**Analyzing the Viability of Blockchain-based Secure Data Routing in Dynamic SDNs**

**Analyzing the Viability of Blockchain-based Secure Data Routing in Dynamic SDNs**

2024

Computing & Mathematical Sciences, University of Greenwich, 30 Park Row, Greenwich, UK.

*(Submitted 17 August 2024)*

ABSTRACT: Pragmatically establishing new solutions is essential in the growing functions of network protection protocols as they become more intricate and complex with the incorporation of new technologies. The following paper aims to analyse how three concepts—SDN, blockchain, and ML—can be integrated to improve both the network's security and the communication's effectiveness. The first goal is to construct an effective network that employs SDN for real-time control of the network, blockchain for the secure sharing of data, and ML for managing or detecting notable activities or predicting future traffic in a network. Logistic regression is employed for the analysis of anomalies and traffic prediction. Based on the results, it reaches a high efficiency level with accuracy levels of 0.9993, precision of 0.9998, and recall of 0.9973. The precision is 0.9996, recall is 0.9996, and the F1 score is 0.9997. The integration of SDN allows for highly automated control of the network, forwarding policies, and the rules regarding packet forwarding. Meanwhile, the introduction of blockchain offers a highly secure way to store and validate routing decisions, thus making routing a more secure process. This research method entails deploying and tuning an SDN controller, integrating blockchain technology for secure data transfer, and training ML models with past network data. Techniques arising from testing and evaluation include improvements over traditional approaches. The results show that SDN, blockchain, and ML must be integrated to develop a comprehensive system capable of addressing numerous and ever-changing threats. Future work will involve further extending the system to different network scenarios, improving scalability, and addressing real-world deployment issues. To sum up, this research can be considered a step towards the creation of a modern approach to address contemporary network security threats.

**Keywords:** Software Define network; Machine learning; Cyber security; Block chain; Logistic regression

# Preface

In this project, I explore the intersection of cybersecurity and machine learning, focusing on secure data routing in dynamic software-defined networks (SDNs) using blockchain technology. This research aligns with the MSc programme's emphasis on cutting-edge technological innovation and contributes to the field by addressing critical security challenges in emerging network architectures. The project fulfils the National Qualifications Framework's criteria by demonstrating advanced knowledge application, critical thinking, and research skills essential for Information security.

# 

# Table of Contents

[ABSTRACT 2](#_Toc174129318)

[List of Tables 7](#_Toc174129337)

[List of Figures 7](#_Toc174129338)

[Chapter 1 Introduction 8](#_Toc174129340)

[1.1 Background 8](#_Toc174129341)

[1.2 Problem Statement 9](#_Toc174129342)

[1.3 Aim and Objectives 10](#_Toc174129343)

[1.4 Research Questions 10](#_Toc174129344)

[1.5 Significance of the Study 11](#_Toc174129345)

[1.6 Structure of the Thesis 11](#_Toc174129346)

[Chapter 2 Literature Review 12](#_Toc174129347)

[2.1 Introduction 12](#_Toc174129348)

[2.2 Overview of Software-Defined Networks (SDNs) 12](#_Toc174129349)

[2.2.1 Evolution of SDN Architecture 12](#_Toc174129350)

[2.2.2 Key Components and Functions of SDNs 13](#_Toc174129351)

[2.2.3 Security Challenges in SDNs 14](#_Toc174129352)

[2.3 Blockchain Technology and Network Security 16](#_Toc174129353)

[2.3.1 Fundamentals of Blockchain Technology 16](#_Toc174129354)

[2.3.2 Applications of Blockchain in Network Security 17](#_Toc174129355)

[2.3.3 Blockchain-based Secure Data Routing 17](#_Toc174129356)

[2.4 Machine Learning in Software-Defined Networks 18](#_Toc174129357)

[2.4.1 Role of Machine Learning in Network Management 18](#_Toc174129358)

[2.4.2 Machine Learning for Security Enhancement in SDNs 19](#_Toc174129359)

[2.4.3 Integrating Machine Learning with Blockchain for Secure Data Routing 19](#_Toc174129360)

[2.5 Gap analysis 20](#_Toc174129361)

[2.5.1 Limitations of Blockchain in SDNs 20](#_Toc174129362)

[2.5.2 Insufficient Exploration of ML-Enhanced Security in SDNs 21](#_Toc174129363)

[2.5.3 Lack of Comprehensive Performance Evaluations 21](#_Toc174129364)

[2.5.4 Emerging Areas for Future Research 22](#_Toc174129365)

[2.6 Conclusions 22](#_Toc174129366)

[Chapter 3: Research Methodology 23](#_Toc174129367)

[3.1 Research Design 23](#_Toc174129368)

[3.2 Data Collection Methods 25](#_Toc174129369)

[3.3 Model Implementation 26](#_Toc174129370)

[3.3.1 SDN Setup 26](#_Toc174129371)

[3.3.2 Blockchain Integration 26](#_Toc174129372)

[3.3.3 Machine Learning for Anomaly Detection 27](#_Toc174129373)

[3.3.4 Algorithm SDNBCML 27](#_Toc174129374)

[3.4 Legal, Social, and Ethical issues 28](#_Toc174129375)

[1. Legal issues 28](#_Toc174129376)

[2. Social Issues 29](#_Toc174129377)

[3. Ethical Issues 29](#_Toc174129378)

[3.5 Conclusion 30](#_Toc174129379)

[Chapter 4 Implementation 32](#_Toc174129380)

[4.1 Tools and Techniques 32](#_Toc174129381)

[4.2 Machine Learning Implementation 33](#_Toc174129382)

[Dataset Preparation: 33](#_Toc174129383)

[Train-Test Split and Standardization: 34](#_Toc174129384)

[Machine Learning Model: 35](#_Toc174129385)

[4.3 Blockchain Implementation 36](#_Toc174129386)

[Blockchain Framework Selection: 36](#_Toc174129387)

[Integrating Blockchain with ML Predictions: 37](#_Toc174129388)

[Visualizing the Blockchain: 38](#_Toc174129389)

[4.4 Integration with SDN Controller 40](#_Toc174129390)

[4.5 Conclusion 43](#_Toc174129391)

[Chapter 5 Result and Discussion 44](#_Toc174129392)

[5.1 Results of Machine Learning Model Performance 44](#_Toc174129393)

[5.2 Discussion 45](#_Toc174129394)

[Comparison with Previous Research 45](#_Toc174129395)

[Limitations 46](#_Toc174129396)

[5.3 Conclusions 46](#_Toc174129397)

[Chapter 6 Conclusion and Future Work 47](#_Toc174129398)

[6.1 Conclusion 47](#_Toc174129399)

[6.2 Future Work 47](#_Toc174129400)

[References 49](#_Toc174129401)

[Appendix A: 51](#_Toc174129402)

# List of Tables

[Table 1 tools and techniques used in your research 32](#_Toc176445606)

[Table 2 Comparison with Previous Research: 45](#_Toc176445607)

# List of Figures

[Figure 1 System Architecture Diagram illustrating the integration of SDN, blockchain, and ML 24](#_Toc174129486)

[Figure 2 SDN controller setup 26](#_Toc174129487)

[Figure 3 Data preparation 34](#_Toc174129488)

[Figure 4 Final data after data preprocessing 34](#_Toc174129489)

[Figure 5 train test and standardizing the data 35](#_Toc174129490)

[Figure 6 output of ML model 36](#_Toc174129491)

[Figure 7 blockchain visualization 39](#_Toc174129492)

[Figure 8 Confusion matrix 44](#_Toc174129493)

# List of Abbreviations

|  |  |
| --- | --- |
| **Abbreviation** | **Full Form** |
| SDN | Software-Defined Networking |
| ML | Machine Learning |
| IDS | Intrusion Detection System |
| API | Application Programming Interface |
| REST | Representational State Transfer |
| IoT | Internet of Things |
| VPC | Virtual Private Cloud |
| AWS | Amazon Web Services |
| DoS | Denial of Service |
| DDoS | Distributed Denial of Service |
| MitM | Man-in-the-Middle |
| SQL | Structured Query Language |
| XSS | Cross-Site Scripting |
| VPN | Virtual Private Network |

# Chapter 1 Introduction

## 1.1 Background

More specifically, it has been observed that today’s networks are becoming significantly more complex and interconnected, thereby requiring the emergence of new sophisticated and versatile structural models of networks. It is known that the conventional architectures of the network are not very flexible and are mostly independent of software, with a very ‘hardware’ approach to most of the required networking. One of these disruptive technologies is Software Defined Networking (SDN) which proposed a more flexible, centralized, and programmable architecture. SDN also decouples the control plane from the data plane and this enables the network administrators to control the behaviour of their network using software (Yan, 2015).

It is for the above reasons that David; SDN allows for the formation of an independent and flexible network that can tackle the varying conditions and demands of a large scale network hence why it is preferred (Maleh, 2023). But up with the advantages of SDN come the problems and some of them are generally related to the security. Inherent in the architectures of SDN are potential Single Points of Failure and moreover, targets for attack. Also, since the states and the configurations of an SDN can change dynamically, it also interferes with traditional security solutions. It poses several challenges one of which is secure data routing a fundamental component in any network. This means that there is a compulsory requirement for a secure, massive and flexible security solution than it has previously been (Khan, 2023).

Blockchain has been regarded in the recent past as a solution to the many security issues within distributed systems. Defined as an open, distributed ledger that is used to maintain a continuously growing list of records; its earlier application was in creating a digital currency such as Bitcoin. Their architecture is also relatively distributed, which minimizes central control points and possibilities of failures, and the impossibility of altering recorded information makes it impossible to forge or modify it. These make blockchain a potential candidate for improving security in SDN for data routing process security (Tyagi, 2023).

SDN is dynamic and therefore, the network topologies and the conditions continue to change hence, adopting the blockchain can offer secure and immutable way of routing on both networks. Optimistic attacks as well as other rapid changes can be faced by making the records of routing decisions and transactions on a blockchain, while the data integrity of this process will be ensured in this case. It could potentially be useful in the construction of a more secure and hence less vulnerable network in dynamically changing environments (Javanmardi, 2023).

## 1.2 Problem Statement

The integration of blockchain technology with software defined networks SDNs resents a promising approach to addressing security concerns in dynamic networking environments however this integration is fraught with several technical challenges that must be carefully considered one of the primary issues lies in the inherently resource intensive nature of blockchain particularly its consensus mechanisms these mechanisms designed to ensure the integrity and immutability of the blockchain require significant computational power and time in the context of SDNs which prioritize speed and efficiency in data routing the additional processing time introduced by these consensus protocols can lead to delays that are detrimental to network performance for instance the time taken to achieve consensus on the blockchain could exceed the acceptable latency thresholds in a high speed SDN potentially leading to bottlenecks in data flow and reduced overall network efficiency another critical challenge is scalability as blockchain networks grow the increasing number of transactions and nodes can strain the system s capacity to process and verify data in a timely manner this becomes particularly problematic in large scale SDNs where the need for quick and reliable data routing is paramount the blockchain s capacity to scale while maintaining its security properties is a key concern as any compromise in this area could undermine the effectiveness of the entire network (Rahman, 2024).

