

https://dspace.org/

Artificial Intelligence for Cybersecurity: Governance Insights from Cybersecurity Experts in the Banking Industry in South Africa

Joyisa, Thabani

2025

University of the Witwatersrand, Johannesburg

https://hdl.handle.net/10539/49354

Joyisa, Thabani. (2025). Artificial Intelligence for Cybersecurity: Governance Insights from Cybersecurity Experts in the Banking Industry in South Africa [Master's dissertation, University of the Witwatersrand, Johannesburg]. WIReDSpace. https://hdl.handle.net/10539/49354

Downloaded from a DSpace repository. https://dspace.org/

ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: GOVERNANCE INSIGHTS FROM CYBERSECURITY EXPERTS IN THE BANKING INDUSTRY IN SOUTH AFRICA

by

THABANI JOYISA (1285042)

SUPERVISOR: DR JOHN MANGUNDU, PHD

Research Report

Submitted in partial fulfilment of the requirements for the degree of
Master of Commerce (Information Systems)
in the
School of Business Sciences,
Faculty of Commerce, Law and Management,
University of the Witwatersrand

Date of submission

30 June 2025

Declaration regarding Plagiarism

I declare that this is my own unaided work and is, to the best of my knowledge and belief, original.

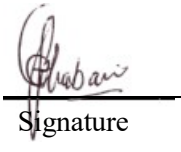
I have read and understood the Senate policy on plagiarism and am aware that plagiarism is the intentional or unintentional "failure to acknowledge the ideas or writing of another" or "presentation of the ideas or writing of another as one's own". In this context "other" means any other person including a student, academic, professional, published author or other resource such as the internet. Failing to acknowledge the use of ideas of others constitutes an important breach of the values and conventions of the academic enterprise.

I am aware that plagiarism offences will be dealt with in terms of Senate policy and may be subject to disciplinary action.

I (full names & surname):	Thabani Joyisa
Student number:	1285042

Declare the following:

1. I understand what plagiarism entails and am aware of the University's policy in this regard.
2. I declare that this assignment is my own, original work. Where someone else's work was used (whether from a printed source, the Internet or any other source) due acknowledgement was given and reference was made according to departmental requirements.
3. I did not copy and paste any information directly from an electronic source (e.g., a web page, electronic journal article or CD ROM) into this document.
4. I did not make use of another student's previous work and submitted it as my own.
5. I did not allow and will not allow anyone to copy my work with the intention of presenting it as his/her own work.



Signature

25 February 2025

Date

DEDICATION

This research report is dedicated to the memory of my late father, **Mbuso Oscar Joyisa**.

Though he did not have the opportunity to complete his secondary education—having made the selfless decision to work and support his family—he instilled in me the value of education, perseverance, and purpose. His unwavering belief in my potential inspired me to pursue my studies with determination and integrity.

I will never forget the joy in his voice when he discovered that one could become a doctor without working in a hospital. It is in his honour that I strive not only to be a master in my field but, one day, to earn the title of "doctor" through a Ph.D.—a dream he helped plant in my heart.

This is for you, *Joyisa Mvubu Thabane*. Your sacrifices were not in vain.

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to all those who supported me throughout the journey of completing this research report.

First and foremost, I extend my sincere appreciation to my supervisor, **Dr. John Mangundu**, for his unwavering guidance, insightful feedback, and academic mentorship. His expertise and encouragement were instrumental in shaping the direction and quality of this study.

I am profoundly grateful to the cybersecurity professionals who participated in this research. Your willingness to share your time, experiences, and insights made this study possible and meaningful. Your contributions have enriched this work beyond measure.

To the University of the Witwatersrand, particularly the School of Business Sciences, thank you for providing a stimulating academic environment and the resources necessary to complete this research.

A special thank you to my employer for generously funding my studies—your investment in my growth has been invaluable. I am also sincerely grateful to my manager, **Christine de Kock**, for her patience and unwavering support throughout this academic pursuit.

Lastly, I am deeply thankful to my family—my wife, **Nomfundo Masikane**, and our children, **Khulubuse** and **Ncebakazi Joyisa**—for their endless love, patience, and encouragement.

Table of Contents

List of Abbreviations and Acronyms vi

ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: GOVERNANCE INSIGHTS FROM CYBERSECURITY EXPERTS IN THE BANKING INDUSTRY IN SOUTH AFRICA 7

ABSTRACT 8

1 INTRODUCTION 9

1.1 BACKGROUND 9

1.2 RESEARCH PROBLEM 11

1.3 AIMS AND OBJECTIVES OF THE RESEARCH 11

1.4 RESEARCH QUESTIONS 12

1.5 STUDY JUSTIFICATION 13

1.6 IMPORTANCE OF THE STUDY 14

1.7 STUDY LIMITATIONS 15

1.8 ETHICS-RELATED MATTERS 16

1.9 CONCLUSION 17

2 LITERATURE REVIEW 19

2.1 INTRODUCTION 19

2.2 REVIEW OF RELATED LITERATURE 19

2.2.1 Global Perspectives on AI for Cybersecurity 22

2.2.2 Sector-Specific Insights and Ethical Considerations 23

2.2.3 Challenges Relating to Ethics and Governance 23

2.2.4 Strategic Models for Cyber Protection 23

2.3 THEORETICAL AND EMPIRICAL THEORY DISCUSSION, CONCEPTUAL MODEL AND RESEARCH PROPOSITIONS 24

2.3.1 The theories underpinning this study. 24

2.3.2 Technology Acceptance Model (TAM) 25

2.3.3 Diffusion of Innovation Theory 25

2.3.4 Institutional Theory 26

2.4 CONCEPTUAL FRAMEWORK OF THE STUDY 27

2.5 CONCLUSION 29

3 RESEARCH METHODOLOGY 30

3.1 INTRODUCTION 30

3.2 RESEARCH PHILOSOPHY (PARADIGM) 30

3.3 RESEARCH DESIGN 31

3.4 STUDY ORGANISATION 32

3.4.1 RESEARCH POPULATION AND SAMPLING 32
3.4.6 Primary Data Collection 34
3.4.7 Data Analysis 36
3.5 ETHICAL CONSIDERATIONS 36
3.6 TRIANGULATION IN A QUALITATIVE STUDY 37
3.7 VALIDATION OF THE INTERVIEW GUIDE 37
3.8 CONCLUSION 38
4 RESULTS 39
4.1 INTRODUCTION 39
4.2 DATA SOURCES 40
4.3 THEMATIC ANALYSIS AND LINK TO RESEARCH QUESTIONS 40
4.3.1 Theme 1: Perceived Benefits of AI for Cybersecurity 40
4.3.2 Theme 2: Challenges in AI Adoption 42
4.3.3 Theme 3: Regulatory and Ethical Concerns 44
4.3.4 Theme 4: Benefits and Ethical Oversight 47
4.3.5 Theme 5: Organisational Readiness and Strategic Alignment 48
4.3.6 Theme 6: Trust and Transparency in AI-Driven Cybersecurity 49
4.3.7 Theme 7: The Role of Human Oversight in AI-Enabled Security 51
4.4 VALIDATION OF RESULTS 52
4.5 CONCLUSION 53
5 DISCUSSION OF FINDINGS 54
5.1 INTRODUCTION 54
5.2 INTERPRETATION OF KEY THEMES 54
5.3 CONCLUSION 58
6 CONCLUSION 59
6.1 SUMMARY OF KEY FINDINGS 59
6.2 RELEVANCE TO RESEARCH OBJECTIVES AND QUESTIONS 60
6.3 THEORITICAL CONTRIBUTION 61
6.4 CONTRIBUTION TO PRACTICE 61
6.5 STUDY LIMITATION 62
6.6 FUTURE RESEARCH 62
6.7 CONCLUDING REFLECTIONS 63
7 REFERENCES 64
APPENDIX A: INTERVIEW PROTOCOL 71

APPENDIX B: ETHICS CERTIFICATE 67
APPENDIX C: CONSENT FORM 68
APPENDIX D: PARTICIPANT SHEET 69
APPENDIX E: LITERATURE REVIEW THEMATICAL ANALYSIS 71

LIST OF FIGURES

Figure 1: Hierarchical Relationship of AI, ML, and DLl 4
Figure 2: Research Rabbit / Network Visualisation 14
Figure 3: Research Rabbit / Timeline Visualisation 14
Figure 4: Technology Acceptance Model (TAM) 24
Figure 5: Conceptual Framework of the Study 27
Figure 6: Research Onion Diagram 29
Figure 7: Percevied Benefits of AI for Cybersecurity 41
Figure 8: Challenges in AI Adoption 42
Figure 9: Severity of AI Adoption Challenges Across Stages 43
Figure 10: Regulatory and Ethical Concerns in AI Adoption 45
Figure 11: Correlation Between AI Benefits, Challenges and Regulatory Concerns 45
Figure 12: Organisational Readiness for AI Adoption 48

LIST OF TABLES

Table 1: Data Sources for the Study 39

List of Abbreviations and Acronyms

The following abbreviations and acronyms are used throughout this report:

1. **AI** - Artificial Intelligence
2. **CISO** - Chief Information Security Officer
3. **DL** - Deep Learning
4. **4IR** - Fourth Industrial Revolution
5. **ML** - Machine Learning
6. **GANs** - Generative Adversarial Networks
7. **POPIA** - Protection of Personal Information Act
8. **TAM** - Technology Acceptance Model
9. **IDT** - Innovation Diffusion Theory
10. **JSE** - Johannesburg Stock Exchange
11. **GDPR** - General Data Protection Regulation
12. **MOT** - Management of Technology
13. **ETM** - Engineering and Technology Management
14. **SDG** - Sustainable Development Goal
15. **AWS** - Amazon Web Services
16. **GRC** - Governance, Risk, and Compliance
17. **NLP** - Natural Language Processing
18. **SOAR** - Security Orchestration, Automation, and Response
19. **BAS** - Breach and Attack Simulation
20. **GPT** - Generative Pre-trained Transformer
21. **MIS** - Management Information Systems
22. **ATT&CK** - Adversarial Tactics, Techniques, and Common Knowledge
23. **EAI** - European Alliance for Innovation
24. **IEEE** - Institute of Electrical and Electronics Engineers
25. **ICT** - Information and Communications Technology

ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: GOVERNANCE INSIGHTS FROM CYBERSECURITY EXPERTS IN THE BANKING INDUSTRY IN SOUTH AFRICA

ABSTRACT

Artificial Intelligence (AI) has emerged as a transformative force in cybersecurity, particularly in the banking sector, where cyber threats continue to evolve rapidly. South African banks, operating in a highly regulated environment, face the dual challenge of leveraging AI to enhance cybersecurity while ensuring compliance with governance and ethical standards. This study investigated the governance mechanisms required for the responsible adoption of AI for cybersecurity within the South African banking sector. Guided by the Technology Acceptance Model (TAM), Innovation Diffusion Theory (IDT), and Institutional Theory, this qualitative research explored cybersecurity experts' perspectives on AI adoption, governance, and ethical concerns. A single-case study design was employed, involving in-depth interviews with ten certified professionals from a major South African bank. Thematic analysis was conducted using Atlas.ti to identify key themes in AI governance. Findings revealed that while AI supports enhanced threat detection, response efficiency, and fraud prevention, notable challenges persist—including integration with legacy systems, skills shortages, regulatory ambiguity, and ethical risks. Experts highlighted the need for transparency, ethical oversight, and regulatory alignment to mitigate the potential harms of AI-driven cybersecurity decisions. Organisational readiness, leadership support, and structured governance frameworks were found to be critical enablers of responsible AI implementation. This study contributes to the evolving AI governance discourse by proposing an AI for Cybersecurity Governance Framework tailored to the South African banking sector. The framework offers strategic insights for banks, regulators, and policymakers seeking to balance innovation with ethical and regulatory imperatives in cybersecurity.

Keywords: Artificial Intelligence, Cybersecurity, AI Governance, AI in Banking, AI for Cybersecurity Governance.

1 INTRODUCTION

Artificial Intelligence (AI) emerged as a transformative force across various sectors, fundamentally altering industry operations and generating new opportunities (Xu et al., 2018). In cybersecurity, AI technologies such as Machine Learning (ML) and Deep Learning (DL) transformed the way in which threats were detected and responded to, enabling organisations to cope with cyber risks promptly and accurately (Sarker, 2021). Yet, the progression of AI for cybersecurity opened up daunting governance and ethical conversations, with growing concerns regarding algorithmic fairness, data privacy, and compliance with regulations, especially in heavily regulated sectors such as banking. One such industry was the South African banking sector, which stood as a prime example of how AI could be a double-edged sword in the context of cybersecurity. On one side, it faced growing threats from increasingly sophisticated cyber-attackers who exploited AI capabilities. Conversely, it operated within tight regulatory requirements and thus had to balance innovation with compliance (Verizon, 2023).

Guided by this context, the study aimed to investigate governance mechanisms that promoted the responsible and impactful application of AI for cybersecurity in this high-risk context. The study linked AI, governance, and cybersecurity literature using the case of the banking sector. The focus was on outlining governance mechanisms that facilitated responsible and effective integration of AI into cybersecurity operations. Notably, the study considered the South African banking sector, which, given the critical nature of data and the complexity of regulatory frameworks, presented a need for the development of context-relevant governance solutions (Halawi et al., 2024). The main scholarly contribution of this research was to develop an empirically grounded framework for understanding the governance of AI for cybersecurity. Building on the Technology Acceptance Model (TAM), Innovation Diffusion Theory (IDT), and Institutional Theory, the research provided a holistic perspective to analyse the adoption and governance of AI technologies for cybersecurity in South Africa's banking sector.

1.1 BACKGROUND

In the Fourth Industrial Revolution (4IR) era of rapid technological advancement, AI became a game changer for all sectors, including cybersecurity (Xu et al., 2018). AI technologies, including ML and DL, revolutionised the identification and response to cyber threats, enabling more rapid and precise detection and mitigation of risks (Sarker, 2021). Recent studies emphasised that

attackers exploited AI to develop progressively sophisticated assault tactics, including generative adversarial networks (GANs) used in spear-phishing campaigns (Iturbe et al., 2024). This increasing sophistication emphasised the need for AI-supported countermeasures that were as effective as AI-empowered attacks.

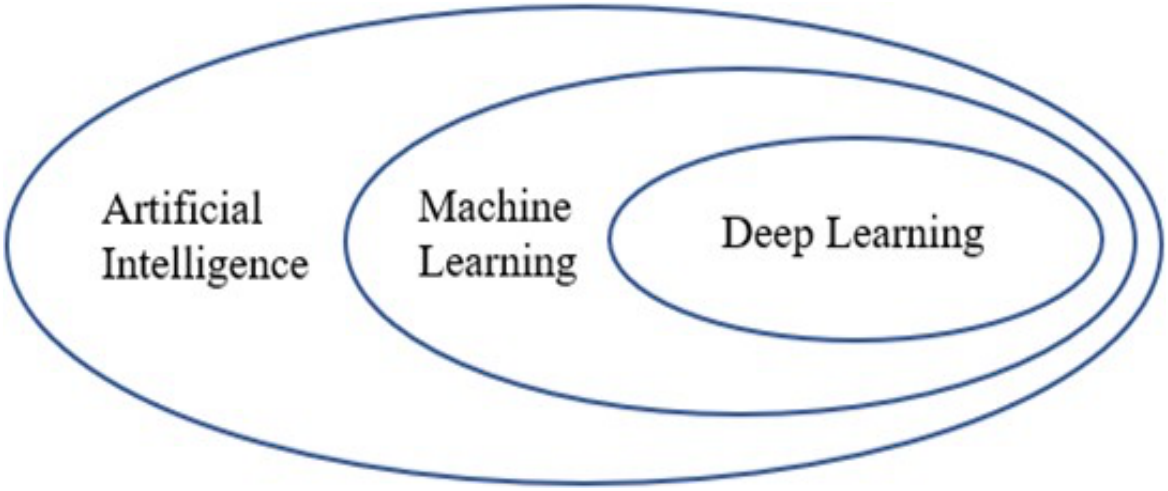


Figure 1: Hierarchical Relationship of AI, ML, and DL (Source: Towards Data Science, 2022).

AI was often misunderstood as a single unifying technology. In reality, it functioned at multiple levels, such as ML specialising in recognising patterns and DL applying neural networks to replicate human thought (Halawi et al., 2024). This technological transformation was especially important in the banking sector, which was often a target for cybercriminals due to the value of the financial data and transactions it processed (Verizon, 2023). The 2024 CISO Report from Splunk highlighted that more than 70% of Chief Information Security Officers (CISOs) believed generative AI would shift the cyber landscape to the attacker's advantage, and 35% had already implemented AI into their defence efforts (Splunk, 2024).

1.2 RESEARCH PROBLEM

The integration of AI into the cybersecurity domain represented a significant advancement in enhancing threat detection and response systems. However, it also introduced substantial governance and ethical challenges, particularly in highly regulated sectors such as banking. Concerns about data privacy, algorithmic bias, and compliance with intricate regulatory frameworks remained unresolved. In the South African banking landscape, these challenges were exacerbated by a rapidly changing and intensely regulated environment. Governance frameworks needed to keep pace with increasingly sophisticated AI-enabled threats. This growth warranted strong governance solutions to reap the benefits of AI for cybersecurity while overcoming challenges like algorithmic bias, data privacy, and nefarious usage of AI by hostile entities. This research critically examined the interactions between regulatory compliance, organisational readiness, and ethics in informing AI adoption in South Africa's banking sector.

Although these challenges were urgent, there was a limited number of academic studies addressing how governance structures could be implemented to mitigate AI risks in the cybersecurity context. Existing studies, such as Mamela et al. (2020), called attention to the necessity of workforce reskilling, while Jobin et al. (2019) addressed ethical dilemmas in AI governance. However, these contributions did not adequately consider governance frameworks suited to the South African banking landscape. This study aimed to bridge that gap by providing insights and a theoretical model for implementing AI within South Africa's banking industry.

1.3 AIMS AND OBJECTIVES OF THE RESEARCH

The primary contribution of this research was the formulation of an "AI for Cybersecurity Governance Framework" tailored to the South African banking sector. This artefact was constructed from empirical insights derived from qualitative interviews with twelve cybersecurity experts, framed using three theoretical lenses: TAM, IDT, and Institutional Theory. The framework considered elements including regulatory compliance, ethical considerations, and organisational preparedness, providing banks with a practical means to balance AI innovation with regulatory and ethical imperatives.

Based on the main research question above, the objectives that the study aimed to achieve were as follows:

i. **Perception**: To determine how IT decision-makers in the South African banking industry perceive the role of AI in enhancing cybersecurity.
ii. **Attitude**: To ascertain the attitudes of IT decision-makers in the South African banking industry on the use of AI for cybersecurity.
iii. **Drivers**: To determine how internal and external push factors influence the adoption of AI for cybersecurity in the South African banking industry.
iv. **Governance and Ethics**: To ascertain how IT decision-makers perceive the ethical and governance challenges related to AI use in cybersecurity within the South African banking industry.

1.4 RESEARCH QUESTIONS

The main research question that this study aimed to answer was: "How can South Africa's banking sector effectively govern the adoption of Artificial Intelligence (AI) for cybersecurity?" Additionally, to address this, the study explored the following sub-questions:

i. **Perception**: How do IT decision-makers in the South African banking industry perceive the role of AI in enhancing cybersecurity?
ii. **Attitude**: How do IT decision-makers in the South African banking industry view the adoption of AI for cybersecurity?
iii. **Drivers**: How do internal and external push factors influence the adoption of AI for cybersecurity in the South African banking industry?
iv. **Governance and Ethics**: How do IT decision-makers perceive the ethical and governance challenges related to AI use in cybersecurity within the South African banking industry?

1.5 STUDY JUSTIFICATION

AI is increasingly being integrated into cybersecurity technologies, presenting substantial opportunities and challenges within the banking sector, which operates under stringent regulatory frameworks. Banks in South Africa are under constant pressure to adopt innovative technologies that improve operational effectiveness while still adhering to increasingly complex legal and ethical standards. Technologies such as Machine Learning (ML) and Deep Learning (DL) are now widely used in cybersecurity, offering unmatched capabilities in threat detection and containment. However, their adoption also necessitates robust governance structures to address ethical dilemmas, algorithmic bias, and data privacy concerns. This study seeks to explore these governance mechanisms and proposes a framework tailored to the specific needs of the South African banking sector.

This research is particularly timely, as cyber-attacks continue to grow in sophistication, with malicious actors increasingly leveraging AI to exploit vulnerabilities in digital systems. According to the 2024 CISO Report by Splunk, over 70% of Chief Information Security Officers (CISOs) believe that generative AI will shift the cybersecurity landscape in favour of attackers, while 35% have already implemented AI in their defence strategies. South African banks, which are custodians of sensitive financial data, are especially vulnerable to such threats. As a result, the development of a governance framework that promotes responsible AI use in cybersecurity is not only a strategic imperative but also a matter of national security and economic stability. Despite the urgency, existing literature offers limited insight into how governance frameworks can practically support or constrain AI adoption in highly regulated environments. While international studies have explored AI's potential in cybersecurity, few have contextualised these insights within the South African banking sector. This study addresses that gap by examining the intersection of regulatory compliance, organisational readiness, and ethical considerations. It draws on legislative instruments such as the Protection of Personal Information Act (POPIA) to assess how external pressures influence AI governance.

From an academic perspective, this study contributes to the theoretical discourse by integrating three well-established frameworks: the Technology Acceptance Model (TAM), Innovation Diffusion Theory (IDT), and Institutional Theory. TAM explores the perceived usefulness and ease of use of AI technologies; IDT examines how innovations are adopted and diffused within

organisations; and Institutional Theory considers the influence of regulatory, cultural, and normative pressures on organisational behaviour. Together, these frameworks offer a comprehensive lens through which to analyse AI governance. Their integration ensures that the study's findings are both theoretically grounded and practically relevant. Given the risks associated with AI, such as perpetuating bias or compromising privacy, ethical governance emerges as a critical concern.

The study highlights the urgent need to align AI adoption with ethical principles and ensure that its implementation in cybersecurity does not inadvertently harm stakeholders or erode organisational culture. The proposed governance framework aims to address these concerns by promoting transparency, accountability, and trust among customers, regulators, and industry stakeholders. Ultimately, the study aspires to position South African banks as leaders in the global discourse on AI governance. By developing a context-sensitive framework, the research supports compliance with local legislation while aligning with international best practices. This dual focus enhances the study's relevance, offering insights that are both locally grounded and globally applicable.

In conclusion, this study addresses a critical gap in the governance of AI for cybersecurity in South African banks. It promotes a holistic understanding of AI governance by bridging theoretical perspectives with practical application. The research lays a foundational step toward ensuring that South Africa's financial sector is equipped to navigate the evolving threat landscape while embracing the transformative potential of AI in a safe, ethical, and sustainable manner.

1.6 IMPORTANCE OF THE STUDY

This study provides critical insights into whether and how artificial intelligence (AI), including machine learning (ML) and deep learning (DL), is being applied to cybersecurity within a South African banking context. Traditionally, cybersecurity functions have been performed by skilled professionals (Kshekri, 2021). However, as AI technologies increasingly demonstrate capabilities that mirror aspects of human intelligence, a growing number of organisations have begun integrating AI into their cybersecurity operations (Tiwari et al., 2022). This shift reflects a broader global trend toward automation and intelligent threat detection. The study also aligns with Sustainable Development Goal (SDG) 9 of the United Nations, which promotes industry, innovation, and infrastructure (United Nations, 2015). As McIntosh et al. (2023) argue, the

deployment of AI in critical sectors such as banking must be accompanied by robust governance mechanisms to ensure ethical and sustainable implementation.

The practical value of this study lies in its potential to equip South African banks with a governance framework that addresses real-world challenges, including vendor-related risks and the regulatory equivalency of AI-based technologies (Halawi et al., 2024). By examining how AI can be responsibly adopted in a highly regulated environment, the study offers actionable insights for improving compliance, operational resilience, and trust. The research also makes a theoretical contribution by extending the Technology Acceptance Model (TAM) to incorporate ethical and governance dimensions within the cybersecurity domain. Without such research, South African banks may lack access to context-specific case studies that can guide the responsible adoption of Industry 4.0 technologies. Furthermore, from an academic standpoint, the absence of empirical research on AI governance in South African cybersecurity contexts would leave a significant gap in the literature.

1.7 STUDY LIMITATIONS

This study was confined to the South African banking sector, which limits the extent to which its findings can be generalised to other industries or geographic regions. While the banking sector provides a rich and highly regulated environment for examining AI governance, its operational and regulatory dynamics differ significantly from those in sectors such as healthcare, education, or government. As a result, the applicability of the findings may be limited in contexts with different institutional, legal, or technological conditions.

Additionally, the study employed a single-case study design, which allowed for in-depth exploration but inherently narrowed the scope of generalisability. The experiences and governance practices of one bank may not fully represent the diversity of approaches across the broader banking sector, even within South Africa. However, the reliability and credibility of the findings were strengthened through triangulation and the use of multiple data sources, including interviews and document analysis (Mamela et al., 2020). Access to participants also posed a limitation. The study targeted senior executives and cybersecurity professionals, many of whom had demanding schedules. This affected the availability of some participants and may have introduced bias if only a subset of perspectives was captured. To mitigate this, the study incorporated flexible interview

formats, including virtual and asynchronous options, which enabled the collection of rich insights despite logistical constraints.

In summary, while the study offers valuable contributions to the understanding of AI governance in cybersecurity, its findings should be interpreted with consideration of the contextual and methodological boundaries outlined above.

1.8 ETHICS-RELATED MATTERS

This study was conducted in accordance with established ethical standards to ensure the protection of participants and the integrity of the research process. Key ethical considerations included confidentiality, privacy, informed consent, and compliance with institutional and national guidelines. Ethical approval was obtained from the University of the Witwatersrand School of Business Sciences Ethics Committee under protocol number CBUSE2289.

A detailed account of the ethical procedures, including data handling, anonymisation, and risk mitigation strategies, is provided in Section 3.5 of this report.

1.9 SUMMARY OF THE INTRODUCTION CHAPTER

This chapter introduced the scope and rationale of the study, highlighting its interdisciplinary focus on artificial intelligence (AI) governance within the cybersecurity domain of the South African banking sector. It outlined the background and context of the research, emphasising the increasing adoption of AI technologies and the associated governance, ethical, and regulatory challenges. The chapter also presented the research problem, aims, objectives, and questions, which collectively guide the investigation. The justification for the study was discussed, demonstrating its relevance to both academic and practical domains, particularly in light of the evolving threat landscape and the need for responsible AI adoption in highly regulated environments.

Furthermore, the chapter addressed the importance of the study, its limitations, and the ethical considerations underpinning the research. These elements establish a foundation for the chapters that follow. Chapter 2 presents a comprehensive review of the literature, including global and local perspectives on AI in cybersecurity, theoretical frameworks, and the conceptual model guiding the study. Chapter 3 outlines the research methodology, followed by the presentation of findings in Chapter 4, discussion in Chapter 5, and conclusions and recommendations in Chapter 6.

2. LITERATURE REVIEW

2.1 INTRODUCTION

This chapter presents the literature underpinning and supporting this research study through a review of existing studies on related topics. The review followed an "onion approach" (Saunders, Lewis, & Thornhill, 2016) to commence with a global perspective of artificial intelligence in cybersecurity, in order to provide a broad foundation. It then narrowed down to the African setting, establishing unique challenges such as infrastructural inadequacies and a shortage of professional human resources, before homing in on the South African banking industry. This methodical framework allowed for a deep understanding of the subject area while identifying key gaps in current literature, including the ethical dimensions of integrating artificial intelligence, the complexity of regulation, and the lack of interrelation among multiple research studies (Taddeo, 2019; Lourens et al., 2022; Mamela et al., 2020). These gaps identified formed the rationale for the present exploration into governance views provided by cybersecurity experts within the banking sector of South Africa.

2.2 REVIEW OF RELATED LITERATURE

The adoption and utilisation of artificial intelligence in the cybersecurity industry garnered significant attention in recent years. Several studies explored the potential benefits and challenges of integrating AI into cybersecurity practices (Sarker & Rashid, 2020). According to Mamela, Sukdeo, and Mukwakungu (2020), organisations could not ignore the need to adopt AI in their cybersecurity strategy. Taddeo (2019) argued that the integration of AI for cybersecurity required a blended approach, combining both human expertise and AI capabilities. Furthermore, research showed that AI enhanced the effectiveness and efficiency of cybersecurity systems (Berman, Buczak, Chavis, & Corbett, 2019).

The diagrams presented in Figures 2 and 3 demonstrated the network and timeline of the selected papers for this literature review. Following a systematic literature review, 36 papers were selected from a pool of 136 papers based on their relevance to the topic. The criteria for selection included topical alignment with AI, governance, and cybersecurity; relevance to the South African or similar regulatory context; and publication in peer-reviewed or academically rigorous sources. Although there was limited interconnectedness in research about AI for cybersecurity in South Africa, recent papers provided a solid foundation for understanding the genesis, current state, and future directions

of AI for cybersecurity.

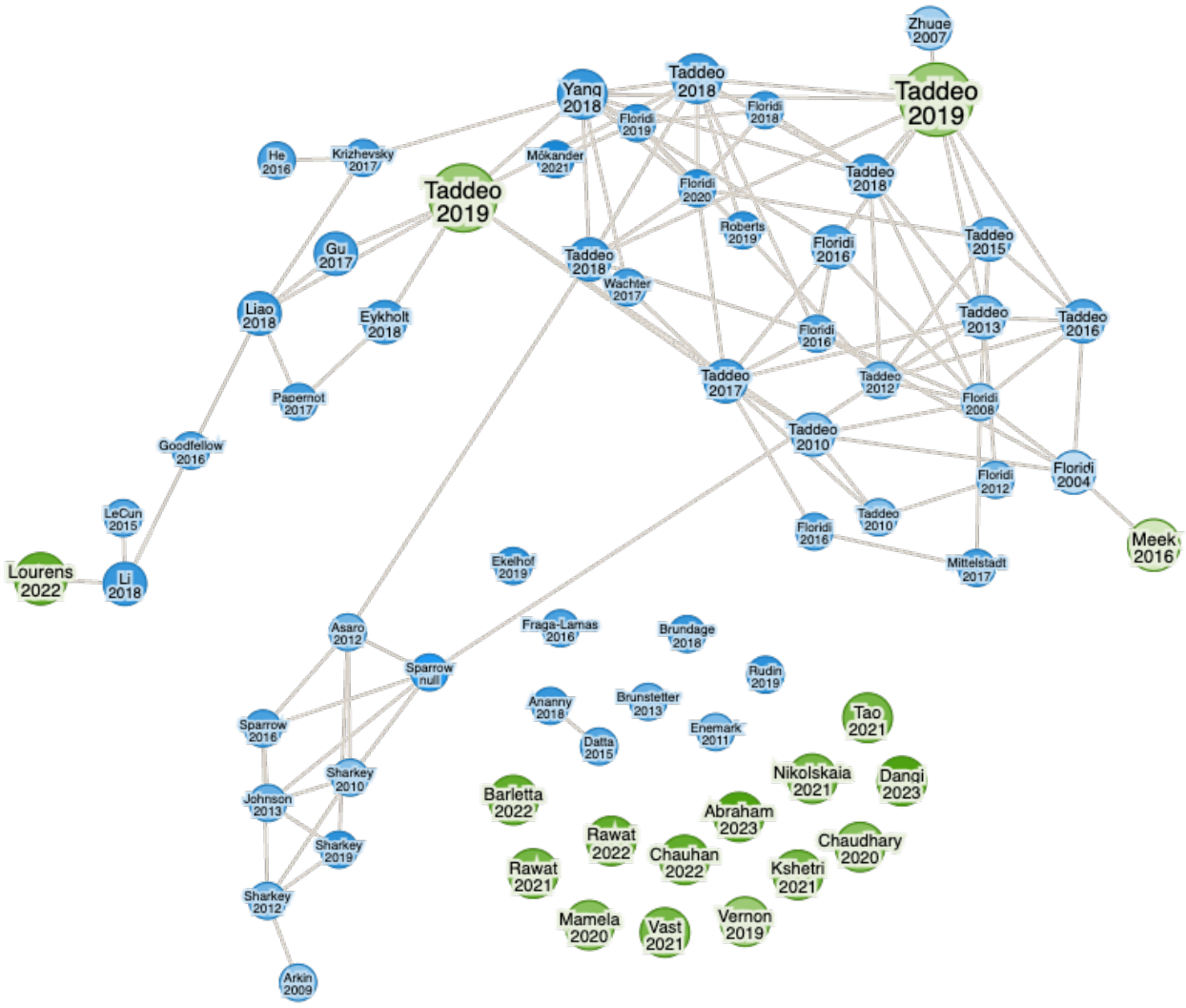


Figure 2: Research Rabbit / Network Visualisation

Figure 2 presented a visual representation of similar and related works to the articles selected for this study, as extracted from Research Rabbit. This network of interconnected studies illustrated how the selected articles formed part of a broader academic ecosystem, ensuring that the literature reviewed was both relevant and grounded in existing research. By mapping these connections, Figure 2 highlighted the careful selection process undertaken to include only articles that aligned with the research topic and contributed meaningfully to the discourse on artificial intelligence (AI) in cybersecurity, governance, and ethics.

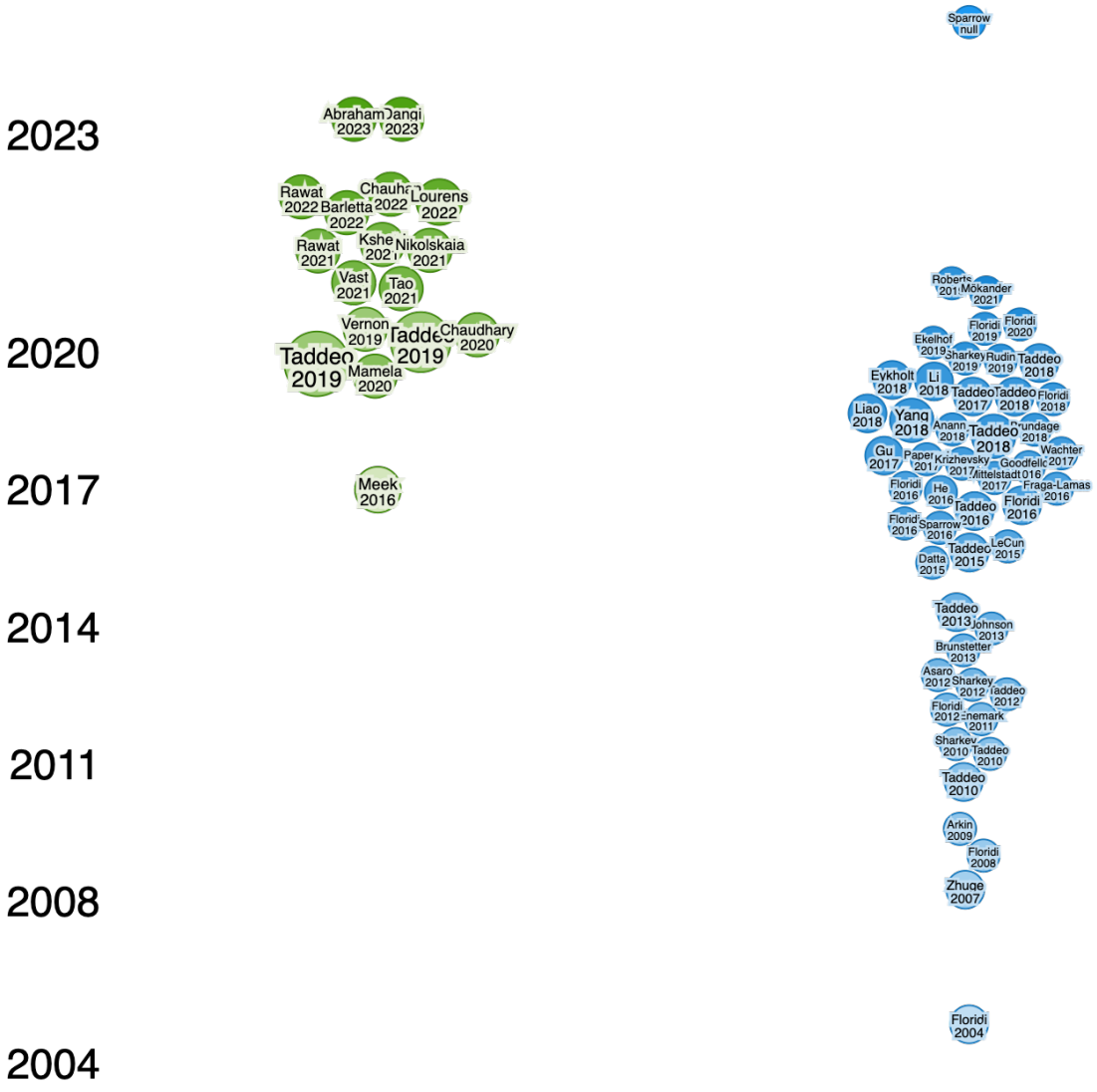


Figure 3: Research Rabbit / Timeline Visualisation

Figure 3 provided a chronological timeline of the selected articles, spanning from 2004 to 2024. This visualisation demonstrated the progression of research in this field, showcasing how scholarly interest in AI-related cybersecurity topics evolved over time. The timeline reflected key developments, including regulatory shifts and global incidents such as COVID-19, which influenced digitalisation and cyber risk exposure. By examining the distribution of articles across the years, Figure 3 underscored the increasing relevance of AI in addressing modern cybersecurity challenges and highlighted key periods of academic development and breakthroughs in the field.

The integration of artificial intelligence (AI) in cybersecurity gained significant attention globally, with various researchers exploring its potential and challenges. This review examined key studies on the topic, focusing on the South African context. Recent studies underscored the transformative impact of AI for cybersecurity, highlighting its ability to automate complex tasks and improve threat detection and response times (Berman et al., 2019). The ethical implications of AI, including concerns about data privacy and algorithmic bias, remained significant. Addressing these issues through robust governance frameworks was crucial (Mamela et al., 2020; Jobin, Ienca, & Vayena, 2019). Case studies from various industries, including banking, provided valuable insights into AI integration's practical applications and challenges (Sarker & Rashid, 2020).

2.2.1 Global Perspectives on AI for Cybersecurity

Taddeo (2019) emphasised the necessity of harmonising AI technologies to mimic the human brain's deep learning capabilities. She advocated for global standards and regulatory frameworks to address concerns such as data privacy, algorithmic biases, and accountability. Taddeo proposed that there must be an in-house development of AI solutions by organisations to ensure control, accountability, and sustainability. This was particularly relevant for countries like Saudi Arabia, European Union countries (due to GDPR), and South Africa, where data sovereignty and localised solutions were crucial due to varying regulatory environments.

Nikolskaia et al. (2021) discussed the integration of AI into various sectors, including cybersecurity. They highlighted the disparity in AI implementation across sectors, with a specific focus on the banking sector in South Africa. This study was pivotal as it underscored the potential for the banking sector to lead in AI adoption for cybersecurity, given its stringent regulatory requirements and significant resources. However, the broader application across other critical sectors like healthcare and government services remained under-explored, presenting an opportunity for further research. Lourens et al. (2022) suggested integrating AI with cybersecurity due to AI's capability to exhibit human-like intelligence. Their study emphasised the potential benefits of AI technologies in enhancing cybersecurity measures. This aligned with the findings of Vernon (2019), who highlighted the positive impact of AI on developing countries. Vernon’s insights were particularly relevant to South Africa, where AI could address challenges in sectors such as healthcare and financial services, providing a comprehensive strategy for national development.

2.2.2 Sector-Specific Insights and Ethical Considerations

Mamela et al. (2020) investigated the workforce impact of AI adaptation, concluding that while it improved convenience and reduced costs, reskilling the workforce was necessary. This was a critical point for South Africa, where unemployment and skills gaps were significant issues. The emphasis on reskilling aligned with the need for a sustainable AI integration strategy that included workforce development as a core component. Rawat et al. (2021) explored the role of AI in warfare and security, emphasising its potential to facilitate military decisions and enhance cybersecurity practices. While their focus was broader, their insights on AI's capability to handle complex security tasks could be applied to South Africa's cybersecurity landscape, especially in critical infrastructure protection and national security. Vast et al. (2021) proposed automation with AI to streamline security processes, reducing the burden on security professionals. This was particularly relevant for South Africa, where there was a shortage of cybersecurity professionals. Automation could alleviate some of the pressures on existing staff, allowing for a more strategic focus on threat analysis and mitigation.

2.2.3 Challenges Relating to Ethics and Governance

Bailey et al. (2023) and McIntosh et al. (2023) shared a common theme of ethical considerations in AI-powered cybersecurity systems. Bailey et al. were concerned about algorithmic bias and data colonialism, situations where the data used for training datasets were biased and ended up amplifying systemic inequities. They suggested the use of synthetic data to overcome these types of biases. McIntosh et al., on the other hand, studied the use of generative AI like GPT-4 in governance, risk, and compliance (GRC) policy development. These tools contributed to policy efficiency but also created challenges for regulatory compliance. Both studies highlighted the importance of strong ethical frameworks and governance mechanisms to guarantee equitable AI practices.

2.2.4 Strategic Models for Cyber Protection

The taxonomy proposed by AlDaajeh and Alrabaee (2024) described ways of categorising national cybersecurity challenges, with an emphasis on holistic frameworks that combined the technical, organisational, and policy aspects. Mehrizi et al. (2024) emphasised that instituting AI in organisations should be interwoven at all levels and embedded at an organisational strategy level. Together, these studies underscored the need for holistic strategies accounting for regulatory requirements and resilience.

The literature review involved a thematic analysis of various studies related to artificial intelligence (AI) and its applications in cybersecurity, governance, and ethical considerations. This analysis identified key themes such as AI-driven threat detection, ethical implications of AI in security, and strategic models for cyber protection. To maintain clarity and readability, a detailed tabular breakdown of the thematic analysis, including references, research designs, and theoretical frameworks, has been moved to Appendix E. Readers seeking an in-depth exploration of these themes and their corresponding studies are encouraged to refer to **Appendix E: Literature Review Thematic Analysis** for further details. Furthermore, the literature review identified several critical issues, including the key issues identified. While AI is firmly established as having transformative potential in enhancing the measures of cybersecurity, the key challenges that are going to remain include issues of ethical considerations, algorithmic biases, and regulatory compliance. The study identifies the are gaps in literature where there is limited research on the practical application of AI in South Africa's banking sector. Moreover, how governance and regulatory frameworks shape AI adoption is an under-explored theme. This study aims to fill these gaps by exploring the governance insights of cybersecurity experts working within the South African banking industry. The next section explains the theoretical lens underpinning this research.

2.3 THEORETICAL AND EMPIRICAL THEORY DISCUSSION, CONCEPTUAL MODEL AND RESEARCH PROPOSITIONS

2.3.1 The theories underpinning this study.

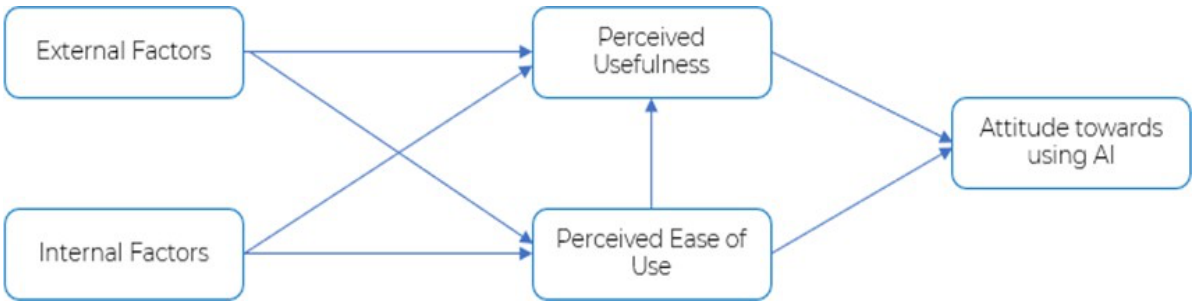
Three theories underpinned and guided this study. These were the Technology Acceptance Model (TAM) developed by Davis (1989), the Innovation Diffusion Theory (IDT) developed by Rogers (1962), and Institutional Theory developed by Meyer et al. (1987) and further refined by Meyer & Jepperson (2000). These theories were considered relevant and complementary to the study as they offered perspectives across individual, organisational, and environmental levels.

2.3.2 Technology Acceptance Model (TAM)

Key arguments underlying the theory

The Technology Acceptance Model (TAM) by Davis (1989) was used in this study as it helped explore the acceptance and use of AI technologies by cybersecurity professionals. This theory was still applicable despite its age, particularly given the emergence of user-facing AI applications such as ChatGPT and automated cybersecurity tools. It helped identify how perceived usefulness and perceived ease of use influenced the acceptance of AI tools, both of which were prominent variables in cybersecurity applications.

Figure 4: TAM



Source (Davis, 1989)

Arguments advanced for this study: The Technology Acceptance Model (TAM) (Davis, 1989) was chosen due to its relevance in understanding technology adoption, particularly in professional environments like cybersecurity. TAM's focus on perceived usefulness and ease of use provides a structured way to analyse the factors influencing AI acceptance among cybersecurity experts, which is crucial given the rapid integration of AI tools in this field. The model's widespread use in technology adoption studies makes it a robust framework for understanding how professionals adapt to new technologies.

2.3.3 Diffusion of Innovation Theory

Key arguments underlying the theory

The Diffusion of Innovation Theory (IDT) by Rogers (1962) offered insights into the adoption of newer AI technologies within an organisation. It explained how individuals and groups adopted innovation and how such innovation diffused through a social system. The relevance of this theory to the banking sector

lay in its focus on innovation characteristics such as compatibility, complexity, and relative advantage, which aligned with how AI was being adopted in cybersecurity operations.

Arguments advanced for this study: The Innovation Diffusion Theory (IDT) (Rogers, 1962) was selected because it offers insights into the mechanisms by which innovations, such as AI, spread within sectors like banking. AI adoption is not just a matter of individual decision-making but also a collective process within organisations and industries. IDT helps explain how technological innovations diffuse through communication channels over time, making it ideal for studying the spread of AI innovations in a highly regulated and interconnected industry like banking.

2.3.4 Institutional Theory

Key arguments underlying the theory

Institutional Theory was also included to address the external pressures that shaped organisational behaviour, including the influence of national regulations such as POPIA, international frameworks such as GDPR, and industry-wide best practices. It explained how institutional forces such as coercive (regulatory), normative (professional standards), and mimetic (peer influence) shaped the way banks responded to the need for AI governance in cybersecurity.

Together, these theories complemented each other. While TAM helped understand the technology's perceived value by individuals, IDT captured how innovations spread, and Institutional Theory framed the external environment's influence. The overlap in their focus on change and adoption helped build a more integrated and multidimensional understanding of AI governance. Their combined use addressed their individual limitations—for example, TAM did not account for organisational or regulatory pressures, while Institutional Theory was weak on individual-level drivers of adoption. The integration allowed the study to analyse AI adoption and governance from multiple angles: technological, organisational, and regulatory.

Arguments advanced for this study: The Institutional Theory (Meyer et al., 1987; Meyer & Jepperson, 2000) was chosen to explore the external pressures that influence AI adoption. This theory is particularly relevant for understanding how regulatory frameworks, industry standards, and

organisational culture shape the acceptance and use of AI. Institutional Theory helps explain how organisations conform to external norms, rules, and standards, which is critical for examining the role of compliance and regulation in the banking and cybersecurity sectors.

2.3.5 Research Propositions

Proposition 1: The perceived usefulness of AI technologies will significantly enhance their acceptance among cybersecurity experts in the banking sector, as highlighted by Davis (1989) in the Technology Acceptance Model.

Proposition 2: The ease of use of AI technologies will positively influence the acceptance and adoption of AI among cybersecurity professionals, supporting the findings of various studies on user experience and technology integration (Mamela et al., 2020).

Proposition 3: The characteristics of AI innovations, as described by the Innovation Diffusion Theory (Rogers, 1962), will significantly impact the rate of AI adoption within the banking sector.

Proposition 4: Regulatory frameworks and industry standards will shape the organisational culture and ethical considerations, influencing the acceptance of AI technologies among cybersecurity experts in the banking sector.

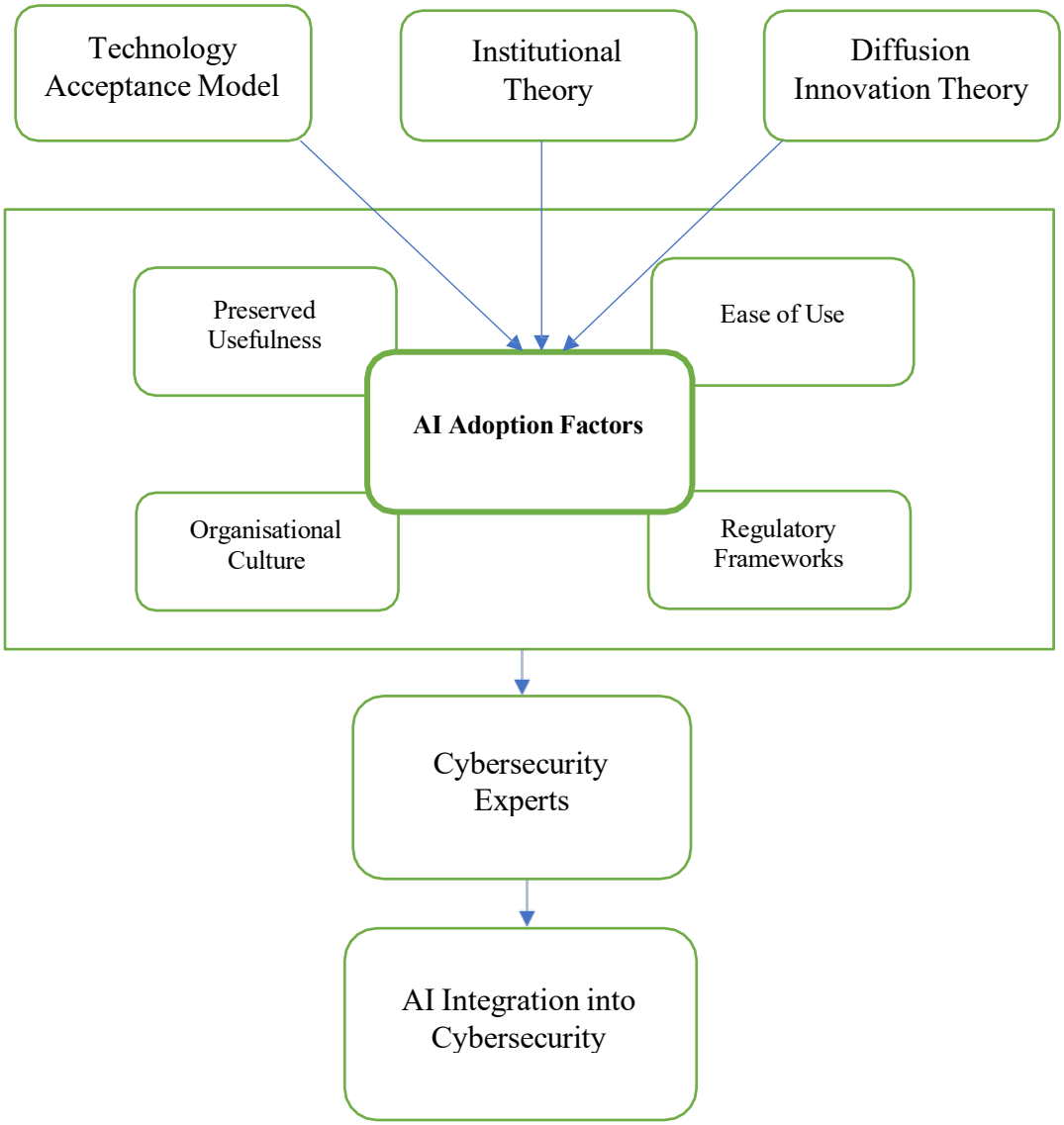
Proposition 5: Workforce reskilling initiatives will be crucial for the successful integration of AI for cybersecurity practices, addressing the skills gap as highlighted by Mamela et al. (2020) and Vast et al. (2021).

2.4 CONCEPTUAL FRAMEWORK OF THE STUDY

The conceptual framework for this study adopts an integrated approach that is theoretically informed by the Technology Acceptance Model, Innovation Diffusion Theory, and Institutional Theory. The integration of these theories in this research captures the multidimensional nature of AI adoption. TAM analyses individual-level adoption issues; IDT focuses on processes through which innovations diffuse in organisations, whereas Institutional Theory focuses on regulatory and cultural factors in shaping the adoption of AI. Using these combined theories will, therefore, provide a good basis to analyse the complexities of integrating AI into cybersecurity practices within the banking industry.

Key items include the perceived usefulness of AI technologies in improving cybersecurity practices, ease of use, nature of AI innovations, regulatory frameworks in shaping the implementation of AI, organisational culture in the course of adopting AI, and workforce reskilling for effective AI integration. In essence, such an integration of the theoretical construct and the consideration of practical reality does ensure that the framework relates to the objectives of the study in order to discover governance insights from cybersecurity experts within the South African banking sector.

Figure 5: Conceptual Framework of the Study



i. **Perceived Usefulness**: The benefits of AI technologies in enhancing cybersecurity practices and effectiveness.
ii. **Ease of Use**: User experience and accessibility of AI tools for cybersecurity experts.
iii. **Innovation Characteristics**: Factors affecting the adoption of AI technologies, including complexity and compatibility with existing systems.
iv. **Regulatory Frameworks**: The impact of laws and regulations on AI implementation and usage.
v. **Organisational Culture**: How institutional norms and values influence AI adoption.
vi. **Workforce Reskilling**: The necessity for training and development to prepare the workforce for AI integration.

2.5 CONCLUSION

This chapter reviewed literature relevant to the governance of AI for cybersecurity. It began by providing a broad overview of global research, narrowed down to the African context, and finally focused on South Africa's banking sector. The literature demonstrated that AI offered several advantages in cybersecurity but also presented ethical and governance challenges that required contextualised approaches.

The chapter also introduced the theoretical underpinnings of the study. It justified the choice of the Technology Acceptance Model, Innovation Diffusion Theory, and Institutional Theory as complementary frameworks that enabled a multidimensional analysis. The conceptual framework built from these theories formed the basis for the study's data collection and analysis. The following chapter details the methodology used to explore these propositions and to empirically investigate AI governance from the perspectives of cybersecurity experts in a South African bank.

3. RESEARCH METHODOLOGY

3.1 INTRODUCTION

This chapter explains the research methodology adopted for this study, which investigates the adoption and governance of artificial intelligence (AI) for cybersecurity in a South African bank. It outlines the research philosophy, approach, design, data collection and analysis methods, ethical considerations, and validation techniques. These methodological components were selected to ensure robustness and alignment with the study's objective: to present practical insights from cybersecurity experts on the governance of AI technologies in the banking sector.

3.2 RESEARCH PHILOSOPHY (PARADIGM)

The methodological framework of this study can be illustrated through Saunders et al.'s (2009) "research onion," which describes the layered choices involved in research design. The outermost layer represents the research philosophy, which forms the foundation upon which all other methodological decisions rest. This study adopted an interpretivist philosophy.

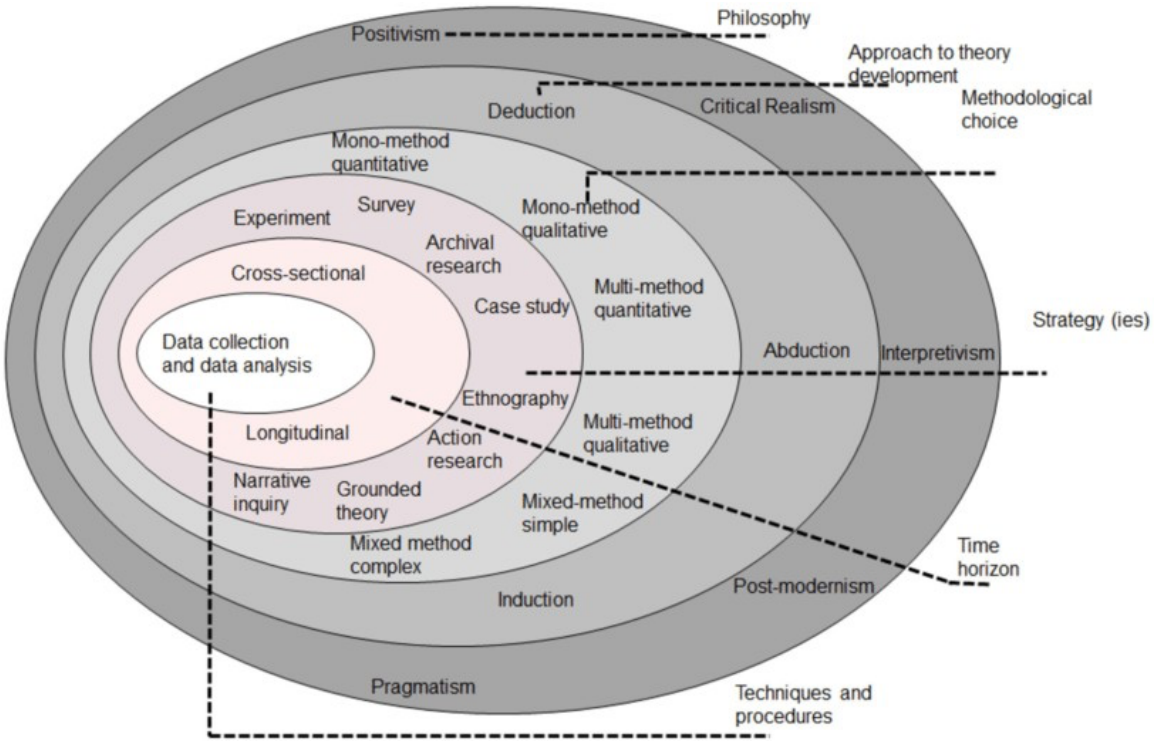


Figure 6: Research Onion Diagram (Source: Saunders et al., 2009, p. 108).

Interpretivism holds that social reality is constructed through human experience and interaction within specific contexts. According to Saunders (2009), a research philosophy refers to the set of beliefs and assumptions about how knowledge is developed. In this study, interpretivism was appropriate because it allowed the researcher to understand how cybersecurity professionals interpret, experience, and engage with the governance of AI in a highly regulated banking environment.

This philosophy provided the flexibility to explore complex, subjective experiences, enabling the researcher to investigate how organisational, social, and regulatory factors influence AI adoption. As Creswell (2018) and Welman et al. (2011) argue, interpretive approaches are especially useful when exploring nuanced issues such as ethics, compliance, and innovation adoption in professional settings. This study's focus on lived experiences and meaning-making among experts aligned well with interpretivist assumptions, ensuring that findings would be context-sensitive and grounded in real-world perspectives.

3.3 RESEARCH DESIGN

This study employed a qualitative single-case study design to examine the governance and adoption of AI for cybersecurity in a South African bank. According to Flick (2015), qualitative research is well-suited for exploring subjective experiences, opinions, and meaning-making processes through non-numerical data. This design was chosen due to its ability to generate deep insight into context-specific, complex phenomena, such as the integration of AI systems within a highly regulated industry. As Welman et al. (2011) assert, qualitative case studies offer rich, contextually grounded insights that are difficult to achieve in broader, multi-case approaches. The single-case study allowed for an in-depth examination of one organisational setting, aligning with the study's aim to understand the interplay between AI technologies, governance practices, and regulatory contexts.

The justification for a qualitative approach stemmed from the need to capture the subjective views of experts involved in AI and cybersecurity governance — particularly around emerging concerns such as data privacy, algorithmic transparency, and compliance. In this sense, qualitative methods were essential for investigating both the technical and human dimensions of AI integration.

3.4 STUDY ORGANISATION

The study was conducted in a JSE-listed South African bank selected based on its prominence in the financial sector and its advanced AI-driven cybersecurity infrastructure. The organisation was an entirely digital bank with no physical branches, operating on a technology-driven model that leveraged cloud computing, AI, and advanced analytics to deliver services. This digital-first model made cybersecurity a core strategic priority, given that all customer interactions occurred online. The bank had demonstrated significant progress in adopting AI tools to manage cybersecurity threats, which made it an appropriate case for examining the challenges and opportunities of AI governance. Furthermore, it operated under strict regulatory frameworks, such as the Protection of Personal Information Act (POPIA) and Basel III, making it representative of a highly regulated industry. With a cybersecurity team comprising 77 professionals, the bank provided a wide range of perspectives on AI adoption and governance. This organisational context offered a rich environment for the study's objectives, enabling the researcher to gather nuanced insights from experts across governance, analytics, infrastructure, and compliance functions.

3.4.1 Research Population and Sampling

The sampling process for selecting the South African bank listed on the Johannesburg Stock Exchange (JSE) followed a judgment sampling approach. The bank was chosen due to its strategic prominence in the sector and the recognised expertise of its cybersecurity professionals. This case provided an ideal setting for a deep investigation into the governance and adoption of AI in a highly regulated environment. Within the bank, a cybersecurity workforce of 77 professionals was identified. From this pool, 12 experts were interviewed for the study. This sample size falls within the range of 12 to 60 recommended by Creswell (2018) for qualitative studies and was deemed sufficient to achieve thematic saturation, allowing for the identification of key patterns and insights (Glaser & Strauss, 1967 as cited in Silverman, 2020).

The study deliberately sought diversity in participant roles, experience levels, and responsibilities, thereby enhancing the richness and reliability of the findings. This justified the use of judgment and stratified purposive sampling rather than random sampling, as the objective was to extract in-depth insights from those directly involved in AI governance. Participants included cybersecurity analysts, IT governance professionals, and compliance specialists, offering varied perspectives on AI integration and oversight in the banking environment.

3.4.2 Data Collection Instrument

The interview guide was designed to align with the study's objectives and included themes such as the perceived usefulness of AI, governance practices, adoption challenges, and ethical considerations. The guide employed open-ended questions to promote expansive discussion and follow-up probes to deepen understanding.

Before formal data collection, the guide was pilot tested with a small subset of experts. Feedback from the pilot phase led to refinements in the wording and sequencing of questions, improving their clarity, focus, and relevance. This pretesting ensured that the final instrument could elicit rich, valid responses aligned with the study's research questions.

3.4.3 Data Collection Procedures

Data were collected through semi-structured, in-depth interviews, a method suited for exploratory, context-driven inquiry. This approach allowed for a balance between guided questioning and flexibility, enabling participants to elaborate on emerging issues during the conversation. The 12 interviews were conducted both in person and virtually, depending on participant availability. Face-to-face interviews were conducted at secure premises, while virtual interviews were held via Microsoft Teams. Each interview lasted approximately 45 to 60 minutes and was audio-recorded (with permission) using secure, password-protected devices. Transcripts were produced verbatim to preserve accuracy and contextual detail.

3.4.4 The Interview Process

The interview process was carefully structured to ensure the collection of rich, qualitative data while accommodating participants' availability. Scheduling was flexible, allowing cybersecurity professionals to participate at their convenience, as recommended by Creswell (2018), who emphasises the importance of adapting data collection to participants' schedules to encourage engagement and maximise response quality. A combination of in-person and virtual interviews was employed to enhance accessibility and inclusivity, aligning with Saunders et al. (2019), who

highlight that mixed-mode interviewing improves participation rates and reduces logistical barriers. Face-to-face interviews facilitated deeper engagement and non-verbal cue observation, as Flick (2015) suggests that physical interactions provide additional context that enhances data richness. Virtual interviews, on the other hand, were crucial for reaching participants who were geographically dispersed or had time constraints, supporting Opdenakker's (2006) argument that online interviews offer flexibility while maintaining the depth of responses. Each interview lasted between 45 minutes to one hour, as recommended by Kallio et al. (2016), who state that semi-structured interviews should allow sufficient time for in-depth discussions without causing fatigue. A semi-structured interview approach was adopted to balance consistency and flexibility, ensuring key themes were addressed while allowing participants to elaborate on their experiences and perspectives. According to Bryman (2016), semi-structured interviews are valuable in qualitative research as they allow for deeper exploration of complex topics while providing a structured framework that ensures comparability across interviews. This approach was particularly useful in understanding AI governance in cybersecurity, as it enabled the researcher to probe further based on participants' responses, generating comprehensive insights into their perceptions and experiences.

3.4.5 Data Collection Methods

3.4.6 Primary Data Collection

Primary data for this study was collected through semi-structured interviews conducted both face-to-face and virtually via Microsoft Teams. This approach allowed for an in-depth exploration of participants' experiences with AI governance, ensuring flexibility in data collection while accommodating participants' availability. Face-to-face interviews took place at 1 Discovery Place, Sandton, providing a structured and interactive setting for discussion. Virtual interviews were conducted via Microsoft Teams, ensuring accessibility for participants who were unable to attend in person. All interviews were voice recorded using a company-issued laptop, and recordings were transcribed verbatim to maintain accuracy and ensure that key insights were captured effectively. The interview questions were designed around core themes such as AI usefulness, governance, and ethics, allowing participants to provide detailed responses on their perspectives and experiences. To enhance the reliability and relevance of the data collected, the interview guide was pilot-tested before formal data collection began, ensuring that questions were clear, appropriately framed, and aligned with the study's research objectives.

3.4.5.1 Secondary Data

Secondary data was collected from various sources to complement primary data and support triangulation. This included company reports on AI governance (view-only versions on OneTrust – not downloadable), which provided insights into how organisations implement and manage AI-driven cybersecurity measures. These reports were crucial in understanding industry-specific governance practices, policies, and risk management strategies related to AI adoption. Additionally, regulatory and compliance documents on AI in financial services were examined to assess the legal frameworks and ethical guidelines governing AI deployment. Documents such as the Protection of Personal Information Act (POPIA) and the General Data Protection Regulation (GDPR) were particularly relevant in understanding compliance requirements and data protection obligations for banks implementing AI technologies. Furthermore, industry reports and white papers on AI in banking cybersecurity were analysed to gain a broader perspective on global trends, challenges, and best practices in AI-driven cybersecurity.

These sources provided valuable comparative insights, allowing the study to contextualise its findings within both local and international banking environments. Document analysis was conducted to identify common themes in these materials, ensuring alignment between industry perspectives and the primary data collected through interviews. The findings from the document analysis were cross-referenced with interview data to validate themes, ensuring a robust and well-rounded examination of AI governance in cybersecurity within the banking sector.

3.4.5.2 Data Collection Challenges

This study did not go without challenges in data collection; thus, it was challenging reaching out to participants to schedule interviews, mainly because of the busy nature of their working schedules. Various participants have said they are very specialised, hence busier; the team is small, so interviews could not be scheduled for the same day, as this would paralyse the workflow. Therefore, flexibility in terms of scheduling had to be made where interviews were spaced out in consideration of the participants' professional lives. Data was collected in December 2024 and January 2025, since during this time participants were most likely to be free since there was a freeze in IT changes over the year's end.

3.4.7 Data Analysis

Thematic analysis was applied in this research to identify patterns and themes in the interview data. This technique is appropriate in qualitative research since it provides a systematic approach to organising and interpreting data. Through multiple close readings of the transcripts, the analysis identified recurrent themes, relationships, and insights relevant to the study's objectives (Silverman, 2020). A Qualitative Data Analysis Software (QDAS) Atlas.ti, was used to support the analysis by labelling ideas, categorising them, relating them to other instances, and developing a conceptual map of findings. The stringent analytical procedure ensures that the study's conclusion is fact-based and reflects the participants' experiences. Various problems, like large datasets, were overcome through systematic coding and iteration of analysis to ensure consistency and depth.

3.5 ETHICAL CONSIDERATIONS

Ethical considerations are critical in qualitative research to ensure the protection of participants and the integrity of findings. One of the foundational ethical principles is voluntary participation, which ensures that individuals are not coerced into taking part in a study. According to Creswell (2018), participants must be given sufficient information about the study to make an informed decision about their involvement. Furthermore, informed consent was achieved by providing participants with detailed study information, including its purpose, potential risks, and confidentiality measures. As supported by Silverman (2020), interviewees need to confirm their willingness to participate by signing an informed consent form, which acknowledges their understanding and agreement. In addition to consent, confidentiality and anonymity were maintained throughout the study to protect participant identities. Data anonymisation techniques, such as assigning pseudonyms and removing identifying information from transcripts, were implemented in line with Saunders et al. (2009), who emphasise the importance of protecting personal data in research. Similarly, Bryman (2016) asserts that ensuring anonymity enhances the credibility of research findings by allowing participants to speak freely without fear of professional or legal repercussions.

Moreover, data integrity and security were upheld to prevent unauthorised access to research materials. As highlighted by Welman et al. (2011), ethical research requires that data be securely stored in encrypted files and only accessible to authorised individuals. In this study, data was stored on a password-protected server, ensuring compliance with institutional ethics policies. The ethical review process also played a vital role, as approval was obtained from the University of the

Witwatersrand's Ethics Committee before data collection commenced. As noted by Flick (2015), ethical clearance from a recognised board ensures that the study meets international standards for research involving human subjects. Furthermore, to mitigate potential harm, the study adopted a non-intrusive approach, allowing participants to withdraw at any stage without justification. Merriam and Tisdell (2016) stress that ethical research should prioritise participant well-being, especially when dealing with sensitive topics such as AI governance in cybersecurity. Triangulation was also used to enhance credibility by comparing findings from different sources, as recommended by Denzin (2012). By ensuring voluntary participation, informed consent, confidentiality, data security, and research credibility, this study adhered to robust ethical standards that align with global best practices.

3.6 TRIANGULATION IN A QUALITATIVE STUDY

Triangulation was used by combining multiple data sources; interviews, company reports, and regulatory documents to ensure consistency and reduce bias. For example, interview insights on AI governance challenges were checked against bank reports to validate themes. This increased the reliability of the findings and gave a full picture of AI adoption.

Also, cybersecurity experts from different levels of leadership (junior, middle, and senior) were interviewed to get a fair spread of perspectives and reduce bias. This ensured that the insights weren't limited to one level of leadership but reflected the whole view of AI governance challenges across different levels of leadership. Triangulation was used by combining multiple data sources; interviews, company reports, and regulatory documents, to ensure consistency and reduce bias. For example, interview insights on AI governance challenges were checked against bank reports to validate themes. This increased the reliability of the findings and gave a full picture of AI adoption.

3.7 VALIDATION OF THE INTERVIEW GUIDE

The interview guide has been validated through a pilot test conducted with a limited sample of cybersecurity experts. Based on the results from the pilot test, refinements to the guide have been made to ensure that the questions are clear, relevant, and well-tailored to the research objectives. This enhances the reliability and credibility of the data collection instrument. Iterative refinements meant that this guide was robust enough for nuanced insights.

3.8 CONCLUSION

This chapter presented the methodology used to investigate AI governance in cybersecurity. It outlined the philosophical orientation, case study design, data collection methods, ethical safeguards, triangulation, and validation strategies. The qualitative approach, grounded in interpretivism and executed through a case study of a prominent digital bank, provided the necessary depth and rigour to uncover governance insights from expert practitioners. The next chapter presents and analyses the findings derived from this methodology.

4. RESULTS

4.1 INTRODUCTION

This chapter presents the findings of the study on the use of artificial intelligence (AI) for cybersecurity in the banking industry in South Africa. The findings are based on in-depth interviews with cybersecurity experts, emphasizing governance insights. Results are consistent with the theoretical models (Chapter 2) i.e., Technology Acceptance Model (TAM) (Davis, 1989), Innovation Diffusion Theory (Rogers, 2003), and Institutional Theory. Responses are organised in such a way as to be in keeping with the research aims as presented in Chapter 1 and the methodological approach as presented in Chapter 3.

The research questions that guided the study include:

i. **Perception:** How do IT decision-makers in the South African banking industry perceive the role of AI in enhancing cybersecurity?
ii. **Attitude:** How do IT decision-makers in the South African banking industry view the adoption of AI for cybersecurity?
iii. **Drivers:** How do internal and external push factors influence the adoption of AI for cybersecurity in the South African banking industry?
iv. **Governance and Ethics:** How do IT decision-makers perceive the ethical and governance challenges related to AI use in cybersecurity within the South African banking industry?

These research questions align with the study objectives, which are to:

i. Determine the perceptions of IT decision-makers regarding the role of AI for cybersecurity.
ii. Ascertain the attitudes of IT decision-makers towards AI adoption for cybersecurity.
iii. Identify the drivers influencing AI adoption for cybersecurity.
iv. Examine governance and ethical challenges related to AI for cybersecurity.

The structure of this chapter is influenced by benchmarking findings from the literature on IT governance in public health care (Mangundu & Jokonya, 2024), while maintaining consistency with best practices in qualitative research. Results are discussed thematically, with each theme containing a detailed presentation of participant perceptions that is further underpinned by relevant literature when applicable.

4.2 DATA SOURCES

This table outlines the various data sources utilised in the study, highlighting their specific purposes in addressing the research questions and ensuring the comprehensiveness of the findings.

Data Source	Description	Purpose
Participant Interviews	In-depth qualitative interviews with cybersecurity experts from the South African banking sector.	To gather insights on perceptions, attitudes, and challenges of AI adoption.
Literature Review	Academic articles, industry reports, and frameworks related to AI and cybersecurity.	To contextualize findings within existing knowledge and theoretical frameworks.
Regulatory Documents	Key policies such as POPIA (Protection of Personal Information Act) and GDPR (General Data Protection Regulation).	To identify governance and compliance challenges linked to AI adoption.
Benchmarking Studies	Comparative insights from studies on IT governance in other sectors (e.g., public healthcare).	To inform best practices and enhance thematic analysis.

Table 2: Data Sources for the Study

4.3 THEMATIC ANALYSIS AND LINK TO RESEARCH QUESTIONS

In order to make sense of the qualitative data, a thematic analysis approach was taken. The analysis was organized around seven themes, which arose from the interviews conducted with participants. Each of the themes analyzed represents an important finding and relates to the research questions and goals of this study. The following sections provide a comprehensive analysis of these themes.

4.3.1 Theme 1: Perceived Benefits of AI for Cybersecurity

This theme is linked to question one: perception and deals with IT decision-makers' perception regarding the potential of AI in improving cybersecurity, particularly the transformational aspects of its use. Respondents cited AI's capability to enhance and improve threat detection, fraud attempts, and automated security responses. AI allows for active monitoring in conjunction with improved detection of novel attack attempts. This theme captures the transformational promise of AI in dealing with the intricacies and ever-changing landscape of cyber threats.

The results of this study demonstrate that AI significantly enhances cybersecurity by enabling more rapid and precise detection of threats. Participants highlighted that AI facilitates real-time monitoring and preemptive responses to cyber threats, which aligns with the findings of Tao et al. (2021). Tao et al. emphasized that AI's predictive analytics capabilities are crucial for identifying and mitigating cyber threats before they can cause significant harm.

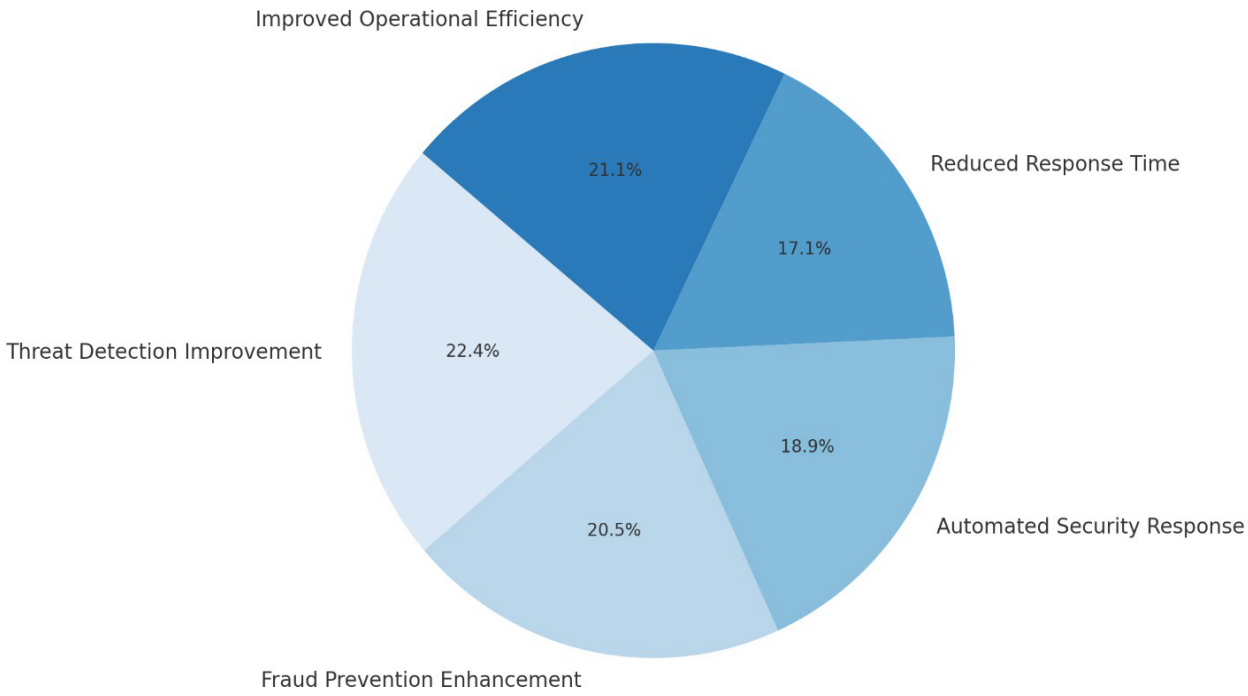
For example, Participant 3, Chief Digital Officer, noted, "AI has transformed cybersecurity by detecting anomalies faster than human analysts ever could. For example, we've prevented numerous incidents by flagging unusual data movements." This observation coincides with Tao et al.'s assertion that AI applications in cybersecurity can surpass human performance in tasks such as data analytics and anomaly detection.

Moreover, the study found that AI's ability to automate complex cybersecurity tasks reduces the burden on human analysts, allowing them to focus on more strategic activities. Participant 7, Information Security Officer, stated, "Cybersecurity is evolving, and AI is now at the forefront. We're seeing a shift from reactive security to proactive defense mechanisms powered by AI." This finding is consistent with Tao et al.'s conclusion that AI can improve the efficiency and effectiveness of cybersecurity systems by automating routine tasks and enhancing threat detection capabilities.

In summary, the results of this study align with the insights provided by Tao et al., demonstrating that AI's advanced capabilities in predictive analytics and automation significantly enhance cybersecurity measures. These findings underscore the transformative potential of AI in the cybersecurity domain, particularly in the banking sector, where rapid and accurate threat detection is paramount

Perceived Benefits of AI for Cybersecurity (Research Question 1)

Figure 7, below, illustrates the various perceived benefits of AI for cybersecurity as identified by the study participants. The figure highlights key areas such as enhanced threat detection, improved response times, and increased operational efficiency. These benefits underscore the transformative potential of AI in strengthening cybersecurity measures within the banking sector. The visual representation helps to summarize and emphasize the positive impacts of AI adoption as reported by the respondents.



.

Figure 7: Perceived Benefits of AI for Cybersecurity (Source: Participant insights)

4.3.2 Theme 2: Challenges in AI Adoption

This theme is linked to question three: drivers, and focuses on the internal and external factors that affect the adoption of AI, such as integration with legacy systems, lack of relevant skills, and costs of deploying AI systems. Even with prescriptive AI benefits, experts pointed out some barriers like lack of integration with modern systems, deficiency of AI professionals, and expensive implementation processes. This theme focuses on the adoption challenges that many organizations have to deal with in the attempt to utilize technologies such as artificial intelligence.

The results of this study reveal significant barriers to AI adoption, including integration with legacy systems, expertise shortages, and high implementation costs. These challenges highlight the importance of technological readiness and workforce development in ensuring successful AI implementation. Participants emphasized that updating legacy systems to be compatible with advanced AI models requires substantial investment and time, which aligns with the findings of Mamela et al. (2023). Mamela et al. identified similar technical and resource challenges in the South African context.

For instance, Participant 5, Senior Information Security Officer, stated, "Many banks hesitate to adopt AI because their legacy infrastructure is not compatible with advanced AI models. Updating these systems requires significant investment and time." This observation coincides with Mamela et al.'s conclusion that legacy infrastructure poses a significant barrier to AI adoption.

Additionally, the study found that the shortage of machine learning experts further complicates AI adoption. Participant 8, Agile Coach & AI Expert, noted, "The problem isn't just deploying AI—it's maintaining and continuously training these systems. We don't have enough machine learning experts to do this effectively." This finding is consistent with Lourens et al. (2022), who emphasized the importance of data quality and infrastructure readiness in AI implementation.

In summary, the results of this study align with the insights provided by Mamela et al. and Lourens et al., demonstrating that technical and resource challenges are significant barriers to AI adoption in the South African banking sector. These findings underscore the need for strategic investments in infrastructure and workforce development to facilitate successful AI integration.

Challenges in AI Adoption (Research Question 3)

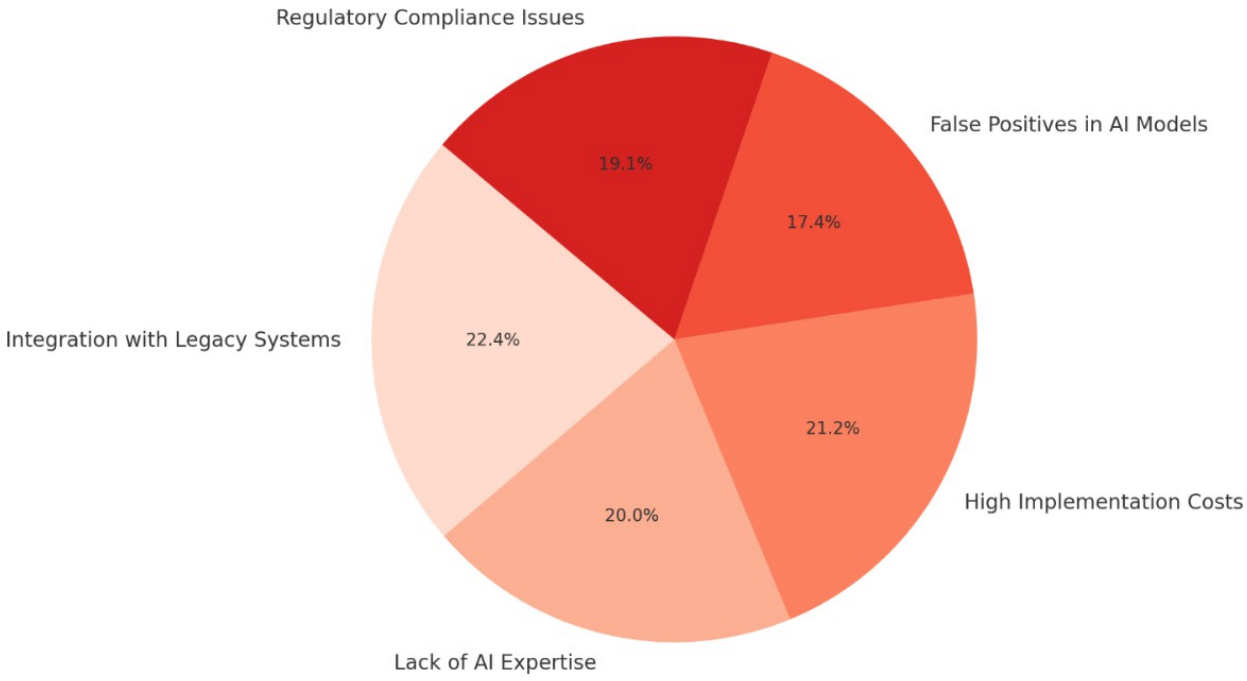


Figure 8: Challenges in AI Adoption (Source: Participant insights)

Figure 8, above, depicts the challenges associated with AI adoption in the banking sector, as identified by the participants. The figure outlines key barriers such as integration with legacy systems, lack of expertise, and high implementation costs. These challenges highlight the complexities and resource requirements involved in successfully implementing AI technologies. The visual summary provides a clear overview of the obstacles that organizations must address to leverage AI effectively.

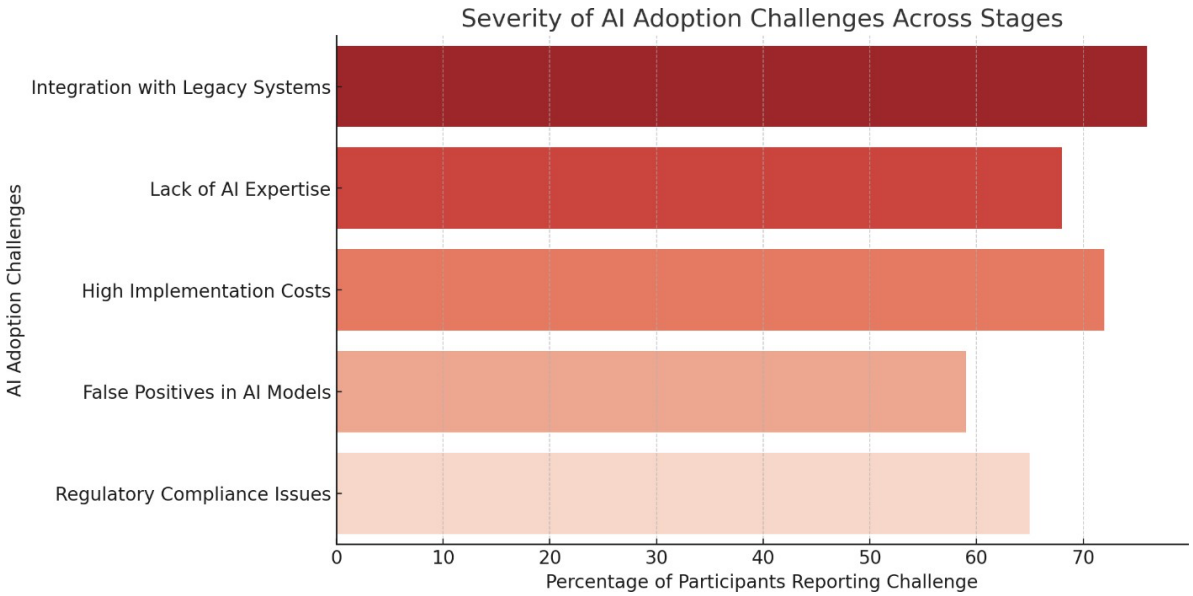


Figure 9: Severity of AI Adoption Challenges Across Stages (Source: Participant insights)

Figure 9 illustrates the severity of AI adoption challenges across different stages of implementation. The figure categorizes challenges into various stages, such as initial adoption, integration, and maintenance, and assesses their impact. This visual representation helps to understand how challenges evolve and vary throughout the AI adoption process. It emphasizes the need for strategic planning and resource allocation at each stage to mitigate these challenges effectively.

4.3.3 Theme 3: Regulatory and Ethical Concerns

This theme is linked to question four: governance and ethics, and speaks directly on compliance and ethics issues arising from AI's implementation of the concepts of compliance, prejudice, and transparency. The participants stated concerns regarding adherence to data protection laws such as the POPIA and GDPR as well as AI's ethical decision making. This theme speaks to the need to adopt AI within the set regulations and ethical frameworks.

The results of this study highlight significant governance and ethical concerns related to AI adoption, particularly compliance with data protection regulations such as POPIA and GDPR. Participants emphasized the importance of transparency and ethical oversight to prevent unintended bias in AI-driven decision-making. These findings align with the insights of Taddeo et al. (2019), who emphasized the need for explicit mechanisms of ethical control to mitigate risks of bias and ensure accountability in AI systems.

For example, Participant 2, Information Security Officer, stated, "There's always a concern about how AI makes security-related decisions, especially when it comes to customer transactions being flagged as fraudulent. How do we explain these decisions to regulators?" This observation coincides with Taddeo et al.'s assertion that transparency in AI decision-making is crucial for regulatory compliance and building trust among stakeholders.

Moreover, the study found that ethical governance is essential to address biases in AI systems. Participant 9, Information Security Officer, noted, "Transparency is key. AI models must be explainable; otherwise, we risk introducing bias into security decision-making." This finding is consistent with Chauhan and Keprate (2022), who emphasized the necessity of developing clear standards and frameworks to address ethical concerns in AI adoption.

In summary, the results of this study align with the insights provided by Taddeo et al. and Chauhan and Keprate, demonstrating that regulatory and ethical concerns are critical considerations in AI adoption. These findings underscore the importance of transparency, accountability, and adherence to regulatory requirements in AI implementations.

Regulatory and Ethical Concerns in AI Adoption (Research Question 4)

Figure 10, below, highlights the regulatory and ethical concerns associated with AI adoption in the banking sector. The figure identifies key issues such as data privacy, algorithmic bias, and compliance with regulations like POPIA and GDPR. These concerns underscore the importance of ethical oversight and transparent governance in AI implementations. The visual summary provides a concise overview of the critical ethical and regulatory challenges that organizations must navigate.

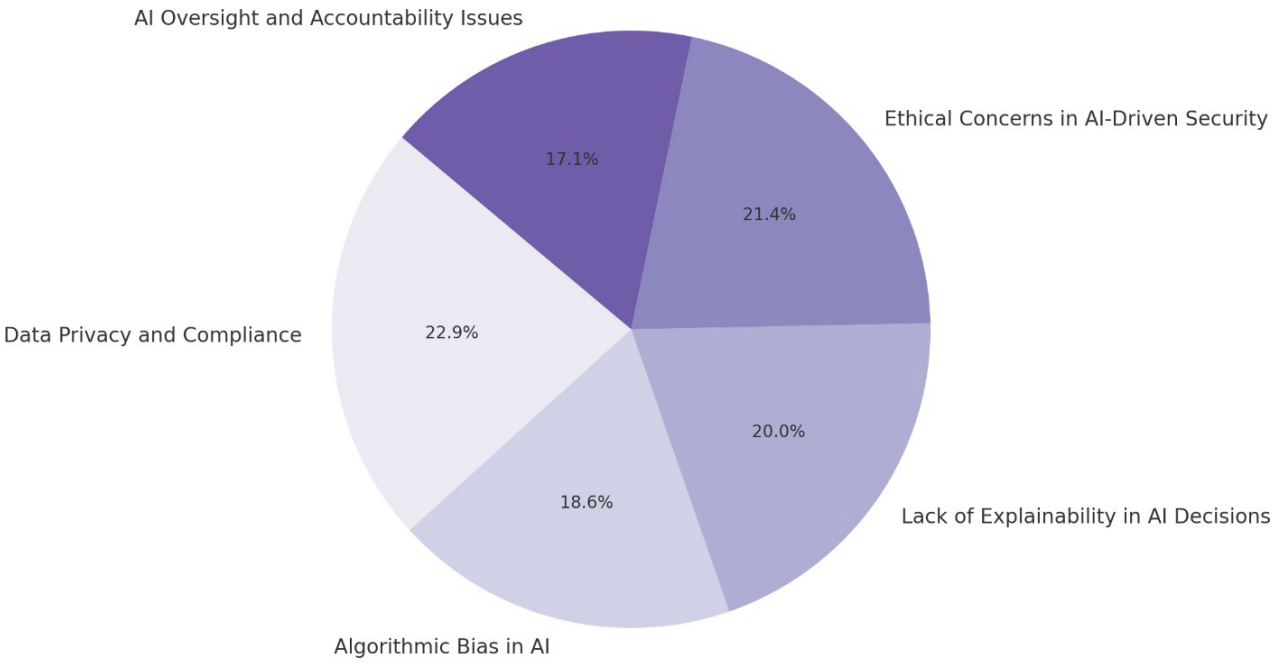


Figure 10: Regulatory and Ethical Concerns in AI Adoption (Source: Participant insights)

Correlation Between AI Benefits, Challenges, and Regulatory Concerns

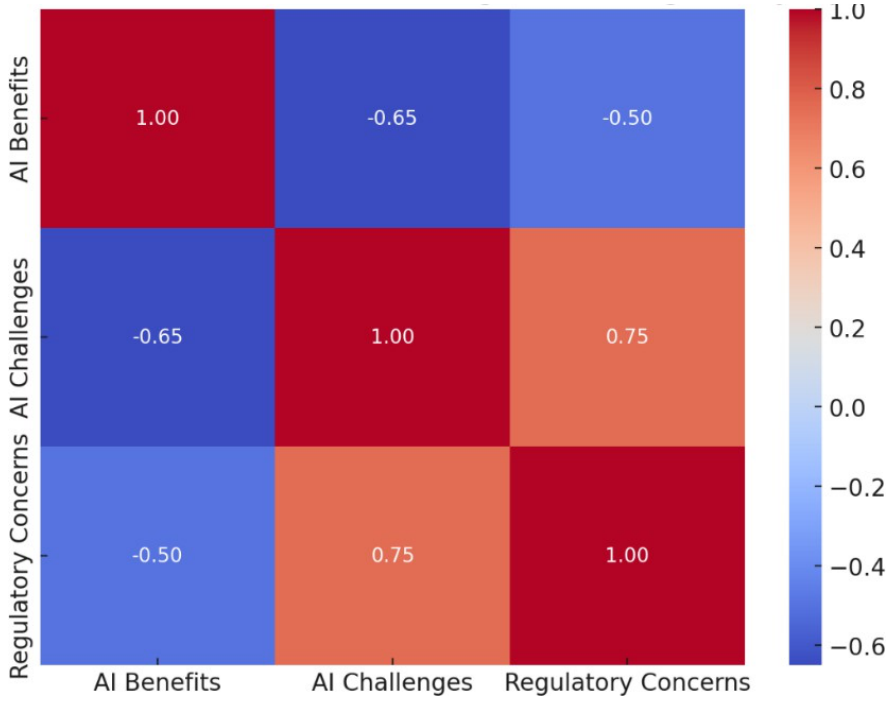


Figure 11: Correlation Between AI Benefits, Challenges, and Regulatory Concerns (Source: Participant insights)

Figure 11, above, illustrates the correlation between the benefits of AI, the challenges of AI adoption, and regulatory concerns. The figure shows how these elements interact and influence each other, highlighting the complex dynamics involved in AI implementation. This visual representation helps to understand the interconnected nature of AI adoption factors and the need for a balanced approach to maximize benefits while addressing challenges and regulatory requirements.

4.3.4 Theme 4: Benefits and Ethical Oversight

This theme is linked to question four: governance and ethics, and enriches the debate on governance and ethics by emphasizing the need for ethical control and responsible governance measures to mitigate unintended effects. While AI automation facilitates greater efficiency, participants noted the need for ethical oversight to prevent unintended bias in security-related decision-making. This theme revolves around balancing the efficiency gains provided by AI with responsible governance practices.

The results of this study highlight the dual importance of AI's efficiency gains and the need for robust ethical oversight. Participants emphasized that while AI automation enhances operational efficiency, it is crucial to implement ethical governance measures to prevent unintended biases and ensure accountability. These findings align with the insights of Dangi et al. (2023), who noted that ethical control is vital in managing potential biases and ensuring AI aligns with organizational goals.

For instance, Participant 10, Information Security Officer, stated, "AI is making my job easier by automating threat detection, but we still need strong ethical governance. The systems must be explainable to all stakeholders." This observation coincides with Dangi et al.'s assertion that ethical oversight is essential to mitigate biases and ensure transparency in AI systems.

Moreover, the study found that AI models must work seamlessly with existing IT frameworks while ensuring biases in the data do not skew results. Participant 1, Information Security Specialist, noted, "AI models must work seamlessly with existing IT frameworks, but we must ensure biases in the data do not skew results." This finding is consistent with Nikolskaia and Naumov (2021), who argued that integrating AI governance into existing regulatory systems enhances trust and transparency in operations.

In summary, the results of this study align with the insights provided by Dangi et al. and Nikolskaia and Naumov, demonstrating that ethical oversight is crucial in balancing AI's efficiency gains with responsible governance practices. These findings underscore the importance of implementing robust ethical frameworks to ensure equitable and accountable AI adoption.

4.3.5 Theme 5: Organisational Readiness and Strategic Alignment

This theme is linked to question two: attitude, and explores attitudes towards adopting artificial intelligence through the lens of organizational readiness, cultural openness, and leadership commitment, which reflect the attitudes needed for successful AI adoption. The respondents highlighted the importance of organizational readiness and leadership commitment. This theme also looks at how internal factors influence the success of AI adoption initiatives.

The results of this study emphasize the critical role of organizational readiness, cultural openness, and leadership commitment in successful AI adoption. Participants highlighted that fostering an environment that supports innovation and aligns AI initiatives with broader business objectives is essential. These findings align with the insights of Kshetri (2021), who highlighted the critical role of leadership and organizational culture in AI adoption success.

For example, Participant 6, Chief Security Officer, stated, "To successfully adopt AI, we need leaders who can articulate a vision that aligns AI projects with broader business objectives." This observation coincides with Kshetri's assertion that leadership commitment is crucial for fostering a supportive environment for AI adoption.

Moreover, the study found that cultural readiness is often overlooked but is essential for successful AI integration. Participant 11, Chief Information Security Officer, noted, "Cultural readiness is often overlooked. Teams need to feel empowered and adequately trained to embrace AI tools." This finding is consistent with Barletta et al. (2022), who emphasized the importance of cross-functional collaboration and training initiatives to foster organizational readiness.

In summary, the results of this study align with the insights provided by Kshetri and Barletta et al., demonstrating that organizational readiness, cultural openness, and leadership commitment are

critical enablers of successful AI adoption. These findings underscore the importance of fostering a supportive environment for innovation and aligning AI initiatives with broader business objectives.

Organisational Readiness for AI Adoption (Research Question 2)

Figure 12, below, depicts the factors contributing to organizational readiness for AI adoption. The figure outlines key elements such as leadership commitment, cultural openness, and strategic alignment. These factors are critical enablers of successful AI integration within organizations. The visual summary emphasizes the importance of fostering a supportive environment and aligning AI initiatives with broader business objectives to ensure effective adoption.

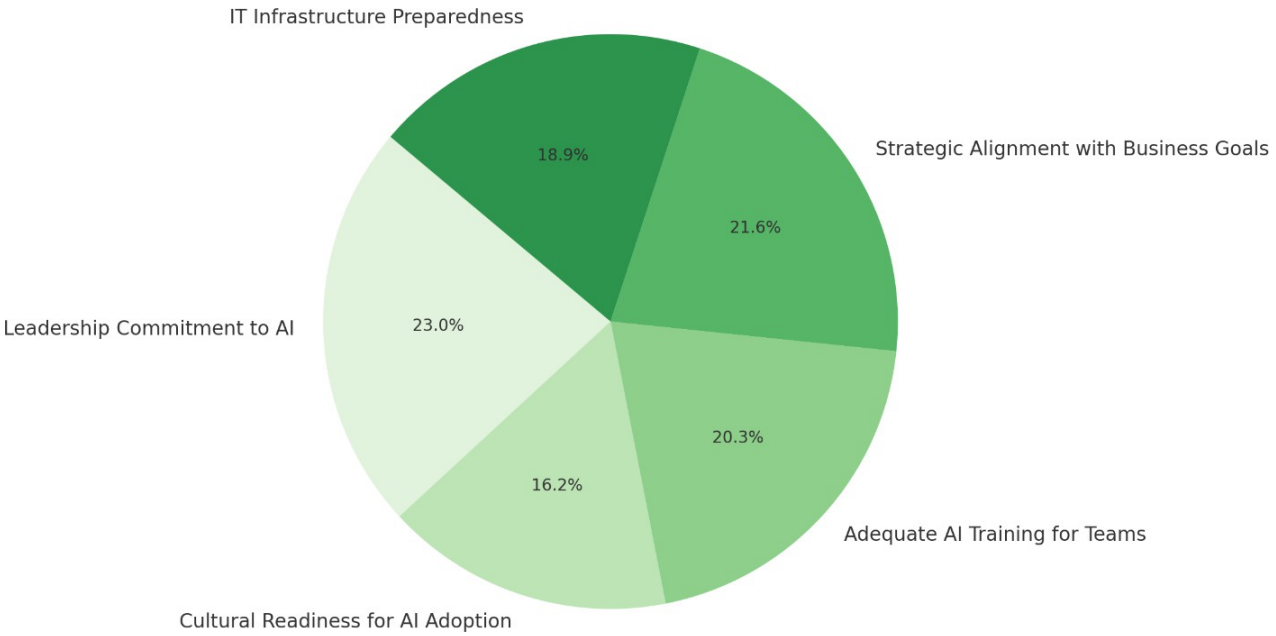


Figure 12: Organisational Readiness for AI Adoption (Source: Participant insights)

This theme aligns with the findings by Kshetri (2021), who highlighted the critical role of leadership and organisational culture in AI adoption success. Barletta et al. (2022) also emphasized the importance of cross-functional collaboration and training initiatives to foster organisational readiness.

4.3.6 Theme 6: Trust and Transparency in AI-Driven Cybersecurity

This theme is linked to question three: drivers, and looks at the drivers of trust as critical factors influencing readiness to adopt artificial intelligence, specifically the need for explainability and

transparency in AI decision-making. The respondents raised concerns over trust and transparency in AI-supported decisions, highlighting the need for explainability and accountability. This theme highlights the importance of good communication and governance in the development of trust in AI systems.

The results of this study underscore the importance of trust and transparency in AI-driven cybersecurity. Participants emphasized that AI models must be explainable to build confidence among users and regulators. These findings align with the insights of Taddeo et al. (2019), who emphasized that transparent AI systems are essential for gaining user trust and achieving regulatory compliance.

For example, Participant 4, Data Protection Officer, stated, "One of our biggest challenges is explaining AI-driven security decisions to both internal teams and regulators. We need better transparency mechanisms to avoid disputes." This observation coincides with Taddeo et al.'s assertion that transparency in AI decision-making is crucial for regulatory compliance and building trust among stakeholders.

Moreover, the study found that AI models must be designed with transparency in mind to ensure that decisions can be easily understood by humans. Participant 9, Information Security Officer, noted, "AI models must be designed with transparency in mind. If the system flags a transaction as fraudulent, we need to be able to explain why, in a way that humans can understand." This finding is consistent with Abraham et al. (2023), who highlighted the importance of humanizing machine intelligence to enhance its acceptance and perceived reliability.

In summary, the results of this study align with the insights provided by Taddeo et al. and Abraham et al., demonstrating that trust and transparency are critical drivers of AI adoption in cybersecurity. These findings underscore the importance of explainable AI models to build confidence among users and regulators.

4.3.7 Theme 7: The Role of Human Oversight in AI-Enabled Security

This theme is linked to question four: governance and ethics, and brings into focus the importance of human involvement as part of governance and ethical structures in managing AI-assisted cybersecurity systems. Despite the automation that AI provides, participants emphasized the utmost importance of human intervention, particularly in resolving complex security breaches. This theme examines the complementary interaction between AI and human expertise.

The results of this study highlight the indispensable role of human oversight in AI-enabled security systems. Participants emphasized that while AI can automate many aspects of cybersecurity, human expertise is crucial for managing complex or ambiguous security incidents. These findings align with the insights of Rawat et al. (2022), who suggested a synergistic approach that combines AI capabilities with human analytical skills to enhance security outcomes.

For example, Participant 8, Agile Coach & AI Expert, stated, "AI does a great job at detecting anomalies, but human oversight is still critical. We need skilled professionals to assess and make final decisions on flagged threats." This observation coincides with Rawat et al.'s assertion that AI systems should operate in conjunction with human decision-makers to ensure nuanced and ethically sound outcomes.

Moreover, the study found that a hybrid approach, where AI works alongside human analysts, is essential for maintaining security effectiveness. Participant 5, Senior Information Security Officer, noted, "We can’t just rely on AI alone. A hybrid approach—AI working alongside human analysts—is the only way to maintain security effectiveness." This finding is consistent with Taddeo et al. (2019), who highlighted the complementary roles of human oversight and AI in achieving effective cybersecurity outcomes.

In summary, the results of this study align with the insights provided by Rawat et al. and Taddeo et al., demonstrating that human oversight is crucial in AI-enabled security systems. These findings underscore the importance of a hybrid approach that combines AI capabilities with human expertise to ensure effective and ethical cybersecurity practices.

4.4 VALIDATION OF RESULTS

Validation of results is a crucial stage in qualitative research, ensuring accuracy, credibility, and reliability. Creswell and Poth (2018) highlight that validation enhances the trustworthiness of qualitative studies by verifying that the findings genuinely reflect participants' views. In this study, validation was achieved through follow-up discussions with participants, allowing them to review and confirm the accuracy of the themes derived from their interviews. This approach, known as member checking, is widely recognized for reducing researcher bias and strengthening the credibility of qualitative findings (Lincoln & Guba, 1985). By engaging participants in this process, the study ensured that misinterpretations were identified and corrected, reinforcing the reliability of the findings.

Moreover, participants were shown preliminary results and asked to confirm or dispute the interpretations, allowing for direct feedback that refined the accuracy of thematic analysis. Birt et al. (2016) argue that member validation enhances qualitative research by incorporating participant insights into the final analysis, ensuring that conclusions are grounded in their lived experiences. Any disagreements were addressed through further clarification and discussion, following an iterative approach that Morse et al. (2002) describe as essential for maintaining the integrity of qualitative research. This process ensured that the themes accurately represented the views of experts, ultimately contributing to the robustness of the study.

Participant insights during the validation process reinforced key findings: "AI adoption is gaining traction, but we must take a structured approach to implementation." (Participant 6, Chief Security Officer)

"Our teams recognize AI’s potential, but ethical concerns must remain a top priority." (Participant 11, Chief Information Security Officer)

By systematically validating the results through participant feedback, the study strengthened its credibility and provided a more comprehensive understanding of AI governance in cybersecurity.

4.5 CONCLUSION

The results presented in this chapter reveal that AI adoption in cybersecurity offers immense potential for enhancing threat detection and operational efficiency. Participants highlighted various advantages of AI, including its ability to automate threat detection, reduce response times, and bolster cybersecurity defenses proactively. However, alongside these benefits, several significant challenges emerged, particularly related to regulatory compliance, ethical oversight, integration with legacy systems, and organisational readiness.

Themes such as trust and transparency in AI-driven cybersecurity and the indispensable role of human oversight emphasize the need for a balanced approach to AI adoption—leveraging its strengths while addressing its limitations. Key barriers, such as a lack of expertise, high implementation costs, and concerns about bias in decision-making, were also evident.

This chapter provides a foundation for Chapter 5: Discussion of Findings, where these insights will be critically interpreted in the context of existing literature and theoretical frameworks. Chapter 5 will examine how the findings align with the Technology Acceptance Model (TAM), Innovation Diffusion Theory (IDT), and Institutional Theory. The discussion will provide a comprehensive analysis of how these findings contribute to the broader understanding of AI adoption in cybersecurity and offer actionable recommendations for addressing the challenges identified.

