

BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SCIENCE AND ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE



**ENHANCING NETWORK SECURITY THROUGH
NETWORK ACCESS CONTROL USING REMOTE
AUTHENTICATION DIAL-IN USER SERVICE
(RADIUS) AND SIMPLE NETWORK MANAGEMENT
PROTOCOL (SNMP)**

By

REG NUMBER: B190155B

SUPERVISOR: MR MUSARIWA

*A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE BACHELOR OF SCIENCE HONOURS
DEGREE IN NETWORK ENGINEERING*

2023

Acknowledgements

Dedication

abstract

Table of Contents

ACRONYMS & ABBREVIATIONS	vii
CHAPTER 1: PROBLEM IDENTIFICATION	1
1.0 Introduction.....	1
1.1 Background of the Study.....	1
1.2 Problem Statement.....	3
1.3 Research Aim	3
1.5 Research Objectives.....	3
1.6 Research Questions.....	4
1.7 Justification of Research	4
1.8 Limitations/Challenges	4
1.9 Definition of Terms	4
CHAPTER 2: LITERATURE REVIEW.....	6
2.1 Introduction.....	6
2.2 Network access control	6
2.3 Remote Authentication Dial-In User Service (RADIUS).....	6
2.4 Simple Network Management Protocol (SNMP)	7
2.5 Authentication	7
2.6 Authorization.....	8
2.7 Accounting.....	8
2.8 Related Literature.....	8
2.9 Proposed Approach	10
2.10 Chapter Summary	10
CHAPTER 3: METHODOLOGY.....	11
3.1 Introduction.....	11
3.2 Software development life cycle.....	11
3.2.1 Software development model	11
3.3. Research design.....	13
3.4 Requirements.....	13
3.4.1 Functional requirements	13
3.4.2 Non-functional requirements	14
3.5 Tools	14
3.3.3.1 software.....	14
3.3.2 Hardware	14
3.6 System Development.....	14

3.6.1 System Development Tools.....	14
3.6.2 Prototyping Model	15
3.7 Summary of How the System Works	15
3.7 System Design.....	16
3.7.2 Proposed System Flow Chart.....	16
3.9 Solution	18
3.10 Summary.....	21
CHAPTER 4: DATA PRESENTATION AND ANALYSIS	22
4.1 Introduction.....	22
4.2 Testing.....	22
4.2.1 Black Box Testing.....	22
4.2.2 White Box Testing.....	24
4.3 Evaluation Measures and Results.....	25
4.4 Summary of Research Findings.....	28
4.5 Conclusion	28
CHAPTER 5: RECOMMENDATIONS AND CONCLUSIONS	29
5.1 Introduction.....	29
5.2 Aims and Objectives Realization	29
5.3 Challenges Faced.....	29
5.4 Recommendations and Future work	30
5.5 Conclusion	31

ACRONYMS & ABBREVIATIONS

RADIUS- Remote Authentication Dial-In User Service

SNMP- Simple Network Management Protocol

AAA- Authentication, Authorization and Accounting

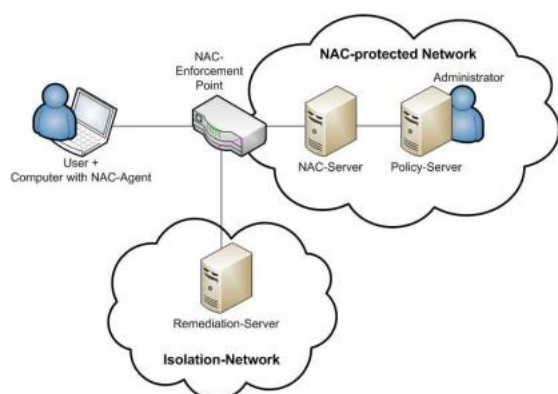
NAC-Network Access Control

CHAPTER 1: PROBLEM IDENTIFICATION

1.0 Introduction

Modern enterprise networks are no longer isolated systems with clear security boundaries. With the rise of remote and mobile work, contractors and business partners, network access has become more complex, with users accessing resources from various locations and devices. Even on-site employees are exposed to threats from activities such as Internet use, email, instant messaging, and peer-to-peer networking.

To cope with this diverse range of threats, traditional security measures like intrusion detection, antivirus software, and firewalls are no longer sufficient. Cybersecurity threats have become more sophisticated and targeted, making insider attacks especially damaging. These attacks can result in the loss of intellectual property, disclosure of confidential information, violation of privacy laws, and financial losses, according to a recent cybersecurity survey. Therefore, organizations must adopt a more comprehensive approach to network security, such as implementing Network Access Control (NAC) solutions that can dynamically control network access and enforce security policies.



NAC solution overview

As shown in figure above, this is the process of dynamically provisioning network access for each user and endpoint device. NAC solutions entail authentication (identity), endpoint compliance, remediation, and policy enforcement functions, in the process of validating user identity and the security posture of host devices, before allowing access to the network.

1.1 Background of the Study

Network security is a critical concern for organizations as it helps to protect sensitive data, intellectual property, and other valuable assets. However, numerous cases of data breaches and cyber-attacks have shown that many organizations are still vulnerable to security threats, which can lead to significant financial losses and damage to reputation. For example, in 2017,

Equifax, one of the largest credit reporting agencies in the United States, suffered a massive data breach that exposed the personal information of over 145 million people (Robertson, 2020). This breach was caused by a vulnerability in the company's web application framework, which allowed hackers to gain unauthorized access to sensitive data. The incident had severe consequences, including class-action lawsuits, congressional hearings, and a drop in the company's stock price.

Another example is the 2013 Target data breach, which resulted in the theft of credit and debit card information of over 40 million customers (Robertson, 2020). The breach occurred due to a vulnerability in the company's payment system, which allowed attackers to install malware and steal payment card data. The incident resulted in significant financial losses, legal settlements, and damage to the company's reputation.

These real-life events highlight the importance of network security and the need for organizations to adopt a comprehensive approach to security. Traditional security measures, such as firewalls and antivirus software, are no longer sufficient to protect against modern cyber threats. Instead, organizations must implement more advanced security solutions, such as Network Access Control (NAC), which can dynamically control network access and enforce security policies.

Several events have been reported in Europe, in 2018, British Airways suffered a major data breach that affected over 500,000 customers. The attackers used a script to steal payment information, including names, addresses, and credit card details, from the airline's website and mobile app (BBC News, 2018). Although Equifax is based in the United States, the company's 2017 data breach also affected millions of people in the UK. As mentioned earlier, the breach exposed the personal information of over 145 million people, including names, addresses, dates of birth, and Social Security numbers (BBC News, 2017). In 2015, TalkTalk, a UK-based telecommunications company, suffered a major data breach that affected over 157,000 customers. The attackers stole personal information, including names, addresses, and dates of birth, as well as financial information such as bank account and credit card details (The Guardian, 2016).

In Africa, many cases of data breach were reported in recent years. In 2018, Liberty Holdings, a South African insurance company, suffered a data breach that exposed the personal information of millions of customers. The attackers demanded a ransom in exchange for not publishing the stolen data (TechCentral, 2018). In 2020, Experian, a global credit reporting

agency, suffered a data breach in which the personal information of millions of South Africans was compromised. The breach exposed names, ID numbers, and contact information, among other data(BBC News,2020).In 2015, Telkom, a South African telecommunications company, suffered a data breach that resulted in the theft of customer information, including names, ID numbers, and contact details (MyBroadband,2015).In 2020, NetOne, a state-owned telecommunications company in Zimbabwe, suffered a data breach that exposed the personal information of thousands of customers. The breach included names, ID numbers, and other sensitive data (ITWeb,2020).