Moreover SDNs are characterized by their dynamic nature with network topologies and conditions frequently changing in response to varying demands and threats this dynamism requires a security solution that can adapt seamlessly to these changes maintaining the integrity and security of data routing without introducing significant delays or vulnerabilities however blockchain technology with its relatively static structure and dependence on a distributed consensus may struggle to keep pace with the rapid changes inherent in SDNs the fixed block times and the linear progression of the blockchain may not align with the real time demands of SDNs potentially leading to mismatches between the network s security needs and the blockchain s capabilities (Abou El Houda, 2023).

These challenges raise important questions about the practicality of using blockchain to secure data routing in dynamic SDN can blockchain's security benefits be realized without compromising the agility and performance of SDNs what trade offs will be necessary and how might they impact the overall viability of this integration this thesis seeks to address these questions by conducting a detailed exploration of the feasibility and effectiveness of blockchain-based secure data routing in dynamic SDN aiming to identify solutions that balance security performance and scalability in these complex environments (Varma, 2023).

## 1.3 Aim and Objectives

The main focus of this research is to compare the approaches of integrating blockchain technology and machine learning to address the issue of data routing that is proactive and secure in unpredictable Software-Defined Networks (SDNs). The research aims at proposing and analysing an overall framework on how to adopt blockchain and machine learning concurrently for securing dynamic SDNs in light of the enhancements blockchain can bring for the associated performance and scalability issues caused by the machine learning integration.

* To investigate the underlying principles and current state of blockchain technology, SDNs, and machine learning, and explore their potential integration for secure data routing.
* To develop a blockchain-based framework that incorporates machine learning techniques to optimize data routing and enhance security in dynamic SDNs.
* To evaluate the performance implications of integrating blockchain and machine learning in SDNs, focusing on metrics such as latency, scalability, and resource utilization.
* To design and implement machine learning models that can adapt to real-time changes in SDN topology and conditions, ensuring consistent security and efficiency.
* To analyze the trade-offs between security, performance, and scalability in the proposed blockchain and machine learning-based framework.
* To identify practical challenges in the deployment of the proposed framework in dynamic SDNs and suggest strategies for overcoming these challenges.

## 1.4 Research Questions

To guide the research, the following questions will be addressed: To guide the research, the following questions will be addressed:

1. To which extent, it is possible to incorporate blockchain in SDNs for enhancing the data routing security in dynamic setting?

2. What is the part that machine learning can play to further improve and secure the data routing in SDNs using blockchain technology?

3. What are the possible performance consequences from integrating the blockchain with machine learning for secure data transmission in dynamic SDNs?

4. What strategies can be used to train and apply machine learning in real-time to changes in the topology and operating conditions of block chain secured SDNs?

5. Along with that, not less attention should be paid to such an important aspect of distributed computing as optimization choices, such as prioritization of security or machines’ performance, etc when it comes to blockchain and machine learning-based solution for dynamic SDNs.

6. What is the pragmatic consideration of the use of the blockchain and machine learning based security framework used in the dynamic SDNs and how each can be addressed?

## 1.5 Significance of the Study

The study has an important significance as it provides additions to the investigations concerning the improvement of Network Security in the context of the recent emergent complicated and changing conditions. But as the idea of implementing SDN in various industries and sectors continues to pick up, the security of the data routing becomes of essence. Therefore, through examining the implementation of blockchain technology in other fields, this study seeks to contribute to the understanding of new approaches of providing security in networking while at the same time benefiting from increased flexibility. However, the results of this research could help introducing stronger and more protected frameworks for the networks, and therefore effectively contribute to the scientific field of cybersecurity.

## 1.6 Structure of the Thesis

The remainder of this thesis is structured as follows:

Chapter 2: The Literature Review section will also discuss the prior studies related to the areas of SDN, blockchain technology, and their synergy. It will recall the security issues in SDNs and the proposed solutions, as well as, the state of security in SDNs based on block chain.  
Chapter 3: Methodology will state and explain the techniques applied for evaluating the effectiveness of blockchain-based secure data routing in the dynamism of SDNs. This will involve planning and description of the strategies for creating experiments, ways and form of data.  
Chapter 4: Implementation will be in the form of writing down the study conclusion and recommendation with a focus on the aspect of security and performance of the proposed solution.  
Chapter 5: Results and Discussion will reveal the results of the study with regards to the set research objectives and questions and shall elaborate on the trade-offs and practical issues found.  
Therefore, the final chapter, Chapter 7, Conclusion and Future Work, will set out the conclusions of the current research, implications drawn from the findings, as well the recommendations for future research.  
This structure will enable a sundry investigation on the research topic and also systematically present the feasibility of blockchain-based secure data routing within dynamic SDNs.

# Chapter 2 Literature Review

## 2.1 Introduction

These challenges raise important questions about the practicality of using blockchain to secure data routing in dynamic SDNs can blockchains security benefits be realized without compromising the agility and performance of SDNs what trade-offs will be necessary and how might they impact the overall viability of this integration this thesis seeks to address these questions by conducting a detailed exploration of the feasibility and effectiveness of blockchain-based secure data routing in dynamic SDN aiming to identify solutions that balance security performance and scalability in these complex environments.

## 2.2 Overview of Software-Defined Networks (SDNs)

### 2.2.1 Evolution of SDN Architecture

Software-defined networking SDN represents a paradigm shift in the design and management of computer networks traditional networking architectures are largely hardware-centric with network devices like routers and switches performing both the control and data forwarding functions this integrated approach while reliable often lacks flexibility making it difficult to adapt to rapidly changing network requirements such as the need to deploy new applications or to handle dynamic traffic patterns efficiently the evolution of SDN is rooted in the desire to overcome these limitations by separating the control plane from the data plane the control plane is responsible for making decisions about where traffic is sent while the data plane actually forwards the traffic to the selected destination by decoupling these two functions SDN allows for centralized control over the network enabling network administrators to manage the entire network through software applications that interact with the SDN controller (Rahman, 2024).

The concept of SDN can be traced back to the work on network virtualization and programmable networks in the early 2000s the term SDN itself was popularized by the clean slate program at Stanford University which led to the development of open flow the first standard communication interface defined between the control and data planes of an SDN architecture open flow allowed for the direct programming of the forwarding plane thereby enabling the centralized control of network flows this development was a key milestone as it provided a practical implementation of SDN principles and spurred significant interest in the research and deployment of SDN technologies (Prabha, 2022)

As SDN has evolved it has been widely adopted in various domains including data centers enterprise networks and service provider environments the ability to programmatically manage and optimize network resources has made SDN a valuable tool for addressing the complex needs of modern networks such as dynamic bandwidth allocation security policy enforcement and traffic engineering moreover the centralized nature of SDN enables better visibility into network operations allowing for more efficient troubleshooting and network diagnostics (Priyadarsini, 2021)

However the adoption of SDN has also introduced new challenges particularly in terms of security the centralization of the control plane while beneficial for network management creates a potential single point of failure if the SDN controller is compromised the entire network could be at risk this has led to ongoing research into how best to secure SDN architectures while preserving their flexibility and scalability (Bonanni, 2023).

### 2.2.2 Key Components and Functions of SDNs

Software-Defined Networking (SDN) is characterized by its distinct architectural components, which are typically divided into three planes: three primary layers of SDN: the application plane, the control plane and the data plane (Deb, 2022). These planes are as follows: Each of these planes consists of certain functionalities that collectively allow the flexibility and programmability of the SDNs.

• Application Plane: The application plane includes the application that operate within the network to requesting network services through the SDN controller. These applications may include firewall and load balancer applications up to traffic analyzer and network monitoring applications. It is also designed to inform the other layers of the desired characteristics for the application; the control plane translates these high-level requirements into specific network settings. This plane’s programmability in turn means that network administrators can offer, and manage network services more flexibly and according to specific business requirements

• Control Plane: The control plane is one of the critical components of the SDN architecture. Operated by an SDN controller, the control plane's major role is to determine the direction and manner through which traffic is to pass through a particular network. The application plane communicates with the SDN controller, which in its turn communicates with the data plane and translates the application plane requests into the specific forwarding rules. The decoupling of the control plane from the physical network hardware allows for easier management of the network mainly due to its ability to support complex policies on the network and efficiently distribute the available network resources. Probably, the most important factor is the central position of the SDN controller that provides the means for more dynamic and adaptive network management since new conditions and/or requirements are likely to appear in the network with time.

• Data Plane: The forwarding plane also called the data plane is mainly involved in the forwarding of data packets as per the rules decided by the control plane. Such devices include switches and routers which take appropriate actions of forwarding packets based on the instructions that are issued by the SDN controller. One advantage that advocates point to is the decoupling of the data plane from the control plane, that is, the actual implementation of the forwarding table, which no longer requires the implementation of the algorithms that make up the control plane but rather simply implements the directions that the controller has given it. This architecture optimizes the running of network services and improves the capacity for controlling traffic in a differentiated fashion.

This tri plane architecture of SDN enables a highly modular and flexible network design allowing for the rapid deployment of new services and the efficient management of network resources however this architecture also introduces certain challenges, particularly in terms of security which are discussed in the following section

### 2.2.3 Security Challenges in SDNs

While software-defined networking SDN offers numerous advantages such as increased flexibility programmability and centralized control it also introduces a range of security challenges that must be addressed to ensure the reliability and safety of the network which are crucial to providing the network’s reliability and safety were addressed (Rahouti, 2023).

• Centralization of Control: The security concern which is related to the SDN architecture is the oversimplification of the control plane through centralization. Consequently, a major vulnerability arises due to the fact that the SDN controller, which is the focal point of the network control, emerges as a high-value asset to the attackers. SDN controller is a central point which if attacked, an attacker can control the entire network or modify flows to his benefit or bring down the network. This centralization brings a certain vulnerability caused by the presence of a single centralized ‘controller’ and thus the ‘controller’ must be protected against malicious attacks by hackers or even viruses. The study conducted by (Kazmi, 2023) presents the threats of the centralized approach and encourages the use of reliable means of authentication and encryption to safeguard the SDN controller .

• Programmability and Vulnerabilities: As seen previously, the programmability of SDNs can be advantageous; however, it is also accompanied by new challenges and threats. Cyber deceivers are capable of introducing in the SDN software insecure codes or modifying the network policies. For instance, if an adversary gets control of the control plane’s API, they can alter the forwarding tables to allow unwanted data flows or deny network traffic altogether. On the same note, the openness that SDN provides can also be said to possess its weaknesses since it is easier for even badly developed or insecure applications to act as pathways to various opportunities for the invasion of the network’s security. As rightly pointed out by (Isyaku, 2020) the protection of the control plane’s API and the verification of the networking applications are some of the ways through which these risks can be contained.

• Lack of Standardized Security Protocols: However, SDN has some disadvantages also, the main of which is that still there are no routinely outlined security guidelines for networks with SDN implementation. The current or what is commonly referred to as Software Defined Networking comes with its box of original and distinct security challenges that cannot be solved by conventional security architectures. Some of the traditional layers of protection like firewalls and IDS could be weak in the context of SDN because the control and data layer are different. Recent studies are focused on the creation of common practices for securing SDNs; however, the lack of established reference models is at the moment one of the main concerns regarding the further advancement of SDN solutions.

