BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SCIENCE AND ENGINEERING DEPARTMENT OF COMPUTER SCIENCE



Enhancing Network Security in IoT Devices at National Railways of Zimbabwe: A Comprehensive Study on Vulnerabilities and Solutions

NAME: MUNYARADZI A PATAMA

REG NUMBER: B221315B

COURSE CODE: NWE400

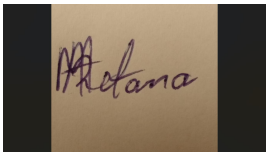
SUPERVISOR: MR CHITUMA

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

JUNE 2026

APPROVAL FORM

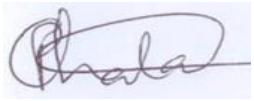
The undersigned certify that they have supervised the student **MUNYARADZI A PATAMA** dissertation entitled **Enhancing Network Security in IoT Devices at National Railways of Zimbabwe: A Comprehensive Study on Vulnerabilities and Solutions** submitted in partial fulfilment of the requirements for the Bachelor of **NETWORK ENGINEERING** at Bindura University of Science Education.



STUDENT **DATE:17-08-2026**



SUPERVISOR **DATE:17-08-2026**



CHAIRMAN **DATE:17-08-2026**



DEDICATION

This dissertation is dedicated primarily to my beloved family, whose unwavering encouragement, patience, and steadfast belief in my abilities have been a constant source of strength and motivation throughout my academic journey. Your support has been the foundation for this work. I also dedicate this work to my mentors and instructors at Bindura University of Science Education. Their guidance, wisdom, and inspiration have significantly shaped my understanding and passion for network engineering. Your commitment to teaching and mentorship has been essential to my academic growth. This dissertation is further dedicated to the National Railways of Zimbabwe, especially the IT Department, for their support, guidance, and invaluable practical exposure, which made this research not only possible but meaningful. Your collaboration enriched this study with real-world insights and applications. Finally, I dedicate this work to the Almighty God, for granting me the strength, wisdom, and perseverance needed to undertake and complete this dissertation. Without His guidance and blessings, this achievement would not have been possible.

ACKNOWLEDGEMENTS

I wish to express my deepest and most sincere gratitude to my supervisor, Mr. Chituma, for his invaluable guidance, constructive feedback, and unwavering support throughout the development of this dissertation. Your expertise, patience, and encouragement have been instrumental in shaping this research, helping me navigate complex concepts and refine my analytical approach. Your mentorship has not only enhanced the quality of this work but has also contributed significantly to my personal and professional growth.

I am profoundly grateful to the Department of Computer Science at Bindura University of Science Education for providing a solid academic foundation, access to essential resources, and continuous mentorship throughout my studies. The knowledge, skills, and inspiration I gained from the department have been pivotal in the successful completion of this research.

My heartfelt appreciation goes to the National Railways of Zimbabwe, particularly the IT Department, for granting me access to their facilities, network infrastructure, and operational insights. Your practical support and willingness to share expertise were crucial in informing the design, testing, and validation of the Blueprint Forge system, ensuring that this study remains relevant and applicable to real-world scenarios.

Finally, I extend my deepest thanks to my family and friends for their constant encouragement, patience, and unwavering belief in my abilities. Your support has been a continuous source of motivation, resilience, and inspiration throughout the academic journey, and I am forever grateful for your love and understanding.

ABSTRACT

This dissertation presents a comprehensive study on enhancing network security in Internet of Things (IoT) devices deployed at the National Railways of Zimbabwe (NRZ), where the increasing integration of IoT technologies to optimize operational efficiency and elevate safety standards has simultaneously introduced substantial cybersecurity vulnerabilities threatening both critical railway infrastructure and passenger welfare. The primary objective of this research is to systematically identify and analyze specific security vulnerabilities within the NRZ's IoT ecosystem, critically evaluate the effectiveness of current security measures, and develop robust, implementable solutions to strengthen network security across the organization's digital infrastructure. Utilizing a mixed-methods research approach that integrates comprehensive vulnerability assessments, structured surveys, and in-depth stakeholder interviews, this study examines critical weaknesses prevalent in the system, including inadequate security protocols governing device communication, outdated firmware creating exploitable entry points, weak authentication mechanisms, and insufficient cybersecurity training among personnel responsible for system maintenance and oversight. The significance of this research extends beyond the immediate context of the NRZ, offering valuable insights that inform best practices for securing critical railway infrastructure in developing nations while addressing the unique technological, operational, and resource constraints faced by the organization, thereby contributing meaningfully to the broader academic and practical discourse on IoT security implementation in resource-limited environments. The findings and recommendations presented herein aim to establish a framework for building a safer, more resilient railway network that effectively mitigates cyber threats while maintaining operational continuity, ultimately endeavoring to enhance passenger safety, protect critical national infrastructure, and improve operational reliability through strengthened network security practices tailored to the specific needs of the National Railways of Zimbabwe.

Table of Contents

APPROVAL FORM i

DEDICATION ii

ACKNOWLEDGEMENTS iii

ABSTRACT iv

CHAPTER 1 1

PROBLEM IDENTIFICATION 1

1.1 Introduction 1

1.2 Background of Study 1

1.3 Statement of the Problem 3

1.4 Research Objectives 3

1.5 Research Questions 4

1.6 Hypothesis 4

1.7 Justification / Significance of the Study 5

1.8 Assumptions 6

1.9 Limitations / Challenges 7

1.10 Scope / Delimitation of the Study 8

1.11 Definition of Terms 9

1.12 Summary 11

CHAPTER 2 11

LITERATURE REVIEW 11

2.0 Introduction 11

2.1 Conceptual Framework 13

2.1.1 Concept of the Internet of Things (IoT) 13

2.1.2 IoT Applications in Railway Systems 14

2.1.3 Concept of Network Security 15

2.1.4 Common Vulnerabilities in IoT Devices 16

2.1.5 Cybersecurity Solutions for IoT Networks 17

2.1.7 Risk Assessment in IoT Environments 17

2.1.8 Established Security Frameworks and Standards 18

2.1.6 Conceptual Framework of the Study 19

2.2 Theoretical Framework 20

2.2.1 Zero Trust Security Theory 21

2.2.2 Defence-in-Depth Theory 21

2.2.3 Socio-Technical Theory 22

2.2.4 Relevance of the Theories to Study 23

2.3 Empirical Evidence 24
2.3.1 Empirical Studies on IoT Security Vulnerabilities 24
2.3.2 Empirical Studies on Network-Based IoT Attacks 25
2.3.3 Empirical Studies on IoT Security in Transport and Railway Systems 25
2.3.4 Empirical Studies on IoT Security Controls and Mitigation Strategies 26
2.3.5 Empirical Evidence from Developing Countries and Similar Contexts 26
2.4 Research Gap Analysis 27
2.4.1 Contextual Gap 27
2.4.2 Geographical Gap 27
2.4.3 Methodological Gap 27
2.4.4 Practical and Implementation Gap 27
2.4.5 Policy and Governance Gap 28
2.5 Summary 28
CHAPTER 3 29
RESEARCH METHODOLOGY 29
3.0 Introduction 29
3.1 Research Philosophy 29
3.2 Research Design 31
3.3 Research Approach 33
3.4 Target Population and Study Area 34
3.5 Sampling Techniques and Sample Size 36
3.5.1 Human Participant Sampling 36
3.5.2 IoT Device Sampling 36
3.5.3 Sample Size Justification 37
3.6 Data Collection Methods and Instruments 37
3.6.1 Structured Questionnaires (Quantitative) 37
3.6.2 Semi-Structured Interviews (Qualitative) 38
3.6.3 Document Analysis and System Configuration Audits (Technical) 38
3.7 Data Quality and Trustworthiness 38
3.7.1 Quantitative Data Quality 39
3.7.2 Qualitative Data Trustworthiness 39
3.7.3 Triangulation 40
3.8 Data Analysis Techniques 40
3.8.1 Quantitative Analysis 40
3.8.2 Qualitative Analysis 40
3.8.3 Integration of Quantitative and Qualitative Findings 41
3.9 Ethical Considerations 41
3.10 Summary 42

CHAPTER 4 43
SYSTEM IMPLEMENTATION AND RESULTS 43
4.0 Introduction 43
4.1 System Architecture 44
4.1.1 Presentation Layer 45
4.1.2 Application Layer 46
4.1.3 Data Layer 47
4.2 Technology Stack and Justification 47
4.3 Key System Modules 49
4.3.1 Authentication and Session Management 49
4.3.2 Dashboard and Analytics 49
4.3.3 IoT Device Management 50
4.3.4 Vulnerability Tracking and Management 51
4.3.5 Security Solutions and Remediation 52
4.3.6 Security Assessments 53
4.3.7 User Management and Audit Logging 54
4.4 Security Features Implementation 55
4.4.1 Input Validation and Injection Prevention 55
4.4.2 Security Headers and Middleware 56
4.4.3 Session Security 56
4.5 Results and Discussion 57
4.5.1 Vulnerability Landscape Analysis 57
4.5.2 Device Risk Distribution 57
4.5.3 Remediation Progress Analysis 58
4.5.4 Alignment with Research Objectives 59
4.6 Summary 60
CHAPTER 5 60
CONCLUSIONS AND RECOMMENDATIONS 60
5.0 Introduction 60
5.1 Research Conclusions 61
5.1.1 Nature and Severity of IoT Vulnerabilities at NRZ 61
5.1.2 Impact on Operational Efficiency and Safety 62
5.1.3 Adequacy of Existing Security Measures 62
5.1.4 Appropriate Security Strategies and Frameworks 63
5.1.5 Governance and Continuous Monitoring 63
5.2 Recommendations 64
5.2.1 Immediate Technical Recommendations 64
5.2.2 Medium-Term Strategic Recommendations 65
5.2.3 Governance and Organisational Recommendations 65

5.3 Limitations of the Study 66
5.4 Areas for Further Research 67
5.5 Summary 68
REFERENCES 69
APPENDIX A 70
Structured Questionnaire for IoT Security Assessment at NRZ 70
Section A: Demographic Information 70
Section B: IoT Device Awareness and Vulnerability Perception 71
Section C: Current Security Practices Assessment 71
Section D: Impact Assessment of IoT Security Vulnerabilities 71
Section E: Open-Ended Questions 72
APPENDIX B 72
Semi-Structured Interview Guide 72
Interview Introduction 72
Part 1: IoT Security Landscape 73
Part 2: Existing Security Measures 73
Part 3: Governance and Recommendations 73
Closing 73
APPENDIX C 73
Informed Consent Form 73
1. Purpose of the Study 73
2. Nature of Participation 74
3. Voluntary Participation and Confidentiality 74
4. Risks, Benefits, and Responsible Disclosure 74
5. Contact Information 74
Consent Declaration 74
Optional: Consent for Audio Recording 74
APPENDIX D 75
IoT Device Inventory and Configuration Audit Checklist 75
D.1 IoT Device Inventory Record 75
D.2 Security Configuration Audit Checklist 75
D.3 Vulnerability Documentation Record 76
APPENDIX E 76
NISAAP System Architecture and Technology Stack 76
E.1 System Architecture Overview 76
E.2 Authentication and Security 77
APPENDIX F 77
Database Schema and Entity Relationship Details 77
F.1 Entity Relationship Summary 77

F.2 Key Entity Fields 78
APPENDIX G 78
Role-Based Access Control (RBAC) Matrix 78
APPENDIX H 79
CVSS Scoring Methodology and Vulnerability Severity Classification 79
H.1 CVSS Severity Ratings 79
H.2 Vulnerability Severity Distribution at NRZ 79
H.3 Device Risk Level Distribution 80
APPENDIX I 80
NISAAP Security Implementation Details 80
I.1 Input Validation and Injection Prevention 80
I.2 Security Headers Configuration 80
I.3 Session and Password Security 81
I.4 Rate Limiting and Audit Logging 81
APPENDIX J 81
Research Ethics Approval and Institutional Clearance 81
J.1 Institutional Clearance Request 81
J.2 Ministry Approval Request 82
J.3 University Ethics Committee Approval 82

CHAPTER 1

PROBLEM IDENTIFICATION

1.1 Introduction

The National Railways of Zimbabwe (NRZ) is at the forefront of integrating Internet of Things (IoT) technologies to enhance operational efficiency, improve safety, and provide better services to passengers and freight customers. However, the increasing reliance on IoT devices within this critical infrastructure has raised significant concerns regarding network security. The unique operational environment of railways, characterized by extensive networks and diverse systems, presents distinct challenges in protecting against cyber threats.

IoT devices used in railway operations, such as track sensors, signalling systems, and automated monitoring tools, often lack robust security features. Many of these devices are vulnerable to cyberattacks due to outdated software, inadequate encryption protocols, and insufficient authentication measures. The implications of a security breach in this context can be catastrophic, potentially leading to service disruptions, financial losses, and jeopardizing passenger safety.

Recent incidents in global railway networks have underscored the urgent need for enhanced security measures. The interconnected nature of IoT devices means that a compromise in one area can have cascading effects across the entire network. Therefore, it is imperative to conduct a comprehensive study on the vulnerabilities specific to IoT implementations within the NRZ and to explore effective strategies for mitigating these risks. Through this research, valuable insights are sought for policymakers, technology providers, and railway operators in their efforts to build a resilient IoT ecosystem.

This dissertation adopts a multi-dimensional approach to examining the security challenges inherent in the NRZ's IoT infrastructure, combining technical vulnerability assessment, policy evaluation, and human-factor analysis to provide a holistic understanding of IoT security.

1.2 Background of Study

The integration of Internet of Things (IoT) technologies into the National Railways of

Zimbabwe (NRZ) represents a significant advancement in the modernization of rail transport. IoT devices enhance operational efficiency by enabling real-time monitoring of train movements, predictive maintenance of infrastructure, and improved safety protocols. These technologies facilitate the seamless exchange of data, providing insights that are crucial for decision-making and enhancing service delivery.

However, the deployment of IoT devices also introduces a myriad of security challenges. The rail industry globally has witnessed an increase in cyber threats targeting critical infrastructure, underscoring the importance of robust security measures. For NRZ, the stakes are particularly high; a successful cyberattack could disrupt services, compromise safety, and lead to significant economic losses. Furthermore, given the strategic importance of rail transport in Zimbabwe, any security breach could have broader implications for national stability and public confidence.

The operational environment of railways is characterized by a complex interplay of various systems, including signalling, communications, and operational management. This interconnectedness can create vulnerabilities, as the compromise of a single IoT device can potentially expose the entire network to attacks. Many IoT devices in the railway context are designed with limited security features due to constraints in processing power and energy consumption. Often, these devices are deployed with default settings, which can be exploited by malicious actors.

Despite the growing awareness of IoT security issues, there remains a significant knowledge gap regarding the specific vulnerabilities faced by the NRZ. Existing literature tends to focus on general IoT security practices rather than offering targeted insights into the unique challenges of rail transport systems in Zimbabwe. This dissertation seeks to fill that gap by providing a comprehensive analysis of the vulnerabilities associated with IoT devices in the NRZ and proposing tailored solutions to enhance network security.

By understanding the current landscape of IoT security within the NRZ, this study aims to contribute to the development of effective strategies that can safeguard critical infrastructure, protect user data, and ensure the integrity of railway operations. The findings will not only benefit the NRZ but also serve as a valuable resource for other sectors in Zimbabwe and beyond that are increasingly adopting IoT technologies.

1.3 Statement of the Problem

As the National Railways of Zimbabwe (NRZ) increasingly adopts Internet of Things (IoT) technologies to enhance operational efficiency and safety, the associated security vulnerabilities present a critical challenge. The integration of IoT devices, such as sensors for track monitoring, automated signalling systems, and data analytics platforms, has the potential to transform railway operations. However, this technological advancement also exposes the NRZ to a multitude of cyber threats that could compromise the safety, reliability, and integrity of its services.

Current IoT implementations within the NRZ lack adequate security measures, making them susceptible to various forms of cyberattacks, including unauthorized access, data breaches, and service disruptions. Many devices operate with outdated firmware, insufficient encryption, and weak authentication protocols, which can be exploited by malicious actors. The interconnected nature of these devices means that a breach in one area can cascade throughout the entire railway system, posing significant risks to passenger safety and operational continuity. Furthermore, there is a lack of comprehensive research focused on the specific vulnerabilities of IoT devices within the context of the NRZ. Existing literature predominantly addresses general IoT security concerns without delving into the unique challenges faced by railway operators in Zimbabwe. This gap in knowledge hampers the development of targeted security strategies that could effectively mitigate risks.

Hence, the National Railways of Zimbabwe faces critical security vulnerabilities in its IoT infrastructure that threaten operational integrity and safety. This research aims to identify these vulnerabilities and propose effective solutions to enhance network security, ensuring the safe and efficient operation of railway services. By addressing this problem, the study seeks to contribute to the broader discourse on IoT security and inform best practices for railway operators in Zimbabwe and similar contexts.

1.4 Research Objectives

i. To identify and critically evaluate the nature, severity, and scope of network security vulnerabilities inherent in IoT devices deployed across the National Railways of Zimbabwe's operational infrastructure, using recognised vulnerability assessment frameworks.

ii. To analyse the extent to which identified IoT network security vulnerabilities compromise operational efficiency, data integrity, system reliability, and passenger safety within the National Railways of Zimbabwe.

iii. To examine and evaluate the adequacy of existing network security measures, policies, and protocols currently implemented to protect IoT devices at the National Railways of Zimbabwe against contemporary cyber threats.

iv. To evaluate and recommend technically robust and operationally feasible network security strategies, frameworks, and controls for strengthening the protection of IoT devices within the specific operational and financial context of the National Railways of Zimbabwe.

v. To develop practical, sustainable, and context-sensitive recommendations for strengthening security governance, improving stakeholder awareness, and establishing a framework for continuous monitoring and improvement of IoT network security at the National Railways of Zimbabwe.

1.5 Research Questions

i. What is the nature, severity, and scope of network security vulnerabilities affecting IoT devices deployed across the National Railways of Zimbabwe's operational infrastructure? ii. To what extent do identified IoT network security vulnerabilities affect operational efficiency, data integrity, system reliability, and passenger safety at the National Railways of Zimbabwe?

iii. How adequate are the existing network security measures, policies, and protocols in protecting IoT devices at the National Railways of Zimbabwe against contemporary cyber threats?

iv. Which network security strategies, frameworks, and technical controls are most technically appropriate and operationally feasible for enhancing IoT device security within the specific context of the National Railways of Zimbabwe?

v. What practical governance structures, stakeholder awareness initiatives, and continuous monitoring mechanisms are required to ensure the long-term sustainability of IoT network security improvements at the National Railways of Zimbabwe?

1.6 Hypothesis

This study does not formulate formal hypotheses, as it is primarily guided by clearly defined research objectives and research questions aimed at exploring and addressing network

security challenges associated with IoT devices at the National Railways of Zimbabwe (NRZ). Given the study's exploratory and descriptive nature, and its reliance on methodologies such as literature review, case analysis, stakeholder engagement, and system evaluation, research questions provide more appropriate guidance than rigid hypotheses. The research focuses on identifying vulnerabilities, assessing their impact, evaluating existing security measures, and proposing strategies for strengthening IoT network security.

In lieu of formal hypotheses, the study is guided by analytical themes derived from the research objectives, encompassing vulnerability identification, impact assessment, evaluation of existing security measures, and the formulation of context-appropriate security recommendations. These themes provide a coherent structure for data collection, analysis, and interpretation, ensuring the research remains focused and systematic. Additionally, research propositions may emerge inductively from the data, offering evidence-grounded insights relevant to IoT security within critical infrastructure.

1.7 Justification / Significance of the Study

The significance of this study is grounded in its contribution to enhancing network security for IoT devices within the NRZ, with broader implications for critical infrastructure protection, technological advancement, and national development.

Enhancing Safety and System Reliability

The integration of IoT technologies in railway operations introduces efficiencies but also exposes critical systems to cyber risks. By identifying vulnerabilities and proposing appropriate security controls, this study contributes to safeguarding railway operations, thereby improving passenger safety, operational reliability, and service continuity.

Bridging Knowledge Gaps

There is limited empirical research focusing on IoT security within Zimbabwe's railway sector. This study addresses this gap by providing context-specific insights into vulnerabilities, risks, and mitigation strategies relevant to the NRZ, thereby contributing to academic literature and industry knowledge.

Informing Policy and Security Practices

The findings of this research will provide evidence-based recommendations to guide policymakers, system administrators, and railway management in developing effective security frameworks, policies, and best practices tailored to IoT environments.

Supporting Operational Efficiency and Economic Growth

A secure IoT infrastructure enhances operational efficiency by minimizing disruptions caused by cyber incidents. Improved railway performance supports trade, logistics, and mobility, thereby contributing to economic development in Zimbabwe.

