Republic of Iraq
Ministry of Higher Education and Scientific
Research University of Babylon
College of Information Technology
Software Department

Detection and Mitigation Distribution Denial of Service Attack Based on Blockchain

A Thesis

Submitted to the Council of the College of Information Technology for Postgraduate Studies of the University of Babylon in Partial Fulfillment of the Requirements for the Degree of Master in Information Technology / Software

By

Noor Alaa Hussein Ghaben

Supervised By

Asst. Prof. Dr. AL Harith Abdulkareem Abdullah

2023 A.D. **1445 A.H.**

بِسْـــمِ

﴿ يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ ﴾

صدق الله العلي العظيم

سورة المجادلة
الآية (11)

Declaration

I hereby declare that this thesis entitled "**Detection and Mitigation Distribution Denial of Service Attack Based on Blockchain**" submitted to the University of Babylon in partial fulfillment of requirements for the degree of Master in Information Technology \ Software, has not been submitted as an exercise for a similar degree at any other University. I also certify that this work described here is entirely my own except for experts and summaries whose source is appropriately cited in the references.

Signature:

Name: Noor Alaa Hussein

Date: / /2023

Supervisor Certification

I certify that the thesis entitled (**Detection and Mitigation Distribution Denial of Service Attack Based on Blockchain**) was prepared under my supervision at the department of Software/ College of Information Technology/ University of Babylon as partial fulfillment of the requirements of the degree of Master of Philosophy in Information Technology-Software.

Signature :

Supervisor Name: **Asst. Prof. Dr. AL Harith Abdulkareem Abdullah**

Date: / /2023

The Head of the Department Certification

In view of the available recommendations, I forward the thesis entitled **"Detection and Mitigation Distribution Denial of Service Attack Based on Blockchain"** for debate by the examination committee.

Signature:

Assistance Professor Dr. Sura Zaki Alrashid

Head of Software Department

Date: / /2023

Certification of the Examination Committee

We, the undersigned, certify that (**Noor Alaa Hussein**) candidate for the degree of Master in Information Technology - Software, has presented his thesis of the following title "**Detection and Mitigation Distribution Denial of Service Attack Based on Blockchain**" as it appears on the title page and front cover of the thesis that the said thesis is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on:

Signature:
Name: Wesam S. Bhya
Title: : Prof.Dr.
Date: / / 2023
(Chairman)

Signature:
Name: Ameer Kadhim Hadi
Title: Asst.Prof.Dr
Date: / / 2023
(Member)

Signature:
Name: ALHarith A. Abdullah
Title: Asst. Prof. Dr.
Date: / / 2023
(Member and Supervisor)

Signature:
Name: Zaid Abdul-Wahid Abod
Title: Asst. Prof.
Date: / / 2023
(Member)

Approved by the Dean of the College of Information Technology, University of Babylon.

Signature:
Name: Wesam S. Bhya
Title: Prof.Dr.
Date: / / 2023
(Dean of Collage of Information Technology)

Dedication

To the one who is familiar with the secrets of what our hearts contain, and the witness to the heart and its intention. To those who wait for knowledge from us that we will help him with when we stand with him under the shade of his banner. To the dream of the prophets and messengers and the family of the descendants. To the Imam of time the rest of God on earth, the owner of the age and time, the awaited Imam Mahdi (may God hasten his honourable reappearance) ...

To those who were martyred, and They sacrificed for the sake of Iraq

To My father, the heroic martyr....

To My mother eternal giving....

To My beloved brothers..

To My beloved family.

Acknowledgments

In the Name of Allah, the Most Merciful, the Most Compassionate All praise be to Allah, the Lord of the worlds; and prayers and peace be upon Mohamed His servant and messenger.

First, Praise be to Allah for giving me the health and strength to complete this thesis.

I am thankful to my supervisor **Asst. Prof. Dr. AL Harith A. Abdullah**, without his help, guidance, and continuous follow-up; this research would never have been done.

I would like to thank the academic staff of the Faculty of Information Technology/Software Department University of Babylon who helped me during my master's study and taught me different courses.

Noor Alaa Hussein

Abstract

Data and network applications are rapid growth, emphasizing the increasing importance of strong security measures. With the proliferation of vulnerable devices and network traffic, Distributed Denial of Service (DDoS) attacks have become easier to launch.

DDoS attacks aim to overwhelm a server or website by flooding it with requests, rendering it inaccessible to legitimate users. While various DDoS mitigation solutions have been attempted, blockchain technology shows promise. Blockchain, as a decentralized and secure system, can securely store attack-related data.

This thesis proposes a decentralized blockchain solution to combat DDoS attacks. The technique involves redirecting excessive requests from the target server to auxiliary nodes, reducing strain and maintaining accessibility for legitimate users.Artificial neural networks be integrated within blockchain technology in different programming and development environments.

The system was tested through a two-level approach. The first level utilizes the Nmap tool for an initial test and early detection of DDoS attacks. If a connection cannot be established, the suspicious traffic is forwarded to the second level.

The second level involves a trained neural network capable of classifying network traffic and detecting potential attacks. A neural network is trained using various data samples to learn patterns and characteristics associated with different types of attacks. By analyzing traffic data, the

neural network accurately identifies malicious activity or DDoS attack attempts and blacklists them.

This thesis demonstrates that blockchain and neural network can offer effective solutions for DDoS mitigation. This promising network security approach has the potential to protect enterprises from DDoS attacks, safeguarding their operations and ensuring uninterrupted service for legitimate users.

Dataset have been implemented to evaluate the suggested model, CICDDOS219 dataset . The consequences of the proposed work have shown encouraging results in terms of high accuracy. The accuracy of 0.96,The recall of 0.89,The precision of 0.96, The F1-Score of 0.92,The specificity of 0.98,The mean squared error (MSE) of 0.032315571.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

AS	Autonomous Systems
CDNs	Content Delivery Networks
DApps	Decentralized Applications
DDoS	Distributed Denial of Service
DeFi	Decentralized Finance
DHTs	Digital Health Technologies
DPoS	Delegated proof-of-stake
HTTP	Hypertext Transfer Protocol
IAT	Inter-arrival time
IoT	Internet of Things
IP	Internet Protocol
KNN	K-Nearest Neighbor
LDDoS	Low-rate Distributed Denial of Service
LSTM	Long Short-term Memory
P2P	Peer to Peer
PoS	Proof of Stake
PoW	Proof of Work
SDN	Software-Defined Networking
SYN	Synchronize
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

CHAPTER ONE
GENERAL INTRODUCTION

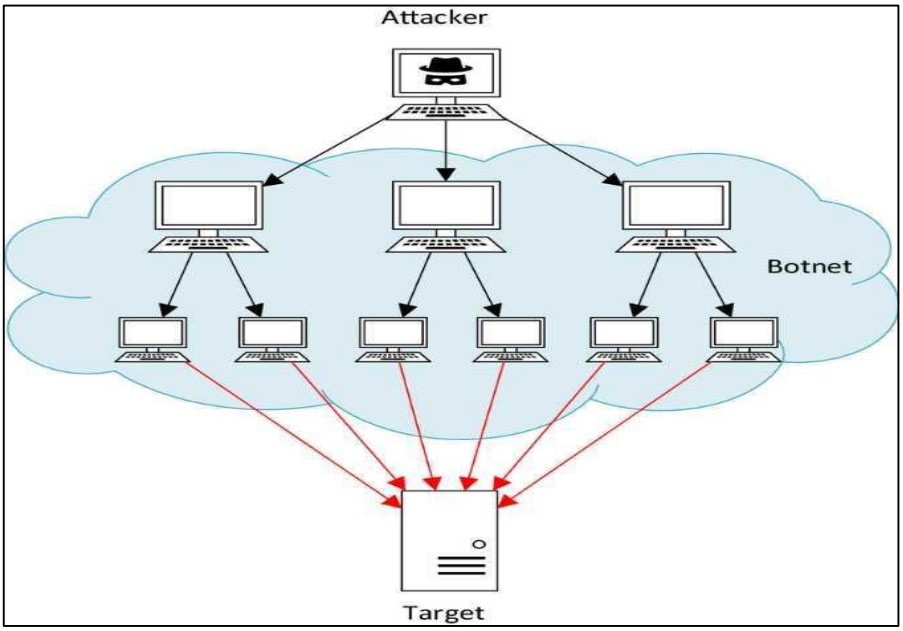
1.1 Introduction

A Distributed Denial of Service (DDoS) attack is a Denial-of-Service (DoS) attack that inundates the intended target or its associated infrastructure with malevolent traffic. The process above is accomplished through bots, a collection of malware-infected computers and other devices remotely controlled by a perpetrator [1] as depicted in Figure(1.1).

The significant reduction in available bandwidth and connectivity can result in the interruption of all network services. The principal objective of (DDoS) attack is to compromise the availability of resources intended for legitimate users. An intentional flood of data can overwhelm a network and cause service interruptions by exceeding its capacity. Financial companies, healthcare providers, and government bodies are all fair game, as are less visible public networks. Discerning the attack traffic from legitimate traffic in a DDoS attack presents a challenge due to their resemblance. The packets exhibit behavior resembling typical network packets, albeit with a greater frequency and a heightened concentration directed towards the targeted victim. This phenomenon is widespread in the initial phases of an attack, particularly in low-rate and low-traffic attacks. Typically, an attack is assessed through volumetric metrics, including packets-per-second, bits-per-second, and connections-per-second. [2]

Detecting and mitigating a malevolent assault originating from a limited number of nodes is comparatively simpler. The utilization of a substantial quantity of nodes in a DDoS attack results in a severe disruption of the ability to fulfil legitimate requests due to the collective behavior of the attack. Compromised devices engage in the uninterrupted transmission of a significant number of packets through the network, deceiving the targeted recipient into perceiving them as authentic traffic. Consequently, the host

communicates with diverse devices and varied categories of packages. The DDoS attack has been established as a contested arena for resources between the assailants and defenders. The greater the availability of resources, the



greater the likelihood of success [3].

Figure (1.1) Distributed Denial-of-service Attacks Work[4]

Blockchain represents a rather recent approach to information technology, initially adverted in 2008 by Satoshi Nakamoto's white paper. Satoshi Nakamoto presented a solution to the issues of implementing and using digital currency, particularly the double spending issue [5].

Blockchain gives an open, decentralized database for any transaction, including values like goods and money. Consequently, blockchain technology has slowly invaded the internet as a guaranteed substitutional digital model that utilizes cryptography and mathematics[6].

The technology blockchain technological basic properties such as decentralization, transparency, shared ledger based on consensus, immutability, and privacy, thereby realizing the features needed for

authentication and authorization, including security, decentralization and anonymity. [6]

Scientific research offers a lot after the emergence of blockchain technology that helped solve the problems of the Internet, so the vision was to use this technology to solve the problem of security and privacy for various electronic services that need a decentralized solution and distribution, and this is one of the most important features of blockchain technology. The following points present some studies and discussions that are so far associated with the proposed work in this thesis:

1.2 Related work

This section presents a discussion of the previous studies related to the proposed of detecting DDoS attacks on the network. Using blockchain technology.

In 2017, Bruno Rodrigues1 et al. [7] The paper endeavors to tackle the issue of network-based “Distributed Denial of Service (DDoS) attacks”. In conjunction with Smart Contracts, blockchain technology is proposed as a viable resolution to the issue above. The present work's architecture comprises Customers, ASes, and Blockchain/Smart Contracts. The primary contributions of this methodology encompass creating and establishing a blockchain-based architecture for disseminating DDoS attacks across various domains. Additionally, the incorporation and assimilation of this approach are expedited due to the public availability of Ethereum and smart contracts and the potential to enforce regulations on the ASes-side through the utilization of SDN. Furthermore, this approach can serve as a supplementary security mechanism without necessitating modifications to pre-existing ones.

In 2018, Uzair Javaid et al. [8] This paper discusses “Distributed Denial of Service (DDoS) attacks on Internet of Things (IoT) networks”. The present study proposes a system that employs Blockchain technology based on Ethereum to address the issue of DDoS and rogue device attacks. This approach is deemed to offer a more robust defense mechanism. The system can differentiate between reliable and unreliable devices and assigns a predetermined allocation of resources to each device, which cannot be exceeded.

In 2018, Kyoungmin Kim et al. [9] The present study focuses on the issue of Distributed Denial of Service (DDoS) attacks that target website services. The present study proposes a novel approach for addressing DDoS attacks by leveraging blockchain technology, which incorporates decentralized content delivery networks (CDNs) and relies on trusted nodes duly authorized by the government or military entities. In operational procedures, the website or a user linked to the system is regarded as a terminal node. Each central node functions as a CDN server and provides the cache information. A network has been established with an assumption regarding the quantity of content delivery network (CDN) data centres utilized by extant corporations. A central node with a high score in a private blockchain network is established within the new geographical location.

In 2019, Zohaib Ahmed et al. [10] The present study addresses the issue of “Mirai Botnet assaults on Internet of Things (IoT) devices”. The present study posits a potential resolution to the issue above by utilizing blockchain technology. The solution entails partitioning the network into Autonomous Systems (AS) that utilize the blockchain network to exchange data on malevolent nodes. The identification and classification of nodes as malicious occur when the volume of traffic generated surpasses a specific threshold.

In 2019, Rahaman Jamader et al. [11] The present study pertains to the potential hazards associated with (DDoS) attacks on the Internet of Things (IoT) platform". The proposed solution endeavors to mitigate these risks by effectively administering analytics to enhance the Internet of Things and implementing a suitable resolution through the utilization of blockchain technology. The dangers and the resources are now in harmony with one another. Providing a Blockchain-based smart contract that guarantees security via the use of a hash-based secret key for encryption and decryption operations allows for the establishment of a secure communication network.

In 2020 Meizhu Chen et al. [12] This study addresses the security concerns of implementing blockchain technology in IoT devices. The proposed solution involves utilizing blockchain to mitigate these security risks. Initially, the methodology scrutinizes the flow characteristics of the Internet of Things and subsequently detects any anomalous attack flow. The classification technique employs LSTM classification to train and evaluate network traffic, aiming to detect the presence of a DDoS attack. The blockchain network's decentralized nature and capacity to regulate access to information attack nodes, such as smart contract code, enables the generalization of the entire chain of nodes. This, in turn, confers a temporal advantage in defending against a DDoS attack.