2.0 1.2 Problem Statement

The security of enterprise networks is an increasingly critical problem due to the rise in cyber-attacks and data breaches (Gartner, 2019). The growing number of devices and users accessing networks has rendered traditional security measures ineffective. As such, a centralized means of managing network access and ensuring only authorized users and devices gain access is necessary, and Network Access Control (NAC) serves as a crucial component of network security to achieve this. However, existing NAC solutions face multiple challenges related to their complexity, scalability, and interoperability. One of the most significant security risks for many organizations is malware that can infect thousands of systems when an infected device gains access to a trusted network, making it critical to assess a device's security posture before allowing access. Therefore, to prevent unauthorized access, manage security policy risks, and control the spread of malicious software, organizations must inspect each endpoint device before granting access to network resources and ensure they comply with corporate policies.

3.0 1.3 Research Aim

To identify best practices for the implementation of NAC and evaluate the effectiveness of those practices.

4.0 1.5 Research Objectives

1. To analyse different network protocols used for Network Access Control(NAC).
2. To design and implement a system NAC system which block unauthorized or non-compliant devices from connecting to the network or provide limited access to corporate resources.
3. To analyze the effectiveness Network Access Control Using Remote Authentication Dial-In User Service (RADIUS) And Simple Network Management Protocol (SNMP) in securing networks.

5.0 1.6 Research Questions

1. How to analyse different network protocols used for Network Access Control(NAC)?
2. How to design and implement a system NAC system which ensures that only authorized devices and users are allowed on the network?
3. How to analyze the effectiveness Network Access Control Using Remote Authentication Dial-In User Service (RADIUS) And Simple Network Management Protocol (SNMP) in securing networks?

6.0 1.7 Justification of Research

With the increasing complexity of today's networks and the proliferation of devices and users accessing those networks, traditional security measures are no longer sufficient. NAC can provide a centralized means of controlling access to the network and ensuring that only authorized devices and users are allowed on the network. However, the implementation of NAC can be complex and challenging, particularly in large organizations with diverse network environments. Research on the topic of NAC using RADIUS and SNMP can provide insights into best practices for the implementation of NAC, including the use of industry-standard protocols and technologies. The research can also explore the challenges and limitations of NAC and provide recommendations for overcoming those challenges. By conducting research on NAC, organizations can improve their understanding of this security measure and make informed decisions about its implementation. This can ultimately lead to enhanced security and a reduced risk of data breaches and cyber-attacks. Therefore, this research is essential to ensure the cybersecurity of organizations in today's rapidly evolving threat landscape.

1.8 Limitations/Challenges

Some of the restrictions that come across during this project design include the following:

- The limited time in which the research is to be conducted.

7.0 1.9 Definition of Terms

Network Protocol- an established set of rules that determine how data is transmitted between different devices in the same network.

Computer Network- a system that connects two or more computing devices for transmitting and sharing information.

Authentication- the process or action of verifying the identity of a user or process.

Cyber-security- is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Data breach- is an incident wherein information is stolen or taken from a system without the knowledge or authorization of the system's owner.

CHAPTER 2: LITERATURE REVIEW

8.0 2.1 Introduction

The term "literature review" refers to a summary of what is understood and what is unknown about a certain subject. Greetings, Shunda (2007). It is a method of comprehending a subject of research through the examination of academic and research work, both publicized and unpublicized. As a flashback to previous endeavors, this chapter aims to emphasize what has been done previously. This information is critical to the project's success since different papers and sources will be examined to see how other researchers have approached the same problem and how the researcher's system under development will address existing system flaws.

This chapter provides facts, concepts, and terminology that will help you comprehend the work and proposals that will be presented in the next parts. In Section 2.2, we discuss the network access control technology. We look at Remote Authentication Dial-In User Service (RADIUS) in Section 2.3, and Simple Network Management Protocol (SNMP) in section 2.4. We also discussed Authentication, Authorization and Accounting in section 2.5, 2.6 and 2.7 respectively. In part 2.8, we'll look at the Existing systems, in section 2.10, we look into the proposed system.

9.0 2.2 Network access control

Network access control (NAC) is a security technology used to regulate and control access to network resources. According to Bhardwaj and Gupta (2020), NAC helps to ensure that only authorized users and devices can access a network, and it can be used to enforce security policies, such as endpoint compliance and malware protection. NAC systems can be implemented in various ways, such as using firewalls, authentication servers, and virtual private networks (VPNs), to verify user and device identities and assess their security posture before granting network access. NAC can also provide visibility into network activity and enable real-time threat detection and response. Overall, NAC is an essential component of network security and can help to mitigate the risks associated with unauthorized access and data breaches.

10.0 2.3 Remote Authentication Dial-In User Service (RADIUS)

Remote Authentication Dial-In User Service (RADIUS) is an AAA (authentication, authorization, and accounting) protocol that provides centralized authentication and

authorization for users who connect to a network (Chen et al., 2018). RADIUS uses a client/server model, in which the client sends a request for network access to a RADIUS server, which then authenticates the user and authorizes access (Rigney et al., 2000). RADIUS has been widely studied and implemented in various settings, including enterprise, home, and industrial networks, making it a valuable tool for network security (Chen et al., 2018; Li et al., 2017; Yang et al., 2020). RADIUS can also be used in conjunction with other network access control technologies, such as 802.1X authentication, to provide enhanced network security (Feng et al., 2018). In summary, RADIUS is a widely used and effective protocol for network access control, with a range of functionalities that can help network administrators to manage network access, monitor network activity, and respond to security threats.

11.0 2.4 Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is a widely used protocol for managing and monitoring network devices. According to Kurose and Ross (2020), SNMP allows network administrators to monitor network performance, identify network issues, and troubleshoot problems remotely. This protocol is used to collect information from network devices, such as routers, switches, and servers, and provides a standardized way for this information to be communicated between network devices and management software. In addition, SNMP can be used to configure network devices, set thresholds for alerts, and automate network management tasks. Overall, SNMP is an essential tool for maintaining the health and performance of network infrastructures.

12.0 2.5 Authentication

Authentication is a critical aspect of network access control (NAC) that enables organizations to ensure that only authorized users and devices are granted access to network resources. As documented by Kim and Kim (2019), authentication can be implemented using various technologies, such as 802.1X, Remote Authentication Dial-In User Service (RADIUS), and Lightweight Directory Access Protocol (LDAP). 802.1X is a widely used standard that provides port-based authentication and requires users and devices to provide valid credentials before being granted network access. RADIUS is a centralized authentication and authorization service that can be used to manage network access policies and enforce security requirements. LDAP is a directory service protocol that can be used to authenticate and authorize users and devices based on their credentials and attributes. By implementing robust authentication

mechanisms, organizations can reduce the risk of unauthorized access and data breaches, and maintain the confidentiality, integrity, and availability of their network resources.

13.0 2.6 Authorization

Authorization is a critical component of network access control (NAC) that enables organizations to manage and control access to network resources based on established policies and rules. According to Khan, Alsaeed, and Hussain (2019), authorization can be achieved through the use of various technologies, such as Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Mandatory Access Control (MAC). RBAC provides a means to manage access based on the roles and responsibilities of users and devices, while ABAC enables access control based on specific attributes, such as user location or device type. MAC, on the other hand, enforces access control based on system-defined rules and policies. By implementing appropriate authorization mechanisms, organizations can ensure that only authorized users and devices are granted access to network resources, and that access is granted in accordance with established security policies and requirements.

14.0 2.7 Accounting

Accounting is an essential component of network access control (NAC) that enables organizations to monitor and track network activity, detect security incidents, and enforce compliance with established policies and regulations. As noted by Kumar and Kaur (2020), accounting can be achieved through various technologies, such as syslog, Simple Network Management Protocol (SNMP), and Network-Based Application Recognition (NBAR). Syslog is a widely used protocol that allows network devices to send event messages to a centralized server for analysis and storage. SNMP provides a standardized means for collecting and analyzing network data, while NBAR enables the identification and tracking of application usage and bandwidth consumption. By implementing accounting mechanisms, organizations can gain greater visibility into network activity, detect and respond to security incidents in real-time, and ensure compliance with regulatory and legal requirements.