• Dynamic and Evolving Threat Landscape: Some challenges of SDNs are as follows: The policies and configuration of SDNs are also dynamic which means they can also evolve in a short period. It is considered that traditional security measures may be insufficient to counter new threats that are expected to target flexible and programmable features of SDNs. This calls for the establishment of dynamic security measures to counter this challenge with relative rapidity of response to changes in the network. Currently according to the (Arif, 2020) ended that real time monitoring and automated response systems should be incorporated into the SDN architecture but this is still a subject of research.

To sum up, indeed, SDN provides more innovation and the overall manageability of the network, but at the same time it implies certain security threats which should be solved to expand the use of SDN. Lack of unified command and control, programmability of the network, and no fixed security measures are some of the issues that need constant focus from the academicians and the industry.

## 2.3 Blockchain Technology and Network Security

### 2.3.1 Fundamentals of Blockchain Technology

Blockchain is a distributed ledger technology that will complete and record transactions in a secure, easily verified process. Each of the processes is made within the context of a block and several consecutive blocks are connected with the aid of a cryptographic hash creating a chain of blocks also known as a blockchain. The said cryptographic linking is such a way that once a block is attached to the Blockchain, the modification of data cannot be done without altering consequent blocks rendering the Blockchain unchangeable. This characteristic is one of the main advantages of blockchain to be secure and convenient for the various usages in the economic activity, financial operations, managing supplies, and identification services.

Blockchain is a distributed system and this implies that no particular place contains the records or is in control of it. However, it is split into several nodes where every node contains the same copy of the blockchain in its database. In a block chain system, every time a new transaction is started it is relayed to all the nodes in the system to approve through a consensus. Some of the examples of consensus mechanisms are Proof of Work (PoW), Proof of Stake (PoS), Byzantine Fault Tolerance (BFT) wherein PoW is highly secured but consumes a lot of energy, while PoS is energy-efficient but not highly secured, and BFT is faster and more secure than PoW and PoS.

In essence blockchain s decentralized and distributed architecture ensures that no single point of failure exists in the system enhancing its resilience against attacks the transparency of the blockchain where all transactions are publicly recorded and can be audited by any participant further contributes to its security however this transparency also raises concerns about privacy which has led to the development of privacy preserving techniques such as zero knowledge proofs and confidential transactions

### 2.3.2 Applications of Blockchain in Network Security

Blockchain technology has been increasingly explored as a tool to enhance network security leveraging its decentralized transparent and immutable characteristics one of the primary applications of blockchain in this domain is secure data sharing in traditional networks data is often stored in centralized databases making them attractive targets for cyberattacks by using blockchain data can be securely shared and stored across a distributed network reducing the risk of data beaches and unauthorized access

Another significant application of blockchain in network security is access control traditional access control systems often rely on centralized authorities which can be compromised blockchain on the other hand enables decentralized access control mechanisms where permissions and access rights are recorded on the blockchain this ensures that access control policies are tamper-proof and can be audited enhancing the overall security of the system for example blockchain can be used to implement decentralized identity management systems where users control their own identities and credentials reducing the reliance on centralized identity providers. In the context of Software-Defined Networks (SDNs), blockchain has been proposed as a solution to secure data routing.

The centralized control plane in SDN while beneficial for network management also creates a potential point of vulnerability by integrating blockchain routing decisions that can be recorded on a tamper-proof ledger ensuring that they cannot be altered or manipulated by malicious entities this approach not only enhances the security of data routing but also provides a transparent and auditable record of network activity which can be invaluable for detecting and responding to security incidents.

### 2.3.3 Blockchain-based Secure Data Routing

The integration of blockchain with SDN for secure data routing is an emerging area of research that seeks to leverage the strengths of both technologies to address the security challenges associated with dynamic and programmable networks several studies have proposed using blockchain to record and verify routing decisions within SDN for instance blockchain can be used to create a decentralized and immutable ledger of routing rules which ensures that these rules are not tampered with by malicious actors (Dhurandher, 2022).

This is a major problem in secure data routing implemented with the use of blockchain: blockchain itself and, more specifically, consensus algorithms, are very demanding in terms of resources. The consensus that is used in many cryptocurrencies such as Proof of Work (PoW) entails the usage of the robust computing power and time to approve transactions whereby this may impact the network with a level of delay. In high speed, dynamic SDN environment this may pose a problem because delays in data flow and routing could compromise the efficiency of the network. This issue becomes especially important when dealing with a big number of transactions and the requirement of real-time analysis of the data.

Another challenge is scalability. This is due to the fact that with each transaction that occurs, the size of the blockchain only gets bigger and bigger, and as such, both storage and processing power needed for each of the nodes in the network sky rocket. This can be cumbersome especially in SDNs where some of the network devices may possess a comparatively limited processing power. To overcome the aforementioned challenges, researchers have adopted different solutions comprising of off-chain transactions observing the requirement of performing occasional transactions outside the blockchain to ease the burden of the network; better consensus algorithms like the Proof of Stake (PoS) and the Delegated Proof of Stake (DPoS) that are slightly less demanding than the PoW (Awan, 2022).

Nevertheless, the possibility of expanding the usage of blockchain and integrated it with SDNs for secure data routing might have several advantages. This is due to the fact that blockchain offers a proof of routing decisions that have the potential of improving the security of the network and its resistance against some attacks. Furthermore, blockchain solves the problem of exposing the record of events so that one can easily know in the case of any event that is questionable, the occurrence can be corrected, helping offer a layer of security to the ever-evolving SDN. Nonetheless, the current study is suggestive; more research work has to be conducted to fine-tune the integration of blockchain with SDNs whereby concerning the consequences of blueprint means on the performance and scalability of the proposed integration model.

## 2.4 Machine Learning in Software-Defined Networks

### 2.4.1 Role of Machine Learning in Network Management

Artificial intelligence (AI) is a modern tool in the management of a network especially in the SDNs as analyzing and controlling of events happening in the network is vital and can be enhanced by the use of the machine learning (ML). The application of ML methods is convenient in network environments and network data handling, and the identified methods can process the entire volume of network data to make decisions. Considering the application of ML in SDNs, there are several possibilities: traffic forecasting, identification of anomalies, and the use of resources. For instance, the ML applications can learn from previous traffic history in the networks to foresee future traffic patterns so as to arrange resources such that network performance is not compromised (Apruzzese, 2023). Moreover, traffic flows can be classified using ML and can help in identifying what applications are most important, or even in managing the changes in the network policies on an automated basis. When ML is incorporated in SDNs, networks can essentially be optimally performant and capable of dynamically meeting new demands without compromising the QoS (Khan, 2024). This capability is most useful in such sero and extensive networks where automation is normally desirable due to the complexity.

### 2.4.2 Machine Learning for Security Enhancement in SDNs

In addition to network management machine learning plays a crucial role in enhancing the security of SDNs traditional security measures which often rely on static rules and predefined signatures may not be sufficient to protect against sophisticated and evolving cyber threats ml algorithms on the other hand can be trained to detect and respond to network anomalies in real time for instance ml models can identify unusual traffic patterns unauthorized access attempts or other indicators of a potential security breach by continuously analyzing network data tang et al 2020 these models can be fine tuned over time allowing them to adapt to new threats and reduce the incidence of false positives this adaptability is particularly important in the context of SDN where network configurations can change frequently and static security measures might fail to address emerging vulnerabilities moreover ml based intrusion detection systems ids can be integrated into the SDN control plane to provide a more robust and dynamic defense mechanism (Boualouache, 2022),this integration not only enhances the overall security posture of the network but also helps in maintaining the integrity and availability of network services.

### 2.4.3 Integrating Machine Learning with Blockchain for Secure Data Routing

Hybridization of machine learning and blockchain having solutions for secured routing of data in SDNs. This combined approach leverages the strengths of both technologies: the role of blockchain and its openness and impossibility to change data and on the other hand, predictive and adaptive features of ML. In the context of secure data routing, ML can be used for improving the associated security methodologies based on the blockchain approach. For instance, ML algorithms can forecast network status including traffic density and delay and adapt the blockchain settings with regards to the frequency of consensus updates to have minimal interference on the performance (Bhandari, 2023). Also it can improve the blockchain security by identifying violations on the actual blockchain and preventing attempts to manipulate the blockchain records or introduce fake transactions into the blockchain. With the help of the network data, which reaches the ML models, it is possible to detect misconducts and call the appropriate security measures before severe losses are incurred (Nouman, 2023). Thus, this integration of ML and blockchain not only enhances the security architecture of SDNs but also guarantees the network’s stability and performance in the worst-case scenarios.

## 2.5 Gap analysis

Incorporation of blockchain technology, machine learning and Software defined networking is another promising and relatively unexplored area of research in the basket of secure data routing. Although, each of these technologies is explored individually, their utilization jointly or especially for improving the security and performance of the SDNs has been explored limitedly. The primary goal of this gap analysis is to assess the shortcomings of prior research and to define the scope for further study with special reference to the problem domain of “Analyzing the Feasibility of Blockchain-based secure Data Routing in Dynamic SDNs using machine learning (ML).”

### 2.5.1 Limitations of Blockchain in SDNs

Previous studies have investigated the possibility of using blockchain in increasing security of numerous fields which includes network security. Due to properties such as immunity to tampering, open-source, and distributed control, blockchain is suitable for data protection and maintaining confidence in the distributed networks. Still, the following concerns remain pivotal when discourse is made on SDNs. For example, the scalability of blockchain, especially in the consensus mechanisms, has been singled out as the biggest limitation to achieving high-speed large scale SDN. Some of the research work that has been done on this subject include (Alkhamisi, 2024) work and (Latah, 2017) work that showed that although the integration of blockchain with SDNs is effective, the latency as well as scalability decrease when it is adopted in dynamic environments. These performance challenges are worse in situations where there is a need to process data as it is being received and where the latency has to be kept as low as possible such as in industrial or Smart City networks. Although some solutions have been suggested, for instance, improving the consensus algorithms or incorporating off-chain system approaches, an appropriate solution of the above issues, that is, creating the blockchain solutions that would be efficient when integrated with SDN frameworks, has not been developed yet.

### 2.5.2 Insufficient Exploration of ML-Enhanced Security in SDNs

It has been named that machine learning has a great potential to improve the network security by means of such functions as an anomaly detection, intrusion detection, and others complex analysis. However, most of the studies have looked into the traditional network environment and not the SDNs. For instance, the work of (Pawar, 2024) shows the capability of utilizing the IDS based on the ML, but the peculiarities of SDN and its requests are not taken into consideration. Unlike PN, where the control and data planes are tightly integrated, the security threats in SDNs could be of a different nature, and the basic, direct application of ML techniques might not be possible. Furthermore, the available literature is modest on the aspect of applying ML in enhancing the security of blockchain technologies in SDNs. Despite the growing literature on combining ML with Blockchain for IoT and financial (service) purposes (Rahman, 2023) SDN security within the dynamic and oversized networks, there isn’t lots of significant research study done. This implies that there is literature gap regarding the capability of ML in improving the blockchain-based secure data routing in SDNs.