In 2020 D.V.V.S. Manikumar et al. [13] The present study aims to enhance security measures against DDoS attacks by leveraging machine learning methodologies to address various such attacks. Additionally, the study seeks to ensure stability and transparency by leveraging Blockchain technology to prevent unauthorized modification of stored IP addresses. This study employed three distinct algorithms, namely KNN, Decision Tree, and Random Forest, to determine the optimal algorithm for identifying malicious IP addresses. The results indicated that the Random Forest algorithm

exhibited superior classification performance compared to the other two algorithms. The utilization of Blockchain technology has been observed to mitigate DDoS attacks, as each node within the Blockchain network possesses the capability to access the distributed ledger and retrieve IP addresses that have been blocked. Furthermore, it is worth noting that the data stored within the Blockchain is immutable and impervious to tampering or modification.

In 2020 Syed Badruddoja et al. [14] The present study aims to investigate the issues related to "Distributed Denial of Service (DDOS) attacks in the Internet of Things (IoT) context". The present study offers a suggested resolution utilizing the DOTS framework in conjunction with Blockchain technology. The association of DOTS with IoT necessitates a substantial enhancement in security assurance. Integrating blockchain technology can eliminate the need for intermediary involvement and enhance the security of engineering transactions in the Internet of Things (IoT) ecosystem, which is situated within the blockchain. The values above underwent threshold calculation to determine whether the IoT sensor was susceptible to a DDoS attack based on the variance in temperature, humidity, pressure, and wind direction recorded on that particular day.

In 2021 Vishwani Patel et al . [15] The present study discusses Distributed Denial of Service (DDoS) attacks targeting cloud networks. Several methodologies have been employed to identify cloud-based attacks, including the utilization of CS_DDoS technology. However, this approach has certain limitations, as it may not accurately detect attacks and can potentially impede system performance, resulting in service disruptions. An alternative solution has been suggested involving the utilization of Blockchain technology. This technology offers enhanced security and privacy for data and networks and a decentralized security framework. As a

result, it enables the sharing of attack information in a fully automated and distributed manner while preventing systems from being controlled by attacks that aim to achieve their objectives within the cloud environment.

In 2022 Rahmeh Fawaz Ibrahim et al . [16] This study aimed to investigate the security issue in the Internet of Things (IoT) context, specifically focusing on Distributed Denial of Service (DDoS) attacks. The Internet of Things (IoT) operates under a centralized system, which poses a security threat. To address this issue, a proposed solution involves utilizing public blockchain technology at the application layer. This consists of authenticating and verifying IoT devices through a trusted allowlist within a smart contract. Subsequently, the IP addresses of malevolent devices can be monitored and documented within the blockchain system to impede their ability to establish communication with Internet of Things (IoT) networks.

1.3 Problem statement

Distributed Denial of Service (DDoS) attacks are a major and complex challenge for the network. These attacks consistently rank as the top security threat in annual reports on online security threats. Additionally, there is a worrisome annual increase in the scale of cyber-attacks and the amount of data transmitted by compromised devices.

The existing centralized DDoS mitigation methods are frequently inadequate in effectively defending against advanced DDoS attacks. This insufficiency poses a significant risk to networks and their security.

1.4 Aim

The thesis aims to develop a secure system that effectively detects and mitigates DDoS attacks using Blockchain Technology, with the integration

of a trained neural network for enhanced defense. The aims to prevent and detect DDoS attacks across various domains on the network.

The research objectives include building a robust network architecture, use dataset controlled DDoS attack , analyzing packet transmission to the server during DDoS attacks, and implementing effective countermeasures.

Additionally, the thesis incorporates a trained neural network to enhance the detection and classification of network traffic, specifically targeting potential DDoS attacks. The neural network learns patterns and characteristics associated with different types of attacks, contributing to a robust defense against DDoS attacks.

1.5 Outline

- **Chapter One: Introduction**

This chapter provides an overview of the research area, highlighting the significance and relevance of the study. It discusses the problems addressed by the research and emphasizes the importance of investigating the subject matter.

- **Chapter Two: Theoretical**

In this chapter, the theoretical foundations of the thesis are presented. It includes a comprehensive review of Blockchain Technology, its principles, and its applications. The chapter also explores the impact of DDoS attacks on network systems, examining their consequences and challenges. Additionally, it discusses the criteria used for evaluating DDoS mitigation systems.

- **Chapter Three: System Design and Implementation**

The aim of this chapter is to elucidate the design and implementation of the proposed system. It provides a detailed explanation of the system's architecture, emphasizing the integration of Blockchain Technology for DDoS mitigation. The chapter covers the various aspects of the system's design, including the selection of appropriate components and technologies.

- **Chapter Four: System Implementation and Evaluation**

This chapter focuses on the practical implementation of the system. It outlines the stages involved in deploying the proposed system and describes the evaluation methodology used to assess its performance. The chapter presents the results obtained from testing the system and analyses the findings to determine its effectiveness in mitigating DDoS attacks.

Chapter Five: Conclusions

The final chapter presents the conclusions drawn from the research. It summarizes the key findings, highlighting the contributions made by the study. The chapter also addresses the limitations of the research and suggests potential directions for future studies in the field of DDoS mitigation using Blockchain Technology.

CHAPTER TWO
THEORETICAL BACKGROUND

2.1 Introduction

This chapter contains an overview of the main axes: (the blockchain, and DDoS attack). And various defensive measures for DDoS attack. As well provides an overview of Blockchain technology, its structure, features, and its most important applications. And criteria used in the evaluation and describes some of the basic terms used in building the proposed system for these axes separately.

2.2 Distributed Denial of Service (DDoS)

A Distributed Denial of Service (DDoS) attack is a deliberate effort to render an online service inaccessible by inundating it with traffic from numerous sources, frequently facilitated by botnets or a concerted hacktivist endeavor. Cyber attackers pose a significant obstacle to disseminating, retrieving, and retrieving crucial information by targeting various vital resources, including financial institutions and media outlets [17].

2.3 Common types of DDoS attacks are as follows:

- The User Datagram Protocol (UDP) is a networking protocol that operates without a session. A denial-of-service attack, a UDP flood, is designed to inundate a computer or network with a high volume of User Datagram Protocol (UDP) packets directed at random ports. The host checks to determine the presence of any application that may be listening at the designated ports. However, the search yields no results, indicating the absence of any such application [18].

- An HTTP flood is a type of DDoS attack that involves overwhelming a web server with many HTTP requests in a short time. This can result in the server becoming unresponsive or crashing, denying legitimate users access to the website. The HTTP Flood phenomenon pertains to the exploitation of legitimate GET or POST requests by a hacker. This

particular type of attack consumes minimal bandwidth yet has the potential to compel the server to utilize its maximum available resources. **[19]**.

- The Ping of Death attack is sending malicious pings to a targeted system in order to manipulate IP protocols. About twenty years ago, this specific kind of distributed denial-of-service (DDoS) attack was quite popular, although its effectiveness has since decreased **[19]**.

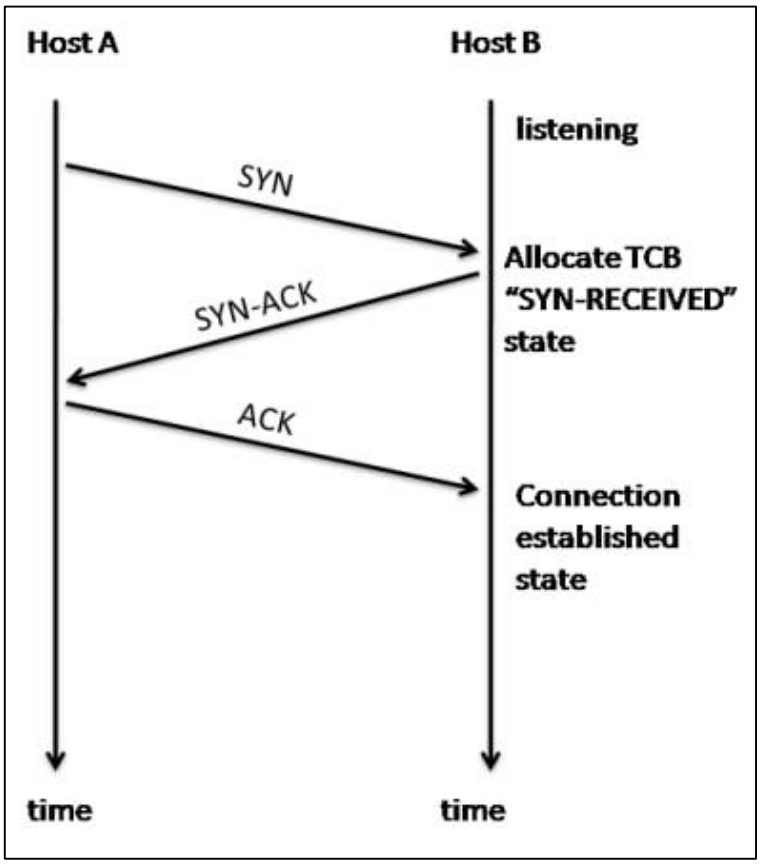


Figure (2. 1) TCP three-way handshaking [19]

- A denial of service (DoS) attack known as a SYN flood uses the Transmission Control Protocol's (TCP) three-way handshake procedure to overload a targeted server with a deluge of connection requests, eventually rendering it unavailable to genuine traffic. A denial-of-service attack known as a SYN flood takes use of flaws in the TCP connection sequence, also known as the three-way handshake. As shown in Figure

(2.1) [18], the offender sends out a string of SYN requests to the target system in an attempt to exhaust sufficient server resources and make the system unresponsive to authorized traffic[18].

2.4 Technical details of a typical SYN Flood attack:

Typically, during the initiation of a TCP connection from a client to a server, a sequence of messages is exchanged between the two entities. This sequence naturally follows a predetermined pattern:

- Initiating a connection by the client involves the transmission of a SYN (synchronize) message to the server.
- The server acknowledges the client's request through the transmission of an SYN-ACK response.
- Upon receipt of the acknowledgment (ACK) from the client, the connection is successfully established.

The process referred to as the TCP three-way handshake serves as the fundamental basis for all connections initiated through the employment of the TCP protocol. The SYN flood attack operates by withholding the anticipated ACK code from the server. The malevolent client can refrain from transmitting the anticipated ACK or manipulating the source IP address in the SYN to induce the server to dispatch the SYN-ACK to a counterfeit IP address. This counterfeit IP address will not issue an ACK as it is cognizant of the fact that it did not transmit a SYN. If the source IP address is accessible, the host shall receive a SYN+ACK from the target server without any prior connection request. In this scenario, the source will transmit an RST packet to the server, resulting in the server resetting the connection. Hence, it is advantageous for a perpetrator to fabricate source addresses that are not associated with hosts that can be accessed from the server targeted by the attack. The objective of the TCP SYN flooding attack

is to exhaust the backlog by endeavoring to transmit a sufficient number of SYN segments to occupy the entire backlog. The minimal level of CPU and network bandwidth that an attacker needs to conduct a persistent attack is insignificant [20].

2.5 Prevention Techniques against DDoS

In order to mitigate the risk and impact of Distributed Denial of Service (DDoS) attacks, various defense and response mechanisms have been proposed to establish a more cyber resilient environment. These defensive measures aim to enhance the security posture of the targeted systems and reduce the likelihood of successful DDoS attacks.

2.5.1 DDoS Attack Defense Method Based on Blockchain

The proposed approach involves the initial extraction of network traffic features from edge nodes, followed by a detailed analysis of the extracted data features to identify any abnormal behavior exhibited by terminal devices. The final step involves the deployment of smart contracts within the blockchain network to facilitate the implementation of attack node information and access control strategies, thereby enabling effective defense against DDoS attacks. The smart contract facilitates the synchronization of DDoS attack node information and defense strategy, thereby circumventing network congestion of the central node and conferring a temporal advantage for attack defense [12].

2.5.2 DDoS Attack Defense Method Using Machine Learning Techniques

By employing machine learning techniques, a greater number of attacks can be effectively managed. Machine learning techniques can yield low positive values with high precision. The Tree Based classifier is employed as a technique for feature selection, which facilitates the

identification of optimal features and minimizes processing time. The CICDDoS2019 dataset was subjected to several classification models, including the KNN classifier, Decision Tree Classifier, and Random Forest, with the Tree Based classifier serving as the feature selection method. The dataset encompasses various types of Distributed Denial of Service (DDoS) attacks that were gathered by the Canadian Institute of Cyber Security. Subsequently, upon identification of the malevolent nature of the packet, the IP address associated with the request is recorded in the Blockchain, thereby rendering any further alteration of the stored IP address impossible. The server in question retrieves the IP address that has been blacklisted from the Blockchain and subsequently imposes a temporary block on it [13].

2.5.3 DDoS Attack Detection using Fast Entropy Approach on Flow Based Network Traffic

The fast entropy method has been utilized to enhance the detection of DDoS attacks through flow-based analysis. The utilization of the thresholding algorithm was deemed necessary due to the temporal variability of network activities and user behavior. During a specific timeframe, the flow count is computed for every connection. If the disparity between the entropy of the flow count at each moment and the mean entropy value of that particular timeframe surpasses the threshold value, a DDoS attack is identified. The adaptive update of the threshold value is contingent upon the prevailing traffic pattern condition [21].

2.5.4 DDoS Attack Defense Method Clustering-Based LDDoS Detection Method

One of the techniques used is Low-rate Distributed Denial of Service (LDDoS), a secure technology, was used to measure attack penetration and secure communication flow. Two data sets were used, broad data sets and any LBNL. Adopting the two-step aggregation method, which enables the

network traffic to be controlled using the discrete-sense TCP traffic characteristics, the results were performed using the NS-2 network simulator version 2. The suspicious group was detected with abnormal analysis.[22]

2.6 The Types of Blockchain

There are primarily three types of blockchains based on their accessibility and control:

2.6.1 Public blockchain architecture

Public Blockchains: Public blockchains are open and decentralized networks that are accessible to anyone. They allow anyone to participate, validate transactions, and contribute to the consensus mechanism of the blockchain. Public blockchains, such as Bitcoin and Ethereum, are maintained by a distributed network of nodes, and anyone can join the network, validate transactions, and create new blocks. These blockchains are transparent, secure, and provide a high degree of censorship resistance. Public blockchains are often used for cryptocurrencies, decentralized applications (DApps), and global peer-to-peer transactions [23].