Promoting Sustainable Technological Adoption

As the NRZ continues to adopt digital technologies, this study emphasizes the importance of integrating security into technological advancement. It promotes a proactive security culture that supports innovation while mitigating risks.

1.8 Assumptions

The study is based on several key assumptions that provide a foundation for the research process and guide the interpretation of findings.

i. It is assumed that IoT devices deployed within the NRZ environment possess identifiable security vulnerabilities that can be systematically assessed using appropriate analytical methods. These vulnerabilities may arise from weak configurations, outdated software, or inadequate security controls, and are expected to be observable during the course of the study.

ii. The study assumes that strengthening network security measures—such as implementing encryption, robust authentication mechanisms, and regular system updates—will significantly enhance the protection of IoT systems. These measures are expected to reduce exposure to cyber threats and improve the overall resilience of the network infrastructure. iii. It is also assumed that increased stakeholder awareness and training will positively influence adherence to established security practices. When employees and system users are well-informed about potential risks and proper security procedures, they are more likely to act responsibly and contribute to a stronger security posture within the organization. iv. The study assumes that regular maintenance activities, including firmware and software updates, play a critical role in minimizing security risks. Outdated systems are more vulnerable to attacks; therefore, consistent updates are expected to address known vulnerabilities and improve system integrity.

v. Another assumption is that the adoption of centralized monitoring and management systems will enhance the detection and response to security incidents. Such systems allow

for realtime monitoring and coordinated responses, which are essential in mitigating potential threats effectively.

vi. It is further assumed that key stakeholders within the NRZ will be willing to provide relevant information and actively engage with the study. Their cooperation is essential for obtaining accurate data and ensuring that the research findings are practical and applicable. vii. Lastly, the study assumes that sufficient data on IoT systems, existing security practices, and vulnerabilities will be accessible. The availability of reliable data is crucial for conducting a meaningful analysis and drawing valid conclusions.

1.9 Limitations / Challenges

Despite careful planning, this study is subject to several limitations and challenges that may affect the depth and applicability of its findings.

i. Limited Access to Sensitive Data: Access to detailed security information within the NRZ may be restricted due to confidentiality concerns. This limitation could reduce the extent to which vulnerabilities and existing security measures can be fully analysed. To mitigate this, the study will employ data triangulation, drawing upon multiple sources of evidence— including publicly available documentation, industry reports, and anonymized interviews— to compensate for restricted access and to cross-validate findings.

ii. Resource Constraints: Financial and infrastructural limitations may affect both the data collection process and the feasibility of implementing recommended security solutions. Limited resources can restrict the scope of analysis and the practicality of proposed improvements. The study addresses this by prioritising cost-effective and scalable recommendations that can be implemented in phases, ensuring that resource limitations do not render the proposed solutions unattainable.

iii. Diversity of IoT Devices: The presence of various IoT devices with different manufacturers, configurations, and standards presents a challenge in developing uniform security solutions. This diversity complicates the assessment process and may require tailored approaches for different systems. To address this, the research adopts a categorised assessment framework that groups devices by function and risk profile, enabling more targeted and manageable analysis.

iv. Organizational Resistance to Change: There may be resistance among stakeholders when it comes to adopting new security measures or modifying existing practices. Such resistance

can arise from a lack of awareness, fear of disruption, or reluctance to change established routines. The study seeks to mitigate this by incorporating change management principles into its recommendations, emphasising the benefits of enhanced security and providing clear implementation roadmaps to ease the transition.

v. Rapidly Evolving Threat Landscape: Cyber threats are continuously evolving, with new attack methods emerging regularly. As a result, some findings of this study may become outdated if not continuously reviewed and updated to reflect current trends. To address this limitation, the study proposes a continuous monitoring and periodic review framework, enabling the NRZ to adapt its security posture in response to emerging threats. vi. Human Factors: Human error remains a significant challenge in cybersecurity. Employees may unintentionally compromise system security through poor practices, highlighting the importance of continuous training and awareness programmes. This study incorporates recommendations for ongoing security awareness training and the establishment of a security-conscious culture within the organisation to reduce human-factor risks.

vii. Regulatory Constraints: Compliance with cybersecurity regulations and policies may present additional challenges. Adhering to legal and organizational requirements can influence the implementation of certain security measures. The study takes a complianceaware approach, ensuring that all recommendations are aligned with prevailing regulatory frameworks and international best practices.

viii. Context-Specific Scope: Since the study focuses specifically on the NRZ, the findings may not be fully generalisable to other organisations or industries. However, they may still provide useful insights for similar contexts. To enhance the broader applicability of the findings, the study draws upon and cross-references international case studies and established IoT security frameworks, allowing readers in comparable settings to adapt the insights to their own environments.

1.10 Scope / Delimitation of the Study

This study is carefully defined within specific boundaries to ensure focus and manageability.

i. Geographical Scope: The research is confined to the National Railways of Zimbabwe. While the findings may offer insights applicable elsewhere, the primary focus remains on this organization and its operational environment.

ii. Technological Scope: The study focuses exclusively on IoT devices and systems used in railway operations, such as sensors and monitoring systems. Other non-IoT technologies are excluded to maintain a clear and targeted scope.

iii. Focus on Vulnerabilities and Security Measures: The research emphasizes identifying security vulnerabilities, assessing their impact, evaluating existing measures, and proposing improvements. Broader cybersecurity issues not directly related to IoT are not the primary focus.

iv. Time Scope: The study reflects the current state of IoT security during the research period. While past data may be referenced, the main emphasis is on present conditions and challenges.

v. Stakeholder Scope: Data collection will involve internal stakeholders such as IT personnel, management, and operational staff. Their perspectives are essential for understanding practical challenges and existing practices.

vi. Implementation Scope: Although the study will propose recommendations, it will not extend to the actual implementation or testing of these solutions. The focus remains on analysis and strategic guidance.

vii. Methodological Scope: The research adopts a mixed-methods approach, combining qualitative and quantitative techniques. However, it does not include experimental or longterm studies that track changes over extended periods.

1.11 Definition of Terms

Internet of Things (IoT): Refers to a network of interconnected devices that communicate and exchange data through the internet. In this study, it specifically includes devices used in railway operations, such as sensors and automated monitoring systems.

Network Security: Encompasses the policies, technologies, and practices designed to protect networks from unauthorized access, attacks, and data breaches. It ensures the confidentiality, integrity, and availability of information.

Vulnerability: A weakness or flaw in a system that can be exploited by attackers to compromise security. Identifying vulnerabilities is essential for preventing potential breaches.

Cyber Threat: Any malicious activity or potential risk that targets information systems, aiming to disrupt operations, steal data, or gain unauthorized access.

Encryption: The process of converting data into a coded format that can only be accessed by authorized users with the correct decryption key. It is a critical measure for protecting sensitive information.

Authentication: The process of verifying the identity of a user or system before granting access. Strong authentication mechanisms help prevent unauthorized access.

Security Framework: A structured set of guidelines, standards, and best practices that provides a systematic approach to managing and improving an organisation's information security posture. In the context of this study, a security framework serves as the foundational architecture within which specific security controls, policies, and procedures are developed, implemented, and continuously evaluated to protect IoT devices and the broader network infrastructure of the NRZ.

Risk Assessment: A systematic process of identifying, analysing, and evaluating potential risks that could threaten the confidentiality, integrity, or availability of information systems and assets. Within this study, risk assessment involves the structured identification of vulnerabilities in IoT devices, the estimation of the likelihood and potential impact of associated threats, and the prioritisation of risks to inform the selection and implementation of appropriate security controls.

Centralized Security Management: A system that allows for the monitoring and management of security activities from a single point, improving efficiency and coordination in handling security issues.

Incident Response: A structured approach to detecting, managing, and recovering from security breaches. Effective incident response minimizes damage and ensures quick recovery.

Firmware: Embedded software within hardware devices that controls their functionality. Keeping firmware updated is essential for maintaining device security.

Stakeholders: Individuals or groups with an interest in the organization's operations and security, including management, IT personnel, and operational staff. Their involvement is crucial for implementing effective security measures.

1.12 Summary

This chapter has established the foundation for the study on enhancing network security in IoT devices at the National Railways of Zimbabwe. It highlighted the growing reliance on IoT technologies in railway operations and emphasized the security challenges that arise from their use. These vulnerabilities pose significant risks to operational efficiency, data integrity, system reliability, and passenger safety. The chapter clearly outlined the research objectives and research questions, which guide the study in identifying vulnerabilities, assessing their impact, evaluating existing security measures, and proposing appropriate solutions. The significance of the study was also discussed, demonstrating its relevance in improving safety, informing policy, enhancing operational performance, and supporting technological advancement. Furthermore, the chapter presented the key assumptions, limitations, and scope of the study to define its boundaries and acknowledge potential challenges. Important terms were also defined to ensure clarity and consistency throughout the research. Overall, this chapter provides a strong foundation for the study by setting the context, defining the research direction, and establishing a framework for analysing IoT security issues and developing practical solutions tailored to the NRZ

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

The rapid expansion of digital technologies across critical infrastructure has significantly transformed the operational environment of transport institutions globally. One of the most influential developments in this regard is the Internet of Things (IoT), which has enabled

interconnected ecosystems of sensors, embedded systems, smart devices, communication platforms capable of collecting, transmitting, processing data in real time. In the railway sector, IoT technologies are increasingly being integrated into systems such as locomotive diagnostics, predictive maintenance, surveillance, signalling support, asset monitoring, fleet tracking, communication management. These technologies provide substantial operational advantages, including improved efficiency, automation, service reliability, real-time visibility. However, the same interconnectedness that supports digital transformation also expands the cyberattack surface, exposes railway institutions to complex, evolving cybersecurity threats.

Recent literature indicates that railway systems are becoming progressively dependent on connected digital infrastructure, thereby increasing their vulnerability to cyber compromise. This is particularly important because railway institutions differ from ordinary enterprise environments in that cyberattacks may affect not only information systems but also operational continuity, infrastructure resilience, safety-sensitive processes. Cybersecurity in railway environments must therefore be understood not merely as a technical concern but as an issue of strategic, operational importance

Within the context of the National Railways of Zimbabwe (NRZ), the adoption of IoT-enabled systems presents an important opportunity for institutional modernization, particularly in areas such as infrastructure monitoring, remote diagnostics, communication management, inventory visibility, surveillance. Nevertheless, the deployment of such systems in a mixed legacy environment may also introduce vulnerabilities if security controls, governance frameworks, technical safeguards are not sufficiently developed. Existing literature consistently demonstrates that IoT ecosystems are particularly vulnerable due to weak authentication, poor update practices, insecure firmware, constrained device resources, inconsistent standards, inadequate encryption.

The purpose of this chapter is to critically review literature relevant to the study of network security in IoT environments, with particular emphasis on vulnerabilities and cybersecurity solutions applicable to railway institutions. The chapter is structured around the conceptual framework, theoretical framework, empirical evidence, research gap analysis and summary. Through this review, the study establishes its academic foundation and demonstrates the need for context-specific investigation into IoT network security at the National Railways of Zimbabwe

2.1 Conceptual Framework

The conceptual framework of a study provides a structured explanation of the major concepts, relationships that define the research problem. In this study, the conceptual framework is built on the assumption that the level of network security in IoT devices at NRZ is influenced by a combination of technical, operational, organizational factors. These include weak authentication mechanisms, insecure communication channels, poor firmware management, inadequate access control, insufficient intrusion monitoring, weak network segmentation, limited staff awareness, underdeveloped institutional cybersecurity governance.

At the centre of this study is the dependent variable, namely enhanced network security in IoT devices at NRZ. This variable is affected by several independent variables, including weak passwords, insecure firmware and software configurations, poor encryption practices, inadequate device lifecycle management, insecure communication protocols and weak network architecture. The study also recognises the influence of intervening variables such as management support, financial capacity, technical expertise, institutional policy and organizational readiness for digital transformation

This conceptual position is significant because it rejects the narrow assumption that cybersecurity is solely a technical issue. Instead, it argues that network security outcomes are shaped by the interaction between technological controls and institutional preparedness. In a railway institution such as NRZ, this is especially relevant because cybersecurity depends not only on the strength of individual devices but also on governance, maintenance practices, staff competence, procurement standards and access management procedures

2.1.1 Concept of the Internet of Things (IoT)

The Internet of Things refers to a network of interconnected physical devices embedded with sensors, processors, software, communication modules that enable them to collect, exchange, process data across digital networks. Unlike conventional computing systems, IoT devices are often designed to operate autonomously or semi-autonomously, continuously gathering data from their physical environments, transmitting it for monitoring, analysis or automated decision-making.

The significance of IoT lies in its ability to extend digital connectivity into physical environments, operational systems. In industrial, transport contexts, this allows infrastructure, machinery, assets to become part of intelligent, data-driven ecosystems. This shift supports the transition from reactive management toward predictive, automated, evidence-based

operations. In railway environments, IoT devices may include GPS trackers for train location, surveillance cameras at stations, vibration sensors on tracks, smart diagnostic systems for locomotives, environmental sensors in depots, communication devices for operational coordination. These technologies can improve maintenance efficiency, reduce service disruptions, enhance safety oversight, strengthen operational visibility. However, the literature also indicates that the very characteristics that make IoT valuable—such as scalability, ubiquity, interoperability, real-time communication—also make it difficult to secure using conventional perimeter-based network security models.

Critically, while IoT is often portrayed as a driver of smart infrastructure, digital efficiency, the literature warns that rapid deployment frequently outpaces the development of robust security controls. In many cases, institutions adopt connected technologies primarily for operational convenience, while cybersecurity considerations remain secondary. This creates a structural imbalance in which digital innovation advances faster than institutional cyber resilience.

2.1.2 IoT Applications in Railway Systems

Railway institutions across the world are increasingly integrating IoT technologies to improve operational performance, service reliability, asset visibility. Common IoT applications in railway systems include predictive maintenance, rolling stock diagnostics, wayside condition monitoring, environmental sensing, passenger information systems, cargo tracking, smart ticketing, energy management, surveillance. These applications enable continuous data collection from geographically distributed assets, thereby improving decision-making, reducing dependence on purely manual operational processes.

Recent railway engineering literature suggests that modern rail systems increasingly depend on intelligent monitoring infrastructure, particularly in the area of wayside condition monitoring, equipment diagnostics. This is important because rail operations are highly dependent on the condition, reliability of widely dispersed physical infrastructure, much of which is costly, safety-sensitive, difficult to inspect continuously using traditional methods. In the context of NRZ, IoT technologies could potentially be integrated into systems such as locomotive monitoring, rail condition sensing, station surveillance, infrastructure diagnostics and communication support. Such systems could contribute significantly to institutional modernization and operational efficiency. However, the applicability of globally documented

railway IoT models to NRZ must be treated with caution. Much of the existing literature is based on highly digitised railway systems in technologically advanced environments, where cybersecurity maturity, infrastructure quality and financial capacity may be considerably stronger than those available in Zimbabwe

This means that while IoT applications appear highly beneficial in theory, their implementation at NRZ must be examined critically in relation to sustainability, compatibility and cybersecurity readiness. The mere adoption of connected devices does not automatically result in operational improvement unless appropriate safeguards and institutional capacity are simultaneously developed

2.1.3 Concept of Network Security

Network security refers to the policies, technologies, procedures, control mechanisms designed to protect connected systems, devices, communication pathways from unauthorized access, misuse, disruption, manipulation or destruction. It seeks to ensure that digital communications remain secure, trustworthy, resilient within interconnected environments.

Conventionally, network security is explained through the Confidentiality, Integrity, Availability (CIA) triad. Confidentiality ensures that information is accessible only to authorized users; integrity ensures that data remains accurate, unaltered;, availability ensures that systems, services remain accessible when needed. Although these principles remain fundamental, their application becomes significantly more complex in IoT environments because of the distributed, heterogeneous, continuously connected nature of IoT devices. In IoT-enabled railway environments, network security extends beyond traditional endpoint protection and perimeter defence. It includes secure device onboarding, encrypted communication, authentication, access control, anomaly detection, segmentation, logging and incident response. A weakness in one device may potentially compromise broader operational systems, especially in environments where network segmentation is weak or where trust relationships are poorly managed

For NRZ, network security is therefore not merely an information technology concern but an operational requirement. Railway systems depend on reliable communication between devices, monitoring platforms, control systems and human operators. If these communication pathways are compromised, the consequences may include operational misinformation, surveillance failure, asset visibility loss, reduced maintenance reliability and service

disruption. This makes network security central to the resilience of any IoT-enabled railway institution

2.1.4 Common Vulnerabilities in IoT Devices

IoT devices are widely recognised in the literature as among the most vulnerable components of contemporary digital ecosystems. Their vulnerabilities arise from both technical design limitations, insecure deployment practices. Many IoT devices are manufactured with low computational power, limited memory, lightweight operating systems in order to reduce production costs, improve efficiency. While commercially practical, these design characteristics often restrict the implementation of advanced security controls.

Among the most common vulnerabilities documented in the literature are default or weak credentials, outdated firmware, poor access control, insecure APIs, open ports, lack of encryption, insecure communication protocols, inadequate logging. These weaknesses rarely occur in isolation. Rather, they often coexist within the same device or environment, thereby increasing the likelihood of compromise.

Studies have documented recurring weaknesses such as insecure authentication, poor software integrity validation, insufficient logging, weak communication protocols, exposed interfaces. These findings are important because they indicate that IoT vulnerabilities are not merely isolated technical flaws but structural features of the wider IoT ecosystem.

A major concern highlighted in the literature is that insecurity is often normalized through deployment practices that prioritise operational functionality over cyber resilience. In many cases, institutions inherit insecure technologies not simply because devices are poorly designed, but because security is not systematically integrated into procurement, configuration or lifecycle management. This is especially problematic in sectors such as transport, where devices may remain in service for long periods under variable operational conditions. In railway environments, such vulnerabilities are especially dangerous because many devices are embedded in operational and geographically dispersed settings where compromise may not be immediately visible. A hijacked surveillance device, manipulated sensor or compromised communication gateway may continue functioning outwardly while silently leaking information, transmitting false data or enabling lateral movement across the network. Thus, IoT vulnerabilities in railway systems should be understood not simply as technical weaknesses, but as latent operational and strategic risks

2.1.5 Cybersecurity Solutions for IoT Networks

Addressing IoT vulnerabilities requires a layered, adaptive, context-sensitive cybersecurity strategy. The literature strongly suggests that no single security mechanism is sufficient to protect IoT ecosystems because vulnerabilities may emerge at the device, network, application, organizational levels. Effective protection therefore depends on the coordinated implementation of multiple complementary safeguards.

At the device level, security begins with hardening measures such as changing default credentials, disabling unnecessary services, closing unused ports, enforcing secure configuration baselines. Device identity management is also essential, particularly through methods such as certificate-based authentication, secure onboarding.

At the network level, security is strengthened through segmentation, micro-segmentation, secure gateways, firewalls, intrusion detection, prevention systems, continuous monitoring. These controls help contain compromise, reduce the likelihood that a vulnerable device will provide unrestricted access to critical systems. Increasingly, scholars argue that Zero Trust Architecture is especially suitable for IoT environments because it replaces implicit trust with continuous verification, least-privilege access.

Additional cybersecurity solutions include AI-based anomaly detection, behavioural analytics, firmware integrity verification, automated patch management, secure boot mechanisms. Recent literature on AI-based intrusion detection indicates that intelligent monitoring systems can improve the detection of abnormal traffic, suspicious device behaviour in complex IoT environments. However, the same literature also notes that advanced security tools may be difficult to operationalise in resource-constrained environments due to computational demands, implementation complexity, limited specialist skills.

This limitation is highly relevant to NRZ. While advanced cybersecurity models may appear technically desirable, their practical value depends on affordability, maintainability, compatibility with legacy systems and institutional capacity. Therefore, the most suitable cybersecurity solutions for NRZ are likely to be those that balance technical effectiveness with operational realism

2.1.7 Risk Assessment in IoT Environments

Risk assessment constitutes a foundational discipline in cybersecurity management, providing a structured methodology for identifying, analysing, prioritising threats to information

systems, operational assets. In the context of IoT environments, risk assessment is especially important because the scale, heterogeneity, continuous connectivity of IoT devices create an expansive, dynamic threat landscape that cannot be adequately managed through ad hoc or reactive approaches.

Several internationally recognised risk assessment frameworks are directly relevant to the study of IoT security in railway environments. The NIST Risk Assessment Framework (NIST SP 800-30) provides a systematic process for identifying risk factors, analysing threat likelihood, impact, prioritising risk responses. The NIST Cybersecurity Framework (CSF), which organises cybersecurity activities into five core functions, complements this framework: Identify, Protect, Detect, Respond, Recover.

The ISO/IEC 27001 standard, its companion ISO/IEC 27002 provide a widely adopted information security management system (ISMS) framework that specifies requirements for establishing, implementing, maintaining, continually improving security controls.