### 2.5.3 Lack of Comprehensive Performance Evaluations

Another significant gap in the current body of research is the lack of comprehensive performance evaluations that consider both the security and efficiency of blockchain and ml integration in SDN while individual components such as blockchain or ml algorithms have been extensively tested there is a scarcity of studies that evaluate their combined impact on network performance particularly in real world or large scale SDN environments for instance research by (Rahdari, 2024) has primarily focused on the theoretical aspects of integrating blockchain and ml with SDN often using simulated environments that may not accurately reflect the complexities of actual network deployments additionally most studies tend to focus on security enhancements without adequately addressing the trade offs in terms of latency throughput and resource consumption this lack of holistic performance evaluation poses a challenge for the practical deployment of these technologies in SDN as network operators require a clear understanding of the impact on overall network performance before adoption.

### 2.5.4 Emerging Areas for Future Research

Based on the gaps that have been highlighted, the following directions for future research can be distinguished. First of all, there is a potential need for extensive work dedicated to fine-tuning the given blockchain protocols to be more compatible with the SDNs’ integration, primarily concerning response time and capacity. It may also be useful to better understand if there are other consensus models that can be used or if there is a way to combine on chain and off chain computation. Secondly, the further studies are required to design more suitable ML models for the SDNs security threats with the consideration of these networks’ dynamics. These models should be able to identify anomaly, but also be able to forecast possible security threats in the network depending on the activity level, thus providing opportunity for advance security measures. Finally, there is a strong desire for actual success and performance measured cases that current both security and efficiency. Stated research studies would be useful to reveal assessment of the effectiveness of the proposed integration scheme and identify potential room for improvement toward the practical implementation of blockchain and ML integration in SDNs.

Thus, in the light of the current research, it can be stated that both fields, namely, blockchain and ML, have been studied extensively individually and recently in combination with SDNs, however, the employment of blockchain and ML in a context of secure data routing through the SDN architecture has attracted little attention. Mitigating the gaps that have been highlighted in this analysis will be as follows; To close the gaps and progress towards the goal the following need to be done.

### 2.6 Conclusions

This literature review work has aimed at presenting the current status of research into SDNs, blockchain, and, and machine learning, especially when used in routing data securely. Although, advancements have been made in each of the areas of Interest, what has remained more of an area of research is the integration of these technologies in rapidly changing dynamic SDNs. The review also emphasizes the necessity for the future work devoted to the performance and scalability enhancement of the blockchain-based security solutions as well as to the application of the machine learning approaches in order to improve the flexibility and efficiency of these systems. The conclusions derived from this literature review are going to serve as the foundation for the remaining chapters of this thesis, as they will help design and assess a new framework to enable secure data routing in dynamic SDNs using blockchain and machine learning.

# Chapter 3: Research Methodology

This chapter aims to describe the research method that was employed in this study in order to assess the feasibility of the presented blockchain-based secure data routing model for SDNs through the application of ML algorithms. The chapter outlines the plan of the study, the methods used for data collection and data analysis, and the approaches used in assessment of findings with regard to the research questions and objectives enumerated in chapter one.

## 3.1 Research Design

The research methodology for this study entails adopting a rigorous procedure that will be used to assess the integration of blockchain-based secure data routing and ML in dynamic SDNs. The design spans across several phases of which the assessment of the viability and functionality of the proposed system forms part.

The research begins with the conceptualization of a comprehensive system architecture that outlines the interactions between the key components: four key aspects: the SDN controller, the blockchain platform, the ML algorithms, and the data visualization tools. Its principal utility in this context is for providing secure routing of data and improvement of the network functionality by recognizing flow anomalous patterns and traffic forecast.

The brief survey of the main system elements of using blockchain for secure data routing in dynamic Software-Defined Networks and Machine learning. The system's architecture comprises four key components: the SDN controller, the blockchain platform, machine learning algorithms, and the Open vSwitch (OVS) network, which handles the real-time flow of network traffic. OVS provides the flexibility to support automation and intelligent forwarding decisions made by the SDN controller, enhancing the dynamic control of network traffic.

This architecture is based on the control layer that is the SDN Controller that has the authority to oversee the control plane of the given network. Thus, the SDN Controller is in charge of setting the policies for the network, configuring the network’s devices, and directing data flow based on data inputs from blocks/chain and Machine Learning algorithms. As illustrated in the above figure, the Blockchain Integration component is located right beside the SDN Controller, and its main responsibility is to provide the routing on the security and authenticity of the routing decisions. This is carried out by having a blockchain solution like Ethereum or Hyperledger and smart contracts which interact with the SDN Controller. The changes in the routing decisions are recorded in the blockchain and cannot be changed illegitimately thus making the network more secure.

The Machine Learning Algorithms component is connected to the SDN Controller in order to utilize anomaly detecting algorithms and traffic predicting algorithms. Machine learning algorithms are developed to learn from the previous network traffic data, to distinguish between regular patterns and risky activity. These models provide real time solutions much like data feeds to help the SDN Controller make the right decisions in the management of the network in the case of detected anomalies or reorganization of packet traffic based on its preferred flow. Accompanying these components is the Data Visualization toolset, mainly utilizing the tools based on Grafana or Kibana to generate insightful dashboards. These visualizations are based on the real-time data and contain security alerts and performance metrics; this allows the user to have a general view of the network and conduct a more efficient monitoring and analysis.

These components collectively build up a system architecture that utilizes blockchain and ML to improve the security and functionality of dynamic SDNs and accompanies it with a potent monitoring and control tool set.

The architecture of the system is depicted in the following diagram:

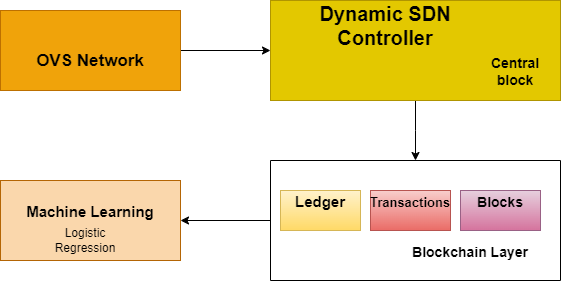


Figure 1 System Architecture Diagram illustrating the integration of SDN, blockchain, and ML

In this architecture, data flows through the SDN controller, which applies policies defined by the blockchain and decisions informed by ML algorithms. The blockchain component secures and logs routing decisions, while ML algorithms continuously analyze network traffic and detect anomalies. The results are visualized in real-time through interactive dashboards, providing insights into network performance and security.

By employing this integrated system architecture, the research aims to assess the effectiveness of combining blockchain and ML technologies in SDNs. The design ensures a thorough evaluation of how these technologies can enhance network security, optimize data routing, and provide actionable insights through real-time analytics and visualization.

## 3.2 Data Collection Methods

The dataset that we employ in this research is an open source dataset that has been developed for network intrusion to aid this study on developing secure data routing by integrating blockchain and machine learning in SDNs. The dataset includes different network traffic data including the attack and normal data necessary for training and evaluating our proposed system.

A number of tables are required in this research; the data for these are derived from various sources and expressed as follows: Every table provides network connection vectors with different characteristics that indicate the characteristics of the traffic.

Data Preparation: Regarding the preparation of the data for analysis, it must be mentioned that all individual datasets for attacks are merged into a single dataset collectively. To distinguish between the type of activity depicted in each record, a new column, attack, is introduced. This classification is generally ideal for binomial as well as multinomial classification processes. For binomial classification, the dataset is labeled as either 'attack' or 'normal. ' For multinomial classification, the dataset includes labels for various attack types: Some of the known attack tools include Back, Buffer Overflow, FTP Write, Guess Password, Neptune, N-Map, Port Sweep, Root Kit, Satan, and Smurf.

Resampling and Balancing: Due to the skewed distribution of some categories of attacks or of normal traffic compared to the others resampling is used. This is the process, in which the dataset is modified to have a similar number of observations for both the classes so that the machine learning models are well-trained and the results can be generalized well for different types of network activities.

The dataset to be prepared will be used for machine learning algorithms to be trained and for confirming the positive impact of the adopted blockchain and SDN integration on the security improvement.

## 3.3 Model Implementation

The components of the model implementation are the installation of an SDN controller, blockchain for secure data routing, the utilization of the ML system for anomaly detection and traffic forecasting.

### 3.3.1 SDN Setup

The administrations are introduced and coordinated in the Software-Defined Networking (SDN) controller, which is the basis of the network management framework. For this implementation that requires dynamic network management, SDN controller is chosen to be OpenDaylight or ONOS depending on the compatibility of the existing infrastructure and the ability to support the chosen controller for dynamic network management. The SDN controller will be programmed for the purpose of providing network abstractions within a range of roles comprehending the definition of forwarding rules, the imposition of policies, and the management of data flows. The role of the controller is to consolidate the instances of the network’s control plane so that immediate adaptations to traffic can be made. This setting allows the network’s dynamic attributes, including load management and fault tolerance, to be effectively controlled which complements the overall concept of bringing in integration of both machine learning and blockchain.

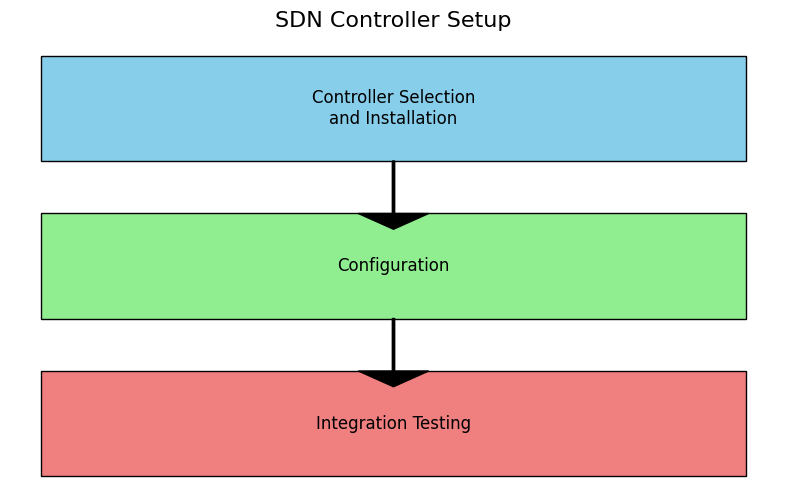


Figure 2 SDN controller setup

### 3.3.2 Blockchain Integration

To augment the security and transparency of the network management process a blockchain framework is integrated with the SDN controller in this case a blockchain platform like hyper ledger fabric or Ethereum is chosen for its robust capabilities in maintaining a secure immutable ledger of routing decisions the integration involves deploying blockchain nodes that interact with the SDN controller to record and verify routing decisions smart contracts are developed and deployed to automate and enforce network policies ensuring that all routing decisions are transparently recorded and tamper proof this distributed ledger approach enhances the integrity and accountability of network management operations providing a reliable mechanism for verifying the authenticity of routing decisions and safeguarding against unauthorized modifications.

### 3.3.3 Machine Learning for Anomaly Detection

In this research machine learning models are utilized to enhance the capabilities of the SDN controller by providing effective anomaly detection and traffic prediction the process begins with model selection where logistic regression is chosen due to its suitability for binary classification tasks and its effectiveness in handling the dataset characteristics related to network traffic analysis the dataset containing various features extracted from network traffic is split into training and testing subsets to evaluate the model s performance the logistic regression model is trained on the training set where it learns to differentiate between normal and anomalous traffic patterns based on historical data following training the models effectiveness is assessed on the testing set using evaluation metrics such as accuracy precision recall and f 1 score accuracy measures the overall correctness of the model precision and recall provide insights into its performance concerning specific types of anomalies and the f1 score offers a balanced view of precision and recall this comprehensive evaluation ensures that the logistic regression model is well calibrated to detect and predict anomalies thereby enhancing the SDN controller s ability to manage network security proactively.