It's worth noting that within these broad categories, there can be variations and combinations. For example, some blockchains may have elements of both public and private access, allowing for different levels of participation and visibility. Additionally, there are also hybrid blockchains that leverage multiple blockchain types to accommodate various requirements and use cases [24] As shown in Figure (2.2)

2.6.2 Private blockchain architecture

Private blockchains, also known as permissioned blockchains, are restricted networks where access and participation are limited to specific entities or participants. These blockchains are often used within organizations, consortia, or specific industry groups. Unlike public

blockchains, private blockchains have predefined access controls and permissions, allowing only authorized participants to validate and maintain the blockchain. Private blockchains offer higher scalability and faster transaction processing compared to public blockchains but sacrifice some decentralization and censorship resistance [23] [24]. As shown in Figure (2.2)

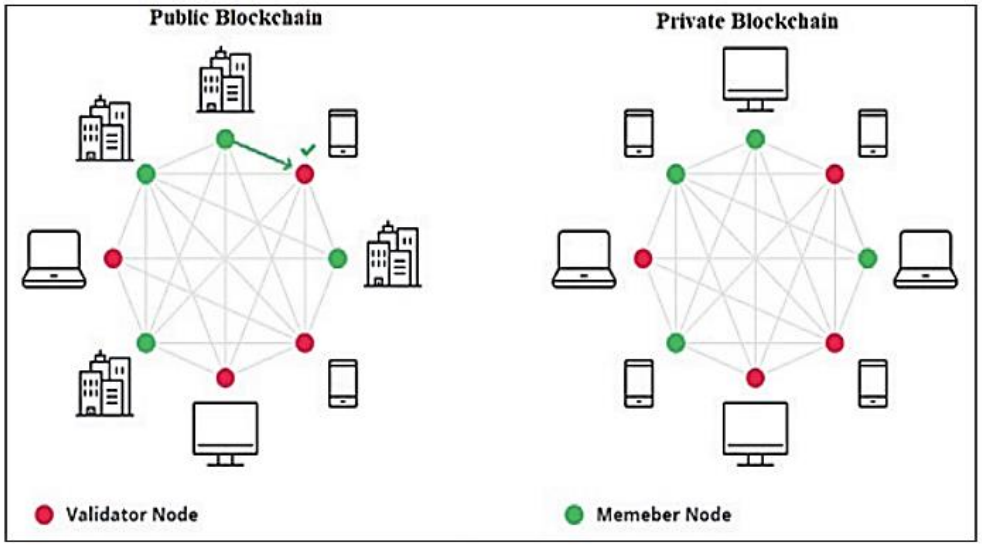


Figure (2. 2) public and private blockchains[23]

2.6.3 Consortium blockchain architecture

Consortium blockchains are a hybrid between public and private blockchains. They are governed and maintained by a group of organizations or entities rather than a single central authority. Consortium blockchains are designed for collaborative use cases where multiple organizations want to share and transact data in a trusted and verifiable manner. The consensus mechanism in consortium blockchains is usually permissioned, allowing predefined participants to validate transactions and maintain the blockchain. Consortium blockchains strike a balance between the openness of public blockchains and the controlled access of private blockchains [23] [24].

2.7 Blockchain Technology

The transaction of currencies among peoples or companies are often subjected to centralization and control by a third party. Digital payments or currency transfers demand a bank/credit card provider functioning as middleman for completing the transacting process, rather than having the two main entities involved in the transaction in control. This often demands an additional fee. Similar processes occur in a variety of other domains like gaming, music, and software [25].

The main aim of blockchain technology is solving this issue, as it creates a decentralized environments with no third party in charge of the transaction. Blockchain technology seems to be a revolution in terms of computer protocol employed to record and store information digitally on multiple devices or multiple nodes. Among the crucial elements of Blockchain is the so-called “Ledger”, similar to a relational database [26].

A Blockchain represents a list of encrypted digital records or transactions referred to as blocks. Each of these blocks is then “chained” to the next one, in a linear, chronological order, using a cryptographic signature [27].

Each block contains a copy of the last transaction made after adding the last block. Thus, the shared block, or ledger, is linked to all participants who use computers within a network to validate or confirm transactions, and so the need for a third-party is eliminated [25].

The blockchain technology is utilized to ensure the safeguarding and dissemination of information in a novel and distinctive manner. The removal of a central authority within a distributed network represents a significant transition towards the direct exchange of transactions among non-intermediaries. The process of updating the blockchain is contingent upon

unanimous agreement among system participants, thereby rendering any modification or removal of a transaction impossible. The decentralized nature of distributed databases precludes any potential for hacking, manipulation, or disruption, in contrast to traditional centralized databases that rely on user-controlled access systems. To clarify, the information contained within a Blockchain is considered to be immutable, meaning that once it has been recorded onto the ledger, it cannot be altered or removed by any party, including those with administrative privileges. The application of Blockchain Technology is versatile and can be extended to various transactions involving value, including but not limited to monetary transactions, exchange of goods, ownership of land, maintenance of medical records, and electoral voting. This is made possible due to the time-stamped nature of each data block and its chronological linkage through cryptographic signatures [25].

Data migration is unnecessary in a blockchain initiative as all pertinent transactions are documented and maintained on the ledger, from which the status is subsequently derived. The decentralized nature of blockchain technology, which lacks a central control point or authority and is not regulated by a singular control center, ensures that there is no single point of failure. Theoretically, it could be inferred that the monitoring of security in a blockchain database within an enterprise may not require the expertise of an IT professional.

2.7.1 Blockchain Architecture

Blockchain architecture refers to the underlying structure and design principles of a blockchain network. It defines how the network is organized, how transactions are processed, and how consensus is reached among participants., as illustrated in Figure (2.3) [28].

2.7.2 Peer to Peer (P2P) Network

A peer-to-peer (P2P) network is a decentralized network architecture in which participants, known as peers, interact directly with each other without the need for a central server or authority. In a P2P network, each peer can act as both a client and a server, allowing for resource sharing and collaboration among the participants.

Here are some key characteristics and concepts related to P2P networks :

- **Decentralization:** P2P networks are decentralized, meaning there is no central point of control. Instead, each peer is equal and has the ability to initiate connections and share resources directly with other peers. [24]
- **Peer autonomy:** Each peer in a P2P network has autonomy and can make independent decisions. Peers can join or leave the network at any time without affecting the overall operation of the network. [24]
- **Resource sharing:** One of the main purposes of P2P networks is resource sharing. Peers can share various types of resources such as files, computing power, storage space, or network bandwidth. Examples of popular P2P file-sharing protocols include BitTorrent and eDonkey. [25]
- **Distributed file systems:** P2P networks can be used to create distributed file systems where files are divided into small pieces and stored across multiple peers. This approach improves scalability and fault tolerance, as files can still be accessed even if some peers are offline. [25]
- **Search and discovery:** P2P networks often employ distributed search algorithms to locate resources across the network. Peers

can use techniques such as distributed hash tables (DHTs) or gossip protocols to locate and retrieve resources from other peers. [29]

- **Security and trust:** P2P networks face challenges related to security and trust, as there is no central authority to enforce rules or authenticate participants. Various mechanisms, such as reputation systems, cryptographic techniques, and consensus algorithms, can be used to enhance security and establish trust among peers. P2P networks have enabled scalable and resilient systems that can leverage the collective resources of a large number of peers. However, they also present challenges related to security, scalability, and efficient resource discovery. As technology continues to evolve, P2P networks continue to find applications in various domains, fostering collaboration and decentralization. [24]

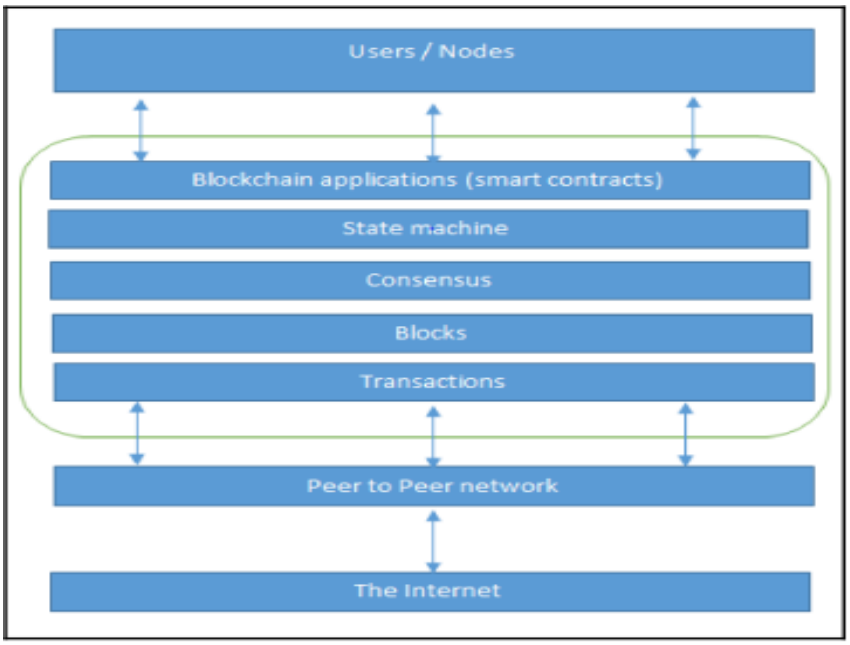


Figure (2. 3) Network view of a Blockchain[30]**.**

2.7.3 Block

The basic building block of a blockchain is called a "block." A block is a data structure that contains a collection of transactions and other relevant information. It serves as a permanent record of a set of transactions that have occurred within a specific timeframe.

Here are some key characteristics and components of a block in a blockchain :

- **Header:** The block header contains metadata and essential information about the block, including a reference to the previous block (previous block hash), a timestamp indicating when the block was created, a unique identifier (block hash), and other relevant data. [30]
- **Transactions:** The block includes a set of transactions that have been validated and grouped together. These transactions represent the actions or data exchanges that have taken place within the blockchain network. The specific format and structure of transactions vary depending on the blockchain protocol being used. [30]
- **Merkle Tree:** To ensure the integrity and efficiency of transaction verification, many blockchains use a Merkle tree structure. A Merkle tree is a hierarchical data structure that summarizes all the transactions in a block by creating a unique hash (Merkle root) that represents the entire set of transactions. This allows for efficient verification of the transaction data. [31]
- **Nonce:** A nonce (number used once) is a random value included in the block header. Miners in a proof-of-work blockchain network perform computations to find a nonce value that results in a hash value that meets certain criteria or difficulty level. This

process is known as mining and is used to secure the blockchain network and reach consensus. [31]

- **Size and Limitations:** Each block has a maximum size limit, which varies depending on the blockchain protocol. For example, in the Bitcoin blockchain, the block size is limited to 1 megabyte (MB). This size limitation helps ensure that blocks can be propagated and validated efficiently within the network. [32]
- **Linking Blocks:** Blocks are linked together in a linear fashion, forming a chain of blocks, hence the name "blockchain." Each block contains a reference (previous block hash) to the hash of the previous block in the chain. This linkage creates an immutable and chronological order of blocks, providing the security and integrity of the blockchain. [32]

By continuously adding new blocks to the chain, the blockchain grows over time, creating a tamper-resistant and transparent ledger of transactions. The structure of blocks and their linkage ensures the integrity and consistency of the data stored within the blockchain network.

A useful instrument for comprehending and creating blockchain-based business models is the block structure. As shown in Figure (2.4), it offers a high-level summary of the various elements of a blockchain-based business model and how they work together.

One of the main components of blockchain technology is the generic chain of blocks. It offers a method for safe and impenetrable data storage. Numerous distinct blockchain-based business models may be implemented using the generic chain of blocks. as seen in Figure (2.5).

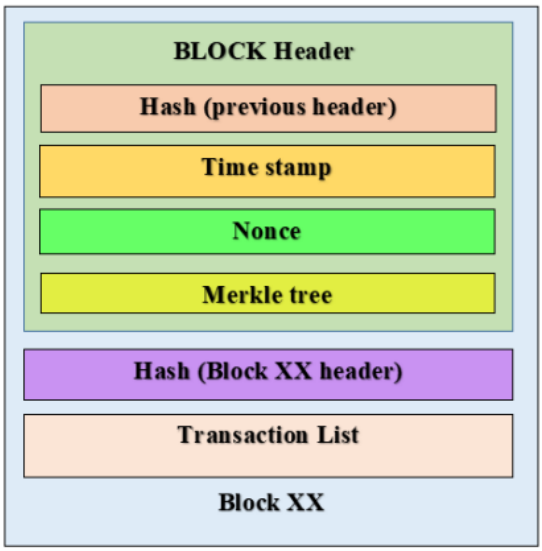


Figure (2. 4) Block structure (Generalized) [33].

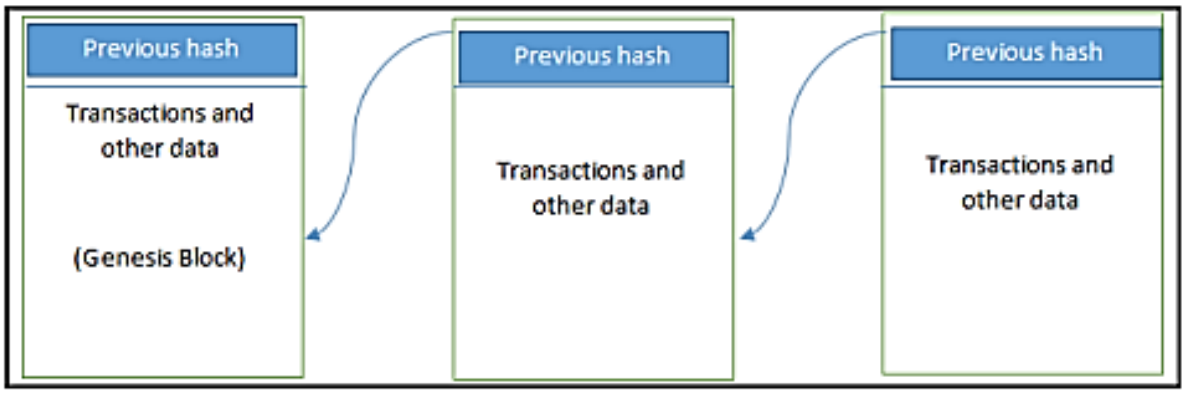


Figure (2. 5) Generic chain blocks[30].

