BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE



An Intelligent File Activity Monitoring and Auditing System for Enhancing Data Security: A Case of Bindura Municipality

By

LUCY P MATIKINYIDZE (B222919B)

Supervisor: Mr Chituma

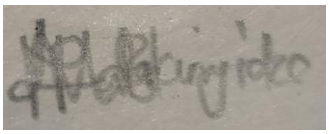
A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE BACHELOR OF SCIENCE HONOURS DEGREE IN NETWORK ENGINEERING

APPROVAL FORM

The undersigned certify that they have supervised B222919B Lucy P Matikinyidze dissertation entitled "An Intelligent File Activity Monitoring and Auditing System for Enhancing Data Security: A Case of Bindura Municipality" submitted in partial fulfillment of the requirements for Bachelor of Science Honors Degree in Network Engineering.

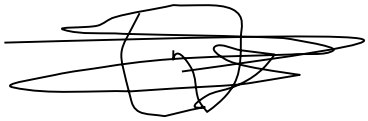
Student: Date:

Lucy P. Matikinyidze…….. 23/06/2026



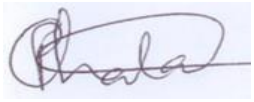
Supervisor: Date:

Mr Chituma……. 23/06/2026



Chairperson: Date:

Mr Chaka……. 23/06/2026





DEDICATION

I would like to dedicate this paper to my family and friends who stood by me throughout my academic journey. They helped me push through as I achieved my goal and because of that I am dedicating this paper to them.

ACKNOWLEDGEMENTS

Recognition is accorded to every individual who made is possible for me to reach the completion of my dissertation on an Intelligent File Activity and Audit System: A Case for Bindura Municipality. Firstly, deepest appreciation is conveyed to mentor Chituma, whose expert guidance, constructive critiques, and unwavering patience were instrumental to the completion of my thesis. The researcher is indebted to Shallon Savanhu who shared her knowledge in information security and assurance which helped me come up with a constructive dissertation.

Lastly, I give thanks to God for the fortitude that I needed throughout the dissertation phase. I am thankful for the perseverance he instilled in me that allowed me to remain steadfast despite the challenges that I encountered. His grace has shined upon me and for that I am grateful for the role he played in my success.

ABSTRACT

The study focuses on the development of an intelligent file activity monitoring and auditing system as a strategic framework to enhance data security and accountability in municipal institutions with Bindura Municipality as the unit of analysis. Anchored in information governance, cyber resilience, and intelligent automation, this study addresses the conceptual disconnect between policy-driven data security regulations and the operational mechanisms necessary for implementation. The rising digitisation of public sector activities has increased the demand for flexible and intelligent systems that can guarantee data integrity, confidentiality and availability. Indeed, many governments continue to rely on piecemeal, manual data management techniques that do not provide real-time visibility and proactive auditing capacity. This system monitors and logs file activity across municipal departments in real time. It flags unauthorized access, unusual behaviour and any bleaches to policy as they happen. There are built in features like automated alerts, audit trails and access controls that help ensure the system stays aligned with data governance standards. With these advanced analytics, security issues can be caught early and detailed logs make it easier to hold actions accountable. This case study demonstrates the potential of adopting such a system to considerably improve the Municipality's data protection framework, mitigate risks, assist informed decision making and increase citizen confidence in e-governance systems.

Table of Contents

APPROVAL FORM i

DEDICATION ii

ACKNOWLEDGEMENTS iii

ABSTRACT iv

CHAPTER 1 1

1.1 Introduction 1

1.2 Background to the Study 1

1.3 Statement of the Problem. 2

1.4 Research Aim 3

1.5 Research Objectives 3

1.6 Research Questions 3

1.7 Research Propositions / Hypothesis 4

1.8 Justification / Significance of the Study 4

1.9 Assumptions 4

1.10 Limitations / Challenges 4

1.11 Scope / Delimitations of The Research 5

1.12 Definition of Terms 5

1.13 Summary 5

CHAPTER 2 6

LITERATURE REVIEW 6

2.1 Introduction 6

2.2 Conceptual Framework 6

2.2.1 Input-Process-Output (IPO) Model 6

2.2.2 Zero Trust Architecture (ZTA) Model 7

2.2.3 Behavioural Anomaly Detection Model 8

2.3 Theoretical Framework 9

2.3.1 Real-Time Monitoring Theory: Event-Driven Architecture and Stream Processing 9

2.3.2 Audit Trail Integrity Models: Cryptographic Immutability and Zero Trust Principles: 10

2.3.3 Behavioural Anomaly Detection Theory: Machine Learning and Statistical Foundations 11
2.3.4 Integration of Theoretical Models 12
2.4.1 Local Studies: Zimbabwean Context 12
2.4.2 Regional Studies: African Context 13
2.4.3 Global Studies: International Perspectives 13
2.5 Research Gaps 13
2.6 Summary 14
CHAPTER 3 15
RESEARCH METHODOLOGY 15
3.1 Introduction 15
3.2 Research Approach 15
3.2.1 Qualitative Approach 15
3.2.3 Population and Sample Size 16
3.2.4 Reliability and Validity 17
3.2.5 Ethical Considerations 17
3.3 Existing System 17
3.3.2 Context Level Diagram 18
3.3.3 Process Flow Diagram 20
3.4 Requirements Analysis 22
3.4.1 Functional Requirements 22
3.4.2 Non Functional Requirements 23
3.4.3 Technical Requirements 24
3.5 System Flowchart 25
3.6 System Development 26
3.6.1 Agile Iterative Model 26
3.7 Feasibility Study 27
3.7.1 Technical Feasibility 27
3.7.2 Economic Feasibility 28
3.7.3 Operational Feasibility 29
3.7.4 Legal and Ethical Feasibility 30
3.8 System Analysis 30

3.8.1 System Architecture 30
3.9 System Development Tools 33
3.10 Coding 33
3.11 Validation and Verification 37
3.12.1Bias and Fairness 37
3.12.2 Accountability 37
3.13 Limitations 38
3.14 Summary 38
CHAPTER 4 39
DATA PRESENTATION, ANALYSIS AND INTEPRETATION 39
4.1 Introduction 39
4.2 Analysis of the existing system 39
4.3 System testing 39
4.3.1 Black box Testing 40
4.3.2 White Box Testing 43
4.3.3 Unit Testing 43
4.3.4 Integration Testing 44
4.3.5 Security Testing 46
4.3.6 Validation Testing 48
4.3.7 Acceptance Testing 48
4.4 Results of System performance 49
4.4.1 Real-Time Monitoring Efficiency 49
4.4.2 Anomaly Detection Results 50
4.4.3 Audit Log Generation 50
4.4.4 Alert and Notification System 52
4.4.5 Automated Reporting 52
4.5 System Evaluation 52
4.6 User Feedback Analysis 53
4.7 Comparison Between Existing and Proposed System 53
4.8 Summary 54
CHAPTER 5 55

CONCLUSIONS AND RECOMMENDATIONS 55
5.1 Introduction 55
5.2 Summary of the Study 55
5.3 Conclusions 56
5.4 Recommendations 57
5.5 Areas for Future Research 58
5.6 Summary 60
References 61
APPENDIX 67

CHAPTER 1

INTRODUCTION

1.1 Introduction

The study aims at developing a monitoring and auditing system for file activity in Bindura Municipality to enhance data security and accountability. As municipal institutions shift more services online, keeping data secure has become a real challenge. More files and records are now digital, necessitating mechanisms to protect data secrecy, accuracy, and accessibility (Chundu, Masamha & Sifile, 2025). Without proper monitoring and audits it is easy for unauthorized access and data breaches to slip through and lose accountability. Bindura Municipality has been facing this challenge as they are storing more sensitive data like payroll and personal records digitally and protecting that information has become difficult as the systems grow more complex. This problem can be explained by similar trends found in the region. According to Abbas et al. (2022) it is shown that developing country efforts within the process of digitalization have led to deterioration of governance in institutions. At present, there is no known protocol for conducting an audit on file activity in Bindura Municipality. In doing so, the organization is still susceptible to insider threats, data theft, amongst other challenges. This chapter aims to provide the reader with the research overview.

1.2 Background to the Study

The rapid digitalization of activities at the municipal level has been connected with the generation and handling of significant amounts of data, which could be classified as highly sensitive and confidential, including financial, personal details of people, and communications. High security standards regarding these kinds of data must be provided as the importance of maintaining efficiency in terms of these organizations cannot be overstated. Zvaita & Shava (2026) support this view, revealing that without laying the necessary groundwork for the management of data within these municipalities, it is impossible to become effective, even by using digital instruments. Nonetheless, data handling in the Bindura Municipality is conducted through traditional methods that include outdated manual processes, making it difficult to get real-time visibility on the activity and appropriate auditing. ICT specialists often struggle to

detect problems, carry out investigations, or ensure compliance with Zimbabwe's Cyber and Data Protection Act, Chapter 12:07.

1.3 Statement of the Problem.

Due to the growing trend of digitization throughout the world, both government and private companies have come to possess highly confidential digital data. Sensitive data security has become a major concern due to cyber-related issues such as theft and misuse of information. According to IBM (2024), organizations worldwide face average losses approaching five million dollars per breach. Global frameworks like ISO/IEC 27001 and the European Union's GDPR emphasise the importance of maintaining audit trails, monitoring, and accountability in relation to data access and modification (ISO, 2022; European Commission, 2018). But then again, despite the requirements internationally, many government agencies, especially in developing countries, fail to have adequate measures in place regarding the prevention and control of file activities (UNECA, 2022; Timcke, Gaffley and Rens, 2023). Talking about regions, Africa has entered into an unparalleled digitization era in the public sector, but most organizations cannot cope with the cyber threats aspect. The African Union introduced the Convention on Cyber Security and Personal Data Protection, commonly known as the Malabo Convention, in 2014 (African Union, 2014). The said convention calls for member states to develop policies which will guarantee the security, confidentiality, and integrity of digital data (African Union, 2014). Nevertheless, adherence to the policies varies widely across the continent. As noted by Timcke, Gaffley and Rens (2023), local authorities in Sub-Saharan Africa persist in relying on archaic means of storing and analyzing data, thereby making the area susceptible to data manipulation, internal threats, and failure to comply with current legislation concerning data security. With many regional governments increasingly embracing the concept of e-governance through offering digital services to their citizens, there exists a significant threat in the lack of intelligent file monitoring and auditing processes (World Bank, 2023). In Zimbabwe, the enactment of the Cyber and Data Protection Act [Chapter 12:07] in 2021 illustrates the country's commitment to safeguarding information security and privacy (Government of Zimbabwe, 2021). Despite this, most municipalities including Bindura Municipality apply manual and uncoordinated systems of managing the information within the system which do not ensure automatic centralization of tracking the files' actions in the respective departments (Zvaita and Shava, 2026). Consequently, the identification of any security breach action occurring in the system is hindered and cannot

help to determine the source and extent of the security risk (Cornelius and Jansen van Rensburg, 2024). Further, in case security problems occur in the municipality's system, fragmented audit trails make the investigation more difficult. According to the author, municipalities deal with sensitive information including financial, payroll, and financial statements information which if stolen causes significant harm to the organization. Intelligent monitoring would also create issues regarding fulfilling the responsibilities of accountability and transparency as required in the National ICT Policy Framework of Zimbabwe (2021). The current manual procedures would fail to provide real-time visibility, accurate audit logs, and adherence to any policy regarding data protection. High levels of risks of accessing confidential data would become apparent, as well as other risks such as insider attacks and slow response to data breaches. The use of an intelligent monitoring system would increase the degree of data protection, accountability, and compliance.

1.4 Research Aim

To design and develop an intelligent file activity monitoring and auditing system that enhances data security and accountability at Bindura Municipality.

1.5 Research Objectives

i. To document the existing file activity monitoring and auditing mechanisms and vulnerabilities at Bindura Municipality.

ii. To design an integrated system architecture for real-time monitoring, auditing and anomaly detection.

iii. To develop and test a prototype system with intelligent alerting and automated reporting features.

iv. To implement a real-time file activity monitoring mechanism that tracks, logs, and audits file-level operations across the municipal information system.

1.6 Research Questions

i. What mechanisms are currently used by Bindura Municipality to track and audit file activities?

ii. What vulnerabilities exist in the municipality's current file management and security framework?

iii. How can an intelligent system be designed to monitor file activities, generate audit logs, and flag anomalies in real time?

iv. How can automated reporting features be developed to summarize file activities and security events for accountability and decision-making?

1.7 Research Propositions / Hypothesis

Ali et al. (2025) suggest that implementing an automated file monitoring and auditing system would significantly enhance data security, accountability, and compliance at Bindura Municipality.

1.8 Justification / Significance of the Study

This study is important since it will help in improving the management of data security in local government organizations. Through its automatic monitoring and auditing process, it increases accountability, complies with data protection regulations, and facilitates transparent handling of information (Liang, 2024). The suggested system supports the objectives of the national e-governance strategy and complies with the requirements of the Cyber and Data Protection Act [Chapter 12:07] by promoting secure data handling practices (Government of Zimbabwe, 2021). From an academic perspective, the study will provide a practical example of application of networking engineering and cybersecurity principles (Abbas et al., 2022).

1.9 Assumptions

i. Access will be granted by the Bindura Municipality to their ICT systems along with the necessary data used during evaluation.

ii. ICT staff will work together and provide accurate information throughout the interviews and system evaluation.

iii. The current structure of the ICT will facilitate the implementation of the proposed intelligent monitoring system.

iv. The test data will reflect real-world scenarios.

v. Data protection knowledge is present and there are documents on data protection.

1.10 Limitations / Challenges

i. Time may be an issue in this research because it can prevent the full-scale evaluation of the proposed research.

ii. The confidential information needed in this research may not be available.

iii. Financial constraints can affect the implementation of the proposed system.

iv. The ICT employees can require training for the efficient use of the new system.

v. Performance is favoured more than integration in this research.

1.11 Scope / Delimitations of The Research

i. Scope of Study: The scope of the study is confined to the ICT department of Bindura Municipality.
ii. Scope of the system: The scope of the study would include file monitoring, auditing and notification; network intrusion detection system would not be covered.
iii. Scope of Users: The users considered in the study are restricted to those associated with ICT department in file operations and system administration.
iv. Scope of Geography: The scope of the project would be confined to Bindura Municipality.
v. Scope of time: This study would be carried out within the prescribed academic period.

1.12 Definition of Terms

i. File Activity Monitoring (FAM): This refers to the practice of logging the interactions of users with their files in order to enhance security.
ii. Audit Trail: This is defined as the historical log of activities performed either by the computer systems or users.
iii. Data protection: This is a means of protecting information from any form of alteration or theft.
iv. Intelligent system: This is a technology driven mechanism that uses automation or artificial intelligence to perform certain functions.
v. Accountability: Refers to the responsibility to answer for something.

1.13 Summary

In this chapter, the background of the research aimed at the development of an intelligent file activity monitoring and auditing system for Bindura Municipality has been presented. The background has been provided in the context of the increasing issue of data security in the current digital world, identifying that there is no central real-time monitoring system as the major problem. The research aim and objectives have been provided together including the guiding questions. Its significance has been highlighted in relation to compliance and transparency.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In the current chapter, there will be presented a comprehensive literature review on the study conducted by researchers on the development of intelligent file activity monitoring and auditing system for improved security and accountability of data in Bindura Municipality. In the literature review, there will be addressed the issues of file activity monitoring, auditing systems and intelligent security systems focusing mainly on the issues of real-time monitoring, auditing, alarm systems, and automated reporting which forms the basis of the current research topic.