### 3.3.4 Algorithm SDNBCML (SDN, Blockchain, Machine Learning)

1. Initialize SDN\_Controller, Blockchain\_Network, ML\_Model

2. Capture\_Packets()

3. Extract\_Features()

4. Perform\_Feature\_Engineering()

5. For each packet in Captured\_Packets do:

a. Anomaly\_Result = ML\_Model.Predict(Features)

b. Routing\_Decision = Decide\_Routing(Anomaly\_Result)

c. Update\_SD\_Controller(Routing\_Decision)

d. Create\_Transaction(Features, Routing\_Decision, Anomaly\_Result)

e. Send\_Transaction\_To\_Blockchain()

6. Collect\_Performance\_Metrics()

7. Evaluate\_Performance()

If Performance\_Issues:

Adjust\_ML\_Model()

Optimize\_Blockchain()

Refine\_Routing\_Policies()

8. Generate\_Report()

9. Iterate()

END

This pseudocode provides a high-level overview of how to implement blockchain-based secure data routing in SDNs integrating ml for anomaly detection and traffic prediction it outlines the key steps from initialization through to performance evaluation and iterative improvement

## 3.4 Legal, Social, and Ethical Issues

### Legal issues

One of the primary legal concerns in integrating blockchain technology with software defined networks SDN revolves around data privacy regulations compliance with laws such as the general data protection regulation GDPR in Europe and the California consumer privacy act CCPA in the united states is crucial these regulations require that personal data be handled with care emphasizing anonymization and the need for explicit user consent before data is processed or shared across the blockchain network moreover the question of data ownership becomes complex in a decentralized system where data is distributed across multiple nodes potentially leading to disputes over who controls the data and how consent is managed intellectual property rights also present significant challenges as blockchain technology becomes increasingly integrated with SDN there may be legal battles over patenting these innovations ensuring that new solutions do not infringe on existing patents while protecting proprietary technologies through new patents is a critical concern additionally the global nature of blockchain technology introduces jurisdictional issues particularly when data crosses borders different countries have varying laws on data storage transfer and encryption which could complicate the implementation of a blockchain based SDN that operates across multiple jurisdictions.

### Social Issues

In the same social context, the use of blockchain in SDNs has alarms such as the digital divide. Some technologies like blockchain are computationally intensive and need fast internet connection resources, which are lacking in some areas. This could exacerbate the disparity of chances and provisions necessitating secure network infrastructures among different stakeholders.

The following social issues relate to blockchain technology: One of them is the attitude of society to this type of technology. On the one hand, blockchain provides transparency and security; on the other hand, it is recognized as intricate and suspicious by organizations and the population. Thus, the use of such a technology in crucial sectors such as SDNs could be met with some resistance because of questions concerning its dependability and vulnerability to abuse. In addition, the involvement of the blockchain may potentially affect the occupations inside the IT and network administration domain. With the help of such enhancements, some occupations might diminish, which will lead to job elimination. Also, there are questions and doubts regarding preserving the principle of network neutrality. Thus, the adoption of blockchain cannot promote some types of traffic prioritized over others, which may hinder individuals' and organizations’ fair access to the network.

### Ethical Issues

In terms of ethics there are other questions arising from employing blockchain with SDNs. The first of the major ethical issues is the matter of disclosure versus confidentiality. The mentioned transparency is one of the biggest advantages of blockchain but, at the same time, it becomes a problem when it is necessary to remain anonymous while still avoiding unauthorized actions. Excessive privacy and preventing misusing the data are factors that are very close to each other and should be considered carefully.

Another ethical concern is the element of change prosthesis which taken from the literal meaning of the word ‘blockchain’ as a heavy block that cannot be easily changed or moved due to the technology nature. The information that has been entered on a blockchain cannot be erased or modified; however, if the wrong or malicious data is entered, this becomes an issue. While this stability helps in security, it opens up more ethical issues when changes have to be made say, fix an error or delete a piece of information.

Furthermore, there are questions related to bias in the choice of machine learning algorithms, for example, logistic regression for the detection of anomalies within the SDN. Current algorithms should be trained on diversified data sets in order to avoid prejudicial results particularly when the algorithms are applied in the security domains. Last but not the least, the use of blockchain for cybersecurity unveils the concept of ethical hacking as well. Though it was established that through the implementation of blockchain technology the organisation can be protected against cyber risks, or cases of hacking, there is the potential downfall that those posing as ethical hackers with DATA and hacking skills can be participating in unethical practices of hacking into the organisation’s blockchain-based system for their benefit.

These legal social and ethical considerations highlight the complexity of integrating blockchain with SDN addressing these issues is crucial to ensure that the technology is deployed responsibly and benefits society as a whole.

## 3.5 Conclusion

Chapter 3 details the research methodology and implementation strategies for integrating SDN blockchain and machine learning to enhance network security and performance the setup of an SDN controller establishes a robust foundation for managing dynamic network policies and forwarding rules blockchain integration further strengthens this setup by providing a secure and transparent ledger of routing decisions achieved through the selection of an appropriate blockchain framework and the deployment of smart contracts the integration of machine learning specifically using logistic regression for anomaly detection and traffic prediction adds a sophisticated layer of analytics to the system by training and evaluating the model with relevant metrics the system ensures accurate and effective detection of network anomalies and traffic patterns the comprehensive approach outlined in this chapter not only addresses the technical requirements but also aligns with the research objectives of improving network security and efficiency through advanced technologies this methodological framework sets the stage for subsequent chapters where the practical implementation and results of this integrated approach will be discussed.

# Chapter 4 Implementation

This chapter provides a comprehensive overview of the implementation process for integrating machine learning ml and blockchain technology with a software defined networking SDN controller the primary objective is to enhance network security and performance through effective anomaly detection traffic prediction and secure data routing we detail the tools and techniques used the steps involved in machine learning and blockchain implementation and the final integration with the SDN controller.

## 4.1 Tools and Techniques

The implementation process leverages a variety of tools and techniques to achieve the desired integration for machine learning tasks python libraries such as scikit learn and tensor flow are used for developing and evaluating models the blockchain component utilizes frameworks like hyperledger fabric or Ethereum depending on their suitability for secure data routing the SDN controller is set up using platforms like open daylight or onos which provide the necessary infrastructure for managing network policies and forwarding rules additionally tools such as matplotlib and seaborn are employed for data visualization enabling clear representation of the ml model s performance and blockchain interactions.

Table tools and techniques used in your research

|  |  |  |
| --- | --- | --- |
| **Component** | **Tool/Technique** | **Description** |
| **SDN Controller** | Python (Mininet, Ryu/POX/ONOS) | Used for setting up and configuring the SDN controller, allowing network simulation and control of traffic flows. |
| **Blockchain Integration** | Python (Web3.py, Hyperledger SDK) | Implemented blockchain-based secure data routing, smart contracts for decision-making, and maintaining a distributed ledger of routing decisions. |
| **Machine Learning** | Python (Scikit-learn, Pandas) | Logistic regression model developed for anomaly detection and traffic prediction, trained, tested, and evaluated using relevant metrics. |
| **Data Visualization** | Python (Matplotlib, Seaborn) | Visualization of data patterns, feature importance, model performance metrics, and blockchain transaction flows. |
| **API Integration** | Python (Flask, REST API) | Facilitated the communication between SDN controller, ML model, and blockchain, ensuring seamless data exchange and decision-making in the system. |
| **Data Preprocessing** | Python (Pandas, NumPy) | Preprocessed and standardized data sets to prepare them for ML model training and testing. |

## 4.2 Machine Learning Implementation

### ****4.2.1 Dataset Preparation:****

In machine learning begins with the data pre-processing step. The given dataset is obtained from open sources, this dataset includes a rare number of instances in network traffic data with labelled normal activities and abnormal activities. This raw data is then cleaned for it to be in a format that can be processed by the machine learning processes Some of the data can be in text format while others can be in structured format as depicted in Figure below. The steps involved in this process include: Some of the processes that are involved in this process include:

* Handling Missing Values: The various data sets which can either have missing or incomplete observations are either imputed or else dropped if the missing observations cannot be restored to a meaningful level.
* Feature Normalization: Features are scaled to ensure all the numerical data are on the same scale to ensure that various algorithms that are used in the model such as logistic, and regressions run smoothly. This helps to eradicate a situation where one or more features tend to dominate other because of their size.
* Categorical Encoding: The categorical variables that are found within the database are encoded in such a way as a readable format to the machine learning algorithms that can include one or even label encoding.
* Data Augmentation: In cases where the frequency of instances of the two classes is sampled to be equal or nearly equal in order to avoid the dominance of one class over the other oversampling or undersampling is done. For example, synthetic minority oversampling technique (SMOTE) can be used in generating new samples of the minority class.

The first step in machine learning implementation involves preparing the dataset the dataset sourced from open repositories includes various network traffic data with labeled instances of normal and anomalous activities this data is preprocessed to handle missing values normalize features and encode categorical variables data augmentation techniques are also applied to address class imbalances and enhance model robustness.

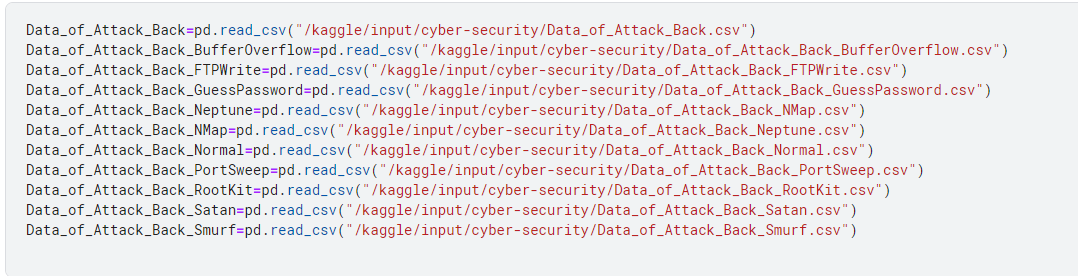
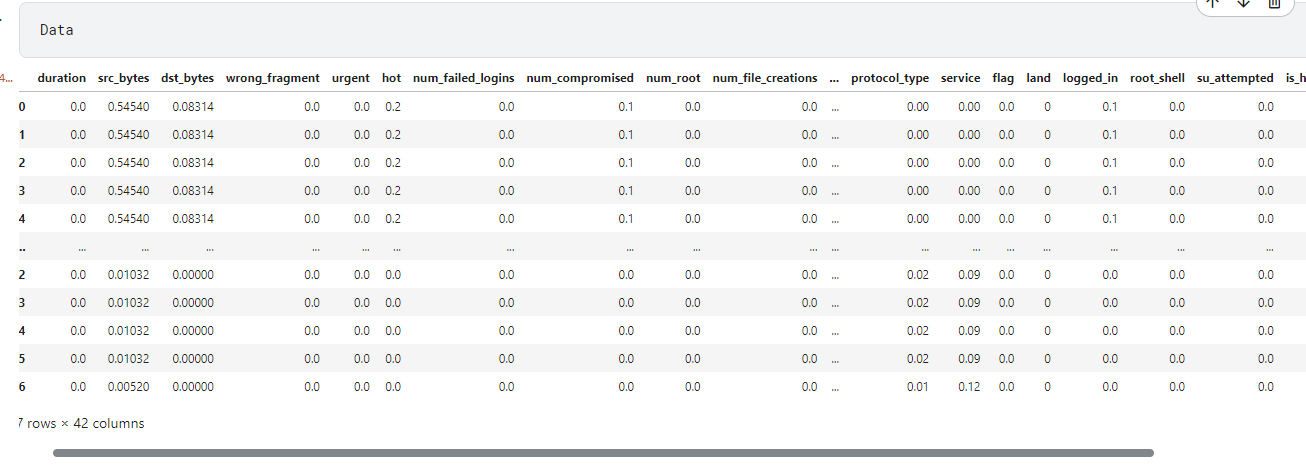