2.7.4 Transaction

In the context of blockchain, a transaction refers to the transfer of data or value from one participant to another within the blockchain network. It represents a specific action or operation that alters the state of the blockchain.

Here are some key aspects of transactions in a blockchain [34] [35]:

- **Participants:** Transactions involve at least two participants, often referred to as the sender and the receiver. These participants could be individuals, organizations, or entities interacting within the blockchain network.

- **Data or Value Transfer:** Transactions can involve the transfer of various types of data or value. In cryptocurrency blockchains like Bitcoin or Ethereum, transactions typically involve the transfer of digital currencies from one address to another. In other blockchain applications, transactions may involve the exchange of assets, tokens, or even the execution of smart contracts.
- **Structure:** A transaction consists of relevant information, including the sender's address or public key, the recipient's address, the amount or value being transferred, and any additional data or instructions associated with the transaction. The specific structure and content of a transaction depend on the blockchain protocol being used.
- **Verification and Validation:** Before a transaction is considered valid and included in a block, it needs to be verified and validated by participants within the blockchain network. This process typically involves checking the digital signatures, ensuring the sender has sufficient funds or assets, and confirming that the transaction complies with the predefined rules and protocols of the blockchain.
- **Consensus Mechanisms:** Transactions are validated and agreed upon through consensus mechanisms employed by the blockchain network. Different blockchain protocols use various consensus algorithms, such as proof-of-work (PoW), proof-of-stake (PoS), or delegated proof-of-stake (DPoS), to achieve agreement and secure the network.
- **Transaction Fee:** Some blockchain networks require participants to pay a transaction fee as an incentive for miners or validators to include their transactions in the blocks. The fee

helps prioritize transactions and prevents spam or denial-of-service attacks.

- **Immutable Record:** Once a transaction is included in a block and added to the blockchain, it becomes a permanent and immutable part of the ledger. It cannot be altered or deleted, ensuring transparency, auditability, and the integrity of the blockchain's transaction history.

Transactions play a fundamental role in blockchain by enabling the transfer of value, executing smart contracts, and recording interactions within the network. They provide the basis for creating decentralized applications, enabling secure and transparent digital transactions across various industries [28].

2.7.5 Ledger

A ledger, in the context of blockchain, refers to a distributed and decentralized database that records all transactions and data exchanges within a blockchain network. It serves as a transparent and immutable record of all activities and changes made within the blockchain. Here are some key aspects of a ledger in the blockchain context [29]:

- **Distributed and Decentralized:** The ledger in a blockchain is distributed across multiple nodes or computers participating in the network. Every participating node maintains a copy of the entire ledger. This decentralization ensures redundancy, fault tolerance, and prevents a single point of failure. [36]
- **Transaction Records:** The ledger contains a chronological sequence of transactions, each representing a specific action or data exchange within the blockchain network. These transactions are organized into blocks and linked together in a chain formation, creating the blockchain. [36]

- **Immutable and Tamper-Resistant:** Once a transaction is recorded in the ledger and added to a block, it becomes immutable, meaning it cannot be altered or deleted. This immutability ensures the integrity and trustworthiness of the ledger, as any attempt to tamper with previous transactions would require a consensus from a majority of participants, making it extremely difficult to manipulate the data. [37]
- **Transparency and Auditability:** The ledger is transparent, meaning that all participants can view and verify the transactions recorded within it. This transparency fosters trust and accountability within the network, as all participants have access to the same information. Additionally, the public nature of the ledger enables auditing and verification of transactions, promoting accountability and reducing the need for trust in centralized authorities. [37]
- **Consensus Mechanisms:** The ledger's integrity and consistency are maintained through consensus mechanisms employed by the blockchain network. These mechanisms ensure that all participants agree on the validity and order of transactions recorded in the ledger. Different consensus algorithms, such as proof-of-work (PoW) or proof-of-stake (PoS), are used to achieve agreement and secure the ledger.
- **Smart Contract Execution:** In addition to transaction records, the ledger can also store and execute smart contracts. Smart contracts are self-executing programs that automatically execute predefined actions when certain conditions are met. The ledger maintains the state and execution history of smart contracts, allowing for decentralized and automated interactions. [36]

- **Privacy Considerations:** Depending on the blockchain protocol, the ledger may offer different levels of privacy. Some blockchains, like Bitcoin, provide pseudonymity, where transactions are associated with cryptographic addresses rather than real-world identities. Other blockchains, such as privacy-focused ones like Monero or Zcash, incorporate additional privacy features to protect the confidentiality of transaction data. [36]

2.7.6 Smart Contract

A smart contract is a self-executing computer program that automatically enforces and executes the terms of an agreement or contract. It operates on a blockchain platform and is designed to facilitate, verify, or enforce the negotiation or performance of a contract without the need for intermediaries [38] .

Here are some key aspects of smart contracts:

- **Automation:** Smart contracts automate the execution of predefined actions or conditions based on the rules and terms encoded within the contract. Once the conditions are met, the contract is automatically executed, and the specified actions are performed without the need for manual intervention. [38]
- **Blockchain-based Execution:** Smart contracts are typically executed on blockchain platforms, such as Ethereum, which provide a decentralized and secure environment for the execution and storage of smart contracts. The blockchain ensures transparency, immutability, and reliability, as the contract's code and execution history are recorded and verified by multiple nodes in the network. [38]
- **Self-Enforcement:** Smart contracts are designed to be self-enforcing, meaning that they automatically enforce the agreed-upon terms and conditions without relying on intermediaries or centralized authorities. The execution of a smart contract is deterministic and follows predefined rules, ensuring fairness and eliminating the need for trust in a third party. [39]
- **Digital Agreement:** Smart contracts represent digital agreements between parties. The terms and conditions of the contract are written in code and stored on the blockchain. This

digital nature eliminates the need for traditional paper-based contracts and streamlines the process of agreement creation, execution, and enforcement. [39]

- **Programmability:** Smart contracts can be programmed to perform a wide range of functions beyond simple transactional transfers. They can incorporate complex logic, conditional statements, and calculations, allowing for the implementation of sophisticated business logic, financial operations, or multi-party interactions. [39]
- **Transparency and Auditability:** The execution and outcome of smart contracts are transparent and auditable. The contract's code and transaction history are recorded on the blockchain, making it accessible to all participants. This transparency enhances trust, as all parties can verify the execution and outcomes of the contract. [38]
- **Interoperability:** Smart contracts can interact and interoperate with other smart contracts, enabling complex and interconnected business processes. This capability allows for the development of decentralized applications (DApps) and the creation of ecosystems where multiple smart contracts collaborate to achieve common goals. [40]

Limitations: Smart contracts are limited to executing actions based on the information available on the blockchain. They cannot directly interact with external data sources that reside outside the blockchain network. However, solutions such as oracles can be used to connect smart contracts with real-world data and external systems [40].

2.8 Blockchain Networks Applications

Blockchain networks have found applications in various industries and sectors due to their decentralized and secure nature. Here are some popular applications of blockchain networks:

2.8.1 Voting Systems

Blockchain networks can enable secure and transparent voting systems. Each vote is recorded on the blockchain, ensuring immutability and preventing fraud or manipulation.[41]

2.8.2 Decentralized Finance (DeFi)

Blockchain networks have given rise to decentralized finance applications. These platforms provide financial services like lending, borrowing, trading, and asset management without the need for traditional intermediaries.[42]

2.8.3 Healthcare

Blockchain networks can improve data security and interoperability in the healthcare industry. They enable secure sharing of patient data among healthcare providers while maintaining privacy and consent management.[43]

2.8.4 Intellectual Property Protection

Blockchain networks can be used to establish proof of ownership and protect intellectual property rights. Artists, musicians, and content creators can timestamp their work on the blockchain to establish a verifiable record of creation.[44]

2.8.5 Energy Trading

Blockchain networks can facilitate peer-to-peer energy trading by enabling direct transactions between energy producers and consumers. This

can help optimize energy distribution and reduce reliance on centralized energy providers.[45]

2.8.6 Gaming

Blockchain networks can be utilized in gaming to enable ownership and trading of in-game assets. Players have true ownership of their virtual assets, and blockchain ensures transparency and security in asset transactions.[46]

2.9 Neural Network

A neural network is a computational model inspired by the structure and functioning of the human brain. It consists of interconnected nodes called neurons that work together to process and transmit information. Neural networks are widely used in artificial intelligence and machine learning applications for tasks such as pattern recognition, classification, regression, and optimization. [47]

The basic building block of a neural network is a neuron, which receives input signals, applies weights to those inputs, performs a summation, and applies an activation function to produce an output. Neurons are organized into layers, with an input layer that receives the initial data, one or more hidden layers that perform intermediate computations, and an output layer that produces the final result.[47]

During the training phase, neural networks adjust the weights of the connections between neurons using a learning algorithm, This process involves feeding the network with training data, comparing the predicted output to the desired output, and updating the weights based on the difference between them. repeating this process, neural networks can learn to make accurate predictions or classifications [16].

2.10 DATASETS

CICDDoS2019 is a dataset that was created for research purposes to study and analyze DDoS (Distributed Denial of Service) attacks. It provides a collection of network traffic data related to DDoS attacks, specifically focusing on the detection and classification of such attacks.

The dataset contains various features or attributes that describe network traffic behavior during DDoS attacks. These features may include information such as packet length, inter-arrival time, packet count, source and destination IP addresses, port numbers, and protocol types.

The dataset is labeled, meaning that each instance or data point is assigned a class label indicating whether it corresponds to a DDoS attack or normal network traffic.

By utilizing the CICDDoS2019 dataset, researchers can develop and test different algorithms and techniques to improve the detection accuracy of DDoS attacks.

The availability of labeled datasets like CICDDoS2019 is crucial for advancing the field of security and developing effective defense mechanisms against DDoS attacks.[48]

2.10 .1 Cross-validation techniques

Cross-validation techniques' basic idea is Splitting data into training and test subsets .the first subset used for the training model, while the other subset used to evaluate the model. There are various methods from

Cross-validation. The most commonly used types of cross-validation common are hold-out cross-validation .

2.10 .2 Hold-out cross-validation

The simplest type of cross-validation is hold-out (or validation), commonly used as a validation process. Unlike other approaches, it only divides the produced dataset into a training and testing dataset once. The training dataset is made up of a randomly chosen part of the data, while the testing dataset is made up of the remaining data. The benefit of this approach is that it takes less computational load. However, its evaluation can have a high variance. As shown in Figure (2.6)

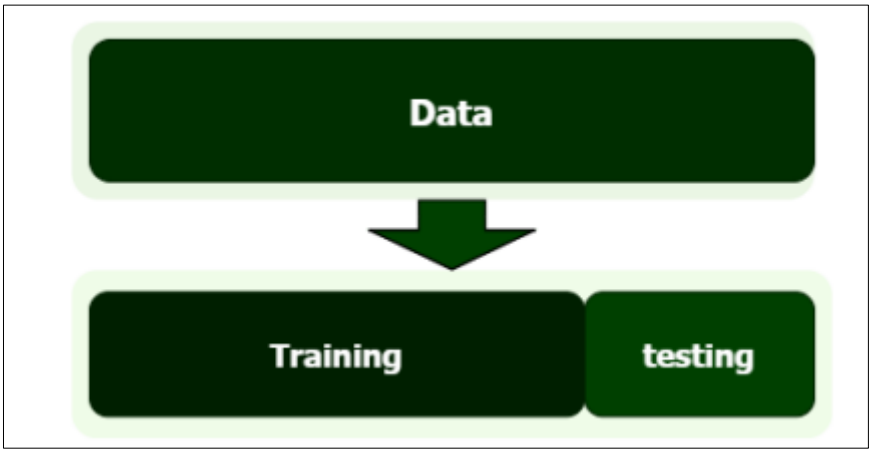


Figure (2.6): Hold-out cross-validation

2.11 The Criteria Used in the Evaluation

There is a set of criteria that have been selected to evaluate the proposed system, despite the lack of evaluation methods for the blockchain system being a recent system, but a set of these criteria has been proposed the following**:**

2.11.1 Accuracy

refers to how close a measured or calculated value is to the true or expected value. In other words, accuracy is a measure of how well a system or process can produce results that are consistent with a known standard or reference point. In different fields and contexts, accuracy can be measured and evaluated in different ways [49].

$$Accuracy=(TP+TN)/(TP+TN+FP+FN) \quad \ldots (2.1)$$

2.11.2 Mean Squared Error (MSE):

The Mean Squared Error (MSE) is a metric used in machine learning and statistics to calculate the average squared difference between a model's predicted and actual values. It is widely used as a loss function in regression situations to minimize the difference between predicted and true values.[50]

2.11.3 confusion matrix

A confusion matrix is a table that is used to evaluate the performance of a classification model. It describes the model's predictions on a test dataset and compares them to the actual class labels. True positive (TP), true negative (TN), false positive (FP), and false negative (FN) are the four components of the confusion matrix. It aids in comprehending the model's accuracy, precision, recall, and robustness.[51]

2.11.4 Recall

Recall is a metric that measures the proportion of genuine positive instances accurately detected by a classification model. It is also known as sensitivity or true positive rate. The ratio of true positive (TP) forecasts to

the sum of true positive and false negative (FN) predictions is used to compute it.[52]

$$Recall=TP/(TP+FN) \quad \dots (2.2)$$

2.11.5 Precision

Precision is a metric that calculates the proportion of accurately predicted positive cases among all positive examples predicted by a classifier. The ratio of true positive (TP) predictions to the sum of true positive and false positive (FP) predictions is used to compute it.[53]

$$Precision=TP/(TP+FP) \quad \dots (2.3)$$

2.11.6 F1 score

The F1 score is a model accuracy metric that combines precision and recall into a single result. It is a balanced evaluation of a classifier's performance because it is the harmonic mean of precision and recall. The F1 score is especially beneficial when the class distribution is skewed .[54]

$$F1\ score = 2 * (precision * recall) / (precision + recall) \quad \dots (2.4)$$

2.11.7 Specificity

The proportion of actual negative cases properly detected by a classifier is measured by specificity. The ratio of true negative (TN) predictions to the sum of true negative and false positive (FP) forecasts is used to compute it. Specificity is frequently utilized in medical diagnostics and binary classification situations where recognizing negatives accurately is critical.[55]

$$Specificity = TN / (TN + FP) \quad \dots (2.5)$$

2.11.8 Program Execution Time

The time it takes for a computer program or algorithm to complete its execution is referred to as program execution time. It is a critical performance parameter that is often measured in seconds or milliseconds. Faster execution times suggest that the software is more efficient and responsive.[56]

CHAPTER THREE
THE
PROPOSED SYSTEM
USING BC

3.1 Introduction

The proposed system aims to enhance network security by implementing a multi-level approach to detect and mitigate potential attacks. The system consists of a server and auxiliary nodes connected in a peer-to-peer architecture. The server handles client requests, while the auxiliary nodes assist in identifying the type of sender.

