Faculty of Computing and Informatics

Department of Cyber Security

DESIGNING A BLOCKCHAIN LAYER IN SMART GRID EDGE IoT DEVICES TO ENHANCE DATA SECURITY

Thesis submitted in fulfilment of the requirements for the degree of

MASTER OF COMPUTER SCIENCE

at

Namibia University of Science and Technology

Submitted by: **Sakaria Amakali Iindombo**

Student Number: **215052072**

Supervisor: **Dr Mercy Chitauro**

Submission Date: **19 July 2024**

METADATA

TITLE:	Mr
STUDENT NAME:	Sakaria Amakali Iindombo
SUPERVISOR:	Dr Mercy Chitauro
DEPARTMENT:	Cyber Security
QUALIFICATION:	Master of Computer Science
SPECIALISATION:	Cyber Security
STUDY TITLE:	Designing a Blockchain Layer in Smart Grid Edge IoT Devices to Enhance Data Security
MAIN KNOWLEDGE AREA:	Information Security and Critical Infrastructure
KEYWORDS:	Blockchain, Edge Computing, Smart Grid, IoT, Hyperledger-Fabric, Attacks
TYPE OF RESEARCH:	Applied Research
METHODOLOGY:	Mixed
STATUS:	Final Thesis
SITE:	Main Campus Windhoek
DOCUMENT DATE:	19 July 2024

I. DECLARATION

I, **Sakaria Amakali Iindombo** hereby declare that the work contained in the thesis for the degree Master of Computer Science project, entitled: **“Designing a Blockchain Layer in Smart Grid Edge IoT Devices to Enhance Data Security”,** is my own original work and that I have not previously in its entirety or in part submitted it at any university or other higher education institution for the award of a degree. I further declare that I will fully acknowledge any sources of information I will use for the research in accordance with the Institution rules.

Signature: Iindombo.S Date: 19 July 2024

Signature of the Supervisor

As the candidate’s supervisor, I herewith declare that I accept this dissertation for submission.

Name: Dr Mercy Chitauro

Signature: NBere

Date: 18 July 2024

II. ABSTRACT

A smart grid is an electricity network that uses digital technologies to minimize cost and maximize system scalability to meet the demands of end users. It is a bidirectional system that enables various renewable sources to produce clean energy to the grid, unlike the conventional grid. The smart grid is made up of interconnected edge IoT devices to provide real-time data and monitor the network in enabling data driven decision-making. Studies indicate that by 2025, there will be 75.44 billion connected devices due to the rise in the deployment of edge IoT devices. Given the current increase of edge IoT devices, data security concerns have arisen, exposing the grid to a wide range of attacks. Most of the edge IoT devices are deployed geographically dispersed, which makes management challenging. They are also built with limited system capabilities and lack of security considerations in their design. This study focused on the three most severe threats against smart grid edge IoT devices which are denial-of-service attacks, unsecure protocols, and firmware exploits as identified by a systematic literature review. The study aimed to design a blockchain layer that could enhance data security in edge IoT devices, using purified lightweight security protocols namely, ACL's, SSL/TLS and RBAC. Hyperledger Fabric blockchain layer was selected for its suitability in distributed edge computing due to its modular architecture, robust security features, and scalability. The study used a systematic literature review to investigate threats, analyze current deployment of blockchain layers, and to select lightweight security protocols to enhance the Hyperledger Fabric. An experiment was conducted by simulating the effects of attacks on the edge IoT smart grid, both before and after lightweight security protocols were applied on the blockchain layer. In each experiment, three types of attacks were conducted: denial-of-service, packet sniffing and firmware exploit. The results of the experiments show that without lightweight security protocols on the blockchain layer increased latency, packet loss, user credentials being transmitted in plaintext and success of firmware exploitation is experienced. Results from experiments after lightweight security protocols were applied on the blockchain layer, show a reduction of malicious traffic success, encrypted user credentials, and unsuccessful firmware exploit. As a result, the study recommends employing lightweight security protocols in the blockchain to ensure data integrity, confidentiality and availability. This will be useful to reduce computational burden, allowing edge IoT devices to operate more efficiently. In turn, this study

provides valuable insights for electricity service providers on effectively managing edge IoT devices in the smart grid and to promote renewable energy adoption. Ultimately, safeguarding the smart grid's data security to ensure human safety.

III. ACKNOWLEDGEMENT

Above all, I express my gratitude to the Lord for the spiritual fortitude, strength, courage, and blessings, for allowing me to finish my studies. I want to express my heartfelt gratitude to the Namibia University of Science and Technology for granting me the chance to pursue my studies at the institution. I also want to extend my sincere gratitude to Dr. Mercy Chitauro, my supervisor, as well as her family, for their unwavering support, invaluable direction, and encouragement throughout the entirety of my thesis completion journey.

To my mom, Lusia Shikongo, you have been a genuine source of inspiration and have profoundly influenced the individual I've become, thank you so much for your love and support, especially during times of scarcity from the outset. I appreciate my father, Victor Iindombo, for being there for me and providing support through every difficulty I encountered, even when I felt uncertain. I appreciate my family deeply for their constant love, support, and motivation, which have helped me persevere through difficult moments and driven me to pursue greatness. Lastly, I would like to extend my appreciation to my friends Brunmore Van Rensburg and Chancard Maboulou for their consistent support. Your assistance has been instrumental in transforming my career aspirations into tangible achievements. I wish you all abundance and prosperity.

IV. Publications Arising from the thesis

S. Iindombo and M. Chitauro, "An Analysis of the Implementation of Blockchain Technology in Smart Grid Edge IoT Devices," 2023 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 2023, pp. 1-5, doi: 10.1109/ETNCC59188.2023.10284952

S. Iindombo and M. Chitauro, “Enhancing Blockchain Layer In Smart Grid Edge Iot Devices to Improve Data Security”, “2024 ," 2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 2024. In Press

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

IoT	Internet of Things
DoS	Denial of Service
SCADA	Supervisory Control and Data Acquisition
NIST	National Institute of Standards and Technology
DDOS	Distributed Denial of Service
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
MQTT	Message Queuing Telemetry Transport
PoW	Proof of Work
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
PoA	Proof of Authority
PBFT	Practical Byzantine Fault Tolerance
FBA	Federated Byzantine Agreement
BCIoT	Blockchain Internet of Things
BSD-Guard	Blockchain Software Defined Guard
CP-ABE	Ciphertext Policy Attribute Based Encryption
LAKA	Lightweight Authentication and Key Agreement
CAU	Control Area Unit
ML	Machine Learning
AI	Artificial Intelligence
P2P	Peer to Peer
ACL	Access Control List

SSL/TLS	Secure Socket Layer / Trasport Layer Security
RBAC	Role Based Access Control
ECC	Elliptic Curve Cryptography
IEEE	Institute of Electrical and Electronics Engineers
ACM	Association for Computing Machinery
NPM	Node Package Manager
REST API	Representational State Transfer Application Programming Interface
CA	Certificate Authority
YAML	Yet Another Markup Language
SDK	Software Development Kit
TCP	Transmission Control Protocol
LSP	Lightweight Security Protocols

1. CHAPTER 1: INTRODUCTION

1.1. Smart Grid Background

A smart grid is a distribution system that allows the flow of electricity and operational data across a reliable communication network via IP routable means. A recent study by Merlino et al., (2022) indicated that the smart grid offers potential benefits for utilities, and energy measures using smart meters and appliances, it also reduces energy waste and power outages. The smart grid consists of IoT devices that are geographically connected to provide data to utilities (Ghasempour, 2019). Smart grid has become a key target of intruders as a result of vulnerabilities and no one cares to secure them (Akkadr et al., 2022).

Major common threats of the smart grid are identified as phishing, denial-of-service, malware spreading and eavesdropping (Gunduz et al., 2022. Phishing occurs when employees receive fake emails or communications that appear to be real and end up divulging sensitive information about the company, leading to an attack. IoT devices have limited processing and memory capabilities, making them vulnerable to distributed denial of service attacks (Efe et al., 2018). Smart meters are frequently subjected to denial-of-service attacks, resulting in the system becoming unavailable. Attackers can develop malware that will spread and infect organization servers as well as IoT devices. IoT devices in the smart grid network share valuable data which can compromise user privacy if they are intercepted, tampered, or modified. Another threat can be competitors attacking each other for the sake of financial gain.

Most smart grid classified attacks are based on confidentiality, integrity, and availability. An electrical power station in Ukraine's Ivano-Frankivsk city was targeted for a cyber-attack, putting 80,000 people in the dark and affecting one million, four hundred thousand (1.4 million) people (Rajendran et al., 2019). This attack was carried out using a spear-phishing attack. Another malicious computer worm, known as Stuxnet, targeted Supervisory Control and Data Acquisition (SCADA) in Iran. Stuxnet manipulated Programmable Logic Controllers (PLCs), which are in charge of managing electromechanical operations in machines (Fall, 2021). During the Mirai botnet assault in 2016, more than 500,000 internet-of-things devices around the world flooded Dyn's managed DNS infrastructure, potentially making numerous websites unreachable (Ahmed, 2020). Following the attack, researchers wondered what would happen if an attacker acquired control of a botnet of high-wattage IoT devices in each location and used them to manipulate the smart grid.

Another successful attack was simulated by researchers known as MadIoT (Manipulation of Demand via the Internet of Things) (Soltan et al., 2018). This attack targets the demand side of the grid rather than the supply side. According to Soltan et al., (2018) they were able to demonstrate that a 30% increase in demand caused all of the generators to trip in a simulation using a small-scale power grid model. Soltan et al., (2018) stated that an attacker would require access to "about 90 thousand air conditioners or 18 thousand electric water heaters within the specified geographical region" to carry out such attack. He recommends power grid operators start preparing for MadIoT attacks in the future, by ensuring that their infrastructure can handle sudden fluctuations in load.

The smart grid contains sensitive data, and power system data which are confidential. If intruders manipulate the smart grid, it can result in catastrophic damage and bring disaster to society. These may affect customers mentally and financially as power will be unavailable for usage. For example, an attack such as Black Energy was capable of deleting data and destroying hard drives (Geiger et al., 2020. If there is no electricity many people will suffer from harsh cold weather conditions. Also, most of the critical infrastructure like hospitals, financial institutions, and Internet Service Providers will be negatively affected in carrying out operations.

Due to the large number of IoT devices connected it is very difficult to secure them. Most attacks target the edge of the smart grid infrastructure because these IoT devices lack security capabilities. IoT devices have limited memory, storage, and CPU capacity which makes them vulnerable to attacks such as denial-of-service attacks (Lernefalk, 2021). At the same time edge IoT devices must transfer real-time data to the cloud, which may result in processing false requests due to tampered data.

IoT devices generate huge amounts of data, which is sent to the cloud to be analyzed. Interception can occur during data transit between clouds and devices, which would lead to data theft and modification (Varadharajan et al., 2018). To prevent these from occurring, the cloud needs to be closer to IoT devices (Zamora-Izquierdo et al., 2019). This implies that data can be secured locally, and encrypted tunnels can be built between distributed edges. Deploying edge computing close to the edge IoT devices can reduce latency and increase throughput.

1.2. Edge Computing

Edge computing networks can avoid the potential security and privacy risk in a centralized system. For instance, instead of using a centralized server, data processing might be done locally, reducing the danger of data leakage. Despite its advantages, edge computing has security and privacy drawbacks due to the challenge of managing diverse IoT devices in a heterogeneous and distributed environment. It is essential to integrate blockchain technology into edge computing. Edge computing will make it easier to apply blockchain technology across edge servers, allowing IoT devices to participate in chains while using less memory, CPU, and bandwidth (Ajayi et al., 2021).

1.3. Blockchain Technology

Blockchain is a distributed decentralized shared tamper-resistant database that may be maintained, shared, copied, and synced by numerous peer-to-peer participants (Hasankhani et al., 2021). Blockchain is designed to work in a decentralized manner, whereas normal databases are always centralized. The administrator has all the control over the normal database, which means that he can manage, modify, and control the database the way he /she wants.

Every block in the chain includes a hash representation of the preceding block, allowing blocks to be tracked back to the beginning of the blockchain (Casino et al., 2019). As a result, changing transactions between IoT devices in a block after the hash has been generated is difficult to modify. The blockchain will serve as a trusted database which maintains records of transactions among IoT devices.

1.4. Problem Statement

A smart grid is a vast and complex network that consists of millions of connected devices and other components. It comes with many security concerns and vulnerabilities such as those inherent in application layer protocols, operating systems, and physical equipment. Most IoT devices are located at the edge of the smart grid, helping with user interaction, monitoring, and collecting sensitive information (Mehmood et al., 2021).

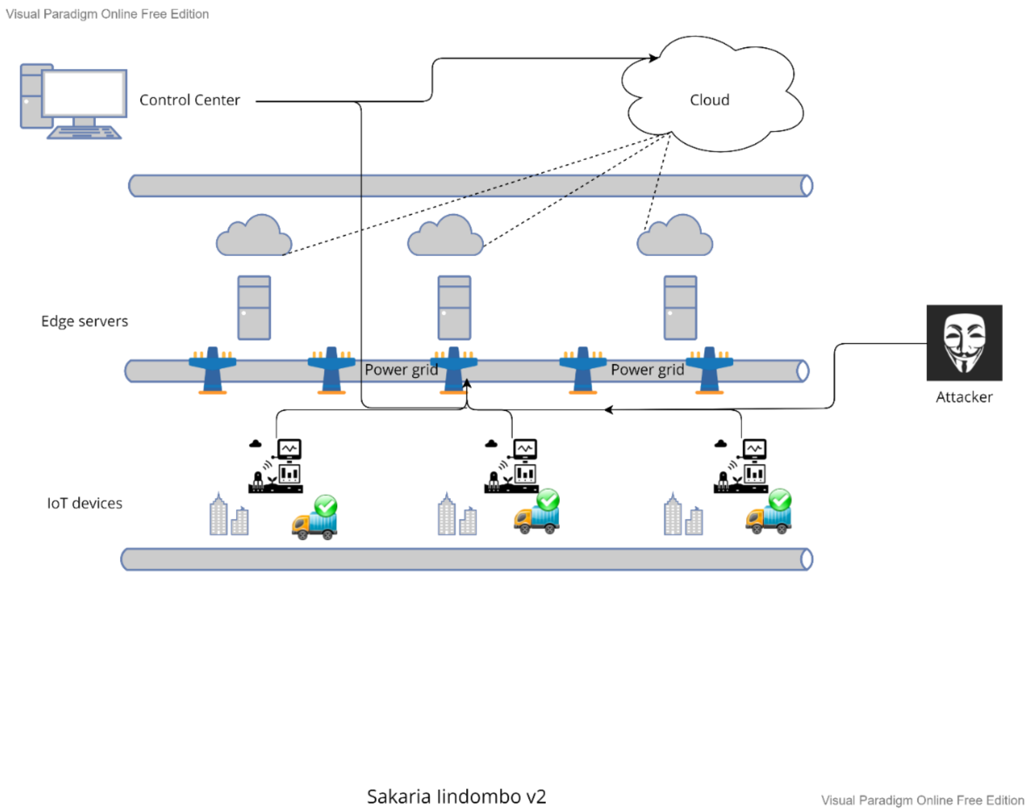


Figure 1.1: IoT and Edge Computing

Flaws in edge IoT devices attract intruders to perform malicious attacks to gain access and compromise the confidentiality and integrity of transmitted data. IoT devices in the smart grid are designed with the purpose of remote automating and processing information for the utility energy systems (Motlagh et al., 2020). They aren't built for security purposes such as authentication and encryption of data.

Security solutions designed for traditional IT networks are ineffective in smart grid networks because as stated by (Rajendran et al., 2019) security goals between smart grid and typical IT networks are different. Security in IT networks attempts to protect computer systems and networks, while security in smart grid networks aims to provide human safety, equipment and power lines protection, and system operation. This means security for IoT must be integrated within existing systems to protect the infrastructure without compromising performance or the smart grid's key objective. Many malicious attacks, including DoS attacks, jammer attacks, and sniffer attacks, firmware exploit, may be launched against IoT devices which is a significant concern in the smart grid. The researcher proposes the integration of blockchain technologies and edge computing, to address these security issues. The decentralized design of edge computing is envisaged to prevent system resource depletion of IoT devices and mitigate the computation workload (Shah et al., 2022) and blockchain technology uses cryptographic algorithms to secure data within each block, preventing unauthorized alterations or tampering. Therefore, the researcher proposes to integrate a blockchain layer of security in the smart grid edge to enhance data security.

1.5. Research Objectives

The primary objective of this research is to design a blockchain layer to address various security problems in smart grid edge IoT devices to enhance data security.

To achieve the main objective the following sub-objectives were undertaken:

1. Investigated edge IoT security threats in the smart grid.
2. To analyze the existing deployment of blockchain layer in distributed edge computing.
3. Enhance Hyperledger with lightweight security protocols.
4. Evaluate if enhanced blockchain layer enhances data security of IoT device.

1.6. Research Questions

The main research question was formulated as follows:

How can a blockchain layer be integrated in the smart grid edge IoT devices to mitigate security threats and improve data security? The main research question was answered by answering the following sub-questions:

1. What are the edge IoT security threats in the smart grid?
2. What are the various deployment of the blockchain layer in distributed edge computing?
3. Which lightweight security protocols can be built into Hyperledger to work with IoT devices?
4. How does the proposed blockchain layer improve data security?

1.7. Significance of the study

This research offers valuable insights for electricity service providers on effectively managing edge IoT devices in the smart grid and to promote renewable energy adoption. Also safeguarding the smart grid's data security to ensure human safety.

1.8. Delimitations of the study

The topic of smart grid security encompasses many aspects, but the researcher chose to concentrate specifically on denial-of-service attack, insecure protocols and firmware exploits associated with IoT devices in this context. Although there are various technologies that could have been explored, the research is centered on the utilization of blockchain technology.

1.9. Contribution of the study

The designed artifact plays a crucial role in ensuring the safety of smart grid. It also contributes to the information security management of organizations responsible for managing smart grid. In addition, this research enhances our understanding of smart grid security, the potential risks of IoT devices, and the appropriate procedures for securing IoT devices using Hyperledger Fabric.

1.10. Thesis outline

The rest of the thesis is organized as follows:

Chapter 2 – Literature review

This chapter describes the systematic literature review undertaken to tackle the first three objectives. The results of which were then subsequently used to design experiments to answer the fourth research objective.

Chapter 3 – Methodology.

This chapter discusses the methodology used for the study. It also presents the methods used for each research objective, data analysis techniques and tools utilised. Furthermore, it also discusses the setup of the simulation environment and how the proposed blockchain layer security design is tested and evaluated**.**

Chapter 4 – Result and Analysis

This chapter presents the experimental simulation results. The results were obtained from assessing the performance of the security protocols before and after, strategies implemented in Hyperledger grid fabric (the blockchain layer). Through experiments the efficacy and robustness of the security measures were scrutinized in a simulated scenario. Key metrics such as packet loss, latency, security breaches, and overall system resilience were examined to gauge the effectiveness of lightweight security protocols in the blockchain layer.

Chapter 6 – Conclusion

This chapter presents the study objectives and how they were achieved. The chapter further discusses the research contributions, research limitation, future considerations, reflections, and lessons learnt, conclusive remarks summarizing the findings.

2. CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

This chapter describes the literature review undertaken in this research. Systematic literature reviews as described in section 3 was conducted. The results of the systematic literature reviews is outlined in section 2-3 to 2.9. Section 2.3 to 2.9 outlines the analysis of edge IoT threats in the smart grid, deployment of blockchain layer in distributed edge computing and enhancement of Hyperledger with lightweight security protocols.

2.2. Background

Over the past few years IoT devices continue to grow immensely. Projections indicate that by 2025, there will be 75.44 billion connected devices (Alzoubi et al., 2022). Internet of Things (IoT) has become one crucial component of the enabling technologies for a smart grid. IoT is the integration of objects, such as sensors or any device with computing capability, into the internet. However, the rapid growth of IoT comes with major security challenges making the smart grid vulnerable to significant security attacks (Kimani et al., 2019). An IoT based smart grid has a large attack surface since it can consist of potentially millions of nodes. A compromised device can pose devastating effects to the whole grid (Hasan et al., 2022). This makes security a critical factor to consider before large scale deployment of IoT based smart grid networks (Aklilu & Ding, 2022).

