Linux. I was able to configure the ifogsim in both Windows as well as Kali Linux. Results were available through sample scripts already in the repository, but it requires a considerable understanding of the architecture to implement HLF in the simulator.

Ns3 Simulation

Through Ns3, the network was effectively configured, enabling the execution of DDoS simulations with assistance from available GitHub repositories that provide sample animation files for IoT nodes. I set up various experiments to set up nodes and perform DDoS tests.



```
#include "ns3/core-module.h"
#include "ns3/network-module.h"
#include "ns3/internet-module.h"
#include "ns3/applications-module.h"
#include "ns3/point-to-point-module.h"
#include "ns3/ipv4-global-routing-helper.h"
#include "ns3/netanim-module.h"
#include "ns3/flow-monitor-module.h"

using namespace ns3;

NS_LOG_COMPONENT_DEFINE("DDoSAttackSimulation6");

int main(int argc, char *argv[]) {
  CommandLine cmd;
  cmd.Parse(argc, argv);

  // Create network nodes
  uint32_t numCameras = 6; // Change the number of cameras
  uint32_t numAttackers = 2; // Change the number of attackers

  NodeContainer cameras;
  cameras.Create(numCameras); // Six IoT cameras
  NodeContainer attackers;
  attackers.Create(numAttackers); // Two attacker nodes
  NodeContainer router;
  router.Create(1); // Router node

  // Create point-to-point links between nodes
```

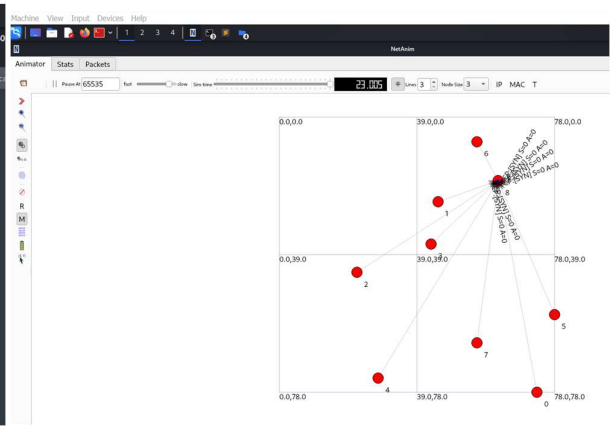


Figure 4.1 code for the ns3 attack simulation. Figure 4.2 NetAnim simulation of syn flood attack on 6 camera nodes by 2 attackers.

DDoS Attack Simulation

DDoS Attack performed from Windows 10 devices on IOT3 using HOIC DDoS too in an internal network setting, isolating the attack internal to the network:

Setting up internal ip addresses by modifying the virtual box internal config files to create a fixed IP network in the range of 192.168.2.1 and so on still assigned by DHCP/

. DDoS attack was done using HOIC from host 192.168.2.3 to 192.168.2.2 flooding with TCP acknowledgment attack.