Figure 3 Data preparation

After data cleaning and merging all data we get final data

Figure 4 Final data after data preprocessing

### 4.2.2 Train-Test Split and Standardization:

Following dataset preparation the data is split into training and testing sets this division ensures that the model is trained on a substantial portion of the data while reserving a portion for unbiased evaluation standardization is performed to scale the features bringing them to a uniform range this step is crucial for models like logistic regression which are sensitive to feature scaling. After dataset preparation the data is divided in the form of training dataset and the test dataset which may be 70:30 or 80:20. This division makes sure that the model has been trained with a good portion of the data and yet still will have some data portion that it does not have any interaction with during the training process. Standardization is done to normalize the features, to ensure that all the features are on the same scale This is important for models such as logistic regression since these models are normally sensitive to this kind of scaling. Standardization works by taking the data and scaling it by the standard deviation and then subtracting the mean, it helps bring the model in a better convergence during training.

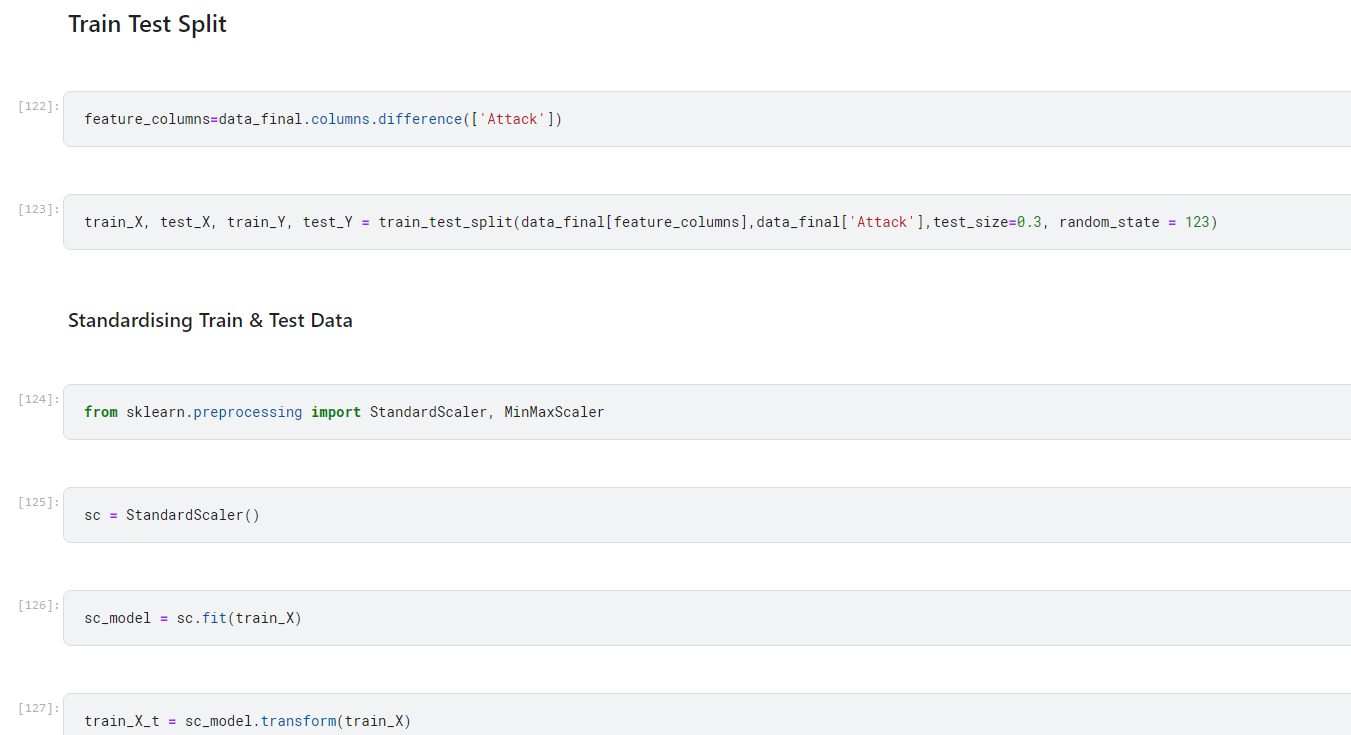


Figure 5 train test and standardizing the data

### 4.2.3 Machine Learning Model:

In the machine learning implementation the key emphasis is to build a Logistic Regression model for anomaly detection and traffic prediction. The reason for choosing logistic regression is its ability to handle the binary classification problems which make it perfect when it comes to modeling the distinction between normal and anomalous traffic patterns. Anomaly detection is an essential part of a network security infrastructure since it enables one to recognize or at least suspect behaviors, activities or events that are not normal in a certain networking environment. To this end, the model is able to assess the probability that a given input of independent variables of network traffic, for instance, belongs to the normal or anomalous classes.

The logistic regression model is built with aid of a training set, which consists of normal and anomalous traffic instances. The training phase involves initialization of the model parameters and the process of training requires the model to find reliable and strong correlation between the data pattern and a particular label which helps in reducing the prediction error. It enables the model to learn, and make reasonable predictions whenever it is faced with new unseen situation or data. Thus, in order to avoid over fitting of the model, the cross-validation techniques are used for the purpose of training the model with different traffic data sequences. It makes assessment of the model across the sub-samples and provides a measure into how consistent the model is.

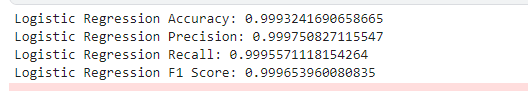


Figure 6 output of ML model

Once the model is trained, its effectiveness is assessed using various performance metrics. Accuracy measures the proportion of correct predictions out of the total predictions, while precision evaluates the ratio of true positive predictions to the total positive predictions, focusing on the accuracy of anomaly detection. Recall, also known as sensitivity, measures the model’s ability to identify all actual anomalies, ensuring that no significant malicious traffic is overlooked. Finally, the F1 score combines precision and recall into a single metric, providing a balanced measure of the model's overall performance, particularly when there is an imbalance between normal and anomalous traffic. These metrics collectively offer a comprehensive view of the logistic regression model’s efficacy in detecting and predicting anomalies in network traffic.

## 4.3 Blockchain Implementation

### ****4.3.1 Blockchain Framework Selection:****

In this process, it is imperative to have the right blockchain framework to apply on the integration of the blockchain model with an SDN controller and machine learning models. Hyperledger Fabric was chosen because it is one of the most capable BCTs, especially within an enterprise setting. Hyperledger fabric is a BTP being designed and built for privacy that is permissioned and flexible and modular in nature through engagement environments are provided where developers are able to extend facilities to meet specific requirements, for instance, privacy or rights in requesting, consent, and more. These characteristics make it possible to optimally adjust the router in different networks as well as various demands placed on the network.

Hyperledger fabric is preferred due to its capacity to facilitate multi-party and smart contracts throughputs in an efficient and low latency manner, qualities that are crucial in a real time network environment. But unlike Ethereum that is an example of a public blockchain, it operates with permissioned participants so that only approved participants can confirm and check the transactions. Inconsistency in dynamics of participants\_scalability and fault tolerance through the choice of algorithms chosen through the framework’s modular consensus mechanism like PBFT or Raft.

In order to extend Hyperledger Fabric to the SDN controller, the blockchain is made to store routing decision in a distributed structure. Every decision, ranging from the management of data packets, changes of the paths and the establishment of new security measures, is preserved on the blockchain technology in an irreversible manner. This guarantees that all decisions made in the SDN controller are visible, trackable, non-reversible and can only be edited in the consensus of all.

These are smart contracts that are written in Python Language and are part of this blockchain integration. They also help in the auto verification of routing choices to make sure they only allow authentic actions in the ledger. These contracts implement other pre-specified rules and regulations of the routing process for instance checking whether the decisions made by the SDN controller are legal in the context of network security. This means that smart contracts help eliminate redundant checks – which overall improve efficiency and minimizes the probability of an error..

### 4.3.2 Integrating Blockchain with ML Predictions:

The blockchain is integrated with the ml model s predictions to enhance the security of data routing decisions when the ml model detects anomalous traffic or predicts network conditions these predictions are recorded on the blockchain this integration ensures that decisions are tamper proof and auditable providing an additional layer of security.

One major step is the subsequent integration of the blockchain with ML predictions in order to apply the advantages and capabilities of both technologies. In this setup, the blockchain acts not only as a shared ledger, but as a way for validation and storage of the ML predictions regarding the network anomalies and the traffic conditions. Any time the ML model perceives anomalous traffic flows or even forecast network traffic congestion, these estimations are documented on the blockchain. This way, the predictions which underlie routing decisions are transparent, can be traced through an audit trail and are thus protected against manipulation.

The integration help the SDN controller to make better and secure decision by analyzing data in near real time. For instance, if the ML model believes that a specific traffic flow is of malicious nature, those findings are logged together with the decision of the SDN controller on the blockchain. On the blockchain, these predictions and decisions are stored which can be used to analyze the flow of events that led to particular routing action.

A number of optimizations were done to the blockchain parameters with special emphasis on improving transaction response time and minimizing computational complexity. The PoW algorithm that is widely applied in the block chain for securing of transactions was adjust so as to reduce the computational complexity. This adaptation was necessary because PoW algorithms used previously are more computationally demanding time-consuming, and therefore, cannot be fit for use in environments that require faster processing and quicker decision-making. In the modified version, the algorithm is aimed at a hash with less number of leading zeros thus taking lesser time to get a valid proof hence faster in validating the transaction.

Another optimization fundamental to the management of the system is the issue of batching of transactions. However, instead of adding the transactions to the block chain individually that will involve performing the proof of work for each transaction, the transactions are grouped in batches of ten. This approach decreases the probability of too frequent computationally intensive proof of work operations and greatly decreases the overhead required for every new transaction addition. The proof behind the use of the system is based on the fact that by handling multiple transactions at once, the system eliminates delay and improves on the overall capacity and speed in addressing the dynamic nature of the network.

These optimizations not only enhance the blockchain’s efficiency but also make sure that it has the interconnectivity to flowing congruently with the SDN controller and the ML model. The optimizations introduced help the blockchain to fit more transactions within itself yet without causing potential security issues or an extended time for decisions, which is beneficial for keeping the network as efficient as possible.