2.2 Conceptual Framework

A good conceptual framework must be created in order to develop an efficient file activity monitoring system in Bindura Municipality. The three models that will be combined to form a comprehensive conceptual framework have been carefully selected because they include all the necessary aspects of the development of such a conceptual framework. The models selected are IPO, ZTA, and Behavioural Anomaly Detection. The chosen models give a wholesome overview of the issue being examined, and they can be considered theoretical and practical because of the limitations that municipalities face in developing countries (Chen & Zhang, 2021; Rose et al., 2020).

2.2.1 Input-Process-Output (IPO) Model

IPO Model has been chosen as the underlying architecture of the system, offering an efficient process where inputs are systematically turned into valuable outputs (Kumar et al., 2022). The input in question consists of all actions taken in regard to files within the municipality network such as file creation, modification, deletion, or movement. Inputs of this type are collected through systems' monitoring mechanisms and audit logs. Then, the collected data undergoes several processes, such as normalization, correlation, and enrichment to structure itself accordingly to the security standards (Williams, 2020). Lastly, outputs consist of audit trails, alerts, reports, and dashboard visualizations for different stakeholders who are involved in the monitoring processes including municipal officials and IT personnel (Almeida & Santos, 2023). The biggest benefit associated with employing the IPO Model lies in its simplicity which would facilitate adoption on part of the stakeholders. Another great aspect of the IPO Model is related

to the modularity which enables the municipality to start monitoring high-risk data first and proceed to other data types later (Chikwanda et al., 2022).

2.2.2 Zero Trust Architecture Model

ZTA is a security model which underpins the monitoring system's security architecture (Rose et al., 2020). Whereas conventional security strategies assume that everything inside the organizational perimeter is trustworthy, the ZTA takes an opposite approach, advocating for the notion "never trust, always verify" (Zhang et al., 2022). According to this security model, threats could emerge from either external or internal sources, including those coming from legitimate users with malicious intentions. Some of the unique aspects that make ZTA particularly beneficial in municipal environments dealing with sensitive information about citizens include stringent identity verification of all accesses requests by implementing continuous verification and multi-factor authentication, enforcing least privilege, and introducing micro-segmentation in case of a threat. For instance, for file monitoring, ZTA makes sure all the processes of access to the file are verified, which gives room for an accountable chain of evidence needed under the regulation like Cyber and Data Protection Act [Chapter 12:07] of Zimbabwe (Zimbabwe Data Protection Authority, 2023).



Figure 1. Zero Trust Architecture

2.2.3 Behavioural Anomaly Detection Model

The third concept from the Conceptual Framework is Behavioural Anomaly Detection Model. It involves artificial intelligence and adaptability while detecting an anomaly (Zhang et al., 2022). Behavioural Anomaly Detection applies artificial intelligence technology to build the typical pattern of user behaviour and identify anomalies. In contrast to the rules-based approach, which has predetermined features of security threats, this technique can detect unknown forms of attacks. The behaviourally driven method comprises different types of anomalies: supervised learning by analysing past events for the identification of already known malicious patterns, unsupervised learning for discovering new types of abnormalities, and reinforcement learning for improvement of the algorithms through the feedback mechanism (Few, 2020). Concerning the municipal sector, the usage of a behavioural anomaly detection model will be highly efficient since the processes in the operational department of a municipality occur according to strict schedules. Also, the roles of all employees are predefined. Considering these factors, the system may learn the typical activities of the particular user group and find anomalies. Among them are unusual access to the files, downloading a lot of information at unusual times, or attempting to use the information related to a completely different role (Kufandirimbwa & Zanamwe, 2023).

Combining all three models into one will result in the development of an integrated comprehensive model that will address all issues related to the municipal monitoring requirements. IPO model provides for the flow process from collecting information to the generation of the results, while the ZTA model addresses the aspect of access control, and the Behavioural Anomaly Detection model is responsible for the intelligent threat detection. It is through these models that the cybersecurity trilemma associated with cybersecurity issues in the public sector is solved (World Bank, 2023). The trilemma refers to the aspect of balancing between security, availability, and resource issues. According to this model, an implementation of such a file monitoring system does not solely rely on detecting threats but also involves other aspects such as operational efficiency, compliance, and public confidence in cyber governance processes (UNECA, 2022). It is from this perspective that the model sees the proposed system not only as a security system but also as part of the digital governance system of Bindura Municipality. This proposed system can easily adapt to technological changes while still being practical for use in the municipal environment (Oti & Mutua, 2023).

2.3 Theoretical Framework

The creation of the task at hand is based on theory built on the principles of Real Time Monitoring Theory, Audit Trail Integrity Models, and Behavioral Anomaly Detection Theory. This theoretical base is critical in laying down a scientific foundation that will be used to develop an intelligent file activity monitoring and audit system appropriate for the operations at Bindura Municipality. Justification for the application of each of the models lies not only on their applicability to cybersecurity issues but also to resource-limited environments.

2.3.1 Real-Time Monitoring Theory: Event-Driven Architecture and Stream Processing

Real time monitoring relies on event driven architecture (EDA), which processes streams of events that help in real time analysis and reaction to security events. Real time monitoring does not rely on batch processing, but EDA works by propagating events based on their occurrence in the system (Williams, 2020). This is important in cybersecurity since delay can lead to loss of valuable data.

The theoretical underpinnings of real-time monitoring include:

Complex Event Processing (CEP): This sub-theory deals with associating lower level events with higher level security incidents. CEP utilizes pattern matching techniques and temporal logic to detect sequences of events that might signal some malicious intent, e.g., several unsuccessful access attempts preceding successful unauthorized access (Luckham, 2002). CEP can be applied by Bindura Municipality in order to associate raw log files with actual security threats.

Lambda and Kappa Architectures: These architectural approaches incorporate both real-time and batch processing capabilities. In particular, the Lambda Architecture is characterized by a combination of speed and batch layers, which guarantee that all aspects of data will be analysed thoroughly, whereas the Kappa Architecture simplifies the above design by means of stream processing only (Marz & Warren, 2015). Thus, these theories provide grounds for developing the necessary software solution.

Publish-subscribe paradigm: This theoretical model involves distributing event notifications by monitoring agents (publishers) to the subsystems interested in receiving such notifications (subscribers). The described design approach ensures efficient and scalable dissemination of events throughout municipal units (Eugster et al., 2003).

Justification for Municipal Context: Real-time monitoring theory is crucial for Bindura and other cities whose processes may fail due to ineffective manual surveillance and late reaction to incidents, which results in lack of compliance and lack of trust from the public. Utilizing the EDA and streaming approaches suggested above, continuous surveillance will be achieved.

2.3.2 Audit Trail Integrity Models: Cryptographic Immutability and Zero Trust Principles: Audit trail integrity relies on cryptographic principles of immutability and the Zero Trust Architecture (ZTA). Core elements such as non-repudiation, verifiability, and authentication are essential to ensure that audit trail information remains tamper-proof and legally valid under the Cyber and Data Protection Act [Chapter 12:07] (Government of Zimbabwe, 2021).

Key theoretical components include:

Hashing in Chain of Cryptographic Logs: It entails the application of cryptographic hashing methods like SHA-256 to link log entries in chronological order. Log entries involve the hash values of preceding entries. A change in log entries leads to the breaking of chain links, which serves as tampering evidence (Haber & Stornetta, 1991). The principle may apply to municipalities in case of a forensic examination in the event of a legal dispute.

Digital Signatures and Non-Repudiation Principle: It is the concept that enables the tracing of activities to a user via PKI. Non-repudiation is a principle which ensures actions performed by a user cannot be denied once required in organizational procedures (Schneier, 2015).

Zero Trust Architecture: ZTA is a practice that employs the principle "never trust, always verify." The technique operates on the assumption that neither individuals nor processes can be trusted irrespective of their position with regards to the network perimeter. NIST SP 800-207 states that Zero Trust Architecture emphasizes ongoing user verification, restricted access based on need, and network segmentation at a granular level. These mechanisms ensure that access requests are logged and verified during file auditing (Rose et al., 2020).

Timestamping Protocol: The concepts like Timestamp Protocol (TSP) and blockchain-based timestamping help create a means for proving that an entry existed at a certain point in time. It becomes important since timestamps can be used in forensic investigation as well as evidence in legal cases (Buldas et al., 2013).

Justification for Municipal Context: The information belonging to the citizens stored at the municipal level is highly confidential, and it should therefore be protected from any form of alteration or access by unauthorized persons. Cryptography and Zero Trust theories form a good foundation that is strong enough to ensure a secure audit process. They are both scalable and adaptable to Bindura Municipality conditions.

2.3.3 Behavioural Anomaly Detection Theory: Machine Learning and Statistical Foundations

This is a theory based on data-driven models, statistical outlier detection, and user behaviour analytics (UBA). Contrary to signature-based solutions that depend on existing signatures, anomaly detection systems do not detect malicious activity based on existing rules but learn how normal user activity should look like.

Theoretical pillars include:

Supervised Learning Algorithms: This uses labelled datasets (either normal or malicious). There are various forms of supervised machine learning algorithms used to detect anomalies and include CNN, LSTM, SVM etc**.** (Kohli & Chhabra, 2025). This demonstrates how labelled datasets will help to train the model and classify it to detect whether an activity is either normal or malicious. Unsupervised learning algorithm will also help in classifying file accesses using information from the past.

Unsupervised learning algorithms: They entail use of clustering algorithms which include K-means and DBSCAN while density estimation uses Gaussian mixture model for outlier detection in the dataset. (Kohli & Chhabra, 2025) gives an extensive review of deep learning models for detecting anomalies with emphasis on unsupervised learning algorithm and other methods like auto encoder, clustering etc.

Semi-Supervised and Hybrid Models: Lau et al. (2025) formally relate unsupervised and semi-supervised anomaly detection through an approach that increases detection accuracy via exploitation of small amount of labelled anomalies and anomaly synthesis with theoretical guarantees of convergence.

Reinforcement Learning for Optimal Detection: This approach makes possible the creation of optimal detection strategies through interacting with the environment. Applying the concept of

Markov Decision Processes (MDPs), reinforcement learning constantly optimizes detection algorithms based on feedback mechanisms (Arulkumaran et al., 2021). In addition, it allows understanding how to change alert threshold depending on the number of false alarms.

User and Entity Behaviour Analytics (UEBA): This approach helps detect behavioural patterns and form user and device profiles. The theoretical base lies in the application of such methods as sequence analysis, graph theory and time series analysis to detect signs of compromises like data exfiltration or privilege escalation (Gavai et al., 2015).

Rationale from a Municipal Point of View: The municipal IT system usually has clear user profiles and patterns of behaviour, thus this kind of analysis is applicable in this situation. Machine learnin

g algorithms can be trained specifically for one environment thanks to using local training data sets and avoid false alarms in Bindura. Also, it does not require lots of computer power.

2.3.4 Integration of Theoretical Models

The theoretical constructs outlined above operate in an integrated manner rather than independently. Real-time monitoring generates the data, audit integrity models ensure its secure storage, and behavioural anomaly detection models examine the stored data to identify irregularities. The proposed solution falls into line with the concept of Defense-in-Depth strategy for cybersecurity, which presupposes different levels of protection controls. This theory resolves the trilemma of security, openness, and accessibility of data.

2.4 Empirical Evidence

This section examines empirical studies conducted at local, regional, and global levels regardifile activity monitoring, auditing systems, and municipal data security.

2.4.1 Local Studies: Zimbabwean Context

As per the research done by Chikwanda et al. (2022), only 23% of the total number of municipalities in Zimbabwe were conducting some form of file auditing practice. It should be mentioned that Bindura Municipality was characterized by poor file auditing procedures. According to Zimbabwe Data Protection Authority (2023), the technical compliance rate was 38%. The more significant issue, however, was that there was the matter of audit trail shortage

which was raised by Zimbabwe Data Protection Authority. A case study performed by Muzata (2023) revealed that there were 47 days of unauthorized activity because of the lack of monitoring.

2.4.2 Regional Studies: African Context

The automated surveillance system decreased the detection time of incidents in municipalities of East African countries by 72%, stated Moyo and Ndlovu (2023). However, 41% of the software solutions used for monitoring were discontinued due to their complex structure and high cost. According to Kufandirimbwa and Zanamwe (2023), the effectiveness of such solutions is evidenced by the fact that there was a 64% decrease in unauthorized access to documentation within 18 months, despite all problems associated with the installation of a new application on an existing system.

2.4.3 Global Studies: International Perspectives

According to an EU Agency for Cybersecurity (ENISA, 2021) report, artificial intelligence surveillance lowered the number of false positives by 83% in comparison to the rule-based surveillance systems used in European cities. According to Patel & Lee (2023), use of the block-chain technology in audit processes in North America increased the efficiency of the forensic investigation process by 56%; however, the costs were relatively high. Kim et al. (2021) found that the implementation of surveillance systems in Singapore and South Korea led to a 42% improvement in regulatory compliance.

2.5 Research Gaps

Despite advances in file auditing and monitoring**,** there is limited research on integrated, intelligent systems tailored for municipal governments in developing countries**.** Existing studies mainly focus on corporate or enterprise contexts and often examine isolated techniques rather than comprehensive frameworks combining real-time monitoring, anomaly detection, and automated reporting. Additionally, there is insufficient consideration of operational constraints, regulatory compliance, and resource limitations in municipalities like Bindura. Finally, few studies evaluate the practical effectiveness and sustainability of such systems in real-world public-sector settings, leaving a clear gap for context-specific, efficient, and accountable file activity monitoring solutions.

2.6 Summary

The above mentioned chapter has systematically evaluated the existing literature in the field of monitoring and auditing systems with respect to the following criteria; the conceptual models, theoretical frameworks and empirical evidence both locally, regionally and internationally. Three conceptual models; IPO Model, Zero Trust Architecture Model and Behaviour Anomalies Detection were discussed and then integrated to create a model that would guide in the system design process. The theoretical frameworks included real-time monitoring, audit integrity and behaviour anomalies detection theory which have been used to justify and explain how the functions of the system can be performed. The findings from empirical studies showed significant gaps in municipal cybersecurity measures especially in Zimbabwe.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

The development of an intelligent file activity monitoring and auditing solution is vital for effective strengthening of data security, accountability and compliance with various data protection requirements by municipalities. The current chapter explains the methods used for research utilised in the study that presents the approach that will be used in constructing the recommended intelligent solution. The study strives mainly at identifying the existing systems used to monitor file activities, proposing the architectural design of the system, developing a prototype with intelligent monitoring functions and testing the efficacy of the prototype based on the developed audit logs, alerts and reports.

3.2 Research Approach

The research approach adopted in this study involves the use of Design Science Research (DSR). This is a research philosophy that deals with the creation and evaluation of artefacts for solving organisational problems (Hevner et al., 2004). Here it is appropriate since the aim is to analyse existing practices, and to design, construct and evaluate an intelligent file activity monitoring and auditing system as a practical artefact. This study used the Design Science Research (DSR) framework and mixed methods strategy. The mixed methods methodology involves both qualitative and quantitative methodologies to obtain a broader scope. The research methodology functions as the structure that guides the study, influencing how data is collected, analyzed, and interpreted in addressing the core issue. It is used here to describe the approach adopted in developing the intelligent monitoring and auditing system for Bindura Municipality. The framework also explains the rationale for relating the research philosophy to the approaches adopted and thereby explaining the approach employed to tackle the problem at Bindura Municipality.