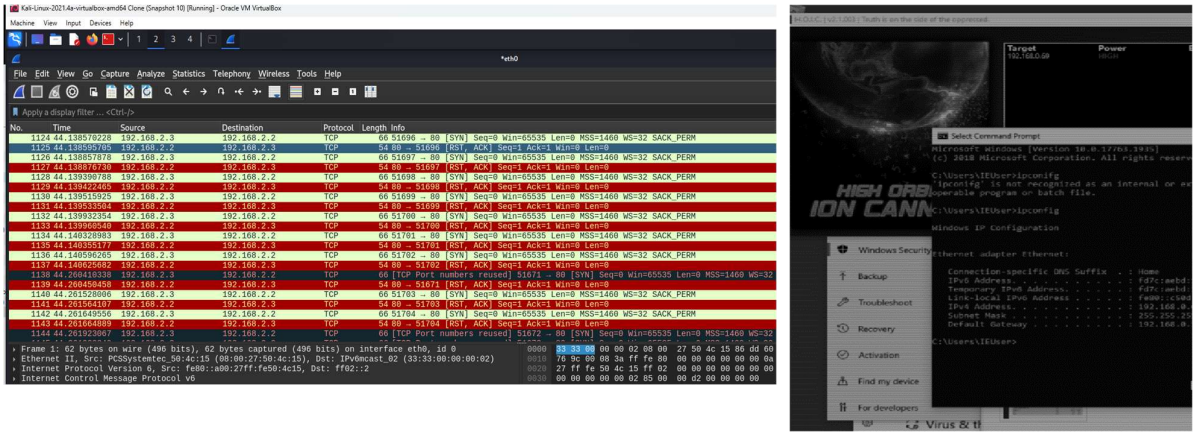


Figure 5. Showing DDoS attack traffic on the IoT machines via HOIC.

HLF Deployment.

HLF was deployed on the virtual machine downloading it from the main web page.

The path was set for the variables. The test network was set up via the following command in the test-network folder. Cd fabric-samples/test-network.

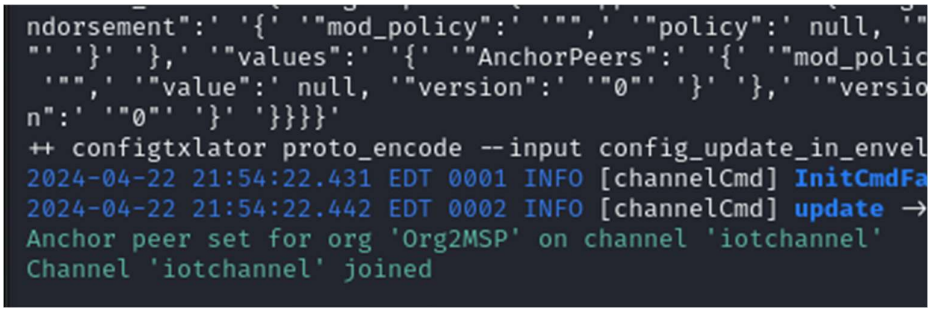


Figure 5. Shows the HLF network up and running with an IoT channel to establish transactions among the nodes.

./network.sh up would start the HLF BC, ./network.sh down would down the network.

Chanel was created for communicating with the IoT nodes and the consensus network was enabled with chain code command.

2 x peers, orgs were created in both virtual machines. Endorser and Orderer were created by default test network settings. A chain code was deployed to carry out the transaction mechanism.

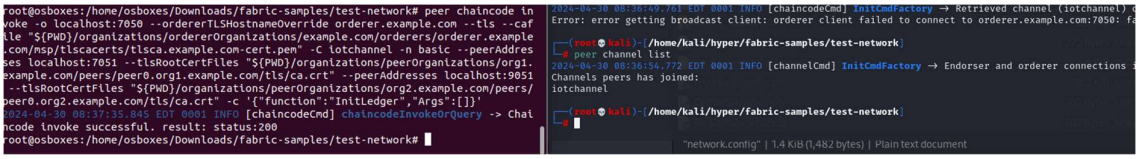


Fig 6 shows block chain active with the IoT channel and carrying out an invoke query with the status result of 200.

Both devices would join a network using a docker swarm to interact. Further development was done to customize CC for the IoT Network setup between the 2 devices where asset information that is the property of the IoT devices like device ID, and name extra would be used to verify the devices and once the information is received in the HLF BC it would be saved into the couch db. as a block. Any outside device will not be allowed to access the network with the implementation of a feature called rate limiting in HLF. (HyperLedger Documentation, n.d.)

6 Evaluation

6.1 DDoS Simulation

Experiment / NS3 Simulation/Ifogsim, Blocksim. All 3 simulators generated results for DDoS and nodes. I was unable to integrate HLF BC mechanisms into these simulators. Good knowledge of C++, Java, and Go is required for Ns3, the same can be said for Blocksim.