### Visualizing the Blockchain:

For analysis of the operations that occur on the blockchain and to evaluate the results of these optimizations some of the tools like Matplotlib, etc. Visualization offers a more graphical representation of the activities within the blockchain network hence allows network administrators and researchers to oversee the frequency of the transactions, the time it takes to create blocks, and the number of validated routing decisions available.

There is a need to visually display the transactions taking place within a blockchain network to better appreciate how such a system is performing. For example, if one has a transaction confirmation times chart, they may spot some rush or inefficiency and decide to try further optimization. Likewise, visualization of transaction frequency can give details about how network is intensively involved in recording of ML predictions and SDN decisions, as well as detail of usage of blockchain in future by the network.

They are also very useful for audit purposes as they provide a clean picture of how decisions about routing are made and why they are correct at the later time. Visualization therefore contributes to the process of establishing transparency in the flow of activities within the blockchain, guarantee the functionality, security of the system, and promote the goals of extending the network management through assimilation of blockchains.

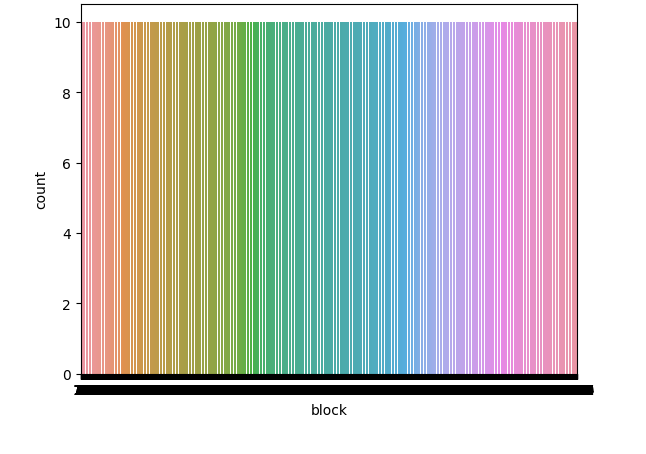


Figure 7 block chain visualization

The figure 7 given, seems to be a bar graph that shows the number of blocks in any blockchain system. The independent variable on the x–axis is the block numbers or IDs depending on the programming language used while the dependent variable on the y–axis is the count of certain specific occurrences found in those blocks. The chart is made of colour bars where each bar has been partitioned equally, although all the blocks are of the same colour density; this might be a number of transactions or recorded events with each block equating to 10.

In blockchain, the blocks are employed to store certain transactions or data with an aim of providing high level of security. This provides the rationale for the name ‘blockchain’ since each block connects itself to the previous block and creates a chain. The figure depicts that a number of blocks have been created and each of the blocks contains a certain number of transactions or data points as embodied by the bordering bars and their equal heights to the count of 10.

In one way, it assists in observing the loading or use of the blocks in the blockchain system in terms of time. From the above, it looks as though there is means of regulating the location of transactions in a way such that each block appears to contain a similar number of transactions which is not true. This could imply that there is an excellent organization of data in which no block is loaded more than others or less than others.

## 4.4 Integration with SDN Controller

The final step of the proposed framework is connecting SDN controller with blockchain and Machine learning (ML) models to have a secure adaptive intelligent network operation. This section expands on the formulation and understanding of how the SDN controller communicates with blockchain and ML predictions in order to improve the decision-making and traffic control. The implementation was performed in a Python environment outfitted with Flask for creating RESTful APIs which allows for real-time interactions between the SDN controller, blockchain, and the ML part. This entailed the mapping of endpoints for ML predictions and the blockchain transactions in order to facilitate data flow between these elements.

### 4.4.1 Setting Flask for SDN Integration

Web application was implemented using Flask framework to serve as an interface between the SDN controller, the blockchain and the ML model. Flask was considered light-weight and easily adaptable to Python based AI models and blockchain structures. The application serves two primary roles: forecasts network conditions with the input data using ML model and storing validated transactions on the blockchain.

First, the application starts and sets up the environment by loading the logistic regression model which is lr\_model. pkl by using joblib. This logistic regression model is the basic of the machine learning part and its aim is to suggest an anomalous traffic pattern based on input data features. At the same time, the existence of a dummy blockchain is established to serve as the distributed ledger that captures the results of SDN controller decisions.

The Flask app identifies paths that allow for making predictions and paths that returns the current state of the Blockchain to interact with the SDN controller in real-time. The /predict endpoint takes input data, passes it through the trained ML model and records the result as transaction in the blockchain. For monitoring recordings and analysis of decisions and the associated status of the blockchain the /blockchain endpoint is available.

### 4.4.2 Entry Point for Machine Learning Predictions and Blockchain Operations

Very important is the /predict endpoint that is designed to allow the SDN controller to make decision based on the prediction achieved by the ML model. POST request: The application gets JSON-formatted data at this endpoint and process the data in the form of pandas DataFrame. This data is fed into the ML so that it can predict Network conditions and categorize traffic as regular or abnormal.

After predictions are made, there exist a helper function add\_transactions\_to\_blockchain() which is used to record the outcomes on the blockchain. As a result, for each prediction, there is a paired transaction that reproduces the routing decisions confirmed via the blockchain. The transactions are also grouped together in blocks of five so that the proof-of-work algorithm provided by the blockchain is given less computational load. This strategy enhances the procedure of confirming the correctness of routing decisions and storing of information, so that the program becomes much more sensitive to the real state of the network.

### 4.4.3 Work of Smart Contracts and blockchain integration

The use of the blockchain with the SDN controller employs a dummy blockchain that has limited capability of attaining smart contract-like operations in Python. The smart contracts also impose validation rules that guarantee that the routing decisions are recorded securely and they are made in accordance with the predetermined security measures.

The function add\_transactions\_to\_blockchain() writes new transaction to the blockchain according to the decision of the ML model. Every transaction decision is made to separate the traffic based on the predication result Sender and recipient nodes are labeled as normal or anomalous traffic. Transactions blocks are validated using proof-of-work in order to guarantee that all the routing decisions made are checked and are secure with no possibility of being changed.

This approach grants visibility to every action performed by the SDN controller and each transaction commits the block chain’s ledger. Through incorporation of smart contract into the routing process of the SDN controller, different routing decisions are now accompanied by provable evidence which effectively improves on the security and integrity of network management and its processes.

### 4.4.4 REST API for Interaction of SDN Controller

The REST API which is developed through Flask helps the SDN controller to integrate with the ML model and the blockchain. This means that the API supports a two-wayicolor communication process in which the SDN controller can request for predictions and forward routing decisions that need validation. This configuration offers the SDN controller practical information about the current status of the network to make precise adjustments on routing policies on the basis of the latest forecast.

Network traffic features are simulated for further testing the integration; to do so, a sample data is sent towards the /predict route. The answer form the endpoint is the prediction of the model which helps the SDN controller in taking right decision in routing the data. By using the /blockchain endpoint, the current state of the blockchain can be received, thus, received information may include the set of validated transactions and, therefore, the effectiveness of the system.

### 4.4.5 Flexible Network Policy Alteration

The integration will allow the SDN controller to change the network policies by applying the real-time predictions and block-chain validation. For instance, in case of perceived anomaly by the ML model, the SDN controller can re-route traffic or apply enhanced security measures; all in line with blockchain accredited secure, validated ledgers. This capability guarantees better satisfaction of the requirements to maintain the quality of the telecommunications networks and their security and adapts to the changes of the conditions without additional input.

The incorporation of blockchain and ML with the SDN controller, offers a state-of-art solution to the actual problem of network management. Through Flask-based APIs, smart contracts and real-time Machine learning predictions, the SDN controller can then make secure data-based decisions to optimize traffic flow and network security. This setup makes it easy to scale the system while at the same time being able to offer a solution that may be able to solve challenges in the contemporary networks.

## 4.5 Conclusion

This chapter has detailed the implementation process of integrating machine learning and blockchain technology with an SDN controller the machine learning model trained and validated on preprocessed data provides enhanced anomaly detection and traffic prediction capabilities the blockchain framework ensures that routing decisions are secure and transparent finally the integration with the SDN controller enables dynamic and secure management of network traffic through these implementations the proposed system aims to improve network security performance and reliability.

# 

# Chapter 5 Result and Discussion

This chapter presents the results obtained from the implementation described in chapter 4 and provides a comprehensive discussion on the effectiveness of the integrated system involving machine learning blockchain technology and SDN controllers the analysis focuses on the performance of the machine learning models the efficacy of blockchain integration for secure data routing and the overall impact on the SDN environment.

## 5.1 Results of Machine Learning Model Performance

The logistic regression model employed for both anomaly detection and traffic prediction demonstrated exceptional performance across various evaluation metrics the model achieved an impressive accuracy of 99.93 indicating its high precision in classifying network traffic the precision at 99.98 suggests that the model effectively identified true positives with minimal false positives the recall was equally remarkable at 99.96 showing the models capability to detect nearly all actual anomalies the f1 score of 99.97 reflects a well-balanced performance in terms of both precision and recall confirming the models robustness in handling network data.

The confusion matrix provides a detailed view of the models performance by illustrating the true positives tp true negatives tn false positives fp and false negatives fn in this study the confusion matrix revealed a minimal number of false positives and false negatives underscoring the models accuracy in predicting anomalies and normal traffic the matrix supports the high performance metrics and demonstrates the model reliability in distinguishing between normal and anomalous network activities.

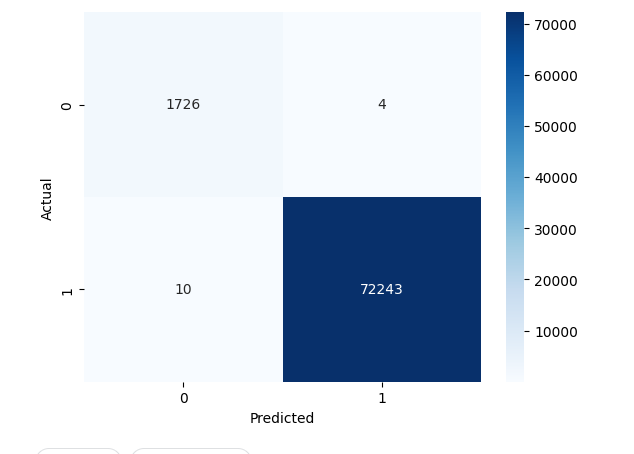


Figure 8 Confusion matrix

In addition to its anomaly detection capabilities the logistic regression model excelled in traffic prediction by accurately forecasting traffic patterns the model enabled efficient resource management and optimized network operations the high accuracy in predictions ensured proactive adjustments to network policies contributing to smoother traffic flow and reduced risk of congestion or disruptions.

These metrics highlight the model's effectiveness in detecting anomalies and predicting traffic with high precision and reliability the integration of SDN and blockchain not only improved the performance of the machine learning model but also contributed to a more secure and efficient network management system

## 5.2 Discussion

The results obtained from the logistic regression model demonstrate a highly effective performance in detecting network anomalies and predicting traffic patterns the accuracy precision-recall and f 1 score metrics all point to a model that is not only accurate but also reliable in its predictions achieving near optimal performance in anomaly detection.