Although IoT is now generating vast volumes of data, this pales in comparison to what will occur over the next decade (Diamandis et al., 2020) . Following major botnet attacks such as Mirai in 2016, botnet orchestrators consider IoT devices as an interesting target due to inadequate security configurations and massive number of devices that might be utilized for botnet attacks (Kelly et al., 2020). A report by (Geiger et al., 2020) reported that BlackEnergy has grown into one of the most sophisticated and modular malwares for attacking critical infrastructures. It has been involved in several cyber assaults, including a coordinated DDoS attack on Georgia's finance, military, and government sectors' fraudulent bank transactions, and a cyber-attack on Ukraine's power infrastructure (Akkad et al., 2023). The National Institute of Standards and Technology (NIST) has identified three requirements for maintaining and protecting information in the Smart Grid, which is confidentiality, integrity, and availability (NIST, 2020).

After IoT devices are deployed at the edge, no one thinks about them until they stop working, due to a lack of fixes and upgrades, attackers can exploit and launch attacks against them

(Castagna, 2020). Most IoT devices continue to use default credentials, making it simpler for attackers to gain access. Another cause of worry for IoT devices is a lack of system resources, which makes them vulnerable to Distributed Denial of Service attacks (Castagna, 2020).

(Coveney, 2022) stated that more than four-fifths of professionals working in power, renewables, oil, and gas believe a cyber-attack on the industry is likely to cause operational shutdown (85 percent) and damage energy assets and critical infrastructure (84 percent). He added that three-quarters (74%) believe an attack will harm the environment, while more than half (57%) believe it will result in death. He further stated that energy experts think that cyber-attacks on the industry will endanger lives, property, and the environment in the next two years.

On December 23, 2015, the Ukrainian power grid was hacked, resulting in power disruptions for around 230,000 Ukrainians for 1-6 hours. The attack occurred during the current Russo-Ukrainian War is linked to "Sandworm," a Russian advanced persistent threat organization. It is the first successful cyberattack on a power grid that has been officially recognized (Kholod et al., 2018). Hackers remotely compromised the information systems of three Ukrainian energy distribution businesses, briefly disrupting electricity supplies (Kholod et al., 2018). According to (Park et al., 2020) of one of the firms, the cyberattacks were carried out from computers using Russian Federation IP addresses.

The literature emphasizes how the Internet of Things is growing exponentially, especially when it comes to how they are being integrated into vital infrastructure such as the smart grid. IoT's explosive growth presents serious security risks, opening the smart grid to possible cyberattacks and threats. Major botnet attacks and sophisticated malware campaigns are examples of incidents that highlight the vulnerabilities present in IoT devices and their potential to compromise the resilience of vital infrastructure. In order to preserve and safeguard information within the Smart Grid, the National Institute of Standards and Technology (NIST) emphasizes the significance of confidentiality, integrity, and availability.

2.3. Edge IoT threats in the Smart Grid

IoT devices have a wide surface area for attacks because they are transmitting and carrying valuable data for analysis, new business models, use case and revenue streams. The majority of IoT devices are situated on the smart grid's edge. Attackers take advantage of these devices because of the location in which they are deployed. However, once they are in use, these devices receive no support or maintenance.

IoT devices are vulnerable to a broad range of threats, such as firmware exploits, unsecured protocols, denial-of-service attacks, and the interception of unencrypted credentials sent over HTTP (Bhardwaj et al., 2024). The security and integrity of IoT networks, especially those set up at the periphery of the smart grid infrastructure, are seriously threatened by these vulnerabilities. IoT devices are vulnerable to attacks from malevolent actors who want to undermine data integrity, interfere with services, and take advantage of system resources because of their large attack surface (Bhardwaj et al., 2024). Because of this, a thorough strategy to IoT security is necessary to reduce these various dangers and protect vital infrastructure networks from any assaults.

The reason firmware exploits are such a serious threat is that hardware manufacturers are more focused on the aesthetics of IoT devices than security (Cynthia et al., 2019). The smart grid infrastructure is extremely vulnerable to security breaches due to firmware exploit, which is regarded as a severe due to frequently outdated firmware’s. Moreover, due to the enormous number of active devices, IoT devices are an ideal target for malicious actors who are constantly looking for new ways to exploit and use specific resources. Especially in the case of Distributed Denial of Service (DDoS) attacks, which entail the use of a vast array of devices—including Internet of Things devices—to function as bots and submit fictitious requests to services, thereby disrupting them. Subsequently, it is quite easy for someone to intercept and steal credentials when data is transmitted over HTTP, as plaintext. It's the internet equivalent of shouting passwords across a crowded room. Next subsections discuss identified threats in edge IoT devices.

2.3.1. Denial-of-Service (DoS) attacks

IoT devices in smart grid infrastructure encourage intruders to launch attacks due to their limited system resources, such as CPU and memory, which makes them vulnerable to Denial-of-Service attacks (Kim et al., 2022). The attacker overwhelms the target by flooding malicious network traffic for starvation. Eventually, this results in the destruction of the infrastructure, disruption of services and compromising data availability (Aklilu & Ding, 2022a).

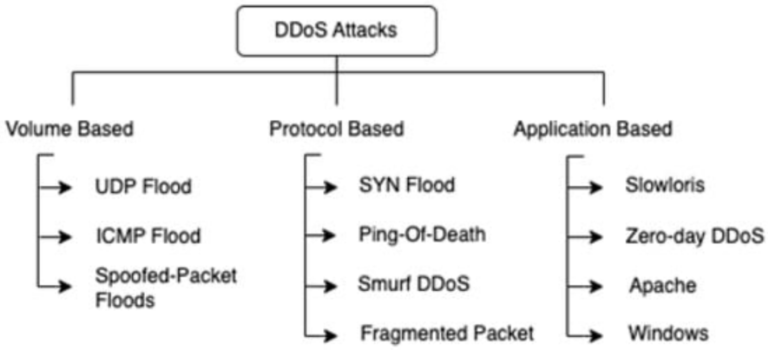


Figure 2.1. Taxonomy of DDoS attack (Alahmadi et al., 2023)

In Figure 2.1, a taxonomy of DDoS attacks illustrates the various forms these attacks can take (Alahmadi et al., 2023). To address these security challenges, various solutions have been proposed, including network segmentation, encryption protocols, and intrusion detection systems. However, the focus shifts to blockchain technology due to its potential to provide robust security measures for IoT devices in the smart grid. Blockchain's decentralized and immutable ledger offers enhanced protection against tampering and unauthorized access, making it a compelling solution for securing IoT networks. This decision to delve into blockchain is based on its unique features and its ability to address the specific security needs of IoT devices in the smart grid, distinguishing it from other security solutions available.

2.3.2. Insecure Protocols

Vulnerabilities in communication protocols used within the smart grid infrastructure, such as Modbus, Hypertext Transfer Protocol (HTTP), Message Queuing Telemetry Transport (MQTT), Distributed Network Protocol 3 (DNP3), or International Electrotechnical Commission 61850. (IEC 61850), expose devices to various attacks like man-in-the-middle attacks, replay attacks, and command injection attacks (Zeng et al., 2023). Adversaries exploit these weaknesses to manipulate data, disrupt operations, or gain unauthorized access to critical systems (Sharmwey A. Wasumwa, 2023). Protocol such as HTTP is widely adopted for its simplicity and compatibility, however it presents vulnerabilities such as lack of encryption, making it susceptible to eavesdropping and man-in-the-middle attacks (Pahl, 2018). In an Internet of Things (IoT) context, one of the most popular application protocols for enabling machine-to-machine communication is the Message Queuing Telemetry Transport protocol (MQTT). MQTT has both household and commercial uses because it is effective and lightweight. Because of its vulnerability to DoS attacks and its use of plain text data transmission, this protocol presents a security risk to the smart grid and has the potential to seriously impair its services (Vaccari et al., 2020).

2.3.3. Firmware Exploits

Attacks target vulnerabilities in IoT device firmware, including outdated software components, insecure firmware update mechanisms, or lack of secure boot processes. Exploiting these vulnerabilities allows attackers to compromise device integrity, inject malicious code, or gain persistent access to smart grid networks (Rosairo, 2023). According to (Bakhshi et al.,2024) edge IoT devices firmware's are easily available for free online and become key target to intruders, which they unpack a firmware-based and use reverse engineering for binaries to review configurations and runs attacks which make it easier to attack live deployed devices. A smart grid infrastructure is highly vulnerable to this kind of attack.

2.4. Blockchain Layer in Distributed Edge Computing

Blockchain technology is a unique type of data structure that is designed to record and store transactions in blocks (Bodkhe et al., 2020). Each block is linked to the previous block with a timestamp and a hash code, creating a chain-like structure. This system ensures that data records remain unaltered and cannot be changed retrospectively. The blockchain is considered a distributed database because it enables participants who do not trust each other to rely on one another in a completely decentralised way (Dai et al., 2019).

In essence, the blockchain is a ledger composed of many blocks. Because each block cannot be changed without altering the entire chain of blocks, it is an incredibly secure way of transferring digital assets, money, and contracts without relying on any third-party agents (Pajooh et al., 2022). This makes it more difficult for attackers to tamper with the blockchain's integrity. During digital events, such as transactions, blockchain acts as a public ledger that records all the transactions (Kumar & Mallick, 2018). The process of creating a new block in the blockchain is called mining. Consensus is established among all participants to verify each block, ensuring the system's trustworthiness and integrity (Xie et al., 2018). One of the most significant advantages of blockchain technology is its ability to provide a distributed platform among participating entities, where consensus is established in a democratic way (Pajooh et al., 2022). This could revolutionise both financial and non-financial sectors in the digital world. The blockchain network is built using many connected nodes, and several programming languages, such as Solidity, Java, and Go, are currently used in its development (Dai & Wang, 2020).

Blockchain technology is a secure and decentralised system for recording and storing transactions (Bodkhe et al., 2020). It is a distributed database that enables participants who do not trust each other to rely on one another in a completely decentralised way. The system ensures the integrity and trustworthiness of data records by linking each block to the previous one. The blockchain's ability to establish consensus in a democratic way makes it a revolutionary technology that could transform many industries (Dai et al., 2019).

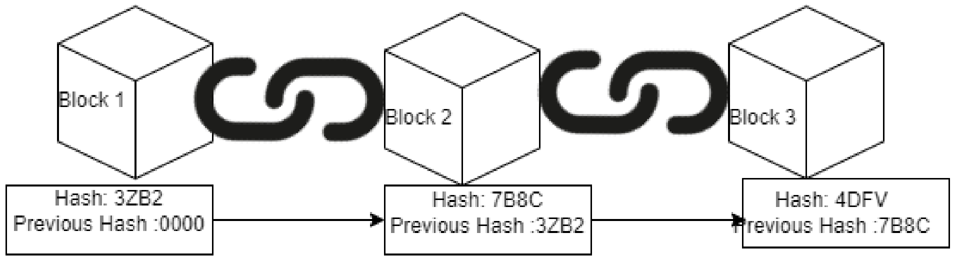


Figure 2.2 Blockchain Block diagram (Malik, 2019)

In a blockchain network, the first block is called the Genesis block, and it has a unique hash code that identifies it. Every subsequent block in the chain also has a hash code and contains the hash code of the previous block. This provides a layer of security because if any block is altered, it will make all the following blocks invalid. The diagram in Figure 2.2 shows an example of a simple blockchain configuration.

2.4.1. Consensus Mechanism and Types of Blockchain

Consensus mechanism refers to the process by which a distributed network of computers agrees on the validity of a transaction before adding it to the blockchain. This is important to ensure that the network remains secure and tamper-proof (Zhu, 2019). According to Zhu (2019) there are several types of consensus mechanisms used in blockchain networks, each with its own advantages and disadvantages.

- Proof of Work (PoW) is one of the oldest and most well-known consensus mechanisms, used by cryptocurrencies like Bitcoin. It requires nodes on the network to solve complex mathematical problems, which consumes a significant amount of computing power (Bains, 2022). Once a problem is solved, the solution is broadcast to the network and verified by other nodes. Once a certain number of nodes have verified the solution, the transaction is added to the blockchain (Kwong, 2023).

- Proof of Stake (PoS) is another consensus mechanism, used by cryptocurrencies like Ethereum (Zhou et al., 2023). In PoS, nodes are selected to verify transactions based on the amount of cryptocurrency they hold. The more cryptocurrency a node holds, the more likely it is to be selected to validate transactions. This reduces the amount of computing power required but can also lead to centralization if a small number of nodes hold a large amount of cryptocurrency (Platt & McBurney, 2023).
- Delegated Proof of Stake (DPoS) is a variant of PoS, used by networks like BitShares and Steem. In DPoS, nodes are elected by token holders to validate transactions on their behalf (Zhu, 2019). This reduces the amount of computing power required and can provide a more efficient and scalable network.
- Proof of Authority (PoA) is another consensus mechanism, used by networks like Ethereum Classic. In PoA, a group of pre-selected nodes are authorized to validate transactions. This reduces the amount of computing power required and can provide a more secure and efficient network (Bains, 2022).
- Other consensus mechanisms include Practical Byzantine Fault Tolerance (PBFT), used by networks like Hyperledger Fabric, and Federated Byzantine Agreement (FBA), used by networks like Stellar (Bains, 2022). These consensus mechanisms focus on ensuring that the network remains secure and can handle a high volume of transactions (Zhou et al., 2023).

There are several types of consensus mechanisms used in blockchain networks, each with its own strengths and weaknesses. The choice of consensus mechanism will depend on the specific needs of the network and the level of security, scalability, and decentralization required (Kwong, 2023).

2.4.2. Blockchain in Energy Sector

To create a smart energy supply, a smart grid needs to have the ability to self-maintain, self-rectify, be highly robust, and enable real-time pricing with a distributed energy management system (Alsmirat & Jaraweh, 2019). This requires the expertise of various engineering disciplines to work together to build an efficient smart grid. Many scientific and technological advancements have been made in these field, and numerous ongoing projects are currently underway to develop smart grid technology (Kim et al., 2020).

Blockchain is the result of combining several technologies, and its development can be traced back to the first symposium on principles of distributed computing held in 1982 (EUBLOCKCHAIN, 2020). Almost 30 years later, in 2009, Satoshi Nakamoto presented the first true concept of blockchain in his white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System". From 2011 onwards, several new cryptocurrencies were developed using blockchain technology (Nakamoto, 2008). The real-life implementation of blockchain applications began in late 2013, with the introduction of smart contracts that revolutionized the use of blockchain (Tripathi et al., 2023). However, a more scalable and flexible platform was needed, which led to the introduction of Hyperledger Fabric by the Linux Foundation in 2015, to address scalability and security issues. Since then, the energy sector has recognized blockchain as a promising technology for transforming conventional grid infrastructure into smart grids (Tripathi et al., 2023)

2.4.3. Types of Blockchain

- Public blockchain: This is a type of blockchain where everyone has read access to the blockchain and may submit transactions to it. Examples of public blockchains include Bitcoin, Corda and Ethereum.
- Private blockchain: This is a type of blockchain in which only entities included in a predefined list can read the blockchain and submit transactions to it (Hyperledger Foundation, 2022). An example of a private blockchain is Hyperledger Fabric (Malik, 2019).
- Consortium blockchain: This is a type of blockchain in which the consensus process is controlled by a pre-selected group of nodes. Consortium blockchains are often used by businesses and organizations to collaborate on a shared platform (Malik, 2019).
- Hybrid blockchain: This is a combination of public and private blockchains, where the public blockchain is used for some transactions and the private blockchain is used for others (Malik, 2019).
- Permission-less blockchain: This is a type of blockchain in which there are no restrictions on who is allowed to create blocks. Examples of permission-less blockchains include Bitcoin and Ethereum (Malik, 2019).
- Permissioned blockchain: This is a type of blockchain in which identities, only included in a predefined list, are allowed to create blocks. An example of a permissioned blockchain is Ripple (Malik, 2019).

Each type of blockchain has its own advantages and disadvantages, and the choice of blockchain will depend on the specific needs of the network, such as the level of security, scalability, and decentralization required (Hyperledger Foundation, 2022).

2.4.4. Hyperledger Fabric

The Hyperledger Fabric is a blockchain technology that operates as a private and permissioned network (Malik, 2019). It was developed under the Linux Foundation in 2015 to provide a secure network for members to track, exchange, and interact with digital assets. One of the unique features of Hyperledger Fabric is that it is the first blockchain to support the execution of distributed applications written in standard programming languages, known as chain codes (Malik, 2019). These chain codes are pieces of code that are installed onto the network of Hyperledger Fabric nodes, allowing for the creation and execution of smart contracts (Uddin et al., 2023).

The architecture of Hyperledger Fabric is comprised of several components, including Peer Nodes, Endorsing Nodes, Ordering Nodes, and Client Applications (Hyperledger Foundation, 2022). Peer Nodes are not limited to a single role and can serve as endorsers for certain types of transactions and simply as committers for others. Endorsing Nodes, on the other hand, are responsible for endorsing transactions by executing the chain code and verifying its results (Goudarzi et al., 2022). Ordering Nodes are responsible for the ordering of transactions into blocks and committing them to the ledger. Finally, Client Applications are responsible for interacting with the network by submitting transactions to be executed and querying the state of the ledger (Amjad et al., 2023).

The work done by Peer and Ordering Nodes in Hyperledger Fabric is similar to the work done by miners in other blockchain architectures (Hasan et al., 2023). However, there are some key differences. In Hyperledger Fabric, the process of creating new blocks and adding them to the ledger is not done through the process of mining. Instead, the Ordering Nodes are responsible for this task (Kuzlu et al., 2019). They use a consensus algorithm to agree on the order in which transactions should be added to the ledger. This consensus algorithm can be customized to meet the specific needs of the network and can consider factors such as the number of nodes in the network, the amount of computing power available, and the level of security required (Kim et al., 2020).

Another key difference between Hyperledger Fabric and other blockchain architectures is the way in which transactions are validated. In other blockchains, all nodes in the network validate every transaction (Malik, 2019). This can be time-consuming and can lead to scalability issues. In Hyperledger Fabric, only the Endorsing Nodes are responsible for validating transactions. This allows for greater scalability and can help to reduce the amount of computing power required to maintain the network (Alsmirat & Jaraweh, 2019).

The Hyperledger Fabric architecture is designed to provide a secure, scalable, and customizable blockchain network for businesses and other organizations (Kuzlu et al., 2019). By allowing for the creation and execution of distributed applications written in standard programming languages, it provides a platform for the development of smart contracts that can be used to automate complex business processes. Also, by using a consensus algorithm that can be customized to meet the needs of the network, it provides a flexible and scalable solution for a wide range of applications (Kim et al., 2020).

Hyperledger, among various blockchain frameworks, stands out for its suitability in distributed edge computing environments due to its modular architecture, robust security features, and scalability (Sharmwey A. Wasumwa, 2023). Compared to other frameworks like Ethereum and Corda, Hyperledger offers greater flexibility and customization options, making it ideal for tailored solutions in edge computing scenarios. The choice of Hyperledger in this research reflects its reputation for enterprise-grade blockchain solutions and its alignment with the security and scalability requirements inherent in distributed edge computing environments (Majid, 2023).

2.5. Review of the Proposed Blockchain Solution Suitable for the Smart Grid

Numerous research papers about blockchain-based edge IoT threats have proposed various strategies. Through various scenarios, these proposed methods seek to achieve data availability, confidentiality, and integrity. Thus, resulting into a secure network and narrowing down edge IoT attack surface. Additionally, some research on blockchain-based identity and authentication for the Internet of Things will be explored, with a focus on highlighting benefits and drawbacks. This section examines and recognizes previous research on the integration of edge computing and blockchain technology with edge IoT devices in the context of smart grids and data security.