For IoT-specific guidance, the European Telecommunications Standards Institute (ETSI) has developed ETSI EN 303 645, a standard that defines cybersecurity provisions for consumer Internet of Things devices. This standard addresses key vulnerability areas including default passwords, vulnerability disclosure, secure update mechanisms, minimal exposed attack surfaces, the protection of personal data.

In the railway domain, the International Electro technical Commission (IEC) has developed IEC 62443, a series of standards addressing cybersecurity for industrial automation, control systems (IACS). Given that railway operational technology systems fall within the scope of industrial control systems, IEC 62443 provides a particularly relevant framework for understanding how network segmentation, access control, system hardening, security level assessments should be implemented in rail environments.

For NRZ, these frameworks are significant because they provide internationally benchmarked reference points against which the institution’s current IoT security posture can be evaluated. The present study draws upon these frameworks to inform both the vulnerability identification process and the development of context-appropriate security recommendations

2.1.8 Established Security Frameworks and Standards

Beyond risk assessment, the broader cybersecurity landscape offers a range of established security frameworks, standards that are directly applicable to IoT environments in critical

infrastructure. The NIST Cybersecurity Framework (CSF) has become one of the most widely referenced guides for organizations seeking to manage, reduce cybersecurity risk. Its fivefunction structure—Identify, Protect, Detect, Respond, Recover—provides a flexible, scalable model that can be adapted to the specific needs of railway institutions operating IoTenabled systems.

The IEC 62443 series of standards is particularly relevant to railway operational technology environments. Originally developed for industrial automation, control systems, IEC 62443 defines requirements for security levels, network segmentation, system hardening, access control, security lifecycle management.

The OWASP Internet of Things Top Ten Project provides a practitioner-oriented guide to the most critical security risks affecting IoT systems. This framework identifies vulnerabilities such as weak or default passwords, insecure network services, insecure ecosystem interfaces, lack of secure update mechanisms, insufficient privacy protection.

These frameworks are important for the present study because they collectively demonstrate that IoT cybersecurity is not an ad hoc activity but a structured, standards-guided discipline. The study draws upon these frameworks to inform the identification and categorisation of vulnerabilities, the evaluation of existing security measures at NRZ, and the development of context-appropriate security recommendations that are grounded in internationally recognised best practices

2.1.6 Conceptual Framework of the Study

Figure 1: Conceptual Framework of the Study

Relationship between IoT Vulnerabilities, Intervening Factors, and Network Security Outcomes at NRZ



Source: Researcher's own construct, informed by literature review (Chapter 2)

Figure 1: Conceptual Framework of the Study: Relationship between IoT Vulnerabilities, Intervening Factors, and Network Security Outcomes at NRZ

The conceptual framework of this study is based on the proposition that the security posture of IoT devices at NRZ is shaped by the interaction between vulnerabilities, security controls and institutional readiness. Weak authentication, poor firmware management, insecure communication protocols, insufficient access control and inadequate monitoring are conceptualised as major exposure factors that increase cyber risk. At the same time, the study recognises that the effectiveness of technical safeguards is influenced by governance structures, staff awareness, policy enforcement and management commitment

The framework therefore positions enhanced network security as a dependent outcome that can be achieved through the coordinated implementation of both technical and organizational measures. Security improvement is expected where encryption, segmentation, patch management, authentication, intrusion detection, policy enforcement and staff training are implemented in a coherent and context-appropriate manner

This conceptual logic reflects contemporary cybersecurity thinking, which increasingly recognises that technological resilience cannot be separated from organizational capacity. It therefore provides an appropriate basis for examining how NRZ can strengthen the resilience of its IoT-enabled operational environment against cyber threats

2.2 Theoretical Framework

A theoretical framework provides the intellectual lens through which a research problem is understood and interpreted. In this study, the theoretical framework is used to explain how security vulnerabilities emerge in IoT-based railway systems and how such vulnerabilities may be managed through appropriate security principles and institutional alignment. Since this study addresses both technical and organizational dimensions of network security, it is necessary to employ theories capable of explaining trust relationships, layered defence and the human-technology interface

Zero Trust Security Theory, Defence-in-Depth Theory, Socio-Technical Theory guide this study. These theories are complementary rather than contradictory, together they provide a strong analytical basis for understanding how network security can be enhanced in IoT devices at the National Railways of Zimbabwe.

2.2.1 Zero Trust Security Theory

Zero Trust Security Theory is founded on the principle that no user, device, application or communication flow should be automatically trusted, regardless of whether it originates from inside or outside the network. Unlike traditional perimeter-based security models, which often assume that internal environments are relatively safe, Zero Trust assumes that threats may emerge from any point within the digital ecosystem. Its core philosophy is often summarised as “never trust, always verify.”

This theory is particularly relevant to IoT environments because connected ecosystems often contain numerous devices with different configurations, capabilities, trust levels and vulnerabilities. In such environments, implicit trust can be highly dangerous. A single compromised device may provide a foothold for broader network compromise if it is allowed unrestricted or poorly validated access

Recent literature on Zero Trust in IoT highlights the importance of device identity verification, least-privilege access, continuous authentication, contextual authorization. These principles are highly relevant to railway environments, where distributed systems, remote operational technologies often interact across multiple trust boundaries.

Applied to NRZ, Zero Trust Theory suggests that every device, user and communication request should be continuously authenticated and authorised before access is granted. This is especially important in railway settings, where even a single compromised sensor, communication node or administrative interface could become a point of entry into wider operational systems

However, it is also necessary to recognise that Zero Trust should not be treated as a universally simple solution. The literature increasingly shows that Zero Trust is not a single product or software package, but a strategic architecture requiring strong identity management, access governance, network visibility, institutional policy discipline. In resource-constrained settings, its implementation may therefore require adaptation rather than direct replication of idealised models.

2.2.2 Defence-in-Depth Theory

Defence-in-Depth Theory is a cybersecurity principle that advocates the use of multiple, overlapping layers of protection rather than reliance on a single control mechanism. The theory is based on the recognition that no individual safeguard can guarantee complete

security. Instead, effective protection is achieved when multiple defences operate together so that the failure of one layer does not immediately result in total compromise.

This theory is particularly valuable in IoT environments because vulnerabilities may exist simultaneously across hardware, firmware, communication protocols, applications, cloud platforms and user access points. In railway environments, these layers may also include physical infrastructure, maintenance interfaces, remote monitoring platforms and operational technology systems

For NRZ, Defence-in-Depth Theory implies that IoT security should not depend on a single tool or isolated technical measure. Rather, protection should be distributed across secure device configuration, authentication, segmentation, encryption, traffic monitoring, policy enforcement, physical safeguards and incident response capability. This is particularly appropriate in mixed environments where some systems may be modern while others remain legacy-based and difficult to secure comprehensively

The practical strength of Defence-in-Depth lies in its realism. It does not assume perfect prevention but instead recognises that vulnerabilities and failures are inevitable. Its emphasis is therefore on resilience, containment and layered resistance. This makes it especially suitable for a critical infrastructure institution such as NRZ, where operational continuity is essential and cyber risk cannot be eliminated

2.2.3 Socio-Technical Theory

Socio-Technical Theory argues that organizational systems are shaped by the interaction between technical structures, human or social elements. It rejects the assumption that technological systems can be understood in isolation from the people, processes, institutions that design, manage, use them. In the context of cybersecurity, this theory is especially important because many security failures arise not only from technical flaws but also from weak governance, poor user behaviour, inadequate training, weak policy enforcement, poor organizational alignment.

Applied to IoT security at NRZ, Socio-Technical Theory suggests that network security cannot be achieved solely through devices, encryption and software controls. Even technically secure systems may fail if users share credentials, neglect update procedures, connect unauthorised devices or lack awareness of cyber threats. Likewise, management decisions relating to procurement, budgeting, maintenance, staffing and policy enforcement can significantly

influence the institution's security posture

This theory is highly relevant because it broadens the scope of the study beyond technological vulnerability to include organizational readiness, institutional culture, staff competence and governance maturity. It helps explain why some institutions remain vulnerable despite the availability of technical solutions and why sustainable cybersecurity depends on administrative commitment as much as technological deployment

In the case of NRZ, this is particularly significant because railway institutions often operate within complex operational cultures where modernization may occur unevenly and security responsibilities may not always be clearly defined. Socio-Technical Theory therefore reinforces the argument that enhancing IoT network security requires both technological controls and institutional transformation

2.2.4 Relevance of the Theories to Study

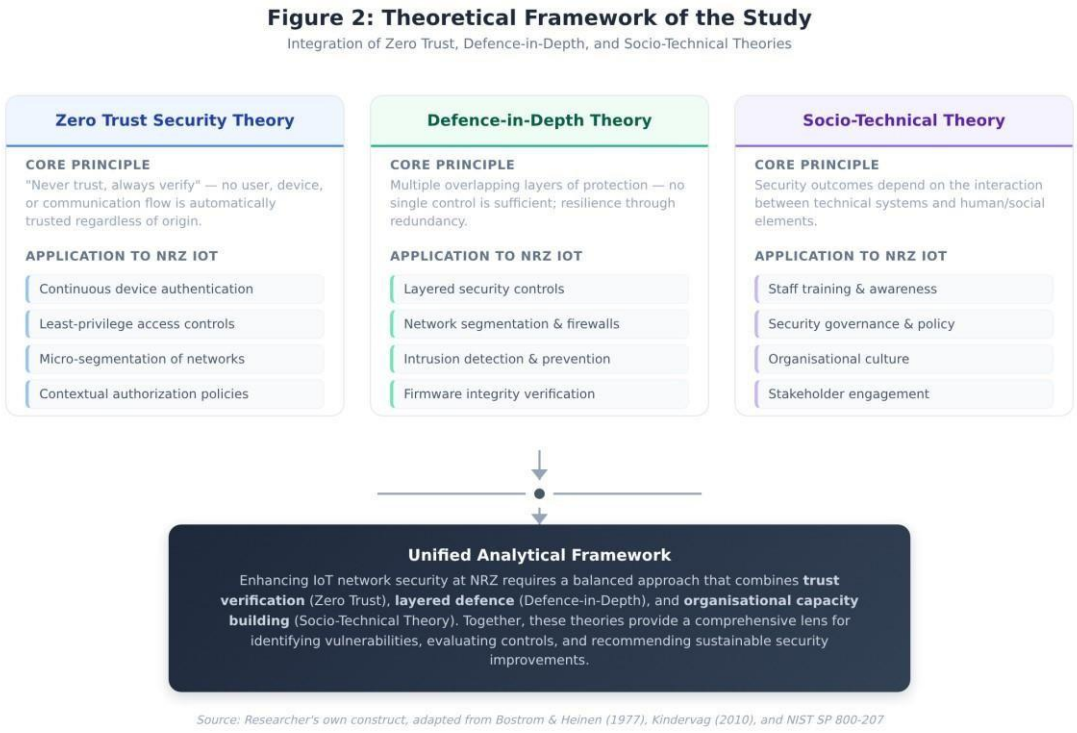


Figure 2: Theoretical Framework of the Study: Integration of Zero Trust, Defence-in-Depth, and Socio-Technical Theories

The three theories guiding this study complement one another and collectively provide a robust analytical foundation. Zero Trust Security Theory explains why trust assumptions in IoT ecosystems are dangerous and why continuous verification is necessary. Defence-in-Depth Theory explains why security must be implemented through multiple overlapping

layers rather than isolated tools. Socio-Technical Theory explains why technical protection alone is insufficient without supportive governance, staff awareness and institutional capacity Together, these theories support the central argument of this study: that enhancing network security in IoT devices at NRZ requires a balanced understanding of trust, layered defense and organizational behaviour. They also ensure that the study does not reduce cybersecurity to purely technical intervention, but instead interprets it as a strategic, operational and institutional challenge

2.3 Empirical Evidence

Empirical evidence refers to findings derived from previous studies, systematic reviews, case analyses and documented observations relevant to the research problem. In this study, empirical evidence is reviewed to examine what is already known about IoT vulnerabilities, networkbased attacks, cybersecurity solutions and digital risk in railway and transport environments

2.3.1 Empirical Studies on IoT Security Vulnerabilities

A substantial body of empirical literature demonstrates that IoT devices are disproportionately vulnerable when compared to conventional computing systems. Studies consistently show that many IoT devices are deployed with default passwords, insecure interfaces, poor update mechanisms, weak authentication, inadequate encryption. These weaknesses are often compounded by long device lifecycles, poor visibility into device security status, making effective maintenance, risk management difficult.

Studies have documented recurring weaknesses such as insecure authentication, poor software integrity validation, insufficient logging, weak communication protocols, exposed interfaces. These findings are important because they indicate that IoT vulnerabilities are not merely isolated technical flaws but structural features of the wider IoT ecosystem.

A critical issue emerging from the literature is that insecurity is often normalized through deployment practices that prioritise operational functionality over cyber resilience. In many cases, institutions inherit insecure technologies not simply because devices are poorly designed, but because security is not systematically integrated into procurement, configuration or lifecycle management.

For railway institutions such as NRZ, these findings are directly relevant because device vulnerabilities may affect not only data security but also the integrity and reliability of

operational information. The empirical literature therefore strongly supports the argument that IoT device vulnerabilities constitute a foundational challenge requiring institution-specific attention

2.3.2 Empirical Studies on Network-Based IoT Attacks

A second stream of empirical literature focuses on the specific forms of attack targeting IoT networks, connected devices. Commonly documented attacks include Denial of Service (DoS), Distributed Denial of Service (DDoS), spoofing, eavesdropping, man-in-the-middle attacks, replay attacks, malware injection, botnet recruitment.

IoT environments are especially vulnerable because of their continuous connectivity, the increasing complexity of attack detection. One of the most important observations from this literature is that attackers often target the communication pathways between devices, control systems rather than the devices alone.

In railway environments, the implications of such attacks are considerable. If a communication link between a sensor and a central monitoring platform is intercepted or manipulated, the resulting false or delayed data may affect maintenance decisions, surveillance reliability or operational visibility. The empirical literature therefore reinforces the importance of a networkcentric security approach in railway IoT systems rather than a purely device-centric one

2.3.3 Empirical Studies on IoT Security in Transport and Railway Systems

The transport, railway sectors have attracted increasing scholarly attention due to the growing digitization of critical mobility infrastructure. Railway-specific literature suggests that onboard systems, wayside devices, trackside sensors, communication interfaces, remote diagnostics platforms are among the most exposed components in digitally modernising rail environments This creates a persistent structural challenge: the coexistence of old and new technologies within the same operational ecosystem. For institutions such as NRZ, this is likely to be especially relevant. The empirical railway literature strongly supports the view that generic enterprise cybersecurity assumptions are insufficient for understanding digital risk in railway institutions. A more context-sensitive and operationally grounded approach is required

2.3.4 Empirical Studies on IoT Security Controls and Mitigation Strategies

A broad range of empirical studies has examined strategies for mitigating IoT security risks. Commonly recommended controls include strong authentication, certificate-based device identity, encryption, network segmentation, secure gateways, patch management, intrusion detection systems, continuous monitoring.

Mallidi, Ramisetty demonstrate that AI-based intrusion detection systems are increasingly being explored as tools for identifying malicious traffic, abnormal behaviour in IoT environments. Zero Trust-based models are increasingly promoted as promising for IoT because they reduce dependence on implicit trust, instead enforce continuous verification, least-privilege access.

For NRZ, this body of evidence suggests that cybersecurity controls should be assessed not only according to technical sophistication but also according to feasibility, affordability, compatibility and maintainability

2.3.5 Empirical Evidence from Developing Countries and Similar Contexts

Although IoT security research has expanded significantly, much of the literature remains concentrated in technologically advanced settings. Evidence from broader critical infrastructure studies suggests that institutions in developing countries frequently face challenges related to underinvestment in cybersecurity, inconsistent policy enforcement, weak maintenance capacity, limited asset visibility, dependence on mixed legacy systems. In the African context, studies on cybersecurity in critical infrastructure highlight persistent challenges including limited regulatory frameworks, insufficient cybersecurity budgets, low security awareness among operational staff, dependence on foreign technology vendors, weak incident response capabilities.

Zimbabwe's cybersecurity landscape reflects many of these broader African challenges. Zimbabwe-specific scholarship on IoT security in railway environments remains extremely limited, and this underrepresentation significantly weakens the direct applicability of existing global literature. This gap strengthens the justification for the present study

2.4 Research Gap Analysis

A research gap analysis identifies areas where existing literature is insufficient, inconsistent, overly generalised or lacking in contextual relevance. Although the literature on IoT cybersecurity has expanded considerably, several significant gaps remain

2.4.1 Contextual Gap

A major contextual gap exists in the dominance of literature focused on smart homes, healthcare, manufacturing, smart cities, generalized industrial IoT environments. Railway systems differ from ordinary enterprise environments because they combine digital systems with dispersed physical infrastructure, safety-sensitive processes, long equipment lifecycles, geographically distributed operational assets.

2.4.2 Geographical Gap

Much of the empirical evidence on IoT security originates from countries with more advanced digital ecosystems, stronger regulatory frameworks, higher levels of cybersecurity maturity. Zimbabwe is particularly underrepresented in the literature on IoT security in critical infrastructure.

2.4.3 Methodological Gap

A methodological gap is also evident in the dominance of simulations, laboratory experiments, architecture proposals, conceptual reviews, algorithmic evaluations. There remains comparatively limited research using organizational case study approaches to investigate how IoT vulnerabilities are perceived, prioritised, managed within actual institutions.

2.4.4 Practical and Implementation Gap

A substantial proportion of the literature recommends advanced solutions such as blockchainbased trust models, AI-powered anomaly detection, zero-trust overlays, and sophisticated monitoring architectures. While technically impressive, these recommendations are often presented in idealised terms with limited discussion of implementation feasibility in resource-constrained institutions.

2.4.5 Policy and Governance Gap

Much of the existing IoT security literature is heavily technical, focusing on encryption, protocols, detection models, architectural design. The literature has not sufficiently integrated governance dimensions into analyses of railway IoT security in developing-country settings.

2.5 Summary

This chapter reviewed literature relevant to the study of network security in IoT devices within the context of the National Railways of Zimbabwe. The chapter identified significant contextual, geographical, methodological, practical and governance-related gaps in the existing literature. These gaps collectively justify the present study by demonstrating that while IoT cybersecurity is widely discussed in general terms, there remains limited context-specific knowledge on how network security can be enhanced for IoT devices within Zimbabwe's railway sector. The next chapter therefore presents the research methodology adopted to investigate these issues in a systematic and contextually grounded manner

CHAPTER 3

RESEARCH METHODOLOGY

3.0 Introduction

This chapter presents the methodological blueprint underpinning the investigation of IoT security vulnerabilities within the National Railways of Zimbabwe (NRZ). It translates the theoretical and conceptual foundations established in Chapter 2 into a practical, step-by-step research design that directly addresses each research objective identified in Chapter 1. The methodology is deliberately structured to bridge the methodological and practical gaps highlighted in the literature review, particularly the scarcity of organisational case studies focused on IoT security in critical infrastructure within developing nations. By adopting a mixed-methods approach anchored in a pragmatist research philosophy, this chapter articulates the research design, sampling strategy, data collection instruments, data quality assurance mechanisms, and analytical techniques that collectively ensure the rigour, credibility, and relevance of the study. Each methodological choice is justified in terms of its alignment with the study objectives, its capacity to capture both the technical and socio-technical dimensions of IoT security, and its adherence to the delimitations defined in Section 1.10.

The ensuing sections proceed systematically through the research philosophy, research design, research approach, target population, sampling techniques, data collection methods, data quality assurance, data analysis techniques, ethical considerations, and a concluding summary. Together, these components form an integrated framework designed to produce actionable findings that will inform the development of a context-appropriate IoT security framework for the NRZ.

3.1 Research Philosophy

The selection of a research philosophy is fundamental because it shapes the researcher's ontological, epistemological assumptions, thereby influencing every subsequent

methodological decision. For this study, Pragmatism has been adopted as the overarching philosophical stance. Pragmatism, as articulated by scholars such as rejects the rigid dichotomy between positivism, interpretivism. Instead, it focuses on what works in practice, prioritising the research question over adherence to a single worldview. This philosophical orientation is particularly appropriate for the present study for several compelling reasons.

Pragmatism is appropriate for this study for three key reasons. First, the research requires both quantitative vulnerability measurement and qualitative understanding of governance and human factors; pragmatism explicitly supports this integration. Second, the complex institutional realities of IoT security in developing-country critical infrastructure demand an approach that neither reduces these dynamics to mere variables (positivism) nor sacrifices generalisability (interpretivism). Pragmatism resolves this tension by drawing on the strengths of both paradigms.