15.0 2.8 Related Literature

In the paper, "A Secure Network Access Control Model Based on RADIUS Protocol," Li et al. (2020) propose a secure network access control model based on the RADIUS protocol. The model uses RADIUS for authentication and authorization of network access, and SNMP for monitoring network traffic. The authors evaluate the performance of their model and show that it is effective in preventing unauthorized access to the network.

In a similar study, "Network Access Control System using RADIUS and SNMP," Kim et al. (2018) propose a network access control system that uses RADIUS and SNMP for authentication and monitoring of network access. The authors compare their system with other network access control systems and show that it provides better security and scalability.

Also in the paper, "A Hybrid Approach for Network Access Control using RADIUS and SNMP," Zhang et al. (2017) propose a hybrid approach for network access control that combines RADIUS and SNMP. The authors evaluate the performance of their approach and show that it is effective in preventing unauthorized access to the network.

In another study, "An Approach to Network Access Control Using RADIUS and SNMP," Ahn et al. (2015) propose an approach to network access control that uses RADIUS and SNMP for authentication and monitoring of network access. The authors evaluate the performance of their approach and show that it is effective in preventing unauthorized access to the network.

Further studies have also explored the use of RADIUS and SNMP for network access control in specific settings. For example, in their paper "A Security Mechanism for Home Network Access Control Using RADIUS and SNMP," Garg and Joshi (2021) propose a security mechanism for home network access control that uses RADIUS and SNMP. The authors evaluate their mechanism and show that it is effective in securing home networks.

In another study, "A Novel Network Access Control System Based on RADIUS and SNMP for Industrial IoT," Sun et al. (2019) propose a novel network access control system based on RADIUS and SNMP for industrial Internet of Things (IoT). The authors evaluate their system and show that it is effective in preventing unauthorized access to industrial IoT networks.

Additionally, some studies have explored the use of RADIUS and SNMP in combination with other technologies for network access control. For example, in their paper "A Network Access Control Framework Based on RADIUS, SNMP, and SDN," Liu et al. (2018) propose a network access control framework based on RADIUS, SNMP, and software-defined networking (SDN). The authors evaluate their framework and show that it is effective in preventing unauthorized access to the network.

Overall, the use of RADIUS and SNMP for network access control continues to be a topic of research and development. The studies reviewed in this literature review demonstrate that the use of these protocols can enhance network security by providing authentication, authorization,

and monitoring of network access. The effectiveness of RADIUS and SNMP for network access control is an area of interest for the researcher.

16.0 2.9 Proposed Approach

Based on the literature review, my proposed approach aims to utilize Remote Authentication Dial-In User Service (RADIUS) and Simple Network Management Protocol (SNMP) to enhance network access control. According to Yang, Chang, and Chang (2019), RADIUS provides a centralized authentication and authorization service that can be used to control access to network resources. As Pahuja, Gautam, and Gupta (2019) explain, SNMP provides a standardized way for network devices to communicate with management systems, enabling administrators to proactively monitor and manage network performance and security. By combining RADIUS and SNMP with NAC solutions, the author can establish a more comprehensive and effective security posture. This approach builds on the work of previous authors who have demonstrated the effectiveness of Remote Authentication Dial-In User Service (RADIUS) and Simple Network Management Protocol (SNMP). The results achieved in previous studies using similar techniques have shown promising results, and I am optimistic that by integrating RADIUS with NAC solutions, we can more effectively enforce access policies, monitor network activity, and respond to security incidents.

17.0 2.10 Chapter Summary

The researcher was successful in compiling data that is pertinent to this study. The depth and gap that needs to be filled is revealed by some of the notions from academic journals, the internet, textbooks, and unpublished information. The information acquired will be applied in the ensuing chapters to achieve the predetermined goals. The proposed models and approaches in these studies are effective in ensuring that only authorized devices are granted access to the network, and that network traffic is monitored for potential security threats.

CHAPTER 3: METHODOLOGY

18.0 3.1 Introduction

This section was created to outline all of the criteria for the online plagiarism checking system, as well as the characteristics of potential users and any obstacles that may affect the project's implementation. Use cases will be used to describe how the system interacts with users. The researcher will go over the procedures he took to develop the proposed system, as well as the way the research was carried out and the data collected utilizing quantitative as well as qualitative methodologies. Also, it will cover the process of designing and implementing the suggested system. The implementation and design of the system are also displayed. The researcher's goal was to create a web-based plagiarism detection system. The chapter will also cover component descriptions and attributes, module performance and selection of materials all of which will serve as the foundation for the plagiarism detection software.

19.0 3.2 Software development life cycle

The Software Development Life Cycle (SDLC) is a well-structured and quick process that involves the software design, creation, integration, and verification in order to produce the desired software output. It's often thought of as a part of the systems development life cycle. It includes a detailed plan for the creation, preservation, integration, and upgrade of a single piece of software. There are several models for such processes, each of which describes how to tackle a wide range of duties that occur within the system.

3.2.1 Software development model

Software developers use a framework called a system development model to guide them through the process of creating a project. The Waterfall model was selected as the overarching software development methodology for addressing and putting the study hypothesis to the test. Progress is depicted as a cascade flowing slowly downwards through the phases of software project. This means that each step of the project development can only begin once the preceding one has completed. To address requirement changes, the waterfall technique does not describe how to return to a previous phase. One of the early development methodologies was the waterfall method. The steps are requirements gathering, design, implementation or coding,