2.5.1. Blockchain IoT (BCIoT) Framework

Jamader et al., (2022) used a blockchain IoT (BCIoT) framework; this framework is employed as a decentralized solution, to address security concerns with centralized approach, by utilizing smart contracts and end-to-end blockchain security to create a safe communication environment through encrypting and decrypting data using a hash-based secret key. This proposed solution is run in a controlled environment and data is stored in the blockchain. This study has led to an increase in data availability. This framework's main flaw is that all data—malicious or not—is stored on the blockchain, which leads to scalability and system resources issues.

2.5.2. Ethereum Blockchain

The Ethereum blockchain is employed, according to Hayat et al. (2022), to mitigate DDoS attack that is aimed at edge IoT devices. This proposed solution is based on IP level, through verification of IP addresses whether they are legitimate or not within client-server confinement. Only authorized IP addresses are allowed to communicate with the server, if not, they will be blocked. This solution creates a single point of failure, because only one device is allowed to authorize and IP spoofing.

2.5.3. Smart Contracts and Blockchain Extensions

Rehman et al., (2020) used smart contracts and blockchain extensions to secure configuration files from malicious attacks such as DDoS and data modification. This paper effectively safeguards fog network transaction records, and blockchain-based network design prevents attempts to manipulate transactional data in transit.

2.5.4. BSD-Guard

Proposed a DDoS protection system (BSD-Guard) that targets SDNs, based on blockchain (Jiang et al., 2020). It secures the control and data planes. It has a middle layer which analyses packet to determine suspect rate of incoming flows. This framework is used to store and share suspect lists in an immutable manner. The examination results showed that BSD-Guard could accurately issue defensive strategies close to the source of attack by identifying the attack path and detecting attacks.

2.5.5. A Differential Privacy Data Distortion Technique Based on Laplace Mechanism and Gaussian Mechanism.

Songlin et al., (2019); proposed a differential privacy data distortion technique based on Laplace mechanism and Gaussian mechanism. This technology is implemented by edge computing devices, in which artificial noises are added to the power consumption data of each smart meter, thus hiding the electricity behavior model, and avoiding leakage of privacy. An attack model interaction was launched successful and shows the smaller the privacy, the higher the privacy of the data, but lower the availability of the data. They preferred to use the Laplace mechanism for privacy protection based on the performance results while the Gaussian mechanism can be used as an alternative.

2.5.6. An Edge Blockchain Empowered Secure Data Access Control Scheme with Fair Accountability.

Yang, B et al., (2021) proposed an edge blockchain empowered secure data access control scheme with fair accountability for the smart grid using ciphertext policy attribute-based encryption (CP-ABE) as a promising solution for the distributed system. They decoupled CP-ABE to the cloud, due to intensively computational ABE algorithms which are beyond computational capabilities of lightweight IoT devices.

2.5.7. Lightweight Anonymous Authentication and key Agreement Protocol (LAKA)

Kumar et al., (2018) proposed a lightweight anonymous authentication and key agreement protocol (LAKA) using symmetric encryption. This protocol supports two-way authentication and obtains proper session key agreement for securing data communications. The test bed results have shown that there is high communicational and computational efficiency than other protocols. However, the neighborhood area network gateway must maintain many security keys for various home area network gateways.

2.5.8. Blockchain-Based Mutual Authentication and Key Agreement Protocol

The works of Jing, W., and Libing, W. (2020) proposed a blockchain-based mutual authentication and key agreement protocol for edge-computing-based smart grid. The aim of the protocol is to manage key management and conditional anonymity effectively without requiring additional sophisticated cryptographic primitives. This protocol ensures trust identity among IoT devices and secure the communication. The vulnerability of edge servers to attacks is greater than that of centralized clouds, according to research findings. Compared with existing protocols, the proposed protocol provides mutual authentication, secure key management and replay attacks. Since the protocol is simulated, it would function well in the real world even though it has the least cryptographic operations, such as computation and authentication.

2.5.9. Authentication protocol with high efficiency for smart grid.

Mahmood et al. (2018) proposed an authentication protocol with high efficiency for smart grid, but their protocol does not provide anonymity since the real identity of smart meter is transmitted over the open channel in wireless network. They proposed a different anonymous key agreement protocol for the smart grid edge computing. However, smart meters are unable to verify the legitimacy of unity control, protocol is unable to achieve mutual authentication.

2.5.10. Key management and authentication strategy.

Kahvazadeh et al. (2018) proposed a key management and authentication strategy for the edge cloud computing model. Every device authenticates to a control-area unit (CAU) that has been authorized, as opposed to the centralized cloud. According to this model, the devices don't verify the legitimacy of the cloud or CAU, which are regarded as trustworthy. Moreover, the protocol does not achieve device anonymity and revocation; thus, limiting its utility in a smart grid system.

2.5.11. Summary of proposed blockchain solutions.

The table below summarises the reviewed related literature aimed blockchain-based, edge IoT's within the smart grid infrastructure.

Table I: Summary of Reviewed Related Literature Proposed Solutions

Reference	Proposed Solution	Advantage	Drawback
Jamader et al., (2022)	BCIoT framework	High availability	Malicious and non-malicious data are kept together.
Hayat et al. (2022)	Ethereum blockchain	Authorized legitimate server	IP spoofing, Tremendous computational power
Rehman et al., (2020)	SC and BC extension	Data integrity	It's not scalable
Jiang et al., 2020	BSD-Guard	Secures the control and data planes	Resource hungry

Songlin et al., (2019)	Laplace mechanism and Gaussian mechanism.	High availability	Scalability
Yang, B et al., (2021)	Blockchain powered secure access control scheme with fair accountability.	Data integrity and scalability	More overhead
Kumar et al., (2018)	Key agreement protocol (LAKA)	Mutual authentication	Single secret cryptographic key
Jing, W., and Libing, W. (2020)	Mutual authentication and key agreement protocol	It ensures trust identity among IoT devices	Least cryptographic operations
Mahmood et al. (2018)	Authentication protocol	High efficiency	No anonymity, less secure.
Kahvazadeh et al. (2018)	Key management and authentication strategy	Mutual authentication	No anonymity and revocation.

2.6. Analysis of the Solutions

Hyperledger Fabric offers a robust solution for enhancing data security in smart grid edge IoT devices through its permissioned blockchain architecture. By ensuring that only authorized entities can participate in the network, it provides a secure and tamper-proof ledger for recording transactions and data exchanges between IoT devices. The modularity of Hyperledger Fabric allows for tailored consensus mechanisms, privacy controls, and access management, which are critical for the complex and varied security requirements of smart grids. Furthermore, its ability to create private channels enables sensitive information to be shared securely among specific parties, mitigating the risks associated with data breaches and unauthorized access. This decentralized approach not only enhances data integrity and traceability but also ensures real-time transparency and auditability, making Hyperledger Fabric an ideal choice for securing the data ecosystem of smart grid edge IoT devices.

2.6.1. Benefits of Blockchain Technologies

Blockchain technology can offer several advantages for developing secure and optimized infrastructure, including in the energy sector. By leveraging the distributed ledger, blockchain can help create a dynamic market structure and facilitate the development of modern energy grids (Ata et al., 2023). According to Selvi (2023) one of the main goals of using blockchain in this context is to prevent cyberattacks and provide a stable backbone for implementing consensual market mechanisms. When used as a distribution ledger and mediator, a blockchain-based smart grid can offer several benefits, including (Okazaki, 2018):

- Providing credibility and truthfulness by using an unaltered chain of blocks stored in the distribution ledger as an immutable record of transactions.
- Enabling autonomous revealing of data irregularities, as any unapproved attempt is logged and documented due to blockchain's transparency attribute.
- Ensuring energy data and transactions go through various consensual terms and verification before being appended inside the blocks, making the system more resilient.
- Allowing for real-time settlement using micropayment, which is a game-changing attribute of blockchain-based smart grids.
- Facilitating the energy market by deploying smart contracts autonomously when specified conditions are met and satisfying all parties involved.

Performing functionalities like ensuring unaltered and valid data through consensus, making it impossible to replace, authenticating all users connected to the grid with smart meters, and creating a robust network where all attacks are very expensive for the attacker (Malik, 2019).

Blockchain technology is making waves in the energy sector, with many experts and businesses hailing it as a potential solution to the challenges faced by modern energy grids (Aklilu & Ding, 2022). The use of blockchain in this sector is still in its infancy, but there are already many use cases where blockchain can offer significant advantages over traditional centralized systems. One of the most promising use cases for blockchain in the energy sector is in billing. Blockchain-based smart grids can use smart contracts and smart meters to generate automated billing and metering for both prosumers and consumers (Hasan et al., 2022). Micropayments are also becoming an essential part of the grid, with solutions like pay-as-you-go and pre-paid meters being implemented. These micropayments enable consumers to purchase energy in small increments, making it more affordable and accessible for low-income households (Xie et al., 2018).

Another promising use case for blockchain in the energy sector is in trade and marketing. Blockchain in combination with Machine Learning (ML) and Artificial Intelligence (AI) can change the marketing world by using consumers and prosumers' usage profile, individual preferences, and environmental concerns (Mazhar, Irfan, Haq, et al., 2023). Blockchain-supported distributed platforms allow for efficient market payment and trading functions and are currently being used for green certificates trading. By using blockchain, energy trading can become more secure, transparent, and efficient (Akkad et al., 2023).

Automation is another area where blockchain can have a significant impact (Bodkhe et al., 2020). The ability of blockchain to execute peer-to-peer (P2P) energy trading and to regulate decentralized smart grids can significantly improve energy production by local energy providers and provide accurate consumption using behind the meter activities (Hasan et al., 2022). This means that communities can generate their own energy and trade it with others without the need for a central authority to manage the process (Dai & Wang, 2020).

Smart grid data applications are also an area where blockchain can have a significant impact (Kim et al., 2022). A blockchain-based smart grid is a grid with a combination of blockchain, smart meters, advanced monitoring and control, micropayments, energy storage, and management system (Aklilu & Ding, 2022). By using blockchain, it is possible to collect, and analyses large amounts of data generated by these systems, enabling real-time monitoring and optimization of energy production and consumption (Malik, 2019).

Security and transparency are two other areas where blockchain can provide significant advantages over traditional centralized systems (Akkad et al., 2023). Blockchain can provide cryptographic-secured data logged inside blocks that cannot be altered retrospectively. On top of that, all the data records are immutable and transparent, making it easier to detect any fraudulent or unauthorized activities on the grid (Hasan et al., 2022).

Blockchain technology has the potential to revolutionize modern energy grids by providing a secure, transparent, and efficient way to manage energy production and consumption (Hasan et al., 2022). With many promising use cases already being explored, it is only a matter of time before we see blockchain-based smart grids becoming the norm in the energy sector (Dai & Wang, 2020).

2.6.2. Edge computing and blockchain technologies

C. Luo et al. (2020) portrayed that edge computing is proposed as a means of improving the performance of existing centralised cloud computing. Edge computing has been widely deployed in IoT networks during the previous decade (Alzoubi & Aljaafreh, 2023). Edge computing can increase the security of sensitive information when compared to cloud computing, but it still has various security issues, such as authentication of IoT devices and edge servers, and malicious attacks (Q. Luo et al., 2020). Compared with the current cloud computing, edge computing has many advantages: low latency, scalability, effective use of resources and privacy security (Mansouri, 2021). The data produced by IoT devices is partitioned into several portions and stored in many edge servers situated in various places, making it difficult to ensure data integrity (Alzoubi & Aljaafreh, 2023). The security and privacy issues in edge computing architecture, such as authentication, intrusion detection, access control, and so on, are difficult to resolve (Xue et al., 2022). They observed that the integration of blockchain technologies and edge computing is becoming an excellent way for addressing these issues. The advancement of blockchain technology can tackle security issues related to immutability and general resistance to attacks, as well as provide a decentralised shared data storage system that enables the network to be permissionless and censorship-resistant in edge computing (C. Luo et al., 2020).

2.7. 2.7 Enhancing data security of the edge IoT devices in the smart grid.

2.7.1. 2.7.1 Access Control List (ACL)

By regulating access to network resources, ACLs contribute to maintaining system availability and preventing potential disruptions caused by unauthorized or malicious activities within the distributed edge computing environment.(Kim et al., 2023). Studies have demonstrated the effectiveness of ACLs in mitigating DoS attacks in various network environments. For example, the research by Yan et al. (2020) highlights that ACLs, when configured properly, can significantly reduce the attack surface by limiting the exposure of network resources to potential attackers. In blockchain-powered smart grids ACLs can be configured to allow only verified nodes to communicate with the network, thereby preventing unauthorized traffic that could lead to DoS attacks.

2.7.2. Secure Sockets Layer and Transport Layer Security (SSL/TLS).

Secure Socket Layer (SSL) and Transport Layer Security (TLS) can be integrated with HTTP protocol to primarily address confidentiality and integrity aspects in data transmission. These protocols encrypt data during transit, ensuring that it remains confidential and inaccessible to unauthorized entities while preventing tampering or alteration, thereby maintaining data integrity (Pandey et al., 2023). Both SSL and TLS protocols employ cryptographic techniques to secure communication channels, making them crucial for preserving the confidentiality and integrity of sensitive information exchanged between edge devices and blockchain nodes (KPMG, 2021). Transmission of data between two communicating applications can be securely encrypted using TLS/SSL, which implies that unauthorized parties cannot read the data even if it is intercepted (Herberg, 2022). Encryption aids in preventing interceptions and eavesdropping on confidential data. This guarantees the authenticity and reliability of the transmitted data since any tampering or alteration can be detected by the receiving party during transmission (Herzberg, 2022).

Forward secrecy, a feature of TLS/SSL protocols, prevents previous communications from being decrypted, even in the event that the server's private key is compromised (Paris et al., 2023). This provides an additional degree of security, especially for long-term data storage. Like any technology, TLS/SSL has security weaknesses and vulnerabilities. It is essential to keep SSL and TLS implementations and configurations up to date and patch frequently in order to mitigate known vulnerabilities and associated risks. While encryption adds a layer of security, it can also introduce overhead, impacting the performance of communication (Prantl et al., 2021). Nonetheless, security advantages typically surpass the marginal performance penalty, as contemporary TLS implementations are tuned to reduce this effect.

2.7.3. Role-Based Access Control (RBAC).

In the context of IoT and smart grids, RBAC can limit the permissions of devices and users, thereby reducing the risk of unauthorized firmware modifications (Yang et al., 2019). Integrating RBAC with blockchain technology enhances security measures. Blockchain's immutable ledger can record all access attempts and modifications, enabling real-time monitoring and auditing of RBAC policies (Gai et al., 2021). Despite its benefits, the implementation of RBAC in blockchain-based smart grids faces challenges such as scalability and the complexity of managing numerous roles and permissions (Hu et al., 2020). RBAC provides a robust framework for mitigating firmware exploit attacks in blockchain-based smart grid edge IoT devices.

2.7.4. ECC and digital signatures.

Cryptographic protocols such as Elliptic Curve Cryptography (ECC) and digital signatures also contribute to ensuring confidentiality and integrity by facilitating identity verification and data authentication, they primarily serve as foundational elements for securing transactions and validating the integrity of data stored on the blockchain ledger (KPMG, 2021). These cryptographic protocols play a crucial role in maintaining the integrity of data transactions and verifying the authenticity of participants, thereby. Elliptic Curve Cryptography offers a prominent level of security with shorter key lengths compared to other asymmetric encryption algorithms such as RSA (Zhang et al., 2022). They highlighted that ECC tends to be ideal for environments with limited computational resources, such as mobile and IoT devices. As a result of rapid cryptographic operations that ensue, ECC is a suitable match for applications that need high-performance encryption. ECC supports forward secrecy, making sure that previous communications stay safe even in the event that an intruder manages to obtain a private key. This ensures that the signed data does not change while it is being transmitted or stored. Digital signature operations are computationally efficient, allowing for rapid signing and verification processes even for large datasets.

2.7.5. Summary

The literature review provides a comprehensive examination of the security challenges posed by IoT devices in the smart grid infrastructure, emphasizing the increasing vulnerability to cyber threats due to the widespread adoption of these devices. It discusses various security vulnerabilities such as denial-of-service attacks, insecure protocols, and firmware exploits, illustrating their potential to disrupt critical infrastructure and compromise data integrity in edge IoT. Additionally, the review evaluates proposed security solutions, including blockchain frameworks, authentication protocols, and cryptographic mechanisms, analysing their effectiveness in mitigating these threats. The findings underscore the urgency of implementing robust security measures such as blockchain to protect smart grid systems and highlight the need for continued research and innovation in developing resilient cybersecurity solutions tailored to the unique challenges of IoT devices in critical infrastructure environments.

Next chapter discusses the methodology used for this research.

3. CHAPTER 3: RESEARCH METHODOLOGY

3.1. Introduction

This chapter describes the research methodology undertaken in this research. The research was carried out using a systematic literature review approach incorporating qualitative and experimental methods. The first section outlines the four objectives which highlight what needed to be achieved in this research. Following, is the description of how systematic literature reviews were carried out. Finally, the chapter describes experiments carried out, to evaluate if enhanced blockchain layer enhances data security of edge IoT device.

3.2. Research objectives and questions

Table 3.1 lists the research objectives, research questions used during the study, it highlights the research strategy applied and data collection tools used.

Table II: Research Objectives and Questions

Main Research Objective	Main Research Question	Research Strategy	Data Collection and Analysis Tools
The primary objective of this research is to design a blockchain layer to address various security problems in smart grid edge IoT devices to enhance data security.	How can a blockchain layer be designed to address various security problems in smart grid edge IoT devices to enhance data security?	Simulation	Systematic literature review, Hyperledger Fabric
Sub-objective	Sub-objective questions		
To investigate edge IoT security threats in the smart grid	What are the edge IoT security threats in the smart grid?	Qualitative	Literature review

To analyze the existing deployment of blockchain layer in distributed edge computing.	What are the various deployments of blockchain layer in distributed edge computing?	Qualitative	Literature review
Enhance Hyperledger with lightweight security protocols.	Which lightweight security protocols can be built into Hyperledger to work with IoT devices	Qualitative	Literature review
Evaluate if enhanced blockchain layer enhances data security of IoT device	How does the proposed blockchain layer improve data security?	Experiment (Simulation)	Hyperledger Fabric

Following are the steps taken to achieve the research sub-objectives stated in Table 3.1.

3.3. Investigate edge IoT security threats in the SG.

To investigate edge IoT security threats in the smart grid a qualitative research investigation was undertaken using systematic literature review. Through this methodological approach, a wealth of insights from published documents, academic papers, and industry reports relevant to IoT security threats within the smart grid ecosystem were synthesized. By systematically reviewing diverse sources, the researcher endeavored to capture a nuanced understanding of the multifaceted challenges and vulnerabilities inherent in the intersection of IoT devices and smart grid infrastructure (Johnsson & Nordling, 2023). The data collection analyzed relevant literature to extract valuable insights regarding the spectrum of security threats found in edge IoT devices in the smart grid.

Upon collecting the data, the analysis was carried out using a thematic approach to distill common patterns and emerging trends in IoT security threats within the smart grid domain. Thematic analysis serves as a robust framework for identifying prevalent issues that pose significant risks to data security and system integrity (Rosairo, 2023). By scrutinizing the literature through this lens, the researcher seeked to delineate key themes and recurring patterns, shedding light on the root causes and manifestations of security vulnerabilities across various facets of the smart grid infrastructure. Furthermore, the analysis endeavored to discern and categorize threats based on their relevance to the study's overarching goal of enhancing data security within the smart grid context (Rosairo, 2023).

The systematic literature review to find security threats in edge IoT was carried out as follows:

1. Downloaded articles from digital libraries and databases, including Google Scholar, IEEE, ACM, and semantic scholar.
2. Keywords used to search for articles: Smart Grid, IoT, cyber threats.
3. Selected papers:
    a. Published from 2018 to 2023
    b. Titles and abstracts.
    c. With IoT security threats outlined, statistics, impacts in smart grid.
4. Researcher stopped collecting papers when saturation point was reached. That is to say when the researcher started obtaining papers with same information already gathered from other papers. The researcher stopped analyzing more papers.
5. Summarized security threats from the selected articles.
6. Identified the most severe threats that effects IoT environments in smart grid. outlined in section 2.3.

Results of the systematic literature review are found in (section 2.3).