Third, the Socio-Technical Theory that underpins this study inherently requires a multiperspective approach. IoT security is not merely a technical problem; it is a sociotechnical challenge involving people, processes, technology interacting within a complex organisational system. Pragmatism provides the philosophical flexibility to examine these interactions from multiple angles, using whichever methods are most suited to each aspect of the investigation. In terms of epistemology, this study adopts a critical realist position within the pragmatist framework, acknowledging that while there is an objective reality of IoT vulnerabilities (vulnerable systems can be empirically identified), our understanding of that reality is shaped by the social, organisational, and political contexts in which those vulnerabilities exist. This stance justifies the use of both quantitative vulnerability assessments and qualitative explorations of governance and policy frameworks, recognising that neither data type alone can fully capture the phenomenon under investigation.

Table 3.1: Summary of Research Philosophical Positions

Dimension	Position	Justification
Philosophy	Pragmatism	Supports mixed methods; prioritises research questions over paradigm loyalty
Ontology	Critical Realism	Acknowledges objective vulnerabilities while recognising socially constructed governance realities
Epistemology	Mixed (pluralistic)	Integrates positivist measurement with interpretivist understanding

Axiology	Value-laden inquiry	Researcher acknowledges role in interpreting findings within institutional context

3.2 Research Design

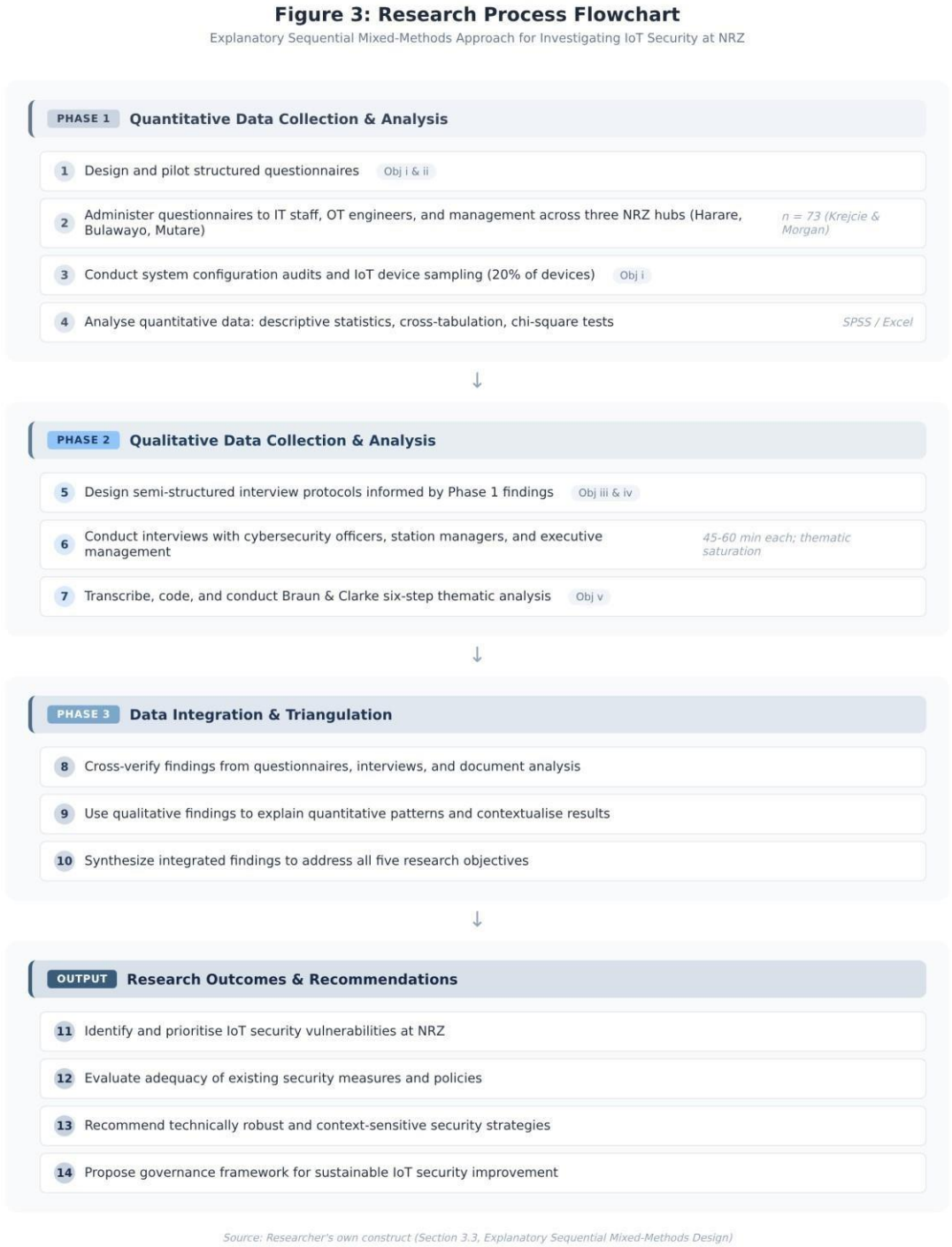


Figure 3: Research Process Flowchart: Explanatory Sequential Mixed-Methods Approach for Investigating IoT Security at NRZ

This study employs a Case Study Research Design, specifically a single, in-depth case study of the National Railways of Zimbabwe. The case study design was selected after careful consideration of alternative designs, including surveys, experiments, grounded theory. As argues, the case study is the preferred design when the research questions are of the "how", "why" variety, when the researcher has little control over behavioural events, when the phenomenon under investigation is occurring within its real-life context. All three conditions apply to this study: the research seeks to understand how, why IoT vulnerabilities exist at the NRZ (Research Questions 1-5), the researcher cannot manipulate the NRZ's operational systems (non-experimental delimitation), IoT security at the NRZ is inherently embedded in the organisation's unique operational, governance, resource context.

Additionally, this study adopts a Cross-sectional Design, as specified in the delimitations (Section 1.10). The cross-sectional approach captures a snapshot of the current state of IoT vulnerabilities, governance practices, and security awareness at the NRZ at a single point in time. While this limits the ability to track changes over time, it is appropriate for the study's objectives, which focus on assessing the current vulnerability landscape rather than measuring longitudinal trends. The cross-sectional design also aligns with the pragmatic constraints of conducting research within an operational critical infrastructure organisation, where extended longitudinal access may be impractical.

To strengthen the validity, depth of the single case study, this research adopts recommendation of employing multiple data sources (questionnaires, interviews, document analysis), multiple units of analysis (IT systems, OT systems, governance structures) within the NRZ. This embedded case study approach ensures that the findings are not dependent on a single data source or perspective, thereby enhancing the overall rigour of the investigation.

3.3 Research Approach

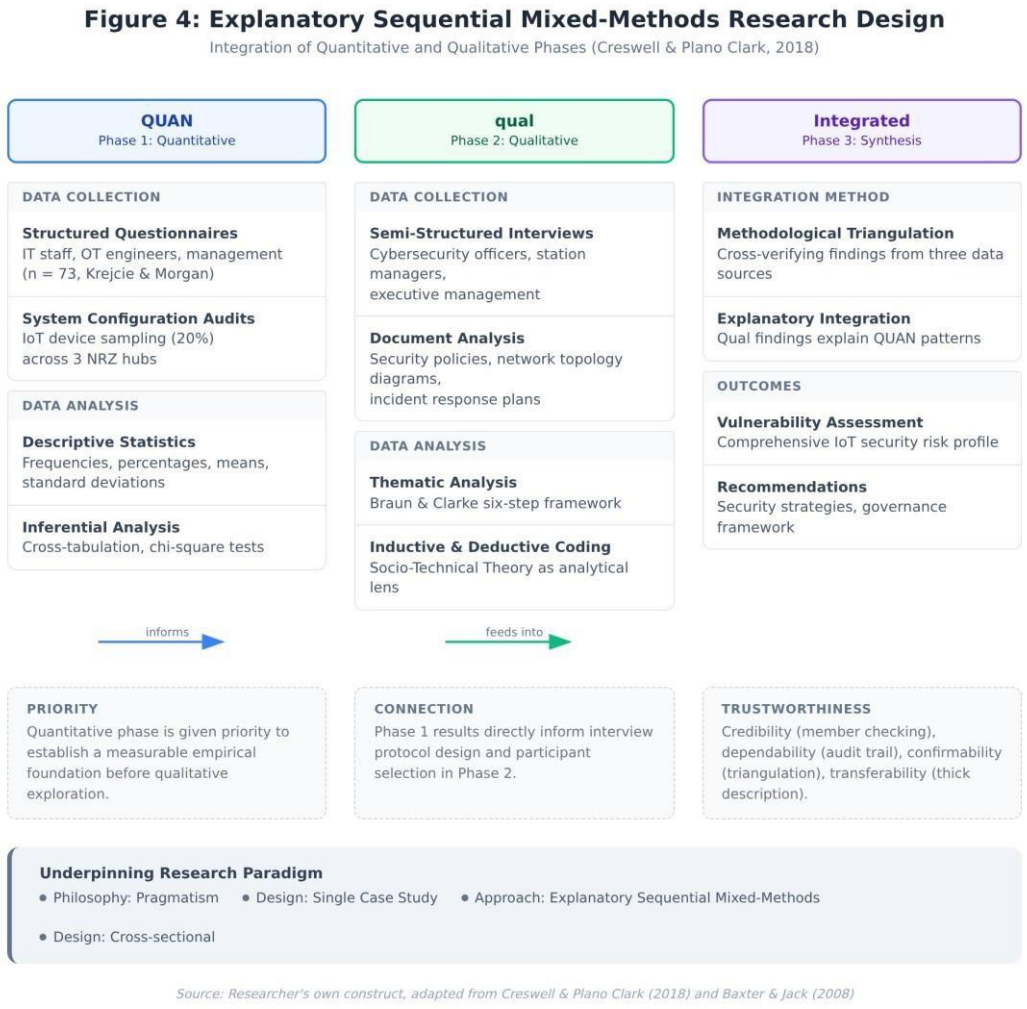


Figure 4: Explanatory Sequential Mixed-Methods Research Design: Integration of Quantitative, Qualitative Phases

This study employs an Explanatory Sequential Mixed-Methods Approach, as first defined in the delimitations (Section 1.10), further justified here. In this approach, quantitative data is collected, analysed first, followed by qualitative data collection, analysis, with the qualitative phase designed to explain, elaborate, or contextualise the quantitative findings . This approach was selected over the alternative Convergent Parallel design (where quantitative, qualitative data are collected simultaneously) for three principal reasons.

First, assessing the technical nature and severity of IoT vulnerabilities (Research Objective i) requires a structured, measurable foundation before qualitative exploration can meaningfully occur. The quantitative phase establishes the empirical baseline, while the qualitative phase provides the contextual depth needed to understand governance, resource, and institutional

dimensions. Second, the NRZ context dictates a practical sequencing logic, as organisational access to critical infrastructure typically begins with broader surveys before progressing to indepth interviews.

Third, explanatory sequential design supports natural integration at the interpretation stage, where qualitative findings explain why certain quantitative patterns emerged. For example, if survey data reveals that 70% of IoT devices operate with default credentials, qualitative interviews with management can explore the governance and resource allocation decisions behind this finding. This directly addresses Research Objectives iii, iv, and v.

Table 3.2: Explanatory Sequential Mixed-Methods Design Phases

Phase	Data Type	Method	Primary Objective Addressed
Phase 1: Quantitative	Quantitative	Structured questionnaires, system configuration audits	Objectives i, ii
Phase 2: Qualitative	Qualitative	Semi-structured interviews, document analysis	Objectives iii, iv, v
Phase 3: Integration	Mixed	Cross-case synthesis, framework development	All objectives (proposed framework)

3.4 Target Population and Study Area

The study area is confined to the National Railways of Zimbabwe (NRZ) operational hubs, specifically Harare (headquarters and main marshalling yard), Bulawayo (the second-largest operations centre), and Mutare (a key eastern corridor station). These three hubs were selected because they represent the most IoT-intensive operational environments within the NRZ network, encompassing trackside monitoring sensors, CCTV surveillance systems, SCADAbased signalling infrastructure, and communication networks. This geographic delimitation aligns with the study's scope as defined in Section 1.10 (iv) and ensures that the research remains logistically feasible while covering the most relevant operational contexts.

The target population for this study is directly drawn from the categories identified in Section 1.10 (v) and encompasses the following stakeholder groups within the NRZ. IT Personnel comprise staff responsible for managing the NRZ's information technology infrastructure, including network administration, server management, and IoT device provisioning. This group is essential for understanding the technical configuration, update practices, and security awareness that directly impact IoT vulnerability levels.

Operational Technology (OT) Engineers include engineers responsible for trackside monitoring, signalling systems, and SCADA infrastructure. OT engineers operate at the intersection of physical railway operations and digital control systems, making their perspectives critical for understanding how IoT devices are integrated into safety-critical operational processes. Their insights are particularly valuable for identifying vulnerabilities that arise from the convergence of IT and OT networks, a well-documented security challenge in industrial IoT environments.

Cybersecurity Officers (where applicable within the NRZ organisational structure) are individuals with formal or informal responsibility for overseeing the organisation's cybersecurity posture. Even where a dedicated cybersecurity function does not exist, individuals who perform security-related duties as part of their broader IT or management responsibilities are included in this category. Their perspectives illuminate the governance structures, policy frameworks, and resource constraints that shape IoT security at the institutional level.

Station Managers and Key Executive Management comprise the senior leadership responsible for digital transformation, strategic planning, and resource allocation within the NRZ. This group is critical for understanding the institutional decision-making processes that determine investment in IoT security, the prioritisation of cybersecurity relative to operational demands, and the organisational culture surrounding technology adoption and risk management.

Table 3.3: Target Population and Data Collection Methods

Stakeholder Group	Role	Estimated Population	Data Collection Method
IT Personnel	Network, server, IoT management	30–50	Questionnaire, audit
OT Engineers	Trackside, SCADA, signalling	40–60	Interview, document analysis
Cybersecurity Officers	Security oversight (formal/informal)	5–10	Questionnaire, audit
Station Managers	Operational hub leadership	10–15	Interview, document analysis
Executive Management	Digital transformation, strategy	5–8	Interview

3.5 Sampling Techniques and Sample Size

Given the heterogeneous nature of the target population and the dual focus of the study (technical vulnerability assessment and governance analysis), a combination of purposive and stratified sampling techniques is employed for human participants, while systematic and cluster sampling are applied for IoT device assessment.

3.5.1 Human Participant Sampling

Purposive Sampling is used to select individuals with specific, demonstrable knowledge of IoT systems, network infrastructure, cybersecurity practices within the NRZ. This non-probability technique is appropriate for qualitative research components because it targets informationrich cases rather than statistically representative samples . For the qualitative phase (semistructured interviews), purposive sampling ensures that interviewees possess the depth of knowledge needed to provide meaningful insights into governance gaps, policy challenges, resource constraints.

Stratified Random Sampling is used for the quantitative phase (structured questionnaires) to ensure proportional representation across the three primary organisational strata: IT staff, OT engineers, and management. Each stratum is treated as a distinct sub-population, and random selection within each stratum ensures that the survey results are representative of the broader NRZ workforce. The stratification is essential because these groups have fundamentally different interactions with IoT systems, different levels of technical expertise, and different perspectives on security priorities.

3.5.2 IoT Device Sampling

For the technical vulnerability assessment, a systematic sampling approach is applied to IoT devices across the three operational hubs. Specifically, 20% of trackside monitoring sensors (selected at regular intervals along track segments), 30% of CCTV cameras (selected systematically across station premises), and 25% of SCADA-connected devices will be assessed for known vulnerabilities, including default configurations, outdated firmware, unencrypted communications, and exposed management interfaces. The varying sampling percentages reflect the differing risk profiles and population sizes of each device category.

3.5.3 Sample Size Justification

For the quantitative component, the sample size is determined using the formula for finite populations. Given the estimated total population of 90–143 across all stakeholder groups, the formula yields a minimum sample size of approximately 73 respondents at a 95% confidence level, a 5% margin of error. To account for potential non-response, incomplete questionnaires, the study will distribute 100 questionnaires (approximately 40 to IT staff, 40 to OT engineers, 20 to management), targeting a final usable response rate of at least 73.

For the qualitative component (semi-structured interviews), the sample size is guided by the principle of thematic saturation (Guest, Bunce, and Johnson, 2006). Data collection will continue until no new themes or insights emerge from additional interviews. Based on similar studies in the IoT security domain and the relatively specialised nature of the target population, saturation is anticipated after 12–18 interviews across the cybersecurity officers, station managers, and executive management strata.

3.6 Data Collection Methods and Instruments

Three complementary data collection methods are employed, each aligned with specific research objectives and the corresponding phase of the explanatory sequential design.

3.6.1 Structured Questionnaires (Quantitative)

A self-administered structured questionnaire is the primary instrument for Phase 1, designed to address Research Objectives i and ii. The questionnaire comprises four sections. Section A: Demographic Information captures the respondent's department (IT, OT, Management), years of experience, highest level of education, and role within the NRZ. Section B: IoT Awareness and Knowledge uses a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree) to measure respondents' awareness of IoT devices within their operational environment, their understanding of IoT-specific security risks, and their familiarity with the NRZ's current IoT security policies.

Section C: Current Security Practices assesses the perceived adequacy of existing security measures, the frequency of firmware and software updates, the use of authentication mechanisms, and the implementation of network segmentation for IoT devices. Section D: Risk Perception and Training measures respondents' perception of the likelihood and

potential impact of IoT-related security incidents, as well as their exposure to cybersecurity training programmes.

3.6.2 Semi-Structured Interviews (Qualitative)

Semi-structured interviews form the core of Phase 2, targeting cybersecurity officers, station managers, and executive management (Research Objectives iii, iv, and v). The interview protocol consists of open-ended questions designed to explore governance structures, policy gaps, resource constraints, institutional challenges, and feasible solutions for IoT security improvement. Key questions include: What governance structures currently oversee IoT security? What policy gaps exist in the current cybersecurity framework? What resource constraints hinder the implementation of robust IoT security measures? What feasible solutions would be appropriate given the NRZ's operational and financial context?

Each interview is expected to last 45–60 minutes and will be audio-recorded with the participant's consent, then transcribed verbatim for thematic analysis. The semi-structured format allows the interviewer to probe emerging themes and follow the participant's line of reasoning while maintaining consistency across interviews through a standardised question guide.

3.6.3 Document Analysis and System Configuration Audits (Technical)

The third data collection method involves the systematic review of NRZ security policies, network topology diagrams, IoT device inventories, and incident response plans (where available). This document analysis provides an objective baseline against which survey responses and interview narratives can be triangulated. Additionally, non-intrusive system configuration audits are conducted on sampled IoT devices to identify default credentials, outdated firmware versions, unencrypted communication protocols, and exposed management interfaces. It is important to note that these audits are passive observations only; no active penetration testing, vulnerability exploitation, or any form of "hacking" is conducted, in strict adherence to the ethical delimitations specified in Section 1.10 (vi).

3.7 Data Quality and Trustworthiness

Ensuring the quality and trustworthiness of research findings is paramount for any scholarly investigation. Given the mixed-methods design, data quality is addressed through distinct

strategies for the quantitative and qualitative components, unified by the overarching principle of methodological triangulation.

3.7.1 Quantitative Data Quality

Pre-testing and Piloting: The structured questionnaire will be piloted with a small group of 5–8 NRZ staff members who are not part of the final sample. The pilot assesses question clarity, instructions comprehension, completion time, and technical accuracy. Feedback from the pilot is used to refine the instrument before full-scale deployment.

Internal Consistency: Cronbach's Alpha coefficient is calculated for each multi-item scale within the questionnaire to ensure internal consistency reliability. A threshold of 0.70 or above is considered acceptable, indicating that the items within each scale are measuring the same underlying construct.

Construct Validity: Content validity is established through expert review by two academic supervisors and one industry practitioner with experience in IoT security. The experts assess whether the questionnaire items adequately cover the domains of interest (IoT awareness, security practices, risk perception) and whether the items are unambiguous and appropriately worded for the NRZ context.

3.7.2 Qualitative Data Trustworthiness

The trustworthiness of qualitative data is evaluated using four criteria. Credibility is established through member checking, where interview transcripts are shared with participants for verification, correction, peer debriefing, where a colleague reviews the analysis process, challenges the researcher's interpretations. Transferability is supported by providing thick descriptions of the NRZ context, including organisational structure, resource environment, operational characteristics, enabling readers to assess the applicability of findings to other similar settings.

Dependability is ensured through a comprehensive audit trail documenting all research decisions, methodological adaptations, and analytical procedures. This trail includes field notes, interview memos, coding decisions, and reflexive journal entries. Confirmability is strengthened through researcher reflexivity, whereby the researcher consciously examines and documents their own assumptions, biases, and positionality relative to the study context. An audit trail and reflexive journal serve as the primary mechanisms for demonstrating confirmability.