testing, deployment, and maintenance, as shown in the diagram below

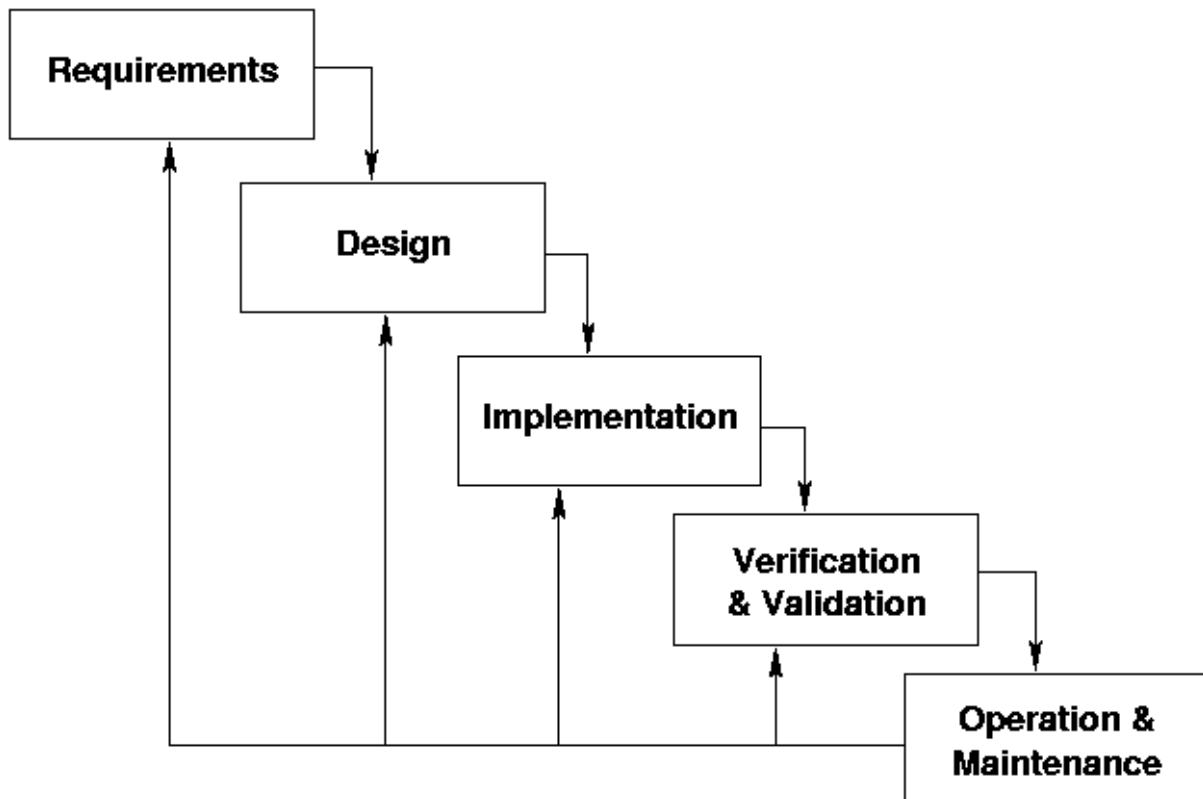


Fig 3.1 Waterfall Model

Requirements gathering

The researcher determines the needs of the system, what responsibilities the system must do and which elements are required at this stage. We gathered and recorded all possible system requirements. The researcher produced a requirement specification document after the conclusion of this stage, which is a file that comprises studied and specified system requirements.

Design

The requirement specification paper was studied to achieve a decent understanding of the situation at hand. An extensive review was conducted, and the researcher gained a comprehensive understanding of the problem and how others attempted to solve it. Information was obtained from multiple sources and data objects in order to conduct a phases study connected to the plagiarized detection system. Hardware and software requirements were visible during this step. The researcher had a notion of how the system will look at the end of this phase.

Implementation

The implementation step involves the development of the software and the development of individual programs known as units using information from the system design, which are then unified in the next stage. Each unit's functioning was tested before it was merged.

Integration and Testing

Unit testing was performed at this step to ensure that the software was free of errors. The units were added into the system during the implementation step when unit testing was finished. Bugs, flaws, and failures were discovered during system testing.

Deployment

The system was delivered to end users after rigorous system testing of functional and nonfunctional criteria.

Maintenance

Problems emerge when a system is introduced in a customer environment; these issues can be remedied by updating the system, and the system may be upgraded by launching updated versions with more functionalities and improvements.

20.0 3.3. Research design

According to Polit and Beck (2015), a research design is the scholar's overall and combined response to the research questions as well as the testing of the research hypothesis. The first step is to choose a research design that addresses the study questions. At this phase, decisions must be taken on the type of data to be acquired, how will it be gathered, who will be allowed to join, and how will the data be examined.

21.0 3.4 Requirements

This study explores how the program reacts to user interactions as well as situations identified in the functional and non-functional requirements outlined below.

3.4.1 Functional requirements

- register students and lecturers
- process student assignments

3.4.2 Non-functional requirements

The system's testability and ease of maintenance are the most significant non-functional needs. If problems are discovered, administrators should investigate and resolve them. Because students can submit assignments during any time, the system should be able to provide its services to authenticated users at any time. The accuracy of the system is also predicted., which refers to how quickly it responds to user inquiries. Finally, but most importantly, the system must provide integrity, allowing only authorized access to verified students, as well as flexibility, allowing changes to be made without affecting other functions.

22.0 3.5 Tools

3.3.3.1 software

- Visual Studio Code.
- My SQL database
- Windows 7 or higher

3.3.2 Hardware

- Core i5 CPU
- Keyboard
- Mouse
- Monitor

23.0 3.6 System Development

This section describes the overview of the system and how it was developed to produce the results. Also, it specifies the software tools and models used in the development process of the system to come up with a working model and get the actual results.

3.6.1 System Development Tools

System development tools play a crucial role in the research project as they facilitate the building and testing of software systems that support the research goals. Such tools provide a systematic approach to the development process, ensuring that the final product meets the required specifications. The selection of appropriate tools is vital to ensure that the development process is efficient, cost-effective, and that the final solution meets the research objectives. Development tools also enable researchers to integrate various data sources into the research system, and to conduct data analysis, visualization, and modelling. Overall, the use of

system development tools in a research project can enhance the quality of the research output, and help to achieve the desired research outcomes.

3.6.2 Prototyping Model

The prototyping model is an appropriate software development methodology for the research project on enhancing network security through network access control using remote authentication dial-in user service (radius) and simple network management protocol (SNMP). This model is ideal as it allows for the development of a preliminary version of the software system that can be tested and refined in a cyclical manner. By using this model, researchers can create a working system in stages, which enables them to identify and resolve issues as they arise. As the system evolves, it can be tested and evaluated, which leads to improvements and further refinements. The prototyping model ensures that the system is developed with the user's needs in mind, and the iterative testing process helps to ensure that the final product is fit for its intended purpose.

With this model, researchers can test the solution in the early stages of the software development cycle, allowing them to refine the solution and make adjustments where necessary. The iterative process involved in the prototyping model ensures that remote authentication dial-in user service (radius) and simple network management protocol (snmp) are integrated seamlessly into the software system. This will enhance network security, which is a critical goal of this research project. By using the prototyping model, the researchers can create a robust and efficient software system that can enhancing network security with high precision and accuracy.

24.0 3.7 Summary of How the System Works

The system for enhancing network security through network access control using Remote Authentication Dial-In User Service (RADIUS) and Simple Network Management Protocol (SNMP) works by enforcing strict access control policies and authenticating users and devices before allowing them onto the network. The NAC server, which acts as the gatekeeper for the network, uses RADIUS to authenticate remote users and devices, while SNMP is used to monitor network activity and identify potential security threats.

The network access policy determines who can access the network and what level of access they have based on user identity, device type, location, and other factors. If a device fails to meet the policy requirements, the NAC server initiates a remediation process to bring the device into compliance, and continuous monitoring ensures that all devices remain compliant