However, I encountered limitations in its scope and a lack of online support. Similarly, Blocksim yielded results for IoT devices under specific conditions but didn't fully meet my requirements. It worked on parameters that could be altered; results were displayed in an Excel file with which nice graphical data can be represented to see anomalies in BC traffic.

6.2 DDoS in Virtual Box Environment

DDoS testing on the virtual machines was successful through Hoic and hping 3 from Linux boxes. Resulted in increased CPU usage. An experiment to do it with the HLF network live was not conducted due to an incomplete setup of the HLF network between the nodes.

6.3 Hyperledger Setup in Virtualized IoT Nodes

I was able to set up the HLF blockchain network with some devices but was unable to configure it to exhibit the concepts I have described in my methodology and design.

6.4 Discussion

Even though the research did not return on what I was expecting in terms of concrete results, it contributes valuable insights into the complexities and challenges of deploying blockchain technology for IoT security. By acknowledging these limitations and reflecting on the lessons learned, the research provides a foundation for future investigations in this critical area of cybersecurity. It has been a challenging and great journey to work on this project. It would be important to note that a variety of IoT devices use multiple protocols which can exhibit different behaviour when working with HLF.

Overall, I think there is a lot more that can be done with a combined team effort of researchers when it comes to HLF BC. There has been a lot more work done on Ethereum the HLF. For DDoS protection, I still think HLF is a better choice as it is available at the private level, permission-based which gives users more control.

Keep in perspective the IoT devices that we use in our homes HLF BC implementation is a challenge till it evolves with new researchers working on this BC. Hyperledger Fabric's architecture and setup process can be more complex compared to a private Ethereum network, especially if you're new to the technology. It involves setting up multiple components like peers, Orderer, and channels, and configuring membership services.

Hyperledger Fabric offers features like identity management, access control, and consensus mechanisms that can enhance IoT security. Implementing and integrating these features into an IoT environment may require additional effort and expertise. Hyperledger Fabric provides flexibility and customization options that may be beneficial for specific IoT use cases and security requirements, but this also means a potentially steeper learning curve that in my case

One of the primary challenges I encountered was the complexity associated with implementing HLF in a home environment, particularly on Fog node Gateways or other high-processing devices. While there was partial success in setting up HLF on Linux boxes, the study faced limitations in terms of scalability, compatibility with existing IoT infrastructure, and resource constraints. Additionally, simulators like Ns3, while powerful and useful tools, proved inadequate for simulating blockchain applications comprehensively. It requires extensive knowledge of how docker containers work and the same for HLF BC which requires development language knowledge to write custom code on how you want the BC transactions to conclude, for example, what values the ledger would store for your specified devices.

Navigating the landscape of blockchain technology and DDoS mitigation posed significant hurdles. Despite an abundance of ongoing research in related areas, accessible information, and resources on deploying blockchain solutions for IoT security were limited. This scarcity hindered the research progress and led to challenges in understanding complex solutions and effectively implementing them in a home environment. The overall findings and learnings are presented in the table below.

Challenges of HLF BC and DDoS Detection Implementation	**Description**
Complex Setup and Configuration	Setting up a Hyperledger network involves configuring multiple components such as peers, Orderer, channels, and smart contracts. The complexity increases with the size and scale of the network.
Limited Documentation	Documentation for HL limited, especially for specific use cases. Developers rely on community forums or experimentation to fill in the gaps.
Smart Contract Development Complexity	Developing smart contracts for HLF requires a solid understanding of chain code programming languages like Go or Node.js, as well as familiarity with the Fabric APIs and transaction flow.
Scalability and Performance Tuning	Achieving optimal performance and scalability in Hyperledger and IoT networks often requires fine-tuning parameters to understand the load that IoT devices can take.
Security and Privacy Considerations	HLF emphasizes security and privacy, code needs to be designed carefully and implement access controls, encryption mechanisms, and privacy-enhancing techniques to protect sensitive data and prevent unauthorized access to IoT devices
Simulating DDoS Attacks	Simulating DDoS attacks and analyzing their impact on HL networks can be challenging due to limited integration options with existing simulators like NS3 or Blocksim. Integrating Hyperledger mechanisms into these simulators requires advanced knowledge of programming languages like C++, Java, or Go.
DDoS Testing in a Virtualized Environment	Conducting DDoS testing on virtual machines within a Hyperledger network may encounter obstacles related to setup or compatibility issues. DDoS testing tools need a thorough setup and closed network to manage risk and legal complications.
HHyperledger Setup on IoT Nodes	Configuring HLF on IoT devices for demonstrating security concepts may face challenges due to the complexity of setup, scalability limitations, and compatibility issues with existing IoT infrastructure. IoT protocols are different for devices.
IoT Home Setup and HLF	Intense development is required by the community to build on the HLF platform with packaged software on standard hardware which is the way forward. The platform needs to evolve to support testing for smaller IoT devices.