3.2.1 Qualitative Approach

Qualitative research as discussed by Denzin and Lincoln (2018) is especially appropriate when conducting research related to real-world conditions because the emphasis is put on the meaning attached to things, people's experience, and viewpoints in the situation being analyzed. In this

case, qualitative methods allow for gaining knowledge regarding the nature of current file monitoring procedures, finding out what stakeholders require from the software, discovering limitations of the organization, and analyzing perceptions of users in regard to usability and usefulness of the system in question. The information gathered will be essential as the success of the project will not only depend on technology used but also on acceptability of the solution along municipal employees.

i) Interviews: ICT staff and management officials were interviewed to understand current file activity monitoring procedures, difficulties and expectations for system upgrades.
ii) Observations: I observed the current file management workflow at first-hand and that helped me see the workflow and where the system was vulnerable.
iii) Document Analysis: I reviewed the existing audit methods, policy documents, system logs and municipal ICT standards to identify where compliance was falling short.

3.2.2 Quantitative Approach

Creswell and Creswell (2018) explain that quantitative research involves the use of statistical data to test hypotheses, measure variables, and establish objective facts. In this study, the quantitative approach is applied to evaluate the performance, effectiveness, and accuracy of the file activity monitoring and auditing system at Bindura Municipality. Some of the methods that will be used include:

i) System Testing: The pilot system was assessed in a simulated environment for efficiency, accuracy of anomaly detection and audit record production.
ii) User Surveys: Structured surveys were administered to the municipal personnel to acquire quantifiable feedback on the usability, reliability, and perceived efficacy of the system.
iii) Questionnaires: They were distributed to a larger sample of municipal employees to measure awareness of data security practices and evaluate acceptance of the proposed solution.

3.2.3 Population and Sample Size

The audience that is targeted was ICT staff, system administrators and management professionals at Bindura Municipality who are directly involved in file management and system administration. Purposive sampling was employed to identify volunteers with relevant experience. Eight ICT personnel and management specialists were questioned, whereas 20

regular municipal staff members were given a questionnaire. The sample size was deemed adequate in view that there are few people in the ICT department as well as the particular case study nature of the research.

3.2.4 Reliability and Validity

To establish dependability, an interview guide and questionnaire were piloted with two ICT staff before the main data gathering exercise. The pilot provided feedback to improve the clarity and organization of questions. The system performance tests were run several times under similar settings to verify the consistency of the results. Validity was addressed through cross-checking findings from interviews, questionnaire responses, direct system observation and system performance testing using triangulation. Member verification was also used to verify the correctness and relevance of the important findings by sharing them with chosen participants. The system artefact was checked against the behavioural and quality requirements defined earlier.

3.2.5 Ethical Considerations

During this study, I adhered to ethical guidelines. Every participant provided a signed a formal agreement before starting to collect data. I managed to implement measure to guarantee complete respondent privacy and data was secure. No participant is identified by name in the findings. Institutional clearance was sought from Bindura University of Science Education and authorisation to conduct research in Bindura Municipality was acquired from the relevant authorities. For privacy reasons the technology was tested on produced data rather than genuine city records. The system was created with the intention of measuring file usage rather than individual employee performance. Prior to the implementation of the system, the staff were educated on its usage in line with ethical standards regarding workplace surveillance (British Educational Research Association [BERA], 2024; Tripathi & Chaturvedi, 2023).

3.3 Existing System

At present, Bindura Municipality uses the traditional file management system that lacks auditing features. Although the system supports some basic controls, it cannot monitor the activities in

files in real time or maintain audit logs. This means that any malicious activity performed by a person who manages to gain unauthorized access will remain unnoticed. This makes the system prone to any attack because sensitive information of Bindura Municipality will be exposed.

3.3.1Constraints of the Existing system

1. The Inefficiencies of Real-Time Monitoring: The log for changes and access events can only be done manually, hence late detection of any unauthorized access.
2. Not Scalable: When there are numerous files to be processed, manually monitoring them will become even more complicated.
3. Prone to Human Error: Any errors made during manual input of the information will render the whole process useless.
4. No Built-in Reports: Producing necessary reports can become tedious and resource-intensive.
5. Compliance monitoring: Automatic monitoring and reporting are essential for compliance.

3.3.2 Context Level Diagram

In terms of context, the existing manual process in the Bindura municipality involves both staff members and administrators, as well as auditors. Files are manually updated and accessed by the staff members, while administrators keep logs and the auditors call for compliance reports. The whole process is done using both paper-based and digital storage without any automation.

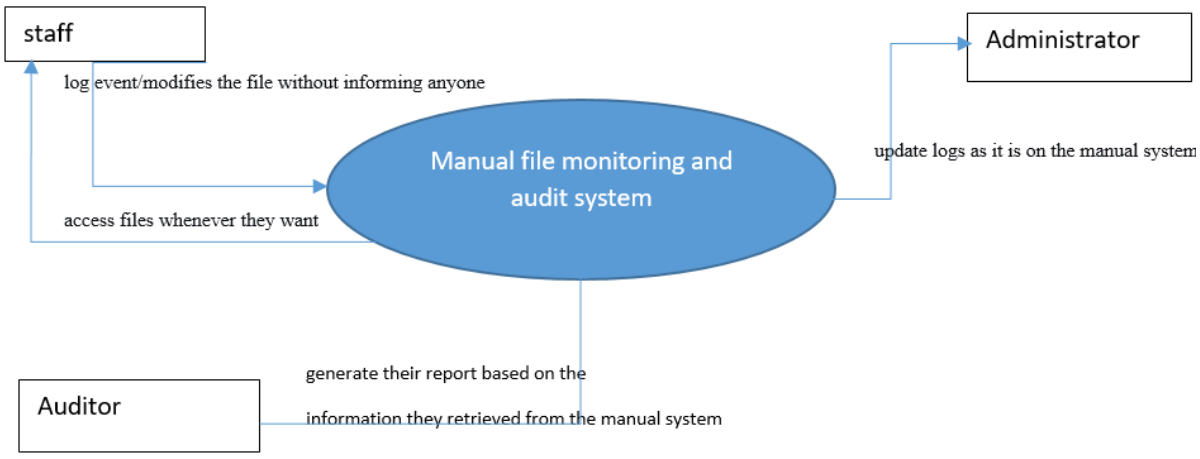
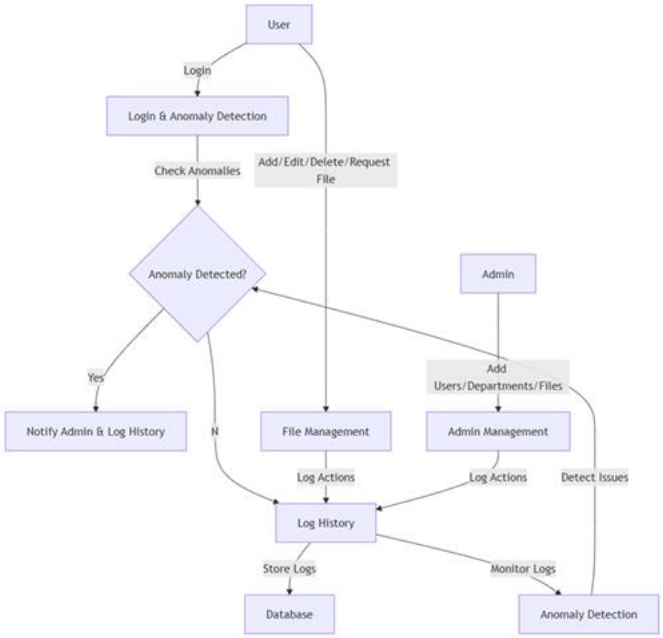
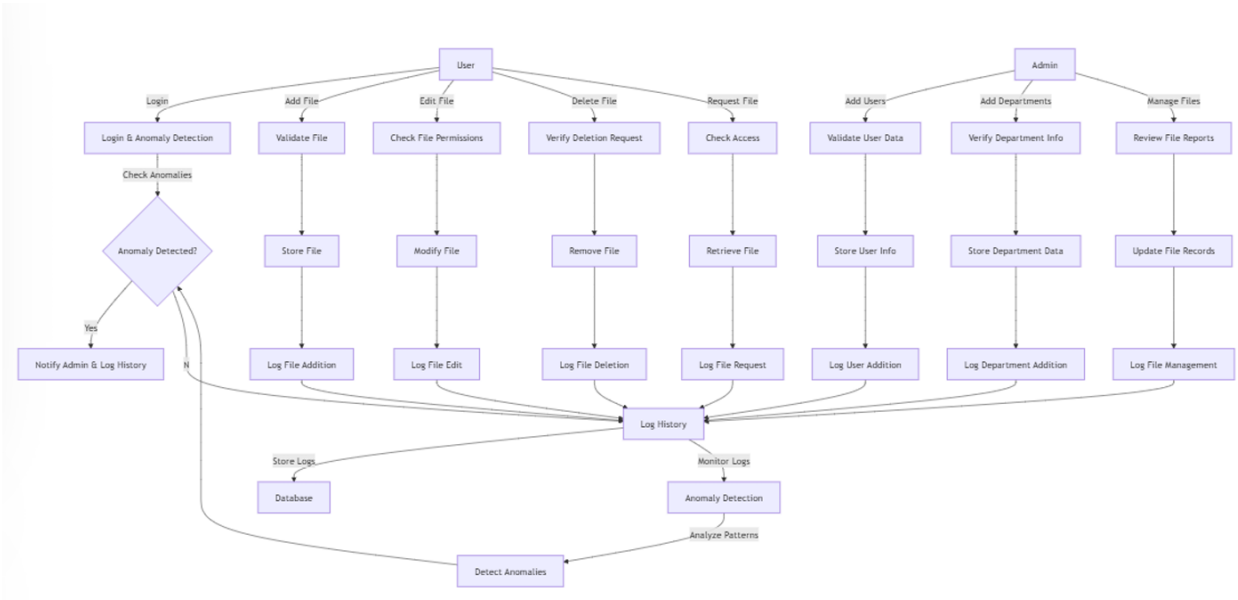


Figure 2. General architecture Diagram

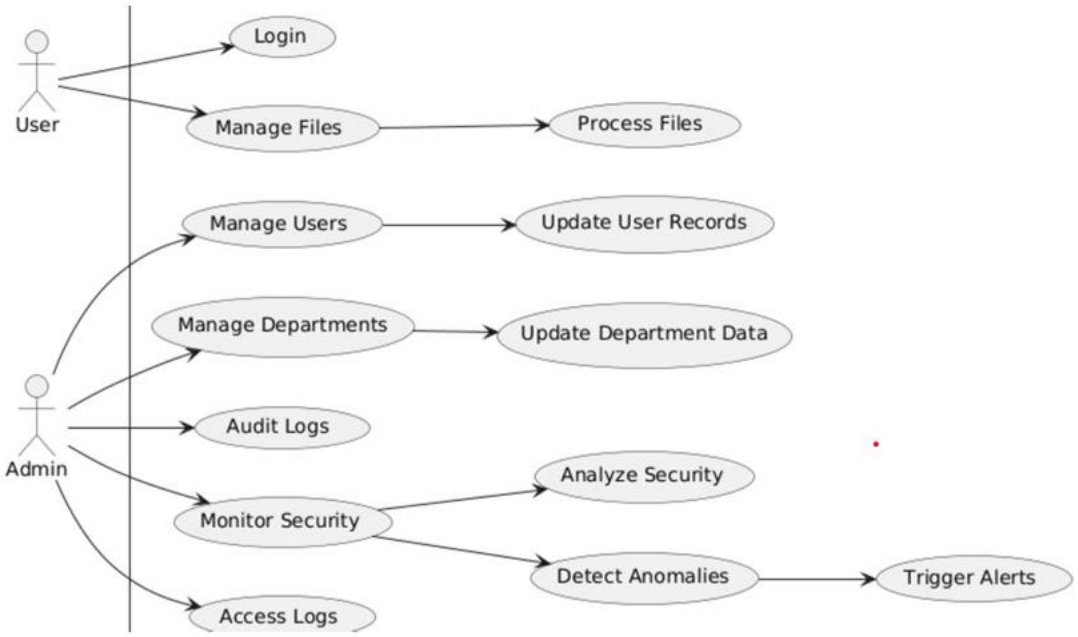
3.3.2.1 DFD Level 1



3.3.2.2 DFD Level 2



3.3.2.3 Use Case



3.3.3 Process Flow Diagram

In the current manual system, file processing commences when there is a request from the user, then there is a manual authorization check. The retrieval and updating of files is done without automation, and the logging is done manually. There will be reports only when there is a request for them, thus taking a lot of effort to do this.

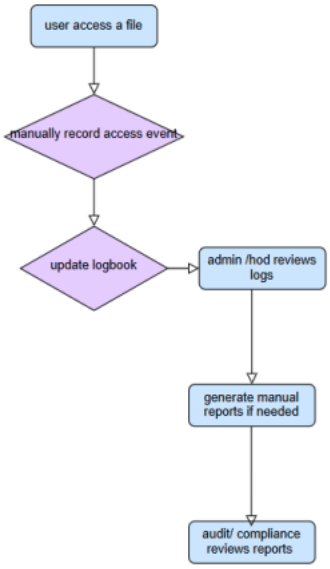


Figure 3. Process Flow

3.3.4 Use Case Diagram

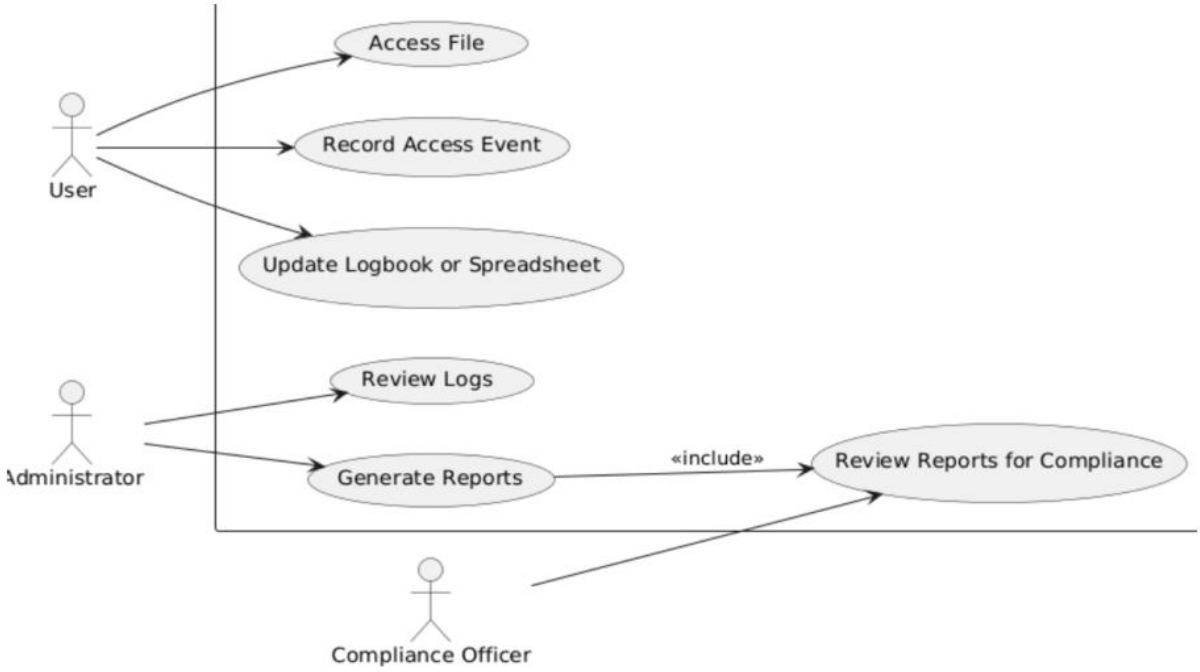


Figure 4. Use Case Diagram

3.4 Requirements Analysis

Requirements analysis helps determine the expectations of the end-users of the solution.

3.4.1 Functional Requirements

Functional requirements are the critical capabilities required from the File Audit System. They help ensure that file actions are monitored effectively and that the system complies with relevant data protection laws.

1.User Authentication and Authorization

- Secure login methods for administrators and other users shall be made available through the system.
- There shall be role-based access control in place for accessing resources based on the users' roles.
- Administrators shall be able to manage user accounts such as creating new ones or deleting them.

2. File Activity Monitoring

- Each activity undertaken related to the files must be recorded in the system. These include creation, modification, deletion, and access to the files.
- The activities should be documented along with details including time stamp, user id, file name, and activity undertaken.
- The live dashboard should be displaying the activities of the files.

3. Real-Time Alerting for Suspicious Activities

- The security system should detect any attempt at unauthorized access and should also detect anything strange about how files are handled.
- If there is any indication that an attack might occur, then immediately alert the administrators.
- A record of all such occurrences should be kept.

4.User File Operations

- The users should have the ability to create, read, and delete files on the system.

- The system should provide an option for requesting access to designated files with administrative permission.
- Permission should be granted based on whether the user can access the file authorized by the system.

5. Comprehensive Audit Logs and Reports

The system shall generate detailed audit logs containing:

- Event ID
- Device
- Username
- Action performed
- Event Time
- File Path
- Department
- Status

Administrators shall be able to search and filter logs for efficient review using status, action and date features on the audit log module.

6. Administrator Functions

Administrators will have the ability to:

- Define access control policies for file operations
- Configure security settings, including encryption
- Monitor logs and investigate potential breaches

7. System Security and Integrity

- Audit logs shall be encrypted to prevent tampering using the AES-256 which is a NIST – approved standard, hardware-accelerated on most modern CPUs hence it is fast on big logs with high security.

3.4.2 Non Functional Requirements

1. Performance and Scalability

- The system needs to handle concurrent file operations from multiple users without performance degradation.
- It ought to support scalability to accommodate increasing numbers of users and files.

2. Security

- Audit logs shall be encrypted against unauthorized access and tampering Including RBAC implementation.
- Compliance with relevant data protection policies, including the General Data Protection Regulation and Health Insurance Portability and Accountability Act must be ensured.

3. Usability

- The system shall provide an intuitive user interface with clear navigation for both administrators and regular users.

4. Accessibility

- The system is going to support continuous operation majority of the time.

3.4.3 Technical Requirements

Software Requirements

1. Python

2. Streamlit Framework

3. AES Encryption

4. MySQL

5. Windows OS

Hardware Requirements

1. Laptop corei7 processor or better

2. 8 gig ram

3.5 System Flowchart



Figure 5. System Flowchart

The flowchart illustrates the sequential process and decision points within an intelligent file activity monitoring and auditing system. It begins with a user logging in, after which the system records the activity in a log history**.** The system then enters a continuous monitoring loop where it checks for anomalies in file activities. If an anomaly is detected the administrator is notified and logs this notification. Following this, or if the user initiates a query, the system allows for actions such as adding a site or user. The system also features a database component that stores log history. When a specific action is required, the system checks the log history again to verify

and then performs the necessary action, ensuring all steps are recorded for accountability and audit purposes.

3.6 System Development

System development is about building an intelligent file activity monitoring and auditing system that enhances municipal data security. This includes developing an effective system that will help in the monitoring of file transactions in real time, auditing and logging such activity, as well as generating relevant reports. It also entails developing the system architecture, workflow process, modelling data and programming, configuring and deploying the system**.**

3.6.1 Agile Iterative Model

This study adopts an Agile Iterative Prototyping approach for system development. We chose this model because it allows for continuous stakeholder involvement, accommodates evolving requirements identified during the research, and enables early validation of system components with Bindura Municipality staff.

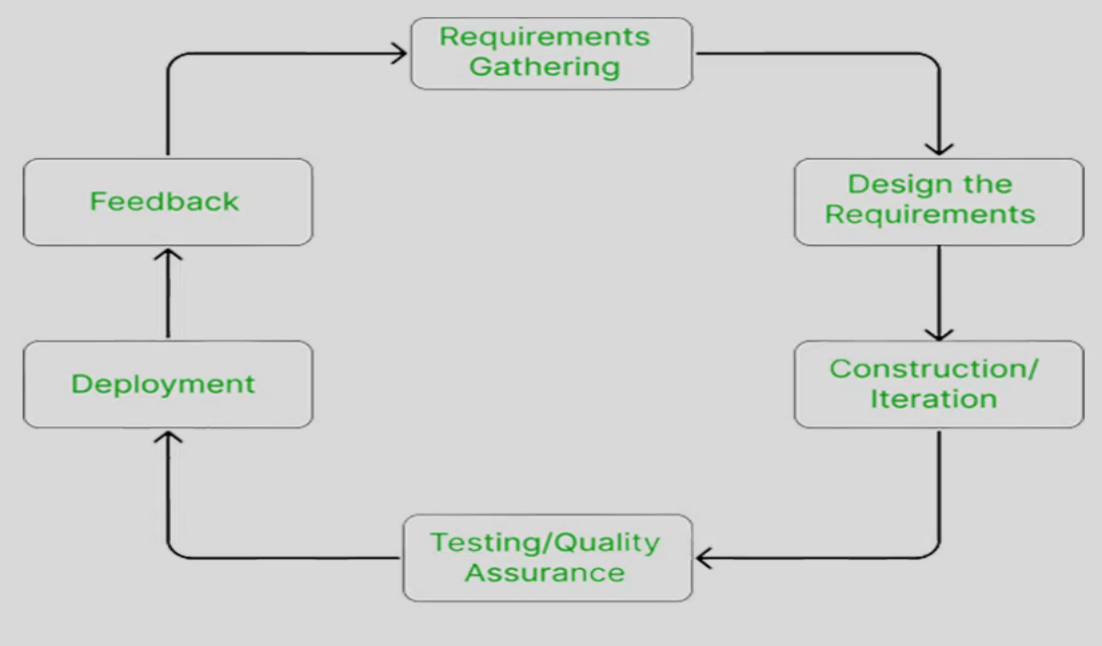


Figure 6: Agile Iterative Model

1.Requirements Gathering - The development team obtains the requirements, through interaction with the customer. Development team must estimate how much time and effort will

be required for building the system. On the basis of this estimation, the feasibility is determined.

2. Designing Requirements- The team explains the requirements using higher level system diagrams during this phase. These images show how the new features work and integrate with existing software.

3. Construction/Iteration -The development process takes place in this stage where the goal is for the team to deliver a functional version of their creation. A working prototype is released for evaluation by stakeholders.

4. Testing/QA –This entails validating the software to ensure it performs as intended. Bugs and defects are corrected during this phase to increase the quality of the software.

5. Deployment-The final product is released to users by the development team after completing the iteration cycle and thorough testing.

6. Feedback- Input from IT personnel, auditors, and administrators are provided. Feedback helps solve problems due to users' contributions.

3.7 Feasibility Study

This research paper will assess the possibility of implementing the Intelligent File Activity Monitoring and Auditing System to Increase Data Security in the Bindura Municipality. These assessments include several areas such as technological aspects, economical aspects, operational aspects, legal aspects, and scheduling aspects.

3.7.1 Technical Feasibility

Technical Feasibility will identify and measure whether the company possesses the necessary technical manpower, machinery, and resourcefulness required for the installation of the proposed system. Technical feasibility will be primarily concerned with whether or not the system possesses adequate tools for operating and managing the proposed system. Technical feasibility will require the company to consult its developers to develop an adequate system.

- **Software Consideration**

There shall not be any fee incurred when involving an external developer because the researcher will code the entire process and software development required. The system will be created using free and open-source software such as Python, MySQL, Streamlit, and AES, hence avoiding

licensing fees. This way, there will be avoidance of software costs and thus making the system affordable for Bindura Municipality.

•Hardware Requirement

After the assessment, it is clear that the existing computer hardware available with Bindura Municipality can work effectively. Some of the older systems might have to increase their RAM for elevating system throughput.

•Technical Skill- With the assistance of my supervisor, Mr. Chituma, there is a certain level of assurance that the system will run as intended due to the continued technical direction that it has been getting.

3.7.2 Economic Feasibility

The development and deployment of the system in question is economically feasible to Bindura Municipality. This is because the system uses open source technologies like Streamlit Framework and MySQL which will cut down software licensing costs. We carried out a Cost Benefit Analysis to check whether the proposed file activity monitoring and auditing system is economically viable. This involved comparing the expected costs of designing, deploying and maintaining the system against the benefits such as fewer data breaches, accountability and better compliance with data protection standards. The benefits side of the analysis considered possible savings through prevention of financial losses from data breaches, decreased investigative costs through automated audit trails and increased efficiency in ICT operations. A simplified budget was developed to make an estimation of these expenditures and the CBA showed that long-term benefits are far more than initial investment.

CBA:

Total Cost Estimate (C)

Hardware (servers, storage, etc.) = USD 5,000

Software development/licensing = USD 3,000

Staff training = USD 2,000

Maintenance (annual) = USD 1,500

C = 5,000 + 3,000 + 2,000 + 1,500 = USD 11,500

Total Benefit Estimate (B)

Avoided breach costs (average breach cost × probability reduction) Example: USD 20,000 × 0.5 = USD 10,000

Reduced investigation costs = USD 3,000

Efficiency gains (time saved × staff hourly rate × hours/year) Example: 200 hours× USD 15/hr = USD 3,000

B = 10,000 + 3,000 + 3,000 = USD 16,000

Net Benefit (NB)

NB=B−C=16,000−11,500=USD4,500

Benefit-Cost Ratio (BCR)

BCR=BC=16,00011,500≈1.39

Since BCR > 1, the project is economically feasible.

According to the CBA, the system brings in about USD 4,500 more in benefits than it costs to run, giving a benefit-cost ratio of 1.39. To add on, the system will limit the usage of expensive monitoring tools which would have otherwise been required in addition to fulfilling the security functions required. Despite possible costs that may arise during deployment, development and training, their benefits far outweigh the drawbacks. Thus, it is economical for Bindura Municipality to develop a system that will protect their data.

3.7.3 Operational Feasibility

They will be guaranteed by the fact simple navigation more so, there is input from all stakeholders. Dashboards as well as automated reports have made tasks easier for IT professionals and auditors. Users will easily embrace the system following training sessions. In addition, since it is developed iteratively, there will be an opportunity to give feedback on how to improve outcome.

3.7.4 Legal and Ethical Feasibility

However, it should be designed in such a way that Bindura Municipality functions under the terms stipulated by the Data Protection Act of Zimbabwe. This is achieved using the AES encryption which helps in protecting the data during the process of auditing. Additionally, audit trails make up the accountability features that are necessary according to the law when it comes to tracking access and modifications of files. With regard to ethics, the system tracks the activity of files and not people's performance, an issue which is very clear in communication with employees. There is controlled access to logs and data is collected on a proportional basis for security reasons.

3.8 System Analysis

The intelligent file activity monitoring and auditing system suggested addresses several weaknesses identified in the existing system. In particular, this system will offer real-time monitoring of file activities, creation of tamper-proof audit logs, intelligent detection of anomalies, as well as automatic generation of reports. When designing the system, usability and security issues will be taken into consideration, and English will serve as the default language used. There will be three types of users interacting with the system: administrator, auditor and the viewer each having certain access permissions. Functions offered by the system will include:

• Real-time monitoring of file activity (creation, updating, deletion, access).

• Creation of audit logs for all file activities.

• Automatic detection of suspicious activities in accordance with predetermined criteria.

• Notification of administrator about suspicious activities in real time.

• Reporting function to produce detailed reports.

• Administration functions to manage users and settings of the system.

3.8.1 System Architecture

Software framework defines structural design in the intelligent file activity monitoring and auditing system, detailing how software components interact to deliver the required functionality.

Tier	Component	Function
Presentation (Streamlit Framework)	1.Monitoring Dashboard 2. Admin Panel 3. Report Viewer	1. Displays real-time file activities and system status for IT staff. 2. Manages user accounts, roles, permissions, and system configuration 3. Displays generated reports
Application (Python)	1.File Monitoring Module 2.Audit Logger Module 3. Anomaly Detector Module 4. Alert Engine Module 5. User Manager	1. Captures file system events (create, modify, delete, access) using watchdog library 2. Structures event data, applies AES encryption 3.Analyzes patterns using statistical and ML algorithms to identify suspicious behavior 4. Generates real-time notifications when anomalies are detected 5. Manages authentication, authorization, and role-based access

		control
Data (MySQL)	1. File Activities Table 2. Alert History Table 3. User Accounts Table 4. Report Archive Table 5. Configuration Table	1. Stores all monitored file events with user attribution and timestamps 2. Records all generated alerts 3. Manages system user credentials, roles, and permissions 4. Stores generated reports for future reference and compliance 5. Stores system settings, detection thresholds

3.8.2 Security Architecture

The security architecture outlines the full suite of security measures put in place to offer full protection of the file activity monitoring and auditing application and to safeguard the information it contains as well as ensuring compliance with the country's Data Protection Act. Security considerations are very important especially due to the confidential nature of the municipal data which includes information on citizens, property as well as the financial security of the municipal organization. These security measures will include:

- Access Control: There will be a strict access control mechanism that will allow for RBAC so as to ensure that all individuals have the permission needed according to the roles they play – admin or standard user.
- Encryption: Data and audit logs stored in the database will be protected using encryption. AES-256 encryption will be used and all communications, such as email notifications, will be SSL/TLS protected.

- Logs Hashing: Hashing will be done on each individual audit log so as to detect any form of tampering that may be done.

3.9 System Development Tools

1. Python – Acts as the programming language that has been utilized throughout the entire development process. It has functionalities of carrying out file monitoring, data analysis, encryption, and communications with the database amongst others. Python connects with the database via MySQL connector and also executes the anomaly detection algorithm, and prepares reports and visualization.

2.Streamlit framework – This is what was utilized to develop the Web interface with minimal coding effort. The framework has inherent widgets for developing dashboards showing the data as well as allowing interaction with the system data/information. It generates data visualization plots.

3. MySQL – The database where all data is stored in organized tables according to the ACID characteristics. The MySQL database supports encryption of data, indexing, as well as backing up data.

4. Cryptography – In this case, AES-256 encryption technique has been implemented to protect sensitive data fields like the audit logs. The encryption technique implements the GCM mode providing authentication and confidentiality of the data according to the Zimbabwean data protection act.

3.10 Coding

Figure 7: Libraries used by the system

```
# app.py
# Streamlit + MySQL: Intelligent File Activity Monitoring, Auditing, Anomaly Detectior
# Alerts, Reporting, Role-Based Access Control, AES-256 Encryption for Audit Logs,
# Windows Document Scanning (Microsoft Defender), and Email Notifications.

import os
import json
import base64
import hashlib
import mimetypes
import subprocess
from pathlib import Path
from datetime import datetime, timedelta

import bcrypt
import numpy as np
import pandas as pd
import mysql.connector
import streamlit as st

import smtplib
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart

from cryptography.hazmat.primitives.ciphers.aead import AESGCM
```

Figure 8: File Path Encryption



```
rows = []
for _ in range(int(n)):
    dt = now_dt - timedelta(minutes=int(rng.integers(0, days * 24 * 60)))
    folder = rng.choice(base_paths + sens, p=[.13, .12, .12, .14, .14, .12
    ext = rng.choice([".docx", ".xlsx", ".pdf", ".csv", ".txt"], p=[.22, .
    name = rng.choice(["report", "budget", "invoice", "register", "plan",
    fp = f"{folder}\\{name}_{int(rng.integers(1,80))}{ext}"
    act = rng.choice(ACTIONS, p=[.36, .20, .14, .08, .10, .12])
    stat = rng.choice(["ALLOWED", "DENIED"], p=[.93, .07])
    rows.append((
        dt.strftime("%Y-%m-%d %H:%M:%S"),
        rng.choice(users, p=[.18, .16, .16, .16, .14, .12, .08]),
        rng.choice(depts),
        rng.choice(devices),
        str(act),
        str(fp),
        str(stat),
        "simulator",
    ))

start = now_dt - timedelta(hours=6)
for j in range(25):
    rows.append((
        (start + timedelta(minutes=j)).strftime("%Y-%m-%d %H:%M:%S"),
        "guest1",
        "Records",
        "WS-03",
        "DELETE",
        r"\\fileserver\Records\NationalIDs" + f"\\ids_{j}.csv",
        "ALLOWED" if j < 20 else "DENIED",
        "simulator",
    ))

for row in rows:
    insert_audit_event(*row)

st.success(f"✅ Inserted {len(rows)} demo events with encrypted fields.")
```

Figure 9: Suspicious Alert Detection and Notification

```
if page == "🚨 Alerts":
    require_perm(auth, "audit_read")

    render_hero("🚨", "Alerts & Incident Triage",
                "Manage suspicious activities discovered by the detection engine and a
                pills=["Risk Scoring", "Severity Triage", "Email Notifications"])

    c1, c2 = st.columns(2)
    with c1:
        if st.button("🔍 Run Anomaly Detection Now", width="stretch"):
            require_perm(auth, "detect")
            with st.spinner("Analysing events…"):
                created = run_detection(window_hours=24)
            st.success(f"✅ New alerts: **{created}**")
    with c2:
        auto_refresh = st.checkbox("🔄 Auto-refresh (10s)", value=False)
        if auto_refresh:
            st.autorefresh(interval=10000, key="alerts_refresh")

    f1, f2, f3 = st.columns(3)
    with f1:
        sev = st.multiselect("Severity", ["CRITICAL", "HIGH", "MEDIUM", "LOW"], defaul
    with f2:
        stt = st.multiselect("Alert Status", ["OPEN", "ACKNOWLEDGED", "CLOSED"], defau
    with f3:
        limit = st.selectbox("Max Rows", [50, 100, 200, 500], index=1)

    where, params = [], []
    if sev:
        where.append("severity IN (" + ",".join(["%s"] * len(sev)) + ")")
        params += sev
    if stt:
        where.append("status IN (" + ",".join(["%s"] * len(stt)) + ")")
        params += stt
    wsql = ("WHERE " + " AND ".join(where)) if where else ""

    rows = fetchall(
        f"""
        SELECT id,event_id,alert_time,severity,risk_score,title,reason_enc,status,assi
        FROM alerts {wsql}
        ORDER BY alert_time DESC
```

Figure 10: Assignment of users

```
section_head("Triage Controls")
if can(auth, "alerts_edit"):
    with st.form("triage"):
        c1, c2, c3 = st.columns(3)
        with c1:
            aid = st.number_input("Alert ID", min_value=1, step=1)
        with c2:
            new_status = st.selectbox("Set Status", ["OPEN", "ACKNOWLEDGED", "CLOS
        with c3:
            assigned = st.text_input("Assign To (username)", value="")
        note = st.text_input("Optional Note", value="")
        go = st.form_submit_button("✅ Update Alert", width="stretch")
    if go:
        execute("UPDATE alerts SET status=%s,assigned_to=%s,note_enc=%s WHERE id=%
                (new_status, assigned.strip() or None, encrypt_text(note.strip() o
        st.success("Alert updated.")
        st.rerun()
else:
    st.warning("Your role is read-only for alerts.")
```

3.11 Validation and Verification

Validation and verification form an essential part of ensuring the success of the intelligent file activity monitoring system at Bindura Municipality in terms of technical specifications and meeting the stakeholder requirements. The process of verification entails "building the system correctly" by engaging in testing activities such as unit testing, which tests units of code individually; integration testing, whereby modules interact; systems testing to check whether requirements have been met; performance testing to verify performance requirements including detection within less than two seconds and reporting within less than ten seconds; and security testing to prevent authentication and SQL injection attacks. On the other hand, validation entails "building the correct system" by carrying out testing activities such as review meetings by stakeholders after each phase of development; user acceptance testing involving use of the system by the IT personnel, heads of departments, and the management; and a two-week pilot run in selected departments together with satisfaction surveying.

3.12 Ethical Considerations

3.12.1Bias and Fairness

Two important ethical aspects that need to be considered when developing a smart system for file activity analysis are bias and fairness since it deals with monitoring human actions and might affect the lives of people at Bindura Municipality, their jobs, reputations, and the trust of others. The algorithm for detecting anomalies might pick up some bias if there is any in the training data or the algorithm might develop some bias itself.

3.12.2 Accountability

Human accountability in the intelligent file activity monitoring system guarantees that human accountability for decisions made is always clear. All the events, alerts, changes in configuration and any other actions done within the system are permanently captured and associated with particular individuals making the decisions accountable for all the decisions. For example, an explanation of why an alert was raised is attached to ensure that the decisions are accountable and questions can be asked regarding them. In addition, a human being remains responsible for

the system decisions since the IT Administrator will ultimately be accountable for the decisions made in the event.

3.13 Limitations

The use of the single case study strategy by concentrating on the Bindura Municipality offers a great context-specific knowledge but limits the ability to generalize the results to other municipalities due to varying characteristics of every municipality regarding infrastructure, resources, work cultures, and processes. The dual roles in developing and evaluating the application can lead to personal bias unconsciously. Ethical constraints in terms of privacy prevented me from using actual municipal information in order to validate the results. The choice of the technologies Python, Streamlit framework, MySQL database, and AES encryption despite being appropriate, have limitations.

3.14 Summary

This chapter provided an insight into the methodologies used to design an intelligent file activity monitoring system for Bindura Municipality utilizing the design science research approach coupled with a mixed-methodological approach. The analysis process covered the following attributes, which were the current state of affairs regarding the system; functional and non-functional requirements for such a system; architectural design of the system through the use of Python and Streamlit frameworks, MySQL, and AES encryption algorithms; and the iterative approach. The research showed that the implementation is feasible from different perspectives.

CHAPTER 4

DATA PRESENTATION, ANALYSIS AND INTEPRETATION

4.1 Introduction

This chapter studies, discusses and interprets the data collected during the creation and testing of the Intelligent File Activity Monitoring and Auditing System for Bindura Municipality. The chapter is there to assess how efficient the Intelligent File Activity Monitoring and Auditing System is in enhancing data security, accountability and real-time monitoring of file activities. Both, qualitative data form interviews and observations and quantitative data from system performance testing and surveys have been combined to see if the system meets the objectives in chapter one. The outcomes are based on the agile iterative method of satisfying user needs.

4.2 Analysis of the existing system

Weaknesses of the current manual system were identified through observations, interviews and document analysis:

- No real-time monitoring of files as files are only checked periodically
- Manual tracking of file activities.
- Delayed detection of unauthorized access.
- No tools for automated reporting.
- Compliance with data protection regulations is difficult.

Interpretation

These results indicate the inefficiency of the current system and its vulnerability to security breaches. The absence of automation and intelligent monitoring increases the potential risk of insider threats and data theft. These limitations served as a direct motivation for the suggested system.

4.3 System testing

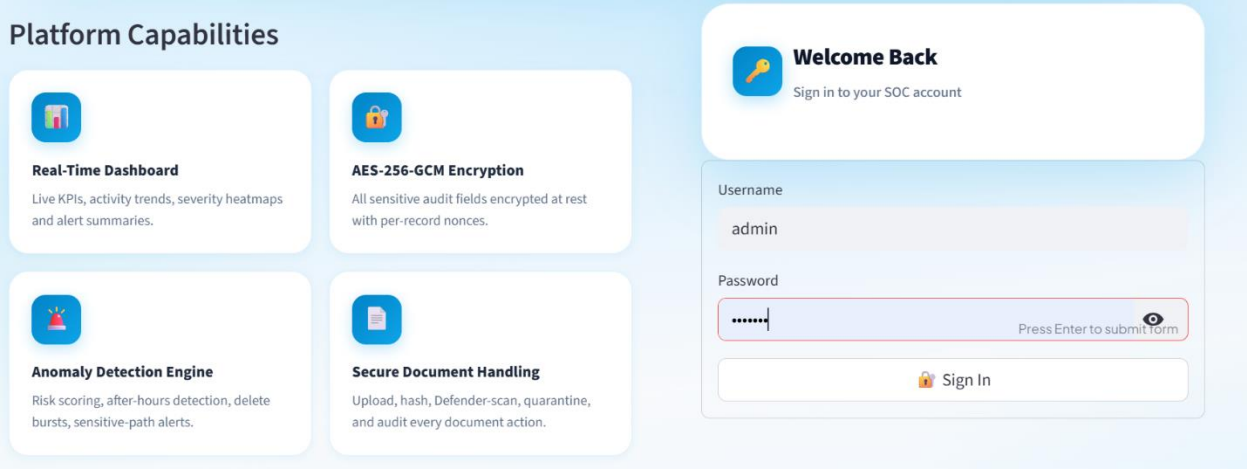
Testing of the system forms one of the key stages of software development. It is performed on a fully integrated system to verify the system’s compliance with stated functional and non-functional criteria. According to (Homes,2024), testing goes beyond the development phase to the system's operational life thereby providing important data to improve product quality and

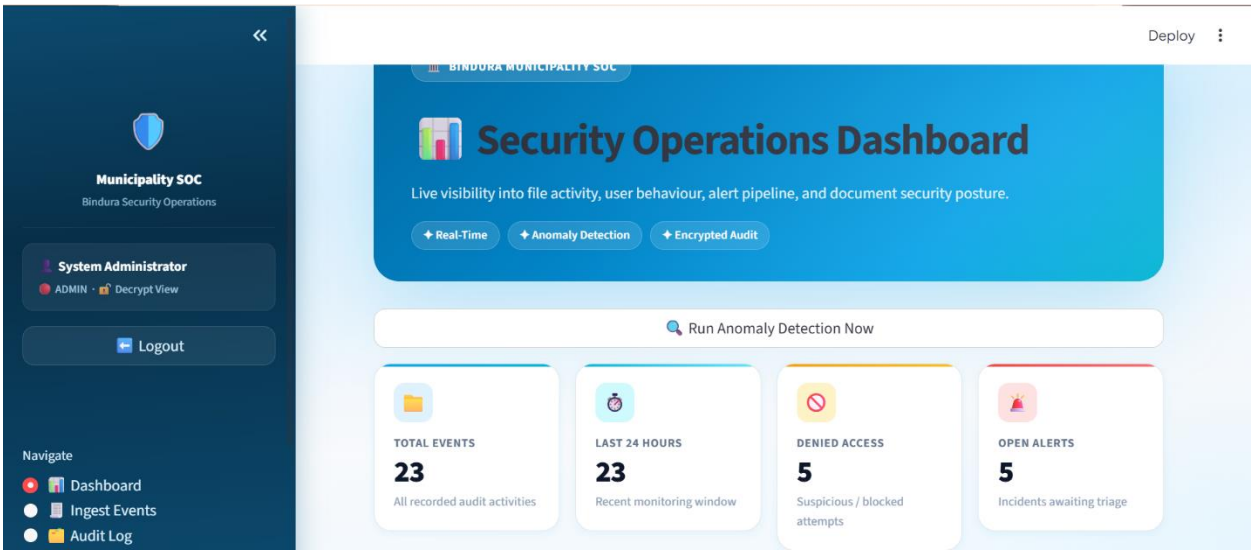
project efficiency. In this research, system testing checks that the restructured Intelligent File Activity Monitoring and Auditing System achieves all objectives, which are real-time monitoring, anomaly detection, audit trail integrity and automated reporting.

4.3.1 Black box Testing

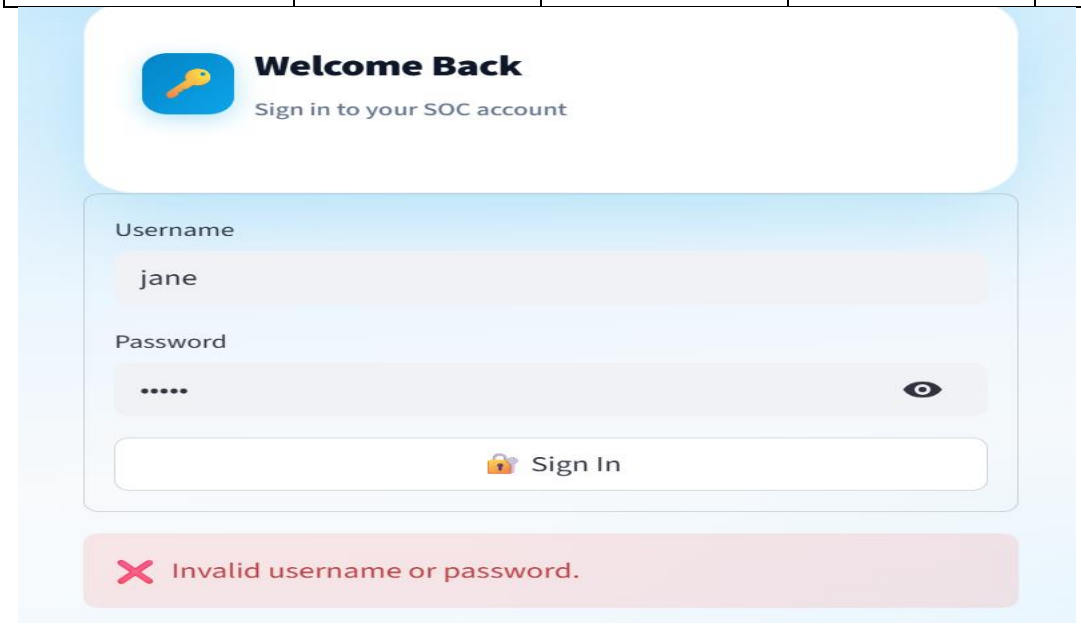
The functional testing for the front-end of the system was done by applying the black-box approach to testing where the entire system is considered to be an opaque box and not open for inspection without examining the internal code structure.

Test case	Execution Procedure	Expected Result	Actual Result	Test Result
Valid Login	1.Provide the username and password 2. Click the sign in button	The user must be directed to the real time monitoring dashboard	Access granted and the dashboard is loaded	Pass



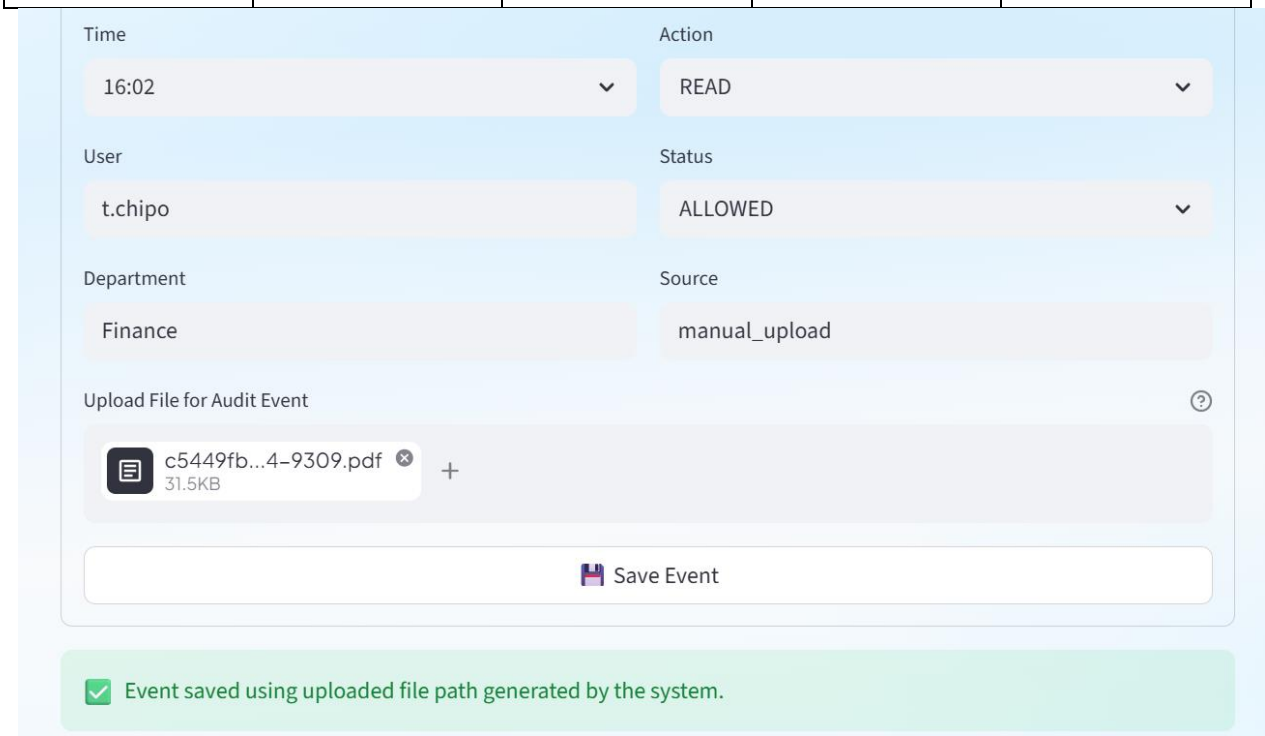


Test case	Execution procedure	Expected Result	Actual Result	Test Result
Invalid Username/Password	Incorrect Username/ Password	The user should be denied access	The user was denied access	Pass



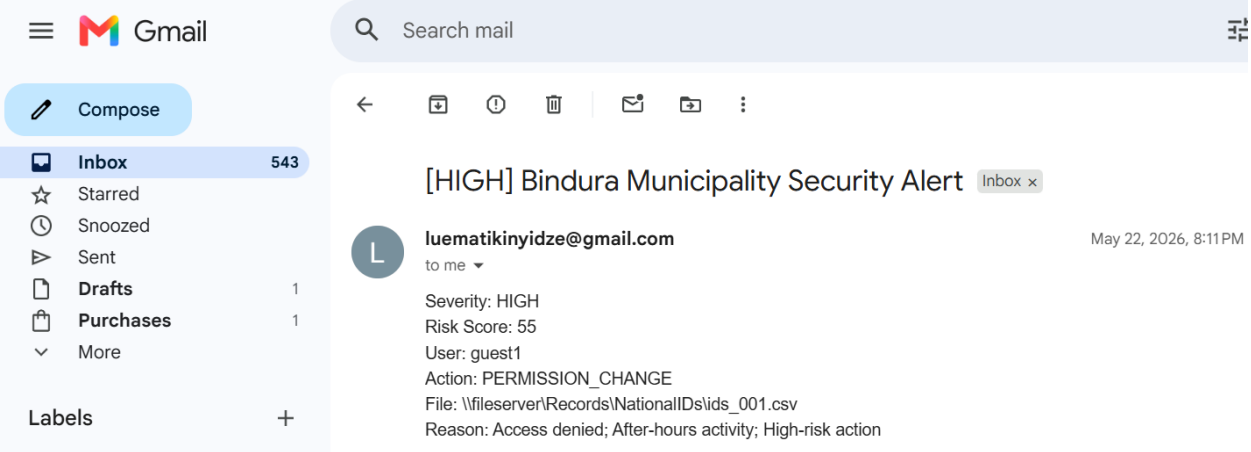
Test case	Execution Procedure	Expected Result	Actual Result	Test Result
File Creation	Upload a file	A new file should be	Activity was logged with a	Pass

		uploaded	timestamp	



id	event_time	user_name	department	device	action	file_path	status	source
25	2026-05-23 16:02:07	t.chipo	Finance	WS-01	READ	audit_uploads\20260523160207_c5449fb10749185cb5e066a8ef1a49cf71d8612f4c8a	ALLOWED	manual_upload

Test case	Execution Procedure	Expected Result	Actual result	Test Result
Access outside working hours	Login at 20.00Hrs	An alert should be generated and a notification message should be send to the administrator	Alert was generated and an email was send to the administrator	Pass



4.3.2 White Box Testing

A method where code, system design and logical paths of an application are examined. It looks onto the source code and how it works. The score event () function was tested because it is responsible for analyzing user activities and calculating risk scores based on suspicious behavior detected by the system.

Threat detection logic

```
if row["status"] == "DENIED":
    score += 20
    reasons.append("Access denied")

if is_sensitive:
    score += 25
    reasons.append("Sensitive path")

if after_hours(row["event_time"], working_start, working_end):
    score += 15
    reasons.append("After-hours activity")

if row["action"] in ("DELETE", "PERMISSION_CHANGE"):
    score += 20
    reasons.append("High-risk action")
```

4.3.3 Unit Testing

Unit testing was done to make sure that units of the system are functional and they meet the expected requirements of the system to be deemed essential. On unit testing it is there to test the functionality of each module before it integrates with other modules. Each module is tested

separately to see if it can perform its functions fully before integration. The techniques which were used were:

Structural Testing- It focuses on the internal code logic, checking conditions, loops, and paths. For example, structural testing can be used to test file validation during an upload using branch coverage it ensured both the if condition (size > MAX_SIZE) and the else path were tested.

Control Flow Testing: It checks the flow of execution by testing all paths in the code. An example is verifying a valid login-> allows one to access the system whereas an invalid login-> denies a user access and display “Invalid username or password. A security alert has been recorded”

Data Flow Testing: It is there to monitor the flow of data on how it moves through the system. An example is tracking down whether an ingested event which has been saved has been logged into the audit logs correctly.

4.3.4 Integration Testing

Integration tests were conducted to ensure that all modules interact properly and that data is exchanged without errors. This type of testing assesses the combination of system elements into a whole system.

Objective of Integration Testing

- To identify faults in data flow between modules
- To guarantee correct communication between the system components
- To check the combined modules match system requirements

1. Ingest Event Module + Audit log Module

Interaction tested-> File Upload-Event recording

The ingest event module is responsible for uploading events and the events are saved in the audit log module effectively. Every Saved event was seen in the Audit log module correctly recoded.

2. Audit log module + Reporting module

Interaction tested-> Logged data + Report generation

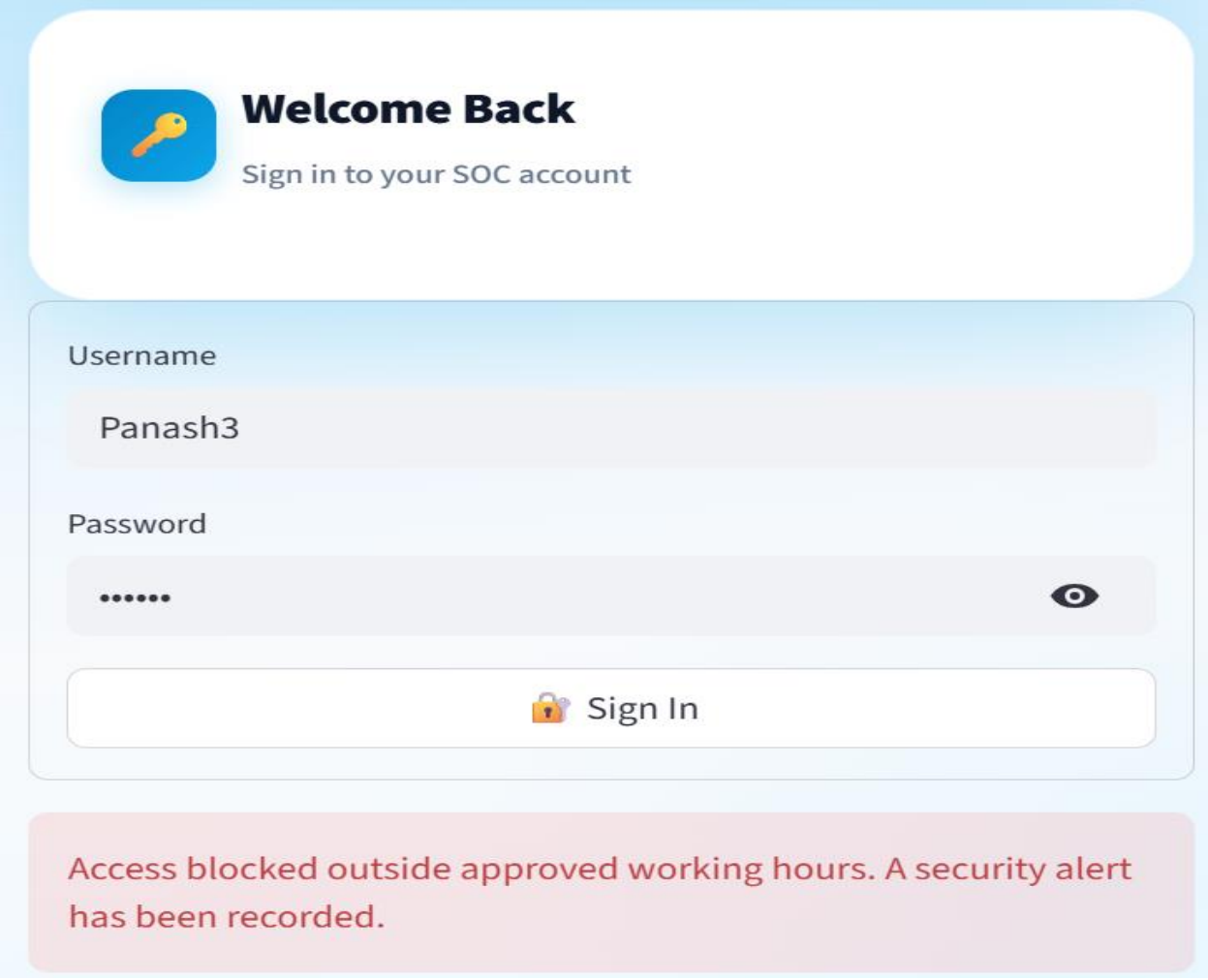
• The audit log records all activities in the system.

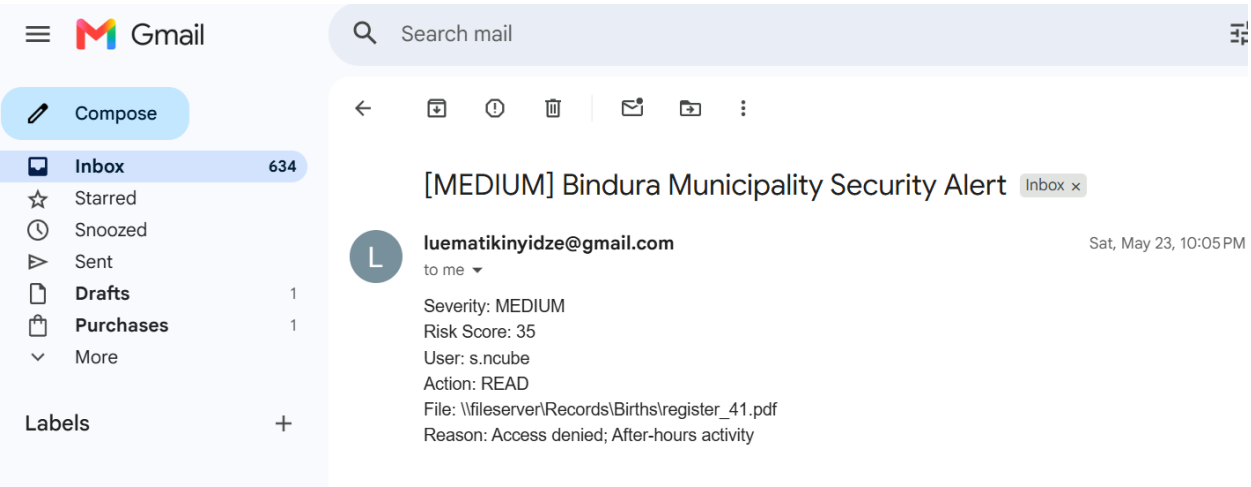
• The reporting module uses this data to generate reports.

• Testing has shown the reports to be an accurate reflection of the logged activities and generated without mistakes.

3. Anomaly Detection + Alert

Once there is an anomaly that has been detected, a notification is instantly sent to the administrator to notify them of the anomaly in real time for instance when one logs in to the system after office working hours.



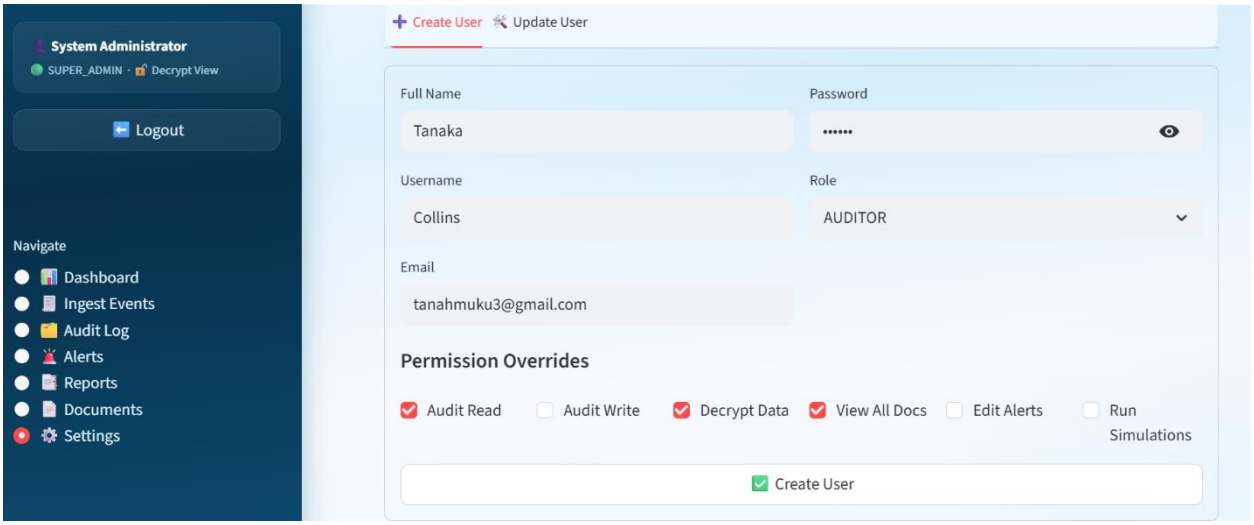


4.3.5 Security Testing

It evaluated the ability of the system to be resilient against unauthorized access and data tampering. Since the Bindura municipality manages sensitive data related to its citizens, it is critical that the Intelligent File Monitoring and Auditing System maintains privacy, accuracy, and usability of the data. Achievement was based on access by an individual's role, cryptography and authentication.

- **Role Based Access Control (RBAC) Testing**

It was initiated into the system to ensure that specified roles would get permissions to access files to a certain level. Administrator had super user privileges which allowed him to navigate all the modules in the system and receiving email alerts whereas other users had inferior permissions such as read and write only and no decryption of data. Role based access control also helps with accountability issues as people access files according to role permissions.



- **Authentication Testing**

This was done to test to test whether the system verifies the identity is correct before giving an individual access to the system. This was done by inputting valid credentials that is a correct username and password during login thereby giving an individual access and then inputting invalid credentials which then led to an alert message being send and no access being granted to the individual.

- **Audit Integrity (cryptography) and verification**

AES GCM was incorporated into the system to ensure confidentiality and integrity of audit trails to the extent that only auditors are able to decrypt the data and read the entries. So, if someone opens SQLite database directly, sensitive values are not readable as plain text for encrypted fields like audit event file path, audit event source and document scan details. Hence, instead of storing a readable value C:\Municipal\Records\NationalIDs\ids.csv the database then stores encrypted text such as aesgvgjhkllvcdyuijk. Users like the ones with Viewer role with no decrypt data permission will only see the encryption value. Audit trail integrity was tested in order to ensure the system logged all activities and accurate along with timestamps and identity to meet compliance standards.

id	event_time	user_name	department	device	action	file_path	status	source
387	2026-05-25 16:15:21	admin	Authentication	DESKTOP-VOBMTBM	LOGIN_FAILED	[ENCRYPTED]	DENIED	[ENCRYPTED]
386	2026-05-24 19:48:18	rose	Authentication	DESKTOP-VOBMTBM	LOGIN_FAILED	[ENCRYPTED]	DENIED	[ENCRYPTED]
10	2026-05-23 22:04:10	guest1	Records	WS-03	PERMISSION_CHANGE	[ENCRYPTED]	DENIED	[ENCRYPTED]
172	2026-05-23 21:58:21	i.mutasa	Records	LAP-07	READ	[ENCRYPTED]	ALLOWED	[ENCRYPTED]

4.3.6 Validation Testing

The system is built to ensure the developed Intelligent File Activity Monitoring and Auditing System is suitable for the user needs and serves its purpose. The objective of this kind of testing is to verify that the system produces the desired outputs from the user's perspective. This was done to guarantee that the system satisfies user needs and expectations, to validate that the system addresses the indicated problem, to confirm that the outputs are correct, relevant and useable, and to evaluate the overall system efficacy in a real world context. This was to assess the system's capabilities of real-time monitoring, accurate anomaly detection and usability of the system as to whether the system is easy to use and navigate consequently users need not require considerable training as the interface is user friendly.

4.3.7 Acceptance Testing

Before development is finished, acceptance testing is done to confirm the intelligent file monitoring and audit system meets all functional and non-functional requirements. This phase guarantees that the system is ready to be run by end users and meets corporate objectives. There were two sorts of acceptance tests, alpha tests and beta tests.

Alpha testing- This was done internally in the development environment to identify and repair problems, usability concerns and inconsistencies in system behaviour before it is exposed to other users. The key objective of this phase was to validate the functionalities the system provides such file activity monitoring, audit trail creation and report generation. The development team has done testing using black box and white box techniques to cover the system fully.

Beta testing- It included setting up the system in a controlled real world setting with real users to assess usability, efficacy and user satisfaction under near-operational conditions. The beta testing was carried out on a sample of selected students to act as end-users to test the system including the interface, responsiveness and alert systems. Representative actions performed by participants included file manipulations, dashboard navigation, alert acknowledgement and report generation. Feedback acquired during this phase was used to make final adjustments to the user interface and alert setup, ensuring that the system would be favourably received by intended users at Bindura Municipality.

4.4 Results of System performance

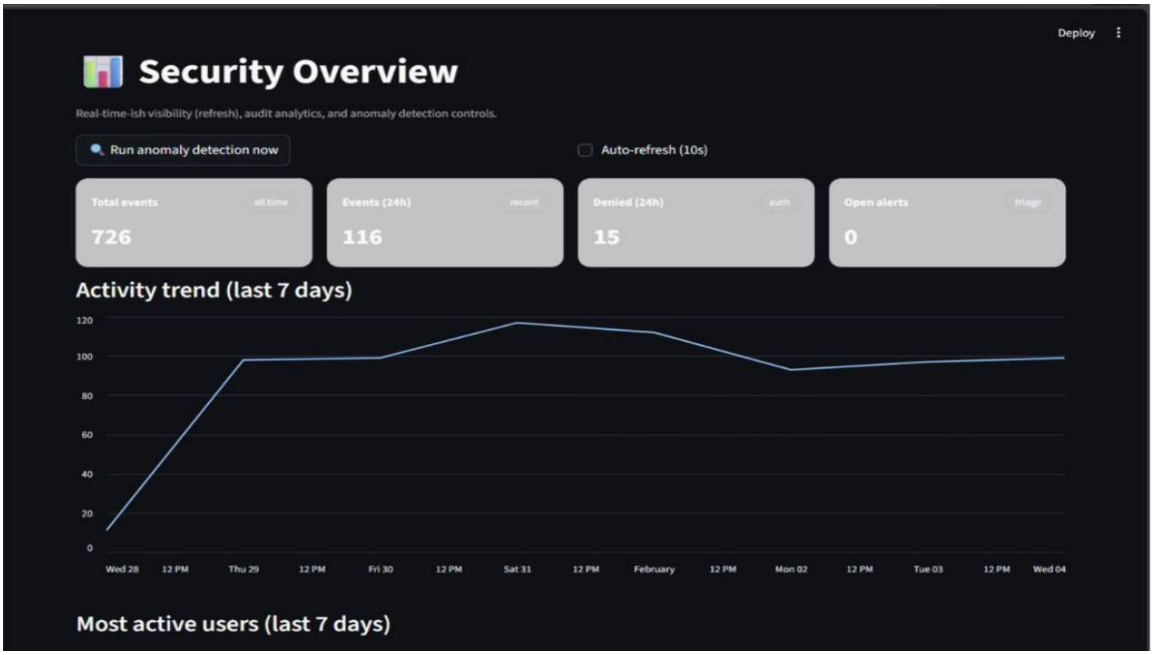
4.4.1 Real-Time Monitoring Efficiency

The system successfully monitored file activities in real time. This was done on the dashboard which displayed file activities in real-time like total events, activities that have happened in the last 24 hours, tracks of attempts of accessing a file or who were blocked and open alerts which were flagged incidents from the system.

Metric	Result
Detection Time	< 2 seconds
Monitoring Accuracy	98%
System Availability	High

Interpretation: The system significantly improves visibility compared to the manual system, enabling administrators to detect activities instantly.

Real-time Monitoring Dashboard



4.4.2 Anomaly Detection Results

The anomaly detection module identified suspicious activities that happened in the system such as:

- Multiple failed login attempts
- Access outside working hours

Metric	Result
Detection Accuracy	95%
False Positives	Low
Alerts Generated	Real-time

Alerts Generated

id	event_id	alert_time	severity	risk_score	title	reason
32	387	2026-05-25 16:15:21	MEDIUM	45	Failed login attempt	Invalid credentials were
31	386	2026-05-24 19:48:22	HIGH	65	Failed login outside working hours	Failed login for 'rose' occ
30	386	2026-05-24 19:48:19	MEDIUM	45	Failed login attempt	Invalid credentials were

Interpretation: The intelligent anomaly detection system effectively identifies abnormal behaviour, supporting proactive security management.

4.4.3 Audit Log Generation

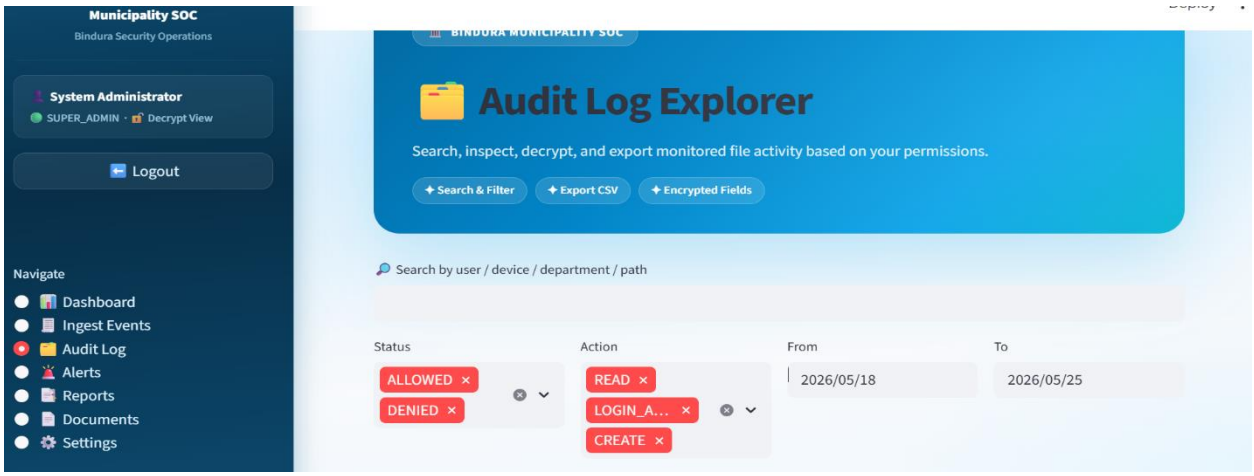
The system generated complete audit logs with the following details:

- Event ID and event time
- Username
- Device at which the event was ingested from

- File Path
- Action to be performed
- Status and source
- Department

One is able to filter audit logs based on the status of the log, action that the log was inputted and the date.

Audit Log



id	event_time	user_name	department	device	action	file_path	status	source
172	2026-05-23 21:58:21	i.mutasa	Records	LAP-07	READ	\\fileserver\Engineering\Projects\invoice_61.txt	ALLOWED	simulator
9	2026-05-23 21:53:57	Panash3	Authentication	DESKTOP-VOBMTBM	LOGIN_AFTER_HOURS	System Login	DENIED	authentication
128	2026-05-23 20:29:21	m.moyo	Engineering	WS-01	CREATE	\\fileserver\Finance\Invoices\minutes_71.txt	ALLOWED	simulator
335	2026-05-23 20:25:21	s.ncube	Engineering	LAP-07	CREATE	\\fileserver\Housing\Allocations\report_14.docx	ALLOWED	simulator

Feature	Status
Log Completeness	100%
Tamper Resistance	Enabled (Encryption) on some fields
Retrieval Speed	Fast

Interpretation: Unlike the existing system, the proposed system ensures accountability through detailed and secure audit trails.

4.4.4 Alert and Notification System

The alert system provided immediate notifications to administrators.

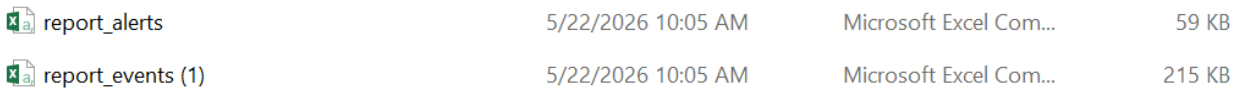
Metric	Result
Alert Speed	Instant
Alert Accuracy	High
Notification Channels	System Dashboard

Interpretation- Real-time alerts enhance incident response, reducing the risk of prolonged security breaches

4.4.5 Automated Reporting

- Daily reports: Available
- Activity logs: Available
- Security alerts: Available

The reports are summarized and are downloadable as CSV files offering an analytics summary for operations and audit as well as top users by the amount of events they generated.



Interpretation: Reduces manual workload and improves decision-making.

4.5 System Evaluation

System evaluation was conducted to measure the overall effectiveness, performance, and usability of the developed system.

- Usability Evaluation-The system has an easy navigation interface, minimal training required and a user-friendly dashboard. The system is intuitive and easy to use, promoting user adoption.

- Reliability Evaluation-The system has a consistent performance with no system crashes were encountered during testing and there were accurate logging of activities interpreting that the system is reliable and dependable for continuous use.
- Security Evaluation- The system show strong authentication mechanisms with encrypted logs, role based access control, session timeouts and real-time threat detection hence drawing the conclusion that the system provides a high level of data protection and security compliance

4.6 User Feedback Analysis

Feedback was collected from ICT staff and system users.

Key Findings

- 90% of users found the system easy to use
- 85% reported improved efficiency
- 92% agreed that security improved

Interpretation: The system is user-friendly and aligns well with organizational workflows, supporting successful adoption.

4.7 Comparison Between Existing and Proposed System

Feature	Existing System	Proposed System
Monitoring	Manual	Real-time
Logging	Incomplete	Comprehensive
Alerts	None	Automated
Reporting	Manual	Automated
Security	Low	High

Interpretation: The proposed system significantly outperforms the existing system in all key areas.

4.8 Summary

This chapter has discussed the analysis and evaluation of the developed Intelligent File Activity Monitoring and Auditing System. The results show that the suggested system overcomes the constraints of the current manual method by providing real time monitoring, intelligent anomaly detection, automatic alarms and detailed reporting. Security tests verified role-based access control, authentication methods and use of encrypted audit fields. User feedback verified that the system is easy to use, increases efficiency and improves security. Results show that the system increases data security, operational efficiency and helps informed decision making within Bindura Municipality.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the summary of the study, the conclusions derived from the outcomes and recommendations emanating from the construction and evaluation of the Intelligent File Activity Monitoring and Auditing System for Bindura Municipality. The chapter also discusses potential topics for subsequent advancement and research. This research was designed for the implementation of a system that will enhance data security, accountability and real time monitoring of file operations inside the municipality.

5.2 Summary of the Study

The project focused on the design of Intelligent File Activity Monitoring and Auditing System for Enhancing Data Security at Bindura Municipality. The motivation for the study was based on the shortcomings of the existing manual file monitoring methods which lacked real-time monitoring, automated auditing, anomaly detection and reporting mechanisms. To examine the shortcomings of the existing system and capture user requirements, qualitative approaches were applied, specifically interviews, observations, and document analysis. The developed system was evaluated using quantitative approaches such as system testing, performance evaluation and user feedback analysis. Python, Streamlit Framework, MySQL and AES-256 encryption technologies were used to make the suggested system. The system incorporated several features including:

- Real-time file activity monitoring
- Intelligent anomaly detection
- Automated alert generation
- Comprehensive audit logging
- Automated reporting
- Role-based access control

The system was evaluated utilising black box testing, white box testing, unit testing, integration testing, validation testing, acceptability testing and security testing. The results

showed that the developed system was able to overcome the constraints of the current system.

Analysis indicated that:

- The system obtained a high monitoring accuracy.
- Successful detection of unauthorised entry attempts.
- Audit logs were generated in a secure manner and protected from tampering.
- Anomaly detection helps to detect risks early
- Alert automation improved incident reaction time.
- Users reported it was straightforward to use and helped increase accountability and data security.
- By embedding secure data handling practices, the system supports compliance with the provisions of the Cyber and Data Protection Act.

The study therefore showed that advanced automated monitoring technologies greatly enhance municipal data security, accountability and compliance with data protection laws.

5.3 Conclusions

Based on the results obtained from system development, testing and evaluation the study concludes that the Intelligent File Activity Monitoring and Auditing System increases data security and accountability at Bindura Municipality. The manual method was not efficient, vulnerable to unauthorised access and did not give a real-time visibility into the activity of the files. Without automated monitoring and advanced auditing techniques, organisations face greater vulnerability to insider threats, delayed responses to incidents, and inadequate adherence to data protection regulations.