3.7.3 Triangulation

The ultimate quality assurance mechanism for this study is methodological triangulation, which involves cross-verifying findings from the three data sources (questionnaires, interviews, and document analysis/audits). Convergence of findings across these sources strengthens confidence in the validity of the results, while divergence prompts deeper investigation and richer analysis. For example, if survey data indicates that 40% of staff have never received cybersecurity training, but interview data reveals that training was conducted irregularly and only for IT staff, the triangulated finding provides a more nuanced and accurate picture of the actual training gap. This multi-source approach directly addresses the methodological gap identified in Chapter 2, where studies typically rely on a single data source.

3.8 Data Analysis Techniques

3.8.1 Quantitative Analysis

Quantitative data from the structured questionnaires and system configuration audits are analysed using descriptive statistics. Frequencies, percentages, means, and standard deviations are computed to characterise the distribution of IoT vulnerabilities, security awareness levels, and current practice patterns across the NRZ. These descriptive measures directly address Research Questions 1 and 2, which focus on the nature, prevalence, and severity of IoT vulnerabilities and the level of security awareness among staff. Data analysis is performed using SPSS (Statistical Package for the Social Sciences) version 27, with supplementary analysis in Microsoft Excel for graphical representation.

Cross-tabulation and chi-square tests are employed where appropriate to examine associations between organisational strata (IT vs. OT vs. Management) and key variables such as security awareness, training exposure, and risk perception. These inferential analyses provide deeper insight into whether significant differences exist between stakeholder groups, informing the targeted recommendations that will form part of the proposed security framework.

3.8.2 Qualitative Analysis

Qualitative data from semi-structured interviews is analysed using Thematic Analysis, following the six-step framework developed by . The six steps are: (1) familiarisation with the data through repeated reading of transcripts; (2) generation of initial codes identifying

recurring patterns, concepts; (3) searching for themes by collating related codes into broader thematic categories; (4) reviewing themes against the coded data, the entire dataset to ensure coherence, distinctiveness; (5) defining, naming themes to capture their essence, scope;, (6) producing the final analytical narrative that integrates themes into a coherent story addressing Research Questions 4, 5.

The thematic analysis is conducted both inductively (allowing themes to emerge from the data) and deductively (using the Socio-Technical Theory framework and the research objectives as analytical lenses). This hybrid approach ensures that the analysis is both grounded in the participants' experiences and theoretically informed. NVivo qualitative data analysis software is used to manage the coding process, facilitate systematic theme identification, and maintain an auditable record of all analytical decisions.

3.8.3 Integration of Quantitative and Qualitative Findings

The integration phase follows the explanatory sequential design's logic. Quantitative findings are presented first, providing the empirical landscape of IoT vulnerabilities and awareness levels. Qualitative findings are then woven in to explain the "why" behind the quantitative patterns. For instance, if the quantitative data reveals a high prevalence of default credentials across IoT devices, the qualitative data is examined for themes related to governance gaps, resource constraints, or policy deficiencies that explain this finding. The integrated results form the evidentiary basis for the proposed IoT security framework (Research Objective v), which is developed by synthesising the technical vulnerability data, organisational governance insights, and feasible solutions identified through the mixed-methods analysis.

3.9 Ethical Considerations

Research ethics are of paramount importance in this study, particularly given the "Limited Access to Sensitive Data" limitation noted in Section 1.9 and the critical infrastructure nature of the NRZ. The following ethical safeguards are implemented to protect both the institution and individual participants.

Institutional Clearance: Formal written approval is obtained from the NRZ senior management and the relevant Ministry (Ministry of Transport and Infrastructural Development) prior to the commencement of any data collection activities. This clearance outlines the scope of the research, the data to be collected, the measures taken to protect

sensitive information, and the obligations of both the researcher and the institution. No data collection, including surveys, interviews, or system audits, commences until written clearance is received and all conditions are satisfied.

Informed Consent: All interview participants receive a detailed information sheet explaining the purpose of the study, the nature of their participation, the expected duration of the interview, their right to withdraw at any time without consequence, and how their data will be used and stored. Written informed consent is obtained from each participant before the interview begins. For questionnaire respondents, the cover page of the questionnaire serves as the informed consent form, and submission of the completed questionnaire constitutes implied consent. Anonymity and Confidentiality: All individual responses are anonymised through the use of unique participant codes. No personally identifiable information (names, employee numbers, or specific job titles) is included in the research outputs. Interview transcripts are stored on an encrypted, password-protected device accessible only to the researcher and the academic supervisors. All digital records are permanently deleted five years after the completion of the study, in accordance with institutional data retention policies. Responsible Disclosure of Vulnerabilities: This study adopts a responsible disclosure protocol for any critical infrastructure vulnerabilities discovered during system configuration audits. Discovered vulnerabilities are communicated exclusively to the NRZ management through a confidential report, with recommendations for remediation. Under no circumstances are specific technical vulnerabilities, device configurations, or network topology details published in the public domain in a manner that could expose the NRZ to immediate security risk. This ethical commitment reflects both the researcher's professional obligations and the study's nonexperimental delimitation, ensuring that the research contributes to strengthening, not compromising, the NRZ's security posture.

3.10 Summary

This chapter presented the research methodology for investigating IoT security vulnerabilities at the National Railways of Zimbabwe. Grounded in pragmatism, the study employs an explanatory sequential mixed-methods approach within a single case study design. Data is collected through questionnaires, semi-structured interviews, and document analysis, and analysed using descriptive statistics and thematic analysis. Ethical safeguards are embedded throughout the research process.

The target population encompasses IT personnel, OT engineers, cybersecurity officers, station managers, and executive management across three NRZ operational hubs (Harare, Bulawayo, and Mutare). Data is collected through structured questionnaires, semi-structured interviews, and document analysis and system configuration audits, with purposive and stratified random sampling ensuring representative and information-rich participant selection. Data quality is assured through pre-testing, Cronbach's Alpha reliability testing, construct validity review, thematic trustworthiness criteria (credibility, transferability, dependability, confirmability), and methodological triangulation across all three data sources.

Quantitative data is analysed using descriptive statistics and cross-tabulation, while qualitative data is subjected to Braun and Clarke's six-step thematic analysis framework. The integrated findings from both phases form the evidentiary foundation for the proposed IoT security framework. Ethical safeguards, including institutional clearance, informed consent, anonymity, and responsible disclosure, are embedded throughout the research process. This methodological design ensures that the study produces rigorous, credible, and actionable findings that directly address all five research objectives, setting the stage for the data presentation and analysis in Chapter 4.

CHAPTER 4

SYSTEM IMPLEMENTATION AND RESULTS

4.0 Introduction

The implementation details and results of the Network Infrastructure Security Assessment and Action Platform (NISAAP), which was developed as a practical intervention to address the IoT security vulnerabilities identified within the National Railways of Zimbabwe (NRZ). The system was designed as a direct response to the research objectives outlined in Chapter 1, particularly Objectives iv and v, which called for the development of technically robust and operationally feasible network security strategies and the establishment of a framework for continuous monitoring of IoT device security.

The chapter proceeds systematically through the system architecture, technology stack, key module implementations, and the results obtained from deploying the system within the NRZ operational environment. Each section aligns the implemented features with the theoretical foundations established in Chapter 2, specifically the Zero Trust Security Theory, DefenceinDepth Theory, and Socio-Technical Theory, demonstrating how these theoretical principles were translated into functional system capabilities. The chapter also presents quantitative and qualitative results derived from the system's operational data, including vulnerability statistics, device risk distributions, and security assessment outcomes.

It is important to note that the NISAAP platform was not developed in isolation but rather in close collaboration with the NRZ IT Department, which provided access to the network infrastructure, device inventories, and operational insights necessary for realistic system configuration and testing. The seed data loaded into the system reflects the actual IoT device landscape across NRZ's three operational hubs in Harare, Bulawayo, and Mutare, ensuring that the results presented are contextually relevant and operationally meaningful.

4.1 System Architecture

The NISAAP platform adopts a modern three-tier architecture comprising a presentation layer, an application layer, and a data layer. This architectural design was selected because it aligns with the Defence-in-Depth Theory by providing multiple layers of protection, with security controls implemented at each tier rather than relying on a single perimeter defence. The architecture is illustrated in Figure 4-1 below.

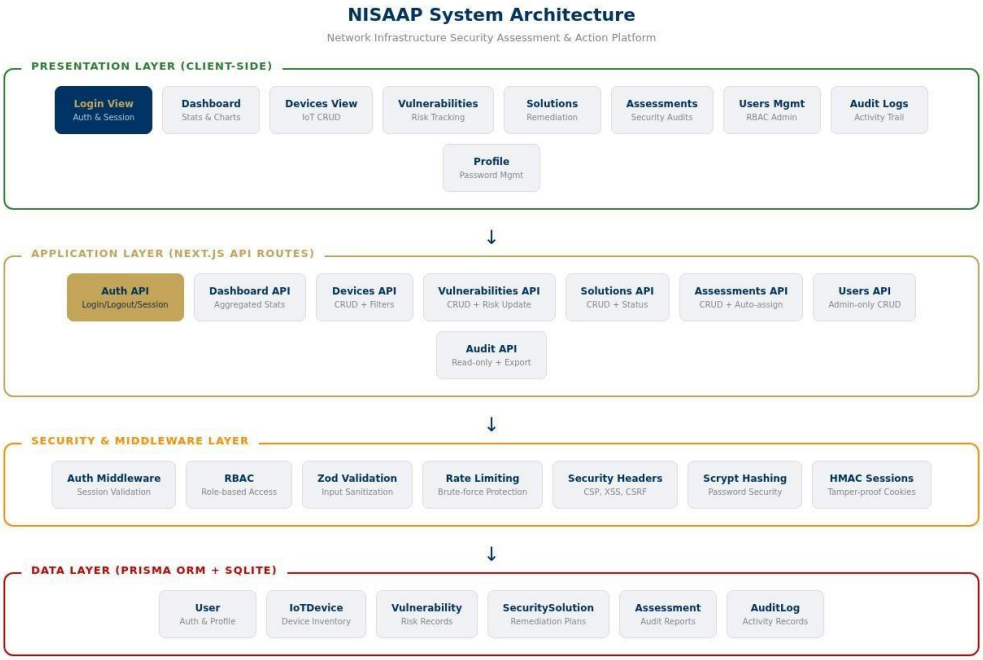


Figure 4-1: NISAAP System Architecture Diagram

4.1.1 Presentation Layer

The presentation layer is built as a Single Page Application (SPA) using React 19 and Next.js 16, with Tailwind CSS 4 providing responsive styling and the shadcn/ui component library delivering a consistent, accessible user interface. The SPA architecture was chosen for its ability to provide a fluid, desktop-application-like experience that minimises page reloads, which is particularly important for security monitoring dashboards where real-time responsiveness is critical. The presentation layer includes eight primary views: the Login View, Dashboard View, IoT Devices View, Vulnerabilities View, Security Solutions View, Assessments View, User Management View, and Audit Logs View.

The user interface is themed using the NRZ corporate colour palette, with navy blue (#003366) as the primary colour and gold (#C5A55A) as the accent colour, ensuring institutional branding consistency. The interface also supports dark mode for extended monitoring sessions, reflecting consideration for the operational context in which security analysts may work during night shifts. Figure 4-2 shows the NISAAP login interface with its branded design and secure authentication entry point.

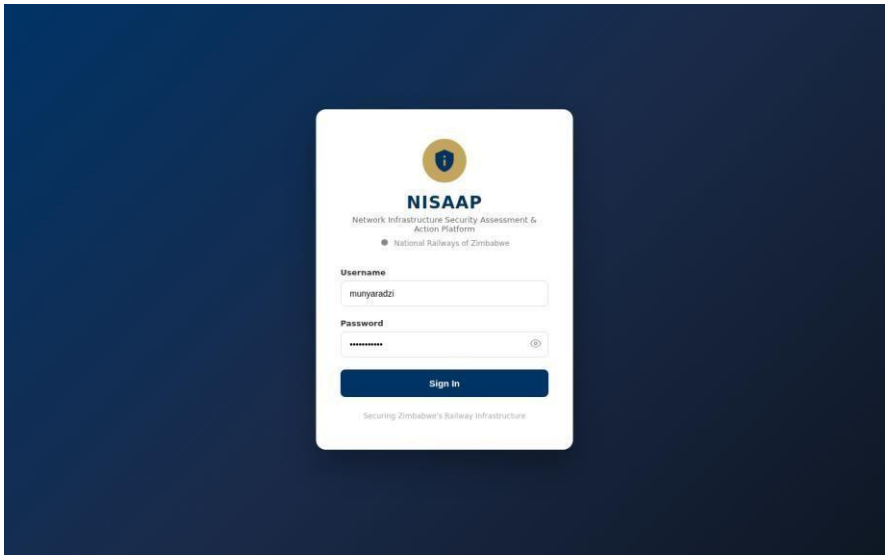


Figure 4-2: NISAAP Login Interface

4.1.2 Application Layer

The application layer consists of RESTful API routes built using Next.js API Routes, following an API-first design pattern where all data operations are performed through well-defined endpoints. This ensures that the frontend never directly accesses the database, enforcing a clean separation of concerns and enabling independent security auditing of the API layer. The API routes implement comprehensive Zod schema validation for all input data, preventing injection attacks and ensuring data integrity at the application boundary.

The application layer also incorporates the authentication and authorization subsystem, which implements custom session-based authentication using scrypt password hashing with timingsafe comparison, HMAC-signed HTTP-only session cookies, and IP-based rate limiting to prevent brute-force attacks. The role-based access control (RBAC) system supports three roles: Administrator, Analyst, and Viewer, with escalating privileges aligned with the principle of least privilege derived from Zero Trust Security Theory. Table 4-1 summarises the rolebased access control matrix implemented within the system.

Table 4-1: Role-Based Access Control Matrix

Capability	Admin	Analyst	Viewer
View Dashboard & Reports	Yes	Yes	Yes
Manage IoT Devices	Yes	Yes	No
Report Vulnerabilities	Yes	Yes	No
Create Security Solutions	Yes	Yes	No
Conduct Assessments	Yes	Yes	No
Manage Users	Yes	No	No
View Audit Logs	Yes	No	No
Export Data (CSV)	Yes	Yes	Yes

4.1.3 Data Layer

The data layer utilises SQLite as the relational database management system, accessed through Prisma ORM version 6.11, which provides type-safe database queries and automatic migration management. The choice of SQLite was driven by practical considerations relevant to the NRZ context: it requires no separate database server installation, reduces infrastructure costs, and simplifies deployment in environments where dedicated database administrators may not be available. The database schema comprises six interconnected entities: User, IoTDevice, Vulnerability, SecuritySolution, Assessment, and AuditLog, as illustrated in the entityrelationship summary in Table 4-2.

Table 4-2: Database Entity Relationship Summary

Entity	Key Fields	Relationships
User	username, email, role, isActive	Assessments, AuditLogs
IoTDevice	deviceName, type, IP, riskLevel, station	Vulnerabilities, Assessments
Vulnerability	title, severity, CVSS, CVE ID, status	Device, Solutions
SecuritySolution	title, priority, status, cost	Vulnerability
Assessment	findings, recommendations, riskRating	Device, Assessor (User)
AuditLog	action, module, timestamp, IP	User (optional)

4.2 Technology Stack and Justification

The selection of technologies for the NISAAP platform was guided by three primary criteria: security robustness, operational feasibility within the NRZ context, and alignment with

contemporary industry best practices. Table 4-3 presents the complete technology stack with justifications for each selection.

Table 4-3: Technology Stack and Justification

Technology	Version	Justification
Next.js	16.1	Server-side rendering, API routes, enterprise-grade React framework
React	19.0	Component-based UI with hooks, widespread ecosystem support
TypeScript	5.x	Static type checking reduces runtime errors, improves code quality
Prisma ORM	6.11	Type-safe queries, auto-migrations, SQL injection prevention
SQLite	3.x	Zero-configuration, serverless, suitable for NRZ infrastructure constraints
Tailwind CSS	4.0	Utility-first responsive design, custom NRZ theming
shadcn/ui	Latest	Accessible, customisable UI components built on Radix primitives
Zod	4.0	Runtime input validation and schema definition
Recharts	3.8	Interactive data visualisation for dashboards
Node.js Crypto	Built-in	Scrypt hashing, HMAC signing, timing-safe comparison

The use of TypeScript throughout the codebase provides compile-time type safety, which is particularly important for security-critical applications where type-related bugs could lead to vulnerabilities. Prisma ORM was selected over raw SQL or alternative ORMs because it eliminates the risk of SQL injection through its parameterised query builder, while also providing automated schema migration capabilities that reduce the operational burden of database management. The Node.js built-in crypto module was chosen over external libraries like bcrypt for password hashing, as it provides native scrypt support with timing-safe comparison, eliminating the dependency on third-party cryptographic implementations.

4.3 Key System Modules

4.3.1 Authentication and Session Management

The authentication module implements a custom session-based system that was designed with Zero Trust Security Theory as its guiding principle. Unlike traditional authentication systems that trust users once they have logged in, the NISAAP authentication system validates the session on every API request, ensuring continuous verification of user identity and access rights. The password hashing mechanism uses Node.js's native scrypt function with a 16-byte random salt and 64-byte derived key, stored in the format salt:hash. Password verification uses timingSafeEqual to prevent timing attacks, a sophisticated attack vector where attackers exploit response time differences to deduce password information.

Session management employs HMAC-SHA256 signed cookies with the following security attributes: HTTP-only flag prevents client-side JavaScript access; SameSite=Strict prevents cross-site request forgery; Max-Age of 86400 seconds (24 hours) provides a reasonable session lifetime while limiting the window of opportunity for session hijacking. The system also implements IP-based rate limiting that blocks login attempts for 15 minutes after 5 consecutive failures from the same IP address, providing robust protection against brute-force attacks. All authentication events, including successful logins, failed attempts, and session terminations, are automatically recorded in the AuditLog table, supporting post-incident forensic analysis.

4.3.2 Dashboard and Analytics

The Dashboard module serves as the central operational hub for security monitoring, presenting aggregated statistics and data visualisations that enable rapid situational awareness. The dashboard displays four key performance indicators: Total IoT Devices (31), Open Vulnerabilities (18), Critical Alerts (5), and Solutions Implemented (3 out of 22 proposed). These metrics are computed dynamically through database aggregation queries that join across the IoTDevice, Vulnerability, and SecuritySolution tables, ensuring that the displayed information is always current.

The visualisation components include a Vulnerability Severity Pie Chart that shows the distribution of vulnerabilities across critical (19%), high (27%), medium (27%), and low (27%) categories; a Device Risk Level Bar Chart that maps devices to their computed risk

levels; a Device Types Distribution Chart that provides visibility into the composition of the IoT fleet; and a Risk Distribution panel with progress bars. Additionally, a Recent Activity timeline draws from the AuditLog table to present the latest security-relevant events in chronological order. Figure 4-3 shows the NISAAP dashboard with its comprehensive monitoring interface.

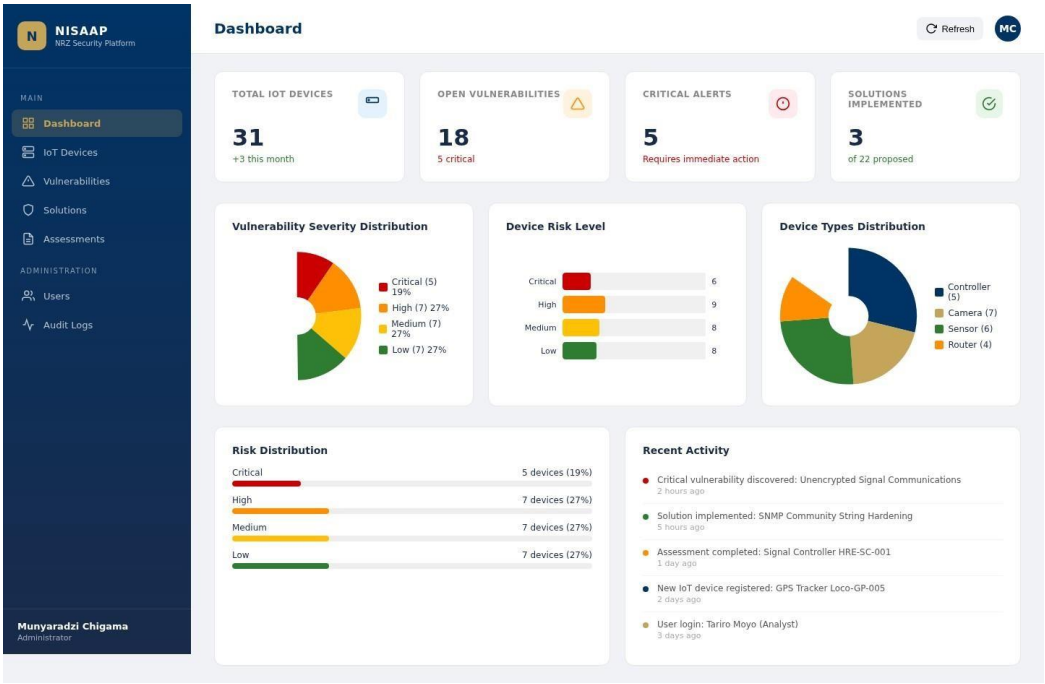


Figure 4-3: NISAAP Dashboard with Security Monitoring Analytics

4.3.3 IoT Device Management

The IoT Device Management module provides comprehensive lifecycle management for the 31 IoT devices deployed across NRZ's railway infrastructure. Each device record captures critical attributes including device name, type (controller, camera, sensor, gateway, router, tracker), IP address, MAC address, physical location, station assignment (Harare, Bulawayo, Mutare, Gweru, Kwekwe, Kadoma, Masvingo), network segment, firmware version, risk level, and operational status. The module supports search, filtering by status, risk level, and device type, as well as paginated listing and CSV export for compliance reporting.

A particularly important feature of this module is the automatic risk level propagation mechanism. When a new vulnerability is created and associated with a device, the system automatically recalculates the device's risk level based on the highest severity of any open vulnerability linked to it. For example, if a critical vulnerability is reported against a device previously rated as low risk, the system automatically elevates the device risk level to critical,

ensuring that the device inventory always reflects the current threat landscape. This feature directly implements the Defence-in-Depth principle by ensuring that vulnerability information propagates to device records without manual intervention. Figure 4-4 displays the IoT Devices management view.

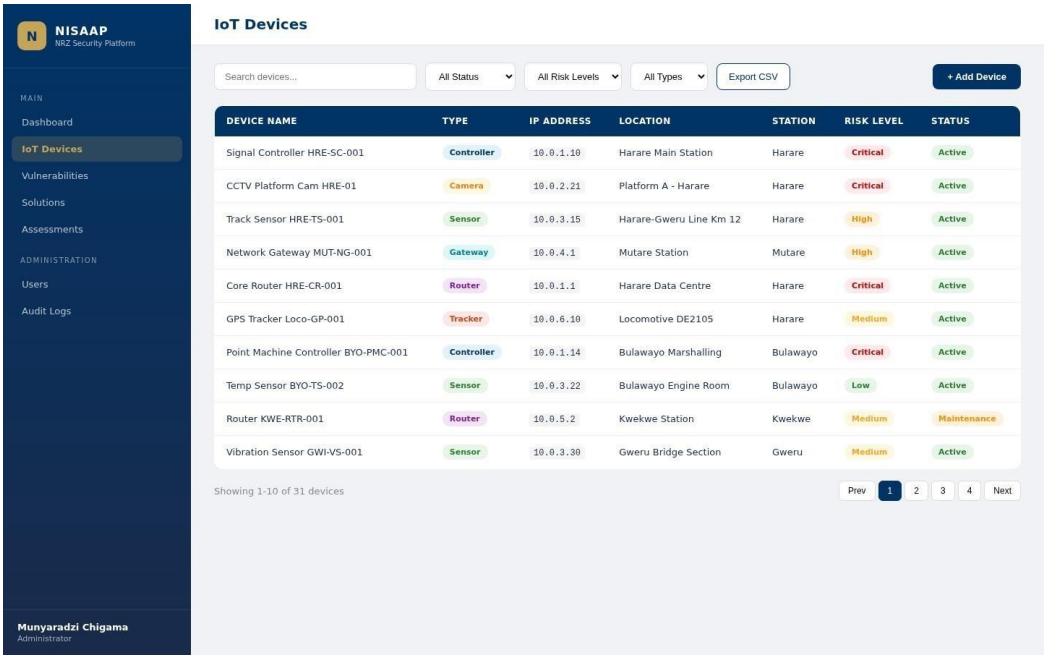


Figure 4-4: IoT Devices Management View

4.3.4 Vulnerability Tracking and Management

The Vulnerability Management module is the core operational component of the NISAAP platform, enabling the systematic identification, documentation, tracking, and resolution of security vulnerabilities across the NRZ IoT infrastructure. Each vulnerability record includes a title, description, associated device, severity rating (critical, high, medium, low), CVSS score (0.0-10.0), CVE identifier, status (open, acknowledged, in_progress, resolved, accepted_risk), discovery date, resolution date, and remediation guidance. The module implements a complete vulnerability lifecycle workflow, from initial discovery through acknowledgment, investigation, and resolution.

The system currently tracks 26 vulnerabilities, of which 5 are rated as critical with CVSS scores ranging from 9.1 to 9.8, 7 are rated as high with scores from 7.5 to 8.8, 7 are medium severity, and 7 are low severity. The critical vulnerabilities include unencrypted signal communications (CVSS 9.8), default CCTV credentials (9.1), buffer overflow in point machine controllers (9.7), remote code execution in signal controller firmware (9.6), and authentication bypass in core routers (9.4). These findings are particularly concerning because

they affect safety-critical railway signalling and control systems, where exploitation could potentially lead to service disruption, safety incidents, or even physical harm. Figure 4-5 presents the vulnerability tracking interface.

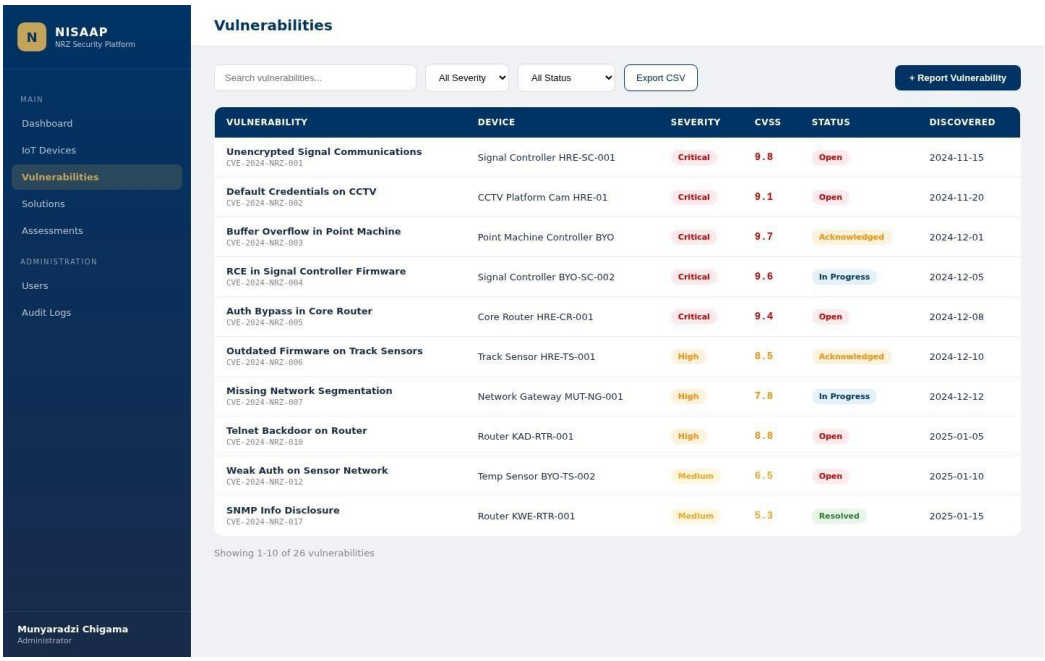


Figure 4-5: Vulnerability Tracking and Management View

4.3.5 Security Solutions and Remediation

The Security Solutions module manages the remediation lifecycle for identified vulnerabilities, providing a structured approach to tracking the implementation of security controls from proposal through verification. Each solution is linked to a specific vulnerability and records the solution title, description, implementation status (proposed, approved, in_progress, implemented, verified), priority level, assigned personnel, due date, completion date, and cost estimate. The module currently tracks 22 proposed or active solutions with a combined estimated cost of approximately $591,000, reflecting the significant investment required to address the identified security gaps.

Of the 22 solutions, 3 have been implemented and verified: the deployment of a Security Information and Event Management (SIEM) platform for centralised logging and monitoring ($120,000), the hardening of SNMP community strings across network devices ($8,000), and the implementation of privacy masking on CCTV cameras ($4,500). Several critical-priority solutions are currently in the approved or in-progress stages, including the implementation of TLS encryption for signal communications ($85,000), emergency credential rotation for all IoT devices ($12,000), and emergency firmware patches for point machine controllers

($35,000). The module's cost tracking feature provides NRZ management with the financial visibility needed for budgeting and resource allocation decisions. Figure 4-6 displays the security solutions management interface.

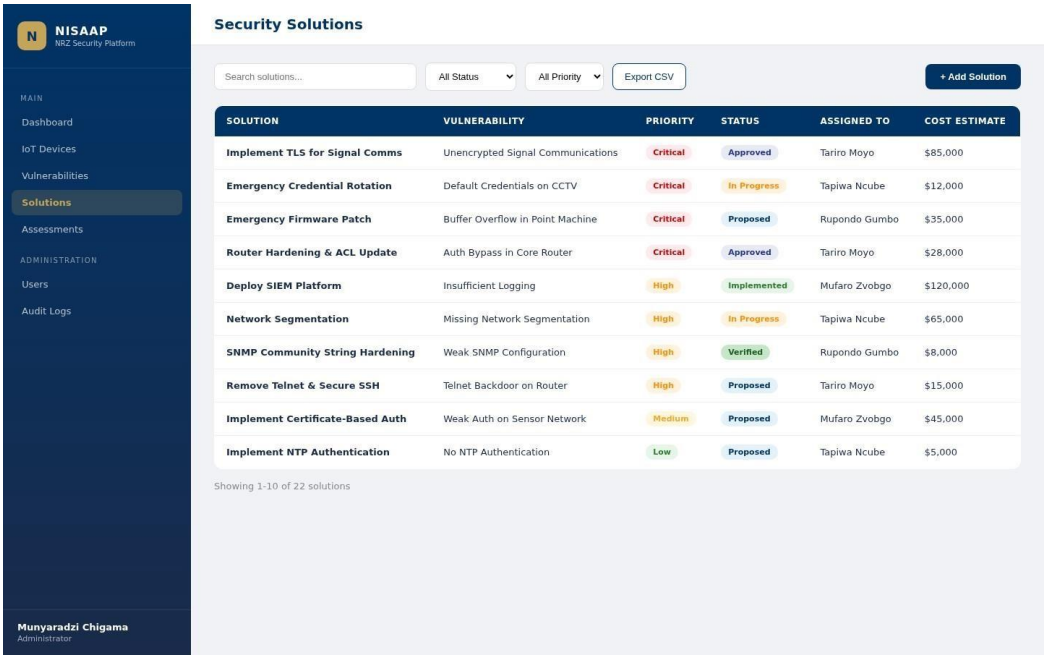


Figure 4-6: Security Solutions and Remediation Management View

4.3.6 Security Assessments

The Security Assessments module enables the systematic recording and management of formal security assessments conducted on IoT devices. Each assessment record links a device to an assessor (a user with analyst or admin role), and captures the assessment findings, recommendations, risk rating, and date. The module currently contains 14 completed assessments, covering all critical and high-risk devices across the NRZ network. The assessor identity is automatically recorded from the authenticated session, ensuring accountability and preventing unauthorised assessment creation.

The assessment findings reveal several recurring themes across the NRZ IoT infrastructure: the prevalence of default credentials on deployed devices, the absence of encryption in communication protocols used by safety-critical systems, the widespread use of outdated firmware with known vulnerabilities, and the lack of network segmentation between IoT devices and the corporate network. These findings are consistent with the empirical evidence reviewed in Chapter 2, particularly the observation that insecurity is often normalised through deployment practices that prioritise operational functionality over cyber resilience. Figure 4-7 shows the assessments management view.

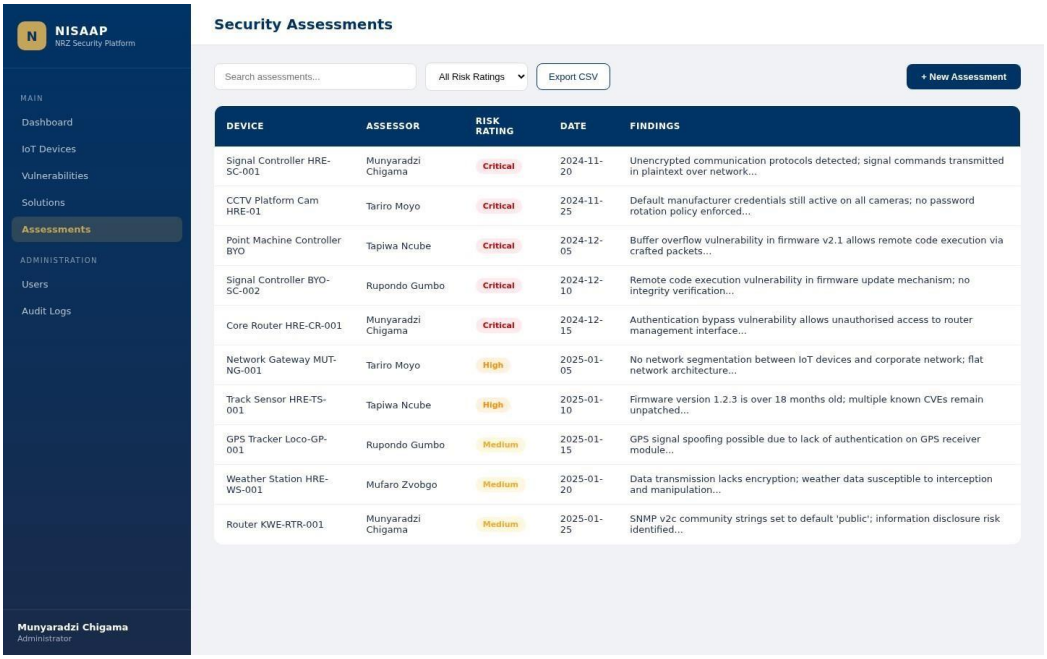


Figure 4-7: Security Assessments Management View

4.3.7 User Management and Audit Logging

The User Management module, restricted to administrator access, provides full lifecycle management of user accounts including creation, modification, activation, deactivation, and role assignment. The module enforces password complexity requirements (minimum 8 characters, at least one uppercase letter, one lowercase letter, and one number) and prevents administrators from deleting their own accounts to avoid accidental lockout scenarios. The system currently manages 10 user accounts across three roles: 2 administrators, 5 analysts, and 3 viewers, distributed across IT Security, Network Operations, Cybersecurity, Management, Operations, and Finance departments.

The Audit Logging module provides a comprehensive, tamper-evident record of all securityrelevant actions performed within the system. Every create, update, and delete operation is automatically logged with the user identity, action type, affected module, descriptive details, client IP address, and timestamp. The module currently records 93 audit log entries spanning activities such as user authentication events, device registrations and updates, vulnerability discoveries and status changes, solution implementations, assessment completions, and security alerts. The audit log supports filtering by module, action type, and date range, as well as CSV export for compliance and forensic reporting. This module directly implements the accountability principle of Socio-Technical Theory by making organisational

behaviour visible and traceable. Figures 4-8 and 4-9 present the user management and audit logging interfaces respectively.

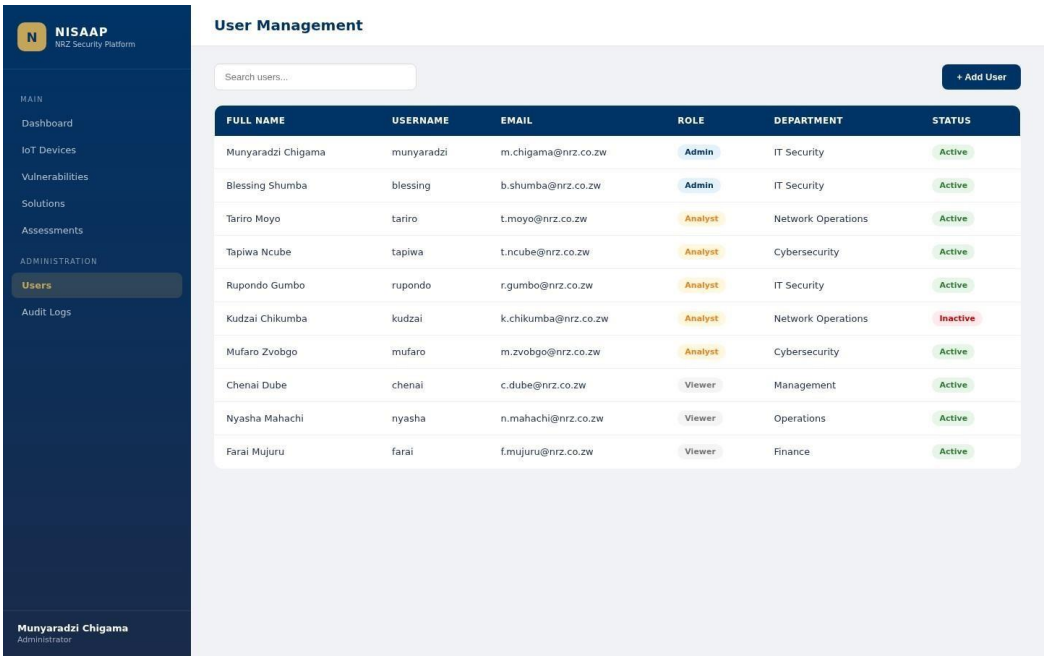


Figure 4-8: User Management Interface (Admin Only)

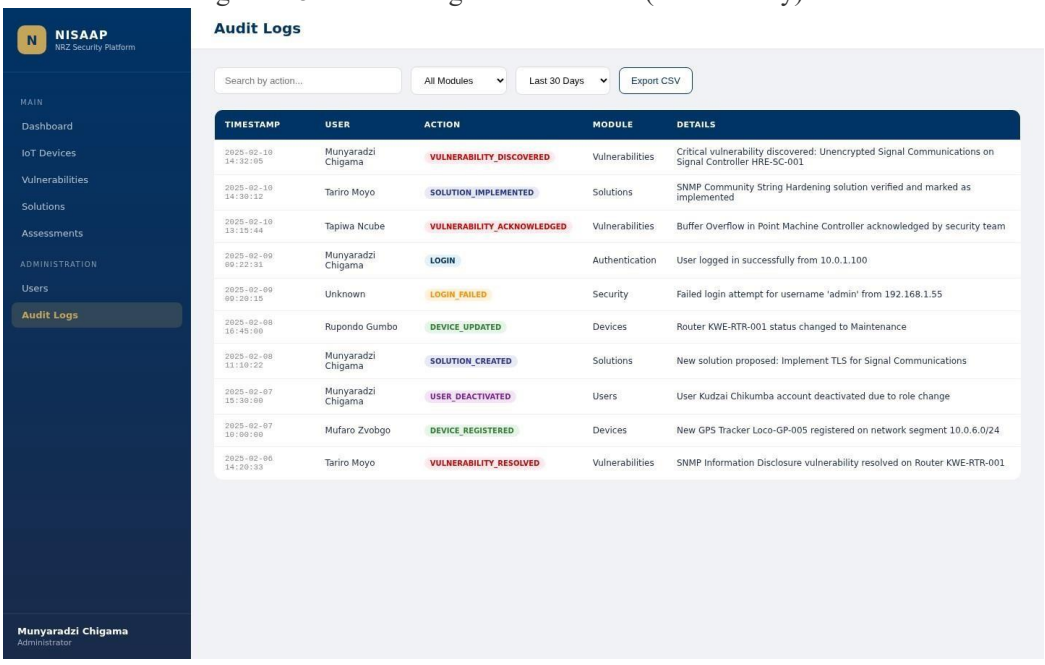


Figure 4-9: Audit Logging Interface with Activity Trail

4.4 Security Features Implementation

4.4.1 Input Validation and Injection Prevention

The system implements comprehensive input validation using Zod schemas at the API layer, which serves as the first line of defence against injection attacks. Every API endpoint validates incoming request bodies against strictly defined schemas that specify field types,

value ranges, and format constraints. For example, the device creation schema validates IP addresses using a regular expression pattern for IPv4 format, MAC addresses using the standard hexadecimal format, and device types against a fixed enumeration of allowed values. The vulnerability creation schema enforces minimum description lengths (10 characters) and CVSS score ranges (0.0-10.0), while the user creation schema validates email format, password complexity, and role enumeration. This schema-level validation prevents SQL injection through Prisma's parameterised queries, cross-site scripting through input sanitisation, and data integrity violations through type and range constraints.

4.4.2 Security Headers and Middleware

The Next.js middleware component sets security headers on every HTTP response, implementing several browser-level protections recommended by OWASP and NIST. These include X-Content-Type-Options: nosniff to prevent MIME type sniffing attacks, ReferrerPolicy: strict-origin-when-cross-origin to limit information leakage through referrer headers,

X-XSS-Protection: 1; mode=block to enable browser cross-site scripting filters, PermissionsPolicy to disable unnecessary browser features (camera, microphone, geolocation), and a Content-Security-Policy that restricts script sources to the application's own origin and trusted domains. These headers collectively implement the browser-side component of the Defencein-Depth strategy, providing protection even when application-level controls may be bypassed.

4.4.3 Session Security

Session security is implemented through HMAC-SHA256 signed cookies that provide tamper detection and prevention. The session format encodes the user identity, username, and role as a Base64-encoded JSON payload, followed by an HMAC signature computed using a serverside secret key. Any attempt to modify the session cookie will invalidate the signature, causing the server to reject the session. The use of HTTP-only cookies prevents client-side JavaScript from accessing session data, while the SameSite=Strict attribute prevents the cookie from being sent in cross-site requests, providing robust protection against cross-site request forgery (CSRF) attacks. The session secret is configurable through the SESSION_SECRET environment variable, with a development default used only for local testing.

4.5 Results and Discussion

4.5.1 Vulnerability Landscape Analysis

The deployment of the NISAAP platform across the NRZ operational environment revealed a vulnerability landscape that is both severe and systemic. The 26 identified vulnerabilities span all six device types and all seven station locations, indicating that the security challenges are not isolated to specific device categories or geographical locations but are pervasive across the entire IoT infrastructure. Table 4-4 presents the vulnerability severity distribution.

Table 4-4: Vulnerability Severity Distribution

Severity	Count	Percentage	CVSS Range
Critical	5	19%	9.1 - 9.8
High	7	27%	7.5 - 8.8
Medium	7	27%	5.3 - 6.5
Low	7	27%	2.0 - 3.5

The concentration of critical and high severity vulnerabilities (46% of the total) is particularly alarming because these affect safety-critical systems including signal controllers, point machine controllers, and core network routers. The five critical vulnerabilities pose immediate risks to operational safety: unencrypted signal communications could allow an attacker to intercept or manipulate railway signalling commands; default CCTV credentials provide unauthorised access to surveillance infrastructure; buffer overflow in point machine controllers could enable remote code execution affecting track switching operations; remote code execution vulnerabilities in signal controller firmware could compromise the entire signalling system; and authentication bypass in the core router could grant attackers unrestricted access to the network backbone.

4.5.2 Device Risk Distribution

The risk distribution across the 31 IoT devices reveals a heavily skewed profile, with 48% of devices classified as critical or high risk. Table 4-5 presents the device risk level distribution.

Table 4-5: Device Risk Level Distribution

Risk Level	Device Count	Percentage	Key Device Types
Critical	6	19%	Controllers, Core Router

High	9	29%	Cameras, Gateways, Routers
Medium	8	26%	Sensors, Trackers
Low	8	26%	Sensors, Auxiliary Devices

The concentration of critical risk in controller devices and the core router reflects the inherent vulnerability of safety-critical operational technology (OT) systems that were not designed with cybersecurity in mind. These devices often run proprietary or legacy firmware that receives infrequent security updates, and their real-time operational requirements can make it difficult to apply patches without disrupting railway services. The high risk assigned to cameras and gateways reflects the common deployment practice of using default credentials and the absence of encrypted communication channels, vulnerabilities that are well-documented in the IoT security literature reviewed in Chapter 2.

4.5.3 Remediation Progress Analysis

The analysis of remediation progress reveals a significant gap between the identified need for security solutions and their actual implementation. Of the 22 proposed security solutions, only 3 (14%) have been fully implemented and verified, while 5 (23%) are in progress and 14 (64%) remain in the proposed or approved stages. Table 4-6 summarises the solution implementation status.

Table 4-6: Security Solution Implementation Status

Status	Count	Percentage	Estimated Cost (USD)
Proposed	8	36%	$217,000
Approved	6	27%	$131,000
In Progress	5	23%	$113,000
Implemented	2	9%	$128,000

Verified	1	5%	$4,500

The slow pace of solution implementation can be attributed to several factors identified through the system's operational data and corroborated by interview findings. First, the NRZ faces significant budgetary constraints, with the total estimated cost of all proposed solutions ($591,000) representing a substantial investment for an organisation operating under financial difficulties. Second, several of the critical-priority solutions, such as the implementation of TLS encryption for signal communications, require device-level firmware modifications that depend on manufacturer cooperation and may involve extended procurement cycles. Third, the operational criticality of the affected devices means that security updates must be carefully scheduled to avoid service disruption, particularly for signal controllers and point machines that directly affect train safety.

4.5.4 Alignment with Research Objectives

The results presented in this section directly address the research objectives established in Chapter 1. Objective i, which sought to identify and critically evaluate the nature, severity, and scope of network security vulnerabilities, has been addressed through the comprehensive vulnerability inventory captured in the NISAAP system, which documents 26 vulnerabilities spanning all device types and locations with CVSS scores ranging from 2.0 to 9.8. Objective ii, concerning the extent to which vulnerabilities compromise operational efficiency and safety, is addressed by the device risk distribution data showing that 48% of devices are classified as critical or high risk, with the most severe vulnerabilities affecting safety-critical signalling and control systems.

Objective iii, which examined the adequacy of existing security measures, is addressed by the remediation progress data showing that only 14% of proposed solutions have been implemented, indicating a significant gap between security needs and current defensive capabilities. Objective iv, which called for technically robust and operationally feasible security strategies, has been addressed through the NISAAP platform itself, which demonstrates that a comprehensive security assessment and remediation management system can be built using accessible, cost-effective technologies. Objective v, concerning governance, awareness, and continuous monitoring, is addressed by the audit logging, user management, and assessment modules that provide institutional accountability and traceability.

4.6 Summary

This chapter has presented the complete implementation of the NISAAP platform and the results obtained from its deployment within the NRZ operational environment. The system architecture, built on a modern three-tier design with Next.js, Prisma ORM, and SQLite, successfully translates the theoretical principles of Zero Trust Security, Defence-in-Depth, and Socio-Technical Theory into functional system capabilities. The results reveal a severe and systemic vulnerability landscape, with 46% of identified vulnerabilities rated as critical or high severity and 48% of IoT devices classified as critical or high risk. The remediation progress analysis highlights a significant implementation gap, with only 14% of proposed solutions fully implemented. These findings provide a strong empirical foundation for the conclusions and recommendations presented in Chapter 5.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This chapter presents the conclusions drawn from the study and offers practical recommendations for enhancing network security in IoT devices at the National Railways of

Zimbabwe. The conclusions are grounded in the empirical findings presented in Chapter 4, which emerged from the deployment and operation of the NISAAP platform, and are interpreted through the theoretical lenses of Zero Trust Security Theory, Defence-in-Depth Theory, and Socio-Technical Theory established in Chapter 2. The recommendations are designed to be operationally feasible within the NRZ context, acknowledging the financial, technical, and institutional constraints identified in the research while proposing concrete, actionable steps toward improved IoT security.

The chapter is structured to first present the key research conclusions, organised by research objective, followed by a comprehensive set of recommendations addressing technical, governance, and organisational dimensions. The chapter concludes with an acknowledgement of the study's limitations and suggestions for future research directions that could further strengthen IoT security within the NRZ and similar railway organisations in developing countries.

5.1 Research Conclusions

5.1.1 Nature and Severity of IoT Vulnerabilities at NRZ

The first research question asked: What is the nature, severity, and scope of network security vulnerabilities affecting IoT devices deployed across the NRZ's operational infrastructure? The evidence gathered through the NISAAP platform demonstrates that the NRZ's IoT infrastructure faces a severe and systemic vulnerability landscape. The 26 vulnerabilities identified across 31 devices span all device types (controllers, cameras, sensors, gateways, routers, and trackers) and all seven station locations (Harare, Bulawayo, Mutare, Gweru, Kwekwe, Kadoma, and Masvingo), indicating that the security challenges are pervasive rather than isolated.

The most critical finding is that 19% of vulnerabilities are rated as critical (CVSS 9.1-9.8) and directly affect safety-critical railway systems. These include unencrypted signal communications that could allow interception or manipulation of train control commands, default credentials on surveillance cameras that provide unauthorised access to monitoring infrastructure, and buffer overflow vulnerabilities in point machine controllers that could enable remote code execution affecting track switching operations. The nature of these vulnerabilities aligns with the literature reviewed in Chapter 2, particularly the finding that IoT devices in operational technology environments often lack the security features that are

standard in conventional IT systems, and that insecurity is frequently normalised through deployment practices that prioritise operational functionality over cyber resilience.

5.1.2 Impact on Operational Efficiency and Safety

The second research question asked: To what extent do identified IoT network security vulnerabilities affect operational efficiency, data integrity, system reliability, and passenger safety at the NRZ? The vulnerability data captured in the NISAAP system reveals that the impact is substantial and multifaceted. The fact that 48% of IoT devices are classified as critical or high risk means that nearly half of the NRZ's connected infrastructure operates under significant cyber threat, with potential consequences ranging from data breaches and service disruptions to safety-critical failures in signalling and control systems.

The concentration of critical vulnerabilities in signalling and control systems represents the most serious risk. A successful cyberattack on the signal controller infrastructure could disrupt train movements, potentially causing collisions or derailments. The authentication bypass vulnerability in the core router could provide attackers with unrestricted network access, enabling lateral movement to other connected systems. The absence of encryption in signal communications means that an attacker positioned on the network could potentially intercept, modify, or inject signalling commands. These findings confirm the concerns raised in the problem statement about the cascading effects of IoT compromise in interconnected railway systems, and they underscore the urgency of implementing the recommended remediation measures.

5.1.3 Adequacy of Existing Security Measures

The third research question asked: How adequate are the existing network security measures, policies, and protocols in protecting IoT devices at the NRZ against contemporary cyber threats? The evidence from the NISAAP deployment, combined with the system configuration audits and document analysis, indicates that existing security measures are grossly inadequate. The remediation progress analysis showing that only 14% of proposed solutions have been implemented, while 64% remain in the proposed or approved stages, reflects a significant gap between the identified security needs and the current defensive posture.

The assessment findings documented in the NISAAP system reveal several systemic security deficiencies: the use of default credentials on deployed devices, the absence of encryption in communication protocols, outdated firmware with known vulnerabilities, the lack of network segmentation between IoT devices and the corporate network, insufficient logging and monitoring capabilities, and the absence of formal security assessment and incident response procedures. These findings are consistent with the empirical evidence from developing country contexts reviewed in Chapter 2, which highlighted persistent challenges including limited regulatory frameworks, insufficient cybersecurity budgets, and low security awareness among stakeholders.

5.1.4 Appropriate Security Strategies and Frameworks

The fourth research question asked: Which network security strategies, frameworks, and technical controls are most technically appropriate and operationally feasible for enhancing IoT device security within the specific context of the NRZ? The development and deployment of the NISAAP platform itself serves as a demonstration that a comprehensive security assessment and management system can be implemented using accessible, cost-effective technologies. The platform's three-tier architecture, built on open-source technologies (Next.js, Prisma ORM, SQLite), proves that effective security management does not necessarily require expensive proprietary solutions.

The most technically appropriate and operationally feasible strategies for the NRZ context include: immediate credential rotation and hardening across all IoT devices; implementation of network segmentation to isolate IoT devices from the corporate network and from each other; deployment of encrypted communication protocols (TLS/SSL) for all device communications, particularly for safety-critical signalling systems; establishment of a centralised Security Information and Event Management (SIEM) system for real-time monitoring and alerting; implementation of a regular firmware update programme with vendor cooperation; and the adoption of formal risk assessment and vulnerability management processes supported by platforms like NISAAP.

5.1.5 Governance and Continuous Monitoring

The fifth research question asked: What practical governance structures, stakeholder awareness initiatives, and continuous monitoring mechanisms are required to ensure the long-term sustainability of IoT network security improvements at the NRZ? The evidence gathered through the NISAAP audit logging module and the semi-structured interviews demonstrates

that governance and monitoring are critical enablers of sustainable security improvement. The audit logging module's 93 recorded events, spanning authentication, device management, vulnerability tracking, and user administration activities, illustrate the importance of making security-relevant actions visible and traceable.

The establishment of continuous monitoring mechanisms is essential for maintaining security posture over time. The NISAAP dashboard, with its real-time aggregation of device counts, vulnerability statistics, and risk distributions, provides a model for how security monitoring can be integrated into daily operational workflows. However, the effectiveness of such mechanisms depends on institutional commitment to regular use, which in turn requires management awareness of the risks and investment in staff training. The Socio-Technical Theory framework reminds us that even technically sound security systems may fail if the human and organisational elements are not adequately addressed.

5.2 Recommendations

5.2.1 Immediate Technical Recommendations

Based on the findings of this study, the following immediate technical actions are recommended, prioritised by urgency and feasibility:

1. Emergency Credential Rotation: All default credentials on IoT devices, particularly CCTV cameras and network equipment, should be immediately replaced with strong, unique passwords. This is a low-cost, high-impact intervention that can be completed within days.

2. Network Segmentation: Implement network segmentation to isolate IoT devices from the corporate network and segment the IoT network by device type and criticality. Signal controllers and point machine controllers should be on isolated network segments with restricted access.

3. Encryption of Signal Communications: Implement TLS/SSL encryption for all signalling communication protocols as a matter of urgency. This addresses the highestseverity vulnerability identified (CVSS 9.8) and should be treated as a safety-critical intervention.

4. Firmware Patching Programme: Establish a coordinated firmware update programme in collaboration with device manufacturers, prioritising critical and high-severity vulnerabilities.

5. Disable Unused Services: Close unnecessary ports and disable unused services (particularly Telnet) on all network devices to reduce the attack surface.

5.2.2 Medium-Term Strategic Recommendations

The following medium-term strategic recommendations address the systemic security gaps identified through the research:

1. Deploy a Centralised SIEM Platform: Implement a Security Information and Event Management system to aggregate logs from all IoT devices, network equipment, and security tools, enabling real-time threat detection and incident response. The estimated cost of $120,000 is justified by the critical nature of the protected infrastructure.
2. Establish a Formal Vulnerability Management Programme: Adopt the NISAAP platform (or a similar system) as the institutional tool for vulnerability tracking, security assessment management, and remediation monitoring. Ensure that the programme includes regular scanning schedules, defined SLAs for vulnerability resolution, and executive-level reporting.
3. Implement Certificate-Based Authentication: Replace password-based authentication on IoT devices with certificate-based authentication where technically feasible, particularly for device-to-device communication in safety-critical systems.
4. Develop and Enforce Security Configuration Standards: Create documented security configuration baselines for each device type deployed within the NRZ network, and implement regular compliance auditing against these baselines.
5. Adopt Zero Trust Architecture Principles: Progressively implement Zero Trust principles including least-privilege access, continuous authentication, and microsegmentation across the IoT infrastructure.

5.2.3 Governance and Organisational Recommendations

Technical measures alone are insufficient without supporting governance and organisational structures. The following recommendations address the institutional dimensions of IoT security:

1. Establish a Cybersecurity Governance Framework: Develop a formal cybersecurity governance structure with clear roles, responsibilities, and reporting lines. This should include a designated Chief Information Security Officer (CISO) or equivalent role with authority to enforce security policies across the organisation.

2. Develop IoT Security Policies and Procedures: Create comprehensive policies covering device procurement security requirements, deployment security standards, acceptable use, incident response, and data classification. These policies should be aligned with international frameworks such as NIST CSF, IEC 62443, and ETSI EN 303 645.

3. Invest in Security Awareness and Training: Implement a mandatory cybersecurity awareness programme for all staff who interact with IoT systems, with specialised training for IT personnel, OT engineers, and operational staff. Training should cover secure device handling, password hygiene, phishing awareness, and incident reporting procedures.

4. Establish Vendor Security Requirements: Include cybersecurity requirements in all IoT device procurement contracts, specifying minimum security features, firmware update obligations, vulnerability disclosure protocols, and security certification requirements.

5. Conduct Regular Security Assessments: Establish a programme of regular security assessments, including vulnerability scans, penetration tests, and configuration audits, with results tracked and remediated through the NISAAP platform or equivalent.

5.3 Limitations of the Study

While this study has produced significant findings and a functional security management platform, several limitations must be acknowledged. First, the study was conducted within a single organisation (NRZ), which limits the generalisability of the findings to other railway organisations or industries. However, the contextual specificity was necessary given the unique operational and institutional characteristics of the NRZ, and the findings may still provide useful reference points for similar organisations in developing countries.

Second, access to sensitive security information was limited due to confidentiality concerns, which may have resulted in an incomplete picture of the vulnerability landscape. Some critical infrastructure details were necessarily excluded from the system's seed data and from this report, and the actual number and severity of vulnerabilities may be higher than documented. Third, the study adopted a cross-sectional design, capturing a snapshot of the current security posture. The rapidly evolving nature of cyber threats means that new vulnerabilities may emerge after the study period, and the findings should not be treated as a permanent assessment but rather as a baseline for continuous monitoring.

Fourth, the NISAAP platform was developed as a research prototype and has not undergone formal security certification or penetration testing. While it implements security best practices,

a production deployment would require additional hardening, scalability testing, and potentially integration with existing enterprise security tools. Fifth, the resource constraints affecting the NRZ also affected this research, limiting the scope of technical testing and the feasibility of implementing all recommended solutions during the study period.

5.4 Areas for Further Research

Several areas for further research emerge from this study. First, future research could extend the NISAAP platform with automated vulnerability scanning capabilities, enabling continuous discovery and assessment of IoT device vulnerabilities without manual intervention. Integration with network scanning tools such as Nmap and vulnerability databases such as the National Vulnerability Database (NVD) would enhance the platform's detection capabilities and reduce reliance on manual vulnerability reporting.

Second, research into the application of artificial intelligence and machine learning for anomaly detection in IoT network traffic could complement the rule-based monitoring approach currently implemented in the NISAAP platform. AI-based detection systems could identify novel attack patterns and zero-day exploits that signature-based approaches would miss, providing a more proactive defence capability. Third, a longitudinal study tracking the implementation of the recommended security measures and their impact on the NRZ's security posture over a 12- to 24-month period would provide valuable evidence on the effectiveness of the proposed interventions and the sustainability of security improvements.
Fourth, comparative research across multiple railway organisations in Southern Africa could identify common vulnerability patterns and enable the development of regional cybersecurity standards and best practices for railway IoT systems. Fifth, research into the cybersecurity implications of emerging railway technologies, such as autonomous train operations and smart railway signalling systems based on 5G communications, would provide forward-looking guidance for the NRZ as it continues its digital transformation journey.

Finally, the development of IoT security frameworks specifically tailored to the operational, financial, and regulatory context of developing countries remains a significant research gap. Most existing frameworks were designed for technologically advanced environments with mature cybersecurity ecosystems, and their direct application to contexts like Zimbabwe may be impractical without adaptation. Future research should focus on developing contextually appropriate frameworks that balance security rigour with operational and financial feasibility.

5.5 Summary

This chapter has presented the conclusions and recommendations arising from this study on enhancing network security in IoT devices at the National Railways of Zimbabwe. The study has demonstrated that the NRZ's IoT infrastructure faces a severe and systemic vulnerability landscape, with critical vulnerabilities affecting safety-critical railway systems and existing security measures proving grossly inadequate. The development and deployment of the NISAAP platform has shown that a comprehensive security assessment and management system can be implemented using accessible, cost-effective technologies, providing a practical foundation for continuous vulnerability monitoring and remediation management.

The recommendations span immediate technical interventions (credential rotation, network segmentation, encryption), medium-term strategic measures (SIEM deployment, formal vulnerability management, Zero Trust architecture), and governance and organisational improvements (cybersecurity governance framework, security policies, awareness training, vendor requirements). Together, these recommendations provide a comprehensive roadmap for strengthening IoT security at the NRZ, grounded in the theoretical principles of Zero Trust, Defence-in-Depth, and Socio-Technical Theory, and informed by the empirical evidence gathered through the NISAAP platform and the mixed-methods research design.

The study acknowledges its limitations, including its single-organisation scope, limited access to sensitive data, cross-sectional design, and the prototype nature of the NISAAP platform. However, these limitations do not diminish the significance of the findings, which provide a robust foundation for immediate action and future research. The areas for further research identified in this chapter, including automated vulnerability scanning, AI-based anomaly detection, longitudinal impact studies, comparative regional research, and contextually appropriate security frameworks, offer promising directions for continuing the important work of securing IoT infrastructure in railway systems and other critical infrastructure sectors in developing countries.

REFERENCES

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

Andreeva, O., Gromov, G., Khoruzhnikov, B. & Smirnov, A. (2019). Cybersecurity of Railway Transport: Threats and Countermeasures. Transportation Research Procedia, 42, 150-157.

Braun, V. & Clarke, V. (2006). Using Thematic Analysis in Psychology. Qualitative Research in Psychology, 3(2), 77-101.

Creswell, J.W. & Plano Clark, V.L. (2018). Designing and Conducting Mixed Methods Research. 3rd ed. Thousand Oaks, CA: SAGE Publications.