Table 4. HLF BC challenges in testing and deployment for DDoS mitigation in IoT devices.

7 Conclusion and Future Work

Mitigating DDoS attacks on home IoT devices using Hyper Ledger Blockchain (HLF-BC)? The research aimed to determine the feasibility of employing Hyperledger Blockchain (HLF) for mitigating Distributed Denial of Service (DDoS) attacks targeting home IoT devices. Despite the research objectives, the study encountered several challenges that hindered the attainment of tangible results.

Apart from these obstacles, the research underscores the critical importance of continued exploration and collaboration in addressing cybersecurity threats to IoT devices. Future research should prioritize several key areas. Efforts should be directed towards simplifying the implementation process of blockchain solutions, ensuring that deploying Hyperledger networks becomes more straightforward and accessible. In addition, there is a pressing need to enhance the availability of pertinent information and resources, facilitating smoother adoption and integration of blockchain technologies, particularly in contexts such as IoT security.

Exploring alternative methodologies for evaluating the efficacy of DDoS mitigation strategies is crucial. This includes devising innovative approaches to testing and assessing blockchain-based solutions within virtual environments. It is imperative to develop custom consensus algorithms tailored specifically for IoT devices, aligning them closely with the protocols

commonly employed by these devices. Such efforts will enable the replication of real-world scenarios in testing, thereby refining the effectiveness of DDoS mitigation strategies.

There is an opportunity to advance the standardization of Hyperledger Fabric for use in gateway devices. These devices can serve as intermediaries between low-powered home IoT devices and the blockchain network, facilitating blockchain transactions while alleviating the computational burden on the IoT devices. By establishing standardized protocols and frameworks for integrating Hyperledger Fabric into gateway devices, the scalability and practicality of blockchain solutions in home IoT environments can be significantly enhanced.

References

GitHub licences: ("ns3-cybersecurity-simulations/LICENSE at master · Saket-Upadhyay/ns3-cybersecurity-simulations," n.d.)

Ahmed, Z., Danish, S.M., Qureshi, H.K., Lestas, M., 2019. Protecting IoTs from Mirai Botnet Attacks Using Blockchains, in: 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). Presented at the 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 1–6. https://doi.org/10.1109/CAMAD.2019.8858484

Al Hwaitat, A.K., Almaiah, M.A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., Alrawad, M., 2023. A New Blockchain-Based Authentication Framework for Secure IoT Networks. Electronics 12, 3618. https://doi.org/10.3390/electronics12173618

Almuqren, L., Mahmood, K., Aljameel, S.S., Salama, A.S., Mohammed, G.P., Alneil, A.A., 2023. Blockchain-Assisted Secure Smart Home Network Using Gradient-Based Optimizer With Hybrid Deep Learning Model. IEEE Access 11, 86999–87008. https://doi.org/10.1109/ACCESS.2023.3303087

amazon, n.d. What is a DDOS Attack & How to Protect Your Site Against One [WWW Document]. Amazon Web Services, Inc. URL https://aws.amazon.com/shield/ddos-attack-protection/ (accessed 4.16.23).