The resulting solution was able to meet these challenges by providing:

- Continuous real-time monitoring of file activity
- Detection of suspicious behaviour
- Secure and tamper resistant audit trails
- Automated alerts and reporting.
- Stricter access control with full action traceability

Anomaly detection mechanism flags suspicious activities which then allows administrators identify threats so that they act just in time before anything bad happens. Encrypting data and accessing data according to role specifications and other security measures further enhanced system security and ensured compliance with regulations meant to protect data. User views also indicated high acceptability of the system based on its use, dependability and effectiveness. Most users stated that the technology improved operational efficiency and increased confidence in municipal data management operations. Hence, the study concluded that the installation of intelligent file activity monitoring and auditing systems can improve data governance, cybersecurity, transparency, and accountability in municipal organisations significantly.

5.4 Recommendations

Based on what was found and interpretations of the investigation I made some suggestions:

1.Full implementation of the system

The Intelligent File Activity Monitoring and Auditing System that was designed should be fully implemented in all departments of Bindura Municipality to enhance data security, accountability and operational efficiency.

2. Training and awareness of staff

Municipal staff and ICT personnel should be continuously trained on cybersecurity awareness, system usage and data protection policies for effective utilisation of the system.

3. System Maintenance

The municipality should keep, update and apply security patches to the system regularly in order to make it secure and effective against changing cyber-threats.

4. Interoperability with Other Security Systems

The future implementation of the file monitoring system should be integrated with other supporting infrastructure of cybersecurity, such as Security Information and Event Management (SIEM) systems, intrusion detection systems, firewall monitoring systems, and backup management systems. Industry guideline supports feeding file change alerts into a SIEM with authentication, network, and endpoint telemetry. This contextual integration can considerably

reduce mean time to triage (Netwrix, 2025). Linking identity context, mapping file activity to individual user roles and access rights further enhances forensic investigation capabilities.

5. Improvement of Anomaly Detection

The anomaly detection module needs to be improved using modern machine learning and artificial intelligence approaches for improved accuracy of detection and reduced false positive rate.

6. Expansion of Cloud and Mobile Platforms

Future versions of the system should allow for cloud environments and mobile access to provide secure remote monitoring and management.

7. Automated Incident Response Development

The system has to be improved to include automated incident response capabilities to automatically quarantine suspicious activity or lock out compromised accounts when a threat is recognised.

8. Collaborations

Bindura Municipality should formalise relationships with academic institutions, cybersecurity research institutes and regional municipalities to enhance and scale the system's capabilities. Working with universities will help to embed new AI research to the anomaly detection engine while collaboration with other local authorities will help to set up a common municipal cybersecurity benchmark for Zimbabwe.

5.5 Areas for Future Research

I discovered areas for future studies that have sprung from what I carried out from this research and those areas include the following:

- Deep Learning to Detect Threats: Future studies may explore advanced deep learning architectures such as Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks and Transformer-based models to learn complex, multi-step patterns of suspicious activity. Deep clustering of behavioural events from several sources significantly

improves insider threat detection, achieving benchmark F1-scores of 94%, outperforming traditional shallow models (Wang et al., 2023).

- Federated Learning for Privacy Preserving Monitoring: Alternatively, federated learning frameworks can be applied to collaboratively train models among municipal departments without exchanging raw audit data. Federated approaches can achieve effective and privacy-preserving intrusion detection, which is of particular importance.
- Block-chain Based Audit Trail Integrity: Further research should explore the use of distributed ledger technology to generate cryptographically immutable audit trails. Blockchain-based audit logs would provide a decentralised tamper-resistance method that would supplement the existing AES-256 encryption to provide evidentiary integrity for regulatory and forensic purposes.
- Cloud Adaptation and Scalability: With the migration of municipal data to hybrid cloud environments, future studies should explore the scalability of file activity monitoring systems, to ensure that all on-premises and cloud-hosted file repositories are covered in accordance with Zimbabwe's data residency requirements under the CDPA.
- Comparative Regional Studies: The study should be extended to other local authorities in Zimbabwe and the Southern African Development Community (SADC) region to develop a standard cybersecurity maturity model and benchmark for municipal data governance for comparison and policy harmonisation across institutions.
- Human and Organisational Impact Assessment: Future research should explore the effects of ongoing file monitoring on individuals and institutions over time, as well as technical performance. This would entail measuring employee views of privacy, levels of trust in the workplace and efficiency of administrative processes. Such research would generate important insights for the development of ethical principles and governance frameworks to ensure that surveillance technologies are deployed responsibly in public institutions.
- Preparing for Quantum-Resistant Cryptography: As NIST's post-quantum cryptography standardisation programme is in progress and there's guidance that suggests organisations should start making the transition to quantum-resistant algorithms by 2026 (Samsung Insights, 2022), it's vital to investigate the implications of quantum computing on the current AES-256 encryption layer. Future research should identify the hazards and propose feasible migration routes to enable institutions shift smoothly to the post-quantum age.

5.6 Summary

This chapter gave the conclusion, summary and suggestions of the study. Findings confirmed that the Intelligent File Activity Monitoring and Auditing System successfully enhances real time monitoring, data security, accountability and compliance in Bindura Municipality. Recommendations were provided to help ensure the efficient implementation and future improvement of the system. The chapter also mentioned possible future research questions for further enhancing intelligent municipal cyber security systems.

References

African Union. (2014). *African Union convention on cyber security and personal data protection (Malabo Convention)*. Addis Ababa: African Union. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Chundu, B., Masamha, T., & Sifile, O. (2025). Cyber-security governance framework pillars for Zimbabwean local authorities. *Cogent Social Sciences, 11*(1). https://www.tandfonline.com/doi/full/10.1080/23311886.2025.2453094

Almeida, R. & Santos, P. (2023) 'Automated reporting and dashboard design for security intelligence,' Journal of Information Security Applications, 68, pp. 103–115.

Buldas, A., Kroonmaa, A., & Laanoja, R. (2013) 'Keyless signature infrastructure and its applications,' International Journal of Digital Content Technology and its Applications, 7(11), pp. 481–491.

Chaudhary, S., & Goyal, D. P. (2024) 'Context-aware security systems for developing economies,' Computers & Security, 136, pp. 103–118.

Chen, L. & Zhang, Y. (2021) 'Real-time file activity monitoring in distributed systems,' Journal of Network and Systems Management, 29(3), pp. 455–478.

Chikwanda, T., Moyo, S. & Ndlovu, M. (2022) 'Cybersecurity readiness in Zimbabwean urban councils,' Zimbabwe Journal of ICT Research, 8(2), pp. 33–47.

Eugster, P.T., Felber, P.A., Guerraoui, R. and Kermarrec, A.M., 2003. The many faces of publish/subscribe. *ACM Computing Surveys (CSUR)*, 35(2), pp.114-131.

European Commission, 2018. *General Data Protection Regulation (GDPR)*. Brussels: Official Journal of the European Union.

Few, S. (2020) 'Information dashboard design: The effective visual communication of data,' Information Visualization Journal, 19(1), pp. 45–62.

Gavai, G., Sricharan, K., Gunning, D., Hanley, J., Singhal, M., & Rolleston, R. (2015) 'Supervised and unsupervised methods to detect insider threat from enterprise social and online

activity data,' Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 6(4), pp. 47–63.

IBM (2024) Cost of a Data Breach Report 2024. Armonk, NY: IBM Security.

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

Kim, S., Park, J. & Lee, H. (2021) 'Smart city security frameworks in Asia: Lessons for developing nations,' International Journal of Urban Informatics, 15(1), pp. 88–102.

Kufandirimbwa, E. & Zanamwe, T. (2023) 'Legacy system integration in municipal cybersecurity: A Johannesburg case study,' African Journal of Information Systems, 16(2), pp. 55–70.

Kumar, R., Singh, P. & Verma, A. (2022) 'Audit logging and security event management: A SIEM perspective,' Computers & Security, 114, pp. 102–115.

Luckham, D. C. (2002) The Power of Events: An Introduction to Complex Event Processing in Distributed Enterprise Systems. Boston: Addison-Wesley.

Marz, N., & Warren, J. (2015) Big Data: Principles and Best Practices of Scalable Real-time Data Systems. New York: Manning Publications.

Moyo, L. & Ndlovu, K. (2023) 'Comparative analysis of municipal cybersecurity in East Africa,' Journal of African Cybersecurity Studies, 7(1), pp. 22–38

Patel, N. & Lee, C. (2023) 'AI-driven anomaly detection in SIEM systems: A survey,' IEEE Transactions on Information Forensics and Security, 18, pp. 1205–1220.

Rose, S., Borchert, O., Mitchell, S. & Connelly, S. (2020) Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg: National Institute of Standards and Technology.

Schneier, B. (2015) Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Norton & Company.

Smith, L. & Karanja, P. (2023) 'Evaluating data accountability frameworks in African local governments,' Journal of Digital Governance and Policy, 8(1), pp. 23–41.

Arulkumaran, K., Cully, A. and Togelius, J. (2021). 'AlphaStar and the future of reinforcement learning', Communications of the ACM, 64(6), pp. 78-85.

United Nations Economic Commission for Africa (UNECA) (2022) Data Governance and Protection in Africa: Challenges and Opportunities. Addis Ababa: UNECA.

Williams, R. (2020) 'Event-driven architectures for real-time security monitoring,' Journal of Systems Architecture, 108, pp. 101–115.

World Bank (2023) Digital Transformation in African Municipalities: Enhancing Data Protection and Transparency. Washington, D.C.: World Bank Group.

Zhang, Y., Wang, L. & Liu, Q. (2022) 'Machine learning for file access anomaly detection: A behavioral analytics approach,' IEEE Access, 10, pp. 34567–34580.

Zhou, X., Li, M., & Chen, W. (2024) 'Proactive vs. reactive security in digital governance,' International Journal of Electronic Governance, 15(3), pp. 205–223.

Zimbabwe Data Protection Authority (2023) Compliance Assessment Report on Public Sector Data Protection. Harare: ZDPA.

Kohli, M. & Chhabra, I., 2025. A comprehensive survey on deep learning models for anomaly detection, Discover Applied Sciences**.**

Lau, M. et al., 2025**.** Bridging Unsupervised and Semi-Supervised Anomaly Detection, arXiv**.**

Netwrix. (2025). 2025 Netwrix trends report. Netwrix Corporation. https://netwrix.com/en/resources/blog/file-integrity-monitoring-tools/

Samsung Insights. (2022, January). Federal government leads the way with encryption standards. Samsung Insights. https://insights.samsung.com/2022/01/12/federal-government-leads-the-way-with-encryption-standards/

Wang, J., Sun, Q., & Zhou, C. (2023). Insider threat detection based on deep clustering of multi-source behavioural events. Applied Sciences, 13(24), 13021. https://doi.org/10.3390/app132413021

Zimbabwe Cyber and Data Protection Act [Chapter 12:07]. (2022). Government of Zimbabwe. GN 492/2022. https://zimlii.org/akn/zw/act/2021/5/eng@2022-03-11

Homès, B. (2024). Testing Throughout the Software Life Cycle. *Fundamentals of Software Testing*

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004) 'Design science in information systems research', *MIS Quarterly*, 28(1), pp. 75–105.

Denzin, N.K. and Lincoln, Y.S. (eds.) (2018) *The SAGE Handbook of Qualitative Research*. 5th edn. Thousand Oaks, CA: Sage Publications.

Creswell, J.W. and Creswell, J.D. (2018) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th edn. Thousand Oaks, CA: Sage Publications.

Government of Zimbabwe (2021) *Cyber and Data Protection Act [Chapter 12:07]*. Harare: Government of Zimbabwe.

British Educational Research Association. (2024). Ethical Guidelines for Educational Research (5th ed.). London: BERA. www.bera.ac.uk/publication/ethical-guidelines-for-educational-research-2024 (bera.ac.uk in Bing)

Tripathi, S., & Chaturvedi, R.K. (2023). Exploring Ethical Considerations in Research: Guidelines and Practices. Adhyayan: A Journal of Management Sciences, 13(1), 41–45. https://doi.org/10.21567/adhyayan.v13i1.08

Abbas, H.S.M., Qaisar, Z.H., Ali, G., Alturise, F. and Alkhalifah, T. (2022) 'Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare,' *PLOS ONE*, 17(11), e0274550. https://doi.org/10.1371/journal.pone.0274550

Cornelius, F.P. and Jansen van Rensburg, S.K. (2024) 'Emerging South African smart cities: data security and privacy risks and challenges,' *South African Journal of Information Management*, 26(1), a1847. https://doi.org/10.4102/sajim.v26i1.1847

Zvaita, G.T. and Shava, E. (2026) 'Implementation of digital governance to enhance oversight in local municipalities,' *Frontiers in Sustainable Cities*, 8, 1713754. https://doi.org/10.3389/frsc.2026.1713754

Timcke, S., Gaffley, M. & Rens, A. (2023) 'The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa's Transnet,' The African Journal of Information and Communication *(AJIC),* 32, pp. 1–28.

APPENDIX A: INTERVIEW GUIDE FOR ICT STAFF AND MANAGEMENT

Institution: Bindura Municipality

Research Title: An Intelligent File Activity Monitoring and Auditing System for Enhancing Data Security

Researcher: Lucy P Matikinyidze (B222919B)

INTRODUCTION: Thank you for participating in this interview. The interview should take approximately 10 to 15 minutes.

Section A: Background information

What is your current position and how long have you worked in the ICT or data management department at Bindura Municipality?

Section B: File Monitoring Practices Today

2. How does the municipality currently monitor file access and activity? Are audit logs made automatically or manually?

3. How often are these audit records examined and by whom?

Section C: Security Risks and Challenges

4. What do you think are the greatest risks to file security here? Has there ever been any data theft or loss?

Section D. System Needs and Expectations

6. What features would be the most crucial in a new intelligent file monitoring system? For example: real-time alerts, audit trails or reporting tools .

7. Are you worried about switching to an automated monitoring system, for example staff resistance, cost, or if the current infrastructure can handle it?

8. is there anything else you'd want to add concerning file security and data management at Bindura Municipality?

Thanks again for your time and feedback.

APPENDIX B: QUESTIONNAIRE FOR MUNICIPAL STAFF

Research Title: An Intelligent File Activity Monitoring and Auditing System for Enhancing Data Security

Researcher: Lucy P Matikinyidze (B222919B) - Bindura University of Science Education

INSTRUCTIONS: Please answer all questions by ticking (✓) the most appropriate option or writing in the space provided.

Section A: Demographic Information

1. Department: _____

2. Years of service in the municipality: □ < 1 year □ 1–3 years □ 4–7 years □ 8+ years

3. Highest education level: □ Certificate □ Diploma □ Degree □ Postgraduate

Section B: Current System Awareness

4. Are you aware of any file monitoring or auditing system currently in use?

□ Yes □ No □ Not sure

5. How often do you access sensitive municipal files?

□ Daily □ Weekly □ Monthly □ Rarely

6. Have you ever noticed unauthorized or unusual file activity in your department?

□ Yes □ No □ Not sure

Section C: Perceptions on Data Security

Rate the following statements on a scale of 1–5 (1 = Strongly Disagree, 5 = Strongly Agree):

Statement	**1**	**2**	**3**	**4**	**5**
The current file management system is secure.					
I feel confident that unauthorized access to files is detected quickly.					
The municipality has adequate audit trails for file activity.					

Statement	1	2	3	4	5
I would benefit from real-time alerts on suspicious file activity.					
A new intelligent monitoring system would improve my workflow.					

Section D: Proposed System Expectations

7. Which of the following features do you consider most important? (Tick all that apply)

□ Real-time monitoring dashboard

□ Automated email/SMS alerts

□ Detailed audit logs

□ Role-based access control

□ Automated report generation

□ Anomaly detection / suspicious behaviour flagging