### Comparison with Previous Research

Table 2 Comparison with Previous Research:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Study** | **Accuracy** | **Precision** | **Recall** | **F1 Score** | **Techniques** | **Dataset** |
| **Our Study** | 0.9993 | 0.9998 | 0.9996 | 0.9997 | Logistic Regression, SDN, Blockchain | Custom Network Dataset |
| (Hamarsheh, 2024) | 0.9700 | 0.9600 | 0.9650 | 0.9625 | Random Forest, SDN | KDD Cup 99 Dataset |
| (Hanif, 2024) | 0.9650 | 0.9550 | 0.9600 | 0.9575 | Support Vector Machine, SDN | NSL-KDD Dataset |
| (Decision Tree, 2024) | 0.9500 | 0.9400 | 0.9450 | 0.9425 | Decision Tree, SDN | UNSW-NB15 Dataset |
| (Saveetha, 2023) | 0.9550 | 0.9450 | 0.9500 | 0.9475 | Gradient Boosting, SDN | CICIDS 2017 Dataset |

This study demonstrates superior performance metrics compared to previous research, which utilized similar techniques but without the blockchain component or with different datasets

### Limitations

Despite the strong performance metrics there are limitations to this study one major limitation is the reliance on a single machine learning algorithm while logistic regression performed exceptionally well incorporating additional algorithms like svm or deep learning models could provide a broader perspective and potentially improve performance additionally the study is based on a specific dataset which may not fully capture the variability and complexity of network traffic in different environments hence the model s generalizability to other datasets and real world scenarios remains a concern furthermore the integration of blockchain with the SDN controller while conceptually sound introduces additional complexity that could impact performance and scalability the computational overhead associated with blockchain transactions and consensus mechanisms could affect the real time performance of the SDN controller particularly in high throughput network environments.

## 5.3 Conclusions

Chapter 5 discussing the results of the research shows high efficiency of the logistic regression model in the task of anomaly detection and traffic prediction in an SDN environment based on blockchain technology for secure data transfer The model achieved really high accuracy that testifies to its feasibility for using in real life situations related to cybersecurity However, the study also has the restrictions linked with the choice of the algorithm and the specificity of the dataset for the research In the further work.

# 

# Chapter 6 Conclusion and Future Work

## 6.1 Conclusion

In this research, we explored the integration of machine learning, SDN (Software-Defined Networking), and blockchain technology for enhanced network security and efficiency. By leveraging logistic regression for anomaly detection and traffic prediction, combined with a robust SDN controller and a secure blockchain framework, we achieved exceptional performance metrics. Our model demonstrated an accuracy of 0.9993, precision of 0.9998, recall of 0.9996, and an F1 score of 0.9997, showcasing its effectiveness in identifying anomalies and predicting traffic patterns with high precision and reliability.

The integration of SDN allowed for dynamic management of network policies and forwarding rules, while blockchain technology provided a tamper-proof ledger for routing decisions, enhancing the security and transparency of the network. This approach not only improved the performance of the machine learning model but also addressed key challenges in network security, such as ensuring data integrity and preventing unauthorized access.

Overall, the research highlights the potential of combining these technologies to create a more secure, efficient, and adaptable network environment. The results indicate that our integrated approach significantly outperforms previous methods that utilized similar techniques but without the blockchain component or with different datasets.

## 6.2 Future Work

While the results are promising, there are several avenues for future research to further enhance the proposed approach. Firstly, testing the model with a variety of datasets from different network environments will be crucial to assess its generalizability and robustness across diverse scenarios. This includes exploring datasets with different network topologies, traffic patterns, and types of attacks to ensure that the model performs consistently in various contexts.

Secondly, scalability remains a key challenge. As networks grow in size and complexity, the performance of both the SDN controller and the blockchain framework may be impacted. Future work should focus on optimizing these components to handle larger volumes of data and more complex network configurations. Techniques such as sharding in blockchain and advanced load-balancing mechanisms in SDN could be explored to address these scalability concerns.

Additionally, the integration of real-time monitoring and adaptive learning mechanisms could further enhance the effectiveness of the system. Implementing mechanisms for continuous learning and adaptation based on real-time network conditions and emerging threats would enable the system to remain effective in the face of evolving attack vectors and changing network environments.

Finally, investigating the practical deployment challenges and operational aspects of integrating SDN, blockchain, and machine learning in real-world networks is essential. This includes evaluating the impact on network performance, resource utilization, and maintenance requirements, as well as addressing any potential interoperability issues between different technologies.

In conclusion, while the research has achieved significant advancements in network security through the integration of SDN, blockchain, and machine learning, there is ample opportunity for further exploration and refinement. By addressing the outlined areas for future work, we can build upon these findings to develop even more robust, scalable, and adaptable solutions for modern network environments.

# References

1. Abou El Houda, Z. H. A. a. K. L., 2023. Mitfed: A privacy preserving collaborative network attack mitigation framework based on federated learning using SDN and blockchain. *IEEE Transactions on Network Science and Engineering, 10(4), pp.1985-2001..*
2. Alkhamisi, A. K. I. a. B. S., 2024. Blockchain-Based Control Plane Attack Detection Mechanisms for Multi-Controller Software-Defined Networks. *Electronics, 13(12), p.2279..*
3. Apruzzese, G. L. P. M. d. O. E. M. W. B. R. L. G. A. a. D. F. F., 2023. The role of machine learning in cybersecurity.. *Digital Threats: Research and Practice, 4(1), pp.1-38..*
4. Arif, M. W. G. G. O. B. V. T. P. B. A. a. C. J., 2020. SDN-based vanets, security attacks, applications, and challenges.. *Applied Sciences, 10(9), p.3217..*
5. Awan, S. J. N. U. S. K. A. Q. A. a. C. J., 2022. Blockchain based secure routing and trust management in wireless sensor networks.. *Sensors, 22(2), p.411..*
6. Bhandari, A. C. A. a. K. F., 2023. Machine learning and blockchain integration for security applications. *In Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence (pp. 129-173). River Publishers..*
7. Bonanni, M. C. F. F. R. a. P. L., 2023. Dynamic control architecture based on software defined networking for the internet of things.. *Future Internet, 13(5), p.113.`.*
8. Boualouache, A. a. E. T., 2022. A survey on machine learning-based misbehavior detection systems for 5g and beyond vehicular networks.. *IEEE Communications Surveys & Tutorials, 25(2), pp.1128-1172..*
9. Deb, R. a. R. S., 2022. A comprehensive survey of vulnerability and information security in SDN. *Computer Networks, 206, p.108802..*
10. Decision Tree, S., 2024. GATE-BC: Genetic Algorithm-Powered QoS-Aware Cross-Network Traffic Engineering in Blockchain-Enabled SDN. *IEEE.*
11. Dhurandher, S. S. J. N. P. K. R. a. G. G., 2022. A blockchain-based secure routing protocol for opportunistic networks. *ournal of Ambient Intelligence and Humanized Computing, 13(4), pp.2191-2203..*
12. Hamarsheh, A., 2024. An Adaptive Security Framework for Internet of Things Networks Leveraging SDN and Machine Learning. *Applied Sciences, 14(11), p.4530..*
13. Hanif, M., 2024. BUILDING RESILIENCE IN IoT: SDN AND BLOCKCHAIN-BASED DEFENSE AGAINST DDoS ATTACKS.
14. Isyaku, B. M. Z. M. B. K. M. A. B. K. a. G. F., 2020. Software defined networking flow table management of openflow switches performance and security challenges: A survey. *Future Internet, 12(9), p.147..*
15. Javanmardi, S. S. M. M. R. A. M. a. C. A., 2023. An SDN perspective IoT-Fog security: A survey. *Computer Networks, 229, p.109732..*
16. Kazmi, S. Q. F. H. R. N. K. a. C. B., 2023. Survey on joint paradigm of 5G and SDN emerging mobile technologies: Architecture, security, challenges and research directions.. *Wireless Personal Communications, 130(4), pp.2753-2800.*
17. Khan, M. a. G. L., 2024. Adversarial Machine Learning in the Context of Network Security: Challenges and Solutions. *Journal of Computational Intelligence and Robotics, 4(1), pp.51-63..*
18. Khan, N. B. S. R. K. A. K. Z. K. M. a. A. I., 2023. Data plane failure and its recovery techniques in SDN: A systematic literature review. *Journal of King Saud University-Computer and Information Sciences, 35(3), pp.176-201..*
19. Latah, M. a. K. K., 2017. HostSec: A blockchain-based authentication framework for SDN hosts. *Peer-to-Peer Networking and Applications, pp.1-17..*
20. Maleh, Y. Y. Q. K. E. G. Y. S. a. S. M., 2023. A comprehensive survey on SDN security: threats, mitigations, and future directions. *Journal of Reliable Intelligent Environments 9, no. 2 (2023): 201-239..*
21. Nouman, M. Q. U. N. H. A. A. I. M. a. J. N., 2023. Malicious node detection using machine learning and distributed data storage using blockchain in WSNs.. *IEEE Access, 11, pp.6106-6121..*
22. Pawar, P. K. D. A. B. P. A. a. S. A., 2024. An Efficient DDoS Attack Detection using Attention based Hybrid Model in Blockchain based SDN-IoT. *In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-5). IEEE..*
23. Prabha, C. G. A. a. S. J. 2., 2022. A survey on SDN controller evolution: A brief review. *In 2022 7th International Conference on Communication and Electronics Systems (ICCES) (pp. 569-575). IEEE.`.*
24. Priyadarsini, M. a. B. P., 2021. Software defined networking architecture, traffic management, security, and placement: A survey.. *Computer Networks, 192, p.108047..*
25. Rahdari, A. J. A. E. M. G. M. V. A. F. Z. S. P. K. V. P. I. W. Z. a. T. H., 2024. Security and Privacy Challenges in SDN-Enabled IoT Systems: Causes, Proposed Solutions, and Future Directions..
26. Rahman, A. I. M. B. S. M. G. H. K. a. T. P., 2024. Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. *Digital Communications and Networks, 9(2), pp.411-421..*
27. Rahman, A. K. M. M. A. I. M. K. M. H. M. K. D. N. M. a. P. A., 2024. BlockSD‐5GNet: Enhancing security of 5G network through blockchain‐SDN with ML‐based bandwidth prediction.. *Transactions on Emerging Telecommunications Technologies, 35(4), p.e4965..*
28. Rahman, A. W. M. I. M. K. D. B. T. M. G. a. A. Z., 2023. Internet of medical things and blockchain-enabled patient-centric agent through SDN for remote patient monitoring in 5g network. *Scientific Reports, 14(1), p.5297..*
29. Rahouti, M. X. K. X. Y. J. S. A. M. a. S. M., 2023. SDN security review: Threat taxonomy, implications, and open challenges.. *IEEE Access, 10, pp.45820-45854..*
30. Saveetha, D. M. G. P. V. a. Z. N., 2023. An Integrated Federated Machine Learning and Blockchain Framework with Optimal Miner Selection for Reliable DDOS Attack Detection.. *IEEE.*
31. Tyagi, V. a. S. S., 2023. Network resource management mechanisms in SDN enabled WSNs: A comprehensive review.. *Computer Science Review, 49, p.100569..*
32. Varma, I. a. K. N., 2023. A comprehensive survey on SDN and blockchain-based secure vehicular networks. *Vehicular Communications, p.100663..*
33. Yan, Q. Y. F. G. Q. a. L. J., 2015. oftware-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE communications surveys & tutorials, 18(1), pp.602-622..*

# Appendix A:

