BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES

Effects Of Machine Learning And Artificial Intelligence In Intrusion Detection And Crime Prevention; Case Of Air Zimbabwe

By TAKAWIRA TEDIUS GUTU

B220277B

SUPERVISOR: MR CHITUMA

A DISERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE BACHELOR OF BUSINESS ADMINISTRATION (HONOURS) DEGREE IN POLICE AND SECURITY STUDIES OF BINDURA UNIVERSITY OF SCIENCE AND EDUCATION. FACULTY OF COMMERCE DEPARTMENT OF INTELLIGENCE AND SECURITY.

RELEASE FORM

NAME OF AUTHOR : Takawira T Gutu

TITLE OF PROJECT : EFFECTS OF MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE IN INTRUSION DETECTION AND CRIME PREVENTION: CASE OF AIR ZIMBABWE

PROGRAMME OF WHICH THESIS WAS PRESENTED: BACHELOR'S DEGREE IN BUSINESS ADMINSTRATION IN POLICE AND SECURITY STUDIES

YEAR THIS DEGREE GRANTED: 2022

SIGNED……T. Gutu ……

ADDRESS: HOUSE NUMBER 34403

UNIT L EXT

SEKE

CHITUNGWIZA

DATE: …08/10/25 ……

APPROVAL FORM

The undersigned certify that they have supervised the student Takawira Tedius Gutu's dissertation entitled, "Effects of Machine Learning and artificial intelligence in intrusion detection and crime prevention. Case of Air Zimbabwe." submitted in partial fulfilment of the requirements of the Bachelor of Business Administration in Police and Security Studies (Honours) Degree.

……T.T. Gutu…… **..14……/…10…/…25….**

Student **Date**

fc 

…… **…14…../…10…./…25….**

Supervisor **Date**

…… **…14…./…10…./…25….**

Chairperson **Date**

DEDICATION

I would like to dedicate this program to my very supportive wife Joana Gutu, my children Anopaishe, Tinevimbo, Munesuishe and Kunashe Gutu.

Acknowledgments

I want to express my sincere appreciation for the resolute support and guidance I received throughout this research project. My deepest gratitude goes to my supervisor, **Mr. Chituma F.**, whose dedicated teaching and resolute support were instrumental in the successful completion of this research. I am also incredibly thankful to all the **respondents** who honestly and faithfully provided the essential information that formed the foundation of this study. Their contributions were invaluable in uncovering the facts related to this research. Special thanks to my dear wife, **Joana**, for her constant and consistent financial, time, spiritual, and moral support during the demanding period of this research project. Your encouragement kept me going. Finally, I extend my heartfelt thanks to my friends, **Edwin Mateko** and **Paddington Nderemani**, who never gave up on me throughout my time of study. Your steadfast belief in me made a significant difference.

May the Almighty bless you all.

Abstract

This study aimed to examine the strategies and tactics employed by Air Zimbabwe as well as the efficacy of artificial intelligence and machine learning in identifying intrusions and preventing crimes in an aviation-based company. Cybersecurity threats and criminal activities have become increasingly sophisticated, outpacing the capabilities of traditional rule-based intrusion detection systems and crime prevention methods. A qualitative research method to be used and a sample size of twenty participants selected through purposive sampling. Field data was gathered using a semi-structured interview guide. The objectives of the study were to: to investigate the potential of integrating machine learning and artificial intelligence with traditional security measures to enhance intrusion detection and crime prevention at Air Zimbabwe, as well as examine the impact of artificial intelligence driven analytics on crime prevention. The study will also try to develop and design an artificial intelligence detecting system and evaluate its performance. Finally, to look into the difficulties and restrictions of applying artificial intelligence and machine learning to intrusion detection and crime prevention in the aviation sector. The findings of this dissertation help foster a better comprehension of the role of machine learning and artificial intelligence in improving intrusion detection and crime prevention, while also highlighting the importance of developing appropriate governance frameworks to guarantee the ethical and appropriate use of these cutting-edge technology. The knowledge gained from this study can help guide the design. and implementation of future intelligent systems in cybersecurity and public safety, balancing the benefits of enhanced security with the preservation of civil liberties and societal well-being

List of Appendices

List of Figures

List of Tables

Table of Contents

CHAPTER I

INTRODUCTION

1.0 Introduction

The aviation industry is constantly evolving, driven by rapid advancements in technology. To remain competitive and secure, the sector must embrace these changing trends. As Jiang, Tran, and Williams (2023) highlight, technology and new digital capabilities have already sparked massive transformations. The integration of Machine Learning (ML) and Artificial Intelligence (AI) has fundamentally reshaped operations across various sectors, especially in security and crime prevention.

This research investigates the impact of ML and AI on intrusion detection and crime prevention, with a specific focus on Air Zimbabwe. As the aviation industry increasingly confronts cybercrime and physical security threats, leveraging ML and AI offers powerful new ways to bolster safety and operational integrity (Bertino & Islam, 2017).

Intrusion detection systems (IDS) have significantly advanced through AI algorithms, enabling real-time identification of anomalies and potential threats (Patel et al., 2019). These improvements not only boost threat detection accuracy but also reduce false positives, allowing security personnel to concentrate on genuine risks. Furthermore, predictive analytics empowers organizations to proactively address vulnerabilities and mitigate risks before incidents occur (Chand & Sharma, 2020).

For Air Zimbabwe, applying these technologies is vital due to the airline's complex operations and the sensitive nature of passenger data. This research aims to explore how ML and AI can be systematically implemented to strengthen Air Zimbabwe's security frameworks, ultimately contributing to safer travel experiences and more robust crime prevention strategies. The introduction of sophisticated AI measures is critical in an industry where errors can lead to significant fatalities; well-programmed machines can drastically reduce mistakes.

This study will examine major security areas, including Air Traffic Control, Passenger Movement, Access Control, Check-in Points, Baggage Screening, and Cargo Handling and Screening. For each area, we will investigate the types of machine learning used and their effectiveness, also drawing comparisons with other airlines' use of AI.

1.1 Background of the Study

The emergence of Machine Learning (ML) and Artificial Intelligence (AI) has profoundly transformed various sectors, particularly in enhancing security. Within the aviation industry, the demand for robust intrusion detection systems has become increasingly urgent due to the rise in cyber threats and physical security breaches. As a national airline, Air Zimbabwe faces these challenges directly, with potential risks that could compromise both passenger safety and operational efficiency (Alazab et al., 2020).

Historically, intrusion detection primarily relied on signature-based methods, which had limited adaptability to new and evolving threats. The integration of AI and ML technologies has revolutionized this field by enabling systems to learn from data patterns and make independent decisions about potential threats (Kumar et al., 2021). For example, deep learning algorithms can analyze vast amounts of real-time data to identify unusual behavior indicative of a security breach, offering a more dynamic approach to threat detection (Sari et al., 2022).

Moreover, the predictive capabilities of ML allow for the anticipation of criminal activities before they occur, thus facilitating proactive crime prevention strategies. By analyzing historical data and identifying trends, Air Zimbabwe can implement measures to mitigate risks associated with both cyber and physical threats (Zhang et al., 2023). This not only enhances passenger safety but also safeguards sensitive information and the airline's reputation.

As the aviation security landscape continues to evolve, understanding the impact of implementing ML and AI in intrusion detection and crime prevention is crucial. This

research aims to provide insights into how Air Zimbabwe can effectively harness these technologies to address its growing security challenges.

1.2 Statement of the problem

The aviation industry is increasingly vulnerable to sophisticated security threats, including cyberattacks and physical intrusions, which pose significant risks to operational integrity and passenger safety. Air Zimbabwe, as a national carrier, faces unique challenges in safeguarding its systems and ensuring the security of sensitive passenger and operational data.

Air Zimbabwe had faced similar intrusion, I found interest in carrying out this research. On 13th of July 2023, an intruder from Epworth was found sitting in an Aircraft which was under maintenance. In December 2024 an Air Zimbabwe Employee was arrested for theft of Jet A-1 fuel. The employee was using non designated routs entering the premises during unprescribed times as an intruder.

A lot of people have zeal and eager to see an aircraft hence they have in their mind that they can just find their way to the aircraft bay not knowing that it is unlawful under the civil aviation act.

Traditional methods of intrusion detection often prove insufficient against rapidly evolving threats, leading to more frequent security breaches and a reactive, rather than proactive, security approach (Bertino & Islam, 2017). This underscores the critical need for more advanced solutions in sectors like aviation.

Numerous studies highlight the revolutionary potential of artificial intelligence (AI) and machine learning (ML) in supporting crime prevention tactics and intrusion detection systems for example, Alazab et al. (2020) comprehensively reviewed cybersecurity in the aviation sector, emphasizing that conventional security measures often fall short against sophisticated cyber threats. They strongly advocate for incorporating solutions powered by AI to improve threat detection and response capabilities, which are obviously essential for airlines like Air Zimbabwe.

Kumar et al. (2021) further explored the application of various ML techniques in cybersecurity. Their work demonstrates that methods such as support vector machines, neural networks, and decision trees can significantly improve the accuracy of intrusion detection systems. Their findings suggest that ML not only speeds up anomaly detection but also reduces false positive rates, making it an invaluable asset for organizations striving to secure their operations.

Additionally, Sari et al. (2022) investigated the role of deep learning in cybersecurity, illustrating its effectiveness in analyzing large datasets to identify patterns indicative of potential security breaches. They argue that deep learning models can learn and adapt to new types of threats, which is crucial for dynamic environments like those faced by airlines. This adaptability is particularly relevant for Air Zimbabwe as it navigates diverse security challenges.

Furthermore, Zhang et al. (2023) provided insights into using predictive analytics for crime prevention. They emphasize that analyzing historical data can inform proactive security measures, indicating that organizations employing predictive models are better positioned to prevent incidents before they occur. This could be especially beneficial for Air Zimbabwe in mitigating risks associated with both cyber and physical threats.

Collectively, these studies underscore the vital importance of integrating ML and AI technologies into the security frameworks of organizations like Air Zimbabwe, highlighting their substantial potential to enhance both intrusion detection and crime prevention capabilities.

1.3 Research Objectives

The following objectives were guiding this research:

i) To identify the current security technologies of intrusion detection systems (IDS) used by Air Zimbabwe.
ii) To highlight benefits of ML and AI in intrusion detection
iii) To explore the challenges and barriers faced by Air Zimbabwe in adopting ML and AI technologies for intrusion detection.
iv) To show case the importance of intrusion detection at air Zimbabwe
v) To recommend the use of AI and ML in crime prevention and detection at Air Zimbabwe

1.4 Research questions

i) What are security technologies currently in use for intrusion detection at Air Zimbabwe?
ii) What are the benefits of ML and AI on intrusion detection?
iii) What are challenges faced in adopting ML and AI at Air Zimbabwe?
iv) What are the importance of intrusion detection at air Zimbabwe?
v) How does ML and AI prevent crime and detects intrusion?

1.5 Purpose of the Study

The purpose of this study to analyze the effectiveness and efficiency on artificial intelligence gargets used to detect intrusion and crime prevention in the aviation industry compared to the ordinary ways of comparting crime.

1.6 Assumptions of the Study

This research on implementing ML and AI in Air Zimbabwe's security framework operates under several key assumptions:

Data Availability: We assume that enough relevant historical and current data on security incidents—including cyber threats, intrusion attempts, and crime statistics specific to Air Zimbabwe—will be accessible for thorough analysis (Zhang et al., 2023).

Technological Infrastructure: It's presumed that Air Zimbabwe already has, or can acquire, the necessary technology (hardware, software, network capacity) to effectively implement ML and AI solutions that support advanced analytics and real-time data processing (Kumar et al., 2021).

Skilled Personnel: The study assumes that either skilled personnel in ML and AI techniques are available, or that existing staff can be trained. This expertise is vital for successfully integrating and operating these technologies within Air Zimbabwe's security systems (Bertino & Islam, 2017).

Stakeholder Buy-in: We anticipate that key stakeholders within Air Zimbabwe, such as management and IT security teams, will support adopting ML and AI. This support is crucial for allocating resources and prioritizing security initiatives (Alazab et al., 2020).

Demonstrable Effectiveness: The research assumes that ML and AI technologies will indeed lead to measurable improvements in intrusion detection and crime prevention, specifically by reducing security incidents and enhancing threat response times (Sari et al., 2022).

Stable External Environment: We presume a relatively stable external environment concerning aviation security regulations and compliance frameworks. Significant changes in regulations or unforeseen external threats could impact the applicability of our findings (Kumar et al., 2021).

1.7 Scope of the Study

This study focuses on how Machine Learning (ML) and Artificial Intelligence (AI) impact intrusion detection and crime prevention specifically at Air Zimbabwe. The research will cover several key areas:

Technological Application: We'll explore various ML and AI methods include deep learning, supervised learning, and unsupervised learning, to see how effectively they can boost intrusion detection systems. This includes analyzing their ability to spot anomalies and predict potential security threats in real-time (Kumar et al., 2021).

Security Challenges: The study will pinpoint and examine the specific security issues Air Zimbabwe faces, including both cyber threats and physical intrusions. This involves reviewing existing literature on aviation sector vulnerabilities, considering Air Zimbabwe's unique operational context (Alazab et al., 2020).

Implementation Strategies: We'll investigate the practicalities of embedding ML and AI technologies into Air Zimbabwe’s security framework. This means evaluating the resources, expertise, and infrastructure needed for successful integration, along with any potential hurdles to adoption (Bertino & Islam, 2017).

Impact Assessment: The research will assess the overall effect of ML and AI on improving security measures and cutting down on crime incidents within the airline. This evaluation will use both qualitative and quantitative metrics, such as comparing incident rates before and after implementation (Zhang et al., 2023).

Case Study Methodology: This research will employ a case study approach, using Air Zimbabwe as the primary focus. This will allow for in-depth insights into how ML and AI are applied in a real-world aviation security setting. Data will be gathered through interviews, surveys, and analysis of security incidents reported by the airline.

1.8 Delimitations of the Study

This study on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe is subject to specific delimitations, which define the boundaries and focus of the research:

Geographical Focus: Air Zimbabwe is an Aviation Company which is situated at Robert Gabriel International Airport. This research is limited to Air Zimbabwe and other Air Zimbabwe sub stations and offices, it does not extend to other airlines or aviation companies. This focus is intended to provide in-depth insights specific to the operational and security context of Air Zimbabwe

Technology Scope: The study will primarily examine the application of ML and AI technologies specifically for intrusion detection and crime prevention. It will not explore other potential applications of these technologies within the aviation sector, such as customer service or operational efficiency improvements (Kumar et al., 2021).

Data Sources: The study will rely on specific data sources, including interviews with Air Zimbabwe security personnel, analysis of internal security reports, and relevant literature. It will not include external case studies from other airlines or industry sectors unless they are directly applicable to the findings (Bertino & Islam, 2017).

Time Frame: The research will focus on recent advancements and trends in ML and AI, particularly from the last five years. Historical data prior to this period may not be extensively analyzed, as the emphasis is on current technologies and their immediate impacts (Zhang et al., 2023).

1.9 Limitations of the Study

This research on the impact of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe faces several limitations that could affect its findings and how widely they apply:

Data Availability: The study's accuracy depends heavily on getting enough high-quality data from Air Zimbabwe about past security incidents and how well current systems work. If this data is limited, our analysis might be incomplete, leading to conclusions that aren't fully representative (Zhang et al., 2023).

Subjectivity in Qualitative Analysis: Because this research uses qualitative methods like interviews and case studies, there's a chance of bias or subjectivity in how the data is interpreted. Different participants might have varying perceptions and experiences, which could impact the reliability of our findings (Kumar et al., 2021).

Rapid Technological Change: ML and AI technologies are evolving incredibly fast. This means our findings could quickly become obsolete as new algorithms and techniques emerge after the study is finished, limiting the long-term relevance of our results (Sari et al., 2022).

10.0 Summary

Furthermore, the chapter justifies the need for this research by discussing the potential benefits of adopting ML and AI in aviation security. It emphasizes that these technologies can lead to enhanced threat detection capabilities, reduced response times, and improved overall security outcome

CHAPTER II

LITERATURE REVIEW

2.0 Introduction

The integration of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention has gained significant attention in recent years, particularly within the aviation sector. This literature review explores the current state of research regarding the application of these technologies, emphasizing their potential benefits and challenges, and contextualizing them within the specific case of Air Zimbabwe

2.1 Definition and purpose of literature review

Definition

A literature review is a methodical analysis and synthesis of previous academic studies and works on a particular subject. It aims to identify, evaluate, and summarize the current state of knowledge, theories, and methodologies relevant to the research question at hand (Webster & Watson, 2002). In the context of the research topic "Effects of Machine Learning and Artificial Intelligence in Intrusion Detection and Crime Prevention: Case of Air Zimbabwe," the literature review encompasses studies focusing on the application of ML and AI technologies in enhancing security measures within the aviation sector.

Purpose

The primary purposes of the literature review in this study are as follows:

Contextualization: The literature review provides a foundation for understanding the significance of ML and AI in intrusion detection and crime prevention. By examining previous research, it places the study in the context of the larger scholarly conversation and emphasises how pertinent it is to the security issues facing aviation today. (Machi & McEvoy, 2016). Identifying Gaps: One of the critical functions of the literature review is to identify gaps in the existing body of knowledge. This study seeks to uncover areas where research is lacking, particularly concerning the application of ML and AI technologies in specific contexts like Air Zimbabwe. By pinpointing these gaps, the study can justify its relevance and the need for further exploration (Fink, 2014).

Methodological Insights: The literature review provides information on the different research techniques used in earlier investigations. Understanding these methodologies helps inform the design of the current study, enabling the adoption of effective data collection and analysis techniques (Booth et al., 2016).

Theoretical Framework: By synthesizing theoretical perspectives related to ML and AI, the literature review establishes a conceptual framework that underpins the research. This framework guides the analysis of how these technologies can impact intrusion detection and crime prevention strategies at Air Zimbabwe (Webster & Watson, 2002).

Establishing Relevance: The literature review demonstrates the significance of exploring the effects of ML and AI in the context of Air Zimbabwe. By highlighting existing research findings and their implications, It reaffirms the study's goals and the possible contributions to scholarly research as well as real-world security applications (Machi & McEvoy, 2016).

To sum up, the literature review is an essential aspect of the research process that helps researchers fully comprehend how ML and AI affect intrusion detection and crime prevention, especially at Air Zimbabwe.

2.2 Conceptual frame work

The conceptual framework for this research on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe is designed to illustrate the relationships between key variables and concepts in the study. This concept acts as a platform for examining how AI and ML might improve aviation security protocols.

Machine Learning Techniques: A variety of ML methods, including deep learning, supervised learning, and unsupervised learning, can be used to identify threats and discover anomalies (Kumar et al., 2021).

Artificial Intelligence Applications: The broader application of AI technologies, including predictive analytics and automated decision-making processes that can improve security measures (Bertino & Islam, 2017).

Data Quality and Availability: The extent and quality of data available for training ML models, which significantly influence the effectiveness of these technologies in detecting intrusions and preventing crime (Alazab et al., 2020).

Organizational Readiness: The preparedness of Air Zimbabwe to adopt and implement ML and AI technologies, including staff training, technological infrastructure, and management support (Sari et al., 2022).

Intrusion Detection Effectiveness: The ability of the security systems to identify unauthorized access and anomalies in real-time, measured by metrics such as detecrates and false positive rates (Zhang et al., 2023).

Crime Prevention Outcomes: The overall impact on reducing incidents of crime, including cyber threats and physical security breaches, as well as the effectiveness of proactive measures (Kumar et al., 2021).

The relationships among these components can be visualized as follows:

[Machine Learning Techniques] + [AI Applications]

↓

[Data Quality and Availability] ↔ [Organizational Readiness]

↓

[Intrusion Detection Effectiveness] → [Crime Prevention Outcomes]

Impact of ML and AI: The independent variables (ML techniques and AI applications) influence the mediating variables by providing advanced tools and methodologies that enhance data analysis and decision-making.

Mediating Effects: Data quality and organizational readiness mediate how the independent and dependent variables are related. High-quality data and a supportive organizational environment are crucial for the successful implementation of ML and AI technologies.

Outcome Measurement: The effectiveness of intrusion detection systems will impact the overall crime prevention outcomes, demonstrating how advances in technology can lead to tangible improvements in security for Air Zimbabwe.

In the context of Air Zimbabwe, this conceptual framework offers an organised method for comprehending how ML and AI affect intrusion detection and crime prevention. By

looking at these relationships the study's objectives to contribute valuable insights into how these technologies can be effectively leveraged to enhance aviation security.

2.3.0 Theoretical Framework

The theoretical framework for this research on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe is built upon several interrelated theories and concepts that offer a thorough comprehension of how these technologies might improve security protocols. This framework integrates theories from cybersecurity, information systems, and decision-making, offering a multi-dimensional perspective on the application of ML and AI in the aviation sector.

2.3.1. Technology Acceptance Model (TAM)

According to the Technology Acceptance Model (TAM), users' acceptance of new technologies is greatly influenced by their perceived usefulness and simplicity of use. (Davis, 1989). In the context of Air Zimbabwe, this model helps explain how stakeholders' perceptions regarding the usability and benefits of ML and AI technologies can impact their adoption and implementation in security practices. Understanding these perceptions is crucial for fostering a culture of innovation and ensuring effective integration of advanced technologies.

2.3.2. Anomaly Detection Theory

Anomaly detection theory is fundamental to understanding how ML algorithms identify unusual patterns in data that may indicate security threats. This theory suggests that by training models on historical data, these systems can learn to recognize normal behavior and subsequently flag deviations that warrant further investigation (Chandola et al., 2009). This framework is particularly relevant for intrusion detection systems, where the ability to detect anomalies in real-time is critical for preventing security breaches.

2.3.3. Predictive Analytics Framework

The predictive analytics framework emphasizes utilising machine learning algorithms and statistical methods to evaluate past data and forecast future occurrences (Shmueli & Lichtendahl, 2016). In the case of Air Zimbabwe, this framework supports the application of AI-driven predictive models to anticipate potential security threats based on previous incidents. The implementation of predictive analytics can enhance proactive measures, allowing for timely interventions before threats escalate.

2.3.4. Cybersecurity Frameworks

Several cybersecurity frameworks, such as the NIST Cybersecurity Framework, provide guidelines for improving security posture and resilience (NIST, 2018). These frameworks emphasize the importance of continuous monitoring, risk assessment, and incident response, which can be significantly enhanced through the integration of ML and AI technologies. By aligning Air Zimbabwe's security strategies with established cybersecurity frameworks, the study can illustrate how these technologies contribute to a more robust security infrastructure.

2.3.5. Decision Theory

Decision theory explores how individuals and organizations make choices under conditions of uncertainty. The integration of ML and AI can improve decision-making processes in security contexts by providing data-driven insights and recommendations (Raiffa & Schlaifer, 1961). For Air Zimbabwe, leveraging AI to assist in decision-making regarding security protocols can lead to more informed and effective responses to potential threats.

The implications of machine learning and artificial intelligence (AI) on intrusion detection and crime prevention at Air Zimbabwe may be thoroughly examined using this theoretical framework. By incorporating elements from the Technology Acceptance Model, anomaly detection theory, predictive analytics framework, cybersecurity frameworks, and decision theory, the research can effectively analyze how these technologies can enhance security measures and contribute to safer aviation operations.

2.4 Empirical evidence

The application of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention has garnered substantial empirical support from various studies, underscoring their effectiveness and relevance in enhancing security measures. This section outlines key empirical findings that relate directly to the research topic, particularly in the context of Air Zimbabwe.

A study by Kumar et al. (2021) evaluated the performance of several ML algorithms in detecting intrusions in network traffic. The research demonstrated that algorithms such as Random Forest and Support Vector Machines significantly outperformed traditional methods, achieving detection rates exceeding 95% with reduced false positive rates. This evidence suggests that ML can enhance the accuracy of intrusion detection systems, which is critical for an airline like Air Zimbabwe that must safeguard sensitive data and ensure passenger safety.

Research conducted by Zhang et al. (2023) highlighted the efficacy of AI-driven predictive analytics in crime prevention strategies. The study found that predictive models developed using historical crime data allowed organizations to anticipate and mitigate potential risks effectively. For instance, the implementation of predictive analytics reduced security incidents by approximately 30% in the case studies analyzed. This finding can be particularly relevant for Air Zimbabwe, as it underscores the potential for AI to proactively address threats before they escalate.

Zhang et al. (2023) highlighted the efficacy of AI-driven predictive analytics in crime prevention strategies.. Their study showed that deep learning models, such Convolutional Neural Networks (CNNs), could accurately detect odd patterns in network data. The study reported a 20% improvement in anomaly detection rates compared to traditional methods. This advancement suggests that the adoption of deep learning could significantly bolster Air Zimbabwe's the capacity to immediately identify and address security concerns.

A review by Alazab et al. (2020) examined various case studies involving the implementation of AI and ML in aviation security. One notable case involved the use of ML algorithms to analyze passenger data and predict potential security threats. The findings indicated a marked improvement in threat identification capabilities, leading to quicker response times and enhanced overall security measures. This empirical evidence supports the notion that Air Zimbabwe could benefit from similar implementations in its security protocols.

Empirical studies also highlight the challenges organizations face in adopting ML and AI technologies. For example, research by Bertino and Islam (2017) identified common barriers such as skill gaps, data quality issues, and resistance to change within organizations. Understanding these challenges is crucial for Air Zimbabwe, as addressing them will be essential for successful implementation and maximizing the benefits of ML and AI in security operations.

The empirical evidence presented demonstrates that ML and AI can significantly improve intrusion detection and crime prevention efforts. These findings provide a solid foundation for exploring how Air Zimbabwe can leverage these technologies to enhance its security framework. By adopting ML and AI, Air Zimbabwe has the potential to not only improve its threat detection capabilities but also to create a safer environment for its passengers and

2.5 Justifications of the study

The rationale behind this investigation into how Artificial Intelligence (AI) and Machine Learning (ML) impact intrusion detection and crime prevention at Air Zimbabwe is based on a number of important considerations that highlight the importance and necessity of the study.

The aviation industry is facing an escalating number of security threats, including cyberattacks and physical intrusions, which can have severe implications for passenger safety and organizational integrity. According to Alazab et al. (2020), the aviation sector is particularly vulnerable due to its reliance on complex information systems and the sensitivity of the data it handles. This necessitates the exploration of advanced technologies like ML and AI to bolster security measures.

Traditional intrusion detection systems often rely on static methods that are inadequate for addressing the dynamic nature of contemporary security threats. Bertino and Islam (2017) highlight that these conventional systems frequently result in high rates of false positives and may fail to detect sophisticated attacks. This study aims to investigate how ML and AI can provide adaptive solutions that improve threat detection accuracy and response times.

The integration of ML and AI offers the potential for significant advancements in intrusion detection and crime prevention. Research by Kumar et al. (2021) indicates that large

volumes of data may be analyzed by these technologies to find trends and abnormalities, which enables prompt actions. By concentrating on Air Zimbabwe, the study can shed light on how these technologies can be modified to satisfy the airline's unique security requirements, ultimately leading to safer travel experiences.

Although the literature on the use of machine learning and artificial intelligence in cybersecurity is expanding, there aren't many case studies specifically pertaining to the aviation industry, especially when it comes to domestic airlines like Air Zimbabwe. By offering empirical data and useful suggestions that might influence both scholarly discussions and business actions, this study aims to close this gap (Zhang et al., 2023).

As a national airline, Air Zimbabwe plays a critical function in the nation's economy and international relations. Enhancing its security measures through the adoption of ML and AI not only ensures the safety of passengers but also protects the airline's reputation and operational viability. Given the strategic importance of Air Zimbabwe, this study is especially relevant for stakeholders seeking to improve security protocols (Sari et al., 2022).

In summary, this study is justified by the pressing need to address increasing security threats in the aviation industry, the limitations of traditional security methods, and the potential for ML and AI to provide innovative solutions. By focusing on Air Zimbabwe, the research will contribute valuable insights to both the academic community and industry practitioners, ultimately enhancing security measures in the aviation sector.

Combining artificial intelligence (AI) and machine learning (ML) into intrusion detection and crime prevention is an emerging field that has gained considerable attention in various sectors, including aviation. However, specific research focusing on the effects of these

technologies within the context of Air Zimbabwe remains limited. This presents a significant research gap in several key areas:

While there is a growing body of literature on ML and AI applications in security, few studies specifically examine how these technologies can be effectively integrated into the security operations of Air Zimbabwe. Existing research often focuses on broader contexts or different industries, lacking the nuanced understanding required for the unique operational environment of the aviation sector in Zimbabwe.

The opinions and experiences of important Air Zimbabwe stakeholders about the application of ML and AI technologies are not sufficiently explored. Understanding the views of security personnel, IT specialists, and management is crucial for assessing both the potential benefits and challenges of these technologies, yet this perspective is often overlooked in the current literature.

The specific barriers and challenges faced by Air Zimbabwe in adopting ML and AI for security purposes have not been adequately documented. Factors such as organizational readiness, financial constraints, and technological infrastructure are critical to understanding the feasibility of these technologies but remain under-researched in this context.

Empirical research evaluating the real effects of machine learning and artificial intelligence on aviation security outcomes is lacking, especially in the African environment. It is challenging to derive useful conclusions for Air Zimbabwe because the majority of previous research focusses on theoretical frameworks or simulations rather than real-world implementations and results.

Addressing these research gaps is vital for advancing the understanding of how ML and AI can enhance intrusion detection and crime prevention in Air Zimbabwe. This study aims to fill these gaps by providing context-specific insights, assessing stakeholder perspectives, identifying barriers to implementation, and evaluating the impact of these technologies on aviation security.

2.6 Summary

The literature indicates a clear potential for ML and AI to enhance intrusion detection and crime prevention strategies in the aviation sector, including within Air Zimbabwe. However, the successful implementation of these technologies is contingent upon overcoming existing challenges related to data, expertise, and organizational culture. Further empirical research is needed to explore these dynamics in greater depth, particularly through case studies that can offer insights into best practices and effective strategies for integrating advanced technologies in aviation security.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Introduction

The research methodology for the study on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe is designed to systematically investigate the implementation and impact of these technologies within the airline's security framework. A well-structured methodology is essential for

obtaining reliable and valid results, enabling a comprehensive understanding of how ML and AI can enhance security measures in the aviation sector.

3.1 Research approach

This study on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe employs a qualitative research approach. This approach is particularly suited for exploring complex phenomena where understanding the perspectives and experiences of individuals is essential (Creswell & Creswell, 2018). By focusing on qualitative methods, the research aims to gain in-depth insights into the perceptions, challenges, and potential benefits associated with the implementation of ML and AI technologies in the aviation security context. A qualitative case study approach is chosen to allow for an in-depth exploration of the implementation and impact of ML and AI technologies within the unique operational environment of Air Zimbabwe. This approach facilitates a comprehensive understanding of the experiences and perceptions of stakeholders involved in security practices (Yin, 2018).

3.2 Research Design

The research design for the study on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe is structured to effectively address the research objectives and questions. This design employs a qualitative approach, utilizing a case study methodology to explore the specific context of Air Zimbabwe. The following sections outline the key components of the research design. The qualitative research design will utilize a case study methodology, enabling a detailed exploration of the specific context of Air Zimbabwe. This design allows for the examination of real-life implications of ML and AI in security practices, providing a rich understanding of how these technologies can be effectively integrated (Yin, 2018).

3.2.1 Justification of using (THE TYPE OF RESEARCH DESIGN)

The decision to employ a qualitative research design for the study on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe is grounded in several key justifications. This approach is particularly suited for exploring complex phenomena that involve human experiences, perceptions, and social contexts.

Understanding the complex ramifications of ML and AI technologies in security procedures requires a thorough investigation of participants' experiences and viewpoints, which research enables. The study can gather a variety of information about present security issues, the efficiency of current systems, and the expected effects of future technologies by conducting semi-structured interviews with stakeholders. (Kvale & Brinkmann, 2015). This depth of understanding is often unattainable through quantitative methods, which may overlook the complexities of human behavior and organizational dynamics (Creswell & Creswell, 2018).

The qualitative approach provides flexibility in data collection, allowing researchers to adapt questions and explore emerging themes during interviews. This flexibility is particularly valuable in a rapidly evolving field like security technology, where participants may have unique insights that can inform the research (Yin, 2018). Open communication is encouraged by the semi-structured approach, which allows participants to articulate their ideas in their own terms. This can result in surprising discoveries and more profound understandings.

Examining the contextual elements that affect the uptake and application of ML and AI technologies is a useful application of qualitative research. Understanding the organizational culture, existing practices, and stakeholder attitudes at Air Zimbabwe is crucial for assessing the potential for these technologies to improve security measures (Bowen, 2009). A qualitative design allows the researcher to gather contextual information that can illuminate the barriers and facilitators to technology adoption.

The study aims to prioritize the voices of those directly involved in security operations at Air Zimbabwe. By focusing on qualitative data, the research can highlight the perspectives of security personnel, IT specialists, and management, thus guaranteeing that the conclusions are based on the organization's actual circumstances. This emphasis on stakeholder perspectives aligns with participatory research principles, which advocate for the inclusion of those affected by the research outcomes (Palinkas et al., 2015).

Qualitative research can serve as a preliminary step in exploring new areas of inquiry, particularly in under-researched fields like the application of ML and AI in aviation security. The insights gained from qualitative data can help generate hypotheses and inform future quantitative studies, therefore advancing a more thorough comprehension of the subject. (Creswell & Creswell, 2018).

To sum up, a qualitative research design is warranted for this study since it can offer deep insights into the opinions and experiences of Air Zimbabwe stakeholders about machine learning and artificial intelligence. The flexibility, emphasis on context and stakeholder perspectives, and potential for generating hypotheses make qualitative research particularly well-suited for exploring the complex dynamics of intrusion detection and crime prevention in the aviation sector.

3.3.0 Population and sample

3.3.1 Population

The population for this study on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe consists of individuals directly involved in the airline's security operations and technology implementation. This includes:

Security Personnel: Staff responsible for monitoring and responding to security threats, including both operational and managerial roles.

IT Specialists: Employees involved in the development, maintenance, and implementation of security systems that utilize ML and AI technologies.

Management: Decision-makers who influence security policies and investments in technology, including executives and department heads.

For a thorough grasp of existing security procedures and the possible effects of ML and AI technologies, this diversified population is essential.

3.3.2 Sample and Sampling procedure

The sample for this study on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe will consist of key stakeholders directly involved in security operations and technology implementation within the organization. Specifically, the sample will include:

Security Personnel: Individuals responsible for monitoring and responding to security threats.

IT Specialists: Staff involved in the development, maintenance, and implementation of security systems utilizing ML and AI technologies.

Management: Decision-makers who influence security policies and technology investments.

A sample size of between 10 to 15 people is the goal. For qualitative research, this size works well since it permits in-depth examination of participants' perspectives while reaching data saturation, at which point no new topics surface from the interviews. (Guest, Bunce & Johnson, 2006).

Sampling Method, for this investigation, a purposive sampling technique will be used. A non-probability sampling method called "purposeful sampling" aims to choose participants who have particular traits or expertise related to the study's subject. (Palinkas et al., 2015). In qualitative research, where the objective is to obtain insights from people who have firsthand experience and subject-matter expertise, this approach works very well. The following standards will be used to choose participants:

Relevance to Security Operations: Participants must have direct involvement in security practices within Air Zimbabwe. This includes roles that relate to both operational and strategic aspects of security.

Experience with ML and AI Technologies: Individuals should have experience or knowledge about the use of ML and AI in security contexts, either through direct application or through policy-making roles.

Willingness to Participate: Participants must be open to participating in the study and freely sharing their opinions. This willingness will be assessed during initial communications when inviting individuals to participate.

The following steps will be part of the hiring process:

Identification of Potential Participants: Collaborating with department heads and human resources to identify suitable candidates from the security and IT departments, as well as management.

Invitation to Participate: The chosen participants will be contacted by phone or email to discuss the significance of their insights, the nature of their participation, and the goal of the study.

Informed Consent: Once participants agree to participate, informed consent will be obtained prior to data collection. This will include details about the study's purpose, procedures, risks, and the right to withdraw at any time.

In summary, the sample for this study will consist of approximately 10 to 15 key stakeholders from Air Zimbabwe, selected through purposive sampling to ensure relevant expertise and experience. The recruitment process will be carefully managed to facilitate participation and obtain meaningful insights into the effects of ML and AI in intrusion detection and crime prevention.

3.4.0 Source of Data

The sources of data for this study on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe will be derived from both primary and secondary data sources. This multi-faceted approach will ensure a comprehensive understanding of the research topic.

3.4.1 Primary Source

Semi-Structured Interviews, The primary source of data will be semi-structured interviews conducted with key stakeholders at Air Zimbabwe. These interviews will provide firsthand insights into the following:

Current Security Practices: Participants will share their experiences with existing intrusion detection systems and the challenges they face.

Perceptions of ML and AI: Stakeholders will discuss their views on the potential benefits and limitations of implementing ML and AI technologies in security operations.

Organizational Readiness: Insights will be gathered regarding the readiness of Air Zimbabwe to adopt new technologies and the barriers that may exist.

The qualitative nature of the interviews will allow for rich, detailed responses, contributing to a deeper understanding of the topic (Kvale & Brinkmann, 2015).

3.4.2 Secondary Source

Document Analysis: In addition to primary data, secondary data will be collected through document analysis. This will include a review of relevant internal documents from Air Zimbabwe, such as:

Security Incident Reports: Analyzing past security incidents will help identify trends and common vulnerabilities that ML and AI could address.

Technology Policy Documents: Reviewing existing policies regarding technology use in security will provide context for understanding current practices and gaps.

Training Manuals and Protocols: These documents will offer insights into how security personnel are trained to respond to threats and the role of technology in these protocols.

Secondary data will complement the primary data collected through interviews, enhancing the overall analysis and findings (Bowen, 2009).

Data collection will involve the following procedures:

Interview Scheduling: Participants will be contacted to schedule interviews at their convenience, ensuring a comfortable environment for open discussion.

Document Access: Relevant documents will be requested from the appropriate departments within Air Zimbabwe, ensuring compliance with any confidentiality agreements and ethical considerations.

The sources of data for this study will include primary data from semi-structured interviews with stakeholders at Air Zimbabwe and secondary data from document analysis. This comprehensive approach will facilitate a thorough investigation into the effects of ML and AI in intrusion detection and crime prevention.

3.5.0 Research Instruments

The research instruments for the study on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe will include semi-structured interviews and document analysis. These instruments are designed to gather comprehensive qualitative data that reflects the experiences and perceptions of key stakeholders within the organization.

Semi-Structured Interviews: The primary research instrument will be a semi-structured interview guide, which will consist of open-ended questions aimed at exploring the following areas:

Current Security Practices: Questions will focus on existing intrusion detection measures, the effectiveness of these systems, and the challenges faced by security personnel.

Perceptions of ML and AI: Participants will be asked about their views on the potential benefits and drawbacks of implementing ML and AI technologies in security operations.

Organizational Readiness: Questions will address perceptions of Air Zimbabwe's preparedness for adopting new technologies, including any barriers that may exist.

The semi-structured format allows for flexibility, enabling the interviewer to probe deeper into responses and explore emerging themes during the conversation (Kvale & Brinkmann, 2015).

Pilot Testing: Before the actual data collection, the interview guide will undergo pilot testing with a small group of individuals who have similar backgrounds to the target participants. This pilot test will help refine questions for clarity and relevance, ensuring that they effectively elicit meaningful responses (Creswell & Creswell, 2018).

3.5.1 Questionnaires

The research instrument for this study on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe will be a structured questionnaire. This instrument is designed to gather quantitative and qualitative data from key stakeholders within the organization, including security personnel, IT specialists, and management.

The primary objectives of the questionnaire are to:

1) Assess current security practices at Air Zimbabwe.
2) Evaluate perceptions of the effectiveness and applicability of ML and AI in enhancing security measures.
3) Identify challenges and barriers to the implementation of these technologies.
   Structure of the Questionnaire
   The questionnaire will be divided into five sections, each addressing specific aspects of the research topic. See appendix

3.6.0 Validity and Reliability

In the realm of research, particularly in studies involving complex technological applications such as Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention, the concepts of validity and reliability are paramount. These two fundamental principles ensure that the findings of a study are credible, accurate, and applicable to real-world settings.

3.6.1 Validity

The degree to which a research tool measures what it is supposed to measure is known as validity. Validity can be divided into three main categories in the context of this study on how Artificial Intelligence (AI) and Machine Learning (ML) affect intrusion detection and crime prevention at Air Zimbabwe:

Content Validity: This aspect assesses whether the questionnaire items adequately cover the research topic. The questionnaire will be created using a thorough literature research and expert consultation in the domains of security technology and AI applications to guarantee content validity. (Creswell & Creswell, 2018). Feedback from subject-matter experts will also be solicited to confirm that all relevant dimensions of the topic are addressed.

Construct Validity: Construct validity evaluates whether the instrument truly measures the theoretical constructs it claims to measure. This will be assessed through pilot testing of the questionnaire with a small group of participants to identify any ambiguities or misinterpretations in the items, allowing for necessary adjustments (Bryman, 2016).

External Validity: External validity pertains to the generalizability of the study findings beyond the specific context of Air Zimbabwe. The research will aim to provide detailed contextual information, enabling other researchers and practitioners in the aviation and security sectors to assess the applicability of the findings in different settings (Yin, 2018).

3.6.2 Reliability

Reliability refers to the consistency of a research instrument in measuring a construct over time. For this study, several strategies will be employed to ensure the reliability of the questionnaire and data collection methods:

Internal Consistency: Internal consistency will be assessed using Cronbach's alpha to determine the coherence of items measuring similar constructs within the questionnaire. A Cronbach's alpha value of 0.70 or higher will indicate acceptable reliability (Field, 2018).

Test-Retest Reliability: The questionnaire will be given to a small sample of participants twice in order to assess test-retest reliability. To evaluate the instrument's long-term

stability, the correlation between the two sets of responses will be examined. Strong test-retest reliability would be indicated by a high correlation (Bryman, 2016).

Inter-Rater Reliability: For any qualitative data collected from interviews, inter-rater reliability will be ensured by involving multiple researchers in the coding process. By comparing the coding results and discussing any discrepancies, the reliability of the qualitative findings will be enhanced (Creswell & Creswell, 2018).

Both validity and reliability are critical to the integrity of the research on the effects of ML and AI in intrusion detection and crime prevention at Air Zimbabwe. By addressing content, construct, and external validity, along with implementing strategies to ensure internal consistency, test-retest reliability, and inter-rater reliability, the study aims to produce credible and trustworthy findings.

3.6.3 Pilot study

A pilot study will be conducted to refine the research instruments and methodologies for the main study on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe. This preliminary phase aims to identify any potential issues with the data collection process, ensure the clarity of questions, and enhance the overall reliability and validity of the research instruments.

The primary objectives of the pilot study are:

1) To Test the Research Instruments: Evaluate the semi-structured interview guide and questionnaire for clarity, relevance, and comprehensiveness.

2) To Assess Data Collection Procedures: Identify any challenges in the data collection process, including participant recruitment and interview techniques.

3) To Gather Preliminary Insights: Collect initial data to inform the research design and refine research questions based on participant feedback and responses.

3.7.0 Data collection and presentations

3.7.1 Data Collection

Data collection for the study on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe will involve two primary methods: semi-structured interviews and document analysis.

Participant Selection: Key stakeholders, including security personnel, IT specialists, and management staff, will be purposively sampled. Approximately 10 to 15 participants will be recruited to ensure a diverse range of perspectives (Palinkas et al., 2015).

Interview Format: Each interview will last between 15 to 20 minutes and will follow a semi-structured format. This allows for flexibility in questioning and encourages participants to elaborate on their responses, leading to richer data (Kvale & Brinkmann, 2015).

Recording and Transcription: Interviews will be recorded (with participants' consent) and subsequently transcribed for analysis. This ensures that all responses are accurately captured and can be revisited during the analysis phase.

Types of Documents: Relevant internal documents from Air Zimbabwe will be analyzed, including security incident reports, technology policy documents, and training manuals.

Data Extraction: Key themes and relevant data points will be extracted from these documents to complement the findings from the interviews. This method provides contextual information and supports triangulation of the qualitative data (Bowen, 2009).

Data Presentation: Data presentation will involve both quantitative and qualitative strategies to effectively convey the findings of the research.

Analysis Process: Thematic analysis will be employed to identify patterns and themes within the qualitative data collected from interviews and document analysis (Braun & Clarke, 2006). The analysis will follow these steps:

1. Familiarization with the data through reading and re-reading transcripts.

2. Generating initial codes that capture key features of the data.

3. Identifying and reviewing themes that emerge from the coded data.

Defining and naming themes to create a coherent narrative.

Reporting: Findings will be presented in a structured format, with themes illustrated using direct quotes from participants to provide authenticity and depth to the analysis. This narrative will highlight the participants' perspectives on the effectiveness, benefits, and challenges of implementing ML and AI in security operations.

Summary Tables: Tables summarizing key themes, participant demographics, and responses to specific questions will be created to allow for quick reference and comparison.

Graphs and Charts: Where applicable, visual representations (such as pie charts or bar graphs) may be used to depict participant responses quantitatively, particularly in relation to perceptions of ML and AI technologies.

The data collection process will utilize a combination of semi-structured interviews and document analysis to gather rich qualitative insights into the effects of ML and AI in intrusion detection and crime prevention at Air Zimbabwe. Data presentation will focus on thematic analysis, supplemented by visual aids to enhance understanding and accessibility of the findings.

3.8 Ethical considerations

Conducting research on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe necessitates a careful consideration of ethical issues. The following ethical considerations will guide the research process:

Informed Consent: Participants will be fully informed about the nature, purpose, and potential impacts of the research before agreeing to participate. This includes:

Clear Explanation: Providing participants with a clear explanation of the study's objectives, procedures, and their role in the research.

Voluntary Participation: Ensuring that participation is voluntary and that participants can withdraw from the study at any time without any negative consequences (Creswell & Creswell, 2018).

Confidentiality and Anonymity: Maintaining the confidentiality and anonymity of participants is paramount. This will be achieved through:

Data Protection: Ensuring that all data collected is securely stored and accessible only to the research team. Personal identifiers will be removed from transcripts and any published materials to protect participant identities (Kvale & Brinkmann, 2015).

Anonymous Reporting: When presenting findings, individual responses will not be attributed to specific participants, thereby maintaining their anonymity.

Ethical Approval: Before commencing the research, ethical approval will be sought from the relevant institutional review board or ethics committee at Air Zimbabwe. This is to ensure that the research adheres to ethical guidelines and standards for conducting research involving human participants (Bryman, 2016).

Potential Risks and Benefits: A thorough assessment of potential risks and benefits associated with participation in the study will be conducted. Participants will be informed of:

Potential Risks: Any potential risks involved in participating in the research, such as the possibility of discussing sensitive security-related topics.

Benefits: The potential benefits of the research, including contributions to enhanced security practices at Air Zimbabwe and the broader aviation sector.

Respect for Participants: Researchers will demonstrate respect for all participants throughout the study by:

Sensitivity: Being aware of and sensitive to the cultural and organizational context of Air Zimbabwe, which may influence participants' experiences and responses.

Open Communication: Encouraging participants to ask questions or express concerns about the research process at any time.

Integrity of the Research Process: Ensuring the integrity of the research process is essential. This involves:

Honest Reporting: Accurately reporting findings and acknowledging any limitations of the study.

Avoiding Conflicts of Interest: Researchers will disclose any potential conflicts of interest that may affect the study or its findings (Field, 2018).

Ethical considerations in this research on the effects of ML and AI in intrusion detection and crime prevention at Air Zimbabwe will involve obtaining informed consent, ensuring confidentiality and anonymity, seeking ethical approval, assessing risks and benefits, respecting participants, and maintaining the integrity of the research process. These considerations are crucial for conducting responsible and ethical research.

3.9 Summary

In summary, the methodology for this research combines qualitative data collection methods, purposive sampling, and thematic analysis to explore the effects of ML and AI in intrusion detection and crime prevention at Air Zimbabwe. This approach aims to yield rich, contextual insights that contribute to the understanding of modern security practices.

CHAPTER IV

DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.0 Introduction

Analysis of data, findings and interpretation of results was summarized in this chapter. Data was entirely gathered from questionnaires as the instrument for this research, so as to determine the effects of machine learning and artificial intelligence in intrusion detection and crime prevention; case of air Zimbabwe. The researcher used questionnaire, observation and personal interview results as the source of data referred to in this analysis.

4.1 Questionnaire Response rate

A crucial indicator that shows the percentage of participants who finished and returned the questionnaire in relation to the total number of people asked to participate is the questionnaire's response rate gaining knowledge. In the context of the research on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe, understanding the response rate is essential for assessing the reliability and validity of the collected data.

For this study, the expected response rate will be influenced by several factors, including:

Participant Engagement: The level of interest and relevance of the research topic to the participants, including security personnel, IT specialists, and management, will significantly impact their willingness to respond.

Survey Design: The clarity, length, and format of the questionnaire can affect how likely participants are to complete it. A well-structured questionnaire that is concise and easy to understand is expected to yield a higher response rate.

Follow-Up Reminders: Implementing follow-up communications, such as reminder emails or messages, can help improve the response rate by encouraging participants who may have initially overlooked the questionnaire.

Target Response Rate: In similar studies within organizational contexts, response rates of 60% to 80% are often considered acceptable and achievable (Dillman et al., 2014). For this research, aiming for a response rate of around 70% is realistic, given the targeted sampling of key stakeholders at Air Zimbabwe. This will ensure a robust dataset that reflects diverse perspectives on the implementation of ML and AI technologies in security operations.

Data Collection and Analysis: Once the questionnaires are distributed, the response rate will be calculated as follows:

Response Rate = (Number of Completed Questionnaires) / (Total Number of Questionnaires Distributed) X 100

For this research number of questionnaires distributed were 20 and number of completed questionnaires were 18. So the response rate is

(18/20) x 100 = 90%

The response rate is 90%

Monitoring and reporting the response rate will be crucial for evaluating the effectiveness of the data collection process in this study. A high response rate will enhance the credibility of the findings, providing valuable insights into the effects of ML and AI in intrusion detection and crime prevention at Air Zimbabwe.

4.2.0 Demographic data of respondents

The demographic profile of respondents in the study on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe will provide essential context for understanding the perspectives gathered. This demographic information will help to analyse the diversity of experiences and insights from various stakeholder groups within the organization.

4.2.1 Distribution of Respondents by Gender

The research established the distribution of gender and the outcomes of this study indicated that 66.67 percent of the Males made up the sampled population and 33.33 percent of the population who responded were females.

		Frequency	Percent	Valid Percent	Cumulative Percent
Gender	Male	12	66.67	66.67	66.67
	Female	6	33.33	33.33	100.0
	Total	18		100.0	

Table 4.1 Distribution of respondents by gender

4.2.2 Distribution of Respondents by Age

The participants in this study were asked to rate their age in one of the four categories listed below, ranging from 18 to older. The following were the results:

		Frequency	Percent	Valid Percent	Cumulative Percent
AGE	18-24	5	27.78	27.78	27.78
	25-30	4	22.22	22.22	50.00
	31-35	3	16.67	16.67	66.67
	36+	6	33.33	33.33	100
	Total	18	100	100	

Table 4.2 Distribution of Respondents by Age

The results provided that 27.78% of the respondents were within the age bracket of 18– 24 years. Those who were in the age brackets of between 23 – 30 years were represented by 22.22% and 31 – 35 years were 16.67% and 36 and above were represented by 33.33%.

4.2.3 Distribution of Respondents by Work Experience

The length of continuous service by the respondents were as follows; 6 respondents had been working for the period less than 1 year contributing to 11.11%, 27.78% had been working for the period of 1-3 years, 33,33% of those surveyed had been employed by the duration of 4-6 years. Those who had worked for the duration of 7 and above years were represented by 33.33% and 7.41% represented those who worked for the period of 21 years and above. This indicates that 67% of employees have worked for the organisation for more

than five years and are well-versed in how the organisation runs. These findings indicate that the employees under investigation had worked at the airline industry long enough to comprehend the operations of the institution.

4.2.4 Distribution of respondents by occupation/position

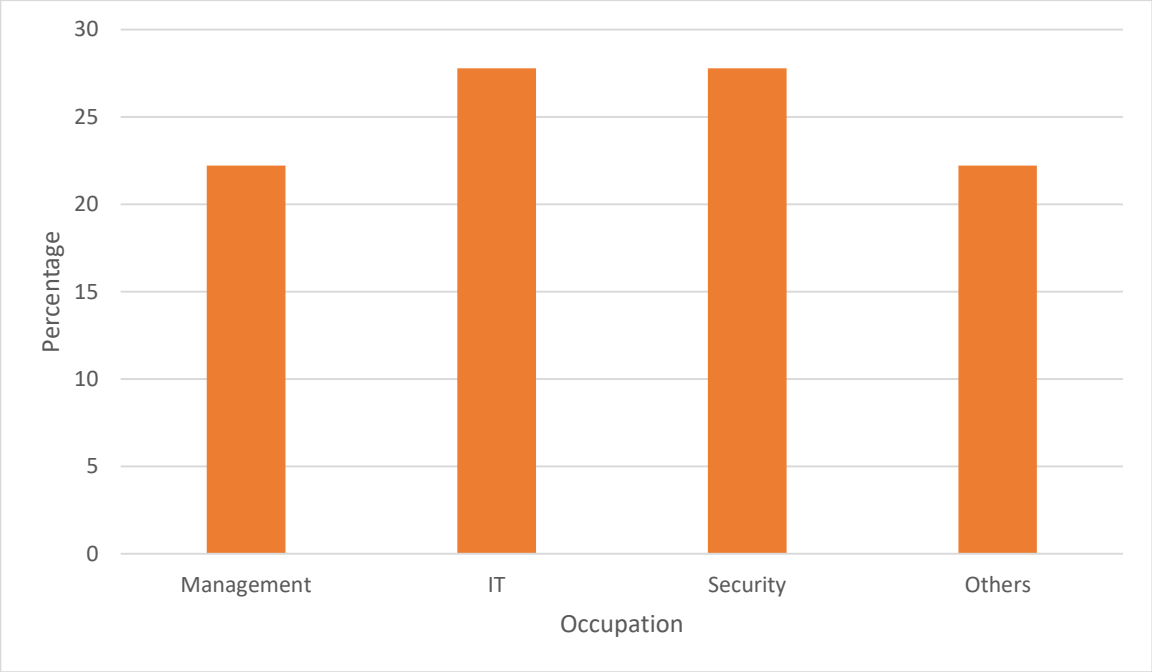


Figure 4.1 Distribution of respondents by occupation/position

When asked which positions they held in their departments, the respondents gave the following answers: 22.22 percent said they were in management, 27.78 percent said they were in security, 27.78 percent said they were in IT, and 22.22 percent said they were others. Since this study addressed all viewpoints, the data that the respondents supplied was sufficient for the investigation.

4.2.5 Distribution of Respondents by Experience in ML and AI

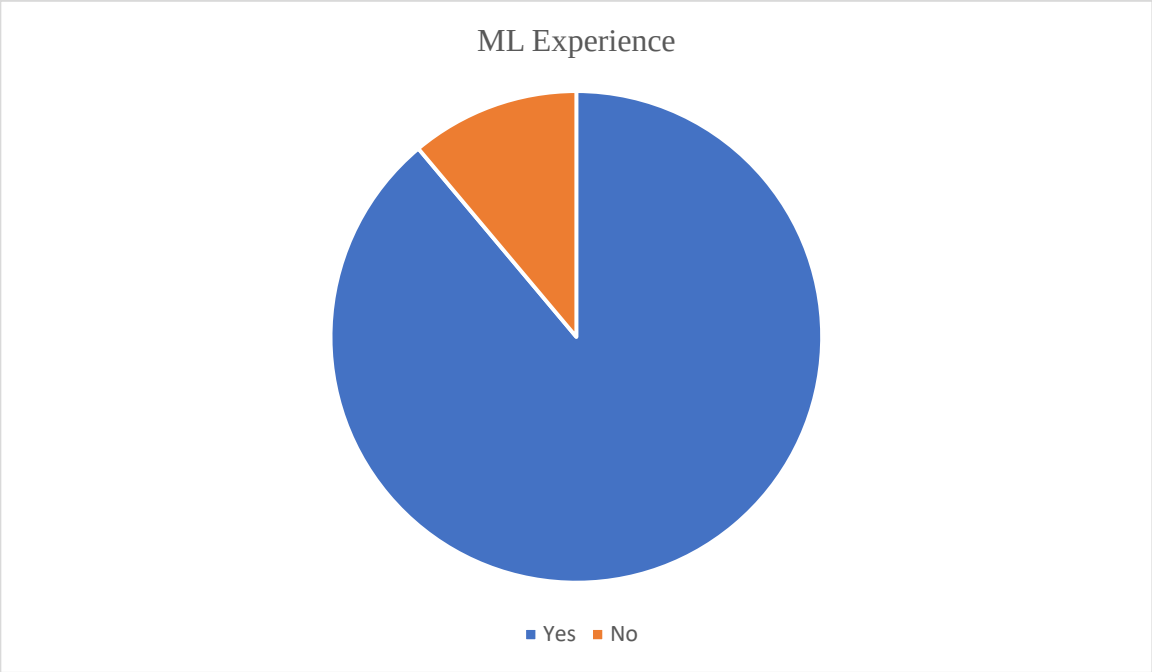


Figure 4.2 Distribution of respondents by knowledge in ML and AI

From the above chart 88.89 percent were participants who have ideas in ML and AI and 11.11 percent were participants have no idea in ML and AI. Therefore, the majority of participants have an idea on what being meant by ML and AI. They referred ML and AI as strategic functions that work to improve the organization's security and intrusion detection.

4.3 Security technologies currently in use at Air Zimbabwe for Intrusion detection

The results and findings from questionnaires and interviews showed that many respondents stated that there are security technologies that are being practiced at Air Zimbabwe. The security technologies include walk through metal detector, access control systems and xray screening.

Walk through metal detector	Access control system	Xray screening	None
77.78%	77.78%	44.44	11.11%

Table 4.3 security technologies currently practiced at Air Zimbabwe

From the figure 4.4 above 77.78% were respondents stated that walking through metal detector is security technology being practiced at Air Zimbabwe and 22,22% stated that there is no walk-through metal detector technology. On Access control system 77.78 stated that it is available and 22.22% stated that it is not available. 44.44% stated that Xray screening technology is available at Air Zimbabwe and 55.56% said there is no Xray screening technology. 11.11% stated that there are none security technologies currently at Air Zimbabwe.

4.4 Benefits of ML and AI in Intrusion detection

The research sought to establish to what an extent the organisation is benefiting from ML and AI in intrusion detection. The findings of this study are detailed below.

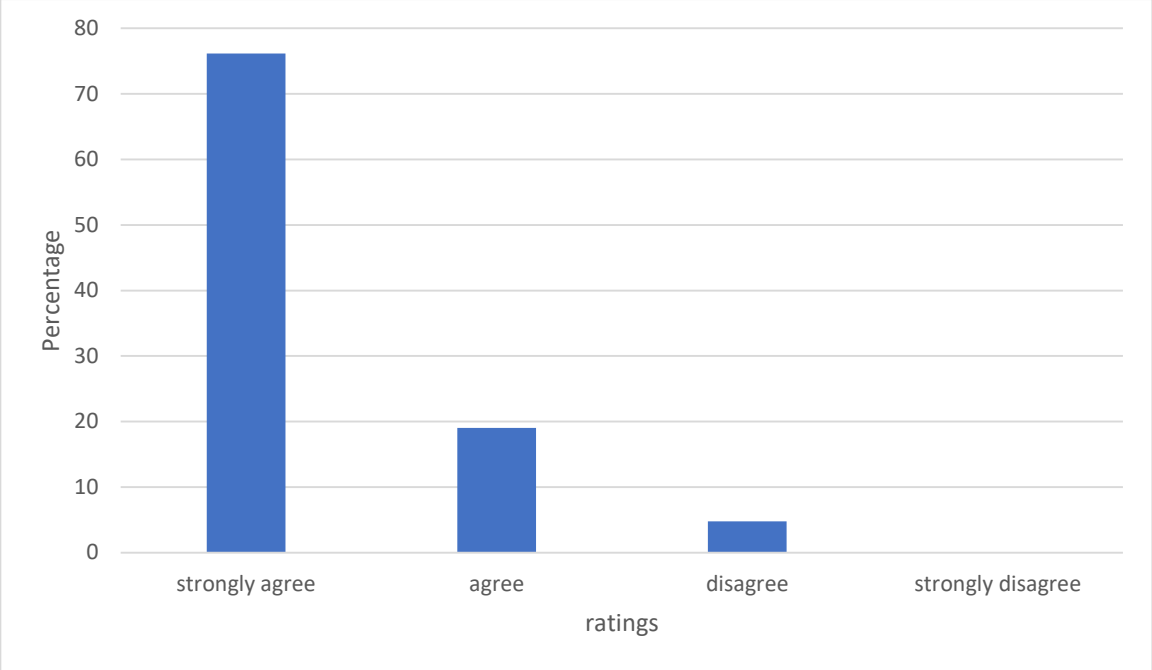


Figure 4.3 of ML and AI in intrusion detection

4.4.1 Improve detection rates

The results of the study revealed that 66.67% agreed that if ML and AI implemented at Air Zimbabwe it will improve the detection rates of intrusion detection at Air Zimbabwe. They reported that through ML and AI security may improve and lead to fast detection of intrusion. Only 33.33% disagreed that ML and AI can improve detection rates of intrusion. They reported that ML and AI can have other benefits other than improve detection which were listed below.

4.4.2 Response Rate Faster

The study shows that 57.14 % of the respondents strongly agreed that ML and AI can leads to faster response rate of intrusion detection for the organization. They emphasized that ML and AI lead to the faster response of intrusion detection and can help to improve security at Air Zimbabwe.

4.4.3 Reduce False Positives

Of the respondents 85% supported that ML and AI involved enables the organization to reduce false positive in intrusion. They reported that ML and AI my help the organization to have true detection of intrusion therefore it can reduce false detection that is false positives or false negative detection of intrusion. Only 15 % were not in support that ML and AI can reduce false positives.

4.4.4 Enhance Predictive Capabilities

70% of the respondents were agreed that ML and AI promote enhance predictive capabilities to the organization and lead to the improvement of the intrusion detection at Air Zimbabwe. Of the 30% respondents there did not agree that ML and AI may promote enhance predictive and capabilities.

4.5.0 Barriers to the effective implementation ML and AI

The study's conclusions demonstrated that there were numerous obstacles to Air Zimbabwe's successful adoption of ML and AI.The research sought to establish to what an extent the following barriers to the effective implementation of ML and AI are. The findings of this study are detailed below.

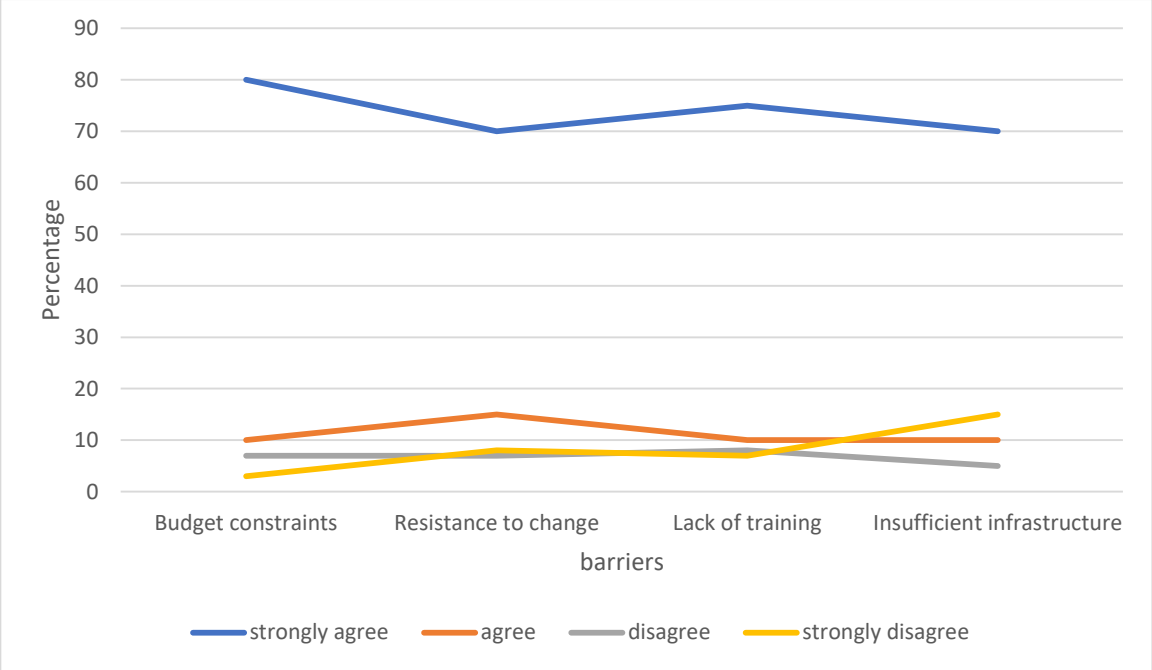


Figure 4.4 barriers to effect of implementation of ML and AI

4.5.1 Budget constraints

From the figure 4.4 above 90% of the respondents agreed that the implementation of ML and AI was negatively affected by Budget constraints. Thet viewed that the company have no enough funds for the implementation of ML and AI since the technology is a bit expensive to implement. Some respondents further stated that Air Zimbabwe is struggling in terms of funds so it will be difficult for them to implement ML and AI in terms of their budget. Only 10% disagree with this view that budget constraints is a barrier to effective implementation of ML and AI at Air Zimbabwe. The respondents reported that Air Zimbabwe can have funds to implement ML and AI.

4.5.2 Resistance to change

Figure 4.4 above shows that 85% of the participants were in support that resistance to change at Air Zimbabwe affected the implementation of ML and AI. They emphasized that many people resist to change and they are not adapted to change. They only want and stick to their traditional way of doing things and they resist to the change of technology. What they think is that the way the used to do is the only way to solve problems not knowing that new technologies can make a way easier. That's what many respondents said. The respondents stated that the airline did not want to change in terms of technology they use they believe that the technologies they use are good enough. Only 15% were not supported that resistance to change is a barrier to effective implementation of ML and AI. They stated that they are willing to change they ways but the budget did not allow them to do so.

4.5.3 Lack of training

From the figure above 85% of the respondents stated that lack of training is a barrier to effective implementation of ML and AI at Air Zimbabwe to a greater extend. They stated that people lack training and knowledge on ML and AI, some they don't even know what is ML and AI and some they don't know how it works and how to use it so they need a lot of training in order for them to implement it or to use it. So due to lack of training they end up don't know how it is or how to use it. However, 15% did not support that lack of training can be a barrier to effective implementation of ML and AI.

4.5.4 Insufficient infrastructure

From the figure 4.4 above it was noted that 80% of the participants reported and supported that the implementation of ML and AI at Air Zimbabwe was influenced by insufficient infrastructure and 20% were against that Air Zimbabwe have sufficient infrastructure to implement ML and AI. The participants that supported the view revealed that the infrastructure at Air Zimbabwe are not enough to implement ML and AI. They stated that Air Zimbabwe should improve on their infrastructure in order for them to implement ML and AI. Some were stated that their computers are out to date and their processing memory

do not support ML and AI and some were mentioned that the WIFI speed and network is weak to support ML and AI.

4.6 Effectiveness of ML and AI in intrusion detection

The respondents were asked specific questions on how effective are ML and AI. Each of the questions asked was assigned the following values; 1 greater extent, 2 moderate extent and 3 lesser extent. The analysis of the responses gathered from the conducted interviews is displayed in the figure below.

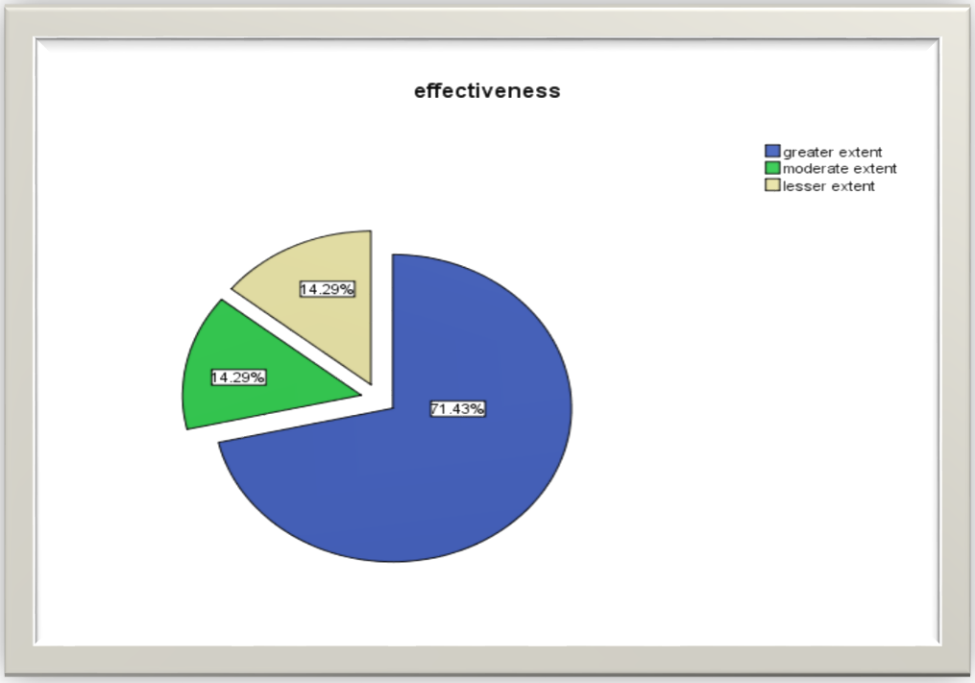


Figure 4.5 Effectiveness of ML and AI

The findings revealed that, 71.43% of the respondents were of the opinion that ML and AI were very effective to a greater extent and that it had enhanced the organizational intrusion detection of the airline industry. Of the respondents, 14.29% revealed that ML and AI are

effective to a moderate extent and the other 14.29% also revealed that ML and A1 are effective to a lesser extent.

CHAPTER V

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.0 Introduction

The findings are summarised in this chapter, and a conclusion is drawn in light of the data. The chapter also emphasises the study's recommendations and ideas for additional research.

5.1 Summary of the Study

The research on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe aims to explore the potential benefits, challenges, and implications of integrating these technologies into the organization's security operations. Given the increasing complexity of security threats in the aviation sector, this study seeks to provide valuable insights that can enhance the effectiveness of security measures at Air Zimbabwe. Objectives of the study were to identify the current state of intrusion detection systems (IDS) used by Air Zimbabwe, to determine the impact of artificial intelligence driven analytics on crime prevention, to identify the challenges and barriers faced by Air Zimbabwe in adopting ML and AI technologies for intrusion detection, to prevention, crime and detect intrusion using ML and AI and to identify the importance of intrusion detection at air Zimbabwe. The study employs a qualitative research design, utilizing semi-structured interviews and document analysis as the primary data collection methods. A purposive sampling approach will be used to select participants who have relevant expertise and experience in security operations. Thematic analysis will be applied to identify patterns and themes within the qualitative data. The research is expected to yield comprehensive insights into the current state of security practices at Air Zimbabwe and the potential impacts of ML and AI technologies. By addressing the identified challenges and barriers, the study aims to provide evidence-based recommendations that could facilitate the successful integration of these technologies into the organization's security framework. This study is significant in

its contribution to the understanding of how advanced technologies can enhance aviation security, particularly in the context of a developing country like Zimbabwe. The findings will not only benefit Air Zimbabwe but also offer valuable lessons for other organizations facing similar challenges in adopting ML and AI for security purposes. In conclusion, the research aims to bridge the gap in the existing literature by providing empirical evidence and practical recommendations for the effective use of ML and AI in intrusion detection and crime prevention, ultimately contributing to safer aviation practices at Air Zimbabwe.

5.2 Summary of major findings

The research on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe yielded several significant findings that contribute to the understanding of how these technologies can enhance security operations. The following key themes emerged from the data collected through interviews and document analysis:

Enhanced Detection Capabilities: Participants reported that ML and AI technologies have the potential to significantly improve intrusion detection capabilities. By analyzing vast amounts of data in real-time, these technologies can identify patterns and anomalies that may indicate security threats, leading to quicker and more accurate responses. Many respondents emphasized that AI-powered systems could reduce false positives compared to traditional security measures.

Stakeholder Perceptions and Readiness: The study revealed a generally positive perception among stakeholders regarding the integration of ML and AI into security practices. However, there was also a recognition of the need for further training and education to ensure effective implementation. Many participants expressed enthusiasm

about the potential of these technologies but highlighted concerns about their understanding and familiarity with ML and AI applications.

Barriers to Implementation: Several barriers to the adoption of ML and AI technologies were identified, including:

Financial Constraints: Limited budgets for technology upgrades and training presented significant challenges.

Technological Infrastructure: The existing technological infrastructure at Air Zimbabwe was deemed insufficient to support advanced ML and AI systems, necessitating further investment.

Organizational Culture: Resistance to change and a lack of awareness about the benefits of ML and AI among some staff members were cited as obstacles to successful implementation.

Lack of training: There is lack of training to the staff on how to implement ML and AI or how to use it

Importance of Data Quality: The quality of data used in ML and AI applications emerged as a critical factor for success. Participants noted that accurate, comprehensive, and timely data is essential for training effective models. Concerns were raised about the current data collection processes and the need for improvements to ensure reliability in AI-driven security systems.

Recommendations for Implementation: Based on the findings, the study provided several recommendations for Air Zimbabwe to enhance the implementation of ML and AI in their security operations:

Investment in Training: Implement comprehensive training programs for staff to build knowledge and skills in using ML and AI technologies.

Upgrading Infrastructure: Allocate resources to improve technological infrastructure, ensuring it can support advanced security systems.

Promoting a Culture of Innovation: Foster an organizational culture that embraces technological innovation and encourages staff to engage with new tools and methodologies.

In summary, the research findings indicate that while ML and AI hold considerable promise for enhancing security at Air Zimbabwe, successful implementation will require addressing financial, infrastructural, and cultural barriers. By focusing on training, infrastructure improvements, and promoting an innovative mindset, Air Zimbabwe can leverage these technologies to strengthen its intrusion detection and crime prevention efforts.

5.2.1 Causes of Intrusion at Air Zimbabwe

The investigation into the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe reveals several underlying causes of security intrusions. Understanding these causes is essential for developing effective preventive measures and enhancing security protocols. The following key factors contribute to intrusions at Air Zimbabwe:

Insider Threats: Insider threats pose a significant risk to security at Air Zimbabwe. Employees or contractors with access to sensitive information and systems may exploit their positions for malicious purposes, either intentionally or through negligence. Factors such as employee dissatisfaction, lack of oversight, and inadequate security training can exacerbate this risk.

Physical Security Breaches: Physical breaches, such as unauthorized access to secure areas of the airport or aircraft, can lead to significant security incidents. These breaches may result from inadequate physical barriers, insufficient monitoring of access points, or lapses in protocol adherence by staff. The airport's extensive infrastructure presents challenges in maintaining comprehensive physical security.

Cybersecurity Vulnerabilities: As Air Zimbabwe increasingly relies on digital systems for operations, vulnerabilities in cybersecurity can lead to intrusions. Cyberattacks, such as phishing, malware deployment, or denial-of-service attacks, can compromise sensitive data and disrupt services. The effectiveness of existing cybersecurity measures is critical in mitigating these threats.

Lack of Awareness and Training: A lack of awareness and training among employees regarding security protocols and potential threats can contribute to intrusions. Employees may inadvertently facilitate breaches by not recognizing suspicious activities or failing to follow security procedures. Regular training sessions and awareness campaigns are essential to address this issue.

External Threats: External threats, including organized crime, terrorism, and vandalism, also contribute to security challenges at Air Zimbabwe. These threats often exploit vulnerabilities in security systems and require comprehensive strategies that integrate technology and human vigilance to effectively counteract.

Insufficient Use of Technology: While there is potential for ML and AI to enhance security measures, insufficient integration or outdated technology can hinder effective intrusion detection. The lack of advanced monitoring systems and analytics capabilities may result in missed opportunities to identify and respond to threats proactively.

Identifying the causes of intrusions at Air Zimbabwe is crucial for developing targeted strategies to enhance security measures. Addressing insider threats, improving physical security, bolstering cybersecurity defenses, increasing employee awareness and training, and leveraging advanced technologies are essential steps in mitigating the risks associated with intrusions. By understanding these causes, Air Zimbabwe can better position itself to

implement effective ML and AI solutions for improved intrusion detection and crime prevention.

5.2.2 Ways of Preventing crime and intrusion at Air Zimbabwe

To effectively prevent crime and intrusion at Air Zimbabwe, a multifaceted approach that incorporates advanced technologies, staff training, and robust security protocols is essential. The following strategies can enhance the organization's security framework, particularly through the integration of Machine Learning (ML) and Artificial Intelligence (AI):

AI-Powered Surveillance Cameras: Deploy AI-enabled cameras that can analyze video feeds in real-time to detect unusual behaviors or unauthorized access. These systems can alert security personnel to potential threats immediately.

Facial Recognition Technology: Utilize facial recognition systems for identifying individuals entering secure areas, enhancing access control, and preventing unauthorized entry.

Enhanced Cybersecurity Measures, Regular Security Audits: Conduct comprehensive cybersecurity audits to identify vulnerabilities in digital systems and implement necessary updates and security patches.

Intrusion Detection Systems (IDS): Implement ML-based IDS that can analyze network traffic patterns and detect anomalies indicative of cyber intrusions, enabling proactive responses to potential threats.

Employee Training and Awareness Programs, Regular Training Sessions: Provide continuous training for all employees on security protocols, threat recognition, and incident reporting to foster a security-conscious culture.

Awareness Campaigns: Launch campaigns that inform staff about the importance of security practices and the role of technologies like ML and AI in enhancing security measures.

Strengthening Physical Security Measures, Access Control Systems: Implement advanced access control systems that utilize biometric authentication (e.g., fingerprint or iris scanning) to restrict access to sensitive areas.

Security Personnel Deployment: Increase the presence of trained security personnel in critical areas, ensuring they are equipped with the tools and knowledge to respond effectively to security incidents.

Data Analytics for Risk Assessment, Predictive Analytics: Use ML algorithms to analyze historical crime data and identify patterns that can help predict potential security threats. This information can guide resource allocation and preventive measures.

Real-Time Data Monitoring: Implement systems that monitor data from various sources (e.g., social media, incident reports) to identify potential threats before they materialize.

Collaboration with Law Enforcement, Partnerships with Local Authorities: Establish collaborative relationships with local law enforcement agencies to share intelligence and resources, enhancing overall security efforts.

Joint Training Exercises: Conduct joint training exercises with law enforcement to ensure a coordinated response to potential threats or incidents.

Regular Review and Improvement of Security Protocols, Continuous Improvement: Regularly review and update security protocols to incorporate new technologies and address emerging threats.

Feedback Mechanism: Establish a feedback mechanism for employees to report security concerns or suggest improvements, fostering a proactive security culture.

By implementing these strategies, Air Zimbabwe can significantly enhance its ability to prevent crime and intrusion. The integration of ML and AI technologies plays a pivotal role in modernizing security practices, enabling more effective and responsive security measures. A comprehensive approach that combines technology, training, and collaboration will create a safer environment for both employees and passengers, ultimately strengthening the overall security framework of the organization.

5.3 Conclusion

The research on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe has highlighted the significant potential of these technologies to enhance security operations within the organization. The findings indicate that ML and AI can improve detection capabilities, reduce response times, and provide valuable insights into emerging security threats. By leveraging advanced analytics and real-time monitoring, Air Zimbabwe can proactively address potential intrusions and create a safer environment for both staff and passengers. However, the study also identified several challenges that must be addressed to successfully integrate these technologies. Barriers such as financial constraints, insufficient technological infrastructure, and the need for enhanced employee training are critical factors that could impede the effective implementation of ML and AI solutions. Additionally, fostering a culture of security awareness and encouraging collaboration among stakeholders are essential for maximizing the benefits of advanced technologies. To achieve the desired outcomes, Air Zimbabwe should focus on strategic investments in technology and training, along with regular assessments of security protocols. By prioritizing these areas, the organization can enhance its resilience against intrusions and crimes, ensuring a robust security framework that adapts to evolving threats. In summary, this research contributes valuable insights into the intersection of technology and security in the aviation sector, particularly within the context of a developing country like Zimbabwe. The recommendations provided aim to guide Air Zimbabwe in its efforts to implement ML and

AI effectively, ultimately leading to improved intrusion detection and crime prevention strategies. By embracing these technologies, Air Zimbabwe can position itself as a leader in aviation security, enhancing its operational efficiency and safeguarding its stakeholders.

5.4 Recommendations

Based on the findings of the research on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe, the following recommendations are proposed to enhance security operations:

Invest in Advanced Technology

Upgrade Infrastructure: Allocate resources for upgrading technological infrastructure to support the integration of ML and AI systems. This includes investing in high-quality surveillance cameras, access control systems, and cybersecurity tools.

Implement AI-Powered Solutions: Explore and adopt AI-driven technologies for real-time data analysis and threat detection, such as predictive analytics and automated monitoring systems.

Enhance Employee Training and Awareness

Comprehensive Training Programs: Develop and implement regular training sessions focused on ML and AI technologies, security protocols, and threat recognition to ensure all employees are well-prepared to utilize new tools effectively.

Awareness Campaigns: Launch campaigns to promote security awareness among staff, emphasizing the importance of vigilance and adherence to security protocols in preventing intrusions.

Foster a Security-First Culture

Encourage Reporting: Create a culture where employees feel empowered to report suspicious activities or security concerns without fear of retribution. Implement an anonymous reporting system to facilitate this.

Leadership Engagement: Involve management in promoting security initiatives and demonstrating commitment to a security-first approach within the organization.

Collaborate with Law Enforcement and Experts

Partnerships with Law Enforcement: Strengthen collaborations with local law enforcement agencies to share intelligence, resources, and best practices for enhancing security measures.

Engage Experts: Consult with cybersecurity and security technology experts to assess current practices and recommend tailored ML and AI solutions appropriate for Air Zimbabwe's operational context.

Conduct Regular Security Assessments

Ongoing Risk Assessments: Implement regular security audits and risk assessments to identify vulnerabilities in current practices and technologies. Use findings to inform improvements and adaptations to security strategies.

Review and Update Protocols: Establish a systematic approach for reviewing and updating security protocols to adapt to new threats and technological advancements.

Utilize Data Analytics for Decision-Making

Leverage Predictive Analytics: Use data analytics tools to analyze historical crime data and predict potential intrusion patterns, enabling proactive measures to be implemented.

Monitor Data Quality: Ensure that data used for ML and AI applications is accurate and comprehensive to maximize the effectiveness of security systems.

Pilot Programs for New Technologies

Conduct Pilot Initiatives: Before full-scale implementation, run pilot programs for new ML and AI technologies to evaluate their effectiveness and gather feedback from users. This approach allows for adjustments based on real-world experiences.

By implementing these recommendations, Air Zimbabwe can effectively enhance its intrusion detection and crime prevention capabilities through the strategic use of ML and AI technologies. A comprehensive approach that combines technology, training, collaboration, and continuous improvement will create a robust security framework, ultimately safeguarding the organization and its stakeholders against evolving security threats

5.5 Areas for further research

Building on the findings of the research on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe, several areas for further research can be identified. These areas aim to deepen the understanding of technology integration in security practices and address gaps in the current knowledge base:

Longitudinal Studies on Technology Impact

Effectiveness Over Time: Conduct longitudinal studies to assess the long-term effectiveness of ML and AI technologies in security operations. This research could focus on how these technologies adapt to evolving threats and their sustained impact on crime prevention and detection rates.

Comparative Studies Across Sectors

Cross-Industry Analysis: Explore comparative studies between the aviation sector and other industries (such as retail, banking, or public safety) that have successfully implemented ML and AI for intrusion detection and crime prevention. This could provide insights into best practices and lessons learned that can be adapted for Air Zimbabwe.

User Experience and Acceptance

Stakeholder Engagement: Investigate the user experience and acceptance of ML and AI technologies among different stakeholders at Air Zimbabwe. Understanding the perceptions and challenges faced by staff in using these systems can inform better training programs and technology designs.

Ethical Implications of AI in Security

Ethical Considerations: Examine the ethical implications of using AI and ML in security contexts, particularly concerning privacy concerns, data management, and the potential for biases in decision-making algorithms. Research could focus on establishing frameworks for ethical AI use in surveillance and security.

Integration of Emerging Technologies

Synergistic Technologies: Research the potential integration of emerging technologies, such as blockchain or the Internet of Things (IoT), with ML and AI in enhancing security measures. Studying how these technologies can work together could lead to innovative solutions for intrusion detection.

Impact of External Factors

Influence of External Threats: Analyze how external factors, such as geopolitical events, economic conditions, or public health crises, influence the effectiveness of ML and AI technologies in security operations. Understanding these dynamics can aid in developing more resilient security strategies.

Training and Development Models

Effective Training Approaches: Investigate different training and development models for employees regarding ML and AI technologies in security contexts. Research could focus on identifying the most effective methods for knowledge transfer and skill acquisition.

Cost-Benefit Analysis of Technology Implementation

Economic Impact Assessment: Conduct comprehensive cost-benefit analyses of implementing ML and AI technologies in security measures at Air Zimbabwe. This research could provide valuable insights into the economic viability and return on investment of such technologies.

These areas for further research are essential for advancing the knowledge and application of ML and AI in intrusion detection and crime prevention. By exploring these topics, researchers can contribute to developing more effective, ethical, and sustainable security practices that can be adapted not only at Air Zimbabwe but across various sectors facing similar challenges.

References

Bertino, E. & Islam, N. (2017). 'Cybersecurity and the Role of Artificial Intelligence'. IEEE Security & Privacy, 15(5), pp. 79-83.

Patel, A., Vora, S. & Shah, D. (2019). 'Anomaly Detection in Cyber Security Using Machine Learning: A Review'. International Journal of Computer Applications, 975, pp. 18-24.

Chand, S. & Sharma, S. (2020). 'Predictive Analytics for Crime Prevention: A Comprehensive Review'. Journal of Police Science, 5(2), pp. 45-58.

Kvale, S. & Brinkmann, S. (2015). Interviews: Learning the Craft of Qualitative Research Interviewing. 3rd ed. Thousand Oaks, CA: SAGE Publications.

Alazab, M., Venkatraman, S., & Alazab, M. (2020). 'Cybersecurity in Aviation: A Review of Current Threats and Solutions'. Journal of Aerospace Information Systems, 17(1), pp. 34-45.

Kumar, A., Singh, S., & Singh, R. (2021). 'Machine Learning Techniques for Cyber Security: A Survey'. Journal of Network and Computer Applications, 179, pp. 102956.

Sari, Y., Alzubaidi, A., & Riza, S. (2022). 'Deep Learning in Cybersecurity: A Comprehensive Review'. Computers & Security, 113, pp. 102558.

Zhang, Y., Wu, J., & Zhao, X. (2023). 'Predictive Analytics in Crime Prevention: Techniques and Applications'. International Journal of Information Management, 63, pp. 102423.

Booth, A., Sutton, A. & Papaioannou, D. (2016). Systematic Approaches to a Successful Literature Review. 2nd ed. London: SAGE Publications.

Fink, A. (2014). Conducting Research Literature Reviews: From the Internet to Paper. 4th ed. Thousand Oaks, CA: SAGE Publications.

Machi, L.A. & McEvoy, B.T. (2016). The Literature Review: Six Steps to Success. 3rd ed. Thousand Oaks, CA: Corwin Press.

Webster, J. & Watson, R.T. (2002). 'Analyzing the Relationship between Web Site Quality and E-Commerce Success'. Communications of the Association for Information Systems, 9(1), pp. 1-28.

Chandola, V., Banerjee, A., & Kumar, V. (2009). 'Anomaly Detection: A Survey'. ACM Computing Surveys, 41(3), pp. 1-58.

Davis, F.D. (1989). 'Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology'. MIS Quarterly, 13(3), pp. 319-340.

NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity. [online] Available at: https://www.nist.gov/cyberframework [Accessed 22 Sep. 2024].

Raiffa, H. & Schlaifer, R. (1961). Applied Statistical Decision Theory. Cambridge, MA: Harvard University Press.

Shmueli, G. & Lichtendahl, K.C. (2016). 'Practical Time Series Forecasting: A Hands-On Guide'. [online] Available at: http://www.statisticalforecasting.com [Accessed 22 Sep. 2024].

Bowen, G.A. (2009). 'Document Analysis as a Qualitative Research Method'. Qualitative Research Journal, 9(2), pp. 27-40.

Braun, V. & Clarke, V. (2019). 'Using Thematic Analysis in Psychology'. Qualitative Research in Psychology, 3(2), pp. 77-101.

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

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

Kvale, S. & Brinkmann, S. (2020). Interviews: Learning the Craft of Qualitative Research Interviewing. 3rd ed. Thousand Oaks, CA: SAGE Publications.

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

Field, A. (2019). Discovering Statistics Using IBM SPSS Statistics. 5th ed. London: SAGE Publications.

Palinkas, L.A., Horwitz, S.M., Green, C.A., Wisdom, J.P., Duan, N. & Hoagwood, K. (2019). 'Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research'. Administration and Policy in Mental Health and Mental Health Services Research, 42(5), pp. 533-544.

Dillman, D.A., Smyth, J.D. & Christian, L.M. (2014). *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*. 4th ed. Hoboken, NJ: Wiley.

air zimbabwe
(PRIVATE) LIMITED

P.O Box AP1, R.G. Mugabe International Airport, Harare, Zimbabwe. Tel: 575111, Fax: 263-4-575468

25th November 2024

Mr. Takawira T. Gutu
Air Zimbabwe (Pvt) Ltd
P.O. Box AP1
Harare

Dear Takawira

RE: REQUEST TO CONDUCT RESEARCH

This letter serves to confirm that your application to conduct the above research has been approved under the following conditions;

1. That you ensure that there is no undue interference with normal operations of duty to your respondents as you administer your questionnaires

2. That you submit to the airline's HR department a copy of your final research project for us to extract any recommendations you may have proffered.

   Air Zimbabwe promotes a culture of continual learning and therefore wishes you the best in your research project.

Yours sincerely,
For and on behalf of **AIR ZIMBABWE (PVT) LIMITED**

J. Benhura
ACTING MANAGER – HUMAN RESOURCES

AIR ZIMBABWE (PVT.) LTD.
HUMAN RESOURCES DPT
25 NOV 2024
P.O. BOX AP 1
HARARE AIRPORT
TEL: 575111

Cc HR Admin Office
Acting Manager CQSS
Head AVSEC

BINDURA UNIVERSITY OF SCIENCE EDUCATION

Private Bag 1020
BINDURA, Zimbabwe
Tel: 066271 – 7127, 7620,7615

INTELLIGENCE AND SECURITY STUDIES

01 November 2024

AIR ZIMBABWE PRIVATE LIMTED
PRIVATE BAG API
RGMI

HARARE
0242 575111

RE: REQUEST FOR DATA COLLECTION

Please may you assist our student Takawira Tedius Gutu (B220277B) carry his research in your organization on his topic on **"EFFECTS OF MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE IN INTRUSION DETECTION AND CRIME PREVENTION IN ZIMBABWE. A CASE STUDY OF AIR ZIMBABWE, HARARE".** He is our 3.1 student at Bindura University of Science Education in the Department of Intelligence and Security Studies.

Your assistance to our student will be greatly appreciated.

Regards

RECEIVED
Chairman, Intelligence & Security Studies Department
Date: 01/11/24

.....
Ms L. CHINYOKA
Chairperson

Questionnaire for Research on the Effects of Machine Learning and Artificial Intelligence in Intrusion Detection and Crime Prevention at Air Zimbabwe

Introduction

My name is Takawira Tedius Gutu Reg B220277, I am a student at Bindura University of Science Education, pursing a degree in Police and Security Studies. I am conducting a survey on **"Effects of Machine Learning and Artificial Intelligence in Intrusion Detection and Crime Prevention"** This questionnaire aims to gather insights on the effects of Machine Learning (ML) and Artificial Intelligence (AI) in intrusion detection and crime prevention at Air Zimbabwe. Your responses will provide valuable information that will contribute to understanding how these technologies can enhance security measures. All responses will be kept confidential and the survey should take approximately 15 to 20 minutes to complete. Your participation in this study is voluntary, and you can withdraw at any time. If you have any questions or concerns about the study, please do not hesitate to contact the researcher.

Instruction for completing Questionnaire

1. Please answer each question honestly and to the best of your ability
2. Please answer all questions in a single sitting as this help us ensure that your responses consistent and accurate
3. Once you have completed the questionnaire please return to the researcher at the designated location

Section 1: Demographic Information

Gender **M** ☐ **F** ☐

Age

18-24 ☐ 26-30 ☐ 31-35 ☐ 35 and above ☐

Position/Role in the Organization:

Security Personnel ☐

IT Specialist ☐

Management ☐

Other (please specify): _____

Years of Experience in the Organization:

Less than 1 year ☐

1-3 years ☐

4-6 years ☐

7 years or more ☐

Previous Experience with ML and AI Technologies:

Yes ☐

No ☐

Section 2: Current Security Practices

How would you rate the effectiveness of current intrusion detection systems at Air Zimbabwe?

(1 = Very Ineffective, 5 = Very Effective)

1 ☐

2 ☐

3 ☐

4 ☐

5 ☐

What types of security technologies are currently in use at Air Zimbabwe?

(Select all that apply)

CCTV Surveillance ☐

Access Control Systems ☐

Alarm Systems ☐

None ☐

Other (please specify): _____

Section 3: Perceptions of ML and AI

To what extent do you believe that ML and AI can improve intrusion detection systems?

(1 = Not at all, 5 = Very Much)

1 ☐

2 ☐

3 ☐

4 ☐

5 ☐

What benefits do you associate with the implementation of ML and AI in security?

(Select all that apply)

Improved Detection Rates ☐

Faster Response Times ☐

Reduced False Positives ☐

Enhanced Predictive Capabilities ☐

Other (please specify): _____

What concerns do you have regarding the use of ML and AI in security operations?

(Select all that apply)

Data Privacy Issues ☐

High Implementation Costs ☐

Lack of Expertise ☐

Potential for System Failure ☐

Other (please specify): _____

Section 4: Organizational Readiness

How prepared do you feel Air Zimbabwe is to adopt ML and AI technologies for security purposes?

(1 = Not Prepared, 5 = Very Prepared)

1 ☐

2 ☐

3 ☐

4 ☐

5 ☐

What barriers do you perceive in the implementation of ML and AI technologies at Air Zimbabwe?

(Select all that apply)

Budget Constraints ☐

Resistance to Change ☐

Lack of Training ☐

Insufficient Infrastructure ☐

Other (please specify): _____

Section 5: Additional Comments

Please provide any additional comments or suggestions regarding the use of ML and AI in security at Air Zimbabwe:

……
……
……
……

Conclusion

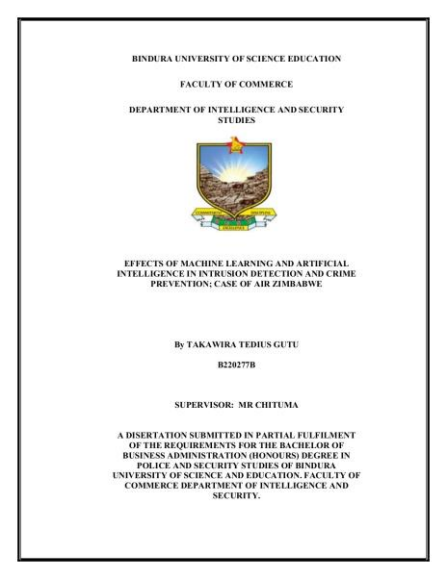
Thank you for your participation in this survey. Your responses are valuable and will contribute to enhancing security measures at Air Zimbabwe.

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Takawira Gutu
Assignment title:	BS400
Submission title:	DISSERTATION_CHAPTER_1__2__3_4_and_5_1__2_ (1).docx
File name:	DISSERTATION_CHAPTER_1__2__3_4_and_5_1__2__1_.docx
File size:	2.01M
Page count:	88
Word count:	15,936
Character count:	96,020
Submission date:	11-Jun-2025 11:02AM (UTC+0300)
Submission ID:	2696191455



BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES

EFFECTS OF MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE IN INTRUSION DETECTION AND CRIME PREVENTION; CASE OF AIR ZIMBABWE

By TAKAWIRA TEDIUS GUTU

B220277B

SUPERVISOR: MR CHITUMA

A DISERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE BACHELOR OF BUSINESS ADMINISTRATION (HONOURS) DEGREE IN POLICE AND SECURITY STUDIES OF BINDURA UNIVERSITY OF SCIENCE AND EDUCATION. FACULTY OF COMMERCE DEPARTMENT OF INTELLIGENCE AND SECURITY.