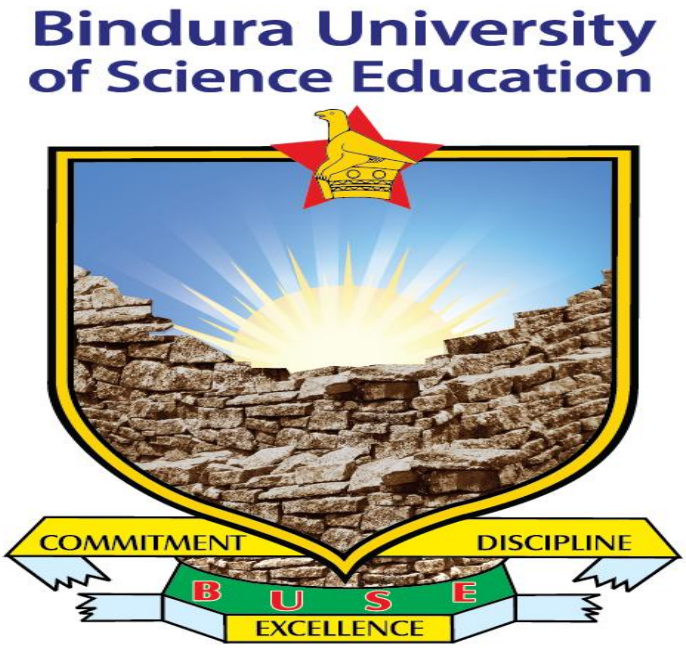


FACULTY OF SCIENCE AND ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE

HOME NETWORK MONITORING SYSTEM WITH PARENT-FRIENDLY DASHBOARD

Name: SITHOLE ETHEL M

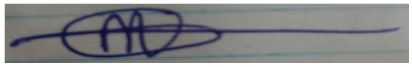
Student Number: B223770B

Supervisor: F CHITUMA

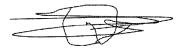
This research project is submitted to the Department of Computer Science at the Bindura University of Science Education in partial fulfillment of the requirements of the Bachelor of Science Honours Degree (BSc Hons) in Network Engineering (2026)

Approval Form

The undersigned certify that they supervised B223770B SITHOLE ETHEL MATTIE dissertation entitled “Home Network Monitoring System with a Parent-Friendly Dashboard” submitted in partial fulfillment of the requirement for Bachelor of Science Honors’ Degree in Network Engineering.

Student 

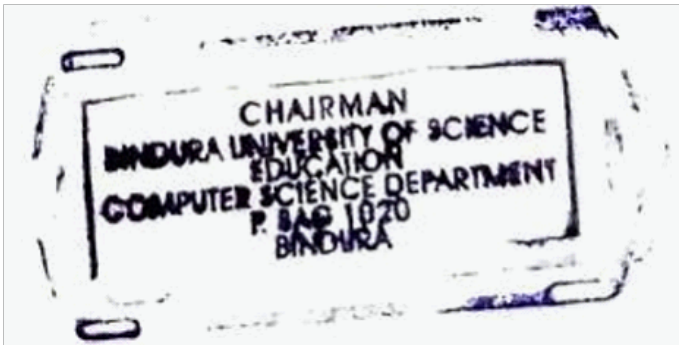
Date 23/06/2026

Supervisor 

Date 23/06/2026

Chairperson 

Date 23/06/2026



Declaration

I hereby declare that all information contained in this project report, titled *"Home Network Monitoring System with a Parent-Friendly Dashboard,"* has been obtained and presented in accordance with scholarly policy and standards. As required by these policies and standards, I have fully written this project based on truth and have cited all activities and tasks carried out during the research and development process. I therefore declare that this work is free from plagiarism. Any other copy presented elsewhere without proper credit to the author shall be regarded as plagiarized, null, and void.

Author: Sithole Ethel M

Reg No: B223770B

Acknowledgements

To all those who provided me with the opportunity to complete this project, I would like to express my deepest appreciation. A special thanks to my Supervisor Mr. Chituma, in his quest for academic excellence for the University and on an individual level shaping me into a better human being. Thank you for the comments, and insights you provided during the development of this dissertation. I extend my gratitude to my family members for their relentless moral and financial support. Fellow Network Engineering colleagues the class of 2026, your feedback, co-operation, team support and intellectual constructive criticism over the course of my upbringing and the rest of the four-year period hence this dissertation. My gratitude goes to my friends, who fueled the last sessions of my fourth year.

Abstract

This project describes the design and implementation of a Home Network Monitoring System with a parent-friendly dashboard, developed for improved supervision of household internet usage. The system aims to provide parents with an intuitive interface to monitor connected devices, track data consumption, and identify suspicious online activity within the home network. The study was conducted because of the growing need for families to maintain secure and responsible Internet access, especially for children. With the growing use of smart devices and online learning tools, many parents find it difficult to track Internet usage and ensure online safety for their children (Cisco, 2023). The system was built using Python and Flask for backend processing, combined with network scanning utilities to capture and display real-time traffic data. An adaptive three-layer scanning strategy (ARP, ICMP, and ARP cache reading) ensures compatibility across home routers, MiFi devices, and phone hotspots, with manual device addition as a fallback when client isolation prevents auto-discovery.

Dashboard design prioritized clarity and accessibility over technical depth, ensuring that parents without ICT backgrounds could interpret device activity and bandwidth usage without assistance. Evaluation showed that the system reliably identifies connected devices, monitors usage levels per device, and notifies parents when unusual patterns are detected, all through an interface that test users found straightforward to navigate. The study concludes that affordable, open-source monitoring tools designed with non-technical users in mind can meaningfully improve parental oversight and digital safety in home environments. Recommended directions for future development include machine learning-based anomaly detection and a mobile application interface for remote monitoring.

Table of Contents

APPROVAL FORM ..... **I**

DECLARATION ..... **II**

ACKNOWLEDGEMENTS ..... **III**

ABSTRACT ..... **IV**

LIST OF TABLES ..... **XI**

LIST OF FIGURES ..... **XII**

CHAPTER 1 ..... **1**

PROBLEM IDENTIFICATION ..... ERROR! BOOKMARK NOT DEFINED.

1.0 INTRODUCTION 1
1.1 BACKGROUND TO THE STUDY 2
1.2 STATEMENT OF THE PROBLEM 3
1.3 RESEARCH OBJECTIVES 3
1.3.1 Main Objective *3*
1.3.2 Specific Objectives *4*
1.4 RESEARCH QUESTIONS 4
1.5 RESEARCH PROPOSITIONS 5
1.6 JUSTIFICATION / SIGNIFICANCE OF THE STUDY 5
1.6.1 Academic Significance *5*
1.6.2 Practical Significance *6*
1.6.3 Institutional and Societal Relevance *6*
1.7 ASSUMPTIONS 6
1.8 LIMITATIONS / CHALLENGES 7
1.8.1 Technical Constraints *8*
1.8.2 Time Constraints *8*
1.8.3 Resource and Infrastructure Limitations *8*
1.8.4 User-Related Limitations *9*
1.8.5 Ethical and Privacy Challenges *9*
1.9 SCOPE / DELIMITATION OF THE RESEARCH 9
1.9.1 Geographical Scope *9*
1.9.2 Technical Scope *10*
1.9.3 User Scope *10*
1.9.4 Research Delimitation *10*
1.10 DEFINITION OF TERMS 11
1.11 SUMMARY 12

CHAPTER 2 ..... **13**

LITERATURE REVIEW **13**

2.0 INTRODUCTION 13
2.1 CONCEPTUAL FRAMEWORK 13
2.1.1 Home Network Monitoring *14*
2.1.2 Parental Engagement in Digital Safety *14*

2.1.3 Usability and User-Friendly Design *15*
2.1.4 Real-Time Visualization *15*
2.1.5 Security and Privacy *16*
2.2 Theoretical Framework 17
2.2.1 Human–Computer Interaction (HCI) *17*
2.2.2 Technology Acceptance Model (TAM) *17*
2.2.3 Systems Theory *18*
2.2.4 Diffusion of Innovation Theory *18*
2.3 Empirical Evidence 18
2.3.1 Global Studies *18*
2.3.2 African and Zimbabwean Context *19*
2.3.3 Usability and Adoption *20*
2.3.4 Security and Ethical Considerations *20*
2.4 Existing Systems and Tools 20
2.5 Research Gap Analysis 21
2.6 Network type comparison 22

CHAPTER 3 24

RESEARCH METHODOLOGY, SYSTEM DESIGN & IMPLEMENTATION 24

3.0 Introduction 24
3.1 Research Design and Data Collection Approaches 24
3.2 Population and Sample 25
3.3 Research Instruments 26
3.3.1 Questionnaire *26*
3.3.2 Interview Guide *26*
3.4 Data Analysis Procedure 27
3.5 Reliability and Validity 27
3.5.1 Reliability *27*
3.5.2 Validity *28*
3.6 Data Collection Process 28
3.7 Ethical Considerations 28
3.8 System Design and Implementation 29
3.8.1 Overview of the System 29
3.8.2 System Requirements *29*
3.8.3 System Architecture *31*
3.8.4 System Design Models *32*
3.8.5 System Implementation *34*
3.8.6 System Output *36*
3.8.7 System Testing and Validation *36*
3.8.7.1 37
3.8.8 System Limitations *37*
3.9 Summary 38

CHAPTER 4 39

DATA PRESENTATION, ANALYSIS AND INTERPRETATION 39

4.0 Introduction 39
4.1 Analysis and Interpretation of Results 40
4.1.1 Demographic Information *40*
4.1.2 Home Network Usage *43*
4.1.3 Child Online Safety *46*
4.1.4 Dashboard Feature Requirements *49*
4.2 Overall Evaluation 52

4.3 Interview Findings (Qualitative Results) 54
4.4 System Testing and Evaluation 55
4.4.1 Functional Testing 55
4.4.2 Performance Evaluation 55
4.4.3 Usability Evaluation 56
4.4.4 Security and Awareness Evaluation 56
4.4.5 Summary of Evaluation 57
4.4.6 Interface Enhancement Evaluation 58
4.5 Summary 58

CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS 59

5.0 Introduction 59
5.1 Major Conclusions Drawn 60
5.1.1 Objective 1: Identifying Challenges Faced by Non-Technical Users 60
5.1.2 Objective 2: Designing a System Architecture for Real-Time Monitoring 61
5.1.3 Objective 3: Developing a User-Friendly Web-Based Dashboard 62
5.1.4 Objective 4: Iterative Testing and Refinement 63
5.1.5 Objective 5: Delivering a Complete Integrated System Package 63
5.1.6 Overall Conclusion 64
5.1.7 Evaluation of Research Propositions 64
5.2 Study Limitations 66
5.3 Recommendations 66
5.3.1 Recommendations for households 67
5.3.2 Recommendations for system developers and organisations 67
5.3.3 Recommendations for Future Research 68
5.4 Summary 69

APPENDIX A: HOUSEHOLD QUESTIONNAIRE 71

APPENDIX B: INTERVIEW GUIDE 75

APPENDIX C: SYSTEM DESIGN DIAGRAMS AND INTERFACE MOCKUPS 78

APPENDIX D: SOURCE CODE 82

D1: Main Flask Application (app.py) 82
D2: Login Page (login.html) 84
D3: Dashboard Interface (dashboard.html) 85

APPENDIX E: SAMPLE SYSTEM OUTPUTS 89

E1: Login Page Screenshot 89
E2: Dashboard Screenshot 90
E3: Device Activity Monitoring Screen 91
E4: Alert Notification Example 92

REFERENCES 93

APPROVAL FORM I

DECLARATION II

ACKNOWLEDGEMENTS III

ABSTRACT IV

LIST OF TABLES XI

LIST OF FIGURES ..... **XII**

CHAPTER 1 ..... **1**

PROBLEM IDENTIFICATION ..... ERROR! BOOKMARK NOT DEFINED.

1.0 INTRODUCTION 1
1.1 BACKGROUND TO THE STUDY 2
1.2 STATEMENT OF THE PROBLEM 3
1.3 RESEARCH OBJECTIVES 3
1.3.1 Main Objective *3*
1.3.2 Specific Objectives *4*
1.4 RESEARCH QUESTIONS 4
1.5 RESEARCH PROPOSITIONS 5
1.6 JUSTIFICATION / SIGNIFICANCE OF THE STUDY 5
1.6.1 Academic Significance *5*
1.6.2 Practical Significance *6*
1.6.3 Institutional and Societal Relevance *6*
1.7 ASSUMPTIONS 6
1.8 LIMITATIONS / CHALLENGES 7
1.8.1 Technical Constraints *8*
1.8.2 Time Constraints *8*
1.8.3 Resource and Infrastructure Limitations *8*
1.8.4 User-Related Limitations *9*
1.8.5 Ethical and Privacy Challenges *9*
1.9 SCOPE / DELIMITATION OF THE RESEARCH 9
1.9.1 Geographical Scope *9*
1.9.2 Technical Scope *10*
1.9.3 User Scope *10*
1.9.4 Research Delimitation *10*
1.10 DEFINITION OF TERMS 11
1.11 SUMMARY 12

CHAPTER 2 ..... **13**

LITERATURE REVIEW **13**

2.0 INTRODUCTION 13
2.1 CONCEPTUAL FRAMEWORK 13
2.1.1 Home Network Monitoring *14*
2.1.2 Parental Engagement in Digital Safety *14*
2.1.3 Usability and User-Friendly Design *15*
2.1.4 Real-Time Visualization *15*
2.1.5 Security and Privacy *16*
2.2 THEORETICAL FRAMEWORK 17
2.2.1 Human–Computer Interaction (HCI) *17*
2.2.2 Technology Acceptance Model (TAM) *17*
2.2.3 Systems Theory *18*
2.2.4 Diffusion of Innovation Theory *18*
2.3 EMPIRICAL EVIDENCE 18
2.3.1 Global Studies *18*
2.3.2 African and Zimbabwean Context *19*
2.3.3 Usability and Adoption *20*
2.3.4 Security and Ethical Considerations *20*
2.4 EXISTING SYSTEMS AND TOOLS 20
2.5 RESEARCH GAP ANALYSIS 21

2.6 NETWORK TYPE COMPARISON 22

CHAPTER 3 24

RESEARCH METHODOLOGY, SYSTEM DESIGN & IMPLEMENTATION 24

3.0 INTRODUCTION 24
3.1 RESEARCH DESIGN AND DATA COLLECTION APPROACHES 24
3.2 POPULATION AND SAMPLE 25
3.3 RESEARCH INSTRUMENTS 26
3.3.1 Questionnaire 26
3.3.2 Interview Guide 26
3.4 DATA ANALYSIS PROCEDURE 27
3.5 RELIABILITY AND VALIDITY 27
3.5.1 Reliability 27
3.5.2 Validity 28
3.6 DATA COLLECTION PROCESS 28
3.7 ETHICAL CONSIDERATIONS 28
3.8 SYSTEM DESIGN AND IMPLEMENTATION 29
3.8.1 OVERVIEW OF THE SYSTEM 29
3.8.2 System Requirements 29
3.8.2.1 Functional Requirements 29
3.8.2.2 Non-functional Requirements 30
3.8.2.3 Security Requirements 30
3.8.3 System Architecture 31
3.8.3.1 Architecture Description 31
3.8.3.2 System Workflow 32
3.8.3.3 Database Design 32
3.8.4 System Design Models 32
3.8.4.1 Use Case Design 32
3.8.4.2 Data Flow Design 33
3.8.4.3 Interface Design 33
3.8.5 System Implementation 34
3.8.5.1 Backend Implementation 34
3.8.5.2 Frontend Implementation 35
3.8.5.3 Real-Time Dashboard Features 35
3.8.6 System Output 36
3.8.7 System Testing and Validation 36
3.8.7.1 Usability Testing 37
3.8.8 System Limitations 37
3.9 SUMMARY 38

CHAPTER 4 39

DATA PRESENTATION, ANALYSIS AND INTERPRETATION 39

4.0 INTRODUCTION 39
4.1 ANALYSIS AND INTERPRETATION OF RESULTS 40
4.1.1 Demographic Information 40
4.1.2 Home Network Usage 43
4.1.3 Child Online Safety 46
4.1.4 Dashboard Feature Requirements 49
4.2 OVERALL EVALUATION 52
4.3 INTERVIEW FINDINGS (QUALITATIVE RESULTS) 54
4.4 SYSTEM TESTING AND EVALUATION 55
4.4.1 Functional Testing 55
4.4.2 Performance Evaluation 55

4.4.3 Usability Evaluation *56*
4.4.4 Security and Awareness Evaluation *56*
4.4.5 Summary of Evaluation *57*
4.4.6 Interface Enhancement Evaluation *58*
4.5 SUMMARY 58

CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS 59

5.0 INTRODUCTION 59
5.1 MAJOR CONCLUSIONS DRAWN 60
5.1.1 Objective 1: Identifying Challenges Faced by Non-Technical Users *60*
5.1.2 Objective 2: Designing a System Architecture for Real-Time Monitoring *61*
5.1.3 Objective 3: Developing a User-Friendly Web-Based Dashboard *62*
5.1.4 Objective 4: Iterative Testing and Refinement *63*
5.1.5 Objective 5: Delivering a Complete Integrated System Package *63*
5.1.6 Overall Conclusion *64*
5.1.7 Evaluation of Research Propositions *64*
5.2 STUDY LIMITATIONS 66
5.3 RECOMMENDATIONS 66
5.3.1 Recommendations for households *67*
5.3.2 Recommendations for system developers and organisations *67*
5.3.3 Recommendations for Future Research *68*
5.4 SUMMARY 69

APPENDIX A: HOUSEHOLD QUESTIONNAIRE 71

APPENDIX B: INTERVIEW GUIDE 75

APPENDIX C: SYSTEM DESIGN DIAGRAMS AND INTERFACE MOCKUPS 78

APPENDIX D: SOURCE CODE 82

D1: Main Flask Application (app.py) *82*
D2: Login Page (login.html) *84*
D3: Dashboard Interface (dashboard.html) *85*

APPENDIX E: SAMPLE SYSTEM OUTPUTS 89

E1: Login Page Screenshot *89*
E2: Dashboard Screenshot *90*
E3: Device Activity Monitoring Screen *91*
E4: Alert Notification Example *92*

REFERENCES 93

List of tables

Table 2.1 Existing Systems and Tools **21**
Table 3.1: Development Tools and Technologies **34**
Table 3:2 Functional Testing **36**
Table 4.1: Age group **40**
Table 4.2: Gender **41**
Table 4.3: Area of residence **42**
Table 4.4: Role in household **42**
Table 4.5: Type of internet connection used **43**
Table 4.6: Number of devices connected **44**
Table 4.7: How confident are you in managing your home network **45**
Table 4.8: Monitoring what children access online **46**
Table 4.9: Issues encountered **47**
Table 4.10: Importance of monitoring dashboard **48**
Table 4.11: Preferred dashboard features **49**
Table 4.12: Easiness of parent-friendly interface **50**
Table 4.13: Willingness to use the dashboard **51**
Table 4.14: Evaluation **57**

List of figures

Figure 4. 1: Age group of respondents **40**
Figure 4.2: Gender of respondents **41**
Figure 4.3: Role in household **42**
Figure 4.4: Type of internet connection used **43**
Figure 4.5: Number of devices connected **44**
Figure 4.6: Are you confident in managing home network **45**
Figure 4.7: What children access online **46**
Figure 4.8: Issues encountered **47**
Figure 4.9: Importance of a monitoring dashboard **48**
Figure 4.10: Preferred dashboard features **49**
Figure 4.11: Easiness of parent- friendly interface **50**
Figure 4.12: Willingness to use the dashboard **51**

Figure C1: Use Case Diagram **78**
Figure C2: Use Case Diagram **79**
Figure C3: Data Flow Diagram (DFD) **80**
Figure C4: Dashboard Interface Mockup **81**

D1: Main Flask Application (app.py) **82**
D2: Login Page (login.html) **84**
D3: Dashboard Interface (dashboard.html) **85**

E1: Login Page Screenshot **89**
E2: Dashboard Screenshot **90**
E3: Device Activity Monitoring Screen **91**
E4: Alert Notification Example **92**

CHAPTER 1

INTRODUCTION

1.0 Introduction

Digital technology now shapes how we live, work, and talk to each other. Homes have turned into small digital ecosystems — phones, tablets, smart TVs, laptops, game consoles, and IoT gadgets all sharing the same network (Cisco, 2023). With that comes a new problem: keeping an eye on home internet use matters more than it used to, especially when it comes to children safety online (Akhtar & Rehman, 2022).

But here is the catch. Most parents are not tech-savvy. They struggle to read network stats, figure out which devices are connected, or tell if something risky is happening and maintaining online safety. Most monitoring tools that do exist were built for IT professionals, not everyday users, and they are usually too complex to be useful at home (Norman, 2013).

This chapter sets the stage. It covers the background, the specific problem, what the research aims to do, and why this system matters. Think of it as the foundation before we get into the literature, methodology, and system design.

1.1 Background to the Study

Network monitoring is not new. Companies have used SNMP-based tools for years to track routers, switches, and servers. As networks got bigger, tools like intrusion detection systems (IDS) and performance analyzers showed up. But they stayed focused on enterprise use, with very little adapted for homes (Patel et al., 2022).

At home, most people just use whatever basic interface their Internet Service Provider (ISP) or router provides. You might see IP addresses or signal strength, but not much about actual usage or behavior. That is a problem when the average household now has 10–20 internet-connected devices (Statista, 2024). Streaming, online classes, and gaming all add pressure, and parents need better ways to understand what is happening on their network.

There is also the digital parenting side. The Internet Watch Foundation (IWF, 2023) reports that many kids under 16 spend over six hours online daily. That exposes them to risks like explicit content and cyberbullying. Parents want to supervise without invading privacy or needing a networking degree or requiring deep technical literacy. Studies show that visual dashboards and summarized data help non-technical users far more than raw logs (Singh & Sharma, 2021.

Smart homes make this messier. IoT devices are always talking to the network, often without the owner realizing it (Rahman & Islam, 2020). If one gets hacked, it can become an entry point for malware or Distributed-Denial-of-Service (DDoS) attacks (Zhou et al., 2022). So, parents and guardians need to watch not just usage, but also weird connections and abnormal traffic spikes.

Recent advances in lightweight data visualization frameworks, such as Streamlit, Grafana, and Power BI, has made it easier to present network data in a simple and understandable manner. Chen and Huang (2022) showed that non-technical users understand network activity better when it is presented visually rather than as raw data.

In many developing countries, including Zimbabwe, home Internet took off fast because of online education, remote work, and social media use (ITU, 2023). Awareness of network management remains low. This creates an opportunity for educational and preventive tools to enhance digital literacy while promoting responsible Internet use.

So, this study focuses on building a home network monitoring system that's simple, clear, and made for parents.

1.2 Statement of the Problem

Smart devices have turned homes into tangled networks — computers, phones, IoT sensors, smart appliances — all connected. That's convenient, but it also creates headaches. Most households don't have the skills to spot weird network activity, bandwidth hogs, or cyber threats, especially when kids are involved (Kumar & Patel, 2023; Miller et al., 2021).

Existing tools, such as Wireshark or Nagios, are primarily designed for IT professionals and network administrators, not for everyday home users (Johnson & Singh, 2022). Consequently, parents do not notice network anomalies, unsafe browsing behavior, or bandwidth misuse until service disruptions occur or cyber incidents are discovered. And the more devices connect, the need for user-friendly network management becomes urgent (Zhou & Leung, 2020).

In many developing countries, including Zimbabwe, home internet is growing fast but has not been matched with easy-to-use monitoring tools (Chikomo et al., 2024). This makes it difficult for parents to manage network usage and ensure their children's online safety which leads to security vulnerabilities, poor user experiences, and exposure to harmful online content for minors.

Bottom line: we need a home network monitoring system with a parent-friendly dashboard. Something visual, something that flags suspicious behavior, something that lets parents manage devices without a tech manual. Such a system would help guardians to make informed decisions about network usage and would improve security and digital well-being at home.

1.3 Research Objectives

This study aims to design and develop a **Home Network Monitoring System with a Parent-Friendly Dashboard** that supports real-time monitoring and visualization of network activities within a household.

1.3.1 Main Objective

To develop and implement a simple home network monitoring system that allows parents or guardians to monitor, control and visualize network traffic in real time through an easily accessible dashboard.

1.3.2 Specific Objectives

The study aims to:

i. identify challenges faced by non-technical users, particularly parents, in managing home network activities.

ii. design a system architecture that captures and analyzes home network traffic in real time using open-source tools and Python-based technologies.

iii. develop a web-based dashboard that presents simplified visualizations of network statistics, device activities, and alerts in a user-friendly format during system operation.

iv. conduct iterative testing and refinement of the system throughout the development process to ensure usability, accuracy, and reliability.

v. implement and evaluate an integrated home network monitoring prototype.

1.4 Research Questions

This study seeks to answer the following key research questions that align with the research objectives:

i. what challenges do parents face in monitoring and managing home network traffic?

ii. how can a system be designed to provide simplified, real-time insights suitable for non-technical users?

iii. what technologies can be used to capture and visualize network data?

iv. how effective is the dashboard in enhancing parental understanding and control of home network usage?

v. to what extent does the system improve security awareness and digital safety within the household?

1.5 Research Propositions

For qualitative interpretation, the following propositions guided the study:

i. a user-friendly interface enhances parental engagement
ii. real-time visualization improves parental awareness of household network activity
iii. simplified alerts and summaries help reduce technical complexity
iv. the use of open-source technologies provides a cost-effective and flexible framework

1.6 Justification / Significance of the Study

The emergence of smart homes and Internet connectivity has created an urgent need for secure, reliable, and manageable home networks. Even though the society has embraced the use of broadband access and IoT device adoption, the monitoring and control of network usage is still a challenge for the majority of households, especially in developing regions (Chikomo et al., 2024).

This study is significant because it addresses this gap by proposing a Home Network Monitoring System with a Parent-Friendly Dashboard that can be used by non-technical users. The proposed system utilizes lightweight web technologies such as Flask, SQLite, and Python-based monitoring tools to provide an affordable and accessible solution for home network management. In doing so, it supports safer digital environments for families, promotes digital literacy, and contributes to broader efforts to enhance cybersecurity and responsible Internet use in the home.

1.6.1 Academic Significance

Academically, the research contributes to the growing body of knowledge in network engineering, cybersecurity, and human-computer interaction (HCI). Most existing studies mainly focus on complex enterprise-level network monitoring, while few have looked at home-based, user-centric **systems** that balance simplicity and functionality (Kumar & Patel, 2023). The study can also be

useful for future research that aims at developing low-cost and user-friendly network monitoring solutions using open-source tools like Python and Wireshark.

1.6.2 Practical Significance

The system offers added value to parents and guardians by presenting network data on an intuitive, easy-to-understand dashboard. The design makes it easy to find connected devices, monitor bandwidth use, and receive alerts about suspicious or excessive activity. This adds a layer of digital parenting support, enabling adults to protect minors from inappropriate online exposure and potential cyber threats (Johnson & Singh, 2022).

This study complements the current digital inclusion goals, promoting technological empowerment among non-technical populations. It also, has the potential to reduce the digital divide by offering a cost-effective, open-source-based solution suitable for low-resource households in regions like Zimbabwe and other parts of Africa (Zhou & Leung, 2020).

1.6.3 Institutional and Societal Relevance

At an institutional level, the findings can guide educational and governmental entities about creating awareness programs on home network security and child-safe Internet usage. For instance, integrate simplified visual dashboards as tools for digital literacy training.

Societally, the system contributes to cyber hygiene practices, reinforcing responsible Internet usage and safe data handling within domestic environments (Nguyen et al., 2023). This study shows how user-friendly network engineering solutions can turn complex security and monitoring processes into accessible, everyday tools, narrowing the gap between professional IT systems and household digital needs.

1.7 Assumptions

This study is guided by a number of assumptions that frame the scope, design, and expected outcomes of the project. These assumptions ensure that the project remains feasible within the available time and resources.

The study assumes that households participating in the research have basic internet connectivity through Wi-Fi routers or equivalent devices, providing the network environment required for data capture and monitoring (Ali & Wang, 2022). It is further assumed that open-source tools such as Python, Wireshark, and packet-sniffing libraries are accessible and can be integrated into the prototype without significant licensing restrictions. Additionally, parents and guardians who participated in testing are assumed to have engaged honestly and cooperatively, providing feedback that accurately reflects their experiences with the system.

It is also assumed that devices connected to the monitored network behave in a broadly predictable manner, meaning that unusual traffic patterns can be meaningfully detected and flagged as anomalies. Related to this, target users are assumed to possess a minimum level of digital literacy sufficient to navigate a graphical interface and interpret basic visual indicators, such as status colors and bandwidth charts, without requiring technical training. Reasonably stable electricity and internet connectivity in the test environment are likewise assumed, given that the monitoring system depends on continuous network access to function reliably (Chikomo et al., 2024).

Finally, the study assumes that the system will be deployed and used ethically, solely for legitimate domestic monitoring purposes. Users are expected to respect the privacy of household members and to obtain appropriate consent before monitoring devices, in accordance with applicable data protection principles and the Cyber and Data Protection Act (2021) of Zimbabwe (Miller et al., 2021). These assumptions collectively define the conditions under which the study findings are valid and should be interpreted.

1.8 Limitations / Challenges

Every research study faces practical and contextual constraints that may affect the design, implementation, and evaluation processes of the study. The following limitations are acknowledged.

1.8.1 Technical Constraints

Developing a network monitoring system requires access to realistic network traffic data and simulation tools. Privacy and security considerations, however, restrict the collection of real-time home traffic data (Nguyen et al., 2023). To mitigate this, the study used open datasets and controlled test environments. Because the project is developed using open-source tools such as Python and Flask, the functionality may be limited compared to a commercial.

A second technical limitation is the hardware diversity found in home networks. Different routers and devices use different communication protocols, which may not be compatible with the monitoring prototype. This may restrict the system's ability to capture traffic or manage devices (Johnson & Singh, 2022). To mitigate this, the study used open datasets and controlled test environments. Phone hotspots often enable client isolation, which prevents device-to-device discovery. The system addresses this through an adaptive three-layer scanning strategy and manual device addition, ensuring functionality across router, MiFi, and hotspot network types.

1.8.2 Time Constraints

The project is being conducted within a limited academic time frame. As a result, the system focuses on core features (real-time traffic visualization, device detection, and alert notifications) rather than extensive functionalities such as deep packet inspection or AI-driven threat prediction.

1.8.3 Resource and Infrastructure Limitations

Limited access to high-performance computing hardware or multiple simultaneous network users affects the testing scale. Internet stability in certain regions of Zimbabwe, makes continuous monitoring and data collection harder (Chikomo et al., 2024). Load shedding is a further obstacle to network monitoring in Zimbabwe.

1.8.4 User-Related Limitations

Because the system targets non-technical users, challenges are likely to arise in user training and interface interpretation. Even a simplified dashboard might be hard to understand for participants unfamiliar with network terminology (Zhou & Leung, 2020). To address this, the system design emphasizes visual representation rather than technical network metrics.

1.8.5 Ethical and Privacy Challenges

Monitoring network activity raises privacy and ethical issues. Although the system does not record personal browsing histories, but it can still reveal device activity patterns. Strict ethical guidelines and consent procedures were followed to ensure compliance with the data protection principles (Ali & Wang, 2022).

Despite these challenges, the study remains feasible and valuable, offering a prototype that balances functionality, usability, and ethical considerations.

1.9 Scope / Delimitation of the Research

This section defines the boundaries of the research to ensure it remains focused and achievable within the available resources and timeframe.

1.9.1 Geographical Scope

The study does not focus on a broad geographical region. It is limited to a simulated home network environment representing a typical household setup. The prototype is developed and tested in a controlled environment, such as a laboratory or home-based setting, using virtual or small-scale network configurations. The system conceptually applies to households anywhere in Zimbabwe or beyond, its development and evaluation were restricted to a local, small-scale setting for demonstration purposes. This ensures feasibility within the project's time and resource limitations (Kumar & Patel, 2023).

1.9.2 Technical Scope

The project covers the design, development, and evaluation of a home network monitoring prototype using open-source technologies. Key functions include:

- real-time device detection and traffic visualization;
- network usage summaries per device;
- alert notifications for unusual network activities;
- a simple web-based interface tailored for parents.

The system does not implement advanced AI analytics, deep packet inspection, or cloud-based remote control features due to time and resource limitations. The emphasis will be on usability and real-time monitoring accuracy (Nguyen et al., 2023).

1.9.3 User Scope

The target users are parents and guardians with basic digital literacy who wish to understand and manage home network activities. The system will not target enterprise or corporate users, since such networks require more robust and scalable monitoring solutions (Johnson & Singh, 2022).

1.9.4 Research Delimitation

The study is limited to local testing environments, such as simulated home networks or small-scale Wi-Fi setups, using tools like Wireshark and Python's network libraries. The evaluation relies on qualitative user feedback rather than large-scale quantitative data analysis, since the aim is to assess usability and awareness rather than system performance metrics alone (Kumar & Patel, 2023). It also does not explore legal or regulatory issues for network surveillance in depth, as its focus is technical and educational rather than policy-driven. These delimitations ensure that the project remains realistic, targeted, and implementable within the academic timeframe while still addressing a meaningful and relevant technological challenge.

1.10 Definition of Terms

For clarity and to ensure a common understanding of key concepts used in this study, the following terms are defined:

Network monitoring refers to the process of continuously observing, measuring, and analyzing data traffic within a computer network to assess performance, detect issues, and ensure efficient operation (Patel et al., 2022). In this study, it refers specifically to monitoring a home network's connected devices and bandwidth usage.

Dashboard is a visual interface that displays critical information in an easy-to-understand format. In the context of this study, the dashboard will present device status, bandwidth consumption, and alerts in a parent-friendly, graphical format (Norman, 2013).

Bandwidth is the maximum rate of data transfer over a network connection within a given period, usually measured in megabits per second (Mbps). The system tracks how much bandwidth each connected device consumes (Cisco, 2023).

Home network refers to a local area network (LAN) that connects devices such as computers, smartphones, tablets, and IoT devices within a household to each other and to the internet.

Parent-friendly describes a design approach that is easily understood and used by parents or guardians who may not possess technical expertise. The interface prioritizes simplicity, clarity, and actionable information (Singh & Sharma, 2021).

Prototype is an initial working version of a system built to demonstrate feasibility, gather feedback, and guide further development. In this study, the prototype refers to the initial dashboard and network monitoring system.

IoT (Internet of Things) device is an Internet connected device that collects, sends, or receives data. Examples include smart thermostats, cameras, and wearable devices (Rahman & Islam, 2020).

Real-time monitoring is the continuous tracking of network activities as they occur, allowing immediate observation of traffic patterns and device activity.

Digital literacy is the ability to access, understand, and use digital technologies effectively. The dashboard aims to enhance parental digital literacy in network monitoring (Chikomo et al., 2024).

Alert notification is a system-generated message indicating unusual or important events in network activity, such as a device exceeding normal bandwidth usage or connecting at unusual times.

Simple Network Management Protocol (SNMP) is a communication protocol used to monitor, manage, and control devices on a network, such as routers, switches, and servers. SNMP allows administrators to collect performance data and receive notifications when device thresholds are exceeded. While it is widely used in enterprise environments, its complexity makes it unsuitable for direct use by the non-technical home users targeted in this study.

1.11 Summary

Background and Problem Context

The chapter emphasized the study on the "Home Network Monitoring System with a Parent-Friendly Dashboard." It outlined how modern homes have evolved into miniature digital ecosystems with multiple connected devices, making it difficult for non-technical users to monitor network activity.

Scope, Objectives and Foundation

It presented the background of the problem, the research objectives, questions and significance of the study. It highlighted the need for a user-friendly system that allows parents to easily understand and control internet usage at home. Also, it discussed the study's scope, assumptions, and limitations, setting a foundation for the development of the proposed monitoring system.

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

Homes today are packed with tech. The proliferation of digital devices and home networks has transformed modern households into complex technological environments. Smartphones, laptops, tablets, smart TVs, and IoT devices, are all hooked up to Wi-Fi and parents are now expected to efficiently regulate and monitor network activities. Studies globally show that non-technical users often struggle to comprehend network usage, security vulnerabilities and device behavior (Al-Kuwari et al., 2021; Zhao & Liu, 2022). In Zimbabwe, households face additional challenges due to intermittent Internet connectivity, limited access to advanced networking equipment, and uneven levels of digital literacy (Moyo & Chikonde, 2024). All of these makes the case for a parent-friendly, locally tailored home network monitoring system that improves digital safety and provides insightful information while being simple to use.

This chapter reviews existing literature. It draws on conceptual, theoretical, and empirical sources to situate the study within existing knowledge and to justify the design choices made in developing the proposed system. The review covers global and local trends in network monitoring, parental digital involvement, and cybersecurity concerns. Particular attention is given to the Zimbabwean context, where digital inclusion and internet safety remain key developmental issues. The chapter concludes by identifying gaps in the current research that this system is trying to fill.

2.1 Conceptual Framework

The conceptual framework provides a structural understanding of the key variables and concepts guiding this study: home network monitoring, parental engagement, usability, real-time visualization and security/privacy.

2.1.1 Home Network Monitoring

Home network monitoring means watching, tracking, and analyzing what's happening on a household's network to keep it secure, fast, and accountable (Schwagele, 2010). It uses tools that detect connected devices, bandwidth usage, and data flow, allowing users to identify suspicious activities.

Home monitoring systems can be classified as passive and active. Passive monitoring observes network traffic without interfering with it, while active monitoring sends test data to measure performance (Zhao & Liu, 2022). For home environments, passive monitoring is usually better because it does not disrupt user experience or slow things down.

In developing countries like Zimbabwe, the adoption of such systems still remains uncommon mainly because of limited awareness and access to affordable technologies (Internet Society, 2022). Most available monitoring tools were made for corporate IT teams and assume a level of technical knowledge that typical Zimbabwean parents do not possess. This reality reinforces the need for simplified, low-cost monitoring solutions designed from the ground up for everyday household users rather than adapted from enterprise-grade platforms.

2.1.2 Parental Engagement in Digital Safety

Parental engagement is just parents actively managing what their kids do online (See et al., 2020). That means checking activity, setting limits, and teaching kids how to use the internet responsibly.

Research shows that many parents in Zimbabwe are concerned about children's exposure to online risks such as explicit content, cyberbullying, and social-media addiction, but they do not have the technical tools and knowledge to intervene effectively Sandada et al. (2025a). Supervision is often informal and based on trust, not technical control.

This points to a clear need for systems that support parents by providing simple monitoring tools without requiring advanced technical knowledge. The lack of accessible tools means that most parental control in Zimbabwe remains reactive and informal rather than proactive and technology-

supported. A good monitoring system should give parents clear, actionable information they can understand and use before problems happen. It's not enough to collect data. The system has to translate it into clear, actionable plain guidance

2.1.3 Usability and User-Friendly Design

Usability is how easy a system is easy to learn, efficient to use, and satisfying for its intended users (Dix et al., 2004). For a home network tool aimed at parents, many of whom may have limited ICT literacy—usability is critical.

Clear visual dashboards, intuitive menus, and minimal technical jargon improve adoption rates and reduce user frustration. Studies back this up: if it's easy, people stick with it. If it's frustrating, they quit (Norman, 2013).

In this study, usability plays a crucial role in ensuring that parents can interact with the system without confusion or frustration. The dashboard was therefore designed to minimize the number of steps required to complete common tasks, use color-coded visual indicators rather than technical text, and provide contextual guidance where needed. This approach is grounded in Norman's (2013) design principles, which emphasise that well-designed systems should make the correct course of action obvious to the user without requiring prior training or external documentation.

2.1.4 Real-Time Visualization

Visualization converts raw network data into visual formats such as graphs, charts, or alerts that users can quickly interpret (Schufrin et al., 2022). Real-time visualization means parents identify anomalies or unauthorized access immediately as they happen. For instance, sudden spikes in data usage or unknown devices connecting to the network can be detected earlier through visual dashboards.

Visual analytics tools like pie charts and bandwidth graphs helps in presenting network statistics in a simplified and interactive format. This approach is particularly useful for non-technical users,

as it simplifies complex data into understandable information and fosters awareness and proactive response to potential security threats.

Recent developments in lightweight web frameworks such as Flask and visualization libraries such as Chart.js have enabled the creation of interactive monitoring dashboards for non-technical users. These technologies allow network information to be displayed in real time through charts, alerts, and graphical interfaces accessible via standard web browsers. According to Chen and Huang (2022), web-based dashboards improve accessibility and user engagement by simplifying complex network information into understandable visual representations.

2.1.5 Security and Privacy

Security and privacy can't be add-ons for a home monitoring system. They have to be built in from day one. Parents need to trust that the system protects their family's info, not exposes it. That means being careful about what data gets collected, where it's stored, and who can see it. Kids and other household members expect some privacy at home.

Ali et al. (2020) found that several commercial parental control applications compromise user privacies through excessive data collection and insecure communication channels. Authentication mechanisms such as login systems and password management are also important components of secure monitoring platforms, ensuring that only authorized users can access sensitive network information.

In Zimbabwe, this concern aligns with the Cyber and Data Protection Act (2021), sets rules for handling personal data. Given that cybersecurity awareness remains low in Zimbabwe and household networks are often shared among multiple users, maintaining secure authentication and encrypted data handling is crucial for protecting user information. This system sticks to device-level traffic only — no browsing history, no personal content, and locks the dashboard behind a password.

2.2 Theoretical Framework

2.2.1 Human–Computer Interaction (HCI)

HCI gives rules for designing user-friendly interfaces. Key concepts include visibility, feedback, consistency and simplicity, which collectively improve usability and reduce errors (Dix et al., 2020). Applying HCI principles to parental dashboards allows parents to interpret device activity, bandwidth usage, and alerts without technical training. In Zimbabwe, where there is limited technical literacy, simplified visualizations and feedback mechanisms are crucial (Moyo & Chikonde, 2024).

Practically, HCI shaped the alert system — parents get notified the second a new device connects or bandwidth goes over a limit. Consistency shows up in the design: same colors, same icons, same layout on every screen. That lowers the mental effort for new users. The point is, a system built on HCI is more likely to get used than one that's technically clever but confusing.

2.2.2 Technology Acceptance Model (TAM)

TAM holds that technology adoption is influenced by perceived ease of use and perceived usefulness (Davis, 1989). Parents in Zimbabwe are more likely to adopt a monitoring system if it is simple and solves a real problem. Past research shows that complicated systems, even if technically robust, are often ignored by non-technical users (Singh & Tan, 2022).

TAM guided several interface decisions of this study. Perceived ease of use influenced the decision to use a single-screen dashboard with large, clearly labelled buttons rather than a multi-menu system that would require navigation training. Perceived usefulness was addressed by ensuring that every feature displayed on the dashboard — device lists, bandwidth charts, and alert logs — maps directly to a concern that the target user research identified as important to parents, namely knowing which devices are connected, how much data they are consuming, and whether anything unusual is happening on the network.

2.2.3 Systems Theory

Systems theory (von Bertalanffy, 1968) views a network as a group of interconnected components that work collectively to achieve a shared goal. Applying this to home network monitoring implies that routers, IoT devices, parental interfaces, and data visualization tools should operate as an interconnected system for effective monitoring and control.

From a systems perspective, a failure in any one component can compromise the monitoring capability of the whole. If the router does not expose traffic data, the monitoring module cannot capture device activity; if the data processing layer is inefficient, the dashboard will display stale information; and if the interface is poorly designed, parents will abandon the system regardless of how well the backend performs. This interconnected view shaped the development approach, which treated backend reliability, data accuracy, and frontend usability as equally weighted requirements rather than addressing them in isolation.

2.2.4 Diffusion of Innovation Theory

Rogers (2003) proposed that adoption of an innovation is influenced by its relative advantage, compatibility, complexity, trialability, and observability. In Zimbabwe, where digital innovation adoption remains uneven, the system was designed with Rogers' five factors in mind. Its relative advantage over informal supervision is clear; it is compatible with commonly available Wi-Fi routers; its simplified interface addresses the complexity barrier; parents can test it on a single device before committing; and the visual dashboard makes its benefits immediately observable to any user who logs in.

2.3 Empirical Evidence

2.3.1 Global Studies

Several studies globally have explored at network monitoring and parental control systems, offering valuable insights into both the technical and usability dimensions of such tools. Most studies show that monitoring technology works, but making it usable for regular people is still a problem. Most solutions were built for experts and aren’t simple or visual enough for home use. For instance, Schufrin et al. (2022) developed a gamified mobile visualization tool that raised cybersecurity awareness among non-technical users through visual interaction. Similarly, Jimenez

(2021) built a Raspberry Pi-based home monitoring system to classify and detect devices on a home network, but it was not user-friendly.

These studies demonstrate technical feasibility but point to a gap in designing tools that fully address usability for parental users. The gamification approach used by Schufrin et al. (2022) is promising but was not tested in a home network management context, while Jimenez's (2021) Raspberry Pi system focused on device classification without considering how parents would interpret or act on the data it produced. Together, these findings point to the need for a system that combines reliable network monitoring capabilities with a deliberately simplified user interface — exactly the design challenge that this study seeks to address.

2.3.2 African and Zimbabwean Context

In Africa, and particularly Zimbabwe, digital challenges include limited internet access, low digital literacy and multiple people share one network. These have a high impact on how home networks are managed and how parental oversight of children's online activity is exercised. Unlike higher-income countries where dedicated parental control tools and broadband infrastructure are more readily available, Zimbabwean households frequently rely on mobile data connections, shared Wi-Fi routers, and informal supervision strategies that provide little technical control over what children can access online.

Sandada et al. (2025b) observed that children are more exposed to online risks, yet parents rely mostly on verbal or informal supervision rather than digital technologies. The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) found that 44 % of children aged 8–18 had accessed adult content online and 13 % had experienced cyberbullying (The Herald, 2024). Furthermore, the Internet Society (2022) reports that only 33 % of Zimbabweans use the Internet regularly, and home networks are often shared among multiple users without proper controls. These findings create an urgent need for accessible, parent-oriented and affordable monitoring systems that can run efficiently on modest devices.

2.3.3 Usability and Adoption

Studies on technology adoption in developing countries consistently indicate that simplicity and local relevance are the most decisive factors in whether a new tool is accepted or ignored by its intended users (See et al., 2020). A system can be powerful, but if it ignores language, literacy, and device limits, it fails. This principle is particularly applicable in Zimbabwe, where wide variation in education levels and internet experience means that a one-size-fits-all approach to interface design will inevitably exclude a significant portion of the intended user base.

In the Zimbabwean context, limited bandwidth, unstable power supply, and cost barriers make lightweight open-source applications a good fit for home use. Open-source technologies have become increasingly popular in educational and low-resource environments because they are free, flexible and allows for scalability. HCI-driven usability testing improves comprehension and adoption, ensuring that systems meet the needs of users with different educational background. Every interface decision made during development was therefore tested against one question: would a parent with no networking background understand what this screen is telling them and know what to do next?

2.3.4 Security and Ethical Considerations

Ali et al. (2020) found that poorly designed monitoring control systems can expose personal data or spy too much, raising ethical concerns. To ensure privacy compliance, modern systems integrate encryption, user authentication, and minimal-data collection principles. For Zimbabwean households, data protection aligns with the Cyber and Data Protection Act (2021.

This study followed three rules. First, collect only what's needed — device IDs, connection times, bandwidth — not URLs or messages. Second, lock the dashboard with hashed passwords via Flask-Bcrypt so only the household admin can see data. Third, get consent. Everyone in the user study was told what data was collected and agreed in writing. That matched the institution's ethics rules.

2.4 Existing Systems and Tools

A number of network monitoring tools are currently in widespread use, and each reflects a particular set of design priorities that reveal why none is well suited to the home parenting context

this study addresses. The table below summarises five common ones and why they are not ideal for non-technical household users.

Table 2.1 Existing Systems and Tools

Tool	**Strength**	**Limitation**
Wireshark	Detailed packet analysis	Too technical steep learning curve, no simple dashboard
Nagios	Enterprise monitoring, alerts, reporting	Complex setup, built for IT admins, overkill for homes
PRTG	Visualization support, good interface	Expensive, heavy on resources, needs config knowledge
Grafana	Excellent dashboards, real-time data	Requires backend setup, not plug-and-play for parents
Proposed System	Parent-Friendly + lightweight	Prototype limitations

Wireshark and Nagios offer powerful diagnostic capabilities but require specialist knowledge that most parents do not have. PRTG and Grafana come closer to providing visual interfaces but carry cost and configuration barriers that make them impractical for low-resource households. The proposed system is specifically designed to fill the gap left by all four: lightweight, visually accessible, and requiring no prior networking knowledge to operate.

2.5 Research Gap Analysis

Although the global literature on network monitoring is extensive, it is heavily skewed towards enterprise applications and expert users (Kumar & Patel, 2023). Most documented systems prioritise technical depth over accessibility. They lack localized features relevant to parental

education, and are rarely integrated with the kind of real-time visual alerts that would allow a non-technical parent to act on network information without external assistance. This gap is particularly pronounced in sub-Saharan Africa, where the combination of growing internet adoption and low digital literacy. Then children are increasingly exposed to online risks that their parents are ill-equipped to monitor or manage.

Local studies from Zimbabwe, like Sandada et al. (2025a) and POTRAZ (2024), confirm that internet-related risks to children are worsening, but they do not offer tech solutions. They document the problem without addressing it. This research therefore occupies a specific and underserved position: it develops a practical, open-source home network monitoring tool tailored to the constraints and priorities of Zimbabwean households, with usability, cost efficiency, real-time visualisation, and data privacy as its guiding design principles. It directly responds to the gap that the reviewed literature identifies but does not fill.

2.6 Network type comparison

Understanding the technical differences between home network types is essential for designing a robust monitoring system. Table 2.2 breaks it down.

Table 2.2 Network Type Comparison

Feature	**Home Router**	**MiFi Device**	**Phone Hotspot**
Client Isolation	Disabled	Disabled	Often enabled
ARP scanning	Works	Works	Blocked
ICMP ping sweep	Works	Works	Usually blocked
Device discovery	Full visibility	Full visibility	No visibility

MiFi devices behave identically to standard home routers, so live discovery. Phone hotspots, by contrast, enforce client isolation as a security measure, which necessitated the development of adaptive scanning methods and manual device addition in the proposed system (Zhao & Liu, 2022; Chikomo et al., 2024).

2.7 Summary

This chapter reviewed the conceptual, theoretical, and empirical foundations relevant to home network monitoring and parental digital engagement. The conceptual framework established the relationships between usability, real-time visualisation, and security. The four theoretical lenses — HCI, TAM, Systems Theory, and Diffusion of Innovation — each contributed specific, actionable design principles that are reflected in the dashboard's interface, architecture, and feature set.

Empirical evidence from global and Zimbabwean sources confirmed two things: the tech to monitor homes exists, but tools for non-technical users do not. The Zimbabwean context, characterized by growing child internet exposure, low parental digital literacy, and limited access to affordable monitoring tools, provided the most direct justification for this study. The research gap identified across all reviewed sources — the absence of a locally relevant, parent-centred, open-source monitoring solution — forms the specific problem that the system developed in Chapter 3 is designed to address.

CHAPTER 3

RESEARCH METHODOLOGY, SYSTEM DESIGN & IMPLEMENTATION

3.0 Introduction

This chapter sets out the methodological processes used in the study. It describes the research design, data collection approaches, population and sampling procedures, research instruments and data analysis techniques employed.

Rather than simply describing what was done, this chapter explains why each methodological decision was made and how it serves the study's specific objectives. The choice of descriptive design, mixed methods, and purposive sampling each reflects the particular challenges of researching home network behaviour among non-technical Zimbabwean households, where data on monitoring practices is scarce and user experiences vary considerably across urban and rural settings.

3.1 Research Design and Data Collection Approaches

This study used a descriptive research design, suitable for examining and documenting the characteristics, behaviours, and perceptions of a population (Creswell, 2014). Descriptive designs work well in studies that seek to understand user experiences and identify existing challenges without manipulating variables. In the Zimbabwean context, the design facilitated the exploration of patterns in home internet usage, parental monitoring practices, cybersecurity concerns and what features are required in a user-friendly monitoring system.

A mixed-methods data collection approach was used, combining both quantitative and qualitative strategies. Quantitative data was collected through structured questionnaires to gather measurable insights on home network usage, monitoring practices, and feature preferences from a larger sample (Saunders, Lewis & Thornhill, 2019).

To deepen the understanding of user experiences, qualitative data was collected through open-ended questions, allowing participants to give detailed explanations of their experiences, concerns, and expectations regarding home network monitoring and child online safety.

Interviews were conducted with a small number of parents and one ICT practitioner to obtain deeper insights into challenges faced in monitoring home networks, usability expectations, and child online safety concerns. This second method enabled the researcher to validate and enrich questionnaire findings through in-depth explanations and real-life practical experiences, thereby strengthening data triangulation.

The combination of both approaches strengthened the validity of the findings through triangulation where findings from one method could be validated and enriched by another (Kothari, 2014).

3.2 Population and Sample

The population for this study consisted of parents, guardians, and household heads in Zimbabwe who actively use home internet services. Zimbabwe has experienced significant growth in home internet adoption, driven by increased digital literacy and expanding mobile broadband access (Chikomo, Moyo & Banda, 2024; POTRAZ, 2024). This population was therefore appropriate for understanding real household experiences related to network monitoring.

The study used purposive sampling, a non-probability sampling technique that enables the selection of participants with specific characteristics relevant to the research (Etikan, Musa & Alkassim, 2016). Participants were selected based on their responsibility for managing or overseeing internet usage within their homes.

A sample size of 30 households from urban, peri-urban and rural areas was determined suitable for an exploratory study aimed at understanding needs, challenges, and system requirements (Cohen, Manion & Morrison, 2018).

In addition, five interview participants (four parents/guardians and one ICT practitioner) were selected from within this group to provide deeper qualitative insights. This sample provided enough variation to identify patterns in household network monitoring practices.

3.3 Research Instruments

Two primary research instruments were used:

3.3.1 Questionnaire

A structured questionnaire was used as the main research instrument. It was administered online via Google forms. Questionnaires are effective tools for collecting standardized data that can be easily analysed and compared across respondents (Bryman, 2016).

The questionnaire included both quantitative and qualitative data across sections covering: demographic information, home network usage, network monitoring behaviour, parental concerns and internet safety, feature requirements for the dashboard, and overall evaluation.

The full questionnaire used for data collection is presented in **Appendix A** for verification and replication purposes.

3.3.2 Interview Guide

A semi-structured interview guide was used to collect qualitative data. Interviews focused on participants' experiences with existing home network tools, challenges in supervising children's internet usage, usability expectations, and desired system features. This method allowed for follow-up questions and clarification of responses, providing deeper insight than closed-ended survey questions.

A sample interview guide is provided in **Appendix B**.

To enhance reliability and validity, the questionnaire was reviewed by two ICT professionals and pre-tested with a small group of five participants, following guidelines by Creswell (2014). Feedback from the pilot study was used to refine unclear questions and improve overall instrument structure.

3.4 Data Analysis Procedure

The study utilized both quantitative and qualitative data analysis techniques.

Quantitative data was analysed using descriptive statistics, including frequencies and percentages, which are effective for summarising large datasets and identifying trends (Saunders et al., 2019). Quantitative data was exported from Google Forms and analysed using Microsoft Excel, where frequencies, percentages, and charts were generated. These statistics helped to highlight common challenges in network monitoring and device usage patterns in Zimbabwean households.

Qualitative data from open-ended questions was analysed using thematic analysis, as outlined by Braun and Clarke (2006). This method involves coding responses, identifying repeating ideas, and grouping them into themes. Thematic analysis enabled the researcher to extract meaningful insights regarding user frustrations, expectations, and suggestions for improving a home network monitoring tool.

The mixed approach ensured that both numerical patterns and detailed user experiences informed the final recommendations and system design requirements.

3.5 Reliability and Validity

Reliability and validity procedures were implemented to ensure data accuracy and consistency.

3.5.1 Reliability

A pilot test was conducted with five participants to identify ambiguities and refine the questionnaire. Pilot testing enhances the reliability of an instrument by improving clarity and ensuring that questions are interpreted consistently (Creswell, 2014). Based on feedback, minor adjustments were made to wording and question order.

3.5.2 Validity

Content validity was ensured by consulting two ICT experts who reviewed the questionnaire for relevance, completeness, and alignment with the study objectives. Their feedback confirmed that the instrument adequately covered key areas of home network usage and monitoring challenges.

The use of mixed methods further strengthened construct validity, as qualitative responses provided additional confirmation of quantitative patterns (Kothari, 2014).

3.6 Data Collection Process

Data collection was conducted through Google Forms, online questionnaires and physical questionnaire distribution. Online questionnaire was distributed through email, WhatsApp, and social media platforms. For physical questionnaire, door-to-door distribution was used where feasible. This approach accommodates households with varying digital access levels, particularly in regions with inconsistent connectivity, as commonly highlighted in Zimbabwean ICT reports (van Stam, 2021; POTRAZ, 2024).

Semi-structured interviews were conducted either face-to-face or via phone calls, depending on participant availability. All respondents participated voluntarily, and responses were recorded in note form for analysis. Completed questionnaires and interview notes were stored securely, with access limited to the researcher only. Respondents were given a two-week period to voluntarily complete the questionnaire.

3.7 Ethical Considerations

Ethical standards were maintained throughout all phases of data collection and system testing. Before any data was collected, participants were given a plain-language explanation of the study's purpose, what their participation would involve, and how their responses would be used. Participation was entirely voluntary and no incentives were offered, ensuring that consent was freely given rather than coerced. All questionnaire responses were collected anonymously, with no names, addresses, or device identifiers recorded, so that no individual response could be traced back to a specific household.

Participants were also informed at the point of recruitment that they could withdraw from the study at any time without needing to provide a reason and without any negative consequence. Interview notes were stored on a password-protected device accessible only to the researcher, and no raw data was shared with third parties. The system itself was tested only within the researcher's own household network and on consented participants' devices, ensuring that no unauthorised monitoring took place at any stage of the project.

3.8 System Design and Implementation

3.8.1 Overview of the System

The Home Network Monitoring System was designed and implemented to provide parents and guardians with a simplified platform for monitoring and managing devices connected to a home network. The central design challenge was building a system that a parent with no networking background could open, understand, and use confidently within minutes of first encounter, without reading a manual or receiving technical support.

The system follows a web-based architecture and is implemented using open-source technologies to ensure affordability, flexibility, and ease of maintenance. The requirements gathered from questionnaire respondents and interview participants, documented in Chapter 4, directly determined which features were prioritized and which were deferred to future development.

3.8.2 System Requirements

System requirements specify what the system must do and how well it should perform in order to meet user needs. Clearly defined requirements provide a foundation for system design, implementation and testing (Pressman and Maxim, 2019).

3.8.2.1 Functional Requirements

The system was designed to meet several functional requirements. It allows parents to log into the system securely using authenticated credentials before accessing the dashboard. The system

displays device details such as device names, IP addresses, connection status, and the last seen time for each connected device. It also monitors bandwidth usage and classifies device activity levels as low, medium, or high depending on network consumption patterns. Alert notifications are generated whenever unusually high bandwidth usage or suspicious activity is detected. In addition, the system enables parents to add, remove, block, and unblock devices connected to the home network. A recent network activity log is maintained to support monitoring and review of previous events. The dashboard further displays all devices currently connected to the network in real time and provides visual usage statistics through charts and graphical analytics. To improve usability, the system supports exporting network activity logs and offers interface customization options such as dark mode alongside real-time date and time display functionality.

Each of these requirements was derived directly from the questionnaire and interview findings presented in Chapter 4, ensuring that the system was built to address observed user needs rather than assumed ones.

3.8.2.2 Non-functional Requirements

On the non-functional side, the system was required to be operable by parents with no networking background, meaning that usability took precedence over feature richness throughout the design process. Secure access through password authentication was mandatory given the sensitive nature of household network data. The system was also expected to reflect network changes with minimal delay, operate continuously without crashing during extended monitoring sessions, and run on the kinds of modest consumer hardware common in Zimbabwean households rather than requiring dedicated server infrastructure.

3.8.2.3 *Security Requirements*

Security was a critical consideration in the design of the Home Network Monitoring System due to the sensitivity of network usage data and parental control functions. The system incorporates several security measures to ensure that only authorised users can access and manage the home network.

Firstly, user authentication is implemented through a login mechanism that requires a valid username and password before access to the dashboard is granted. This ensures that only parents or guardians can monitor connected devices and perform control actions such as blocking or

unblocking devices. Session management is used to maintain secure access throughout the user's interaction with the system and to prevent unauthorised access once a user logs out.

Secondly, access control is enforced by restricting all monitoring and management functions to authenticated users only. Any attempt to access the dashboard without proper authentication redirects the user to the login page. This protects the system from unauthorised users attempting to manipulate network settings.

Thirdly, the system limits exposure of sensitive network information by displaying only essential device details such as device name, IP address, bandwidth usage, and status. This design choice aligns with the project's objective of providing a parent-friendly interface while maintaining data privacy.

Although the current implementation is a prototype, these security measures provide a foundational level of protection suitable for a home environment. Passwords are securely protected using hashing techniques implemented through the Flask-Bcrypt library. Future improvements may include multi-factor authentication and secure HTTPS communication protocols *(Ali and Wang, 2022; Zhou and Leung, 2020)*

3.8.3 System Architecture

The proposed system adopts a client–server architecture in which network data is captured and processed on the backend and presented to users through a web-based dashboard on the frontend. Client–server architecture is widely used in distributed systems because it separates data processing from user interaction, thereby improving scalability, security and maintainability (Tanenbaum and Van Steen, 2017).

3.8.3.1 Architecture Description

The system is composed of four major components that work together to provide network monitoring and management functionality. The Network Monitoring Module is responsible for capturing network traffic and discovering devices connected to the home network through packet inspection and device discovery techniques. The Data Processing Module filters and analyses the captured information in order to extract useful details such as IP addresses, device names,

connection status, and usage patterns. The Data Storage Component stores monitoring logs, device records, alerts, and configuration settings to support historical analysis and reporting functions. Finally, the Dashboard Interface serves as the frontend component through which parents and guardians interact with the system, allowing them to monitor devices, view usage statistics, receive alerts, and manage network activity through a simplified and user-friendly web interface.

3.8.3.2 System Workflow

The system operates through the following sequence. The parent logs into the dashboard using secure authentication credentials. The backend continuously monitors connected devices and network activity. Device information and bandwidth usage are processed and stored. The dashboard updates dynamically to display device status, charts, and alerts. Parents can perform management actions such as blocking, unblocking, adding, or removing devices. All activities are recorded in the activity log database for monitoring and reporting purposes.

A detailed system architecture diagram illustrating component interaction is provided in Appendix C.

3.8.3.3 Database Design

The system uses SQLite as the database management system for storing activity logs and monitoring records. SQLite was selected because it is lightweight, serverless, and suitable for small-scale web applications (Connolly and Begg, 2015).

The database holds four categories of records: device activity entries, login events, alert notifications, and general network monitoring logs. The central table is the Activity Logs table, where each record captures a log ID, the name of the device involved, the action that was performed, and the timestamp at which it occurred. This structure allows the dashboard to retrieve and display recent activity quickly and to export historical records as CSV files when the parent requests a report

3.8.4 System Design Models

3.8.4.1 Use Case Design

Use case modelling is used to describe the functional interactions between users and a system (Sommerville, 2016). The primary user of the proposed system is the parent or guardian responsible for managing household internet usage. The system supports several major interactions, including logging into the dashboard securely, viewing all connected devices,

monitoring network usage and bandwidth consumption, receiving notifications and alerts regarding suspicious activities, blocking or unblocking devices, viewing network activity reports, and logging out of the system after completing monitoring tasks. These interactions collectively enable parents to supervise and manage home network activities effectively through a simplified interface.

3.8.4.2 Data Flow Design

Data Flow Diagrams (DFDs) illustrate how data moves through a system and how it is processed at different stages (Yourdon, 1989). For the proposed system the DFD illustrates the flow of network data from capture to processing and display.

Context Level (Level 0): The user interacts with the dashboard, which communicates with the backend system that collects and processes network data from the home network environment.

At Level 1, the system processes are decomposed into several interconnected activities. The system first captures network traffic from devices connected to the home network. The captured data is then processed and analysed to identify device information, usage patterns, and abnormal activities. Processed information is subsequently stored in the database to support monitoring, historical analysis, and reporting functions. Finally, the analysed data is displayed on the dashboard interface where parents can monitor network activity through charts, alerts, and device summaries. **The DFDs are provided in Appendix C.**

3.8.4.3 Interface Design

The user interface was designed using a minimalist and intuitive layout to accommodate non-technical parents and guardians. Usability principles emphasise simplicity, clarity and ease of navigation in order to reduce user errors and improve user satisfaction (Nielsen, 2012). The dashboard also incorporates graphical visualization components such as pie charts and bandwidth statistics to improve comprehension and simplify network monitoring for non-technical users. The main interface components include:

The dashboard interface was designed using a simple and intuitive layout suitable for non-technical users. The interface includes a device list panel that displays all devices currently connected to the

network together with their status information. A usage statistics section presents bandwidth consumption and network activity through charts and visual summaries to simplify interpretation. The dashboard also contains an alerts panel that notifies users about suspicious activity, unknown device connections, or unusual bandwidth usage. In addition, control options are provided to allow parents to block, unblock, pause, or manage selected devices directly from the dashboard interface. **Sample interface mockups and screenshots are provided in Appendix C.**

3.8.5 System Implementation

This section describes the technologies and tools used to build the proposed system and explains how the major components were implemented following standard web-based system development practices (Pressman and Maxim, 2019).

Table 3.1: Development Tools and Technologies

Technology	**Purpose**
Python	Backend and logic
Flask	Web framework
SQLite	Database storage
HTML/CSS	Interface design
Javascript	Dynamic dashboard
Bootstrap	Responsive UI
Chart.js	Data visualization
Flask-Bcrypt	Password hashing

3.8.5.1 Backend Implementation

The backend component performs device discovery, traffic analysis, and alert generation. It continuously monitors network packets, identifies connected devices, and computes usage metrics. Processed data is stored and made available to the dashboard through application programming interfaces (APIs). Separating device discovery and traffic analysis into distinct backend functions

meant that each component could be tested and refined independently, which proved useful during the iterative development process described in Section 3.8.7.

The backend component performs several important functions required for monitoring and managing network activities. It is responsible for device detection and identification within the home network environment. The backend also performs traffic monitoring and bandwidth usage calculations to determine network activity levels for each connected device. In addition, the system generates alerts whenever suspicious connections, abnormal bandwidth consumption, or unknown devices are detected on the network.

The network scanner employs three progressive discovery methods to ensure compatibility across diverse network environments. First, ARP scanning via Scapy attempts to discover devices by broadcasting address resolution requests across the local subnet, which works reliably on standard home routers and MiFi devices. Second, if ARP scanning returns no results — a common occurrence on phone hotspots due to client isolation — the system falls back to ICMP ping sweeps to identify active devices. Third, when both active methods fail, the system reads the operating system's ARP cache to extract recently communicated devices. This adaptive approach ensures the system functions across router-based, MiFi, and phone hotspot networks, with graceful degradation to manual device addition when network security policies block all discovery methods (Zhao & Liu, 2022). **The full backend source code is provided in Appendix D.**

3.8.5.2 Frontend Implementation

The frontend consists of a web-based dashboard that presents network information in a clear and user-friendly manner. The frontend component consists of a web-based dashboard that enables parents to interact with the monitoring system easily. Through the dashboard, users are able to view connected devices in real time, observe bandwidth usage statistics through charts and visualizations, receive alert notifications, and apply management actions such as blocking or unblocking devices connected to the network.

The frontend was designed in line with the findings from Chapter 4, which emphasised ease of use, simplicity, and clarity.

3.8.5.3 Real-Time Dashboard Features

The dashboard supports near real-time monitoring through dynamic updates implemented using JavaScript and Flask API routes. Features such as bandwidth visualization, alert notifications, and

device activity updates are refreshed automatically without requiring complete page reloads. This improves responsiveness and enhances user experience for non-technical users.

The full frontend source code is provided in Appendix D.

3.8.6 System Output

The system produces four categories of output visible through the dashboard interface. The device list shows each connected device's name, IP address, and current connection status, updated in near real time. Bandwidth consumption is displayed graphically for each device, allowing parents to compare usage across the household at a glance. Alert notifications appear automatically when a new or unrecognized device joins the network. Finally, control actions allow the parent to enable or disable internet access for any individual device directly from the dashboard without accessing the router. Screenshots and output samples illustrating each of these outputs are provided in Appendix C.

3.8.7 System Testing and Validation

Testing was conducted to ensure that the system meets the specified functional and non-functional requirements. System testing verifies that implemented functions behave as expected and that performance and usability objectives are achieved (Pressman and Maxim, 2019).

Table 3:2 Functional Testing

Test Case	Expected Result	Actual Result	Status
Login	User accesses dashboard	Successful	Pass
Add device	Device added to list	Successful	Pass
Block device	Status changes to Blocked	Successful	Pass
Export logs	CSV downloaded	Successful	Pass
Alert detection	Notification displayed	Successful	Pass

3.8.7.1 *Usability Testing*

Five parents with no prior networking experience were asked to complete three tasks using the dashboard without any instruction: locating a specific connected device, identifying which device was using the most bandwidth, and blocking a device from network access. All five completed all three tasks successfully on their first attempt. Verbal feedback collected after the session indicated that the color-coded activity indicators were particularly helpful, with three participants specifically mentioning that they understood immediately what green, amber, and red statuses meant without being told. One participant noted that the alert panel was the first thing they noticed when the dashboard loaded, which confirmed that the layout hierarchy was working as intended.

Results indicated that users were able to understand and operate the system with minimal guidance, confirming that the design objectives were achieved in line with usability evaluation principles (Nielsen, 2012).

3.8.8 System Limitations

Despite its effectiveness, the proposed system has several limitations. The system requires access to the home network monitoring point or router configuration in order to function properly. Advanced intrusion detection and deep packet inspection features commonly found in enterprise-level monitoring solutions were not fully implemented because of time and resource limitations. System performance may also vary depending on hardware specifications and the number of devices connected to the network. Furthermore, some monitoring activities were simulated within controlled environments because of limited access to live household network infrastructures during testing. A further limitation concerns the phone hotspot environment used for development and demonstration. Phone hotspots frequently enable client isolation as a security feature, which prevents connected devices from discovering each other on the network. This affected the live device discovery capability during the demonstration, as described in Section 1.8.1. To mitigate this, the system implements a three-layer adaptive scanning strategy and supports manual device addition. On standard home routers or MiFi devices — where client isolation is disabled —the live discovery feature operates as intended.

Each of these constraints was documented during testing and directly informed the recommendations made in Chapter 5 regarding what a production-ready version of the system would need to address.

3.9 Summary

This chapter covered two distinct but connected dimensions of the project: how the study was conducted and how the system was built. On the methodological side, a descriptive mixed-methods design was chosen because the research questions required both measurable patterns across households and the kind of detailed personal accounts that only interviews can provide. Purposive sampling ensured that every participant had direct experience managing home internet use, making their responses relevant to the system's design requirements.

On the technical side, the chapter documented the progression from requirements gathering through architecture design, implementation, and testing. Each design decision — from the choice of SQLite over heavier database systems to the single-screen dashboard layout — was made in direct response to the constraints and preferences identified in the user data. The testing results confirmed that the system performs as specified and that non-technical users can operate it without assistance. Chapter 4 now presents the data collected from questionnaires and interviews and analyses what participants said about their home network monitoring experiences and dashboard preferences.

CHAPTER 4

DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.0 Introduction

This chapter presents, analyses, and interprets the data collected from 30 Zimbabwean households through structured questionnaires and five semi-structured interviews as part of the study on the Home Network Monitoring System with a Parent-Friendly Dashboard. The data collection process was carried out using Google Forms for online questionnaire distribution and physical door-to-door delivery where internet connectivity was limited. Semi-structured interviews were conducted with four parents or guardians and one ICT professional to supplement and validate the quantitative findings.

Both quantitative and qualitative data analysis methods were applied. Quantitative data was exported from Google Forms to Microsoft Excel, where frequencies, percentages, and charts were generated to identify patterns in home network usage, parental monitoring behaviour, and feature preferences. Qualitative data from open-ended questionnaire responses and interview transcripts was analysed using thematic analysis to extract recurring ideas and deeper insights regarding user challenges and expectations.

The results are organized according to four thematic sections aligned with the study objectives: demographic information, home network usage patterns, child online safety, and dashboard feature requirements. Each section presents data in tabular and graphical format, followed by an interpretation that connects findings to the relevant research questions and objectives. The chapter concludes with a summary of interview findings and an overall evaluation of the data, which informs the system design decisions presented in Chapter 3 and the conclusions drawn in Chapter 5.

4.1 Analysis and Interpretation of Results

4.1.1 Demographic Information

Table 4.0-1: Age group

Age group	Frequency(f)	Percentage (%)
18-24	8	26.7
25-34	7	23.3
35-44	7	23.3
45+	8	26.7
Total	**30**	**100**

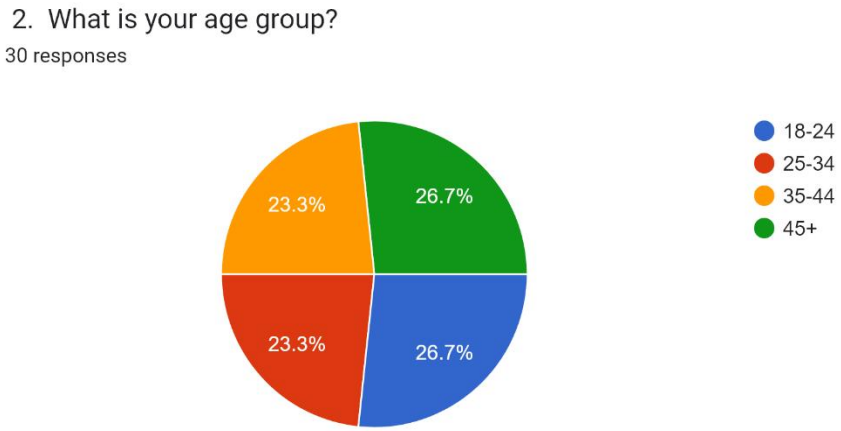


Figure 4. 1: Age group of respondents

Interpretation:

Most respondents fall within the adult age groups, who are likely responsible for managing home internet and supervising children online indicating that the data reflects the views of individuals directly responsible for managing home networks and supervising children's online activities, which strengthens the relevance of the findings to the study objectives. The relevance of parental

involvement in home network management has been widely emphasised in previous studies, which highlight parents as key stakeholders in ensuring online safety for children (See et al., 2020; Sandada et al., 2025b)

Table 4.0-2: Gender

Gender	**Frequency (f)**	**Percentage (%)**
Male	**13**	**43.3**
female	**15**	**50**
Prefer not to say	**2**	**6.7**
total	**30**	**100**

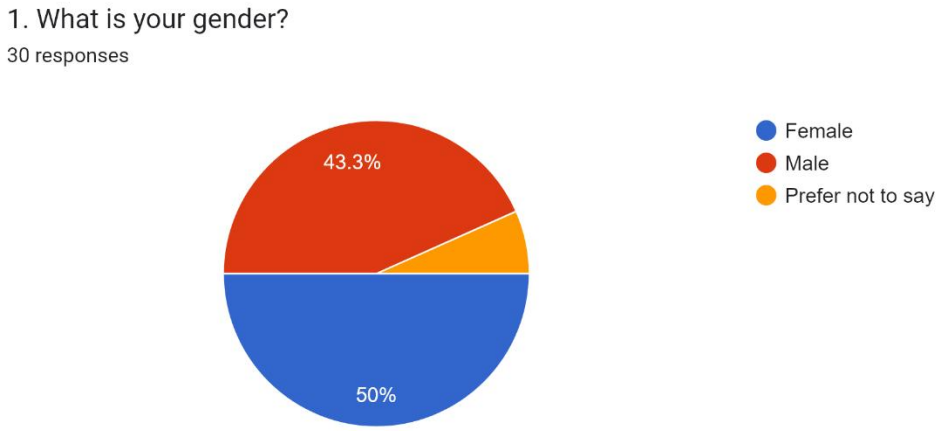


Figure 4.2: Gender of respondents

Interpretation:

The results indicate that 50.0% of the respondents were female, 43.3% were male, and 6.7% preferred not to disclose their gender. This balanced representation suggests that both male and female household heads or guardians are actively involved in managing home internet usage, suggesting the system should be inclusive, easy to use and accessible to all users regardless of gender.

Table 4.3: Area of residence

Area Type	Frequency (f)	Percentage (%)
Urban	**16**	**53.3**
Peri- urban	**9**	**30**
Rural	**5**	**16.7**
Total	**30**	**100**

Interpretation:

Most respondents are from urban and peri-urban areas, indicating that Wi-Fi usage is higher in developed locations. However, the system should remain simple, lightweight and adaptable to rural households with limited connectivity.

Table 4.4: Role in household

Role	Frequency (f)	Percentage (%)
Parent/Guardian	17	56.7
Older sibling	10	33.3
Other	3	10
Total	**30**	**100**

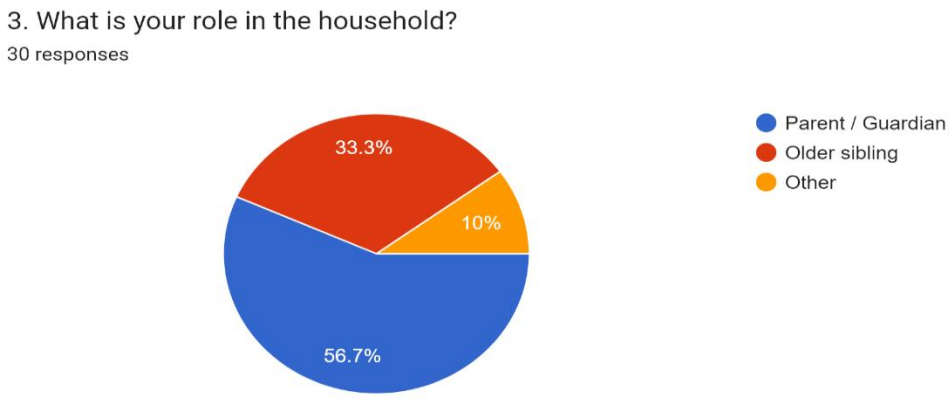


Figure 4.3: Role in household

Interpretation:

The majority of respondents are parents or guardians, highlighting their role in managing household internet and monitoring child activity which justifies the focus on parental monitoring features in the proposed system.

4.1.2 Home Network Usage

Table 4.5: Type of internet connection used

Internet type	Frequency (f)	Percentage (%)
Fibre	5	16.7
LTE	11	36.7
ADSL	1	3.3
Mobile hotspot	7	23.3
Not sure	6	20
Total	**30**	**100**

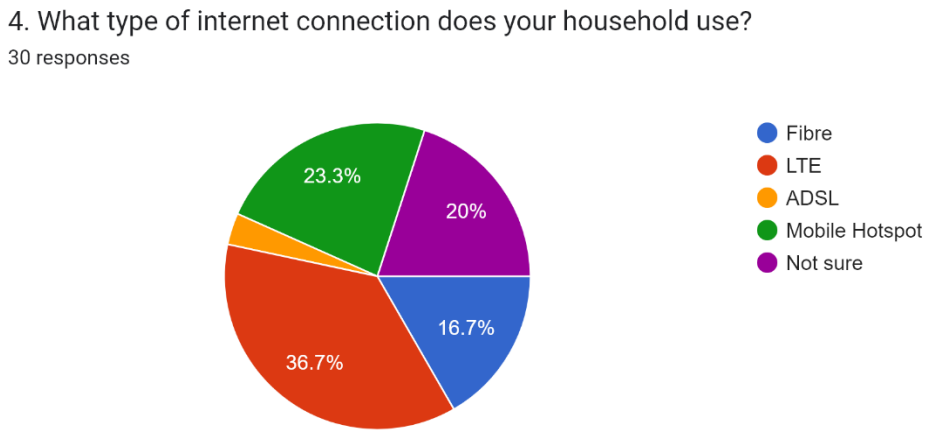


Figure 4.4: Type of internet connection used

Interpretation:

The dominance of LTE connections, used by 36.7% of respondents, indicates that most participating households have sufficient bandwidth to support real-time monitoring. However, the 20% who were unsure of their connection type reinforces the importance of designing the system to be lightweight and functional on modest connection speeds rather than assuming consistently high-bandwidth environments.

Table 4.6: Number of devices connected

Devices	Frequency (f)	Percentage (%)
1-3	4	13.3
4-6	13	43.3
7-10	9	30
More than 10	4	13.3
Total	**30**	**100**

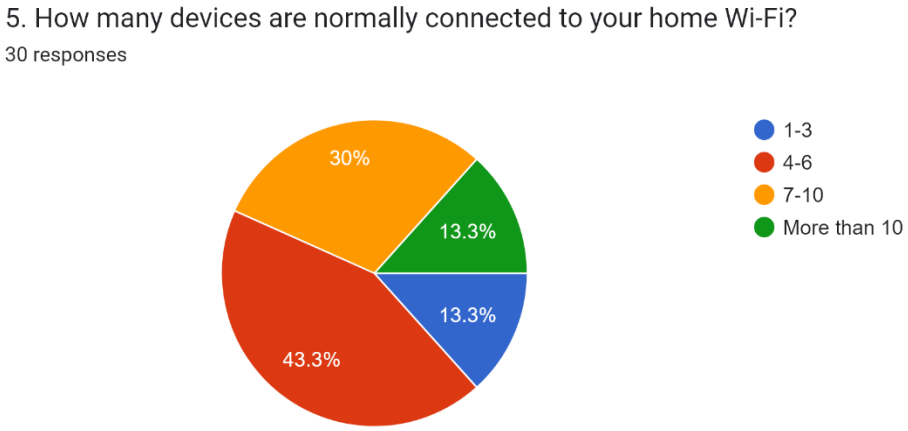


Figure 4.5: Number of devices connected

Interpretation:

Most households connect multiple devices, which may contribute to network congestion and monitoring challenges thereby justifying the need for a centralized dashboard to manage multiple devices effectively.

Table 4.7: How confident are you in managing your home network

Confidence	Frequency (f)	Percentage %
1-Not confident	12	40
2	6	20
3	6	20
4	3	10
5- Very confident	3	10
total	30	100

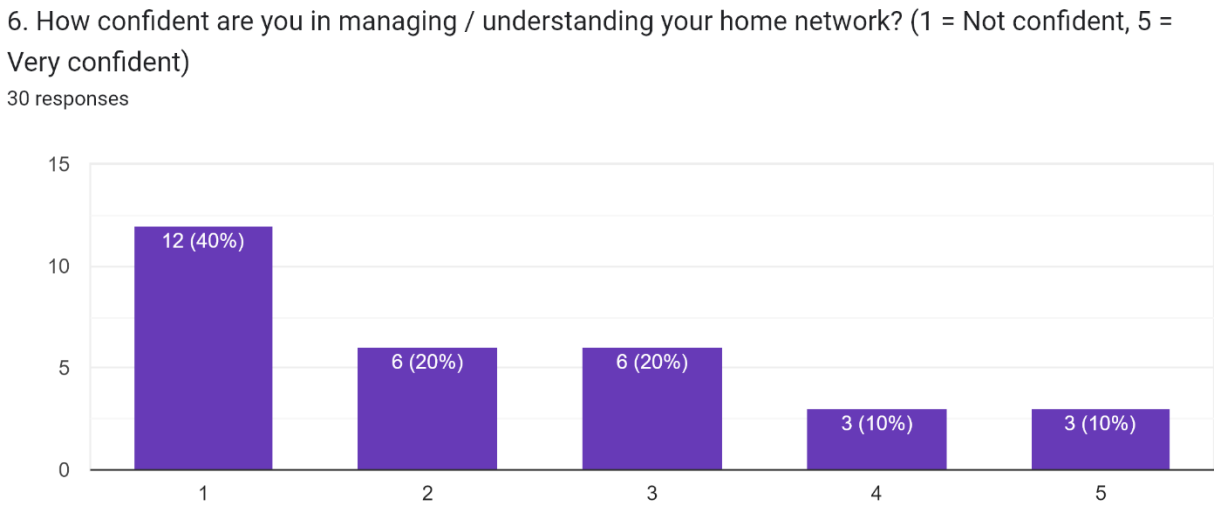


Figure 4.6: Are you confident in managing home network

Interpretation:

The concentration of responses at the lower end of the confidence scale is striking — 40% selected the lowest option and a further 20% selected two out of five, meaning that three in five respondents consider themselves poorly equipped to manage their own home network. This is not simply a preference for simplicity; it indicates that the majority of the target user group would be effectively excluded from any monitoring tool that requires prior networking knowledge. The implication for system design is that the dashboard must function as a complete substitute for technical knowledge rather than a supplement to it.

4.1.3 Child Online Safety

Table 4.8: Monitoring what children access online

Response	Frequency (f)	Percentage %
Yes	**12**	**40**
No	**12**	**40**
Sometimes	**6**	**20**
Total	**30**	**100**

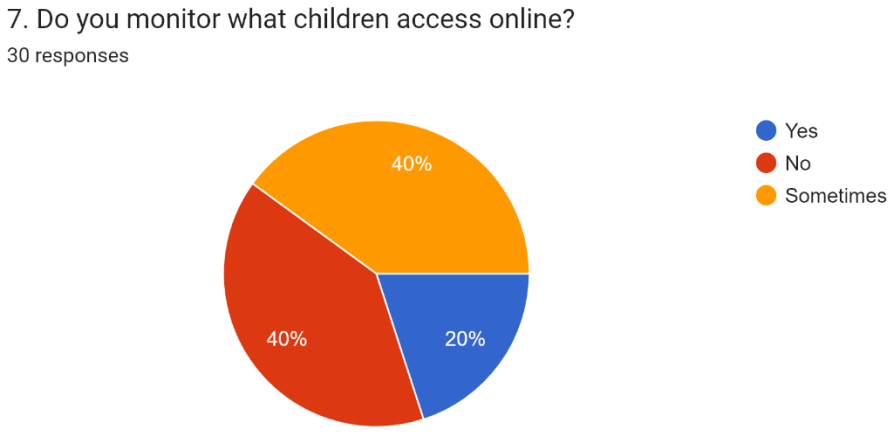


Figure 4.7: What children access online

Interpretation:

The even split between parents who monitor regularly and those who do not — with 40% in each category — is more informative than it first appears. It suggests that the barrier to consistent monitoring is not parental motivation but the absence of tools that make monitoring easy enough to sustain. Parents who responded 'sometimes' may represent those who attempt monitoring when a problem becomes visible but lack the means to do it routinely. A system that runs continuously and notifies parents only when action is needed removes the effort barrier that appears to be preventing consistent oversight.

Table 4.9: Issues encountered

Issue	**Frequency (f)**	**Percentage %**
Excessive screen time	10	33.3
Inappropriate content	14	46.7
Unknown devices joining WI-FI	16	53.3
Slow network due to unknown traffic	11	36.7
Other	3	10

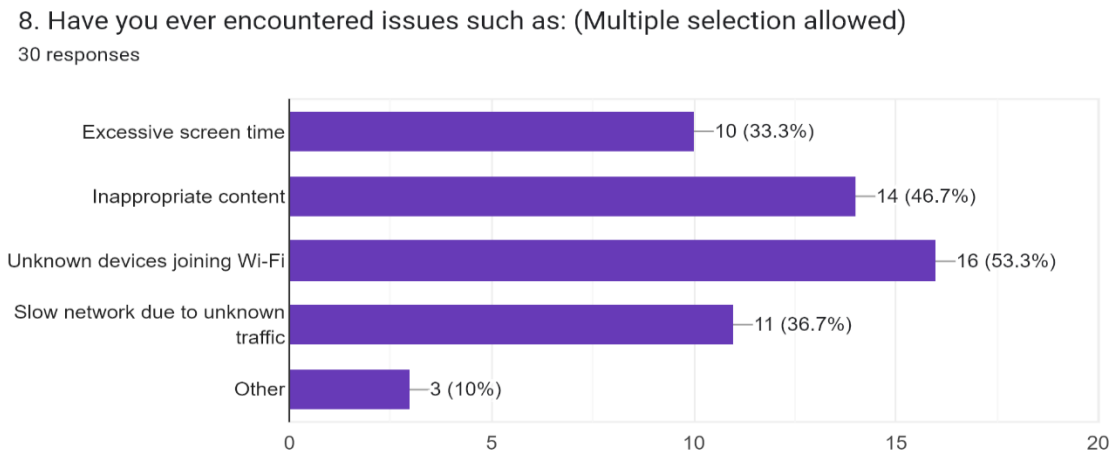


Figure 4.8: Issues encountered

Interpretation:

The most frequently reported issue — unknown devices joining the Wi-Fi, cited by 53.3% of respondents — is significant because it represents a security concern that parents are aware of but cannot currently address. Unlike excessive screen time, which a parent can observe directly, an unknown device connecting silently to the network is invisible without a monitoring tool. The fact that this topped the list of issues ahead of inappropriate content and slow network speeds suggests that security awareness among the target population is higher than digital literacy studies might predict, and that parents are specifically looking for tools that make the invisible visible

Table 4.10: Importance of monitoring dashboard

Importance level	Frequency (f)	Percentage %
1- Not important	1	3.3
2	0	0
3	2	6.7
4	4	13.3
5- very important	23	76.7
Total	30	100

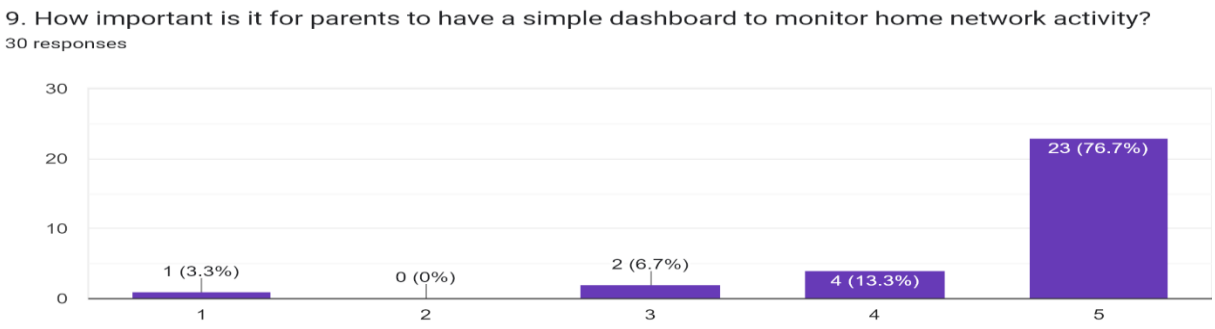


Figure 4.9: Importance of a monitoring dashboard

Interpretation:

Most respondents consider a parent-friendly dashboard important or very important, confirming the need for an accessible system confirming both the relevance and demand for the proposed system.

4.1.4 Dashboard Feature Requirements

Table 4.11: Preferred dashboard features

Feature	Frequency (f)	Percentage %
List of connected devices	**12**	**40**
Alerts of new devices	**16**	**53.3**
Block/pause devices	**18**	**60**
Usage statistics per device	**14**	**46.7**
Alerts for suspicious websites	**16**	**53.3**
Parental mode (child activity report)	**17**	**56.7**

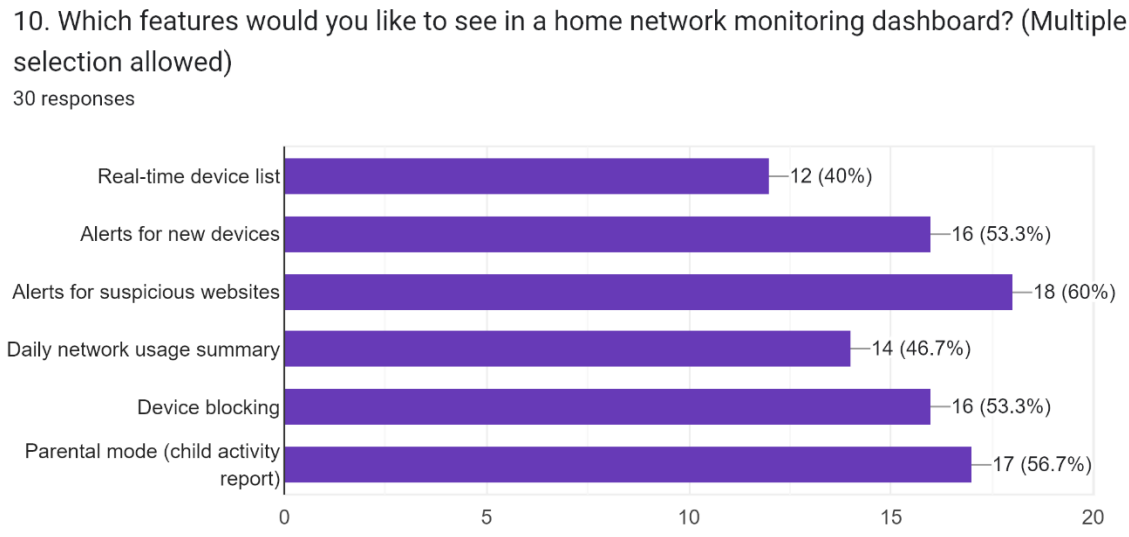


Figure 4.10: Preferred dashboard features

Interpretation:

The results reveal that respondents consider device monitoring and control features, such as blocking and unblocking devices, to be essential. Parents indicated that these features would enable them to regulate children's internet usage and reduce exposure to inappropriate online content. This directly addresses **Objective 3**, which focused on implementing basic parental control mechanisms. This finding is consistent with earlier research that highlights the effectiveness of parental control tools in enhancing child online safety (Ali et al., 2020; Kumar and Patel, 2023).

Table 4.12: Easiness of parent-friendly interface

Scale	Frequency (f)	Percentage (%)
1-Very difficult	1	3.3
2	0	0
3	4	13.3
4	2	6.7
5-Very easy	23	76.7
Total	30	100

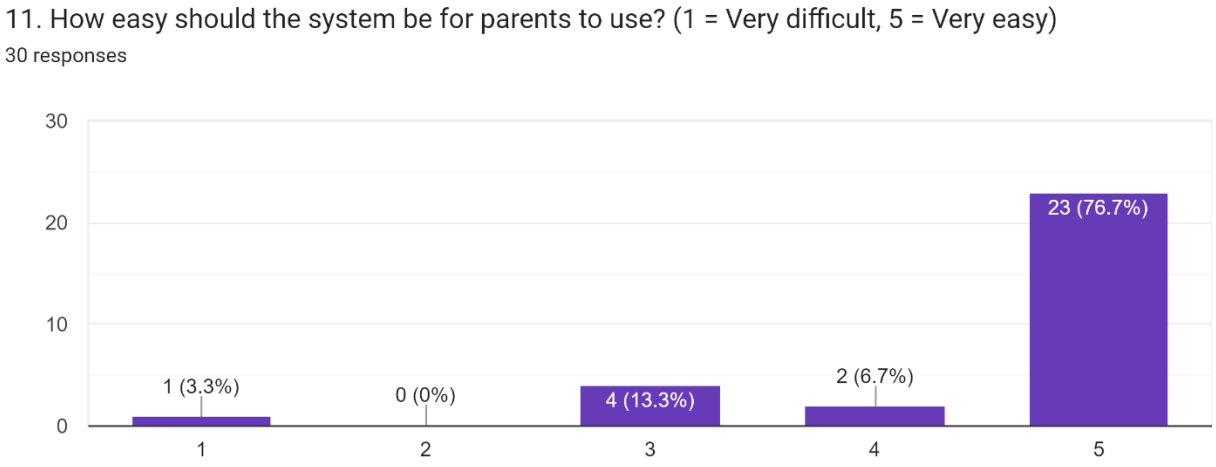


Figure 4.11: Easiness of parent- friendly interface

Interpretation:

The strong skew toward the upper end of the scale — with 76.7% selecting five and no respondent selecting two — suggests that ease of use is not merely preferred but expected by the target user group. This finding is particularly significant given that 60% of the same respondents rated themselves in the lower half of the network management confidence scale, confirming that the users who need the system most are also those who will abandon it fastest if the interface places any unnecessary demand on their technical knowledge.

Table 4.13: Willingness to use the dashboard

Response	Frequency (f)	Percentage %
Yes	**26**	**86.7**
No	**4**	**13.3**
Maybe	**0**	**0**
Total	**30**	**100**

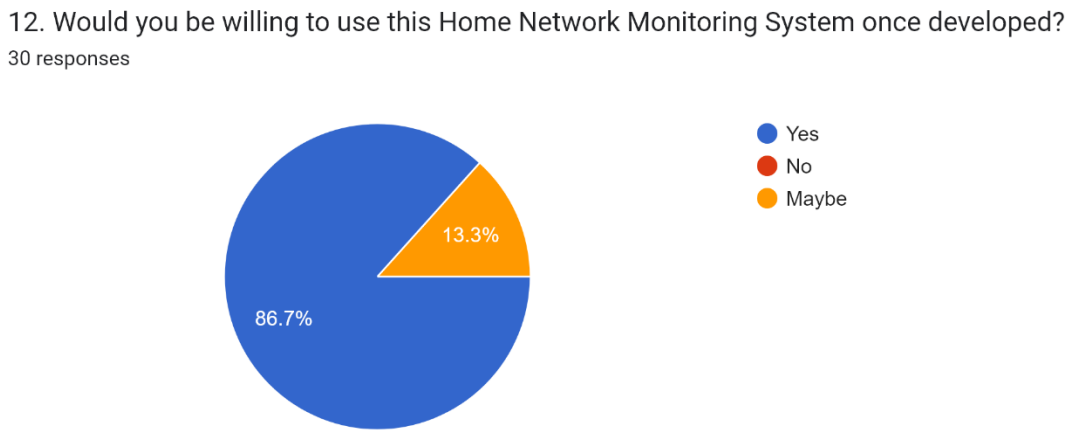


Figure 4.12: Willingness to use the dashboard

Interpretation:

An 86.7% adoption intention rate is notably high for a prototype system that respondents had not yet used, suggesting that the problem the system addresses is felt acutely enough that parents are willing to try a new tool without prior experience of it. The 13.3% who indicated they would not use the system did not provide reasons through the questionnaire, though interview data suggests that privacy concerns about monitoring household members may account for some of this reluctance.

4.2 Overall Evaluation

The overall evaluation draws on both the quantitative questionnaire results and the qualitative data obtained from open-ended questionnaire responses and semi-structured interviews. Taken together, the findings provide a comprehensive picture of the monitoring challenges experienced by Zimbabwean households and the features that parents and guardians consider essential in a home network monitoring system.

The quantitative data revealed strong and consistent demand across all feature categories. Over 86% of respondents confirmed willingness to use the proposed system, while 76.7% rated a parent-friendly monitoring dashboard as very important (Scale 5). These figures indicate not only awareness of the problem but active readiness for a practical solution. The highest-rated feature preference was the ability to block or pause internet access for specific devices (60%), followed by a parental mode with child activity reports (56.7%) and alerts for suspicious websites (53.3%). These preferences directly align with the functional requirements defined in Section 3.8.2 and confirm that the system was designed to address genuine, felt needs rather than hypothetical ones.

The data also highlighted a significant gap in technical confidence among the target user group. Forty percent of respondents rated themselves as not at all confident in managing their home network, with a further 20% selecting a confidence level of two out of five. Collectively, 60% of respondents fell within the lower half of the confidence scale. This strongly reinforces the design decision to prioritise usability and visual clarity over technical depth, as discussed in Sections 3.8.4 and 3.8.5. The finding is consistent with existing literature, which shows that non-technical users are more likely to adopt monitoring tools when interfaces remove technical barriers and present

data through familiar visual formats such as charts and color-coded indicators (Norman, 2013; Singh and Sharma, 2021).

Qualitative feedback from open-ended questionnaire items provided additional nuance to these quantitative patterns. Respondents commonly suggested the inclusion of mobile push notifications so that alerts could be received on smartphones rather than only through the web dashboard. Several participants also requested time-limit scheduling features that would allow parents to automatically cut off internet access at set times — for example, during study hours or after a child's bedtime. Others proposed that the system should flag specific categories of websites rather than only reporting unknown device connections. These suggestions go beyond the current prototype's capabilities and represent a valuable roadmap for future system enhancement, as noted in the recommendations of Chapter 5.

The interview data confirmed and extended these findings. Parents uniformly described existing router interfaces as inaccessible, citing small text, technical terminology, and multi-step navigation as key barriers. The ICT practitioner interviewed reinforced this view, noting that even basic router configuration tasks such as viewing connected devices or changing a Wi-Fi password are frequently mishandled by home users due to interface complexity. This testimony validates the theoretical grounding of the study in Human-Computer Interaction (HCI) principles and the Technology Acceptance Model (TAM), both of which predict that perceived ease of use is a primary determinant of technology adoption (Davis, 1989; Dix et al., 2004).

One concern raised by three respondents related to privacy — specifically, whether the system might expose household members' browsing habits to each other. This reflects a broader ethical tension in home monitoring systems, as noted by Ali et al. (2020), who found that commercially available parental control tools frequently over-collect data. The proposed system was designed to avoid this by displaying only essential device-level metrics — bandwidth usage, connection status, and last-seen timestamps — rather than detailed browsing histories. This design choice was validated by the interview findings, with the ICT practitioner affirming that device-level monitoring strikes an appropriate balance between parental oversight and individual privacy within the household.

Overall, the data analysis confirms that the research objectives were successfully addressed. The challenges faced by non-technical users were clearly identified (Objective 1), the feature requirements for the dashboard were specified based on empirical evidence (Objective 3), and the high level of willingness to adopt the system suggests that the usability principles applied in system design are appropriate for the target population. The findings presented in this chapter provided the empirical foundation that guided the system architecture, interface design, and implementation decisions documented in Chapter 3.

4.3 Interview Findings (Qualitative Results)

Thematic analysis of the five interview transcripts produced three recurring themes: usability barriers with existing tools, specific parental control needs, and security awareness gaps.

On the theme of usability, all five participants described current router interfaces as inaccessible. One parent stated that she had never successfully logged into her router's admin page despite owning the device for three years, while another described giving up trying to identify connected devices after encountering a screen full of IP addresses and MAC addresses, he could not interpret. The ICT practitioner confirmed this pattern, noting that home users regularly contact service providers for help with tasks that the router interface technically supports but presents in a way that assumes prior networking knowledge.

Regarding parental control needs, four of the five participants specifically requested the ability to cut off internet access for individual devices without disconnecting the entire household. Time-based scheduling came up unprompted in three interviews, with parents describing a recurring frustration of children continuing to use devices after agreed bedtimes because manual intervention required either taking the device away or switching off the router entirely, which disrupted other household members.

On security awareness, three participants had experienced unknown devices connecting to their Wi-Fi without knowing how to identify or remove them. None had received any notification from their router when this happened. The ICT practitioner observed that most home routers do support device management but that the notification and alert functionality is disabled by default and

requires several configuration steps to activate — a barrier that the proposed system eliminates entirely.

4.4 System Testing and Evaluation

This section presents the testing and evaluation of the developed Home Network Monitoring System. The aim is to assess the system's performance, usability, and effectiveness in supporting parental understanding and control of home network activity.

4.4.1 Functional Testing

Functional testing was conducted to verify that all core features of the system operate as intended. The main functionalities tested included user authentication, device detection, bandwidth monitoring, device control (block/unblock), and activity logging.

The login system was tested to ensure that only authorised users could access the dashboard. The results confirmed that the system correctly validated credentials and restricted access when incorrect details were entered. The device detection feature was tested by scanning the local network, and active devices were successfully identified and displayed on the dashboard.

Bandwidth monitoring was evaluated using real-time network statistics. The system was able to capture and display current bandwidth usage, allowing users to observe network activity. Device control features were also tested, and the system successfully blocked and unblocked selected devices, with changes reflected immediately on the dashboard. Activity logs were updated accordingly, confirming that system events were recorded correctly.

Overall, functional testing confirmed that the system meets its intended design requirements.

4.4.2 Performance Evaluation

Performance evaluation focused on measuring the responsiveness and efficiency of the system. Three key performance indicators were considered: device detection time, dashboard load time, and system responsiveness.

The average time taken to detect devices on the network was approximately 5 to 10 seconds, depending on the number of connected devices. The dashboard loading time was observed to be less than one second under normal conditions, providing a smooth user experience. Updates to bandwidth usage and device status were reflected in near real-time, ensuring that users receive up-to-date information.

These results indicate that the system performs efficiently within a typical home network environment and is capable of delivering timely feedback to users.

4.4.3 Usability Evaluation

To evaluate usability, a small-scale user test was conducted involving five participants. Each participant was asked to perform a set of tasks using the system, including logging in, identifying the device with the highest bandwidth usage, and blocking a selected device.

Participants were able to complete all tasks successfully with minimal assistance, indicating that the system is easy to use. Following the interaction, participants were asked to rate their confidence in managing their home network on a scale of 1 to 5, both before and after using the system.

The average confidence rating increased from 2.2 before using the system to 4.1 after interaction. This suggests that the system improves user understanding and confidence in managing network activity. Participants also reported that the dashboard was clear and easy to interpret, particularly the visual representation of device activity and bandwidth usage.

Participants appreciated the inclusion of dark mode, indicating that it improved readability and reduced eye strain during extended dashboard use.

4.4.4 Security and Awareness Evaluation

The system includes basic security features such as device monitoring, activity logging, and alerts for high bandwidth usage. During testing, simulated high-usage scenarios triggered alert messages, allowing users to identify unusual activity.

Participants indicated that these alerts helped them become more aware of network behaviour and potential issues. The visibility of connected devices and their activity levels contributed to improved awareness of network security within the household.

Although the system does not implement advanced intrusion detection mechanisms, it provides a practical and accessible way for parents to monitor and respond to potential network concerns.

4.4.5 Summary of Evaluation

Table 0-3.14: Evaluation

Feature Tested	Expected Result	Actual Result	Status
User Login	Only authorised access allowed	Access restricted successfully	Pass
Device Detection	Detected connected devices	Devices detected correctly	Pass
Bandwidth Monitoring	Display real-time usage	Usage updated successfully	Pass
Block/Unblock Device	Restrict or allow device access	Function worked correctly	Pass
Notification Popups	Alert users of events	Alerts displayed correctly	Pass
Search Function	Locate devices quickly	Devices found successfully	Pass

The evaluation results demonstrate that the Home Network Monitoring System is functional, responsive, and user-friendly. The system successfully enables parents to monitor network activity, control connected devices, and gain a better understanding of their home network.

The usability findings indicate that even users with limited technical knowledge can effectively interact with the system. Additionally, the performance results confirm that the system operates efficiently in a real-world home network environment.

Taken together, these results indicate that the system fulfils the core requirements identified in the user research: non-technical parents can operate it independently, it responds to network events in near real time, and its security controls are sufficient for a domestic monitoring context.

4.4.6 Interface Enhancement Evaluation

The enhanced dashboard interface was evaluated to determine whether additional usability features improved user interaction and overall experience. Features evaluated included dark mode support, search functionality, notification popups, pie chart visualizations, and the real-time clock display.

Participants reported that the dark mode interface improved visual comfort during prolonged use, particularly in low-light environments. The search functionality enabled users to quickly identify connected devices, especially in households with many active devices.

Notification popups were positively received because they immediately informed users when new devices connected to the network or when unusual activity was detected. Users also found graphical pie chart representations easier to understand compared to textual bandwidth statistics alone.

The real-time clock displays improved dashboard awareness by helping users associate activity logs and alerts with actual monitoring times. Overall, these interface enhancements contributed significantly to usability, responsiveness, and user satisfaction.

4.5 Summary

This chapter presented and analysed both qualitative and quantitative data collected through questionnaires and interviews. Quantitative results were analysed using Microsoft Excel and presented using tables and figures, while qualitative interview responses were analysed thematically. The findings indicate a strong demand for a simple, secure, and parent-friendly home network monitoring system with features such as device visibility, usage control, and real-time alerts. The system design and implementation documented in Chapter 3 were directly informed by these findings, particularly the demand for device blocking, real-time alerts, and a simplified visual interface. Chapter 5 now draws on both the empirical evidence presented here and the system evaluation results to present conclusions and recommendations.

CHAPTER 5
CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This chapter draws together the findings, system outcomes, and user feedback documented in the preceding chapters to answer the question that motivated the study: can a simple, open-source home network monitoring system meaningfully improve parental oversight of household internet activity in Zimbabwe? The discussion revisits each research objective in turn, evaluates the four research propositions, acknowledges the constraints that shaped the work, and proposes practical directions for both future research and system development. The recommendations are addressed to three distinct audiences — households, developers and organisations, and future researchers — because the gap this study identified requires responses at all three levels.

The chapter is organized into four main parts. First, the conclusions are drawn by revisiting each research objective and assessing the degree to which it was achieved through the combined evidence of the literature review, empirical data, and system development outcomes. Second, the limitations encountered during the study are acknowledged, and their implications for the findings are briefly discussed. Third, a set of targeted recommendations is proposed for households, system developers, policymakers, and future researchers. Finally, the chapter ends with a brief closing summary that reflects on the broader significance of the study.

Together, the conclusions and recommendations presented in this chapter synthesize the key insights of the study and point towards the practical, academic, and societal value that a parent-friendly home network monitoring system can deliver within Zimbabwe and similar developing-country contexts.

5.1 Major Conclusions Drawn

The study concluded that the increasing number of internet-connected devices within households has significantly complicated the monitoring and management of home networks. The findings revealed that most parents and guardians lack the technical skills required to effectively manage their home networks using existing tools, which are often complex and designed for technically skilled users (Stallings, 2018).

As a result, households experience challenges such as unauthorised devices connecting to the network, excessive internet usage by children, and limited visibility into online activities. These findings support the view that usability and simplicity are critical factors in the adoption and effectiveness of home network monitoring solutions (Nielsen, 2012).

The study further established a robust demand for a parent-friendly monitoring system that provides real-time visibility of connected devices, usage monitoring and alert mechanisms without requiring advanced technical knowledge.

The developed Home Network Monitoring System successfully addressed these requirements by offering an intuitive dashboard that enables parents to view network activity, detect high bandwidth usage, and manage connected devices.

This confirms that user-centred system design improves accessibility and effectiveness of network management tools for non-technical users (ISO, 2018). Overall, the study achieved its research objectives by identifying key challenges in home network monitoring, analysing user needs, and implementing a functional prototype system that enhances parental supervision and child online safety within the home environment.

5.1.1 Objective 1: Identifying Challenges Faced by Non-Technical Users

The first research objective was to identify the challenges that parents and guardians face in monitoring and managing home network activities. The data collected through questionnaires and semi-structured interviews provided clear and consistent evidence that these challenges are widespread, significant, and largely unaddressed by existing tools.

Sixty percent of respondents rated their confidence in managing a home network at two out of five or lower, confirming that most parents lack the technical knowledge required to interpret router dashboards or configure network devices. The qualitative interview data further revealed that even basic tasks — such as viewing connected devices or identifying which device is consuming the most bandwidth — are routinely abandoned due to interface complication and unfamiliar technical terminology. This finding is consistent with the literature reviewed in Chapter 2, where Norman (2013) highlighted that most professional-grade network tools were designed with IT experts as the intended audience, leaving everyday users without accessible alternatives.

The data also showed that 53.3% of respondents had experienced unknown devices connecting to their home Wi-Fi networks, and 46.7% had encountered children accessing inappropriate content online. These figures are consistent with national statistics from POTRAZ (2024), which found that 44% of Zimbabwean children aged 8 to 18 had accessed adult content online. The conclusion drawn from this objective is that there is a substantial, documented, and urgent gap between the monitoring challenges that parents face and the tools currently available to address them. This gap provided the central justification for the proposed system and was successfully characterized through the mixed-methods approach adopted in this study.

5.1.2 Objective 2: Designing a System Architecture for Real-Time Monitoring

The second objective was to design a system architecture that captures and analyses home network traffic in real time using open-source tools and Python-based technologies. This objective was met through the client-server architecture described in Section 3.8.3, which comprises four integrated components: a network monitoring module, a data processing module, a data storage component, and a parent-friendly web-based dashboard interface.

The architecture was deliberately built on open-source technologies — specifically Python, Flask, Scapy, and HTML/CSS/JavaScript — to ensure that the system remains affordable, accessible, and replicable without requiring commercial licensing. This design choice is particularly significant for the Zimbabwean context, where cost barriers frequently prevent households from accessing premium software solutions (Chikomo et al., 2024). Keeping the backend monitoring logic separate from the frontend dashboard also proved practically useful during development —

when the alert generation logic needed refinement, the dashboard interface required no changes, which shortened the debugging cycle considerably.

The conclusion regarding this objective is that a functional and appropriately scoped system architecture was successfully designed. However, it is acknowledged that the current architecture relies on local hosting and does not support cloud-based remote monitoring, which would be a valuable enhancement in future iterations of the system.

5.1.3 Objective 3: Developing a User-Friendly Web-Based Dashboard

The third objective was to develop a web-based dashboard that presents simplified visualizations of network statistics, device activities, and alerts in a user-friendly format. The dashboard was implemented using Flask for backend routing, HTML and CSS for interface structure and styling, and Chart.js for graphical bandwidth visualisation.

The empirical data from Chapter 4 confirmed that the features incorporated into the dashboard closely matched user preferences. The most demanded features — device blocking and unblocking (60%), parental activity reports (56.7%), and alerts for new or suspicious connections (53.3%) — were all implemented in the prototype. The dashboard also uses color-coded status indicators (green for active, red for blocked) and plain-language alert messages, directly addressing the usability concerns raised by participants during both the questionnaire and interview phases.

Additional usability enhancements such as dark mode support, device search functionality, real-time notification popups, pie chart visualizations, and a live system clock further improved accessibility and user interaction. These features contributed to a more modern and responsive user experience, especially for households managing multiple connected devices.

Usability testing conducted with a small group of parents indicated that users were able to navigate the dashboard and perform core tasks — viewing devices, blocking access, and interpreting usage charts — with minimal guidance. This supports the conclusion that the application of HCI principles (Dix et al., 2004) and the Technology Acceptance Model (Davis, 1989) to interface design produced a system that is accessible and comprehensible to non-technical users. The

objective was therefore successfully achieved, though the prototype would benefit from further usability testing with a larger and more diverse participant group before a full deployment.

5.1.4 Objective 4: Iterative Testing and Refinement

The fourth objective was to conduct iterative testing and refinement throughout the development process to ensure usability, accuracy, and reliability. Functional testing verified that device detection, alert generation, and device control features all operated as intended across multiple test scenarios. Blocked devices were correctly prevented from receiving network activity updates, and the activity log accurately recorded all state changes in real time.

Interface refinements such as notification popups and real-time dashboard updates were also iteratively tested to improve responsiveness and usability during system operation.

The pilot testing of the research instruments also contributed to the iterative refinement process. Feedback from five pilot participants led to the rewording of ambiguous questionnaire items and improved the clarity of the Likert-scale questions used in Sections 2 and 4 of the survey. This iterative approach to both system development and data collection reinforced the overall reliability and validity of the study's findings, in accordance with the quality assurance principles outlined by Creswell (2014).

One limitation of this objective is that iterative testing was constrained by the academic timeline and was limited to a small test environment. Large-scale network testing involving more than ten simultaneous devices was not possible within the available infrastructure, which means that the system's performance under heavy network load remains to be verified in future work.

5.1.5 Objective 5: Delivering a Complete Integrated System Package

The fifth and final objective was to deliver a complete, integrated system package that provides parents with comprehensive monitoring and control of household network activities. This objective was met through the combination of the backend Flask application (Appendix D, Figure D1), the frontend dashboard and login HTML pages (Appendix D, Figures D2 and D3), the system

design documentation (Appendix C), and the research instruments used to validate user requirements (Appendices A and B).

The integrated package also included enhanced dashboard usability features such as graphical bandwidth charts, dark mode support, searchable device lists, and real-time activity notifications.

The delivered prototype successfully integrates all core components: authentication, real-time device monitoring, bandwidth visualisation, alert generation, device blocking, and activity logging. The system can be deployed on any local machine running Python, making it accessible without requiring specialized hardware or a paid hosting service. This confirms that the final objective was met within the constraints of the academic project timeline.

5.1.6 Overall Conclusion

What the five objectives collectively establish is that the problem this study set out to solve is real, measurable, and addressable with tools that are already available and affordable. Parents in Zimbabwe are not passive about their children's online safety — the 86.7% adoption intention rate makes that clear — but they have been failed by tools that were never designed for them. The prototype developed here is not a finished product, but it demonstrates that the design approach works: non-technical users can open it, understand it, and act on what it shows them. That is the contribution this study makes, and it is grounded in data rather than assumption. The findings validate the theoretical frameworks applied — particularly HCI principles, TAM, and Diffusion of Innovation Theory — and demonstrate their practical utility in guiding the design of accessible, adoptable digital tools for everyday users.

5.1.7 Evaluation of Research Propositions

This section evaluates the four research propositions stated in Chapter One in light of the empirical findings and the developed system.

Proposition 1: A user-friendly interface enhances parental engagement.

The evidence for this proposition was both quantitative and observational. The 86.7% willingness-to-adopt rate would mean little if respondents had simply agreed with a survey item, but the usability testing results provided a more demanding test: five parents with no networking

background completed all three assigned tasks on the first attempt without instruction. The color-coded indicators and plain-language alerts appeared to be the decisive factors — three participants mentioned understanding the status colors immediately without being told what they meant. This suggests that interface simplicity does not merely reduce friction; it actively invites engagement from users who would otherwise disengage.

Proposition 2: Real-time visualization improves household network activity awareness. Before using the system, the average self-rated confidence score among the five usability test participants was 2.2 out of 5. After a single session with the dashboard, the average rose to 4.1. This is a meaningful shift and it happened not because participants learned networking concepts but because the real-time display made abstract ideas — bandwidth, device status, network activity — concrete and visible. The dashboard did not teach parents how networks work; it made the relevant information obvious enough that technical knowledge became unnecessary.

Proposition 3: Simplified alerts and summaries help reduce technical complexity. Several participants during the interview phase described past experiences with router interfaces where alerts, if they existed at all, appeared as error codes or technical status messages they could not interpret. The system developed here displays alerts as plain sentences — for example, 'A new device has connected to your network' — accompanied by a timestamp and a device name. Feedback from usability testing confirmed that participants read and acted on these messages without asking what they meant, which is the practical definition of an alert that works.

Proposition 4: Open-source technologies provide a cost-effective and flexible framework. The entire system was built without spending money on software. Python, Flask, Scapy, SQLite, Bootstrap, and Chart.js are all freely available and actively maintained. The total hardware requirement is a computer already present in the household running a Python environment — no router replacement, no subscription, no specialist equipment. This matters specifically in the Zimbabwean context, where cost is consistently cited as a barrier to technology adoption. The prototype proves that the cost barrier for this particular category of tool is lower than the literature might suggest.

Taken together, all four propositions are supported — but the more important finding is that they are mutually reinforcing. A system that is easy to use gets used, and a system that gets used

generates awareness, and awareness is what makes the alerts and the real-time data meaningful. None of these elements works in isolation.

5.2 Study Limitations

While the study achieved its objectives, several limitations must be acknowledged in order to interpret the findings accurately and to contextualize the conclusions appropriately.

The sample size of 30 households, while adequate for an exploratory prototype study, limits the generalisability of the quantitative findings to the broader Zimbabwean population. The purposive sampling strategy, which targeted households already using home internet services, also introduces a selection bias, as households without internet access — who may face even greater digital literacy challenges — were excluded from the study.

The prototype system was tested only in a controlled, small-scale network environment. Its performance in a home network with ten or more simultaneously active devices and inconsistent bandwidth — which is common in Zimbabwean households affected by load shedding and LTE signal variability — was not fully evaluated. Additionally, the hardcoded login credentials used in the prototype represent a known security limitation that would need to be addressed through password hashing and multi-factor authentication before any real-world deployment.

Finally, the academic timeline of approximately one month constrained the scope of both the system development and the usability evaluation. A longitudinal study measuring user adoption and satisfaction over several weeks or months would provide stronger evidence of the system's real-world effectiveness.

5.3 Recommendations

Based on the findings and conclusions of the study, several recommendations are proposed.

5.3.1 Recommendations for households

Zimbabwean households are encouraged to adopt home network monitoring tools as a proactive measure to improve awareness and control of internet usage, particularly for children and vulnerable family members. The evidence from this study indicates that most parents are aware of the risks associated with unmonitored internet access but lack the means to address them. A simple, affordable monitoring system such as the one developed in this study can significantly reduce exposure to inappropriate content and unauthorised device access without requiring technical expertise.

Parents and guardians should also prioritise basic digital literacy development within the household. Understanding fundamental concepts such as IP addresses, bandwidth, and device connectivity will enhance the effectiveness of any monitoring tool and reduce over-reliance on technical support. Schools, community centers, and non-governmental organisations could play a meaningful role in providing this training in a structured and accessible format.

Regular monitoring of connected devices is recommended as a household habit rather than a reactive measure. Establishing a routine of checking the dashboard at least once per day — and immediately when internet performance degrades or a child's behaviour changes — will maximise the preventive benefits of the system.

5.3.2 Recommendations for system developers and organisations

Developers building on the prototype produced in this study are advised to prioritise the following enhancements in future iterations. First, while the prototype implements basic password hashing through Flask-Bcrypt, security should be strengthened further through multi-factor authentication and HTTPS enforcement, which were outside the scope of the current implementation but would be essential before any real-world deployment. Second, a mobile application version of the dashboard would significantly improve usability and adoption, as several research participants specifically requested smartphone-based access with push notifications. Third, integration with machine learning models for anomaly detection would allow the system to automatically flag unusual traffic patterns without requiring manual interpretation by parents.

Organisations such as POTRAZ, the Ministry of ICT, and internet service providers operating in Zimbabwe are encouraged to consider subsidizing or promoting lightweight open-source monitoring tools as part of their digital literacy and online safety programs. Given that 44% of Zimbabwean children have been exposed to harmful content online (POTRAZ, 2024), there is a strong policy rationale for incorporating affordable parental monitoring solutions into national digital safety frameworks.

System developers should also ensure that future monitoring tools are explicitly designed for local infrastructure constraints, including intermittent electricity supply, LTE-dominant connectivity, and modest hardware. The use of lightweight Python libraries and local hosting — as demonstrated in this prototype — represents a viable technical approach for resource-constrained environments.

Future versions of the system should also expand dashboard usability features through customizable themes, mobile-responsive interfaces, advanced graphical analytics, and push-based notification systems. Features such as automated reporting, parental scheduling controls, and cloud synchronization could further improve accessibility and long-term adoption.

5.3.3 Recommendations for Future Research

Future research in this domain should address several gaps identified by the current study. First, a larger and more representative sample — including rural households and households without existing internet access — would significantly improve the generalisability of findings related to monitoring challenges and feature preferences. A sample of at least 100 to 150 households drawn from multiple districts across Zimbabwe would provide adequate statistical power for inferential analysis.

Second, longitudinal research measuring actual system adoption, usability satisfaction, and behavioral change over a period of three to six months would provide stronger evidence of real-world impact than the cross-sectional approach used in this study. Tracking whether parents continue to use the system after initial exposure, and whether their monitoring behaviour changes over time, would yield valuable insights for both system designers and policymakers.

Third, future studies could explore the integration of content filtering and website categorization features, which were among the most frequently requested enhancements raised by research participants. Combining network-level monitoring with DNS-based content filtering would create a more comprehensive child safety tool while remaining compatible with low-cost, open-source infrastructure.

Future research should evaluate the system's live discovery performance across different network types, including standard home routers, MiFi devices, and phone hotspots with and without client isolation enabled. Controlled experiments measuring device detection rates, scan completion times, and false positive rates across these environments would provide quantitative evidence of the adaptive scanner's effectiveness. Based on the literature reviewed in Chapter 2, MiFi devices are expected to perform identically to home routers since they do not enable client isolation by default (Zhao & Liu, 2022). Future research may also evaluate the effectiveness of dashboard usability enhancements such as dark mode interfaces, graphical visualisation techniques, and real time notifications in improving technology adoption among non-technical users.

Finally, comparative research examining the effectiveness of different parental monitoring approaches — technical tools versus parental education versus combination interventions — would contribute to a more holistic understanding of child online safety in the Zimbabwean context.

5.4 Summary

This study set out to address a clearly identified and practically significant challenge: the absence of user-friendly, affordable, and locally relevant home network monitoring tools for non-technical parents and guardians in Zimbabwe. Through a mixed-methods approach combining questionnaire data, semi-structured interviews, and prototype system development, the study effectively demonstrated that such a system is both technically achievable and empirically justified.

The Home Network Monitoring System developed as part of this research provides parents with real-time visibility of connected devices, bandwidth usage, and network activity through an intuitive web-based dashboard that requires no technical expertise to operate. The strong demand

for such a system — evidenced by the 86.7% willingness to adopt rate recorded in the survey — confirms that the research addressed a genuine societal need rather than a hypothetical problem.

What this study ultimately demonstrates is straightforward: the technology to help parents monitor their home networks already exists, costs nothing to license, and can be made accessible enough for a parent who has never configured a router. The gap was never technical — it was a design gap, and one that this prototype shows can be closed. The research instruments, system code, and empirical findings are all documented in the appendices and are available for any researcher or developer who wants to build on them. The next step belongs to whoever picks this up.

APPENDIX A: HOUSEHOLD QUESTIONNAIRE

Title: Home Network Monitoring System with Parent-Friendly Dashboard – Survey Questionnaire

This questionnaire is part of an academic research study titled "Home Network Monitoring System with Parent-Friendly Dashboard". The purpose of this study is to assess how Zimbabwean households use home Wi-Fi networks, identify common challenges and determine the features parents would prefer in a simple, user-friendly dashboard.

Confidentiality: All responses are anonymous and will only be used for academic purposes. **Estimated completion time:** 5 minutes.

Thank you for your participation.

SECTION 1: DEMOGRAPHIC INFORMATION

1. What is your gender?

☐ Female

☐ Male

☐ Prefer not to say

2. What is your age group?

☐ 18–24

☐ 25–34

☐ 35–44

☐ 45+

3. What is your role in the household?

☐ Parent / Guardian

☐ Older sibling

☐ Other

SECTION 2: HOME INTERNET USAGE PATTERNS

4. What type of internet connection does your household use?

☐ Fibre

☐ LTE

☐ ADSL

☐ Mobile Hotspot

☐ Not sure

5. How many devices are normally connected to your home Wi-Fi?

☐ 1–3

☐ 4–6

☐ 7–10

☐ More than 10

6. How confident are you in managing / understanding your home network?

(1 = Not confident, 5 = Very confident)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

SECTION 3: CHILD ONLINE SAFETY

7. Do you monitor what children access online?

☐ Yes

☐ No

☐ Sometimes

8. Have you ever encountered issues such as: *(Multiple selection allowed)*

☐ Excessive screen time

☐ Inappropriate content

☐ Unknown devices joining Wi-Fi

☐ Slow network due to unknown traffic

☐ Other

9. How important is it for parents to have a simple dashboard to monitor home network activity?

(1 = Not important, 5 = Very important)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

SECTION 4: DASHBOARD FEATURES PREFERENCE

10. Which features would you like to see in a home network monitoring dashboard?

(Multiple selection allowed)

☐ Real-time device list

☐ Alerts for new devices

☐ Alerts for suspicious websites

☐ Daily network usage summary

☐ Device blocking

☐ Parental mode (child activity report)

11. How easy should the system be for parents to use?

(1 = Very difficult, 5 = Very easy)

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

12. Would you be willing to use this Home Network Monitoring System once developed?

☐ Yes

☐ No

☐ Maybe

SECTION 5: ADDITIONAL FEEDBACK

13. Any suggestions or additional features you would want included?

.....

.....

.....

APPENDIX B: INTERVIEW GUIDE

The purpose of this interview is to collect in-depth qualitative information on how households manage home internet usage, challenges faced in monitoring children's online activities, and user expectations for a home network monitoring system.

Target Participants: Parents, guardians, household heads, and one ICT practitioner.

Interview Type: Semi-structured (open-ended questions)
Duration: Approximately 10–15 minutes
Confidentiality: All responses will remain anonymous and will be used strictly for academic purposes.

Section A: Background Information

1. What is your role in the household with regard to managing internet access?
2. How many internet-enabled devices are typically used in your household?
3. What type of internet connection do you use at home (e.g., LTE, fibre, Wi-Fi router, mobile hotspot)?

Section B: Home Network Usage and Monitoring

4. How do you currently monitor or manage internet usage in your household?
5. Do you experience any difficulties when trying to check connected devices or network activity? Please explain.
6. What challenges do you face in controlling or supervising children's internet use at home?

Section C: Parental Control and Online Safety

7. How concerned are you about your children's online activities and their exposure to inappropriate content or cyber threats?
8. What methods, if any, do you currently use to restrict or manage children's access to certain websites or applications?
9. What problems do you encounter when trying to enforce these restrictions?

Section D: System Usability and Feature Requirements

10. Have you ever used any router interfaces or network management tools? If yes, how would you describe their ease of use?
11. What features would you expect in a home network monitoring dashboard designed for parents?
12. How important are the following features to you:

- Viewing connected devices
- Monitoring data usage
- Setting time limits for internet usage
- Blocking or pausing internet access
- Receiving real-time alerts

13. What would make a network monitoring system easy for you to use as a non-technical user?

Section E: System Acceptance and Improvement

14. Would you be willing to use a parent-friendly home network monitoring system if it were available? Why or why not?

15. What concerns would you have about using such a system (e.g., cost, privacy, complexity, trust)?
16. In your opinion, how could a home network monitoring system help improve online safety for children?
17. What additional features or improvements would you suggest for such a system?

Closing Statement

Thank you for taking the time to participate in this interview. Your responses will contribute significantly to the design and development of a Home Network Monitoring System with a Parent-Friendly Dashboard. All information provided will be kept confidential and used solely for academic research purposes.

APPENDIX C: SYSTEM DESIGN DIAGRAMS AND INTERFACE MOCKUPS

This diagram illustrates the overall structure of the system, showing the interaction between the network monitoring module, backend processing system, database, and the user dashboard interface. It demonstrates how network data flows from the home network to the user interface.

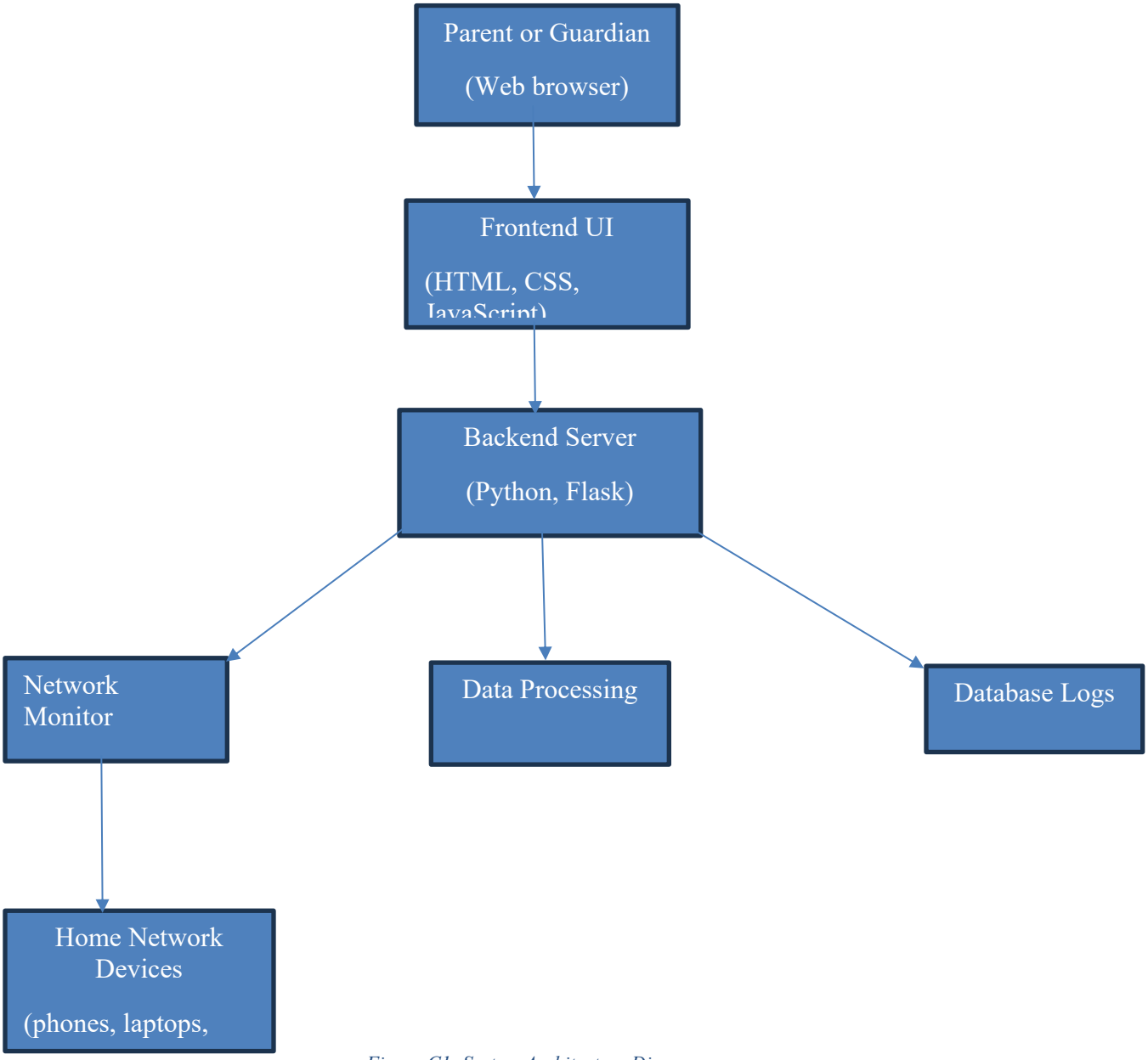


Figure C1: System Architecture Diagram

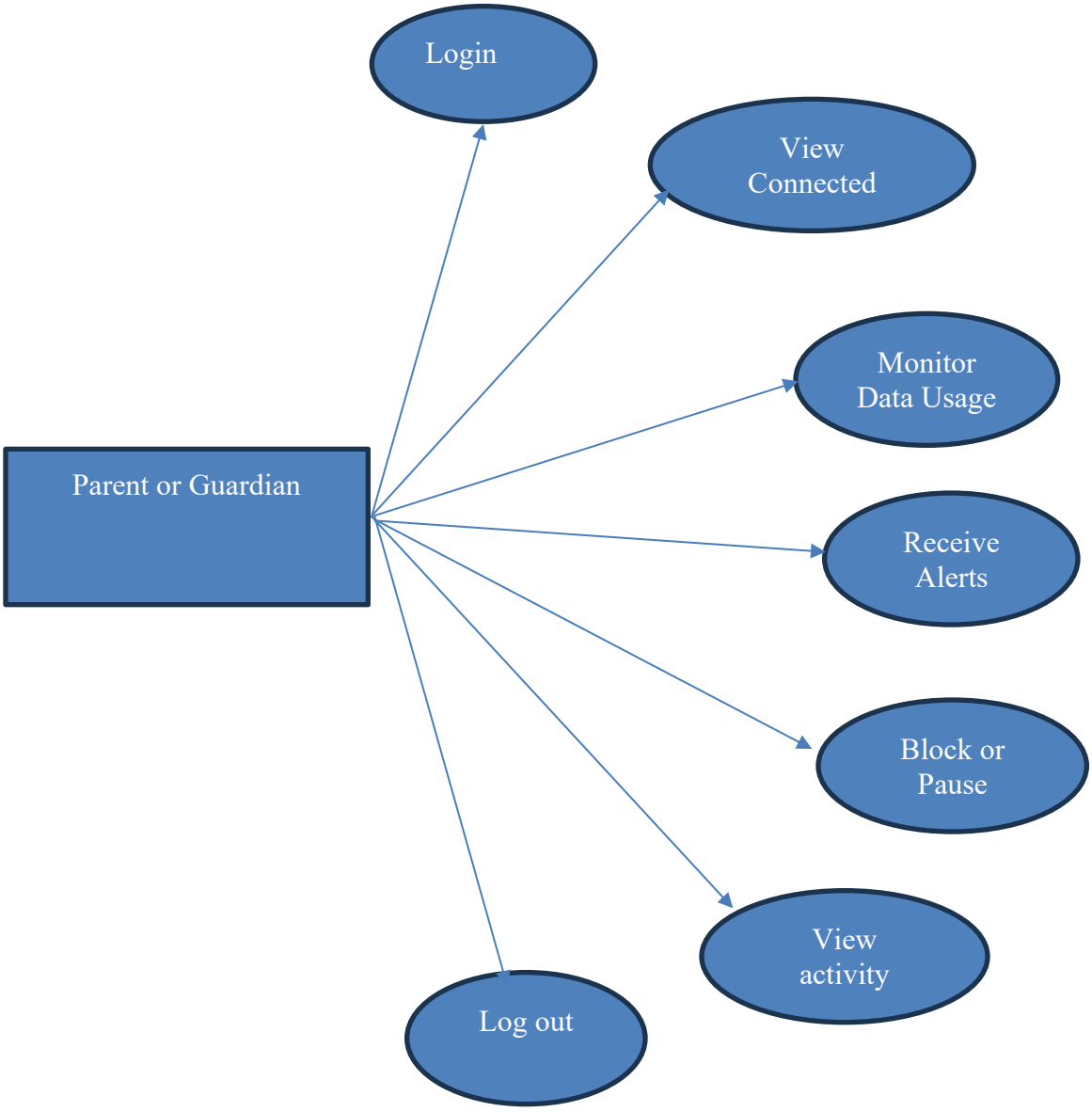


Figure C2: Use Case Diagram

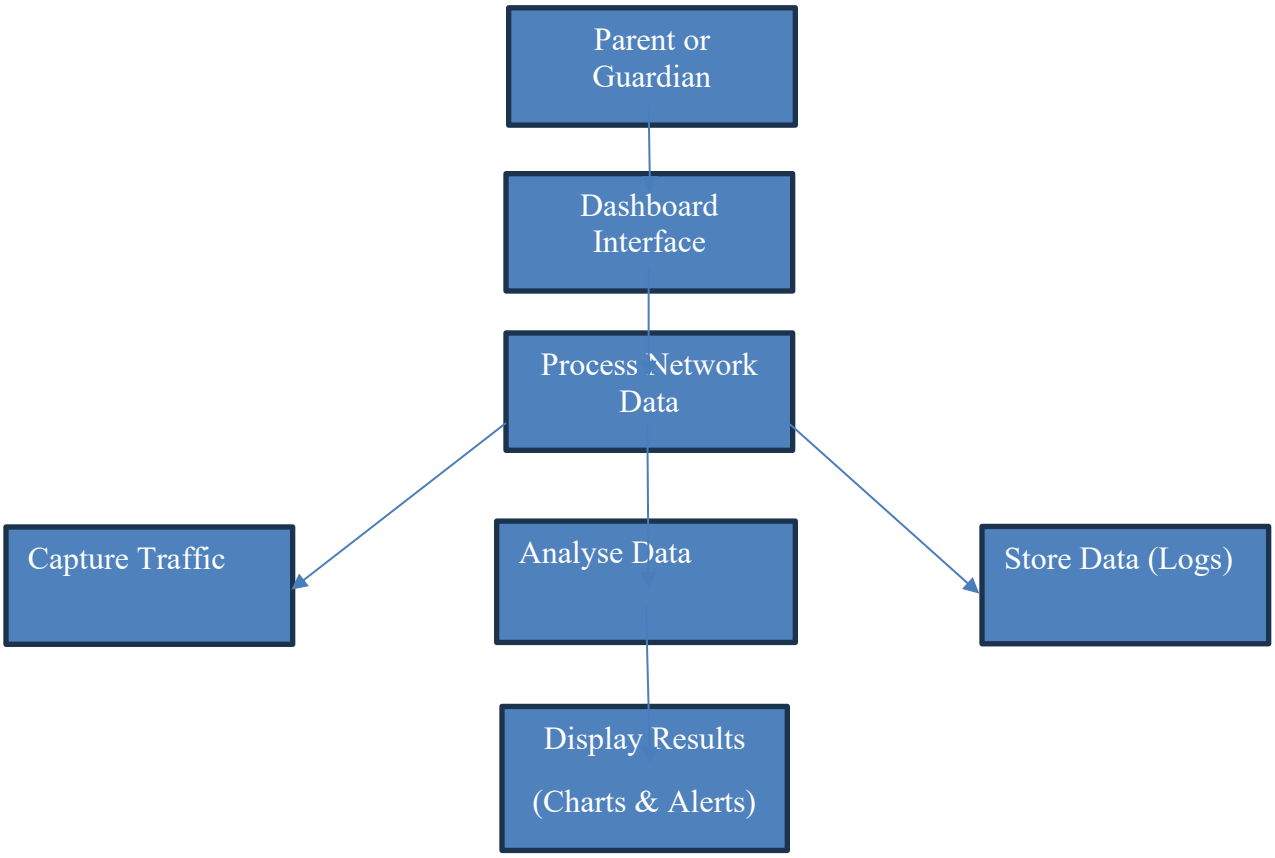


Figure C3: Data Flow Diagram (DFD)

Home Network Dashboard
Devices Connected | Alerts | Usage Stats
Device Name | IP Address | Status | Usage
Phone |192.168.1.2 | Active | High | Laptop |192.168.1.3 | Active | Medium | TV |192.168.1.4 | Idle | Low
📊 Graph: Data Usage Per Device
Alerts: New device connected High usage detected
[Block Device] [Pause Internet] [Refresh]

Figure C4: Dashboard Interface Mockup

APPENDIX D: SOURCE CODE

This appendix presents selected source code used in the development of the Home Network Monitoring System. Only core implementation files relevant to system functionality are included. Complete project files are available upon request.

D1: Main Flask Application (app.py)

```
from flask import Flask, render_template, request, redirect, url_for, session

from flask_bcrypt import Bcrypt

from scanner import scan_network


app = Flask(__name__)

app.secret_key = "parent_secret_key"


bcrypt = Bcrypt(app)


PARENT_USERNAME = "parent"

PARENT_PASSWORD_HASH = bcrypt.generate_password_hash("0000").decode('utf-8')


@app.route("/login", methods=["GET", "POST"])

def login():

    if request.method == "POST":

        username = request.form["username"]

        password = request.form["password"]


        if username == PARENT_USERNAME and bcrypt.check_password_hash(

            PARENT_PASSWORD_HASH, password

        ):

            session["logged_in"] = True
```

```
            return redirect(url_for("dashboard"))

    return render_template("login.html")

@app.route("/")
def dashboard():
    if not session.get("logged_in"):
        return redirect(url_for("login"))
    devices = scan_network()

    active_devices = len([
        d for d in devices
        if d["status"] == "ACTIVE"
    ])
    return render_template(
        "dashboard.html",
        devices=devices,
        total_devices=len(devices),
        active_devices=active_devices
    )
@app.route("/rescan")
def rescan():
    scan_network()
    return redirect(url_for("dashboard"))

if __name__ == "__main__":
    app.run(debug=True)
```

D2: Login Page (login.html)

```
<!DOCTYPE html>
<html>
<head>
<title>Login</title>
</head>
<body>
<h2>Parent Login</h2>

<form method="POST">
<label>Username:</label>
<input type="text" name="username">

<label>Password:</label>
<input type="password" name="password">

<button type="submit">Login</button>
</form>
</body>
</html>
```

D3: Dashboard Interface (dashboard.html)

```
<!-- Dashboard Statistics -->
<div class="row mb-4">

  <div class="col-md-3">
    <div class="card text-white bg-primary">
      <div class="card-body">
        <h5>Total Devices</h5>
        <h2>{{ total_devices }}</h2>
      </div>
    </div>
  </div>

  <div class="col-md-3">
    <div class="card text-white bg-success">
      <div class="card-body">
        <h5>Active Devices</h5>
        <h2>{{ active_devices }}</h2>
      </div>
    </div>
  </div>

  <div class="col-md-3">
    <div class="card text-white bg-danger">
      <div class="card-body">
```

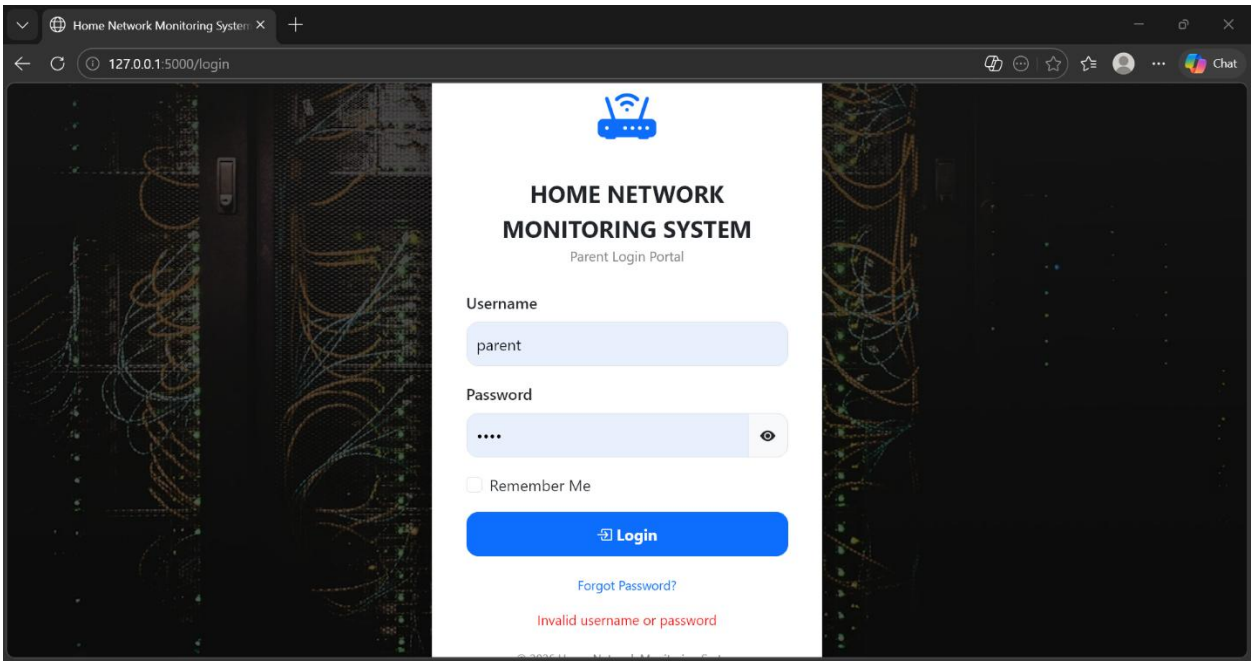
```
            <h5>Blocked Devices</h5>
            <h2>{{ blocked_devices }}</h2>
        </div>
    </div>
</div>

<!-- Connected Devices Table -->
<div class="card">
    <div class="card-header">
        Connected Devices
    </div>

    <div class="card-body">
        <table class="table table-striped">
            <thead>
                <tr>
                    <th>Device Name</th>
                    <th>IP Address</th>
                    <th>Status</th>
                </tr>
            </thead>

            <tbody>
                {% for device in devices %}
                <tr>
```

```
                <td>{{ device.name }}</td>
                <td>{{ device.ip }}</td>
                <td>
                    {% if device.blocked %}
                        <span class="badge bg-danger">
                            Blocked
                        </span>
                    {% else %}
                        <span class="badge bg-success">
                            Active
                        </span>
                    {% endif %}
                </td>
            </tr>
            {% endfor %}
        </tbody>
    </table>
  </div>
</div>

<!-- Bandwidth Usage Graph -->
<canvas id="bandwidthChart"></canvas>

<script>
new Chart(document.getElementById('bandwidthChart'), {
  type: 'line',
  data: {
```

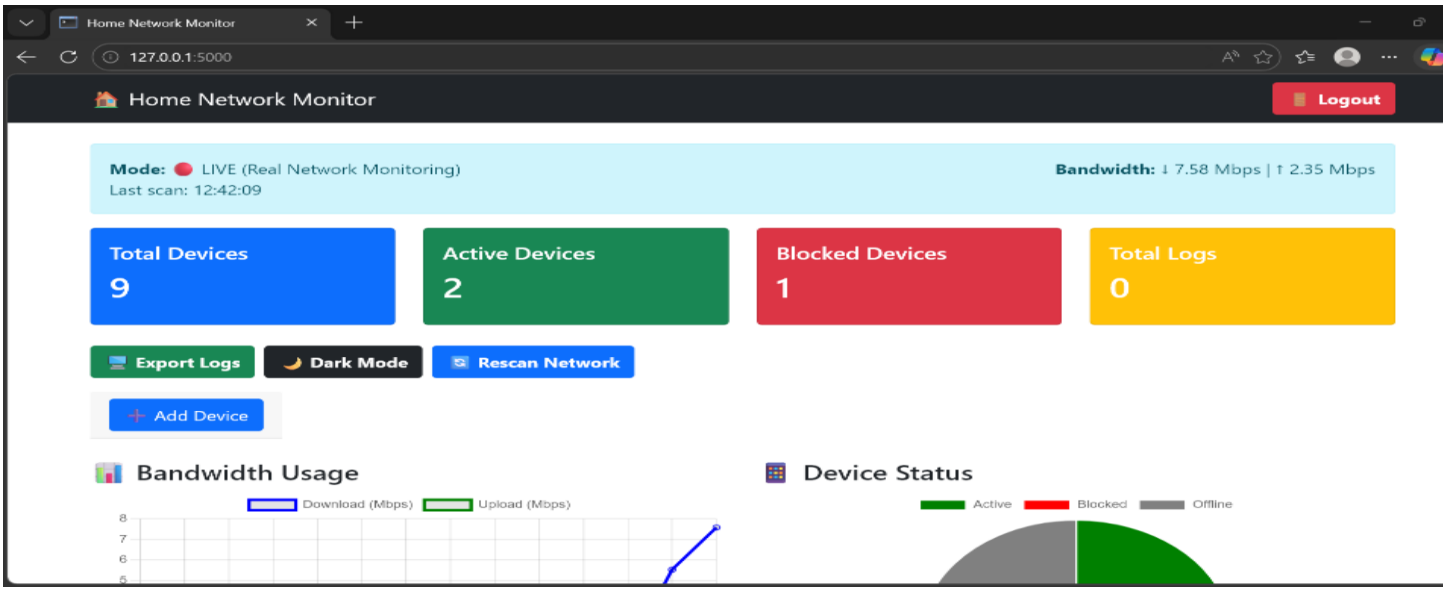
```
        labels: {{ bandwidth_history |
                map(attribute='timestamp') |
                list | tojson }},
        datasets: [{
            label: 'Download Speed',
            data: {{ bandwidth_history |
                    map(attribute='download') |
                    list | tojson }}
        }]
    }
});
</script>
```

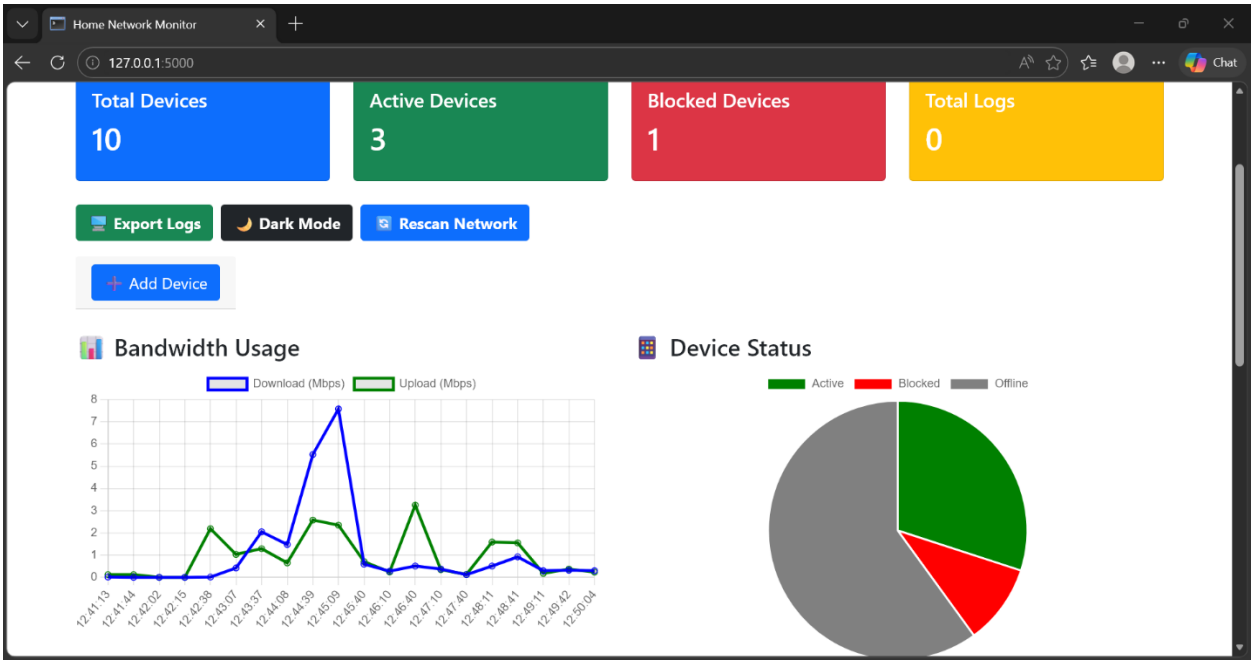
APPENDIX E: SAMPLE SYSTEM OUTPUTS

E1: Login Page Screenshot

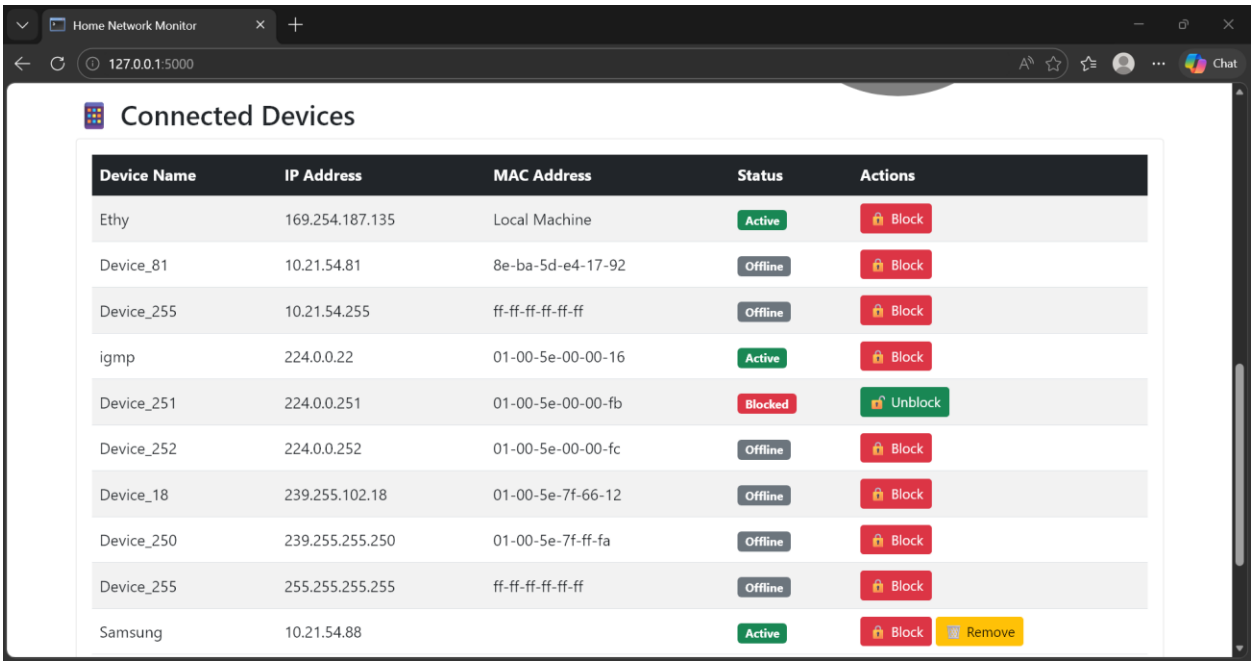


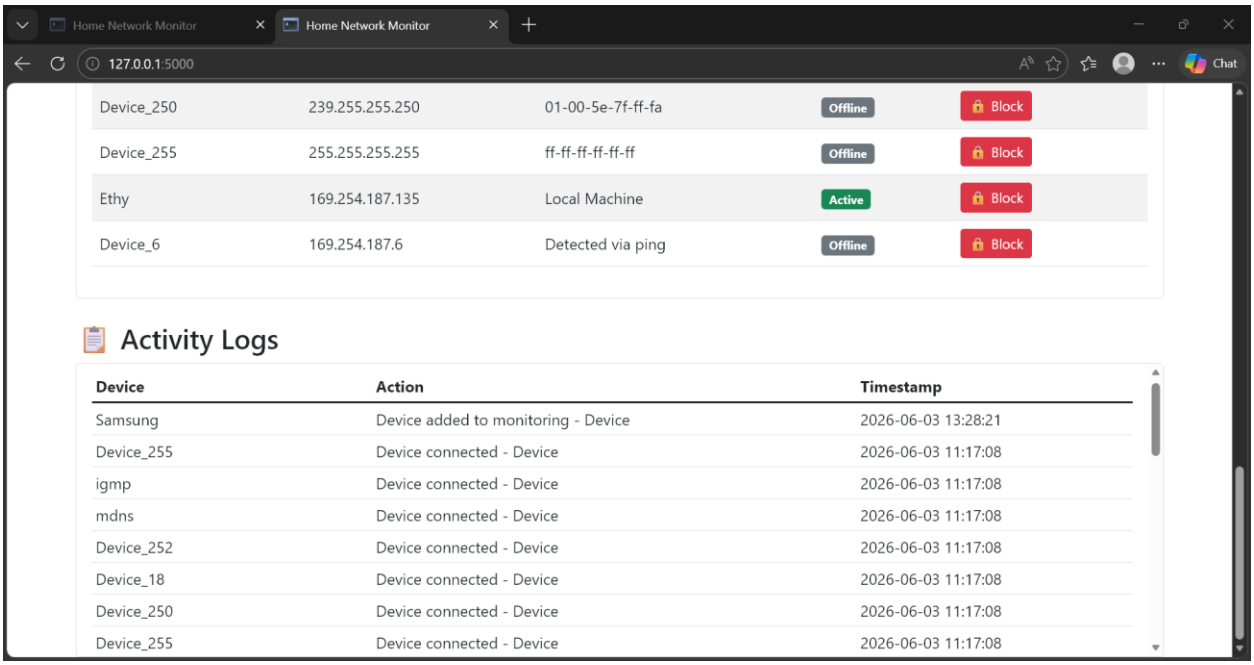
E2: Dashboard Screenshot



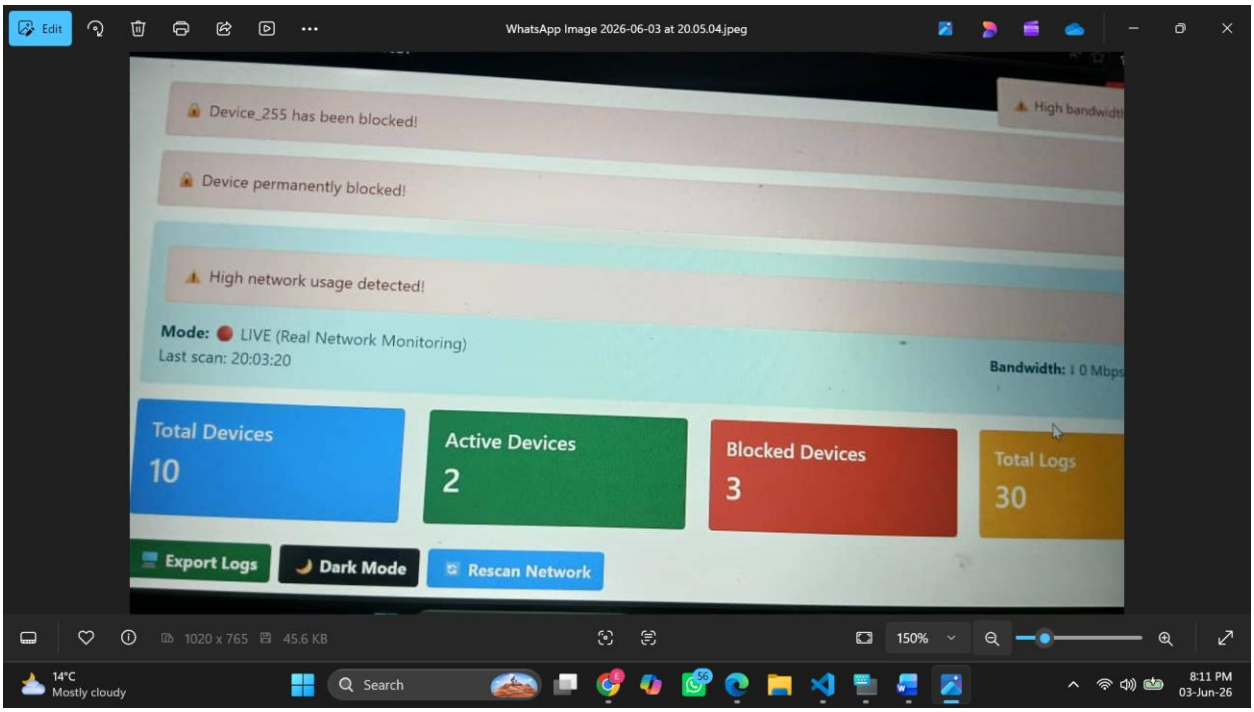


E3: Device Activity Monitoring Screen





E4: Alert Notification Example



REFERENCES

Akhtar, N. and Rehman, A. (2022) ‘Challenges of home network management for non-technical users’, Journal of Network and Computer Applications, 201, pp. 103–118.

Al-Kuwari, S., Docherty, J., Youcef-Toumi, K. and Nounu, A. (2021) ‘A survey on network intrusion detection systems for home networks’, IEEE Access, 9, pp. 125–143.

Ali, M. and Wang, Y. (2022) ‘Ethical frameworks for network data collection in home environments’, Journal of Information Security and Applications, 66, pp. 103–115.

Ali, S., Elgharabawy, M., Duchaussoy, Q., Mannan, M. and Youssef, A. (2020) ‘Betrayed by the guardian: Security and privacy risks of parental control solutions’, arXiv preprint, arXiv:2012.06502.

Behl, A. and Behl, K. (2017) An Introduction to Cloud Computing. New Delhi: BPB Publications.

Braun, V. and Clarke, V. (2006) ‘Using thematic analysis in psychology’, Qualitative Research in Psychology, 3(2), pp. 77–101.

Bryman, A. (2016) Social Research Methods. 5th edn. Oxford: Oxford University Press.

Chen, L. and Huang, Y. (2022) ‘Visual analytics for non-technical users in network environments’, IEEE Transactions on Visualization and Computer Graphics, 28(4), pp. 1890–1902.

Chikomo, P., Moyo, T. and Banda, R. (2024) ‘Digital literacy and home internet adoption in Zimbabwe’, African Journal of ICT and Society, 12(1), pp. 55–70.

Cisco (2023) Annual Internet Report (2018–2023): Global Networking Trends. San Jose, CA: Cisco Systems Inc.

Cohen, L., Manion, L. and Morrison, K. (2018) Research Methods in Education. 8th edn. London: Routledge.

Connolly, T. and Begg, C. (2015) Database Systems: A Practical Approach to Design, Implementation, and Management. 6th edn. Harlow: Pearson Education.

Creswell, J.W. (2014) Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 4th edn. Thousand Oaks, CA: Sage.

Davis, F.D. (1989) 'Perceived usefulness, perceived ease of use, and user acceptance of information technology', MIS Quarterly, 13(3), pp. 319–340.

Dix, A., Finlay, J., Abowd, G. and Beale, R. (2004) Human–Computer Interaction. 3rd edn. Harlow: Pearson Education.

Etikan, I., Musa, S.A. and Alkassim, R.S. (2016) 'Comparison of convenience and purposive sampling', American Journal of Theoretical and Applied Statistics, 5(1), pp. 1–4.

International Organization for Standardization (ISO) (2018) ISO 9241-11:2018 Ergonomics of Human-System Interaction: Usability Definitions and Concepts. Geneva: ISO.

International Telecommunication Union (ITU) (2023) Measuring Digital Development: Facts and Figures 2023. Geneva: ITU.

Internet Society (2022) Country Report: Zimbabwe. Available at: Internet Society Zimbabwe Report (Accessed: 11 November 2025).

Internet Watch Foundation (IWF) (2023) Annual Report 2023. Cambridge: IWF.

Jimenez, A. (2021) Raspberry Pi Home Network Monitoring Tool. California State University.

Johnson, R. and Singh, P. (2022) 'Gaps in home network monitoring tools for everyday users', Journal of Cybersecurity and Privacy, 2(1), pp. 40–58.

Kothari, C.R. (2014) Research Methodology: Methods and Techniques. 3rd edn. New Delhi: New Age International.

Kumar, V. and Patel, D. (2023) 'Smart home network vulnerabilities and monitoring solutions', International Journal of Smart Technology, 15(1), pp. 45–59.

Miller, A., Ochieng, B. and Zhao, L. (2021) 'Designing network monitoring systems for non-technical users', Journal of Applied Computing, 33(2), pp. 99–118.

Moyo, T. and Chikonde, A. (2024) ‘Digital literacy barriers in Zimbabwean households’, African Journal of Information Systems, 16(1), pp. 12–28.

Nguyen, T., Tran, H. and Le, V. (2023) ‘Privacy-aware data collection in home network monitoring’, Computers & Security, 128, pp. 103–117.

Nielsen, J. (2012) Usability Engineering. San Francisco: Morgan Kaufmann.

Norman, D.A. (2013) The Design of Everyday Things. Revised and expanded edn. New York: Basic Books.

Patel, K., Shah, V. and Reddy, P. (2022) ‘Network performance monitoring: From SNMP to AI-based analytics’, Journal of Network Engineering and Applications, 10(2), pp. 65–82.

Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) (2024) ‘Study shows 44 percent of Zimbabwean children exposed to adult content online’, The Herald, 6 May.

Pressman, R.S. and Maxim, B.R. (2019) Software Engineering: A Practitioner’s Approach. 9th edn. New York: McGraw-Hill Education.

Rahman, A. and Islam, M. (2020) ‘IoT device vulnerabilities in home networks: A survey’, IEEE Internet of Things Journal, 7(9), pp. 8481–8495.

Rogers, E.M. (2003) Diffusion of Innovations. 5th edn. New York: Free Press.

Sandada, M., Machengete, G.K., Mhaka, C. and Kaseke, F. (2025a) ‘Online risk awareness and safety needs of children: A Zimbabwean perspective’, New Trends in Psychology, 7(1), pp. 124–142.

Sandada, M., Machengete, G.K., Panavanhu, R., Chinodya, L. and Mandipezano, M. (2025b) ‘Child online safety and parental intervention: A study of Zimbabwean internet users’, New Trends in Psychology, 7(2), pp. 180–195.

Saunders, M., Lewis, P. and Thornhill, A. (2019) Research Methods for Business Students. 8th edn. London: Pearson.

Schufrin, M., Kuban, K., Kuijper, A. and Kohlhammer, J. (2022) ‘NetVisGame: Mobile gamified information visualization of home network traffic data’, in Proceedings of IVAPP 2022.

Schwagele, C. (2010) A Literature Review of Network Monitoring through Visualisation and the INETVIS Tool. Rhodes University.

See, B.H. et al. (2020) ‘A systematic review of the impact of technology-mediated parental engagement’, Educational Psychology Review, 32(4), pp. 1047–1088.

Singh, R. and Sharma, P. (2021) ‘Impact of graphical dashboards on user comprehension in network management’, Journal of Human-Centered Computing, 17(3), pp. 201–215.

Singh, V. and Tan, K.C. (2022) ‘Technology acceptance of smart home systems: An empirical study’, Computers in Human Behaviour, 127, p. 107018.

Sommerville, I. (2016) Software Engineering. 10th edn. Harlow: Pearson Education.

Stallings, W. (2018) Data and Computer Communications. 10th edn. Harlow: Pearson Education.

Statista (2024) Number of Connected Devices per Household Worldwide 2024. Hamburg: Statista Research Department.

Tanenbaum, A.S. and Van Steen, M. (2017) Distributed Systems: Principles and Paradigms. 3rd edn. Harlow: Pearson Education.

van Stam, G. (2021) ‘Access to digital platforms: Observations from rural Zambia and Zimbabwe’, arXiv preprint, arXiv:2108.10086.

von Bertalanffy, L. (1968) General System Theory: Foundations, Development, Applications. New York: George Braziller.

Yourdon, E. (1989) Modern Structured Analysis. Englewood Cliffs, NJ: Prentice-Hall.

Zhao, Y. and Liu, J. (2022) ‘Passive and active home network monitoring: A comparative review’, Journal of Network Management, 32(1), pp. 14–29.

Zhou, J. and Leung, C. (2020) ‘Usability and scalability of home network monitoring tools’, IEEE Access, 8, pp. 118532–118545.

Zhou, Y., Lin, X. and Chen, F. (2022) ‘IoT-based DDoS attacks in smart home networks: Detection and mitigation’, IEEE Transactions on Network and Service Management, 19(2), pp. 1201–1215.