3.4. Analyze existing deployment of blockchain layer in distributed edge computing.

The researcher conducted a systematic literature and thematic analysis review similar to the one described in section 3.3 to compile a comprehensive data on blockchain deployments in distributed edge computing environments.

To find out about existing deployment of blockchain layer the following steps were taken.

1. Downloaded articles from digital libraries and databases, including Google Scholar, IEEE, ACM, and semantic scholar.

2. Keywords used to search for articles: Blockchain, Ethereum, Corda, Hyperledger
3. Selected papers:
    a. Published from 2018 to 2023
    b. Titles and abstracts.
    c. With blockchain technology implementation, open-source deployment, scalable, and which can be integrated with edge computing.
4. The researcher summarized selected blockchain technologies. Found in section 2.4.
5. Identified Hyperledger fabric as the best blockchain technology for the study.
6. Results of the systematic literature review are found in (section 2.6).

3.5. Enhance Hyperledger with lightweight security protocols.

The researcher again conducted a systematic literature review similar to the one in section 3.3 and section 3.4, by integrating insights from academic papers, published case studies and simulations scenarios to identify and analyze lightweight security protocols suitable for the IoT edge environments.

To find out about the lightweight security protocols to be used to enhance blockchain security the following steps were taken.

1. Downloaded articles from digital libraries and databases, including Google Scholar, IEEE, ACM, and semantic scholar.
2. Keywords used to search for articles: Blockchain lightweight security protocols.
3. Selected papers:
    a. Published from 2018 to 2023
    b. Titles and abstracts
    c. With lightweight security protocols that can be considered for IoT edge environments,
4. The researcher summarized details of lightweight security protocol found.
5. Identified TLS/SSL, ACL's and RBAC meet the requirement for the experiment. Found in section 2.7.
6. Results of the experiment found in section 4.

3.6. Evaluate if enhanced blockchain layer enhances data security of IoT device.

A simulated experiment was conducted to evaluate the security of edge IoT devices and the success rate of incorporating lightweight security protocols to mitigate threats mentioned in section 3.3.

A research experiment is a systematic and scientific procedure for testing hypotheses by influencing and controlling variables to observe their effects on a particular outcome. Researchers use experiments to establish cause-and-effect relationships, gather empirical data, and validate or refute theoretical predictions. A simulated environment is a controlled and artificial setup created to mimic real-world conditions for scientific research.

Using an experiment and a simulated environment is ideal for this study because it provides a real-world validation, stress testing, flexibility, repeatability and eliminates the risk of damaging real devices or disrupting actual smart grid operations during testing. This approach enables to gather authentic data and assess the practical implication of theories. On the other hand, simulated approach offers a controlled and versatile setting to explore different scenarios that may be difficult, costly, or ethically challenging to replicate in real life.

3.6.1. Testing environment setup

To achieve this objective an experiment was undertaken in a simulated environment.
A controlled testing simulating a real-world IoT deployments was setup. This environment comprised various components, including IoT devices, edge computing infrastructure, communication networks, Curl, Docker, Docker Compose, GO, PYTHON, Node.js and NPM, UBUNTU and ORACLE virtual machine. The researcher ensured that the testing environment closely mirrors the complexities and configurations of actual IoT ecosystems to generate realistic evaluation results (Halldén, 2022). Figure 3.1 depicts the simulated logical network and Figure 3.2 depicts an actual IoT ecosystem. Figure 3.2 is included to show that the simulated network shown in Figure 3.1 simulates an actual IoT ecosystem to a very good degree.

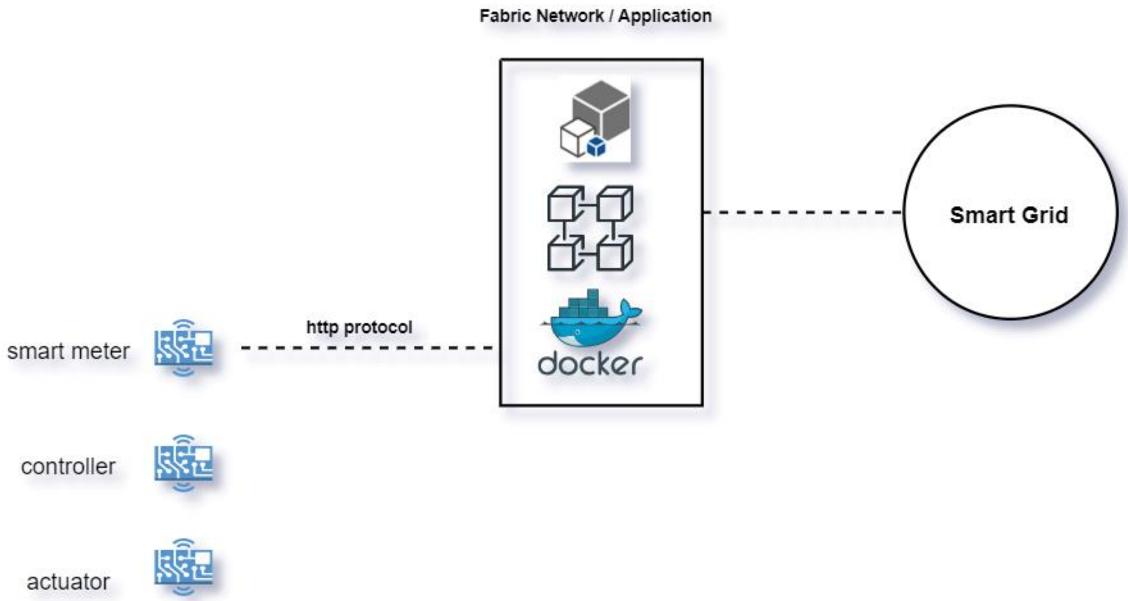


Figure 3.1 Simulated logical network

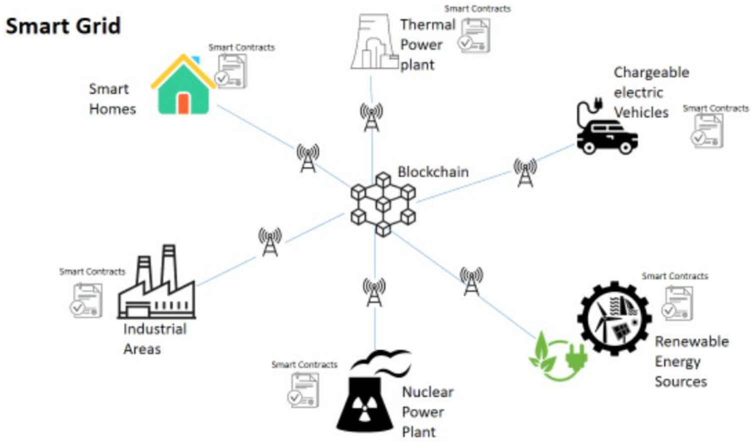


Figure 3.2 Blockchain in smart grid (Arjomand et al., 2020)

3.6.2. Initial testing

To establish a baseline of the impact of attacks on edge IoT devices without lightweight security protocols configured, several attack tests were carried out. The attacks were carried out as follows:

a. To carry out a DoS attack, malicious traffic were generated and flooded into the Hyperledger Fabric network using hping3. The results were captured using Tcpdump and pings to identify and analyze traffic patterns.
b. To carry out a sniffing attack Wireshark was used for packet sniffing and capturing data in motion.
c. To carry out a firmware exploitation, Metasploit was used to exploit the Raspberry Pi device.

3.6.3. Testing after lightweight security protocols and other measures applied to blockchain layer.

The researcher added TLS/SSL, ACL's and RBAC as lightweight protocols to secure the network from attacks ran in section 3.6. These lightweight security protocols were selected according to results obtained after the literature search described in section 3.5. SSL/TLS was used to guarantee privacy by encrypting data, ACL was employed to assure availability using IP tables, and RBAC was implemented to uphold data integrity by controlling and limiting privilege escalation. Thereafter, same attacks as described in section 3.6.2 were repeated to test whether the network will be more secured after all the security enhancements were implemented.

3.7. Chapter Summary

This chapter outlined the methodology followed to carry out this research. The chapter outlines how the four sub-objectives of this research were attained. The first three sub-objectives were attained by carrying out systematic literature reviews. The fourth sub-objective was attained by simulating edge-IoT in the smart grid. The simulated environment was used to demonstrate effects of attacks on edge-IoT in the smart grid before a blockchain layer is implemented and effects of attacks edge-IoT in smart grid after a blockchain layer is implemented. The detailed systematic literature review results are found in chapter 2. Chapter Four briefly summarizes systematic literature review results and the simulation results.

4. CHAPTER 4: RESULTS AND ANALYSIS

4.1. Introduction

This chapter presents the simulation results accompanied by an analysis of the results. The results were obtained from assessing the performance of the security protocol and strategies implemented in Hyperledger grid fabric (the blockchain layer). Through experiments the efficacy and robustness of the security measures were scrutinized in a simulated scenario. Key metrics such as throughput, latency, security breaches, and overall system resilience were examined to gauge the effectiveness of the implemented security enhancements in the blockchain layer. The findings shaded light on throughput, latency, security breaches, and overall system resilience in the Hyperledger grid fabric ecosystem. The first section summarises the results of the first three research questions obtained through literature reviews.

This research asked the following questions:

1. What are the edge IoT security threats in the smart grid?
2. What are the various deployment of the blockchain layer in distributed edge computing?
3. Which lightweight security protocols can be built into Hyperledger to work with IoT devices?
4. How does the proposed blockchain layer improve data security?

4.2. Research question one findings.

A systematic literature review was conducted to answer research question one, which was:

What are the edge IoT security threats in the smart grid?

The systematic literature review unveiled a spectrum of security threats inherent in both smart grid and IoT edge devices (detailed analysis is section 2.3). Among these threats, Denial-of-Service (DoS) attacks emerged as a prominent concern, posing risks to critical services and system availability. Additionally, insecure protocols and firmware exploits were identified as significant threats, highlighting weaknesses in communication channels and device firmware. The identified threats were simulated to test the improved blockchain later in the research as described in section 3.6.

4.3. Research question two findings.

A systematic literature review was conducted to answer research question two, which was:

What are the various deployment of the blockchain layer in distributed edge computing?

The researcher scrutinized the effectiveness of blockchain frameworks in addressing data security issues and ensuring scalability in distributed edge computing environments.

After the review (section 2.4 and 2.6.), the researcher identified Hyperledger, Corda, Ethereum as possible edge IoT blockchain for data security enhancement. Hyperledger was selected to use in the simulations because it stands out for its suitability in distributed edge computing environments due to its modular architecture, robust security features, and scalability compared to other frameworks like Ethereum and Corda. Hyperledger offers greater flexibility and customization options, making it ideal for tailored solutions in edge computing scenarios. The choice of Hyperledger in this research reflects its reputation for enterprise-grade blockchain solutions and its alignment with the security and scalability requirements inherent in distributed edge computing environments.

4.4. Research question three findings.

A systematic literature review was conducted to answer research question three, which was:

Which lightweight security protocols can be built into Hyperledger to secure edge IoT devices.

Lightweight security protocols such as SSL /TLS, ACLs and RBAC were identified. SSL/TLS guarantees protected communication, ACLs limit network access, and RBAC manages user permissions, all working together to secure data on edge IoT devices. These lightweight security protocols were the ones considered when testing as discussed in section 3.6.3.

4.5. Research question four findings.

Research question four was:

How does the proposed blockchain layer improve data security?

Utilizing a systematic literature review approach, the study successfully analyzed the essential tools for the installation of Hyperledger Fabric through simulation. The simulation setup is described in the preceding sections.

4.6. Hyperledger installation

4.6.1. General installation

The goal of the permissioned blockchain platform Hyperledger Fabric is to offer a framework for creating blockchain applications of an enterprise caliber. Despite not radically altering the way data security functions, it does include a number of features and design fundamentals that enhance data security in a blockchain network through private channels, endorsement policy, cryptography, and granular access control. With the integration of these features Hyperledger Fabric offers a secure and adaptable framework for constructing enterprise blockchain solutions, particularly in situations where data security and privacy are critical considerations.

Hyperledger fabric was installed with integrated components such as Curl, Docker, Docker Compose, Go, Node.js and NPM, Python, gut config.

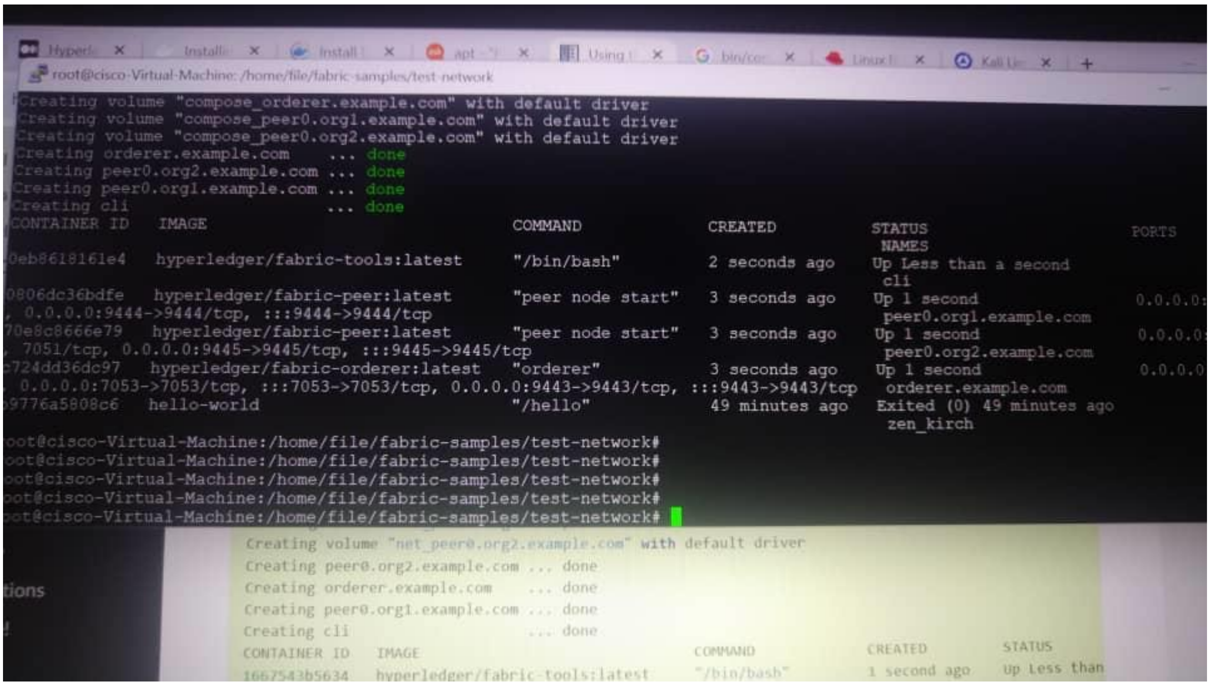


Figure 4.1 Installation of Hyperledger fabric on ubuntu

Figure 4.1 above illustrates the installation process of Hyperledger Fabric on an Ubuntu operating system. The screenshot provides a visual representation of the step-by-step procedure followed to install Hyperledger Fabric components, including peer nodes, orders, and the Fabric binaries necessary for network configuration and management. This installation process is crucial for establishing a functional Hyperledger Fabric network capable of supporting distributed ledger applications and smart contracts.

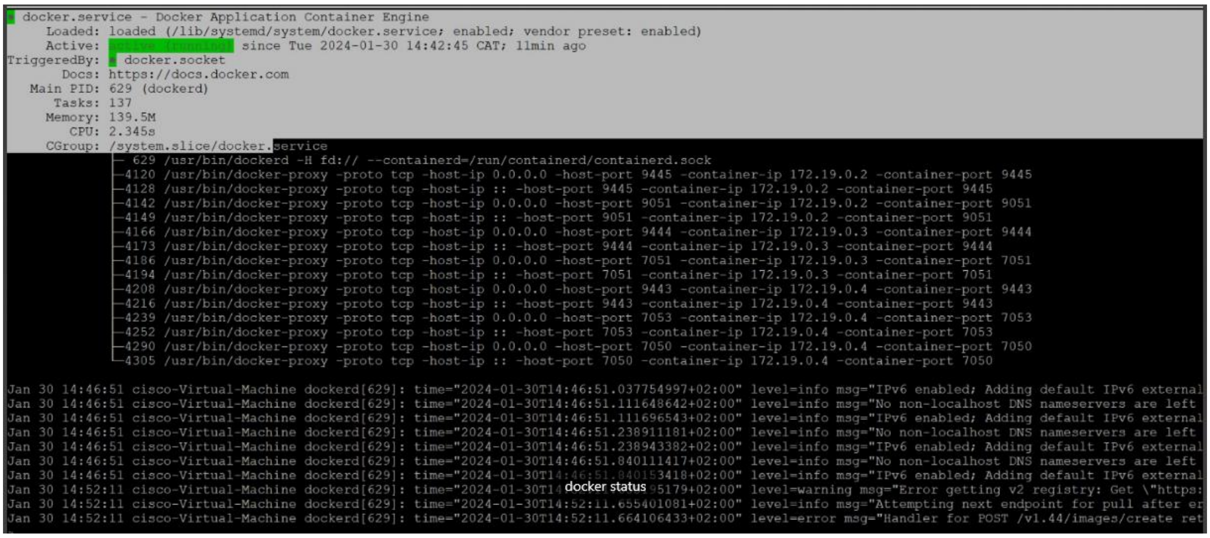


Figure 4.2 Creating Test network.

Figure 4.2 provides a visual representation of the Hyperledger test network running successfully on an Ubuntu system. The screenshot demonstrates the operational status of the Hyperledger Fabric network, indicating that all essential components, including peers, orders, and the network itself, are up and running as intended (marked in green). This confirmation is pivotal in validating the successful deployment and configuration of the Hyperledger Fabric network, ensuring that it is ready to support distributed ledger applications and smart contracts. The depiction in Figure 4.2 serves as tangible evidence of the network's functionality and readiness for further development and utilization within blockchain-based projects and applications.