5. DISCUSSION OF FINDINGS

5.1 INTRODUCTION

This chapter presents analysis of the findings outlined in Chapter 4, providing a critical analysis in line with relevant theory and existing literature. The discussion addresses the research questions, particularly enhancing our understanding of artificial intelligence (AI) adoption in the context of cybersecurity within South Africa's banking industry. In addition, this chapter delves into practical implications, policy considerations, and potential areas of future research that arise from these results. The narrative is organized around themes that relate to those presented in Chapter 4.

5.2 INTERPRETATION OF KEY THEMES

5.2.1 Perceived Benefits of AI for Cybersecurity

The results indicate that AI has transformative potential in the sphere of cybersecurity, specifically in improving threat detection, protection against fraud, and optimization of business processes in general. The results concur with Tao et al. (2021), noting that AI's capability to forecast and predict cyberattacks has become a key trend across the world in the sphere of cybersecurity. The current research depicts that, in particular in South Africa's banking institutions, AI adoption is contextual in nature, depending on resource constraints and regulation requirements. The observed discrepancies between local contexts and global trends point to a need to tailor strategies to AI adoption in developing economies. The participants also agreed that AI's capability to monitor events in real-time facilitates a preemptive response to threats, hence shortening response times and strengthening overall security systems.

Notwithstanding the evidence offered by Tao et al. (2021) of artificial intelligence applications of predictive analytics across a global scale, participants in this study were more cautious in their approach in the banking sector of South Africa owing to certain contextual challenges such as financial aspects and regulation limitations. Conceptually, this is in line with the Technology Acceptance Model (TAM), in that perceived usefulness of AI systems is key to their adoption. The highlighted benefits of participants point towards a need to increase the perceived usefulness of AI solutions to enable their more expansive adoption and organizational integration.

5.2.2 Challenges in AI Adoption

The participants noted various challenges to artificial intelligence adoption, such as challenges in AI integration in legacy systems, a lack of enough experts, and high installation expenses. The observations agree with those of Mamela et al. (2023), who also found similar technical and resource challenges in the South African context. However, in contrast to Mamela et al. (2023), participants in this study noted more intense structural challenges such as legacy infrastructure and weak integration capabilities. Lourens et al. (2022) also highlighted infrastructure readiness and data quality as key enablers, a view that agrees with technical challenges noted among participants. The cross-cutting themes of challenges across various sectors indicate both the extent of challenges that cut across sectors and also those that are unique to the banking sector. The observations concur with those of Mamela et al. (2023) and Lourens et al. (2022), who also noted technical and resource constraints as key adoption barriers in organizations in South Africa.

Notably, whereas Mamela et al. (2023) indicated a deficiency of leadership support as a key challenge, participants in this study emphasized more intense structural challenges such as legacy infrastructure. This difference in perceived challenges indicates a need for context-based studies to better understand challenges to AI adoption. The challenges encountered can be explained using the Innovation Diffusion Theory (IDT), which highlights the role of simplicity in adopting technologies. The technical challenges of incorporating AI in legacy infrastructure point to a need to put organizational readiness in line with technology to allow easy adoption.

5.2.3 Regulatory and Ethical Concerns

Governance and ethical challenges have emerged as key concerns, with participants stressing the need for observance of data protection legislations, such as POPIA and GDPR. The observations concur with the claims of Taddeo et al. (2019), who emphasized the need for explicit mechanisms of ethical control to help avert threats of bias and transparency in artificial intelligence systems. Similarly, Chauhan and Keprate (2022) emphasized that institutions need to embrace standardized frameworks to obtain ethical as well as legislative conformity in adopting AI technologies. The similarity in observations serves to underscore a collective global concern in tackling challenges of ethics coupled with revealing the unique focus on conformity to regulation in the South African context. The observations concur with Taddeo et al.'s (2019) and Chauhan and Keprate's (2022) studies, which underscored the importance of transparency and ethical control in adopting AI solutions. Contrarily,

in a departure from Taddeo et al.'s (2019) focus on the ethical consequences of AI algorithmic bias, participants in this study highlighted the operational challenges in satisfying conformity to regulation requirements. The observation indicates that even though there is a concern of international nature in terms of ethics, institutions in South Africa place more concern on concrete governance challenges. The observations also shed light on the role of Institutional Theory in guiding organizational behavior. The demand for accountability coupled with ethical governance in AI adoption is driven by conformity to regulation frameworks coupled with institutional forces. In order to meet stakeholder expectations and build trust, institutions need to devise clear-cut ethical frameworks and institutionalize them in their AI strategies.

5.2.4 Trust and Transparency in AI Systems

Trust and transparency emerged as essential drivers of AI adoption. These findings align with Taddeo et al. (2019), who emphasized that trust in AI systems is contingent on their transparency and ethical design, which help build confidence among users. Similarly, Abraham et al. (2023) highlighted the psychological aspects of trust, underscoring the importance of making AI systems human-centric to enhance their acceptability. However, while Abraham et al. (2023) focused on the emotional dimensions of trust, this study's participants stressed operational transparency, such as the need for explainability in AI-driven decisions to satisfy regulatory requirements and address stakeholder concerns. Participants emphasized the need for explainable AI systems to build confidence among users and regulators. These findings align with Taddeo et al. (2019) and Abraham et al. (2023), who highlighted the importance of humanizing AI to enhance its acceptability.

Interestingly, Abraham et al. (2023) focused on the psychological dimensions of trust in AI systems, while participants in this study emphasized operational transparency, such as the ability to explain AI-driven decisions to regulators. This operational focus reflects the practical challenges faced by South African institutions in gaining stakeholder trust. Theoretical insights from TAM suggest that perceived ease of use and trustworthiness significantly influence user acceptance. Transparent AI systems not only address regulatory requirements but also foster a culture of trust and collaboration within organizations.

5.2.5 The Role of Human Oversight

The findings underscore the crucial need for human supervision in AI-based security systems. As artificial intelligence is increasingly utilized to boost business processes in terms of efficiency, participants indicated that human knowledge is required to be combined with AI capabilities to manage complex security scenarios effectively. The findings support the viewpoint given by Rawat et al. (2022), suggesting a synergistic approach that unites AI capabilities with human analytical capabilities to build a stronger security system. In contrast to the view of Rawat et al. (2022), that highlighted the need for expert training in sophisticated economies, this work brings to light a more basic concern regarding acquiring a skilled human resource in resource-constrained settings, such as in South Africa. In addition, it highlights the need for continuous learning and upgradation of skills for professionals to coexist in harmony with AI technologies. Human supervision is crucial in ensuring accountability and adherence to ethic principles in AI-based security processes.

5.2.6 Comparative Analysis with Benchmarked Studies

The section compares results of this study to those of Mangundu and Jokonya (2024) and other benchmarked studies:

Perceived Benefits of AI: Where Mangundu and Jokonya (2024) found that IT governance in healthcare was mainly driven by process automation, participants in this study highlighted AI's use in threat detection and defense against cyberattacks. This indicates sectoral variance in AI adoption.

Challenges in Adoption: Both studies found infrastructural and resource limitations to be primary challenges in adoption. Mangundu and Jokonya (2024), however, indicated more leadership and policy support in overcoming such challenges, compared to this study that highlighted technical challenges in adoption in South African banking.

Ethical and Regulatory Concerns: Similarly to Mangundu and Jokonya (2024), this study found concern over governance and compliance issues. The banking sector participants, though, indicated more seriousness in dealing with protection of data rules.

5.3 CONCLUSION

The chapter presents a critical analysis of the results presented in Chapter 4, interpreting these in the light of existing theory and literature. The discussion highlighted the transformative potential of AI in the sphere of cybersecurity, challenges in adopting it, and the importance of ethical governance and organizational readiness. It set aside the results of the study in juxtaposition to existing studies, identifying areas of consistency and inconsistency, in particular in the sphere of banking in South African contexts.

The theoretical integration provided further insights into how frameworks such as TAM, IDT, and Institutional Theory apply to the findings. Practical implications were outlined, offering actionable recommendations for improving AI adoption and governance in cybersecurity. Limitations of the study were acknowledged, and recommendations for future research were proposed to address gaps and extend the findings to broader contexts.

These discussions provide a solid foundation for the next chapter, **Chapter 6: Conclusion**, which will summarize the study's key contributions, revisit its objectives, and offer final reflections on the implications for theory, practice, and policy. Chapter 6 will also emphasize the significance of these findings in shaping the future of AI-driven cybersecurity in emerging economies such as South Africa.

6. CONCLUSION

This chapter concludes the study by summarizing the key findings, emphasizing its contributions to theory and practice, and revisiting the research objectives and questions. It also outlines the limitations of the study and provides recommendations for practitioners, policymakers, and future research. The chapter concludes with final reflections on the significance of the study in advancing the adoption of artificial intelligence (AI) for cybersecurity in the South African banking industry.

6.1 SUMMARY OF KEY FINDINGS

The study explored the adoption of AI for cybersecurity in the South African banking industry, focusing on governance insights from cybersecurity experts. The findings, presented in Chapter 4 and discussed in Chapter 5, are summarized as follows:

6.1.1 **Perceived Benefits of AI:** AI was found to enhance threat detection, fraud prevention, and operational efficiency. These benefits were viewed as transformative, particularly in enabling proactive cybersecurity measures. However, the realization of these benefits is contingent upon overcoming contextual challenges such as regulatory constraints and resource limitations.

6.1.2 **Challenges in AI Adoption:** Significant barriers to AI adoption include integration with legacy systems, expertise shortages, and high implementation costs. These challenges highlight the importance of technological readiness and workforce development in ensuring successful AI implementation.

6.1.3 **Regulatory and Ethical Concerns:** Governance and ethical issues, particularly compliance with data protection regulations (e.g., POPIA and GDPR), emerged as critical concerns. Ethical oversight and transparency were identified as essential for addressing bias and ensuring accountability in AI-driven decision-making.

6.1.4 **Trust and Transparency:** Trust in AI systems was deemed essential for their adoption, with participants emphasizing the need for explainable and transparent AI models to satisfy stakeholder and regulatory expectations.

6.1.5 **Organizational Readiness and Strategic Alignment:** Leadership commitment, cultural preparedness, and strategic alignment were found to be critical enablers of successful AI adoption. Organizations must foster an environment that supports innovation while aligning AI initiatives with broader business objectives.

6.1.6 **Human Oversight:** Despite the efficiency gains from AI, human oversight was deemed indispensable, particularly for managing complex or ambiguous security incidents. A hybrid approach that combines AI capabilities with human expertise was advocated.

6.1.7 **Benefits and Ethical Oversight:** Participants emphasized that while AI offers numerous advantages, robust ethical oversight mechanisms are necessary to mitigate unintended consequences and ensure equitable and responsible outcomes.

These findings provide a comprehensive understanding of the opportunities and challenges associated with AI adoption for cybersecurity, particularly in the context of the South African banking industry.

6.2 RELEVANCE TO RESEARCH OBJECTIVES AND QUESTIONS

The study achieved its objectives and addressed the research questions as follows:

Objective 1: Determine the perceptions of IT decision-makers regarding the role of AI for cybersecurity.

- ✓ **Addressed by:** The findings revealed that participants viewed AI as transformative in enhancing cybersecurity, particularly in its ability to improve threat detection, fraud prevention, and operational efficiency. These perceptions align with the Technology Acceptance Model (TAM), which emphasizes the role of perceived usefulness in influencing technology adoption.

Objective 2: Ascertain the attitudes of IT decision-makers towards AI adoption for cybersecurity.

- ✓ **Addressed by:** Participants expressed cautious optimism, balancing enthusiasm for AI's benefits with concerns about challenges such as high implementation costs, legacy systems, and expertise shortages. This duality of attitudes reflects the complexity of decision-making in technology adoption and highlights the need for organizational readiness.

Objective 3: Identify the drivers influencing AI adoption for cybersecurity.

- ✓ **Addressed by:** Key drivers included operational efficiency, trust, and the potential for proactive threat detection. However, barriers such as regulatory compliance, data quality issues, and infrastructure limitations were also significant. These findings underscore the interplay of enablers and obstacles, consistent with the principles of Innovation Diffusion Theory (IDT).

Objective 4: Examine governance and ethical challenges related to AI for cybersecurity.

- ✓ **Addressed by:** The study identified governance and ethical concerns, particularly compliance with data protection regulations (e.g., POPIA, GDPR) and the risks of bias in AI decision-making. Participants emphasized the importance of ethical oversight and transparency, aligning with Institutional Theory's focus on regulatory and societal pressures.

By addressing these objectives, the study contributes to a nuanced understanding of the factors shaping AI adoption for cybersecurity in the South African banking industry. It also highlights the importance of aligning organizational strategies with technological, ethical, and regulatory considerations.

6.3 THEORITICAL CONTRIBUTION

The study advances theoretical understanding by extending existing frameworks such as the Technology Acceptance Model (TAM), Innovation Diffusion Theory (IDT), and Institutional Theory to the domain of AI adoption in cybersecurity. Specifically, it demonstrates how these theories can explain the interplay between organizational readiness, perceived usefulness, regulatory pressures, and ethical considerations in an emerging market context. Unlike many studies that focus on developed economies, this research provides a nuanced understanding of AI adoption within the South African banking sector, contributing to the underexplored area of technology diffusion in emerging markets. For instance, it identifies unique challenges such as stringent regulatory compliance and limited infrastructure readiness. The study also bridges theory and practice by linking theoretical perspectives with empirical data, highlighting the role of governance and trust-building mechanisms in overcoming barriers to AI adoption. By incorporating the influence of ethical and regulatory pressures as external factors, the study expands IDT and enriches Institutional Theory by demonstrating how organizational responses to regulatory compliance pressures are shaped by both external expectations and internal governance capabilities.

6.4 CONTRIBUTION TO PRACTICE

In terms of practical contributions, the study offers actionable insights for practitioners and policymakers. Organizations can use the findings to formulate strategies to overcome challenges such as expertise shortages, high costs, and integration with legacy systems. By adopting phased approaches to modernization, banks can ensure incremental benefits while managing risks. The study

emphasizes the importance of leadership buy-in and cultural transformation to foster a conducive environment for AI adoption, including targeted training programs to bridge the skills gap and align teams with organizational objectives. Additionally, the study highlights the necessity of developing transparent and explainable AI models to address regulatory and ethical concerns, which is particularly relevant for organizations aiming to build trust among stakeholders. Policymakers are guided to create flexible, context-sensitive regulations that balance innovation with accountability, addressing unique socio-economic and technological constraints. Encouraging collaboration across the banking sector to establish shared standards for AI governance can reduce duplication of efforts and foster a cohesive approach to cybersecurity challenges.

6.5 STUDY LIMITATION

Despite providing useful insights, the study has certain limitations that should be acknowledged. The focus on the banking sector in South Africa limits the generalizability of the findings to other sectors and geographic locations. While the qualitative approach offers depth, it may not capture the entire spectrum of perspectives on AI adoption. The relatively small sample size of cybersecurity practitioners may also not fully represent the diverse experiences and viewpoints within the industry. These limitations suggest the need for follow-up studies to build on the findings and address these constraints. Future research should consider expanding the scope to include more industries and geographic contexts to enhance the generalizability of the results. Employing quantitative research methods could support the findings and explore additional variables influencing AI adoption. Longitudinal analyses would be valuable in examining the long-term effects of AI adoption on organizational performance and cybersecurity outcomes. Comparative research across different emerging economies could also provide insights into prevailing patterns and unique challenges in AI adoption. By addressing these recommendations, future studies can contribute to a more comprehensive understanding of AI adoption in cybersecurity and inform strategies for effective implementation.

6.6 FUTURE RESEARCH

The study presents several recommendations for practice and future research. Organizations should improve technological readiness by investing in legacy system upgrades to facilitate easy AI integration. Continuous training programs are essential to equip employees with the necessary skills to work effectively alongside AI systems. Implementing robust ethical governance mechanisms is

crucial to ensure transparency and accountability in AI-driven decision-making. Engaging stakeholders, including regulators and customers, is vital to build trust and enable smooth AI adoption. Future research should broaden the contexts of inquiry to include more sectors and geographic areas, enhancing the generalizability of the findings. Employing quantitative research methods can support the evidence and explore additional variables that affect AI adoption. Longitudinal analyses are recommended to investigate the long-term impacts of AI adoption on organizational performance and cybersecurity outcomes. Comparative research across different emerging economies can provide valuable insights into common patterns and unique challenges in AI adoption. By addressing these recommendations, future studies can contribute to a more comprehensive understanding of AI adoption in cybersecurity and inform strategies for effective implementation.

6.7 CONCLUDING REFLECTIONS

The current research is a contribution to the growing body of literature in artificial intelligence adoption, specifically in terms of cybersecurity challenges and more specifically in emerging economies. By offering empirical evidence in the banking industry in South Africa, it highlights artificial intelligence's transformative capabilities while also tackling contextual challenges that need to be traversed to reap its benefits.

The findings underscore the need to balance technological advancement with governance frameworks and organizational readiness for its consequences. As artificial intelligence keeps advancing, its adoption hinges on the ability of organizations and policymakers to navigate the complex dynamics between potential gains and challenges.

Overall, this research lays a cornerstone for future inquiries and practical interventions, offering crucial knowledge to facilitate artificial intelligence adoption in cybersecurity and pave a more secure digital path forward.