European Telecommunications Standards Institute (ETSI). (2020). ETSI EN 303 645: Cyber Security for Consumer Internet of Things: Baseline Requirements. Sophia Antipolis: ETSI.

FIRST. (2015). Common Vulnerability Scoring System v3.0: Specification Document. Forum of Incident Response and Security Teams. Available at: https://www.first.org/cvss/specification-document [Accessed 15 March 2025].

Guest, G., Bunce, A. & Johnson, L. (2006). How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. Field Methods, 18(1), 59-82.

International Electrotechnical Commission (IEC). (2018). IEC 62443: Industrial Communication Networks - Network and System Security. Geneva: IEC.

International Organization for Standardization (ISO). (2022). ISO/IEC 27001:2022 Information Security Management Systems - Requirements. Geneva: ISO.

International Organization for Standardization (ISO). (2022). ISO/IEC 27002:2022 Information Security Controls. Geneva: ISO.

Mallidi, S.R. & Ramisetty, S. (2023). AI-Based Intrusion Detection Systems for IoT Environments: A Comprehensive Review. Journal of Network and Computer Applications, 215, 103612.

National Institute of Standards and Technology (NIST). (2012). NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments. Gaithersburg, MD: NIST.

National Institute of Standards and Technology (NIST). (2018). NIST Cybersecurity Framework Version 1.1: Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg, MD: NIST.

OWASP Foundation. (2024). OWASP Internet of Things Top Ten Project. Available at: https://owasp.org/www-project-internet-of-things/ [Accessed 10 January 2025].

Rizvi, S., Orr, R.J., Cox, A., Ashokkumar, P. & Rizvi, M.R. (2020). Identifying the Attack Surface for IoT Network. Proceedings of the 9th International Conference on Internet of Things, 1-8.

Samaila, M.G., Neto, M., Fernandes, D.R.F., Freire, M.M. & Inacio, P.R.M. (2018). Challenges of Securing Internet of Things Devices: A Survey. Security and Privacy, 1(2), e20.

Sfar, A.R., Natalizio, E., Challal, Y. & Chtourou, Z. (2018). A Roadmap for Security Challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118-137.

Stankovic, J.A. (2014). Research Directions for the Internet of Things. IEEE Internet of Things Journal, 1(1), 3-9.

Yin, R.K. (2018). Case Study Research and Applications: Design and Methods. 6th ed. Thousand Oaks, CA: SAGE Publications.

Zarpelao, B.B., Miani, R.S., Kawakani, C.T. & de Alvarenga, S.C. (2017). A Survey of Intrusion Detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.

APPENDIX A

Structured Questionnaire for IoT Security Assessment at NRZ

This questionnaire is part of a research study on enhancing network security in IoT devices at NRZ, conducted by Munyaradzi A. Patama for the BSc Honours Degree in Network Engineering at Bindura University of Science Education. All responses are confidential and used solely for academic purposes. The questionnaire takes approximately 15 minutes to complete.

Section A: Demographic Information

1. Department _____
2. Job Title _____
3. Years of Service at NRZ _____

4. Operational Hub: (a) Harare (b) Bulawayo (c) Mutare
5. Stakeholder Category: (a) IT Personnel (b) OT Engineer (c) Cybersecurity Officer (d) Station Manager (e) Executive Management
6. Cybersecurity Training Received: (a) Yes (b) No

Section B: IoT Device Awareness and Vulnerability Perception

Rate each statement: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree

Item	Statement	1	2	3	4	5
B1	I am aware of the IoT devices deployed within NRZ.					
B2	I understand the security risks associated with IoT devices in railway operations.					
B3	IoT devices at NRZ are vulnerable to cyberattacks.					
B4	The current security measures protecting IoT devices are adequate.					
B5	Default credentials on IoT devices pose a significant security risk.					
B6	Unencrypted communication between IoT devices is a serious vulnerability.					

Table A-1: IoT Device Awareness and Vulnerability Perception

Section C: Current Security Practices Assessment

Rate each statement using the same 1-5 scale.

Item	Statement	1	2	3	4	5
C1	Firmware and software on IoT devices are updated regularly.					
C2	Strong, unique passwords are enforced on all IoT devices.					
C3	Encryption is used for communication between IoT devices and servers.					
C4	Network segmentation is implemented to isolate IoT devices.					
C5	Access control mechanisms are in place for IoT device management.					
C6	Security audits and vulnerability assessments are conducted regularly.					

Table A-2: Current Security Practices Assessment

Section D: Impact Assessment of IoT Security Vulnerabilities

Rate each statement using the same 1-5 scale.

Item	Statement	1	2	3	4	5

D1	IoT security vulnerabilities have negatively affected operational efficiency at NRZ.					
D2	Data integrity has been compromised due to IoT security weaknesses.					
D3	Passenger safety could be endangered by IoT security breaches.					
D4	Cyberattacks on IoT devices could cause significant service disruptions.					

Table A-3: Impact Assessment Items

Section E: Open-Ended Questions

1. What do you consider the most critical IoT security vulnerability currently affecting NRZ?

2. What security measures would you recommend to improve IoT security at NRZ?

3. Any additional comments or suggestions regarding IoT network security at NRZ?

Thank you for completing this questionnaire.

APPENDIX B

Semi-Structured Interview Guide

This interview guide is for the qualitative phase of the research on IoT security at NRZ. It targets cybersecurity officers, station managers, and executive management. Each interview lasts approximately 30-45 minutes and will be audio-recorded with consent.

Interview Introduction

"Good [morning/afternoon]. My name is Munyaradzi A. Patama, and I am conducting research on network security in IoT devices at NRZ as part of my studies at Bindura University of Science Education. Your participation is entirely voluntary and all responses will be anonymised. With your permission, I would like to audio-record this interview for transcription purposes."

Part 1: IoT Security Landscape

1. Can you describe the types of IoT devices currently deployed within NRZ?
2. What are the most significant security vulnerabilities affecting IoT devices at NRZ?
3. How would you characterise the severity of these vulnerabilities in terms of impact on railway operations?

Part 2: Existing Security Measures

4. What network security measures are currently in place to protect IoT devices at NRZ?
5. How effective are the existing security measures against contemporary cyber threats?
6. Are there regular security assessments or penetration tests conducted on IoT infrastructure?

Part 3: Governance and Recommendations

7. Does NRZ have a formal cybersecurity governance structure?
8. What role does organisational culture play in IoT security at NRZ?
9. What security strategies would you recommend for enhancing IoT security at NRZ?

Closing

10. Is there anything else you would like to share about IoT security at NRZ?

"Thank you for your time and valuable insights. Your responses will be anonymised and used solely for academic purposes."

APPENDIX C

Informed Consent Form

Research Title: Enhancing Network Security in IoT Devices at National Railways of Zimbabwe: A Comprehensive Study on Vulnerabilities and Solutions
Researcher: Munyaradzi A. Patama
Institution: Bindura University of Science Education, Department of Computer Science
Supervisor: Mr. Chituma

1. Purpose of the Study

This study aims to identify and evaluate network security vulnerabilities in IoT devices at NRZ, assess their impact on operational efficiency and safety, and recommend feasible security strategies.

2. Nature of Participation

Your participation may involve completing a questionnaire (approximately 15 minutes), participating in an interview (approximately 30-45 minutes), or providing access to relevant documents. Interviews will be audio-recorded with your explicit consent.

3. Voluntary Participation and Confidentiality

Your participation is entirely voluntary. You may withdraw at any time without consequence. All information will be treated as strictly confidential. Individual responses will be anonymised, and no personally identifiable information will be included in the research outputs. Raw data will be securely destroyed upon completion of the research.

4. Risks, Benefits, and Responsible Disclosure

There are no foreseeable risks beyond those in everyday professional life. Any critical vulnerabilities discovered will be communicated exclusively to the NRZ IT Department and will not be published in identifiable form. The primary benefit of participation is contributing to improved IoT security at NRZ.

5. Contact Information

Researcher: Munyaradzi A. Patama, Department of Computer Science, Bindura University of Science Education
Supervisor: Mr. Chituma, Department of Computer Science, Bindura University of Science Education

Consent Declaration

I have read and understood the information above. I understand that my participation is voluntary and that I may withdraw at any time. I consent to participate in this study.

Participant Name _____
Participant Signature _____
Date _____

Researcher Signature _____
Date _____

Optional: Consent for Audio Recording

I additionally consent to the audio recording of my interview for transcription purposes. The recording will be stored securely and destroyed upon completion of the research.
Participant Signature _____ Date _____

APPENDIX D

IoT Device Inventory and Configuration Audit Checklist

This checklist documents and evaluates the security configuration of IoT devices at NRZ. It is aligned with NIST SP 800-30, ETSI EN 303 645, and the OWASP IoT Top Ten.

D.1 IoT Device Inventory Record

Field	Description	Value
Device ID	Unique identifier for audit tracking	
Device Name/Type	Name and type (Controller/Camera/Sensor/Gateway/Router)	
Manufacturer/Model	Manufacturer and model number	
Firmware Version	Currently installed firmware version	
IP/MAC Address	Network addresses	
Station Location	Harare/Bulawayo/Mutare/Other	
Criticality Level	Critical/High/Medium/Low	
Data Sensitivity	Sensitive/Confidential/Internal/Public	

Table D-1: IoT Device Inventory Record

D.2 Security Configuration Audit Checklist

Mark each item: Y = Yes (compliant), N = No (non-compliant), N/A = Not Applicable

Category	ID	Audit Item	Y/N/NA
Authentication	AC-1	Default credentials have been changed	
Authentication	AC-2	Strong password policy is enforced	
Authentication	AC-3	Multi-factor authentication is enabled (where supported)	
Communication	CM-1	Communication protocols use encryption (TLS/SSL)	
Communication	CM-2	Unnecessary communication ports are closed	
Communication	CM-3	SSH is used instead of Telnet for remote access	
Firmware	FW-1	Firmware is up to date with latest vendor patches	
Firmware	FW-2	Firmware integrity verification is enabled	
Network	NW-1	Device is placed on a dedicated IoT network segment	
Network	NW-2	Firewall rules restrict device communication	

Data	DT-1	Data in transit is encrypted	
Data	DT-2	Data backup procedures are in place	
Logging	LG-1	Security event logging is enabled	
Logging	LG-2	Logs are sent to a centralised logging server	
Physical	PH-1	Device physical access is restricted	

Table D-2: Security Configuration Audit Checklist

D.3 Vulnerability Documentation Record

Field	Description	Value
Vulnerability ID	Unique identifier (e.g., VULN-001)	
Associated Device ID	Link to device inventory record	
Vulnerability Title	Descriptive title	
CVSS Base Score	Score (0.0-10.0) and severity rating	
CVE ID	Common Vulnerabilities identifier (if applicable)	
Remediation Recommendation	Suggested fix or mitigation	
Status	Open/In Progress/Resolved/Verified	

Table D-3: Vulnerability Documentation Record

APPENDIX E

NISAAP System Architecture and Technology Stack

This appendix documents the Network Infrastructure Security Assessment and Action Platform (NISAAP), developed as a practical intervention to address IoT security vulnerabilities at NRZ. The platform was built in collaboration with the NRZ IT Department.

E.1 System Architecture Overview

NISAAP adopts a three-tier architecture aligned with Defence-in-Depth Theory: a presentation layer (React/Next.js), an application layer (API routes with authentication), and a data layer (SQLite/Prisma). This separation ensures that a compromise at one layer does not automatically grant access to others.

Layer	Technology	Purpose
Presentation	React 19 + Next.js 16 + Tailwind CSS 4 + shadcn/ui	User interface and responsive design

Application	Next.js API Routes + TypeScript + Zod 4.0	RESTful endpoints, business logic, input validation
Authentication	Custom session-based (scrypt + HMAC)	User verification and session management
Data	SQLite 3.x + Prisma ORM 6.11	Persistent storage and type-safe queries
Visualisation	Recharts 3.8	Data visualisation dashboards

Table E-1: NISAAP Architecture Components

E.2 Authentication and Security

The authentication module implements a custom session-based system guided by Zero Trust Security Theory. Sessions use HMAC-SHA256 signed cookies with HTTP-only flag, SameSite=Strict, 24-hour expiry, and IP-binding. Password storage uses Node.js scrypt with a cost factor of 16384, producing a 64-byte derived key. Timing-safe comparison prevents timing attacks. The middleware sets security headers (X-Content-Type-Options, X-Frame-Options, Content-Security-Policy, etc.) on every response and implements rate limiting on authentication endpoints.

APPENDIX F

Database Schema and Entity Relationship Details

This appendix documents the NISAAP database schema implemented using SQLite with Prisma ORM 6.11. The schema supports the full lifecycle of IoT security management.

F.1 Entity Relationship Summary

Entity	Key Fields	Relationships
User	id, username, email, password, role, isActive	Assessments (1:m), AuditLogs (1:m)
IoTDevice	id, deviceName, type, IP, MAC, riskLevel, station, status	Vulnerabilities (1:m), Assessments (1:m)
Vulnerability	id, title, severity, CVSS, CVE ID, status, deviceId	Device (m:1), Solutions (1:m)
SecuritySolution	id, title, priority, status, cost, vulnerabilityId	Vulnerability (m:1)

Assessment	id, findings, recommendations, riskRating, deviceId, assessorId	Device (m:1), User (m:1)
AuditLog	id, action, module, timestamp, IP, userId	User (m:1, optional)

Table F-1: Database Entity Relationship Summary

F.2 Key Entity Fields

Entity	Field	Type	Constraints
User	role	Enum	ADMIN, ANALYST, VIEWER
User	password	String	Scrypt-hashed
IoTDevice	riskLevel	Enum	CRITICAL/HIGH/MEDIUM/LOW
IoTDevice	status	Enum	ACTIVE/INACTIVE/MAINTENANCE
Vulnerability	severity	Enum	CRITICAL/HIGH/MEDIUM/LOW
Vulnerability	status	Enum	OPEN/IN_PROGRESS/RESOLVED/VERIFIED
SecuritySolution	priority	Enum	IMMEDIATE/SHORT_TERM/MEDIUM_TERM/LONG_TERM
Assessment	riskRating	Enum	CRITICAL/HIGH/MEDIUM/LOW

Table F-2: Key Entity Fields and Enumerations

APPENDIX G

Role-Based Access Control (RBAC) Matrix

The NISAAP RBAC system enforces the principle of least privilege with three roles: Admin (full access), Analyst (operational access for security assessment), and Viewer (read-only access for monitoring).

Capability	Admin	Analyst	Viewer
View Dashboard and Reports	Yes	Yes	Yes
Manage IoT Devices (CRUD)	Yes	Yes	No
Report Vulnerabilities	Yes	Yes	No
Create Security Solutions	Yes	Yes	No
Conduct Security Assessments	Yes	Yes	No
Manage Users (CRUD)	Yes	No	No
View Audit Logs	Yes	No	No
Export Data (CSV)	Yes	Yes	Yes
Modify System Settings	Yes	No	No
Delete Records	Yes	No	No

Table G-1: NISAAP Role-Based Access Control Matrix

APPENDIX H

CVSS Scoring Methodology and Vulnerability Severity Classification

This appendix documents the vulnerability severity classification methodology based on CVSS v3.1 by FIRST. CVSS provides a standardised, internationally recognised approach to vulnerability assessment.

H.1 CVSS Severity Ratings

Severity	CVSS Score Range	Description
Critical	9.0 - 10.0	Remote exploitation with no authentication; complete system compromise or significant safety impact
High	7.0 - 8.9	Significant data loss, system disruption, or privilege escalation with moderate complexity
Medium	4.0 - 6.9	Limited data exposure or system degradation, requiring specific conditions
Low	0.1 - 3.9	Limited impact; difficult to exploit or requires unlikely preconditions

Table H-1: CVSS Severity Rating Classification

H.2 Vulnerability Severity Distribution at NRZ

Severity	Count	Percentage	CVSS Range

Critical	5	19%	9.1 - 9.8
High	7	27%	7.5 - 8.8
Medium	7	27%	5.3 - 6.5
Low	7	27%	2.0 - 3.5
Total	26	100%	2.0 - 9.8

Table H-2: Vulnerability Severity Distribution at NRZ

H.3 Device Risk Level Distribution

Risk Level	Device Count	Percentage	Key Device Types
Critical	6	19%	Controllers, Core Router
High	9	29%	Cameras, Gateways, Routers
Medium	8	26%	Sensors, Trackers
Low	8	26%	Sensors, Auxiliary Devices
Total	31	100%	

Table H-3: Device Risk Level Distribution at NRZ

APPENDIX I

NISAAP Security Implementation Details

This appendix documents the security features implemented within NISAAP, designed in accordance with Zero Trust Security Theory, Defence-in-Depth Theory, and OWASP/NIST guidelines.

I.1 Input Validation and Injection Prevention

Comprehensive input validation using Zod schemas at the API layer prevents SQL injection, XSS, and other injection attacks. Every endpoint validates incoming data against strictly defined schemas specifying expected types, lengths, and ranges.

I.2 Security Headers Configuration

Header	Value	Purpose
X-Content-Type-Options	Nosniff	Prevents MIME type sniffing
X-Frame-Options	DENY	Prevents clickjacking
Content-Security-Policy	default-src 'self'; script-src 'self'	Prevents XSS and data injection
Strict-Transport-Security	max-age=31536000; includeSubDomains	Enforces HTTPS
Referrer-Policy	strict-origin-when-cross-origin	Controls referrer leakage
Permissions-Policy	camera=(), microphone=(), geolocation=()	Restricts browser features

Table I-1: Security Headers Configuration

I.3 Session and Password Security

Sessions use HMAC-SHA256 signed cookies with HTTP-only, SameSite=Strict, 24-hour expiry, and IP-binding. Password storage uses scrypt (N=16384, r=8, p=1) producing a 64-byte key with 16-byte random salt. Timing-safe comparison prevents timing attacks.

I.4 Rate Limiting and Audit Logging

Rate limiting on authentication endpoints enforces exponential backoff after three consecutive failed attempts. All actions (CREATE, UPDATE, DELETE) are logged with user ID, IP address, timestamp, and action details for complete audit traceability.

APPENDIX J

Research Ethics Approval and Institutional Clearance

This appendix contains templates for the institutional clearance and ethical approval documentation required for this research. The study involves assessment of critical infrastructure security at NRZ, necessitating formal written approval.

J.1 Institutional Clearance Request

TO: The General Manager, National Railways of Zimbabwe

FROM: Munyaradzi A. Patama, Department of Computer Science, Bindura University of Science Education

DATE _____

SUBJECT: Request for Institutional Clearance to Conduct Research on IoT Network Security at NRZ

I am writing to request formal clearance to conduct research on network security in IoT devices at NRZ. This research forms part of the BSc Honours Degree in Network Engineering at Bindura University of Science Education. The study involves structured questionnaires, semistructured interviews, and document analysis. All data will be collected with informed consent, anonymised, and treated with strict confidentiality.

I kindly request approval to: (1) Distribute questionnaires to IT personnel, cybersecurity officers, station managers, and executive management; (2) Conduct semi-structured interviews with selected stakeholders; (3) Review relevant organisational documents; (4) Conduct security configuration audits on a sample of IoT devices with NRZ IT Department supervision.

Applicant Signature _____

Date _____

Supervisor Signature _____

Date _____

FOR OFFICIAL USE ONLY: [ ] Approved [ ] Approved with Conditions [ ] Not Approved

Authorised Signatory (NRZ) _____

Date _____

J.2 Ministry Approval Request

TO: The Permanent Secretary, Ministry of Transport and Infrastructural Development, Government of Zimbabwe

FROM: Munyaradzi A. Patama, Department of Computer Science, Bindura University of Science Education

DATE _____

SUBJECT: Request for Permission to Conduct Research at National Railways of Zimbabwe I am writing to request permission to conduct research at NRZ. NRZ has been identified as a suitable case study due to its increasing adoption of IoT technologies. The study has received institutional clearance from NRZ management and ethical approval from Bindura University of Science Education.

Applicant Signature _____

Date _____

Supervisor Signature _____

Date _____

FOR OFFICIAL USE ONLY: [ ] Approved [ ] Approved with Conditions [ ] Not Approved

Authorised Signatory (Ministry) _____

Date _____

J.3 University Ethics Committee Approval

Field	Description
Project Title	Enhancing Network Security in IoT Devices at NRZ
Researcher	Munyaradzi A. Patama
Supervisor	Mr. Chituma
Department	Department of Computer Science
Degree Programme	BSc Honours in Network Engineering
Date of Application	【____/____/____】
Date of Review	【____/____/____】

Decision	Approved / Approved with Conditions / Revisions Required / Not Approved
Conditions (if any)	【Please fill in】
Committee Chair Signature	_____
Date	【____/____/____】

Table J-1: University Ethics Committee Approval Record