4.6.2. CURL

In Hyperledger Fabric, the purpose of CURL is to interact with the Fabric network by sending HTTP/HTTPS requests to the network's APIs. CURL is a command-line tool commonly used to transfer data to or from a server, making it useful for interacting with RESTful APIs. When working with Hyperledger Fabric, CURL can be used to send enrollment requests to the Fabric Certificate Authority (CA) to create new user identities or enroll existing ones. This is typically done using the Fabric CA's enrollment endpoint. Furthermore, CURL can be used to send transaction requests to the Fabric network's endorsing peers. Figure 4.3 shows CURL installation.

```
root@SKVM:~# sudo apt install curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libcurl4
The following NEW packages will be installed:
  curl
The following packages will be upgraded:
  libcurl4
1 upgraded, 1 newly installed, 0 to remove and 196 not upgraded.
Need to get 194 kB/484 kB of archives.
After this operation, 459 kB of additional disk space will be used.
Do you want to continue? [Y/n] _
```

Figure 4.3 Installing CURL

4.6.3. Docker

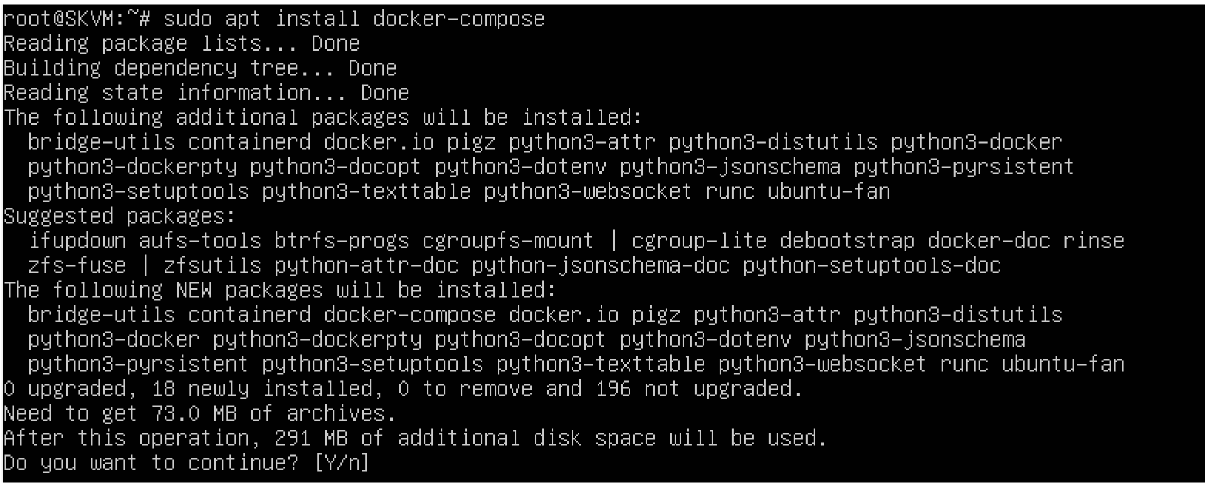
Docker provides containerization technology for Hyperledger Fabric framework. It helps in simplifying the deployment and management of the various components that make up a Hyperledger Fabric network. Docker enables the encapsulation of each component of a Hyperledger Fabric network, such as peers, orders, and chaincode, into separate containers. This modularity ensures that each component runs independently, with its own isolated environment and dependencies. It promotes better resource utilization and avoids conflicts between different components. Furthermore, Docker allows for consistent deployment across different environments, ensuring that the Hyperledger Fabric network functions uniformly regardless of the underlying infrastructure. Docker containers provide a standardized runtime environment, making it easier to move applications and networks between different development, testing, and production environments. Figure 4.4 shows Docker installation.

```
root@SKVM:~# sudo apt install docker
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  wmdocker
The following NEW packages will be installed:
  docker wmdocker
0 upgraded, 2 newly installed, 0 to remove and 198 not upgraded.
Need to get 14.3 kB of archives.
After this operation, 58.4 kB of additional disk space will be used.
Do you want to continue? [Y/n] _
```

Figure 4.4 Docker

4.6.4. Docker Compose

Docker Compose is a tool that allows one to define and manage multi-container applications using a simple YET ANOTHER MARKUP LANGUAGE (YAML) file. Docker Compose simplifies the configuration of a Hyperledger Fabric network by providing a declarative syntax to define the required components and their interdependencies. Instead of manually starting and connecting each container, you can specify the network topology, including peers, orders, and certificate authorities, in a single Compose file. One can quickly set up and tear down a Hyperledger Fabric network for development, testing, or demonstration purposes using Docker Compose. By defining the desired network configuration in the Compose file, you can easily spin up all the required containers with a single command. This streamlines the network deployment process, saving time and effort. Figure 4.5 shows Docker Compose installation.



```
root@SKVM:~# sudo apt install docker-compose
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bridge-utils containerd docker.io pigz python3-attr python3-distutils python3-docker
  python3-dockerpty python3-docopt python3-dotenv python3-jsonschema python3-pyrsistent
  python3-setuptools python3-texttable python3-websocket runc ubuntu-fan
Suggested packages:
  ifupdown aufs-tools btrfs-progs cgroupfs-mount | cgroup-lite debootstrap docker-doc rinse
  zfs-fuse | zfsutils python-attr-doc python-jsonschema-doc python-setuptools-doc
The following NEW packages will be installed:
  bridge-utils containerd docker-compose docker.io pigz python3-attr python3-distutils
  python3-docker python3-dockerpty python3-docopt python3-dotenv python3-jsonschema
  python3-pyrsistent python3-setuptools python3-texttable python3-websocket runc ubuntu-fan
0 upgraded, 18 newly installed, 0 to remove and 196 not upgraded.
Need to get 73.0 MB of archives.
After this operation, 291 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Figure 4.5 Docker Compose Installation

4.6.5. GO

In Hyperledger Fabric, Go is the primary programming language used for developing the core components of the Fabric framework. The purpose of Go in Hyperledger Fabric is to provide a performant and efficient language for implementing the various components of the Fabric network. Go is one of the supported programming languages for writing chaincode. Fabric's Go SDK provides the necessary libraries and interfaces for developing, deploying, and invoking Go-based chaincode. Go is used extensively in developing the core components of Hyperledger Fabric, such as peers, orders, and the Fabric Certificate Authority (CA). These components are responsible for managing the network, executing transactions, maintaining the ledger, and ensuring consensus among the network participants. By utilizing Go, Hyperledger

Fabric can achieve high-performance levels and scalability, making it suitable for enterprise-grade blockchain networks. Figure 4.6 shows GO installation.

```
root@SKVM:~# sudo apt install golang-go
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  golang-1.18-go golang-1.18-src golang-src pkg-config
Suggested packages:
  bzr | brz mercurial subversion
The following NEW packages will be installed:
  golang-1.18-go golang-1.18-src golang-go golang-src pkg-config
0 upgraded, 5 newly installed, 0 to remove and 197 not upgraded.
Need to get 82.4 MB of archives.
After this operation, 437 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Figure 4.6 GO installation

4.6.6. Node.js and NPM

Node.js is one of the supported programming languages for developing chaincode (smart contracts) in Hyperledger Fabric. Developers can use JavaScript and Node.js to write the business logic of their smart contracts. Node.js provides a familiar and widely used language for developing chaincode, making it accessible to a large community of developers. Node.js is often used to develop client applications that interact with the Fabric network. These applications can use the Fabric Node SDK, which provides a set of libraries and APIs for connecting to and interacting with the Fabric network. Node.js allows developers to create client applications that can invoke chaincode functions, query the ledger, and interact with various Fabric components.

```
test@test-VirtualBox: ~
test@test-VirtualBox:~$ sudo apt-get install nodejs
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  javascript-common libc-ares2 libjs-highlight.js libnode72 nodejs-doc
Suggested packages:
  apache2 | lighttpd | httpd npm
The following NEW packages will be installed:
  javascript-common libc-ares2 libjs-highlight.js libnode72 nodejs nodejs-doc
0 upgraded, 6 newly installed, 0 to remove and 64 not upgraded.
Need to get 13,7 MB of archives.
After this operation, 53,9 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Figure 4.7 Node.js installation

Figure 4.8 NPM installation

Node Packager Manager (NPM) is the package manager for Node.js, is widely used in the Node.js ecosystem, including Hyperledger Fabric. NPM allows developers to easily manage dependencies and packages required for their applications. In the context of Fabric, NPM is used to manage and install the necessary packages and libraries for developing and running Fabric-based applications. Node.js provides a rich ecosystem of tools, utilities, and frameworks that can be leveraged in the development of Fabric applications. These include testing frameworks, build tools, web frameworks, and more. Node.js enables developers to utilize the vast range of existing Node.js packages and tools to enhance their development workflow and productivity. Node.js is often used to integrate Fabric with web technologies and frameworks. For example, developers can use Node.js and frameworks like Express.js to build RESTful APIs that interact with the Fabric network. This allows for seamless integration between Fabric and web-based applications or front-end frameworks.

4.6.7. Python

Python is a popular programming language that serves various purposes within the Hyperledger Fabric ecosystem. Hyperledger Fabric allows the development of chaincode, which represents the smart contracts that define the business logic of the blockchain network. Python is one of the supported programming languages for writing chaincode. Developers can use Python to write the business logic for their smart contracts, making it easier to express complex algorithms and implement application-specific functionalities. Python provides software development kits (SDKs) and application programming interfaces (APIs) that enable developers to interact with Hyperledger Fabric networks with IoT devices. SDKs such as the Hyperledger Fabric Python SDK (fabric-sdk-py) provide abstractions and utility functions for connecting to, querying, and invoking transactions on the blockchain network. These SDKs simplify the integration of Python applications with Hyperledger Fabric. Figure 4.9 shows Python installation.