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S.W., Yellick, J., 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the Thirteenth EuroSys Conference. Presented at the EuroSys '18: Thirteenth EuroSys Conference 2018, ACM, Porto Portugal, pp. 1–15. https://doi.org/10.1145/3190508.3190538

Baucas, M.J., Spachos, P., Plataniotis, K.N., 2022. Public-Key Reinforced Blockchain Platform for Fog-IoT Network System Administration. IEEE Internet of Things Journal 9, 22366–22374. https://doi.org/10.1109/JIOT.2021.3104740

Chaganti, R., Bhushan, B., Ravi, V., 2022. The role of Blockchain in DDoS attacks mitigation: techniques, open challenges and future directions.

DDoS threat report for 2023 Q1 [WWW Document], 2023. . The Cloudflare Blog. URL http://blog.cloudflare.com/ddos-threat-report-2023-q1/ (accessed 4.17.23).

de Assis, M.V.O., Carvalho, L.F., Rodrigues, J.J.P.C., Lloret, J., Proença Jr, M.L., 2020. Near real-time security system applied to SDN environments in IoT networks using

convolutional neural network. Computers & Electrical Engineering 86, 106738. https://doi.org/10.1016/j.compeleceng.2020.106738
Fred Donovan, 2021. What is STRIDE and How Does It Anticipate Cyberattacks? [WWW Document]. Security Intelligence. URL https://securityintelligence.com/articles/what-is-stride-threat-modeling-anticipate-cyberattacks/securityintelligence.com/articles/what-is-stride-threat-modeling-anticipate-cyberattacks (accessed 12.4.23).
Friha, O., Ferrag, M.A., Shu, L., Nafa, M., 2020. A Robust Security Framework based on Blockchain and SDN for Fog Computing enabled Agricultural Internet of Things, in: 2020 International Conference on Internet of Things and Intelligent Applications (ITIA). Presented at the 2020 International Conference on Internet of Things and Intelligent Applications (ITIA), pp. 1–5. https://doi.org/10.1109/ITIA50152.2020.9312286
hping3 Tutorial - TCP SYN Flood Attacks, 2022.
HyperLedger Documentation, n.d. Writing Your First Chaincode [WWW Document]. URL https://hyperledger-fabric.readthedocs.io/en/release-2.2/chaincode4ade.html (accessed 4.30.24).
Hyperledger Fabric Glossary — fabricdocs 1.0 documentation [WWW Document], n.d. URL https://fabrictestdocs.readthedocs.io/en/latest/glossary.html (accessed 4.29.24).
Ibrahim, R.F., Abu Al-Haija, Q., Ahmad, A., 2022. DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology. Sensors 22, 6806. https://doi.org/10.3390/s22186806
install documentation, 2020. HLF installation [WWW Document]. URL https://hyperledger-fabric.readthedocs.io/pt/latest/install.html (accessed 4.25.24).
Jamader, A.R., Das, P., Acharya, B.R., 2019. BcIoT: Blockchain based DDos Prevention Architecture for IoT, in: 2019 International Conference on Intelligent Computing and Control Systems (ICCS). Presented at the 2019 International Conference on Intelligent Computing and Control Systems (ICCS), pp. 377–382. https://doi.org/10.1109/ICCS45141.2019.9065692
Jay, A., 2020. Number of Internet of Things (IoT) Connected Devices Worldwide 2022/2023: Breakdowns, Growth & Predictions [WWW Document]. Financesonline.com. URL https://financesonline.com/number-of-internet-of-things-connected-devices/ (accessed 4.13.23).
Kobialka, D., 2023. Google, Amazon Face Massive Denial-of-Service Attack [WWW Document]. MSSP Alert. URL https://www.msspalert.com/news/google-amazon-face-massive-denial-of-service-attack (accessed 4.24.24).
Lee, Y., Rathore, S., Park, Jin Ho, Park, Jong Hyuk, 2020. A blockchain-based smart home gateway architecture for preventing data forgery. Hum. Cent. Comput. Inf. Sci. 10, 9. https://doi.org/10.1186/s13673-020-0214-5
maher243, 2024. maher243/BlockSim.
Mohapatra, D., Bhoi, S.K., Jena, K.K., Nayak, S.R., Singh, A., 2022. A blockchain security scheme to support fog-based internet of things. Microprocessors and Microsystems 89, 104455. https://doi.org/10.1016/j.micpro.2022.104455
Nakamoto, S., n.d. Bitcoin: A Peer-to-Peer Electronic Cash System.
ns3-cybersecurity-simulations/LICENSE at master · Saket-Upadhyay/ns3-cybersecurity-simulations [WWW Document], n.d. . GitHub. URL https://github.com/Saket-Upadhyay/ns3-cybersecurity-simulations/blob/master/LICENSE (accessed 12.10.23).
oetman tech media, n.d. internal network Virtual box [WWW Document]. URL https://www.youtube.com/watch?v=04pAiANkr_s&ab_channel=PeymanTechMedia (accessed 4.25.24).