To simulate realistic network traffic, the system utilizes the CICDDOS219 dataset. This dataset provides suitable scenarios and data representations for the system's requirements.

The detection process involves two levels. During Level 1 detection, the auxiliary nodes analyze redirected requests and extract the sender's IP address. They initiate a connection request to the IP address and evaluate the response. An open or up status indicates a normal client, while a closed or down status signifies a potentially malicious sender.

If an attack is suspected, the system escalates it to Level 2, which utilizes a trained neural network for further analysis. The neural network classifies and categorizes incoming traffic based on patterns associated with malicious behavior. If the traffic is classified as malicious, it is added to a blacklist or blocklist, effectively preventing further access to the system.

By employing this multi-level approach, the system can proactively detect and mitigate potential attacks, enhancing network security and protecting the system's integrity.

3.2 The Mechanism of the Proposed System

After the server receives a high number of requests that exceed its processing capacity, they are distributed to the nodes in a round-robin fashion every 5 seconds. This ensures that each node gets a fair share of the incoming requests for processing.

At Level 1, the nodes perform an initial detection phase. If a node suspects that it is under attack, it forwards the IP address of the suspicious traffic to Level 2 for further analysis using the neural network.

The values t1 and t2 are used to calculate a 5-second interval. These values help determine when the traffic should be redirected to the nodes.

During Level 1 detection, each node utilizes the perform early identification of potentially malicious traffic. If a node fails to establish a connection or receives a "close" result it considers the IP address associated with the suspicious traffic and forwards it to Level 2.

Level 2 detection involves the use of a neural network. The neural network has been trained on a dataset of known suspicious traffic, enabling it to classify and categorize incoming traffic. It evaluates the IP address forwarded from Level 1 and determines if it exhibits patterns associated with suspicious or malicious behavior.

If the neural network classifies the traffic as suspicious, it is added to a blacklist or blocklist, indicating that it should be blocked or prevented from accessing the system.

By following this process, the system detects and mitigates potential attacks. This multi-level approach enhances the system's ability to proactively identify and block potential threats, ensuring the security and integrity of the system. As shown in Figure (3.1).

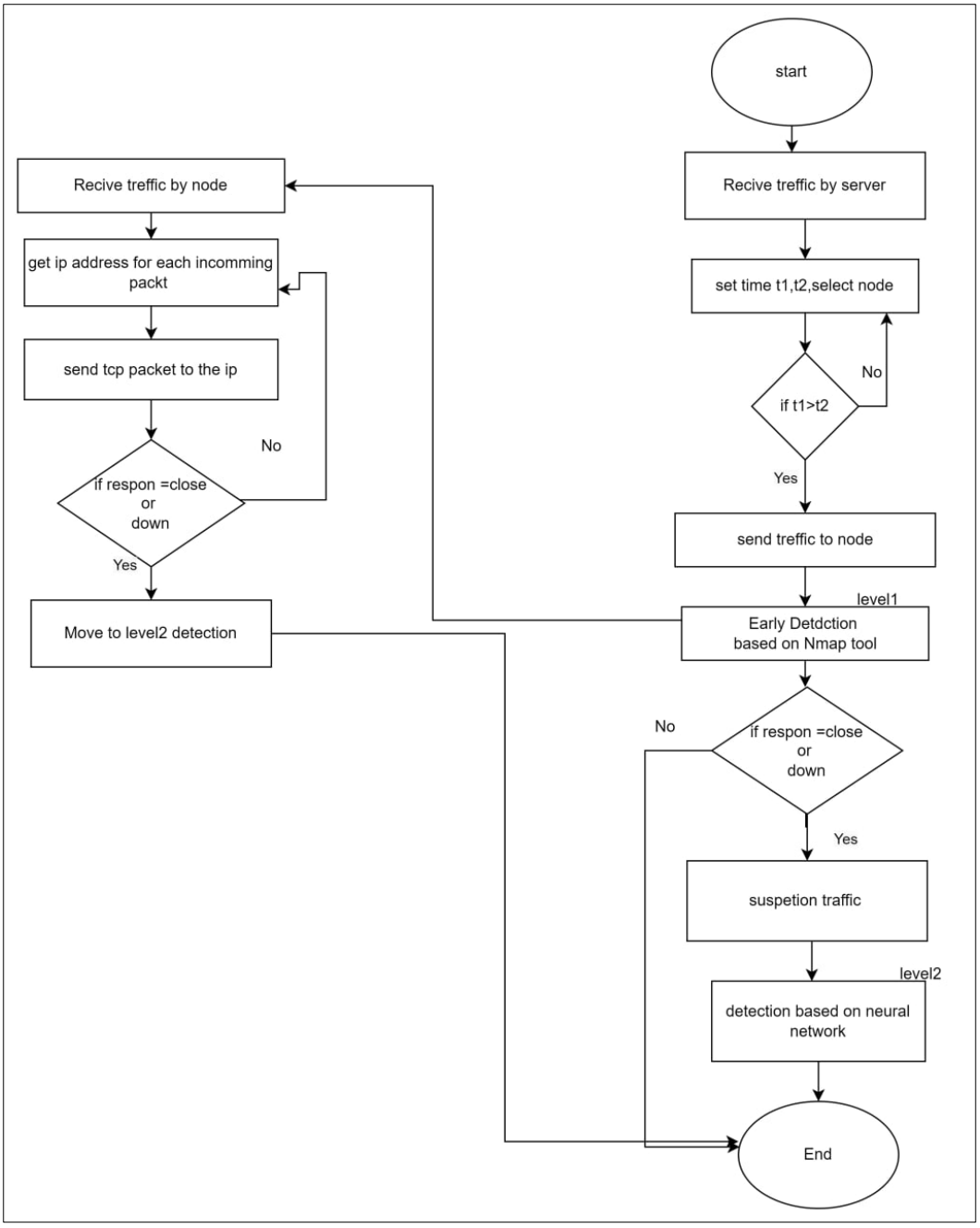


Figure (3. 1) Flowchart of the proposed system.

3.3 Algorithm for a neural network

A feed-forward neural network, also known as a multilayer perceptron (MLP), is one of the most common types of artificial neural networks. It is a type of artificial neural network where information flows in only one direction, from the input layer through the hidden layers (if any) to the output layer, without any loops or feedback connections.

The basic building block of a feed-forward neural network is a neuron or a node. Each neuron takes input values, applies weights to those inputs, performs a summation, and applies an activation function to produce an output. The output of one neuron becomes the input to the next neuron in the network.

A feed-forward neural network typically consists of three types of layers:

1. Input Layer: This layer receives the input data and passes it to the next layer. The number of neurons in the input layer corresponds to the number of input features.

2. Hidden Layers: These layers are located between the input and output layers. Each hidden layer consists of multiple neurons, and the number of hidden layers and neurons within each layer can vary. The hidden layers perform nonlinear transformations on the input data, extracting higher-level features and representations.

3. Output Layer: This layer produces the final output of the network. The number of neurons in the output layer depends on the specific task. For example, in a classification problem with multiple classes, the number of output neurons would equal the number of classes.

During the training phase of a feed-forward neural network, the weights and biases of the neurons are adjusted iteratively using various optimization algorithms, such as gradient descent, to minimize the difference between the predicted output and the desired output. This process is known as backpropagation. The network learns to make better predictions by updating the weights and biases based on the errors calculated during the backpropagation process.

3.4 The proposed system stepes

The proposed system for (DDoS) attacks based on blockchain involves the following steps:

- **Step 1: The Network Creation and Configuration**

The proposed system consists of two types of nodes: the server and auxiliary nodes. The server is responsible for receiving and responding to client requests, while auxiliary nodes are connected to the server and assist in detecting the type of sender. The system employs a peer-to-peer connection architecture, with four auxiliary nodes directly connected to the server and all nodes interconnected.

- **Step 2: Traffic Simulation**

To simulate traffic for the system, the CICDDOS219 dataset was utilized due to its modern nature and suitability for the system's requirements. This dataset provides realistic scenarios and data that can effectively represent various types of network traffic.

- **Step 3: Traffic Redirection**

When the server is flooded with requests beyond its processing capacity, it redirects the requests to the connected auxiliary nodes. This redirection occurs in a round-robin manner, distributing the requests evenly among the nodes for further analysis.

- **Step 4: Attack Detection**

Upon receiving redirected requests, each auxiliary node examines the request to determine if it originated from an attacker or a normal client. The node extracts the sender's IP address from the incoming packet and initiates a connection request to that IP address. Based on the response

received, the node determines whether the sender is a normal client or a spoofed one.

- If the response indicates an open or up status, the client is considered normal (Figure 3.2A).
- If the response indicates a closed or down status, there was no response from the client, indicating a spoofed client (Figure 3.2B).

— Step 5: Countermeasures

When an attack is detected, it is escalated to the second level of analysis for more accurate classification using a Neural Network. This additional layer of classification enhances the system's ability to distinguish between different types of attacks and respond accordingly with appropriate countermeasures.

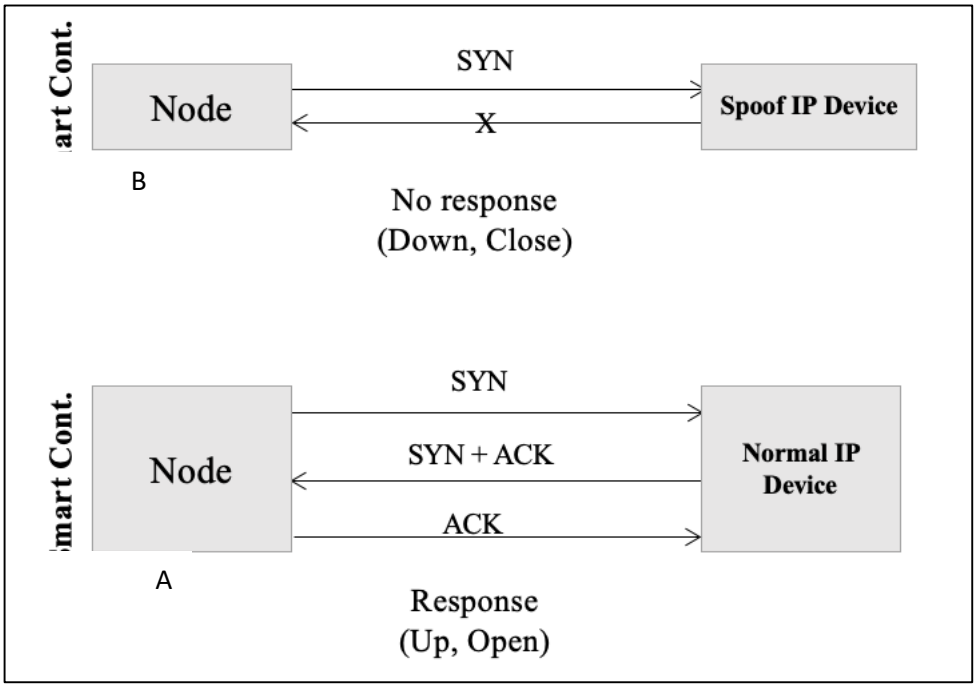


Figure (3. 2) Discovering process of normal and attack traffic.

3.5 Integrating Neural Networks into Smart Contracts

The integration of neural networks into smart contracts enables various applications such as price prediction for assets or identification of counterfeit items. By incorporating neural networks, complex smart contracts can adapt to changing conditions and learn from new data, enhancing their functionality.

Smart contract neural network nodes are responsible for executing neural network-based smart contracts within blockchain networks. These nodes require more powerful hardware and software capabilities due to the computationally intensive nature of neural network operations. The training and execution of neural networks within smart contracts can be resource-intensive, posing challenges for implementation.

To address these challenges, several solutions are being developed. Some blockchain platforms are working on developing specialized hardware and software specifically designed for neural networks. These advancements aim to optimize the performance of neural network-based smart contracts on blockchain systems, making their implementation more feasible.

3.6 ML-Based Detection Approach

There are many ML techniques applicable to DDoS detection. This study applies Neural Network Feed Forward machine learning classifiers to perform the classification task for identifying the DDoS traffic. This section and its subsections explain the main techniques of the ML stage, such as dataset, preprocessing, feature selection, and how the suitable classifier has been chosen.

3.6.1 Datasets

The CICDoS2019 dataset is a comprehensive dataset that has been developed by the Canadian Institute for Cybersecurity (CIC). It consists of millions of records of both legitimate and malicious traffic.

The data was collected from the Canadian Institutes of Cybersecurity (CIC) honeypot network during the period from August to October 2019. The data set is designed to enable the development of new machine learning algorithms that can accurately detect and classify DDoS attacks. It divided into two parts, namely the benign traffic and the malicious traffic. The benign traffic consists of normal user-initiated activities such as web browsing, email, file transfers, etc. The malicious traffic includes various types of network-based attacks such as TCP SYN floods, UDP floods, ICMP floods, etc see Table (3.1). All the traffic is labeled according to its type. For example, all the malicious traffic is labeled as ‘malicious’ while all the benign traffic is labeled as ‘benign’. The CICDDoS2019 dataset also contains several features that can be used to characterize the traffic. These features include the source and destination IP addresses, ports, packet length, payload size, protocol, flags, etc. All the records in the dataset also contain the timestamp of when the traffic was generated. This helps in understanding the timing of the attack and can be used for further analysis. Overall, the CICDDoS2019 dataset provides an excellent platform for researchers and practitioners to develop new machine-learning algorithms for accurately detecting and classifying DDoS attacks. It is a great resource for the development of new machine-learning algorithms that can accurately detect and classify DDoS attacks.