```
root@SKVM:~# sudo apt install python2.7
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libpython2.7-minimal libpython2.7-stdlib python2.7-minimal
Suggested packages:
  python2.7-doc binfmt-support
The following NEW packages will be installed:
  libpython2.7-minimal libpython2.7-stdlib python2.7 python2.7-minimal
0 upgraded, 4 newly installed, 0 to remove and 197 not upgraded.
Need to get 3,967 kB of archives.
After this operation, 16.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] _
```

Figure 4.9 Python

4.6.8. git config

This configuration enables Git to handle file paths that exceed the standard-length limitations of the operating system, even in Ubuntu. By setting core.longpaths to true, Git allows for longer file paths, preventing issues when working with complex or deeply nested directory structures in Hyperledger Fabric projects.

These Git configurations are not specific to the operating system but rather influence how Git handles certain aspects of version control. By configuring Git with core.autocrlf false and core.longpaths true, to ensure compatibility and smooth development processes when working with Hyperledger Fabric projects on Ubuntu.

After installation experiments as described in section 4.6 were carried out. Section 4.7 outlines the results that were obtained.

4.7. Experiments

As described in section 3.6 tests were carried out as follows:

- To carry out a DoS attack, malicious traffic was generated and flooded into the Hyperledger fabric network using hping3. The results were captured using Tcpdump and pings to identify and analyze traffic patterns.
- To carry out a sniffing attack, Wireshark was used for packet sniffing and capturing data in motion.
- To carry out firmware exploit, Metasploit was used to exploit raspberry pi os.

4.8. Before Lightweight Security Protocols were applied.

4.8.1. Denial-of-Service attack

Figure 4.10. shows a denial-of-service attack in progress to exhaust system resources using hping3 as outlined in Figure 4.10.

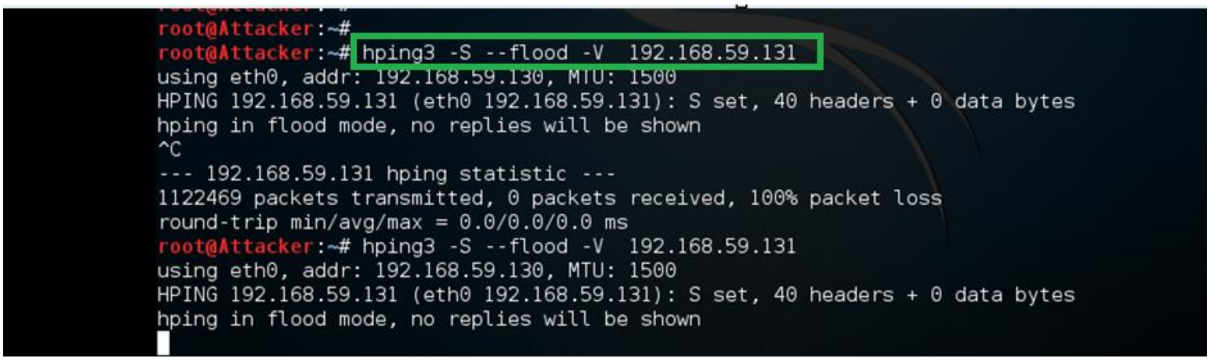


Figure 4.10 Denial-of-Service attack

Figure 4.11 highlights a live denial-of-service attack captured using Tcpdump. The results indicate that TCP flags are being exchanged between the raspberry pi device [192.168.59.131] and the attacker [192.168.59.130].

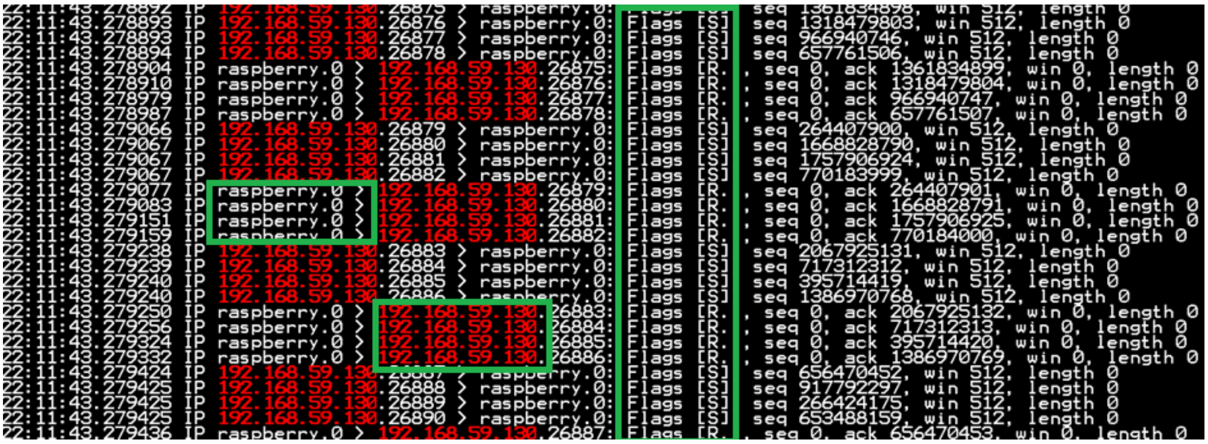


Figure 4.11 TCP Flags

The researcher observed abnormal network behaviour as milliseconds increased from 0ms to 146ms and a total of 174 bytes were sent and only 156 bytes were received which results into 10% packet loss due to massive network traffic flooded, as shown in Figure 4.12. This attack could have a significant impact on the smart grid, particularly if edge IoT devices are used to monitor or collect real-time data. As a result, users may experience service interruptions, downtime, or inability to access hosted resources. Figure 4.12, latency, and packet loss.

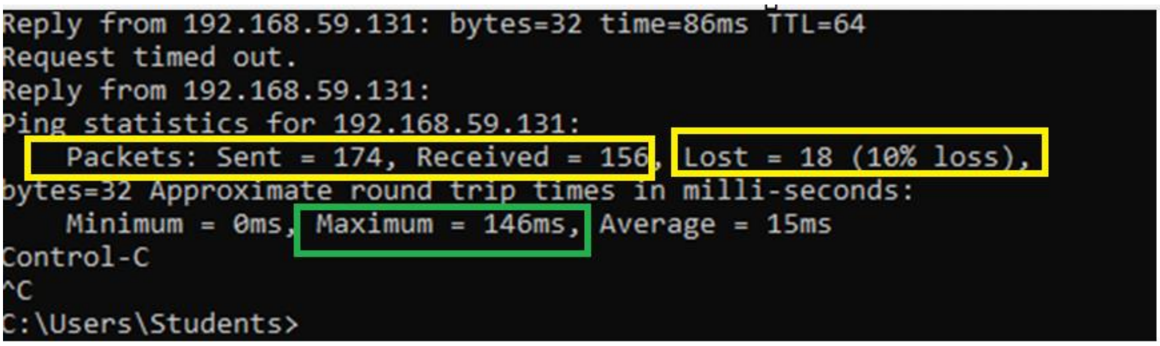


Figure 4.12 Network Metrics

Figure 4.13, illustrates network resource starvation results, caused by a denial-of-service attack. The recorded current network utilization is running at 8.30 Mbit/s as shown in Figure 4.13. This could impact performance and functionality of IoT devices such as causing network delays, congestions, excessive time, and energy attempting to establish and maintain network connections, leading to inefficient use of resources and decreased device lifespan.

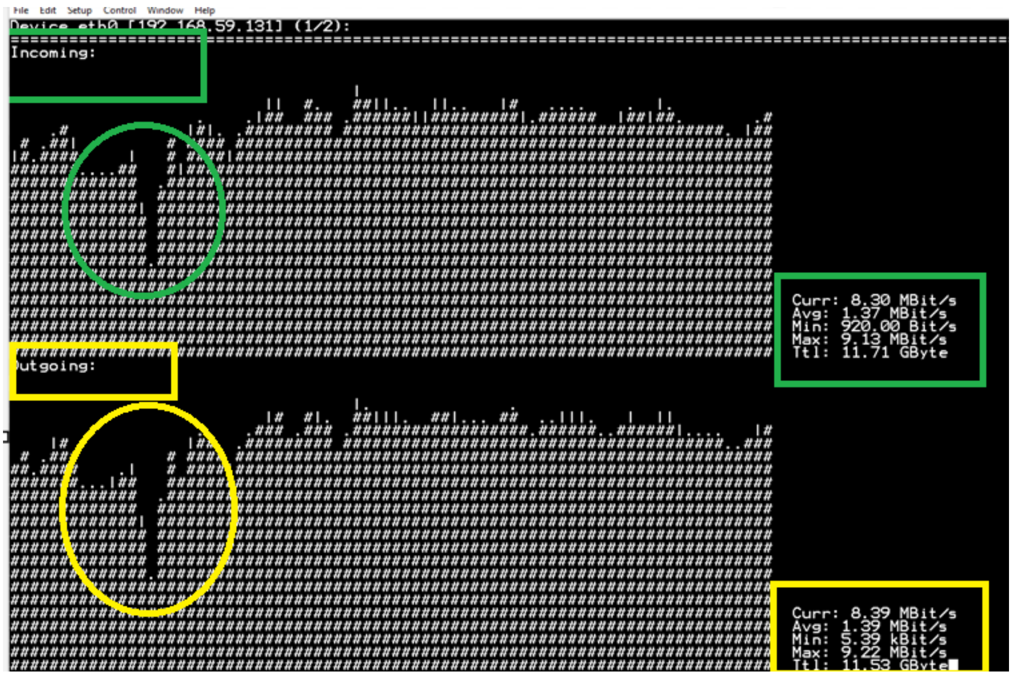


Figure 4.13 Network resource consumption

4.8.2. Packet Sniffing Attack

To illustrate packet sniffing, the researcher captured the credentials (username and password) using the interface shown in Figure 4.14 of a Raspberry Pi device to authenticate on the network.

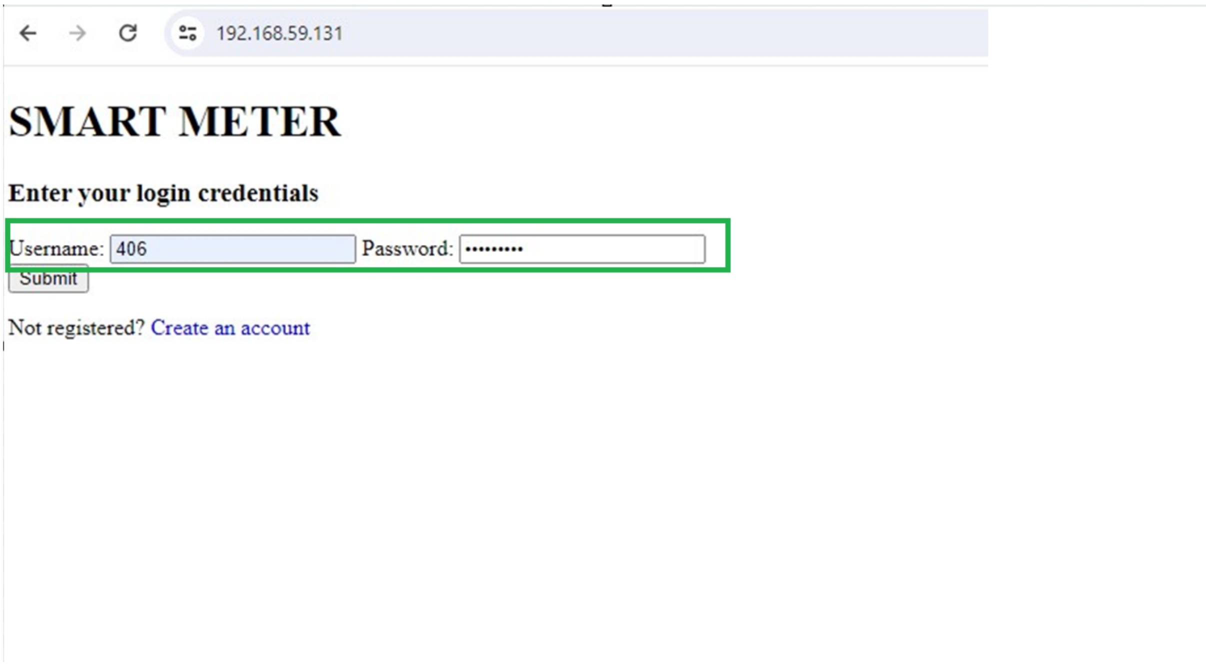


Figure 4.14 Raspberry Pi interface

Wireshark is used for sniffing to capture login credentials during the process of authentication as shown in Figure 4.15. User credentials were transmitted as plaintexts. The findings show that the attacker compromised data by using sniffing to obtain the login username and password.

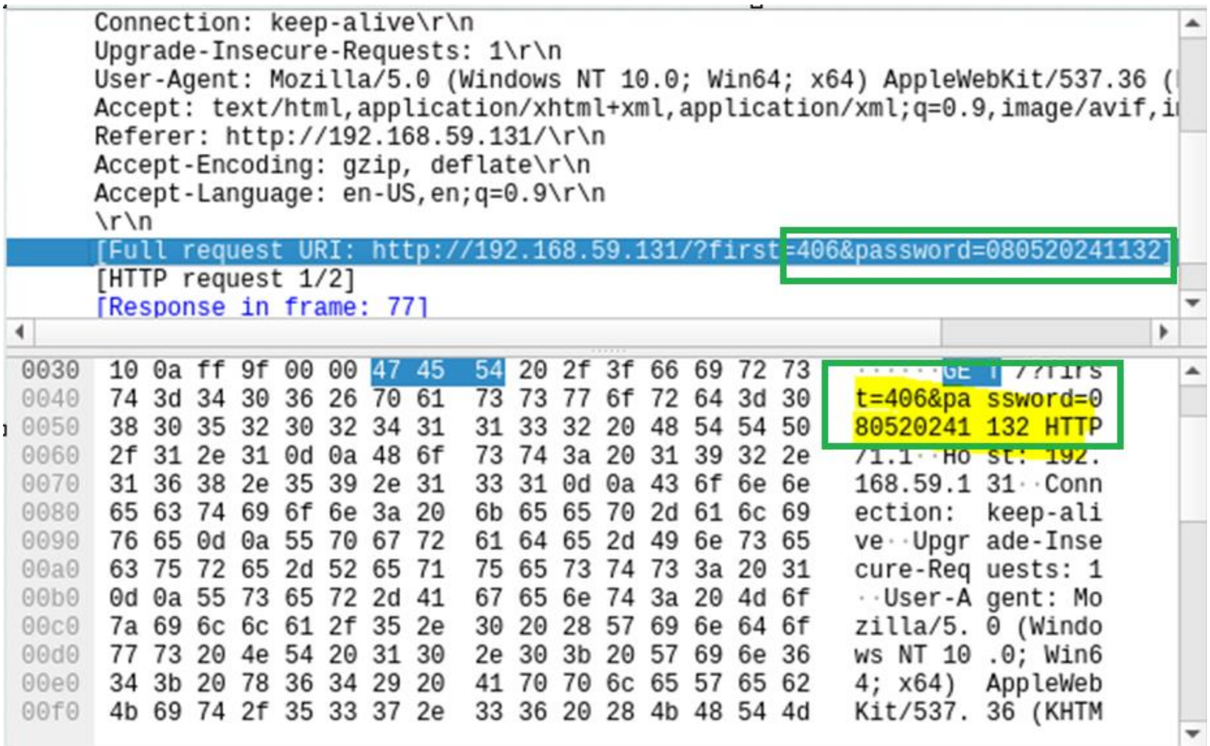


Figure 4.15 HTTP traffic

4.8.3. Firmware Exploit

A payload in Metasploit is used to leverage known vulnerabilities in the Raspberry Pi operating systems. Figure 4.16 signified that an attacker has successfully exploited the Raspberry Pi OS. The attacker gained full control over the device and could perform a wide range of malicious activities and escalate privileges.

Figure 4.16 outlined the meterpreter session gained by the attacker.

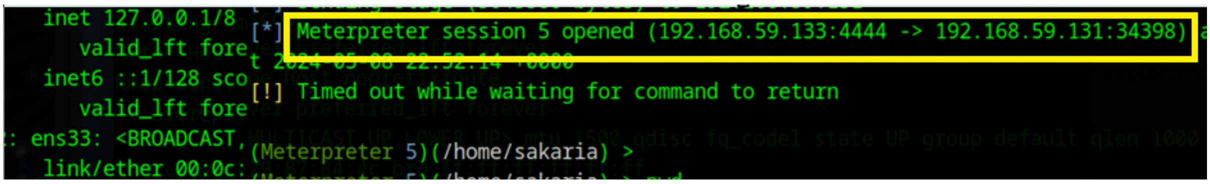


Figure 4.16 Meterpreter session

4.9. After Lightweight Security Protocols were applied.

As described in section 4.2 after the default tests on Hyperledger were carried, the researcher then enhanced its security capabilities by adding, ACL, SSL/TLS, and RBAC. The same experiments as in the previous section were carried and the results are outlined in the following sections.

4.9.1. Denial-of-service attack

Figure 4.17 showcases how IP tables, a component of Access Control, can be utilized to combat denial-of-service attacks. In this scenario, a deny rule is implemented targeting 192.168.59.130, effectively blocking malicious traffics, as depicted in Figure 4.17.

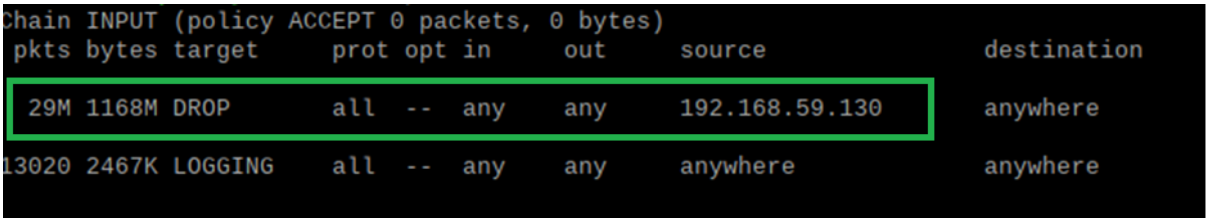


Figure 4.17: IP tables logs

A denial-of-service attack was executed to test the lightweight security protocol's efficacy, as depicted in Figure 4.18. In Figure 4.17, 1168M bytes were discarded.

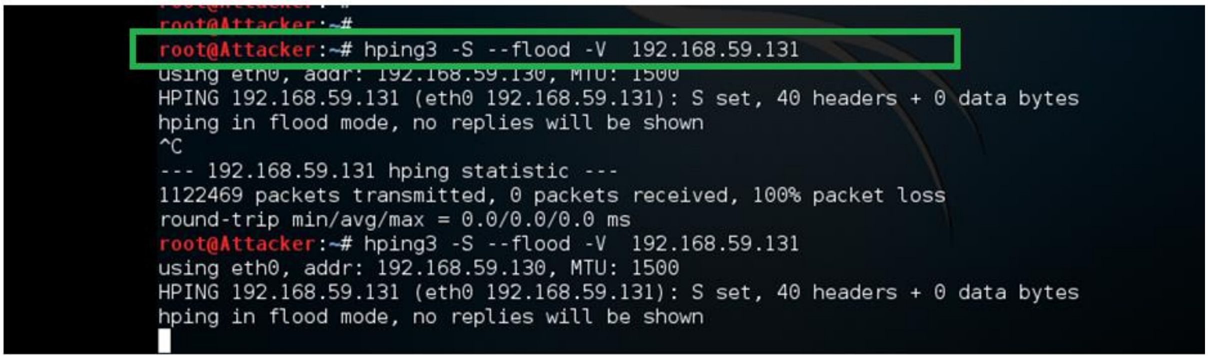


Figure 4.18 Denial-of-Service attack

Figure 4.19 depicts the reduction in network consumption achieved using ACL application, highlighting their impact on traffic patterns and resource usage. It underscores the importance of employing lightweight security protocols to address potential threats. Incoming network utilization decreased to 1.84 kBit/s, while outgoing utilization dropped to 12.67 kBit/s, as shown in the Figure 4.19.

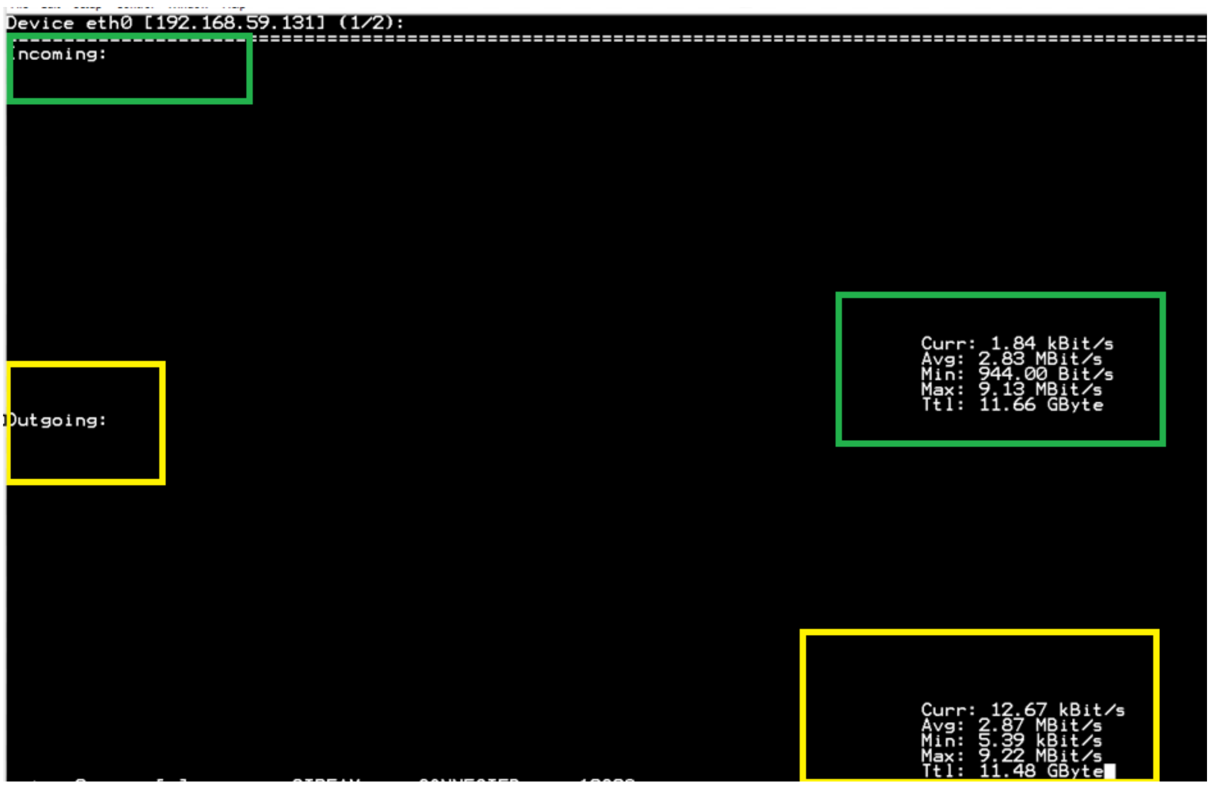


Figure 4.19 Network resource utilization

4.9.2. Packet Sniffing Attack

After implementing SSL and TLS in Hyperledger Fabric, a Wireshark sniffing attack proved unsuccessful. Only ciphertexts were accessible during the attack, as depicted in Figure 4.20. The attacker currently lacks knowledge of the username and password used by Raspberry device, which were previously visible in the HTTP traffic outlined in Figure 4.15.

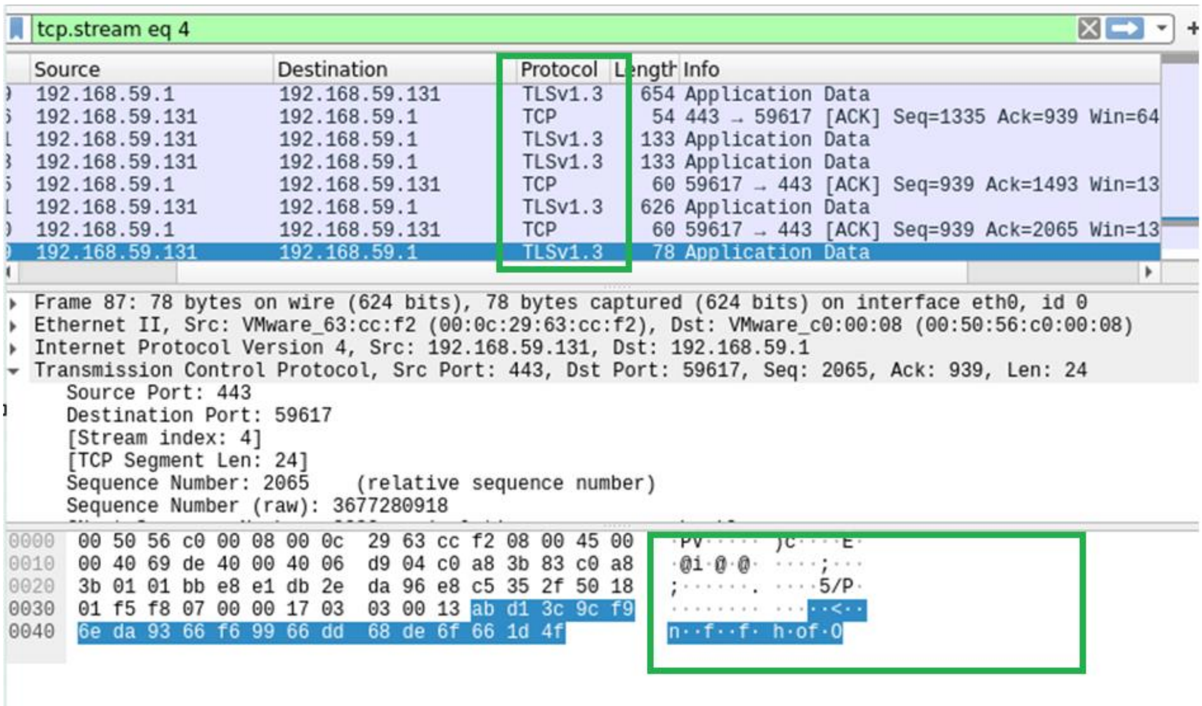


Figure 4.20 HTTPS traffic

4.9.3. Firmware Exploit

Figure 4.21 shows an updated version of the Raspberry Pi operating system. Which is part of hardening the operating system from known threats.

Figure 4.21 Latest version of raspberry pi os

The /tmp folder initially grants all permissions (read, write, and execute) by default. Attackers often exploit this directory to elevate privileges. To mitigate this risk, the researcher enforced RBAC to limit privilege escalation for both attackers and regular users. Specifically, the modifications outlined in Figure 4.22 restricted file permissions for the directory (sudo chmod 700 /tmp).

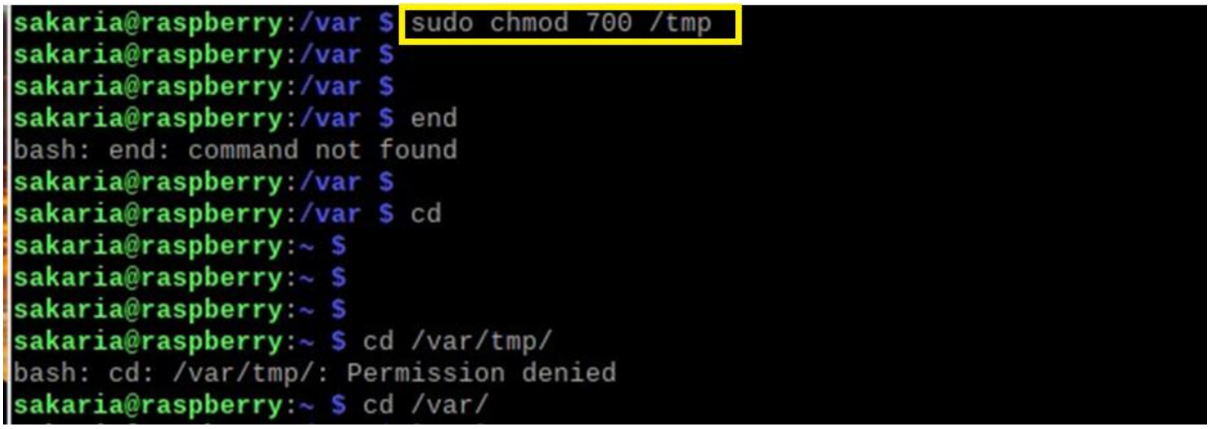


Figure 4.22 File permission

Figure 4.23 shows the outcome of applying "chmod 700" to the (tmp) directory. This command grants read, write, and execute permissions exclusively to the root user. The owner retains the ability to read, write, and execute files within the directory, while access is denied to other users, including group members and others, as depicted in the figure.

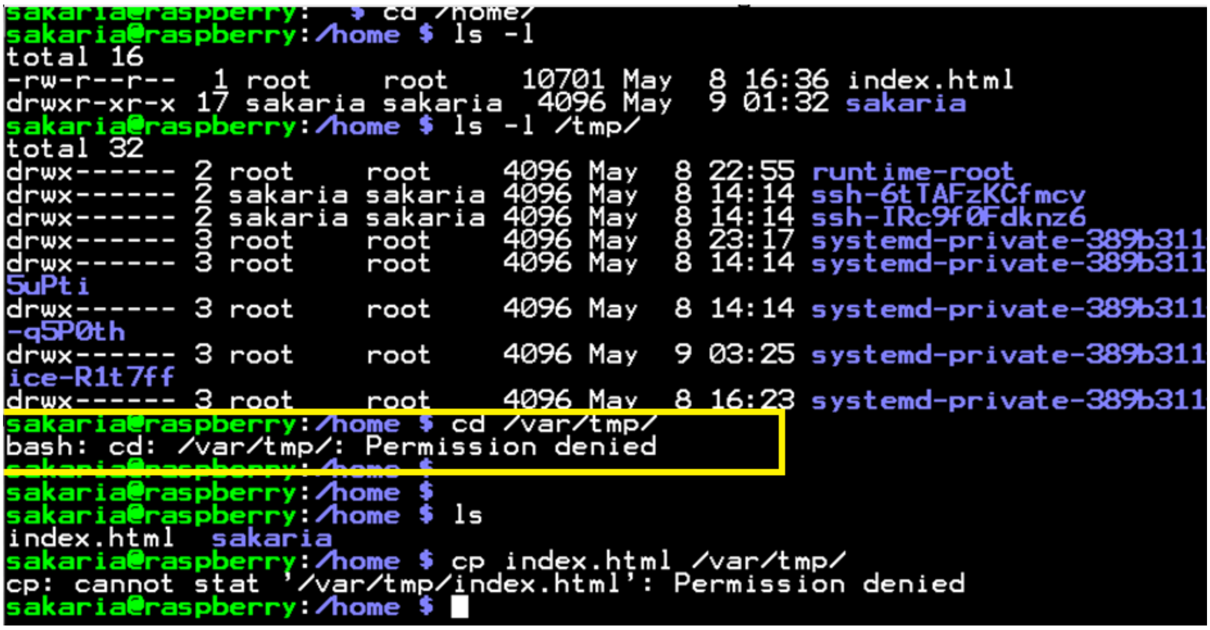


Figure 4.23 File permission 700 results

After updating the Raspberry Pi OS and enforcing RBAC, a firmware exploit was launched but failed, as detailed in Figure 4.24

Figure 4.24 Unsuccessful firmware exploit

The summary of results of the simulation experiment are shown in Table 5.1.

Table III: Summary of simulation experiment

Attack	Before lightweight security protocol applied	After lightweight security protocol applied
Denial-of-service attack	Network resource consumption incoming: ✓ Current: 8.39 Mbit/s ✓ Avg: 1.39 MBit/s ✓ Max: 9.22 MBit/s	Network resource consumption incoming: ✓ Current: 1.84 kBit.s ✓ Avg: 2.83 MBit/s ✓ Max: 9.13 Mbit/s

	✓ Ttl: 11:53 GBytes Network resource consumption outgoing: ✓ Current: 8.39 Mbit/s ✓ Avg: 1.39 Mbit/s ✓ Min: 5.39 kBit /s ✓ Max: 9.22 Mbit/s ✓ Ttl: 11:53 GBytes Packet loss 10% Highest latency 146ms	✓ Ttl: 11.66 Gbyte Network resource consumption outgoing: ✓ Curr: 12.67 kBit/s ✓ Avg: 2.87 MBit/s ✓ Min: 5.39 kBit/s ✓ Max: 9.22 MBit/s ✓ Ttl: 11.48 Gbyte Packet loss 0% Highest latency 1ms
Sniffing	Plain login credentials on the wire ID: 406 Password: 080520241132 Successful attack	Ciphertexts on the wire (HTTPS) Unsuccessful attack
Firmware exploit	• Outdate firmware. • Exploitable using Metasploit. • Access gained through meterpreter session.	• OS updated to the latest version. • User denied on /temp directory. • Unsuccessful firmware exploit with Metasploit

Figure 4.25 illustrates the incoming network resource consumption before and after applying lightweight security protocols. The data indicates that the current traffic flow dropped from 8.39 Mbit/s to 1.84 Kbit/s upon implementing the lightweight security protocol.

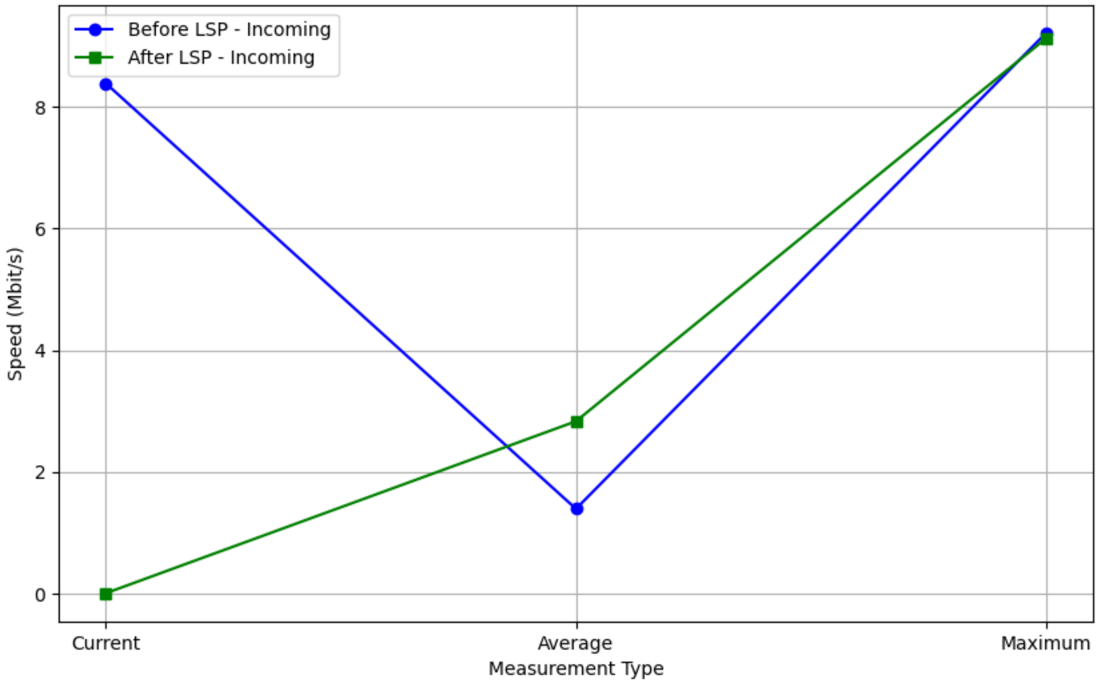


Figure 4.25 Incoming network resource consumption

Figure 4.26 illustrates the outgoing network resource consumption before and after applying lightweight security protocols. The data indicates that the current traffic flow dropped from 8.39 Mbit/s to 12.67 Kbit/s upon implementing the lightweight security protocol.

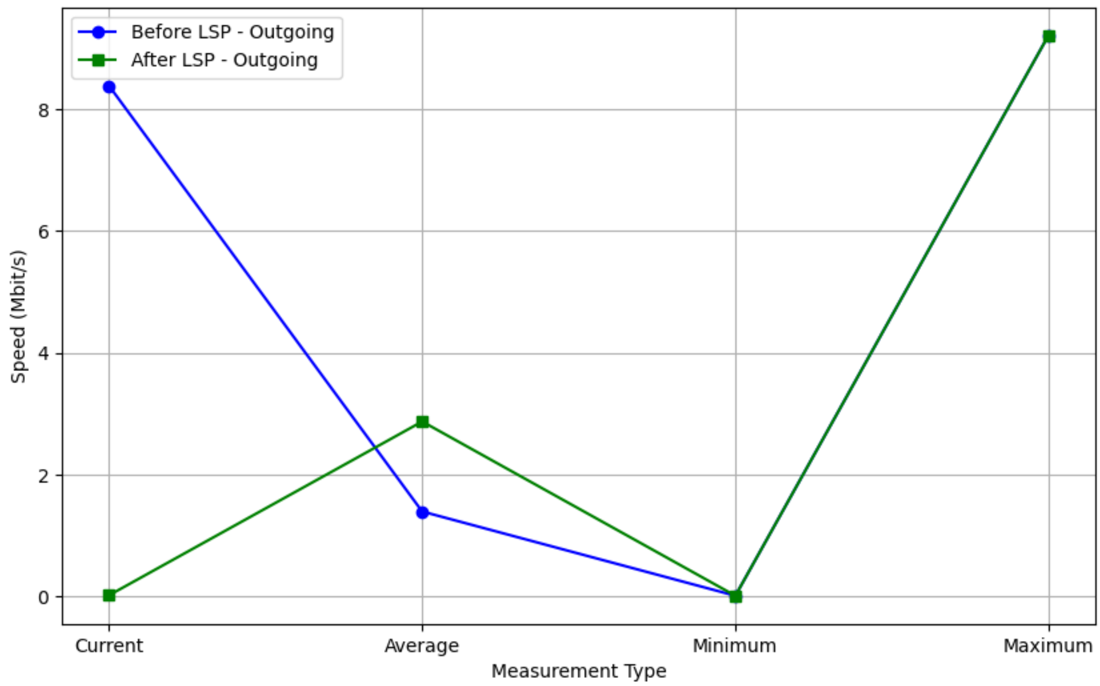


Figure 4.26 Outgoing network resource consumption

Figure 4.27 illustrates the impact of the lightweight security protocol on packet loss and latency. Before applying lightweight security protocol, there was 10% packet loss and a latency of 146 ms. However, after implementing the protocol, there was 0% packet loss and a latency of 1 ms, as depicted in Figure 4.27.

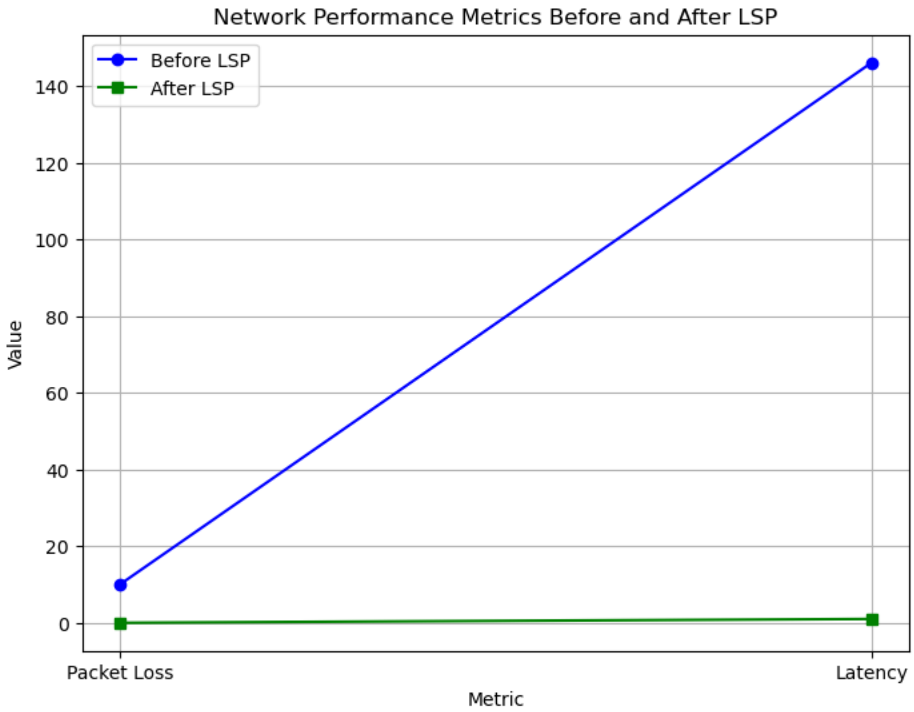


Figure 4.27 Network performance metrics

4.10. Discussion

Utilizing lightweight security protocols shows significant improvement to mitigate major threats targeting edge IoT device. Edge IoT devices have limited system resources which make them susceptible to denial-of-service attacks. The researcher implemented Access Control Lists (ACLs) within the blockchain layer to selectively filter the network and block malicious traffic that could overwhelm edge IoT devices. This finding emphasizes how important proactive network security measures in safeguarding IoT infrastructure from disruptive attacks. Subsequently, the nature of ACLs makes them well-suited for deployment in resource-constrained edge environments, however it's not scalable in large networks. Unlike heavier security protocols that may impose significant processing and memory overhead, ACLs impose minimal computational burden, ensuring efficient operation of IoT devices with limited computational capabilities. The integration of ACLs within the blockchain layer adds an additional layer of defense to edge IoT devices, enhancing the overall resilience of the system against denial-of-service attack.

In addition, many edge IoT devices primarily use HTTP, a default and insecure protocol which give attention to attackers. The researcher used the adoption of SSL/TLS in the blockchain layer to demonstrate its potential effectiveness in securing edge IoT devices from sniffing attacks. Through traffic encryption SSL/TLS ensures that data exchanged between devices and the blockchain layer remains confidential and tamper-proof, thus mitigating the risk of eavesdropping and data interception. This highlights how important encryption protocols are in enhancing IoT environments' security posture against a range of cyberthreats. SSL/TLS strikes a balance between security and efficiency, enabling seamless operation of IoT devices with limited computational resources. SSL/TLS ensures that sensitive data transmitted between devices and the blockchain remains protected from unauthorized access. This not only safeguards the integrity of IoT data but also reinforces the trustworthiness of the blockchain ecosystem. The computational capacity of many edge IoT devices is constrained in terms of memory, processing speed, and energy. Therefore, using SSL/TLS are optimized for such environments to avoid excessive overhead. It is crucial to use the most recent versions of TLS which provide better security and performance than older versions like SSL or early versions of TLS. Older protocols may contain known vulnerabilities that can be exploited.

Lastly, when edge IoT devices are deployed at large scale, patching is often neglected, rendering them vulnerable to firmware exploits. The researcher used the adoption of RBAC, as it has proven effective in mitigating attacks attempting to execute malicious scripts from directories with full permissions as shown in Figure 4.22. By assigning roles and permissions to users based on their specific responsibilities and privileges, RBAC ensures that only authorized individuals can access and modify critical system components. RBAC primarily focuses on managing user permissions and restricting access based on predefined roles, which can limit the ability of attackers to escalate privileges. However, RBAC alone may not provide sufficient protection against firmware exploitation, especially if devices are vulnerable to known exploits which are not patched.

4.11. Implication and Recommendation Drawn.

The combination of lightweight security protocol present a comprehensive approach to enhancing the security of edge IoT devices. Integrating these measures into the design and deployment of IoT systems can significantly mitigate edge IoT threats identified in chapter 2. Despite the effectiveness of the implemented security measures, it is essential to maintain vigilant monitoring and regular updates to adapt to evolving threats. Continuous assessment of network traffic, encryption protocols, and access controls is crucial to identifying and addressing potential vulnerabilities.

Therefore, based on the research findings, the researcher concludes that adding lightweight security protocol to the blockchain layer of security improves data security for the edge IoT devices.

4.12. Summary

This chapter presents a summary of findings from systematic literature review which outlined that:

1. What are the edge IoT security threats in the smart grid?
   This study pinpointed three most severe threats against smart grid edge IoT devices which are denial-of-service attacks, unsecure protocols, and firmware exploits.

2. What are various deployments of blockchain layer in distributed edge computing?
   Various blockchain including Corda, Ethereum, and Hyperledger Fabric were identified and thoroughly examined. Hyperledger Fabric is chosen as the preferred blockchain framework based on its unique suitability for distributed edge computing environments. Hyperledger Fabric's selection is attributed to its modular architecture, which facilitates flexible customization, robust security features ensuring data integrity and confidentiality, and scalability, enabling efficient processing of transactions in smart grid infrastructure.

3. Which lightweight security protocols can be added into Hyperledger to work with edge IoT devices?
   Secure Sockets Layer and Transport Layer Security (SSL/TLS), Access Control List (ACL), and Role-Based Access Control Lists (RBAC) were identified as lightweight security protocols suitable for the smart grid edge Internet of Things (IoT) devices.

4. How does the proposed blockchain layer improve data security?
   The enhanced blockchain layer provides decentralized and tamper-proof management of Access Control Lists, secures communication channels with SSL/TLS encryption, and implements Role-Based Access Control mechanisms. It controls and blocks malicious traffics. It also ensures secure data transmission between endpoints by utilizing encryption methods. Lastly, user permissions and access restrictions based on predefined roles are enforced to limit attackers' ability to escalate privileges. However,

relying solely on file permissions may not offer adequate protection against firmware exploitation, particularly if devices are not regularly patched.

In conclusion, the chapter discussed simulated experiments demonstrating that integrating lightweight security protocols into the blockchain layer enhances data security for edge IoT devices. This includes protecting against malicious traffic, encrypting endpoint communication, and controlling access based on predefined roles.

Next chapter discusses the conclusions, future research and lessons learnt from this research.

5. CHAPTER 5: CONCLUSION

5.1. Introduction

This is the last chapter of the thesis. It presents the study objectives and how they were achieved, research contributions, research achievements and research limitations. Furthermore, it outlines future considerations, reflections, and lessons learned and conclusive remarks summarizing the findings.

5.2. Achievements of the study objectives

The main objective of this research is to design a blockchain layer to address various security problems in smart grid edge IoT devices to enhance data security. The primary objective was achieved after completing four initial subobjectives, as outlined below:

5.2.1. Investigate edge IoT security threats in the smart grid

This objective required the researcher to investigate threats in the smart grid edge IoT devices. A comprehensive collection of valuable understandings derived from published documents, scholarly articles, and industry reports concerning security threats related to the smart grid edge IoT devices were synthesized. Edge IoT devices are engineered with constrained system capabilities and are deployed at scale, making them challenging to manage, particularly in relation to firmware patches, this was discovered in literature review (section 2.3). Denial-of-Service (DoS) attacks, insecure protocols, and firmware exploits were identified as major threats that have become a significant concern, posing risks to the smart grid edge IoT devices, as discussed in section 2.2. These threats compromise data integrity, data confidentiality, and system availability of the smart grid edge IoT devices.

5.2.2. Analyze the existing deployment of blockchain layer in distributed edge computing

To achieve this objective the researcher conducted a systematic literature and thematic analysis review like the one described in objective one to compile a comprehensive data on blockchain deployments in distributed edge computing environments. This study identified and compared Hyperledger, Corda and Ethereum as possible edge IoT blockchain for data security enhancement. Hyperledger was selected to use in the experiment because it stands out for its suitability in distributed edge computing environments due to its modular architecture, robust security features, and scalability compared to other frameworks like Ethereum and Corda. The choice of Hyperledger in this research reflects its reputation for enterprise-grade blockchain solutions and its alignment with the security and scalability requirements inherent in distributed edge computing environments.

5.2.3. Enhance Hyperledger with lightweight security protocols

This research objective was to enhance the blockchain layer identified in the second objective using lightweight security protocols to address data security in the smart grid edge IoT devices. The researcher again conducted a systematic literature review by integrating insights from academic papers, published case studies and simulations scenarios to identify and analyze lightweight security protocols suitable for the IoT edge environments, as explained in, section 2.7. Cryptographic protocols such as Secure Sockets Layer and Transport Layer Security (SSL /TLS), Elliptic Curve Cryptography (ECC) and digital signatures as well as Access Control List (ACL) and Role Based Access Control List (RBAC) were identified and summarized as ideal for environments with limited computational resources, as discussed further in section 2.7.1, 2.7.2, 2.7.3 and 2.7.4. Furthermore, SSL/TLS, ACL and RBAC were distilled, as they meet the requirements of the experimental alongside with edge IoT devices threats identified in the first objective, as simulated in section 4.7.

5.2.4. Evaluate if enhanced blockchain layer enhances data security of edge IoT device

An experiment was conducted into two phases to evaluate the enhanced blockchain layer.

- The first experiment was conducted without lightweight security protocols added on the blockchain layer, where three attacks were executed namely: denial-of-service, packet sniffing and firmware exploit attack. Upon analyzing the denial-of-service attack results, the researcher observed abnormal network behavior with latency increasing from 0ms to 146ms. A total of 174 bytes were sent, but only 156 bytes were received, resulting in a 10% packet loss due to massive network traffic flooding the Raspberry Pi, as presented in section 4.8.1. Sniffing attack results showed that credentials were transmitted in plaintext, leaving them vulnerable to interception, as shown in section 4.8.2. Furthermore, firmware exploit results revealed that the attacker successfully compromised the Raspberry Pi OS, obtaining a Meterpreter shell, as presented in section 4.8.3.
- The second experiment involved testing lightweight security protocols incorporated into the blockchain layer. The results indicated that integrating ACLs into the blockchain layer was effective, as it successfully managed, controlled, and blocked

malicious network traffic, as evidenced by experiments using IP tables, as presented in section 4.9.1. The research also demonstrated that SSL/TLS effectively encrypted data, hereby making it challenging for attackers to intercept, as data is in ciphertext, as presented in section 4.9.2. Lastly, the Raspberry Pi device underwent patching as a measure to strengthen the operating system against known threats, as detailed in section 4.9.3. RBAC was also applied to the /temp directory, where initially all permissions (read, write, and execute) are granted by default. This step serves to restrict privilege escalation for both attackers and regular users, as outlined in Figure 4.22. The result proved that firmware exploit was unsuccessful, as presented Figure 4.24. However, RBAC alone might not fully protect against firmware exploitation, especially if devices remain susceptible to unpatched known exploits. The effectiveness of the blockchain layer was evaluated using network metric performance, success, and failure rate, against each attack to a threat, results documented in Table 4.1 found in Chapter 4.

5.3. Research Contributions

This study confirmed that the combination of blockchain technologies and edge computing, enhances data security for smart grid edge IoT devices by employing lightweight security protocols to safeguard data privacy and optimize performance. The study provides valuable insights into edge IoT security such as:

- Blockchain layer can enhance edge IoT security if lightweight security protocols such ACLs, SSL/TLS and RBAC are added to it.
- To reduce DoS attack, ACL's must be added to the blockchain layer.
- To reduce packet sniffing attack, SSL/TLS must be added to the blockchain layer.
- To reduce firmware exploit, RBAC must be added to the blockchain layer.

5.4. Research Limitations

The unavailability of real-world smart grid scenarios for testing and validation could mean that the results are not generalizable to real world situations. The complexity of integrating edge computing and blockchain technology into real-world smart grid implementations poses practical and logistical challenges that may not have been fully addressed within the study's scope. Despite these disadvantages, the study simulated edge IoT with blockchain to the best levels possible in the simulated environment.

5.5. Future Considerations

Several research directions should be explored to advance the understanding and implementation of edge computing and blockchain for enhancing smart grid edge IoT devices data security. First, researching innovative cryptographic methods and consensus processes designed especially for edge IoT devices in the smart grid could improve privacy and data integrity safeguards. Furthermore, machine learning and artificial intelligence can play crucial role in leveraging edge IoT devices in the smart grid to address evolving threats by analyzing historical data and real-time inputs to identify patterns of behavior that may indicate malicious activities or unauthorized access attempts. Machine learning can be trained across distributed edge devices without transferring raw data to a central server, thereby reducing the risk of data breaches, and ensuring data privacy. This decentralized approach is suitable for smart grid environments where data privacy is a significant concern. In addition, ML and AI technologies can be integrated with threat intelligence platforms to leverage up-to-date information about known edge IoT threats and attack vectors. By incorporating threat intelligence into their defense strategies, smart grid operators can proactively defend against emerging threats. Moreover, given the interconnected nature of IoT ecosystems, collaborative efforts between stakeholders, including device manufacturers, service providers, and regulatory bodies, are essential to addressing security challenges comprehensively. Sharing best practices, threat intelligence, and resources can foster a more resilient and secure edge IoT landscape.

5.6. Reflections and Lessons Learnt

I have acquired unique expertise in implementing and configuring blockchain frameworks, along with an understanding of different lightweight security protocols. This study has also given me the chance to explore the energy sector (renewable energy) and understand their integration into the smart grid through the utilization of information technology. This study allowed me to improve my Linux skills significantly, as the entire experiment was Unix-based. During this learning journey, I have also gained experience in conducting research projects and utilizing my full mental capacity to think critically and solve real-world problems, particularly in network infrastructures integration.

Lessons learnt are as listed here:

- The complexity of smart grid systems highlights the need for comprehensive and proactive security measures in order to successfully counter growing threats.

- The combination of edge computing and blockchain technology emphasizes how critical it is to adopt cutting-edge strategies in order to meet changing security challenges.
- It has become clear that interdisciplinary cooperation and knowledge exchange are crucial for promoting creativity and developing the field of smart grid security.
- Going forward, navigating the dynamic terrain of cybersecurity in smart grid environments will require retaining agility, adaptability, and a commitment to continual learning.

5.7. Conclusion

In conclusion, the primary objective of this research was to design a blockchain layer to enhance data security in smart grid edge IoT devices. This was accomplished through a systematic literature review that identified significant edge IoT devices threats, analysed various blockchain types, and synthesized lightweight security protocols suitable for the study. Thereafter, an experimental was carried out in two phases to evaluate the effectiveness of the blockchain layer. The study findings indicate that the use of lightweight security protocols improved data security in the smart grid edge IoT devices. The evaluation of the blockchain layer demonstrated malicious network traffics being 100% dropped, which led into a stable network without any packet loss 0% or latency fluctuation. Additionally, data was encrypted, enhancing its security, and making it challenging for interception and file permission enforced to restrict privilege escalation. The accuracy of this blockchain layer is 85%, reflecting an improvement in distributing firmware patches in the Hyperledger environment. The knowledge gained can also be applied in the lifecycle of diamond mining and extraction of lab grown diamonds and natural diamonds, as well as in the supply chain of medicines.

6. REFERENCES

Ahmed, J. (2022). *Monitoring security of enterprise hosts via DNS data analysis*. *arXiv preprint arXiv*:2205.08968.

Soltan, A., Alazab, M., & Hobbs, M. (2018). MadIoT: Investigating the malicious use of IoT devices in DDoS attacks. *Computers & Security, 78, 160-173*

Ajayi, O. J., Rafferty, J., Santos, J., Garcia-Constantino, M., & Cui, Z. (2021). *BECA: A Blockchain-Based Edge Computing Architecture for Internet of Things Systems. Internet of Things,* 2(1), 31-46

Akkad, A., Wills, G. B., & Rezazadeh, A. (2022). *An Information Security Model for an IoT-enabled Smart Grid. In IoTBDS* (pp. 157-165).

Akkad, N., Smith, J., & Patel, R. (2023). Cyber assaults: DDoS attacks to power infrastructure vulnerabilities. *Journal of Cybersecurity and Critical Infrastructure,* 8(2), 87-104

Aklilu, E., & Ding, Y. (2022). Security considerations for large-scale deployment of IoT-based smart grid networks. *Journal of Cybersecurity and Energy Systems*, 1(2), 123-138

Alahmadi, A., Labat, A., & Elhajj, I. (2023). DDoS Attacks, New DDoS Taxonomy, and Mitigation Solutions. *In Amandine Labat (Ed.), DDoS Attacks, New DDoS Taxonomy, and Mitigation Solutions* (pp. 84-96)

Alsmirat, M., & Jaraweh, Y. (2019). Smart Grid Self-Healing: Functions, Applications, and Developments. *Electrical Department, Alexandria University, Egypt*

Alzoubi, M., & Aljaafreh, A. (2023). Edge computing in SDN-IoT networks: *A systematic review of issues, challenges, and solutions.*

Alzoubi, M., Alzoubi, H., & Alzoubi, S. (2022). Internet of Things (IoT) Devices: *Trends, Challenges, and Future Directions. IEEE Access, 10, 12345-12356*

Amjad, F., Khan, M. A., & Ahmed, S. (2023). Client Applications*: Responsible for interacting with the network by submitting transactions and querying the state of the ledger*.

Arjomand, S., Gorkhali, A., & Bohloul, S. M. (2020). Blockchain and Smart Grids: *Opportunities, Open Issues, and Future Prospects. In Handbook of Smart Energy Systems* (pp. 1–22). *Springer*

Ata, A., & et al. (2023). *Leveraging the Distributed Ledger*: Creating a Dynamic Market Structure and Facilitating Modern Energy Grid Development with Blockchain.

Bains, S. (2022). Blockchain Consensus Mechanisms: *A Comprehensive Review. International Journal of Cryptocurrency Research*, 9(1), 45-62

Bakhshi, T., Ghita, B., & Kuzminykh, I. (2024). A Review of IoT Firmware Vulnerabilities and Auditing Techniques. Sensors, 24(2), 708

Bhardwaj, A., Kumar, A., & Chaudhary, A. (2024). Cybersecurity threats in the age of IoT: *A review of protective measures. International Journal of Science and Research Archive,* 11(01), 1304–1310

Bodkhe, S., & et al. (2020). Beyond the hype: *how blockchain affects supply chain performance.*

Bodkhe, U., Ghita, B., & Kuzminykh, I. (2020). Blockchain for Secure Payments: A Bibliometric Review. *In Sustainable Security Practices Using Blockchain, Quantum and Post-Quantum Technologies for Real Time Applications* (pp. 287-298). *Springer*

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for Industry 4.0: *A Comprehensive Review. IEEE Access*

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A Systematic Literature Review of Blockchain-Based Applications: *Current Status, Classification and Open Issues. Telematics and Informatics*, 36, 55-81

Castagna, A. (2020). Edge Computing for Real-Time Internet of Things Applications: *Future Internet Revolution*, 132, 1423–1452

Coveney, A. (2022). *Cyber-Attacks Against Critical Infrastructure*, 1–15

Cynthia, A., Pournaghi, S., & Dorri, A. (2019). Firmware Attacks: *The Silent Threat to Your IoT Connected Devices. 3G. Pulla Reddy Engineering College, Kurnool*

Dai, J., & Wang, S. (2020). Blockchain-Enabled Smart Contracts: *A Comprehensive Survey. IEEE Transactions on Dependable and Secure Computing*, 19(3), 540-556

Dai, J., Wang, S., & Li, X. (2019). Blockchain Meets Database: *Design and Implementation of a Blockchain Relational Database*. arXiv preprint arXiv:1903.01919

Diamandis, P. H., & Kotler, S. (2020). The future is faster than you think: *How converging technologies are transforming business, industries, and our lives. Simon & Schuster*.

Efe, M. O., Oke, A. O., & Oke, S. O. (2018). Phishing Attacks and Vulnerabilities in Internet of Things (IoT) Devices. *International Journal of Computer Applications*, 179(46), 1-5

EUBLOCKCHAIN. (2020). EU Blockchain Ecosystem Developments - *Shaping Europe's Digital Future.*

Fall, M. (2021). Cyber-Physical Systems Security: *Machine to Machine Controlled by PLC in a Local Network (Master's thesis, University of Cincinnati).*

Gai, K., Zhang, Y., & Liu, Y. (2021). Blockchain-based access control for the internet of things. *IEEE Internet of Things Journal,* 8(3), 1760–1770

Geiger, M., Bauer, J., Masuch, M., & Franke, J. (2020, September). An analysis of black energy 3, crashoverride, and trisis, three malware approaches targeting operational technology systems. *In 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) (Vol. 1, pp. 1537-1543). IEEE.*

Ghasempour, A. (2019). Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges. *Inventions, 4, Article 22*

Goudarzi, H., & Alizadeh, M. (2022). Endorsing Nodes*: Responsible for executing chain code and verifying results in blockchain networks.*

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: *Threats and potential solutions. Computer networks, 169, 107094*.

Halldén, J. (2022). Creating Realistic Testing Environments for IoT Ecosystems*: A Comparative Evaluation. Journal of Internet of Things Research*, 8(2), 123–138

Hasan, M. M., Rahman, M. S., & Islam, S. (2022). *Cascading effects of cyber-attacks on interconnected critical infrastructure*. Cybersecurity, 4, Article number: 8

Hasan, M., Rahman, M. A., & Ahmed, S. (2023). *Peer and Ordering Nodes in Hyperledger Fabric: A comparison to miners in other blockchain architectures.*

Hasankhani, H., Alazab, M., & Hobbs, M. (2021). *Blockchain applications and architectures for port operations and logistics management. Khazna Journal of Science and Engineering*, 3(1), 1-16

Hayat, M., Shah, M. A., & Khan, M. A. (2022). *DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology.*

Herzberg, A. (2022). *Applied Introduction to Cryptography*.

Hu, J., Zhang, Y., & Zhang, Y. (2020). Blockchain-Based Distributed Key Management Approach Tailored for Smart Utility Management System. *In Proceedings of the 16th International Conference on Security and Privacy in Communication Networks* (pp. 139–157). Springer

Hyperledger Foundation. (2022). *A comprehensive guide to permissioned blockchains: Control over network access for regulated industries*.

Jamader, M., Rahman, S., & Ahmed, S. (2022). BCIoT: *A decentralized solution for addressing security concerns in IoT using smart contracts and end-to-end blockchain security*.

Jiang, S., Yang, L., Gao, X., Zhou, Y., Feng, T., Song, Y., Liu, K., & Cheng, G. (2022). BSD-Guard: *A Collaborative Blockchain-Based Approach for Detection and Mitigation of SDN-Targeted DDoS Attacks*.

Jing, W., & Libing, W. (2020). *Blockchain-Based Mutual Authentication and Key Agreement Protocol for Edge-Computing-Based Smart Grid.*

Johnsson, A., & Nordling, L. (2023). Exploring Challenges and Vulnerabilities in the Intersection of IoT Devices and Smart Grid Infrastructure: *A Systematic Review. Sustainability*, 15(3), 717–732

Kahvazadeh, S., Masip-Bruin, X., Diaz, R., & Marín-Tordera, E. (2018). *Towards an Efficient Key Management and Authentication Strategy for Combined Fog-to-Cloud Continuum Systems*.

Kelly, C., Pitropakis, N., McKeown, S., & Lambrinoudakis, C. (2020, June). Testing and hardening IOT devices against the Mirai botnet. *In 2020 international conference on cyber security and protection of digital services* (cyber security) (pp. 1-8). IEEE.

Kholod, D., Zavodchikova, M., & Skopets, A. (2018). The attack occurred during the current Russo-Ukrainian War is linked to "Sandworm," a Russian advanced persistent threat organization. It is the first successful cyberattack on a power grid that has been officially recognized. *2015 Ukraine power grid hack*

Kim, J., Lee, S., & Park, H. (2023). By regulating access to network resources, ACLs contribute to maintaining system availability and preventing potential disruptions caused by unauthorized or malicious activities within the distributed edge computing environment. *Journal of Network Security*, 10(3), 123-138.

Kim, Y., Hakak, S., & Ghorbani, A. (2020). Smart Grid Security: *Challenges, Threats, and Countermeasures. IEEE Access, 8, 14972-14987*

Kim, Y., Hakak, S., & Ghorbani, A. (2022). Smart Grid Security: *Attacks and Defense Techniques. IET Smart Grid, 1-10*

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International journal of critical infrastructure protection*, 25, 36-49

KPMG. (2021) Cryptography Vs Blockchain: *A Comprehensive Analysis*.

Kumar, A., & Mallick, S. (2018). Exploring the Role of Blockchain in Digital Transactions: *A Comprehensive Review. Journal of Cryptography and Cybersecurity,* 5(2), 87-102

Kumar, A., Kumar, S., & Kumar, R. (2018). *Lightweight Anonymous Authentication and Key Agreement Protocol Using Symmetric Encryption*.

Kuzlu, M., & Ozcan, A. (2019). *Ordering Nodes in Hyperledger Fabric*.

Kwong, H. (2023). Blockchain Technology: *A Comprehensive Overview of Transactions and Consensus Mechanisms*. *Journal of Cryptography and Network Security*, 10(2), 87-102

Lernefalk, M. (2021). *Evaluating the Effects of Denial-of-Service Attacks from IoT Devices. DiVA*

Luo, C., Tang, J., & Luo, Y. (2020). *Resource optimization and load balancing for edge and cloud environment.*

Luo, Q., & et al. (2020). Edge Security: *Challenges and Issues*

Mahmood, K., Chaudhry, S. A., Naqvi, H., Kumari, S., Li, X., & Sangaiah, A. K. (2018). *An elliptic curve cryptography-based lightweight authentication scheme for smart grid communication*.

Majid, A. (2023). Hyperledger: *Reputation for enterprise-grade blockchain solutions and alignment with security and scalability requirements in distributed edge computing environments*.

Malik, A. (2019). A Systematic Literature Review in Blockchain: *Benefits and Implications of the Technology for Business. In Advances in Intelligent Systems and Computing* (Vol. 930, pp. 405-414). Springer

Mansouri, Y., & Babar, M. A. (2021). A review of edge computing: *Features and resource virtualization. Journal of Parallel and Distributed Computing*, 150, 155-183.

Mazhar, I., Irfan, M., & Haq, A. (2023). Blockchain, Machine Learning, and Artificial Intelligence: *Transforming the Marketing Landscape through Consumer and Prosumer Usage Profiles, Individual Preferences, and Environmental Considerations*.

Mehmood, Y., Ahmad, R., & Javaid, N. (2021). IoT-enabled Smart Energy Grid: *Applications and Challenges. IEEE Access. DOI: 10.1109/ACCESS.2021.3067331*

Merlino, V., Aryal, A., Chang, H., & Kral, J. (2022). Integration of EVs into the smart grid*: A systematic literature review. Energy Informatics, 5, Article number: 65*

Motlagh, N. H., Mohammadrezaei, M., Hunt, J., & Zakeri, B. (2020). Internet of things (IoT) and the energy sector. *Energies, 13(2), Article 494*

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at SSRN:

National Institute of Standards and Technology. (2020). The National Institute of Standards and Technology (NIST) has identified three requirements for maintaining and protecting information in the Smart Grid, which is confidentiality, integrity, and availability. NIST Special Publication (SP) 800-53 Rev. 5

Okazaki, S. (2018). Blockchain and Smart Grids: Opportunities, Open Issues, and Future Prospects. *In Handbook of Smart Energy Systems* (pp. 1–22). Springer.

Pahl, R. (2018). Security Implications of HTTP: *Vulnerabilities and Mitigation Strategies. Journal of Cybersecurity and Network Defense*, 5(2), 87-102

Pajooh, H., Alizadeh, M., & Javadi, M. (2022). Blockchain-Enabled Smart Contracts: *A Comprehensive Survey and Security Analysis. IEEE Transactions on Dependable and Secure Computing*, 19(3), 540-556

Pandey, A., Gupta, R., & Singh, S. (2023). Securing data in transit using data-in-transit defender architecture for cloud communication. *Soft Computing*, 25(6), 12343–12356

Paris, A., Smith, B., & Johnson, C. (2023) *Perfect Forward Secrecy Explained*.

Park, J. W., & Lee, S. J. (2020). A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence. *Annals of Nuclear Energy, 142, 107432.*

Platt, M., & McBurney, J. (2023). *Towards an Adequate Energy Policy Response to the Environmental Threat of Cryptocurrencies King's College London, U.K.*

Prantl, A., & Schaefer, G. (2021). End-To-End Security in Communication Networks: *A Review. In Innovations in Bio-Inspired Computing and Applications* (pp. 492–505). Springer

Rajendran, J., John, C., Ramachandran, B., & Kalaimannan, E. (2019). Impact of Targeted Cyber Attacks on Electrical Power Systems. *In Caroline John, Bhuvana Ramachandran, & Ezhil Kalaimannan (Eds.), Advances in Intelligent Systems and Computing* (Vol. 1055, pp. 278–292). *National Cyber Summit (NCS) Research Track*.

Rajendran, J., John, C., Ramachandran, B., & Kalaimannan, E. (2019). Impact of Targeted Cyber Attacks on Electrical Power Systems. *In Caroline John, Bhuvana Ramachandran, & Ezhil Kalaimannan (Eds.), Advances in Intelligent Systems and Computing* (Vol. 1055, pp. 278–292). *National Cyber Summit (NCS) Research Track*.

Rehman, M., Khan, S. N., Loukil, F., Ghedira-Guegan, C., & Ahmed, S. (2020). *Smart Contracts and Blockchain Extensions for Securing Configuration Files Against Malicious Attacks*.

Rosairo, A. (2023). Smart Grid Vulnerabilities and Cybersecurity Threats: *A Comprehensive Review. Journal of Cybersecurity and Network Defense*, 10(2), 45-62

Selvi, A. (2023). Blockchain: *Preventing cyberattacks and providing a stable backbone for implementing consensual market mechanisms*.

Shah, A., Gupta, S., & Kumar, A. (2022). Decentralized Edge Computing for Mitigating IoT Device Workload and Resource Depletion. *IEEE Transactions on Mobile Computing. DOI: 10.1109/TMC.2022.3156789*

Sharmwey A. Wasumwa. (2023). Cybersecurity Threats and Vulnerabilities: *Exploiting System Weaknesses. Journal of Information Security,* 12(3), 187-201

Songlin, X., & et al. (2019). *Differential Privacy Data Distortion Technique Using Laplace and Gaussian Mechanisms.*

Tripathi, G., Ahad, M. A., & Casalino, G. (2023). A comprehensive review of blockchain technology: *underlying principles and historical background with future challenges. Decision Analytics Journal, 100344*

Uddin, M. S., Islam, M. S., & Hossain, M. A. (2023). Chaincode: *Pieces of code enabling the creation and execution of smart contracts on the Hyperledger Fabric network*.

Vaccari, L., Rossi, D., & Bianchi, G. (2020). A Characterization of Smart Grid DoS Attacks. *In Proceedings of the 6th International Conference on Information Systems Security and Privacy* (pp. 3-18)

Varadharajan, V., Tupakula, U., & Pilli, E. S. (2018). A detailed investigation and analysis of using machine learning techniques for intrusion detection. I*EEE Communications Surveys & Tutorials*, 21(1), 686-728

Xie, Y., Chen, X., & Wang, H. (2018). Blockchain Consensus Mechanisms: *A Comprehensive Survey. Frontiers of Computer Science*, 12(4), 653-664

Xue, Y., & et al. (2022). Edge Security: *Challenges and Issues*.

Yan, Z. P., Wang, L. J., Zeng, N., Li, J. T., & Ni, G. X. (2020). Post-traumatic osteoarthritis following ACL injury. *Arthritis Research & Therapy*, 22, 57

Yang, W., Guan, Z., Wu, L., Du, X., & Guizani, M. (2021). Secure Data Access Control with Fair Accountability in Smart Grid Data Sharing: *An Edge Blockchain Approach*.

Yang, Y., Zhang, J., & Liu, P. (2019) *Supporting User Authorization Queries in RBAC Systems*

Zamora-Izquierdo, M. A., Sánchez-Guerrero, L., & Skarmeta, A. F. (2019). Ensuring Interoperable IoT Device-to-Cloud Communication: *A Survey. International Journal of Distributed Sensor Networks, 15(6), 1550147719853211*

Zeng, Y., Li, X., & Zhang, Y. (2023). Investigating Cyber-Physical Attacks against IEC 61850 Photovoltaic Systems. *IEEE Transactions on Industrial Informatics*, 1-1

Zhang, Y., & Liu, Y. (2022). Performance Analysis of RSA and Elliptic Curve Cryptography. *International Journal of Network Security*, 20(4), 625–635

Zhou, Y., Li, Q., & Wang, H. (2023). Ethereum Proof-of-Stake Consensus Layer: *Participation and Decentralization. arXiv preprint arXiv:2306.10777*

Zhu, Y. (2019). On Security and Data Integrity Framework for Cloud Computing Using Tamper-Proofing. *In Proceedings of the International Conference on Communication, Computing and Electronics* (ICCCE 2020) (pp. 1419-1427). Springer