Oracle VM VirtualBox [WWW Document], n.d. URL https://www.virtualbox.org/ (accessed 4.25.24).
Rate Controllers [WWW Document], n.d. . Hyperledger Caliper. URL https://hyperledger.github.io/caliper/v0.5.0/rate-controllers/ (accessed 4.25.24).
Saha, V., Anand, G., Ghosh, M., Singhal, S., 2023. Analysis of Blockchain-Based Techniques for the Mitigation of DDoS Attacks in IoT Devices, in: 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). Presented at the 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1–7. https://doi.org/10.1109/ICCCNT56998.2023.10307642
Shah, Z., Ullah, I., Li, H., Levula, A., Khurshid, K., 2022. Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. Sensors 22, 1094. https://doi.org/10.3390/s22031094
Shahbazi, Z., Byun, Y., Kwak, H.-Y., 2021. Smart Home Gateway Based on Integration of Deep Reinforcement Learning and Blockchain Framework. Processes 9, 1593. https://doi.org/10.3390/pr9091593
Spydra, 2023. HLF consensus mechanisms , Kafka, solo Raft [WWW Document]. URL https://www.linkedin.com/pulse/exploring-consensus-mechanisms-hyperledger-fabric-raft-solo-kafka/ (accessed 4.29.24).
Sundareswaran, N., Sasirekha, S., 2022. Packet Filtering Mechanism to Defend Against DDoS Attack in Blockchain Network, in: Suma, V., Fernando, X., Du, K.-L., Wang, H. (Eds.), Evolutionary Computing and Mobile Sustainable Networks. Springer, Singapore, pp. 201–214. https://doi.org/10.1007/978-981-16-9605-3_14
Uddin, M.A., Stranieri, A., Gondal, I., Balasubramanian, V., 2021. A survey on the adoption of blockchain in IoT: challenges and solutions. Blockchain: Research and Applications 2, 100006. https://doi.org/10.1016/j.bcra.2021.100006
Ullah, A., Ullah, S.I., Salam, A., 2021. Internal DoS Attack Detection and Prevention in Fog Computing, in: 2021 International Conference on Information Technology (ICIT). Presented at the 2021 International Conference on Information Technology (ICIT), pp. 763–768. https://doi.org/10.1109/ICIT52682.2021.9491127
Xu, Q., He, Z., Li, Z., Xiao, M., 2018. Building an Ethereum-Based Decentralized Smart Home System, in: 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). Presented at the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), pp. 1004–1009. https://doi.org/10.1109/PADSW.2018.8644880
Zheng, J., Dike, C., Pancari, S., Wang, Y., Giakos, G.C., Elmannai, W., Wei, B., 2022. An In-Depth Review on Blockchain Simulators for IoT Environments. Future Internet 14, 182. https://doi.org/10.3390/fi14060182
Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H., 2017. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, in: 2017 IEEE International Congress on Big Data (BigData Congress). Presented at the 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564. https://doi.org/10.1109/BigDataCongress.2017.85