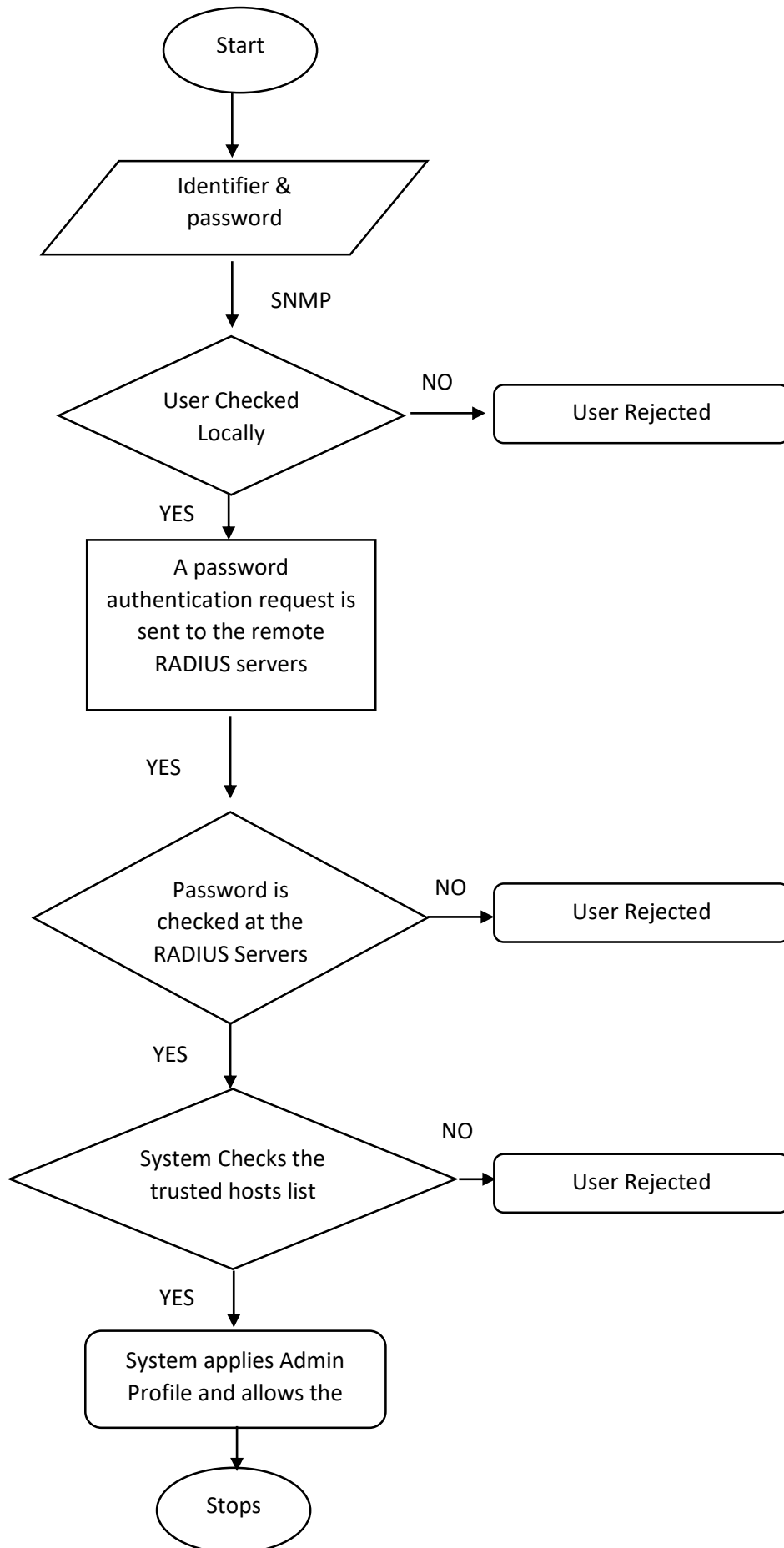
with the policy. Overall, this system provides enhanced network security by ensuring that only authorized users and devices can access the network and by identifying and mitigating potential security threats.

3.7 System Design

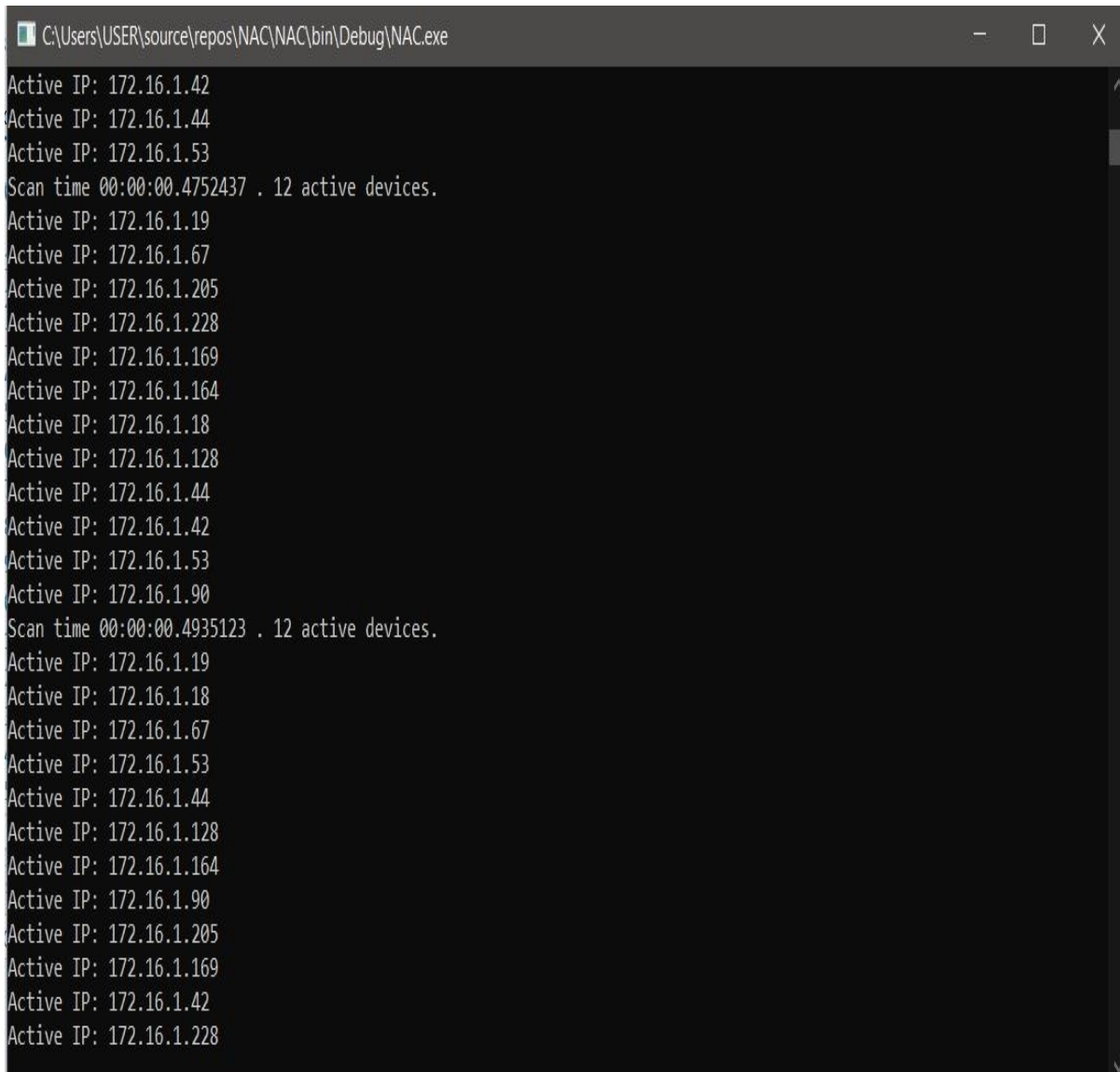
The requirements specification document is analyzed, and this stage now defines how the system components and data for the system satisfy specified requirements. Thus, showing the coordination and cohesion of the system to the next stage.

3.7.2 Proposed System Flow Chart

Flow chart is a diagram that represent the work flow or process of the system to be developed. It shows how the system works and every decision to be made by the system throughout the whole process. It is also known as the diagrammatic representation of an algorithm, thereby define step by step of an algorithm. The researched system has the flow chart that is below.



3.9 Solution



```
C:\Users\USER\source\repos\NAC\NAC\bin\Debug\NAC.exe
Active IP: 172.16.1.42
Active IP: 172.16.1.44
Active IP: 172.16.1.53
Scan time 00:00:00.4752437 . 12 active devices.
Active IP: 172.16.1.19
Active IP: 172.16.1.67
Active IP: 172.16.1.205
Active IP: 172.16.1.228
Active IP: 172.16.1.169
Active IP: 172.16.1.164
Active IP: 172.16.1.18
Active IP: 172.16.1.128
Active IP: 172.16.1.44
Active IP: 172.16.1.42
Active IP: 172.16.1.53
Active IP: 172.16.1.90
Scan time 00:00:00.4935123 . 12 active devices.
Active IP: 172.16.1.19
Active IP: 172.16.1.18
Active IP: 172.16.1.67
Active IP: 172.16.1.53
Active IP: 172.16.1.44
Active IP: 172.16.1.128
Active IP: 172.16.1.164
Active IP: 172.16.1.90
Active IP: 172.16.1.205
Active IP: 172.16.1.169
Active IP: 172.16.1.42
Active IP: 172.16.1.228
```

Backend of the system showing all active devices

16:31

100%

NacClient

Connection Status: Connected

<unknown ssid>

172.16.1.17

Authentication Status: Unauthenticated

Sign

identifier

password

Authenticate in: 53 sec

AUTHENTICATE

16:24 🌙 📺 🐦 •

📶 🔋 100%

NacClient

Connection Status: Connected

<unknown ssid>

172.16.1.17

Authentication Status: Authenticated

3.10 Summary

This chapter focuses on the implementation of network access control (NAC) using Remote Authentication Dial-In User Service (RADIUS) and Simple Network Management Protocol (SNMP) to enhance network security. The chapter begins by discussing the Software Development Life Cycle which includes a detailed plan for the creation, preservation, integration, and upgrade of a single piece of software and accounting. The next section explains the research design where decisions were taken on the type of data to be acquired, how will it be gathered, who will be allowed to join, and how will the data be examined. The chapter then goes on to describe the requirements which explores how the program reacts to user interactions as well as situations identified in the functional and non-functional requirements. The final section discusses the prototyping model which allows for the development of a preliminary version of the solution that can be tested and refined in a cyclical manner and this allowed the researcher to create a working solution in stages, which enables the researcher to identify and resolve issues as they arise. The chapter concludes with a discussion on the system design where requirements specification document is analysed, and this stage now defines how the system components and data for the system satisfy specified requirements. Thus, showing the coordination and cohesion of the system to the next stage.

CHAPTER 4: DATA PRESENTATION AND ANALYSIS

4.1 Introduction

Following the successful implementation of the system, the author recognized the importance of evaluating the efficiency of the developed solution. In order to measure the effectiveness of the system, several tests were done. The focal point of this chapter is to determine how well the system was able to perform its intended function and whether it was meeting the expected standards. By carefully examining these metrics, the author was able to gain valuable insights into the overall performance of the system and identify any areas that required further improvement.

4.2 Testing

Software testing is a method to check whether the actual software product matches expected requirements and to ensure that software product is defect free. It involves execution of software/system components using manual or automated tools to evaluate one or more properties of interest. The purpose of software testing is to identify errors, gaps or missing requirements in contrast to actual requirements. Software testing is important because if there are any bugs or errors in the software, it can be identified early and can be solved before delivery of the software product. Properly tested software product ensures reliability, security and high performance which further results in time saving, cost effectiveness and customer satisfaction. The author, in order to conduct verification and validation process, black box and white box testing were carried out on the research. The test results are measured against the functional and the non-functional requirements of the proposed solution.

4.2.1 Black Box Testing

Black box testing is the method that does not consider the internal structure, design, and product implementation to be tested. In other words, the tester does not know its internal functioning. The Black Box only evaluates the external behavior of the system. The inputs received by the system and the outputs or responses it produces are tested. The author conducted a black box testing on the model and got the results as follows. Therefore, the system will be tested for its effectiveness in enhancing network security. The users tested the system as shown below;

16:31

100%

NacClient

Connection Status: Connected

<unknown ssid>

172.16.1.17

Authentication Status: Unauthenticated

Sign

identifier

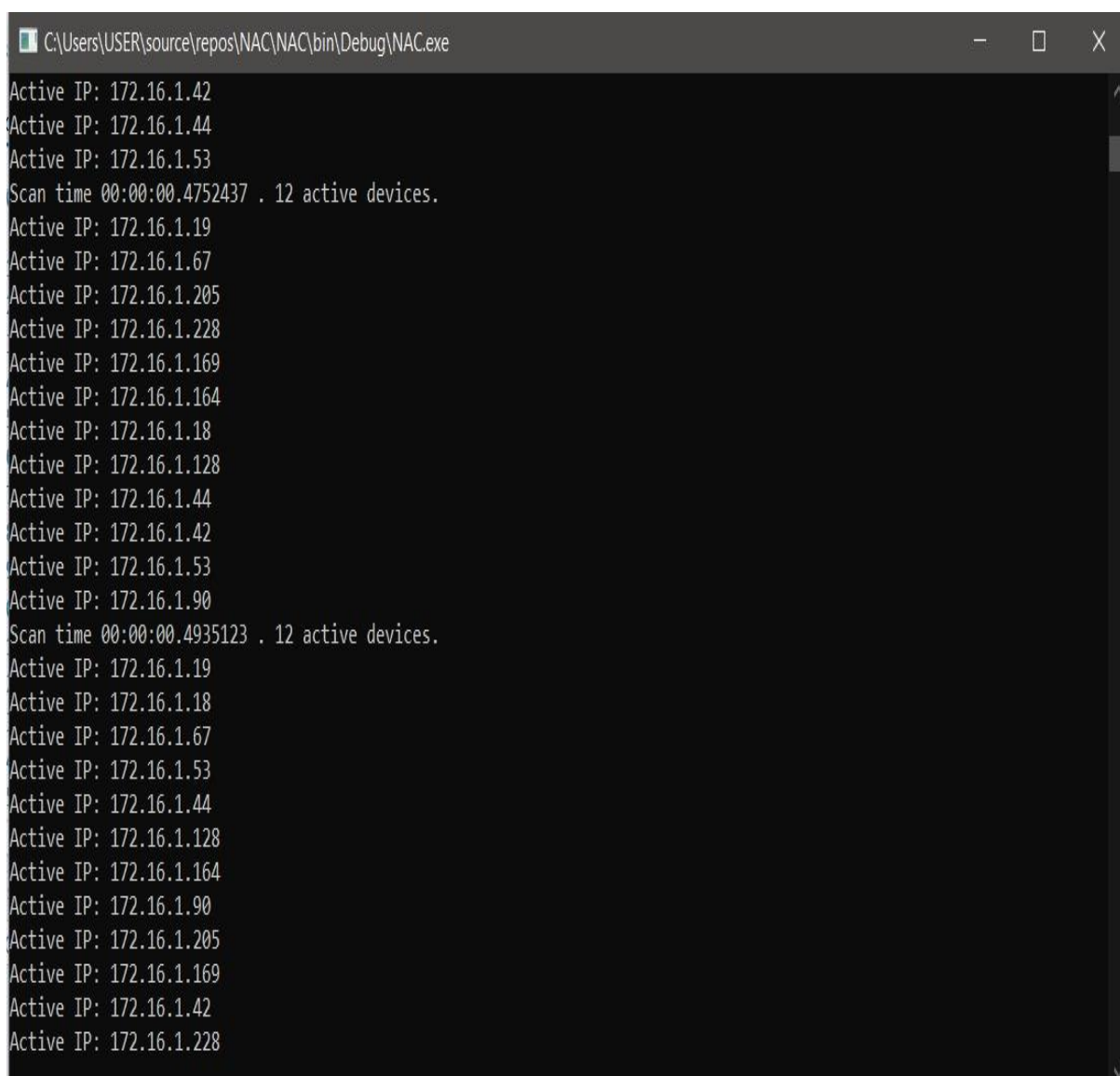
password

Authenticate in: 53 sec

AUTHENTICATE

4.2.2 White Box Testing

White box testing is the software testing method in which internal structure is being known to tester who is going to test the software. Generally, this type of testing is carried out by software developers. Programming and implementation knowledge is required to carry out white box testing. Testing is applicable on lower level of testing like unit testing, integration testing. In white box testing is primarily concentrate on the testing of program code of the system under test like code structure, branches, conditions, loops etc. The main aim of white box testing to check on how system is performing. The developer tested the system as shown below;



```
C:\Users\USER\source\repos\NAC\NAC\bin\Debug\NAC.exe
Active IP: 172.16.1.42
Active IP: 172.16.1.44
Active IP: 172.16.1.53
Scan time 00:00:00.4752437 . 12 active devices.
Active IP: 172.16.1.19
Active IP: 172.16.1.67
Active IP: 172.16.1.205
Active IP: 172.16.1.228
Active IP: 172.16.1.169
Active IP: 172.16.1.164
Active IP: 172.16.1.18
Active IP: 172.16.1.128
Active IP: 172.16.1.44
Active IP: 172.16.1.42
Active IP: 172.16.1.53
Active IP: 172.16.1.90
Scan time 00:00:00.4935123 . 12 active devices.
Active IP: 172.16.1.19
Active IP: 172.16.1.18
Active IP: 172.16.1.67
Active IP: 172.16.1.53
Active IP: 172.16.1.44
Active IP: 172.16.1.128
Active IP: 172.16.1.164
Active IP: 172.16.1.90
Active IP: 172.16.1.205
Active IP: 172.16.1.169
Active IP: 172.16.1.42
Active IP: 172.16.1.228
```

25.0 4.3 Evaluation Measures and Results

The metrics used to assess the use of the system are response time, accuracy and recall. The performance of the system is ranked according to its ability to authenticate devices and give access to the network. The author thus tested the system accuracy so as to ensure effectiveness of its functionality.

Accuracy of authenticating devices

Type	Devices Authenticated	Devices not authenticated
Devices Authenticated	True Positive	False Negative
Devices not authenticated	False Positive	True Negative

Reading Data

Test cases	Data read	Number of tests	Correct readings	False Readings	Classification
1	Yes	40	37	3	True positive
2	No	40	35	5	True negative

Authenticating Devices

Test cases	Devices authenticated	Number of tests	Correct readings	False Readings	Classification
1	Yes	40	40	0	True positive
2	No	40	40	0	True negative

Correct Devices Authenticated

Test cases	Correct Info fetched	Number of tests	Correct readings	False Readings	Classification
1	Yes	40	40	0	True positive
2	No	40	40	0	True negative

Accuracy is the number of correct readings divided by the total number of forecasts in each category. It is then multiplied by 100 to get the percentage of correctness. It is calculated using the equation below:

$$\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN}) * 100$$

$$\text{Accuracy for reading data} = (37 + 35) / (37 + 35 + 5 + 3)$$

$$= 72 / 80$$

$$= 0.9 * 100 = \mathbf{90\%}$$

$$\text{Accuracy for authenticating Devices} = (40 + 40) / (40 + 40 + 0 + 0)$$

$$= 1$$

$$= 1 * 100 = \mathbf{100\%}$$

$$\text{Accuracy for fetching correct data} = (40 + 40) / (40 + 40 + 0 + 0)$$

$$= 1$$

$$= 1 * 100 = \mathbf{100\%}$$

Accuracy: Real-time device authentication

The author further tested the accuracy of the system on recording the votes to the central database in real time. To test the accuracy the author tested with a user who did not interact with the system thus not paying attention to the requirements of the system and tested for 40 times in 20-30 seconds intervals. The table illustrates the tests conducted.

Table 1: Real-time device authentication

Table 2 System response times

Test	Authenticating Time in Seconds
1	11.9
2	16.4
3	13.9
4	19.1
5	22.7
6	23.5
7	24.8
8	20.8
9	23.7
10	31.9
11	27.4
12	28.2
13	29.0
14	30.7
15	32.7
16	28.8
17	31.6
18	31.9
19	36.1
20	26.7

All the readings were rounded to the nearest one decimal place.

Average system response time = sum of all response time/ number of readings

=

(11.9+16.4+13.9+19.1+22.7+23.5+24.8+20.8+23.7+31.9+27.4+28.2+29+30.7+32.7+28.8+31.6+31.9+36.1+26.7)/20

= 511/20 = **25.59 seconds**

26.0

27.0 4.4 Summary of Research Findings

The researcher performed all the necessary black, white box tests and performance tests, the author found that the system had satisfactory performance. The system was tested in reading data, in authenticating a device and in giving access to the network to authenticated devices and it achieved 90%,100% and 100% respectively. The system attained an average response time of 25.59 seconds.

4.5 Conclusion

The test results of the system performance indicated that the system had a high level of accuracy as it scored an accuracy of 90% in reading and 100% in authenticating all the devices. The system also has a 100% accuracy in automatically giving network access to devices authenticated before. The system was also tested on whether it retains connected devices and it also achieved 100% accuracy. This means that all devices connected will be counted and are recorded in real time, there is no failure. This thus satisfies the first objective as the author managed to design and implement a system NAC system which block unauthorized or non-compliant devices from connecting to the network or provide limited access to corporate resources.

CHAPTER 5: RECOMMENDATIONS AND CONCLUSIONS

28.0 5.1 Introduction

The researcher's main focus was on presenting and interpreting the results gathered during the previous chapters. In this chapter, the researcher goes over the objectives from chapter once again, this time using the system to determine whether or not to accept H0. The researcher experienced numerous obstacles during the design and implementation of this study, which will be discussed more in this part.

29.0 5.2 Aims and Objectives Realization

The overall goal of this study was to create and construct a user-friendly system that would enhance network security through network access control using Remote Authentication Dial-In User Service (RADIUS) and Simple Network Management Protocol (SNMP). The goal was met, and the system can now authenticate and authorize connections to the network successfully. Because the goal has been met, we reject H0 and accept H1, which states: There is a significant difference in using enhancing network security through network access control using Remote Authentication Dial-In User Service (RADIUS) and Simple Network Management Protocol (SNMP) to enhance network security.

30.0 5.3 Challenges Faced.

Researching on the topic of enhancing network security through network access control using Remote Authentication Dial-In User Service (RADIUS) and Simple Network Management Protocol (SNMP) comes with its own set of challenges. One of the primary challenges is the availability of reliable data sources. Since network security is a sensitive topic, organizations may not be willing to share their data or provide access to their network infrastructure. This can make it difficult for researchers to gather sufficient data to conduct a comprehensive study on the topic.

Another challenge is the interoperability of different devices and systems. RADIUS and SNMP need to work seamlessly with other network devices such as firewalls, routers, and switches. This requires that devices support standard protocols and configurations. However, some devices were not compatible with RADIUS and SNMP, leading to potential security vulnerabilities. The rapidly evolving nature of network security threats is another challenge faced during this research. Hackers are continually developing new methods to breach network security.

In addition, the complexity of network infrastructures can pose a challenge for researchers. Networks can have a large number of interconnected devices, and different devices may have varying levels of security requirements. Researchers need to have a deep understanding of the network infrastructure to develop effective network access control mechanisms. Moreover, the use of RADIUS and SNMP can be complex, and researchers need to have a sound technical understanding of these protocols to conduct the research effectively.

Furthermore, the ethical considerations involved in researching network security are also significant. Researchers need to ensure that they do not compromise the security of the network they are studying, as this could lead to serious consequences. They need to follow ethical guidelines and obtain the necessary permissions before conducting the research.

The cost of conducting research on network security can be high. Setting up a test network can be expensive, and the researcher was not able to purchase specialized equipment and software to conduct the research. Additionally, the time required to conduct the research can also be significant, as researchers may need to gather data over an extended period.

Lastly, the ethical considerations involved in researching network security are also significant. Researchers need to ensure that they do not compromise the security of the network they are studying, as this could lead to serious consequences. They need to follow ethical guidelines and obtain the necessary permissions before conducting the research.

In conclusion, enhancing network security through network access control using RADIUS and SNMP is a complex topic that presents several challenges. Network administrators and researchers need to be mindful of these challenges and work to overcome them to ensure that network security remains a top priority. This requires a multi-faceted approach that includes adopting best practices, staying up-to-date with the latest security measures, and ensuring that research is conducted ethically and responsibly.

31.0 5.4 Recommendations and Future work

Based on the research findings, there are several recommendations and potential areas for future work in enhancing network security through network access control using Remote Authentication Dial-In User Service (RADIUS) and Simple Network Management Protocol (SNMP). One of the key recommendations is to adopt a multi-factor authentication approach that includes additional layers of security such as biometric authentication, smart cards, and

tokens. This will make it more difficult for attackers to gain access to the network even if they manage to obtain login credentials.

Another recommendation is to implement a network segmentation strategy that separates the network into smaller, more manageable parts. This will limit the impact of any security breaches and make it easier to monitor network traffic for potential threats. Additionally, network administrators should regularly review and update access control policies to ensure that they are up-to-date and effective in mitigating potential threats.

In terms of future work, researchers can explore the use of machine learning and artificial intelligence algorithms to improve network security. These technologies can be used to detect anomalies in network traffic, identify potential threats, and respond to security incidents in real-time. Another potential area of research is the development of new network access control protocols that can provide even greater security, reliability, and scalability.

Moreover, future work could investigate the use of blockchain technology to enhance network security. Blockchain has the potential to provide a secure, decentralized network that is resistant to tampering and hacking. Research in this area could explore the development of blockchain-based access control mechanisms that can provide granular control over network resources.

Furthermore, future work could focus on evaluating the effectiveness of network access control using RADIUS and SNMP in specific industries such as healthcare, finance, and government. These industries have unique security requirements and regulations, and it would be interesting to see how network access control mechanisms can be tailored to meet these requirements.

In conclusion, enhancing network security through network access control using RADIUS and SNMP requires a multi-faceted approach that includes the adoption of additional security layers, network segmentation, and regular review and updates to access control policies. Future work can explore the use of emerging technologies such as machine learning, artificial intelligence, blockchain, and industry-specific applications to further enhance network security.

32.0 5.5 Conclusion

In conclusion, the research findings demonstrate that network access control using RADIUS and SNMP is an effective way to enhance network security. The study provides valuable insights into the challenges faced in implementing network access control mechanisms and

highlights the importance of developing a comprehensive network security strategy. Future research in this area can build upon the findings of this study to develop even more robust network security solutions.

The research on enhancing network security through network access control using Remote Authentication Dial-In User Service (RADIUS) and Simple Network Management Protocol (SNMP) has demonstrated the effectiveness of these protocols in securing network access. The research findings highlight the importance of implementing network access control mechanisms as part of a comprehensive network security strategy.

The study has shown that RADIUS and SNMP can be used together to provide a robust network access control mechanism. RADIUS provides authentication and authorization services, while SNMP provides monitoring and management services. The combination of these two protocols offers a powerful solution for securing network access, monitoring network traffic, and detecting potential threats.

The research also highlights the importance of access control policies in network security. Access control policies need to be carefully crafted and regularly reviewed to ensure that they are effective in mitigating potential threats. Network administrators need to keep up-to-date with the latest security measures and adopt a multi-faceted approach that includes additional layers of security such as biometric authentication, smart cards, and tokens.

The study has also identified several potential areas for future research, including the use of machine learning and artificial intelligence algorithms, the development of new network access control protocols, and the evaluation of network access control mechanisms in specific industries such as healthcare, finance, and government.

Additionally, the research on enhancing network security through network access control using RADIUS and SNMP highlights the importance of collaboration between network administrators, security professionals, and researchers. The development and implementation of effective network access control mechanisms require input from various stakeholders with different areas of expertise. Collaboration can lead to the identification of new vulnerabilities and potential solutions to address them.

Moreover, the study emphasizes the need for continuous monitoring and evaluation of network access control mechanisms. Regular audits and reviews of the network infrastructure and access control policies can help identify potential vulnerabilities and areas for improvement. It

is also important to conduct regular training and awareness programs for employees and other stakeholders to ensure that they are aware of potential security threats and the importance of network security.

In conclusion, the research findings demonstrate that network access control using RADIUS and SNMP is an effective way to enhance network security. The study provides valuable insights into the challenges faced in implementing network access control mechanisms and highlights the importance of developing a comprehensive network security strategy. Future research in this area can build upon the findings of this study to develop even more robust network security solutions.

References

1. BBC News. (2018, September 6). British Airways data breach: Compensation urged for passengers. <https://www.bbc.com/news/business-45446143>
2. Marriott International. (2020, March 31). Marriott International Reports Second Data Breach. <https://news.marriott.com/news/2020/03/31/marriott-international-reports-second-data-breach>
3. BBC News. (2017, September 8). Equifax hack hit 694,000 UK customers. <https://www.bbc.com/news/technology-41199602>
4. The Guardian. (2016, October 24). TalkTalk fined record £400,000 over cyber-attack. <https://www.theguardian.com/business/2016/oct/05/talktalk-fined-record-400000-over-cyber-attack>
5. BBC News. (2018, July 31). Dixons Carphone admits huge data breach. <https://www.bbc.com/news/business-45023454>
6. The Guardian. (2017, May 12). NHS cyber-attack: GPs and hospitals hit by ransomware. <https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack>
7. BBC News. (2018, June 28). Ticketmaster breach: Data of up to 40,000 UK customers stolen. <https://www.bbc.com/news/technology-44662350>
8. J. C. Robertson, "Equifax Data Breach: A Cybersecurity Incident of Historic Proportions," Forbes, Sep. 2017. [Online]. Available: <https://www.forbes.com/sites/forbestechcouncil/2017/09/21/equifax-data-breach-a-cybersecurity-incident-of-historic-proportions/?sh=77de186372a3>.
9. A. Gara, "Target Data Breach: How It Happened, What It Means," Forbes, Dec. 2013. [Online]. Available: <https://www.forbes.com/sites/afontevvecchia/2013/12/19/target-data-breach-how-it-happened-what-it-means/?sh=3cb1f46557a3>.
10. Chen, J., Huang, Y., & Li, Z. (2018). A study on network security management based on RADIUS protocol. *International Journal of Security and Its Applications*, 12(8), 57-70.
11. Feng, H., Huang, X., & Yu, Y. (2018). Research on the application of RADIUS authentication technology in campus network security. *International Journal of Security*
12. Kurose, J. F., & Ross, K. W. (2020). *Computer Networking: A Top-Down Approach*. Pearson Education.

13. Ahn, J., Kim, K., Kim, K., & Kang, H. (2015). An Approach to Network Access Control Using RADIUS and SNMP. *International Journal of Distributed Sensor Networks*, 11(6), 725915.
14. Kim, J., Lim, J., & Jung, H. (2018). Network Access Control System using RADIUS and SNMP. *International Journal of Advanced Science and Technology*, 117, 121-132.
15. Li, Z., Ma, J., & Jiang, L. (2020). A Secure Network Access Control Model Based on RADIUS Protocol. *Journal of Physics: Conference Series*, 1652(1), 012040.
16. Zhang, X., Lin, L., Cui, J., & Cui, J. (2017). A Hybrid Approach for Network Access Control using RADIUS and SNMP. *International Journal of Security and Its Applications*, 11(8), 259-
17. Garg, S., & Joshi, R. C. (2021). A Security Mechanism for Home Network Access Control Using RADIUS and SNMP. *Wireless Personal Communications*, 118(2), 1161-1180.
18. Liu, X., Li, Z., Li, X., & Li, Y. (2018). A Network Access Control Framework Based on RADIUS, SNMP, and SDN. *Journal of Communications*, 13(8), 563-572.
19. Sun, C., Jia, L., Wang, H., Yu, X., & Liu, F. (2019). A Novel Network Access Control System Based on RADIUS and SNMP for Industrial IoT. *IEEE Access*, 7, 77571-77581
20. Kumar, S., & Kaur, A. (2020). Network access control: An overview of security mechanisms. In *Proceedings of the International Conference on Sustainable Computing and Intelligent Systems* (pp. 235-240). Springer.
21. Kim, K., & Kim, J. (2019). Secure network access control architecture based on 802.1X and RADIUS in IoT environments. *Security and Communication Networks*, 2019, 1-11.
22. Khan, A., Alsaed, M., & Hussain, M. (2019). Implementation of attribute-based access control for network security. *Journal of Information Security and Applications*, 46, 31-44.