Table (3.1): CICDDoS-2019 dataset summary

Dataset DDos Attack Files	Label	Quantity	Ratio Percentage	The Total Number
SYN	BENIGN	389	0.03	1,380,404
	DDoS _Syn	1,380,015	99.97	

Over the course of working days, network traffic flows were recorded, and 84 features were retrieved as shown in Table (3.2).

Table (3.2): The features of the CICIDS2019 Dataset

No	Feature Name	No	Feature Name	No	Feature Name
1	Flow ID	29	Fwd IAT Std	57	ECE Flag Count
2	Source IP	30	Fwd IAT Max	58	Down/Up Ratio
3	Source Port	31	Fwd IAT Min	59	Average Packet Size
4	Destination IP	32	Bwd IAT Total	60	Avg Fwd Segment Size
5	Destination Port	33	Bwd IAT Mean	61	Avg Bwd Segment Size
6	Protocol	34	Bwd IAT Std	62	Fwd Avg Bytes/Bulk
7	Timestamp	35	Bwd IAT Max	63	Fwd Avg Packets/Bulk
8	Flow Duration	36	Bwd IAT Min	64	Fwd Avg Bulk Rate
9	Total Fwd Packets	37	Fwd PSH Flags	65	Bwd Avg Bytes/Bulk
10	Total Backward Packets	38	Bwd PSH Flags	66	Bwd Avg Packets/Bulk
11	Total Length of Fwd Packets	39	Fwd URG Flags	67	Bwd Avg Bulk Rate
12	Total Length of Bwd Packets	40	Bwd URG Flags	68	Subflow Fwd Packets
13	Fwd Packet Length Max	41	Fwd Header Length	69	Subflow Fwd Bytes
14	Fwd Packet Length Min	42	Bwd Header Length	70	Subflow Bwd Packets
15	Fwd Packet Length Mean	43	Fwd Packets/s	71	Subflow Bwd Bytes
16	Fwd Packet Length Std	44	Bwd Packets/s	72	Init_Win_bytes_forward
17	Bwd Packet Length Max	45	Min Packet Length	73	Init_Win_bytes_backward
18	Bwd Packet Length Min	46	Max Packet Length	74	act_data_pkt_fwd
19	Bwd Packet Length Mean	47	Packet Length Mean	75	min_seg_size_forward
20	Bwd Packet Length Std	48	Packet Length Std	76	Active Mean

21	Flow Bytes/s	49	Packet Length Variance	77	Active Std
22	Flow Packets/s	50	FIN Flag Count	78	Active Max
23	Flow IAT Mean	51	SYN Flag Count	79	Active Min
24	Flow IAT Std	52	RST Flag Count	80	Idle Mean
25	Flow IAT Max	53	PSH Flag Count	81	Idle Std
26	Flow IAT Min	54	ACK Flag Count	82	Idle Max
27	Fwd IAT Total	55	URG Flag Count	83	Idle Min
28	Fwd IAT Mean	56	CWE Flag Count	84	Label

3.6.2 Feature Selection

Feature selection methods play an important role in improving model performance, there is a tradeoff between the number of features and the time complexity of an algorithm, the more features model leads to the most time complexity and the most accuracy, and vice versa. The number of features in the data set is 84. Reduce the number of features to enhance the current study.

Based on previous research on feature selection, the chosen features for the "Ip address normal" are Packet Length Mean and Fwd IAT. These variables represent the mean packet length and the forward inter-arrival time for normal IP addresses.

On the other hand, for the "Ip address attack," the selected feature can either have the maximum value or the minimum value, depending on the specific context or criteria being considered.

CHAPTER FOUR
IMPLEMENTATION AND RESULTS

4.1 Introduction

This section presents a comprehensive analysis of the outcomes achieved in each stage of the proposed approach, as outlined in Chapter 3. The results are presented in the same order as described in Chapter 3. Additionally, a comparative analysis is conducted to evaluate the effectiveness of the proposed approach in comparison to similar studies. The section also provides a detailed account of the implementation steps undertaken during the thesis.

4.2 Dataset

CICDDoS2019 datasets consists of (50063112) instances including (50006249) DDoS attacks and (56863) instances of benign (legitimate) network traffic,with more than 80 features along with 13 class labels to predict DDoS attacks.

4.2.1Min-Max Normalized Results

This proposed system used min-max normalized with 0 as a new minimum value and 1 as a new maximum value, the range of results is between 0 and Figure (4.1) show a sample from the normalized dataset.

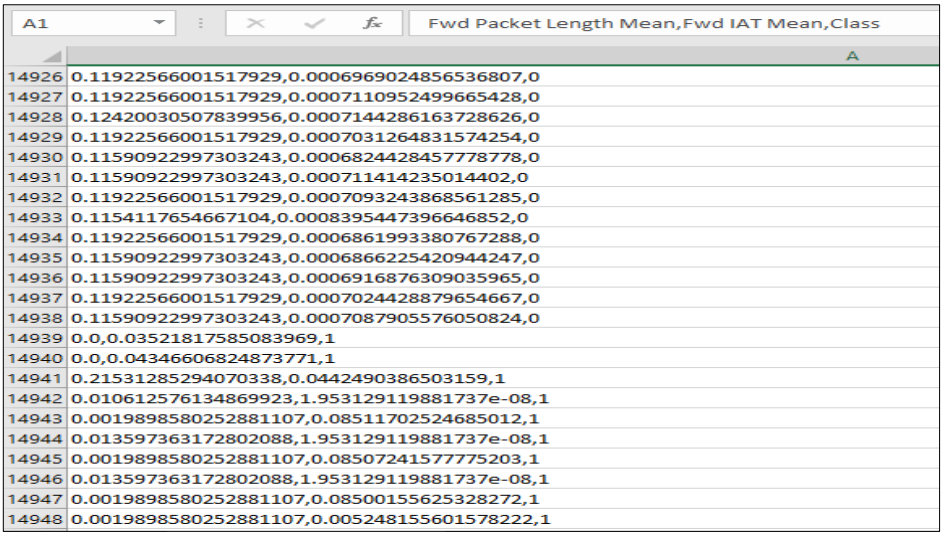


Figure (4.1): sample from min-max normalized of dataset

4.3 The network implementation and result

A blockchain network has been implemented consisting of a server and four node. Each node serves as a smart contract responsible for detecting whether the traffic is normal or an attack. Through these smart contracts, traffic patterns are analyzed to identify and differentiate between normal and attack behavior.

4.3.1 Level 1 Detection in implementation and result

The Nmap tool was utilized to conduct an initial detection of potential attacks on the smart contract. The results revealed a discovery of a spoofed IP address. When the sender's IP address was used in the three-way handshake process, no response was received from this IP. Consequently, it was forwarded to the second stage of deep detection for further analysis. Figure (4.2) shows the process of detecting a suspicious IP

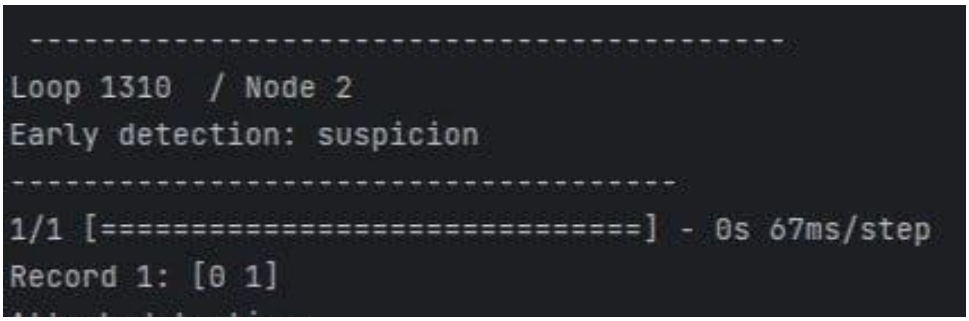


Figure (4. 2) suspicious traffic

4.3.2 Level 2 Detection(neural network)

This part was implemented on the same network as in the following steps:

4.3.2.1Building the model

The system for detecting DDoS attacks involves constructing a model with a server and neighboring nodes, where the neighboring nodes incorporate a Neural Network. Neighbor nodes represent a blockchain network that is connected peer to peer with each other The server is designed

to handle up to 1000 requests. In the event that the number of requests surpasses the server's processing capacity, they are redirected to the neighboring nodes in order to alleviate the server's workload. The model is tested using the remaining data from the dataset, with 30% allocated for the testing phase, as 70% of the data was used during the model construction phase, which yielded results. showed in Figure (4.3)

```
Epoch 1/100
9437/9437 [==============================] - 15s 1ms/step - loss: 0.1370 - accuracy: 0.9505 - val_loss: 0.1341 - val_accuracy: 0.9545
Epoch 2/100
9437/9437 [==============================] - 14s 1ms/step - loss: 0.1167 - accuracy: 0.9550 - val_loss: 0.1083 - val_accuracy: 0.9585
Epoch 3/100
9437/9437 [==============================] - 15s 2ms/step - loss: 0.1044 - accuracy: 0.9606 - val_loss: 0.0935 - val_accuracy: 0.9644
Epoch 4/100
9437/9437 [==============================] - 15s 2ms/step - loss: 0.0940 - accuracy: 0.9636 - val_loss: 0.0891 - val_accuracy: 0.9661
Epoch 5/100
9437/9437 [==============================] - 14s 1ms/step - loss: 0.0907 - accuracy: 0.9645 - val_loss: 0.0859 - val_accuracy: 0.9659
Epoch 6/100
9437/9437 [==============================] - 14s 1ms/step - loss: 0.0889 - accuracy: 0.9648 - val_loss: 0.0870 - val_accuracy: 0.9660
Epoch 7/100
9437/9437 [==============================] - 14s 1ms/step - loss: 0.0881 - accuracy: 0.9647 - val_loss: 0.0848 - val_accuracy: 0.9652
Epoch 8/100
9437/9437 [==============================] - 14s 1ms/step - loss: 0.0869 - accuracy: 0.9650 - val_loss: 0.0874 - val_accuracy: 0.9652
Epoch 9/100
9437/9437 [==============================] - 14s 1ms/step - loss: 0.0863 - accuracy: 0.9651 - val_loss: 0.0817 - val_accuracy: 0.9672
Epoch 10/100
9437/9437 [==============================] - 14s 1ms/step - loss: 0.0857 - accuracy: 0.9657 - val_loss: 0.0888 - val_accuracy: 0.9644
Epoch 11/100
9437/9437 [==============================] - 13s 1ms/step - loss: 0.0853 - accuracy: 0.9656 - val_loss: 0.0813 - val_accuracy: 0.9672
Epoch 12/100
9437/9437 [==============================] - 14s 1ms/step - loss: 0.0854 - accuracy: 0.9658 - val_loss: 0.0825 - val_accuracy: 0.9666
Epoch 13/100
9437/9437 [==============================] - 14s 2ms/step - loss: 0.0845 - accuracy: 0.9656 - val_loss: 0.0803 - val_accuracy: 0.9674
Epoch 14/100
9437/9437 [==============================] - 14s 1ms/step - loss: 0.0839 - accuracy: 0.9658 - val_loss: 0.0830 - val_accuracy: 0.9670
Epoch 15/100
9437/9437 [==============================] - 14s 2ms/step - loss: 0.0835 - accuracy: 0.9658 - val_loss: 0.0805 - val_accuracy: 0.9668
Epoch 16/100
9437/9437 [==============================] - 14s 1ms/step - loss: 0.0833 - accuracy: 0.9661 - val_loss: 0.0819 - val_accuracy: 0.9660
Epoch 17/100
9437/9437 [==============================] - 14s 2ms/step - loss: 0.0832 - accuracy: 0.9663 - val_loss: 0.0796 - val_accuracy: 0.9672
Epoch 18/100
9437/9437 [==============================] - 14s 2ms/step - loss: 0.0827 - accuracy: 0.9660 - val_loss: 0.0810 - val_accuracy: 0.9672
```

Figure (4. 3) Training Steps

Figure (4.4) show the results for Accuracy of a training model

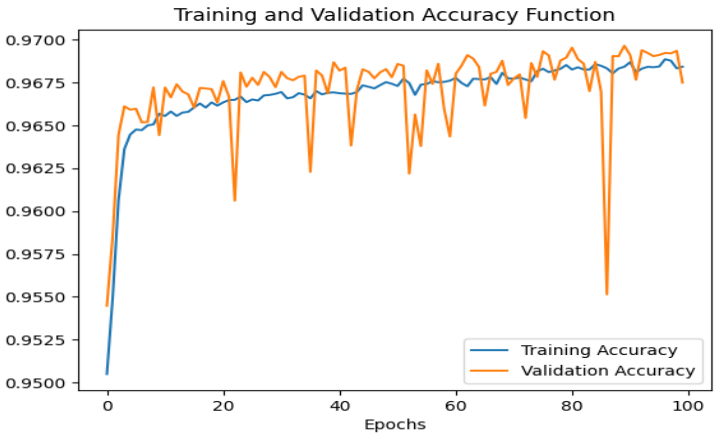


Figure (4. 4) Training and validation accuracy function

Figure (4.5)show the results for loss function

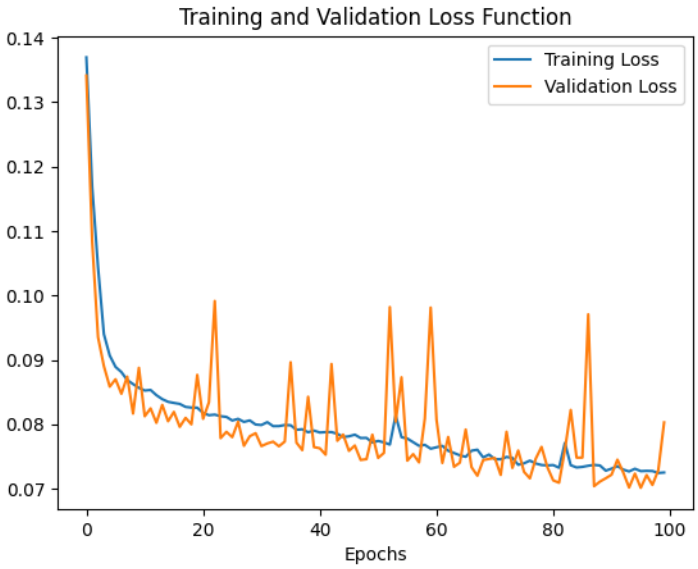


Figure (4. 5) Training and validation loss function

4.3.3.2 Discovery Stage

After constructing the model and achieving satisfactory results during the testing phase, the next step involves deploying the model onto the blockchain network environment. This deployment is done to leverage the blockchain network's capabilities in order to detect potentially suspicious or malicious activities, such as attacks targeting the system.

By placing the model on the blockchain network, it becomes an integral part of the network's infrastructure. This allows for continuous monitoring and analysis of incoming data and transactions within the network. The model utilizes its detection algorithms and neural network capabilities to identify any luxury or abnormal activities that could potentially indicate an attack on the system.

The blockchain network provides a decentralized and transparent environment, enabling the model to verify and validate the integrity of transactions and network activities. Through this deployment, the model contributes to the overall security and resilience of the blockchain network

by actively identifying and mitigating potential attacks or fraudulent actions. showed in Figure (4.6)

A
Fwd Packet Length Mean,Fwd IAT Mean,Class
348,43326.2,Attack
401,2,Attack
383,48,Attack
349.5,35773,Attack
359.5,35757,Attack
401,48,Attack
383,1,Attack
359.5,36380.668,Attack
401,1,Attack
348,43166.8,Attack
383,1,Attack
383,1,Attack
359.5,35814.332,Attack
349.5,36204.332,Attack
386,36905.668,Attack
348,42776.2,Attack
349.5,35049.668,Attack
375,1,Attack
359.5,35953,Attack
483.3,Attack

Figure (4. 6) Before preprocess

During the preprocessing phase, two specific properties, namely packet length mean and inter-arrival time (IAT), were selected for inclusion in the model. These properties were chosen based on their relevance to DDoS attack behavior and to keep the model focused without unnecessary complexity. By considering the packet length mean, which represents the average size of packets, and the IAT, which indicates the time interval between successive packets, the model can effectively capture and analyze patterns related to DDoS attacks. These properties play a crucial role in identifying and distinguishing abnormal network traffic associated with such attacks, enabling the model to accurately detect and mitigate potential threats. showed in Figure (4.7)

Fwd Packet Length Mean,Fwd IAT Mean,Class
0.1154117654667104,0.0008462166287382012,0
0.13298884469008873,3.906258239763474e-08,0
0.12701927061422438,9.375019775432338e-07,0
0.11590922997303243,0.0006986928800552938,0
0.11922566001517929,0.0006983803793961128,0
0.13298884469008873,9.375019775432338e-07,0
0.12701927061422438,1.953129119881737e-08,0
0.11922566001517929,0.0007105614207154967,0
0.13298884469008873,1.953129119881737e-08,0
0.1154117654667104,0.0008431033409211098,0
0.12701927061422438,1.953129119881737e-08,0
0.12701927061422438,1.953129119881737e-08,0
0.11922566001517929,0.0006995001473831234,0
0.11590922997303243,0.0007071173509506621,0
0.12801419962686844,0.0007208153485948758,0
0.1154117654667104,0.0008354744185788516,0
0.11590922997303243,0.0006845652721298709,0
0.12436612658050691,1.953129119881737e-08,0
0.11922566001517929,0.0007022085124710809,0

Figure (4. 7) After preprocess

Figure show the normal traffic where no attack has been detected showed in Figure (4.8).

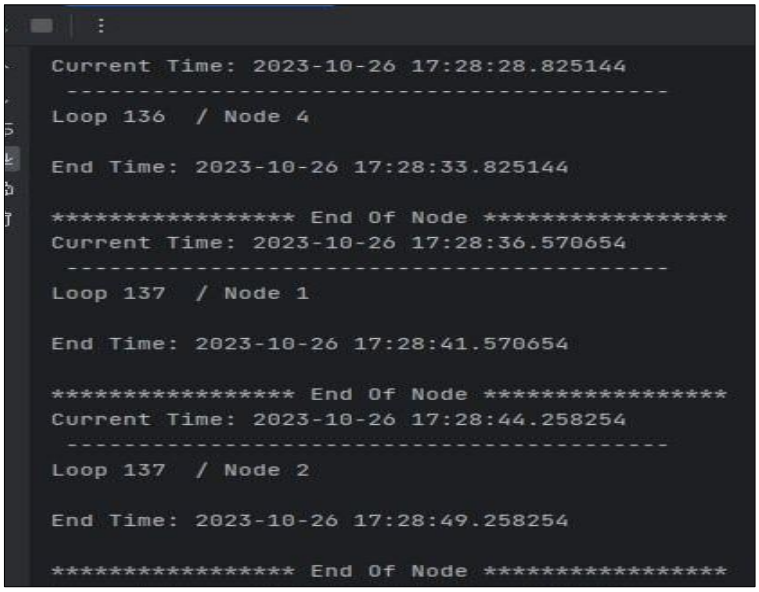


Figure (4. 8):Normal traffic

appears that the image signifies the detection of suspicious traffic movement. Consequently, this traffic data was sent to a neural network for deep analysis. As a result, the neural network classified this traffic as an attack and it was subsequently blocked and added to a blacklist showed in Figure (4.9), Figure (4.10)

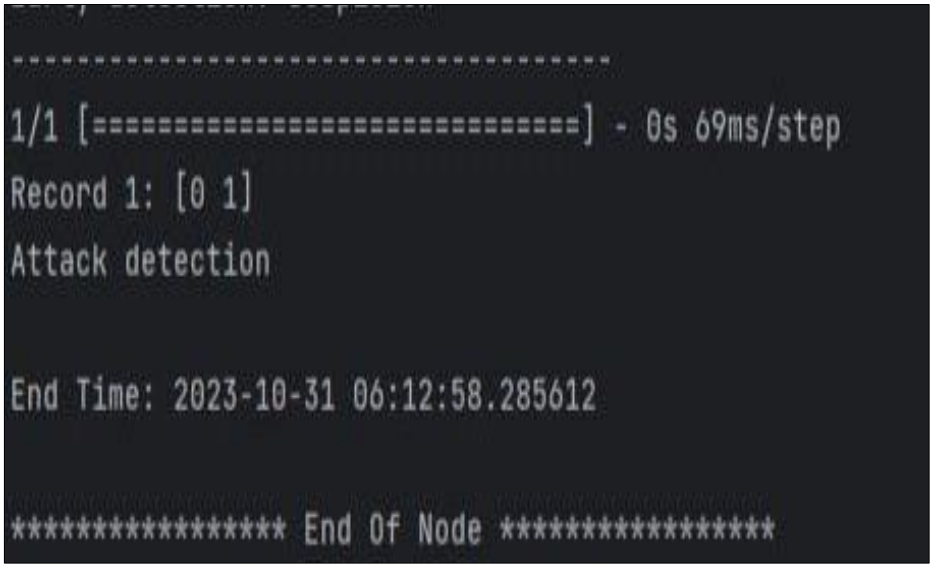


Figure (4. 9) attack detection

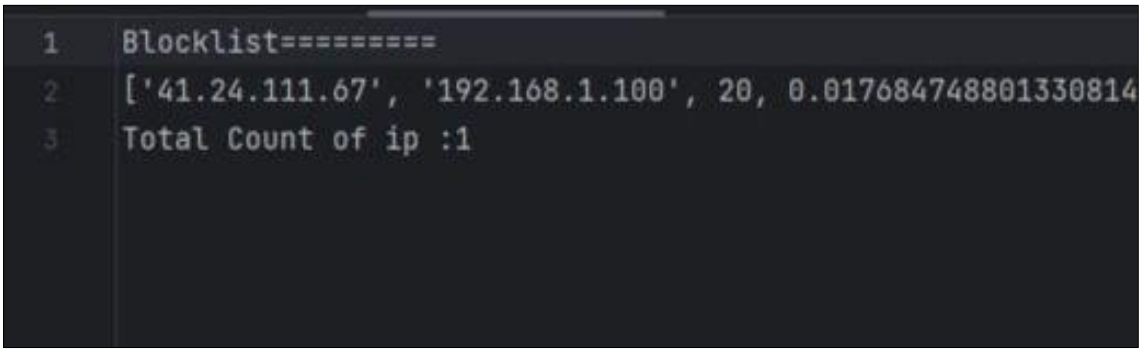


Figure (4. 10) IP blocking in the block list

4.3The Evaluation

Through the results obtained during the previous section, the proposed system can be evaluated based on some criteria as follows:

The evaluation metrics and performance results of a model.

Confusion Matrix:

Table (4.1): confusion matrix

	Normal	**Attack**
Normal	**TN**(329897)	**FP**(3643)
Attack	**FN**(10,297)	**TP**(87,534)

Accuracy	0.967684429
Recall	0.894747064
Precision	0.960044748
F1-Score	0.926246508
Specificity	0.989077772
Program Execution Time	17.1501677
Mean Squared Error (MSE)	0.032315571

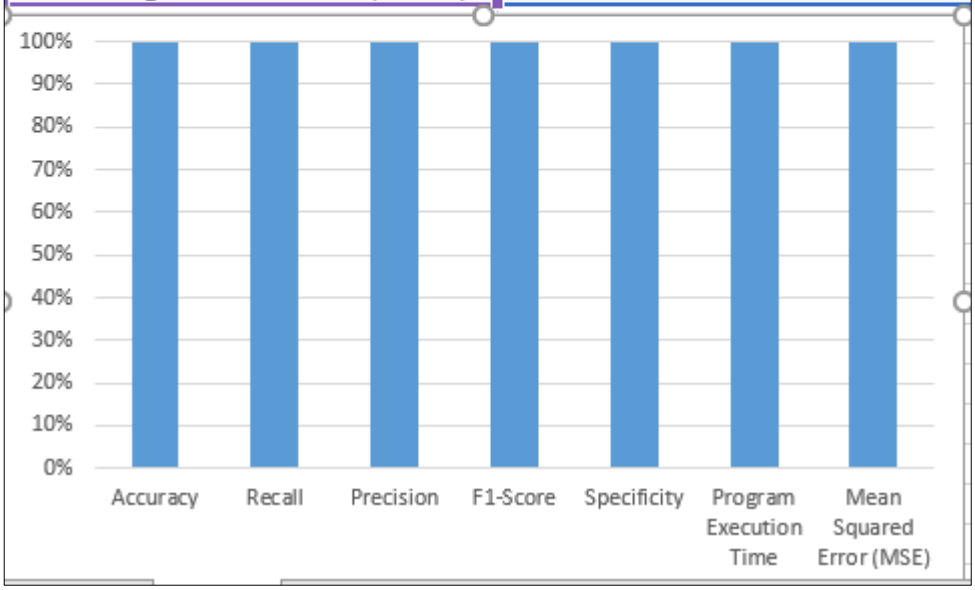


Figure (4.11): Evaluation results for testing data

CHAPTER FIVE
CONCLUSION
AND
FUTURE WORKS

5.1 Conclusion

This thesis explores the use of blockchain technology and artificial neural networks to combat Distributed Denial of Service (DDoS) attacks. The proposed decentralized blockchain solution effectively redirects excessive requests from the target server to auxiliary nodes, alleviating strain and maintaining accessibility for legitimate users. By integrating artificial neural networks within the blockchain, the system achieves accurate classification of network traffic and detection of potential DDoS attacks.

The two-level approach employed in the system, utilizing the Nmap tool for initial testing and early detection, followed by the trained neural network for advanced classification, proves to be effective in identifying and detection DDoS attacks.

The accuracy, precision, recall, F1-Score, and specificity values obtained in the evaluation demonstrate the system's ability to correctly identify both malicious and normal traffic instances.

The results of this thesis highlight the potential of blockchain and neural networks as powerful system for DDoS mitigation. By implementing this network security approach, enterprises can protect their operations and ensure uninterrupted service for legitimate users, safeguarding against the disruptive impact of DDoS attacks.

5.2 Futre works

1. In future research, the system can improve its ability to detect and mitigate DDoS attacks more effectively, adapt to evolving attack techniques, and handle larger-scale attacks with improved methods.

2. The continuous evolution of blockchain and neural network technologies offers promising opportunities for advancing DDoS detection strategies and strengthening overall network security.

References

References:

[1] N. Tripathi and B. Mehtre, “DoS and DDos Attacks: Impact, Analysis and Countermeasures,” *Proc. Natl. Conf. Adv. Comput. Netw. Secur.*, no. July, pp. 1–6, 2013.

[2] K. M. Prasad, A. R. M. Reddy, and K. V. Rao, “DoS and DDoS Attacks: Defense, Detection and TracebackMechanisms -A Survey,” *Glob. J. Comput. Sci. Technol.*, vol. 14, no. 7, p. 19, 2014.

[3] S. Wani, M. Imthiyas, H. Almohamedh, K. M. Alhamed, S. Almotairi, and Y. Gulzar, “Distributed denial of service (Ddos) mitigation using blockchain—a comprehensive insight,” *Symmetry (Basel).*, vol. 13, no. 2, pp. 1–21, 2021, doi: 10.3390/sym13020227.

[4] M. Najafimehr, S. Zarifzadeh, and S. Mostafavi, “A hybrid machine learning approach for detecting unprecedented DDoS attacks,” *J. Supercomput.*, vol. 78, no. 6, pp. 8106–8136, 2022, doi: 10.1007/s11227-021-04253-x.

[5] I. O. Adam and M. Dzang Alhassan, “Bridging the global digital divide through digital inclusion: the role of ICT access and ICT use,” *Transform. Gov. People, Process Policy*, vol. 15, no. 4, pp. 580–596, 2020, doi: 10.1108/TG-06-2020-0114.

[6] Z. Chen and Y. Zhu, “Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging,” *Proc. - 2017 IEEE 6th Int. Conf. AI Mob. Serv. AIMS 2017*, pp. 93–99, 2017, doi: 10.1109/AIMS.2017.31.

[7] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, “A blockchain-based architecture for collaborative DDoS mitigation with smart contracts,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol.

10356 LNCS, pp. 16–29, 2017, doi: 10.1007/978-3-319-60774-0_2.

[8] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, "Mitigating IoT device based DDoS attacks using blockchain," in *CRYBLOCK 2018 - Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Part of MobiSys 2018*, Jun. 2018, pp. 71–76. doi: 10.1145/3211933.3211946.

[9] K. Kim, Y. You, M. Park, and K. Lee, "DDoS Mitigation: Decentralized CDN Using Private Blockchain," *Int. Conf. Ubiquitous Futur. Networks, ICUFN*, vol. 2018-July, pp. 693–696, 2018, doi: 10.1109/ICUFN.2018.8436643.

[10] Z. Ahmed, S. M. Danish, H. K. Qureshi, and M. Lestas, "Protecting IoTs from mirai botnet attacks using blockchains," *IEEE Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD*, vol. 2019-Septe, pp. 1–6, 2019, doi: 10.1109/CAMAD.2019.8858484.

[11] A. R. Jamader, P. Das, and B. R. Acharya, "BcIoT: Blockchain based ddos prevention architecture for IoT," *2019 Int. Conf. Intell. Comput. Control Syst. ICCS 2019*, no. Iciccs, pp. 377–382, 2019, doi: 10.1109/ICCS45141.2019.9065692.

[12] M. Chen, X. Tang, J. Cheng, N. Xiong, J. Li, and D. Fan, "A DDoS Attack Defense Method Based on Blockchain for IoTs Devices," *Commun. Comput. Inf. Sci.*, vol. 1253 CCIS, pp. 685–694, 2020, doi: 10.1007/978-981-15-8086-4_64.

[13] D. V. V. S. Manikumar and U. Maheswari, "Blockchain Based DDoS Mitigation Using Machine Learning Techniques," 2020.

[14] S. Badruddoja, R. Dantu, L. Widick, Z. Zaccagni, and K. Upadhyay, "Integrating DOTS with blockchain can secure massive IoT sensors," *Proc. - 2020 IEEE 34th Int. Parallel Distrib. Process. Symp. Work.*

IPDPSW 2020, pp. 937–946, 2020, doi: 10.1109/IPDPSW50202.2020.00156.

[15] V. Patel, F. Khatiwala, and Y. Choksi, “An Approach to Detect and Prevent Distributed Denial of Service Attacks Using Blockchain Technology in Cloud Environment,” *Lect. Notes Electr. Eng.*, vol. 676, pp. 247–258, 2021, doi: 10.1007/978-981-15-6229-7_20.

[16] R. F. Ibrahim, Q. A. Al-haija, and A. Ahmad, “DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology,” 2022.

[17] S. T. Zargar, J. Joshi, and D. Tipper, “A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks,” *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013, doi: 10.1109/SURV.2013.031413.00127.

[18] M. Azahari Mohd Yusof, F. Hani Mohd Ali, and M. Yusof Darus, “Detection and Defense Algorithms of Different Types of DDoS Attacks,” *Int. J. Eng. Technol.*, vol. 9, no. 5, pp. 410–444, 2018, doi: 10.7763/ijet.2017.v9.1008.

[19] R. M. Bani-hani and Z. Al-ali, “SYN Flooding Attacks and Countermeasures : A Survey,” no. November 2016, 2013.

[20] M. Singhof, “Analysis of DDoS detection systems,” *CEUR Workshop Proc.*, vol. 1020, pp. 22–27, 2013.

[21] J. David and C. Thomas, “DDoS attack detection using fast entropy approach on flow-based network traffic,” *Procedia Comput. Sci.*, vol. 50, pp. 30–36, 2015, doi: 10.1016/j.procs.2015.04.007.

[22] D. Method, “Implementation of a Clustering-Based LDDoS,” pp. 1–17, 2022.

[23] P. K. Paul, “Blockchain Technology and its Types—A Short Review,” *Int. J. Appl. Sci. Eng.*, vol. 9, no. 2, pp. 189–200, 2021, doi: 10.30954/2322-0465.2.2021.7.

[24] C. S. T. G. O. V Sa, “Overview and Opportunities of Blockchain Technology,” pp. 1–26.

[25] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, no. October, pp. 557–564, 2017, doi: 10.1109/BigDataCongress.2017.85.

[26] A. Kaur and V. Singh Sankhala, “Blockchain Technology in India-Prospects and Challenges,” *IOSR J. Econ. Financ.*, vol. 10, no. 4, pp. 28–40, 2019, doi: 10.9790/5933-1004012840.

[27] O. Juszczyk and K. Shahzad, “Blockchain Technology for Renewable Energy: Principles, Applications and Prospects,” *Energies*, vol. 15, no. 13, pp. 1–25, 2022, doi: 10.3390/en15134603.

[28] A. Prashanth Joshi, M. Han, and Y. Wang, “A survey on security and privacy issues of blockchain technology,” *Math. Found. Comput.*, vol. 1, no. 2, pp. 121–147, 2018, doi: 10.3934/mfc.2018007.

[29] H. Feng, X. Wang, Y. Duan, J. Zhang, and X. Zhang, “Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges,” *J. Clean. Prod.*, vol. 260, 2020, doi: 10.1016/j.jclepro.2020.121031.

[30] “Blockchain 101 | Finivi,” 2008, [Online]. Available: https://www.finivi.com/blockchain-101/

[31] Y. Liu *et al.*, “Building blocks of sharding blockchain systems:

Concepts, approaches, and open problems," *Comput. Sci. Rev.*, vol. 46, no. Tong Li, pp. 1–64, 2022, doi: 10.1016/j.cosrev.2022.100513.

[32] A. Bahga and V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 09, no. 10, pp. 533–546, 2016, doi: 10.4236/jsea.2016.910036.

[33] J. Weking, M. Mandalenakis, A. Hein, S. Hermes, M. Böhm, and H. Krcmar, "The impact of blockchain technology on business models – a taxonomy and archetypal patterns," *Electron. Mark.*, vol. 30, no. 2, pp. 285–305, 2020, doi: 10.1007/s12525-019-00386-3.

[34] F. Glaser, "Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2017-Janua, pp. 1543–1552, 2017, doi: 10.24251/hicss.2017.186.

[35] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learn. Environ.*, vol. 5, no. 1, pp. 1–10, 2018, doi: 10.1186/s40561-017-0050-x.

[36] J. Zarrin, H. Wen Phang, L. Babu Saheer, and B. Zarrin, "Blockchain for decentralization of internet: prospects, trends, and challenges," *Cluster Comput.*, vol. 24, no. 4, pp. 2841–2866, 2021, doi: 10.1007/s10586-021-03301-8.

[37] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, "A review of Blockchain Technology applications for financial services," *BenchCouncil Trans. Benchmarks, Stand. Eval.*, vol. 2, no. 3, p. 100073, 2022, doi: 10.1016/j.tbench.2022.100073.

[38] L. Cocco, A. Pinna, and M. Marchesi, "Banking on blockchain: Costs savings thanks to the blockchain technology," *Futur. Internet*, vol. 9,

no. 3, pp. 1–20, 2017, doi: 10.3390/fi9030025.

[39] K. Lauslahti, J. Mattila, and T. Seppala, “Smart Contracts How Will Blockchain Technology Affect Contractual Practices?,” *SSRN Electron. J.*, no. 68, 2018, doi: 10.2139/ssrn.3154043.

[40] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, “Step by Step towards Programming a Safe Smart Contract,” *Fc*, pp. 1–10, 2016.

[41] K. M. Khan, J. Arshad, and M. M. Khan, “Secure digital voting system based on blockchain technology,” *Res. Anthol. Blockchain Technol. Business, Heal. Educ. Gov.*, pp. 1280–1290, 2020, doi: 10.4018/978-1-7998-5351-0.ch071.

[42] R. Auer, B. Haslhofer, S. Kitzler, P. Saggese, and F. Victor, “The Technology of Decentralized Finance (DeFi),” *BIS Work. Pap.*, no. 1066, pp. 1–36, 2023, [Online]. Available: https://www.bis.org/publ/work1066.htm

[43] A. Tiwari and U. Batra, “Blockchain for healthcare,” *Blockchain Mach. Learn. e-Healthcare Syst.*, pp. 231–266, 2021, doi: 10.1049/pbhe029e_ch10.

[44] Y. Wu, D. Ambersley, A. Filipour, S. Bindu, and A. O. Abuzaghleh, “Blockchain Technology & Intellectual Property Protection The Nature of Blockchain Hard Fork in Blockchain Consists of Blockchain The Immunability of Hash,” vol. 256, p. 256.

[45] S. Chen, J. Ping, Z. Yan, J. Li, and Z. Huang, “Blockchain in energy systems: values, opportunities, and limitations,” *Front. Energy*, vol. 16, no. 1, pp. 9–18, 2022, doi: 10.1007/s11708-022-0818-8.

[46] A. Mudgal, “Introduction to Blockchain,” *Blockchain Bus. How it*

Work. Creat. Value, pp. 1–28, 2021, doi: 10.1002/9781119711063.ch1.

[47] K. L. Du and M. N. S. Swamy, *Neural networks and statistical learning, second edition*. 2019. doi: 10.1007/978-1-4471-7452-3.

[48] M. Sinthuja and K. Suthendran, "DDoS Attack Detection using Enhanced Long-Short Term Memory with Hybrid Machine Learning Algorithms," *3rd Int. Conf. Smart Electron. Commun. ICOSEC 2022 - Proc.*, pp. 1213–1218, 2022, doi: 10.1109/ICOSEC54921.2022.9951976.

[49] DePauw University, "Accuracy, Precision and Analytical Measurements What are accuracy and precision?," pp. 7–9.

[50] D. E. Stem and R. K. Steinhorst, "Telephone interview and mail questionnaire applications of the randomized response model," *J. Am. Stat. Assoc.*, vol. 79, no. 387, pp. 555–564, 1984, doi: 10.1080/01621459.1984.10478081.

[51] Tri Nova Aprianti ; Usman Seri ; Sarliana Zaini, "Journal of Applied," *J. Appl. Probab.*, vol. 32, no. 1, pp. 10–12, 2013.

[52] Department of Health Hong Kong, "Pharmaceutical Products Recall Guidelines 2022," no. March, 2022.

[53] J. Campbell and T. Neumann, "Precision phenomenology with MCFM," *J. High Energy Phys.*, vol. 2019, no. 12, 2019, doi: 10.1007/JHEP12(2019)034.

[54] A. Fujino, H. Isozaki, and J. Suzuki, "Multi-label text categorization with model combination based on F1-score maximization," *IJCNLP 2008 - 3rd Int. Jt. Conf. Nat. Lang. Process. Proc. Conf.*, vol. 2, pp. 823–828, 2008.

[55] A. Lorincz and Z. Nusser, “Specificity of immunoreactions: The importance of testing specificity in each method,” *J. Neurosci.*, vol. 28, no. 37, pp. 9083–9086, 2008, doi: 10.1523/JNEUROSCI.2494-08.2008.

[56] C. Y. Park, “Predicting program execution times by analyzing static and dynamic program paths,” *Real-Time Syst.*, vol. 5, no. 1, pp. 31–62, 1993, doi: 10.1007/BF01088696.

الخلاصة

تتطور تطبيقات البيانات والشبكات بسرعة كبيرة، مما يؤكد أهمية زيادة التدابير الأمنية القوية. مع انتشار الأجهزة الضعيفة وحركة المرور على الشبكة، أصبحت هجمات الخدمة المنتشرة المرفوعة (DDoS) أكثر سهولة في التنفيذ.

تهدف هجمات DDoS إلى غمر خادم أو موقع ويب بالطلبات، مما يجعله غير متاح للمستخدمين الشرعيين. في حين تمت محاولة مختلف حلول مكافحة هجماتDDoS ، إلا أن تكنولوجيا البلوكتشين تظهر وعودًا. فالبلوكتشين، كنظام لامركزي وآمن، يمكنه تخزين البيانات المتعلقة بهجمات الأمان بطريقة آمنة.

يقترح هذا البحث حلاً لامركزيًا بلوكتشين لمكافحة هجمات .DDoS تتضمن التقنية إعادة توجيه الطلبات الزائدة من الخادم المستهدف إلى عقد فرعية، مما يقلل الضغط ويحافظ على إمكانية الوصول للمستخدمين الشرعيين.تندمج الشبكات العصبية الاصطناعية داخل تكنولوجيا البلوكتشين في بيئات برمجة وتطوير مختلفة.

تم اختبار النظام من خلال نهج مستويين. يستخدم المستوى الأول أداة Nmap للاختبار الأولي والكشف المبكر عن هجمات .DDoS إذا تعذر تأسيس اتصال، يتم توجيه حركة المرور المشبوهة إلى المستوى الثاني.

يشمل المستوى الثاني شبكة عصبية مدربة قادرة على تصنيف حركة الشبكة وكشف الهجمات المحتملة. يتم تدريب الشبكة العصبية باستخدام عينات بيانات مختلفة لتعلم الأنماط والخصائص المرتبطة بأنواع مختلفة من الهجمات. من خلال تحليل بيانات حركة المرور، تتمكن الشبكة العصبية من تحديد الأنشطة الخبيثة أو محاولات هجمات DDoS ووضعها في القائمة السوداء.

يوضح هذا البحث أن البلوكتشين والشبكة العصبية يمكن أن تقدم حلولًا فعالة لمكافحة هجمات DDoS يمتلك هذا النهج الأمني الواعد القدرة على حماية المؤسسات من هجمات DDoSوضمان استمرارية الخدمةللمستخدمين الشرعيين.

تم تنفيذ مجموعة البيانات لتقييم النموذج المقترح وهو مجموعة بيانات .CICDDOS219 وقد أظهرت نتائج العمل المقترح نتائج مشجعة من حيث الدقة العالية. الدقة 0.96، الاستدعاء 0.89، الدقة 0.96، درجة F1 0.92، الخصوصية 0.98، متوسط الخطأ المربع (MSE) 0.032315571.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل
كلية تكنولوجيا المعلومات
قسم البرمجيات

كشف وتقليل هجمات حجب الخدمة بالاعتماد على السلسله الكتليه

رسالة مقدمة الى

مجلس كلية تكنولوجيا المعلومات للدراسات العليا بجامعة بابل
وهي جزء من متطلبات نيل درجة الماجستير في تكنولوجيا
المعلومات / البرمجيات

من قبل

نور علاء حسين غبن

بإشراف
أ.م.د الحارث عبدالكريم عبدالله

1445ه
2023م