7. REFERENCES

1. Abraham, J., Cherian, G. J., & Jayapandian, N. (2023). Systematic review on humanizing machine intelligence and artificial intelligence. Proceedings of the Second International Conference on Electronics and Renewable Systems (ICEARS-2023). https://doi.org/10.1109/ICEARS56392.2023.10084967
2. Albrecht, C., Albrecht, C. C., & Wernz, C. (2021). Cybersecurity automation: Redefining threats in AI ecosystems. Journal of Cybersecurity, 7(1), 53–69. https://doi.org/10.1016/j.jocs.2021.02.015
3. AlDaajeh, S., & Alrabaee, S. (2024). Strategic cybersecurity. Computers & Security, 141, 103845. https://doi.org/10.1016/j.cose.2024.103845
4. Bailey, T., Faraj, S., Hinds, P., Leonardi, P., & von Krogh, G. (2023). Risk and the future of AI: Algorithmic bias, data colonialism, and marginalization. Information and Organization, 33, 100478. https://doi.org/10.1016/j.infoandorg.2023.100478
5. Bank of International Settlement. (2004). TT Mboweni: The South African banking sector - An overview of the past 10 years. Bank of International Settlement. https://www.bis.org/review/r041231f.pdf (Accessed: 1 April 2024)
6. Barletta, V. S., Cassano, F., Pagano, A., & Piccinno, A. (2022). New perspectives for cybersecurity in software development: When end-user development meets artificial intelligence. Journal of Cybersecurity and Software Engineering, 7(2), 531-534.
7. Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cybersecurity. Information, 10(4), 122. https://doi.org/10.3390/info10040122
8. Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.
9. Chauhan, S., & Keprate, A. (2022). Standards, ethics, legal implications, and challenges of artificial intelligence. Journal of AI and Governance, 5(3), 1048-1052.
10. Creswell, J. W. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). Sage Publications.
11. Cybersecurity Ventures. (2023). Cybersecurity statistics and figures.
12. Dangi, A. K., Pant, K., Alanya-Beltran, J., Chakraborty, N., Akram, S. V., & Balakrishna, K. (2023). A review of the use of artificial intelligence in cybersecurity and the fifth-

generation cyber-attacks and its analysis. Journal of Cybersecurity Research, 7(1), 553-558.

13. Darraj, E., Sample, C., & Justice, C. (2019). Artificial intelligence cybersecurity framework: Preparing for the here and now with AI. Academic Conferences International Limited.
14. Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2019). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. Information Systems Frontiers, 21, 719-734. https://doi.org/10.1007/s10796-019-09941-1
15. Flick, U. (2015). Introducing research methodology: A beginner's guide to doing a research project. Sage Publications.
16. Glaser, B., & Strauss, A. (1967). The discovery of grounded theory: Strategies for qualitative research. Aldine Publishing Company.
17. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
18. Halawi, N., Meyrueis, V., Benfriha, K., Guiltat, T., & Loubere, S. (2024). A review on the static and dynamic risk assessment methods for OT cybersecurity in industry 4.0. Computers & Security, 148, 104295. https://doi.org/10.1016/j.cose.2024.104295
19. Insight. (2023). The 5 stages of AI adoption. Insight. https://www.insight.com/en_US/content-and-resources/blog/the-5-stages-of-ai-adoption--how-to-sustain-momentum-at-every-level.html (Accessed: 27 August 2023)
20. Iturbe, E., Llorente-Vazquez, O., Rego, A., Rios, E., & Toledo, N. (2024). Unleashing offensive artificial intelligence: Automated attack technique code generation. Computers & Security, 147, 104077. https://doi.org/10.1016/j.cose.2024.104077
21. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2
22. Khoa, B. T., Hung, B. P., & Hejsalem-Brahmi, M. (2023). Qualitative research in social sciences: Data collection, data analysis, and report writing. International Journal of Public Sector Performance Management, 12(1-2), 187-209.
23. Kshetri, N. (2021). Economics of artificial intelligence in cybersecurity. IT Professional, 23(5), 73–80. https://doi.org/10.1109/MITP.2021.3100177
24. Kshetri, N. (2021a). AI in cybersecurity: Challenges, opportunities, and countermeasures. Computer, 54(4), 53-58. https://doi.org/10.1109/MC.2021.3052340

25. Kshetri, N. (2021b). Economics of artificial intelligence in cybersecurity. IT Professional, 23(5), 73-77. https://doi.org/10.1109/MITP.2021.3100177
26. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.
27. Lidestri, N. (2018). The impact of artificial intelligence in cybersecurity. Utica College.
28. Lourens, M., Rathour, N., Dabral, A. P., Tida, N., Gangodkar, D., & Chadha, A. (2022). Integration of AI with cybersecurity: A detailed systematic review with practical issues and challenges. 2022 5th International Conference on Contemporary Computing and Informatics (IC3I). https://doi.org/10.1109/IC3I.2022
29. Lourens, P., & Smith, M. (2022). The human-AI partnership in cybersecurity. AI & Society, 37(3), 345–357.
30. Lumen Learning. (n.d.). Chapter 12 interpretive research. Lumen Learning. https://courses.lumenlearning.com/suny-hccc-research-methods/chapter/chapter-12-interpretive-research/#:~:text=Interpretive%20research%20is%20a%20research,context%20by%20reconciling%20the%20subjective (Accessed: 13 October 2023)
31. Mamela, J., Rawat, K., & Chauhan, M. (2020). The workforce impact of AI adaptation in emerging economies. Journal of Cybersecurity, 12(4), 198–209.
32. Mamela, T. L., Sukdeo, N., & Mukwakungu, S. C. (2020). Adapting to artificial intelligence through workforce reskilling within the banking sector in South Africa. IEEE Access, 8, 1-9. https://doi.org/10.1109/icABCD49160.2020.9183817
33. Mangundu, J., & Jokonya, O. (2024). Investigating drivers of information technology governance in South African public healthcare sector. *African Journal of Science, Technology, Innovation and Development, 16*(5), 655–673. https://doi.org/10.1080/20421338.2024.2374615
34. McIntosh, T., Liu, T., Susnjak, T., Alavizadeh, H., & Ng, A. (2023). Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. Computers & Security, 134, 103424. https://doi.org/10.1016/j.cose.2023.103424
35. Meek, T., Barham, H., Beltaif, N., Kaadoor, A., & Akhter, T. (2016). Managing the ethical and risk implications of rapid advances in artificial intelligence: A literature review. In 2016 Portland International Conference on Management of Engineering and Technology (PICMET) (pp. 682-693). IEEE. https://doi.org/10.1109/PICMET.2016.7806752

36. Mehrizi, M. H. R., Nicolini, D., & Mòdol, J. R. (2024). How do organisations learn from information systems incidents? A synthesis of the past, present, and future. MIS Quarterly, 48(4), 1531. https://doi.org/10.25300/MISQ/2024/14305
37. Mersinas, K., Bada, M., & Furnell, S. (2024). Cybersecurity behavior change: A conceptualisation of ethical principles for behavioral interventions. Computers & Security, 148, 104025. https://doi.org/10.1016/j.cose.2024.104025
38. Mogoale, P. D. (2023). Developing an information systems capability framework for South African mining firms (Doctoral dissertation, North-West University).
39. Nikolskaia, E., & Vast, T. (2021). AI in South Africa's banking sector. Journal of AI Applications, 19(2), 345–370.
40. Nikolskaia, K. Y., & Naumov, V. B. (2021). The relationship between cybersecurity and artificial intelligence. Cybersecurity and AI Journal, 2(1), 94-97.
41. Nomnga, P., & Ngqulu, N. (2021). Advancing artificial intelligence to combat escalating cyberspace human rights violations in Africa. In 2021 IST-Africa Conference (IST-Africa) (pp. 1-9).
42. Rawat, G., Kumar, D., & Agarwal, K. L. (2021). Use of artificial intelligence in modern warfare and national security. In 2021 9th International Conference on Reliability, Infocom Technologies and Optimisation (Trends and Future Directions) (ICRITO) (pp. 1-5). IEEE. https://doi.org/10.1109/ICRITO51393.2021.9596126
43. Rawat, K., Chauhan, M., & Mamela, J. (2021). The role of AI in warfare and cybersecurity. Defence Technology, 17(4), 509–521. https://doi.org/10.1016/j.dt.2021.05.004
44. Reuters. (2023). Elon Musk says he will launch a rival to Microsoft-backed ChatGPT. Reuters. https://www.reuters.com/technology/musk-says-he-will-start-truthgpt-or-maximum-truth-seeking-ai-fox-news-2023-04-17/ (Accessed: 3 August 2023)
45. Roy. (2022). Understanding the difference between artificial intelligence, machine learning and deep learning. Towards Data Science. https://towardsdatascience.com/understanding-the-difference-between-ai-ml-and-dl-cceb63252a6c (Accessed: 23 August 2023)
46. Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach. Prentice Hall.

47. Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications, and research directions. SN Computer Science, 2(3), 160.
48. Sarker, I. H. (2021). Machine learning: Applications in security and decision-making. Applied Intelligence, 51(1), 56-77. https://doi.org/10.1007/s10489-021-02192-9
49. Sarker, I. H., & Rashid, M. M. (2020). Cybersecurity data science: An overview from machine learning perspective. Journal of Big Data, 7, 1–29. https://doi.org/10.1186/s40537-020-00318-5
50. Saunders, M. (2009). Research methods for business students (5th ed.). Pearson Education.
51. Saunders, M., Lewis, P., & Thornhill, A. (2016). Research Methods for Business Students. Pearson Education.
52. Scribbr. (2020). What is qualitative research? | Methods & examples. Scribbr. https://www.scribbr.com/methodology/qualitative-research/#:~:text=Qualitative%20research%20involves%20collecting%20and,generate%20new%20ideas%20for%20research (Accessed: 14 October 2023)
53. Shi, Z., Li, H., Zhao, D., & Pan, C. (2024). Research on quality assessment methods for cybersecurity knowledge graphs. Computers & Security, 142, 103848. https://doi.org/10.1016/j.cose.2024.103848
54. Silverman, D. (2020). Doing qualitative research (6th ed.). SAGE Publications.
55. Silverman, D. (2020). Qualitative research (5th ed.). Sage Publications.
56. Splunk. (2024). 2024 CISO report: The impact of AI on cybersecurity and governance challenges. Splunk. https://www.splunk.com/pdfs/reports/2024-ciso-report.pdf (Accessed: 30 August 2023)
57. Splunk. (2024). The 2024 CISO report: Generative AI and cybersecurity challenges. Splunk Reports. Retrieved from https://www.splunk.com
58. Stanford University. (2023). Sample interview protocol. Stanford University. https://web.stanford.edu/group/ncpi/unspecified/student_assess_toolkit/sampleInterviewProtocol.html (Accessed: 10 October 2023)
59. Stohr, A., Ollig, P., Keller, R., & Rieger, A. (2021). Automating the future: A comprehensive review of AI in cybersecurity. Computers & Security, 103, 91–102. https://doi.org/10.1016/j.cose.2021.102101

60. Taddeo, M. (2019). Governing artificial intelligence: Ethical, legal, and societal issues. Philosophy & Technology, 32(4), 645–660. https://doi.org/10.1007/s13347-019-00379
61. Taddeo, M. (2019). Three ethical challenges of applications of artificial intelligence in cybersecurity. Minds and Machines, 29(2), 187–191. https://doi.org/10.1007/s11023-019-09504-8
62. Taddeo, M. (2019). Three ethical challenges of applications of artificial intelligence in cybersecurity. Minds & Machines, 29, 187-191. https://doi.org/10.1007/s11023-019-09504-8
63. Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. Nature Machine Intelligence, 1(12), 557–560. https://doi.org/10.1038/s42256-019-0109-1
64. Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies, 8(28), e3. https://doi.org/10.4108/eai.7-7-2021.170285
65. Tiwari, S., Sharma, S., & Verma, R. (2022). Ethical implications of AI in cybersecurity: A conceptual framework. Computers & Security, 104, 112–127. https://doi.org/10.1016/j.cose.2022.105452
66. Turing, A. M. (1950). Computing machinery and intelligence. Mind, 59(236), 433-460. https://doi.org/10.1093/mind/LIX.236.433
67. United Nations. (2015). Sustainable Development Goals. Retrieved from https://www.un.org/sdgs/
68. United Nations. (2015). The 17 goals. United Nations. https://sdgs.un.org/goals (Accessed: 25 August 2024)
69. University of the Witwatersrand. (2023). Research support: Research methodology. University of the Witwatersrand. https://libguides.wits.ac.za/c.php?g=693518&p=4914913 (Accessed: 12 October 2023)
70. Vast, R., Sawant, S., Thorbole, A., & Badgujar, V. (2021). Artificial intelligence-based security orchestration automation and response system. Journal of Information Security and Applications, 6, 1-5.
71. Vast, T., & Nikolskaia, E. (2021). Automation in cybersecurity. Journal of AI and Cybersecurity, 15(3), 200–220.

72. Verizon. (2023). 2023 data breach investigations report. Verizon. https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 15 August 2024)
73. Vernon, D. (2019). Robotics and artificial intelligence in Africa [Regional]. IEEE Robotics & Automation Magazine, 26(4), 131-135. https://doi.org/10.1109/MRA.2019.2946107
74. Vernon, R. (2019). Artificial intelligence and development. Development Quarterly, 26(3), 255–275.
75. Welman, C., Kruger, F., & Mitchell, B. (2011). Research methodology (3rd ed.). Oxford University Press.
76. Xu, D., David, J., & Kim, S. (2018). Transforming cybersecurity with artificial intelligence. Journal of Technology Innovation, 11(2), 66-81. https://doi.org/10.1016/j.techinnov.2018.06.005
77. Xu, M., David, J. M., & Kim, S. H. (2018). The fourth industrial revolution: Opportunities and challenges. International Journal of Financial Research, 9(2), 90-95. https://doi.org/10.5430/ijfr.v9n2p90
78. Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). Sage Publications.
79. Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.
80. Yuli. (n.d.). Qualitative research design. Yuli Learning. https://yulielearning.com/pluginfile.php/4833/mod_resource/content/1/2.%20qualitative%20research%20design.pdf (Accessed: 15 October 2024)

APPENDIX A: INTERVIEW PROTOCOL

Below is an interview protocol adopted from Stanford University (2023).

Institutions: A South African Bank
Interviewee: Cybersecurity Expert 1
Interviewer: Thabani Joyisa

Interview Section Used:

A. **Background**

Good day. My name is Thabani Joyisa. I am a Master of Commerce student in the School of Business Science (Information Systems) at the University of the Witwatersrand. My master's study focuses on the adoption and use of Artificial Intelligence for Cybersecurity in a South African bank.

I would like to invite you to participate in my study to get insights from you as a cybersecurity expert on your experience in adopting and using AI for cybersecurity in your organisation.

B. **Demographics**

Gender:	**Age:**	**Ethnicity:**
Male	18 – 25	Black
Female	26 – 35	White
Prefer not to say.	36 – 45	Indian
	45+	Coloured
		Asian
		Other
		Prefer not to say
Highest level of qualification:	**Industry Experience in IT or Cybersecurity**:	
Matric	0 – 3 years	
Diploma	4 – 6 years	
BTech	7 – 9 years	
Degree	10+ years	
Honours		
Master		
PhD		
Other		

C. Discussion / Interview

1. Talk me through your organisation's experience of adopting and using AI for cybersecurity and some of the challenges faced in integrating artificial intelligence into existing cybersecurity infrastructure.

2. How experienced and skilled is your organisation's personnel to manage and operate AI-based cybersecurity systems?

3. Has your organisation experienced ethical concerns related to the use of AI technologies in cybersecurity, such as privacy and bias issues? How is the organisation managing this risk?

4. Does AI have the potential to significantly enhance cybersecurity measures in your organisation? If yes, how so?

5. What are some of the low-hanging fruits has AI-based cybersecurity solutions have been able to assist your organisation in attaining? Has there been improvement in the accuracy and efficiency of threat detection and prevention?

6. What are some of the shortcomings of the AI-based cybersecurity solutions have your organisation identified and how are they being addressed?

7. Which part of cybersecurity have AI-based cybersecurity solutions been deployed in? How is AI performing compared to human teams?

8. What is the future of AI for cybersecurity in your organisation?

Other topics discussed.
There will be no other topics to be discussed outside of the governance of AI for cybersecurity in a South African bank.

Documents obtained.
E.g., company-published reports.

Post interview comments or leads.
There will be no post-interview comments or leads that will be recorded.

APPENDIX B: ETHICS CERTIFICATE

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

SCHOOL OF BUSINESS SCIENCES ETHICS COMMITTEE
CONSTITUTED UNDER THE UNIVERSITY HUMAN RESEARCH ETHICS COMMITTEE (NON-MEDICAL)

CLEARANCE CERTIFICATE **PROTOCOL NUMBER: CBUSE2289**

PROJECT TITLE	Artificial Intelligence for Cybersecurity: Governance Insights from Cybersecurity Experts in the Banking Industry in South Africa
INVESTIGATOR	Thabani Joyisa
SCHOOL/DEPARTMENT OF INVESTIGATOR	School of Business Sciences
DATE CONSIDERED	20 November 2024
DECISION OF THE COMMITTEE	Approved Unconditionally
RISK LEVEL	Low Risk
EXPIRY DATE	31 December 2027

ISSUE DATE OF CERTIFICATE 22 November 2024 **CHAIRPERSON** _____
(Neetu Ramsaroop)

cc: Supervisor: John Mangundu

DECLARATION OF INVESTIGATOR

To be completed in duplicate and **ONE COPY** returned to the Chairperson of the School/Department ethics committee.

I fully understand the conditions under which I am are authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I/we undertake to resubmit the protocol to the Committee.

_____ 25 / Nov / 2024
Signature **Date**

PLEASE QUOTE THE PROTOCOL NUMBER ON ALL ENQUIRIES

APPENDIX C: CONSENT FORM

Artificial Intelligence for Cybersecurity: Governance Insights from Cybersecurity Experts in The Banking Industry In South Africa.

Thabani Joyisa (Student Number: 1285042)

I, ..., agree to participate in this research project.

I agree to the following:

(Please circle the relevant options below)

The research study was explained to me. I understand what this study is about.	YES	NO
I understand that I can volunteer to take part in the study	YES	NO
I agree that the interview may be audio-recorded	YES	NO
I agree that direct quotations from my interview may be used by the researcher in their research report	YES	NO
I agree that my participation will remain anonymous (my name or other identifying data will not be used by the researcher in their research report)	YES	NO
I agree that other researchers may use the information I provide in my interview (depending on their own ethics clearance being obtained) but my name and any personal information will not be used or passed on	YES	NO

…..... (signature)
…..... (name of participant)
…..... (date)

…..... (signature)
…..... (name of researcher/person seeking consent)
…..... (date)

APPENDIX D: PARTICIPANT SHEET



University of the Witwatersrand
School of Business Science, Information Systems

1 Jan Smuts Ave
Braamfontein
Johannesburg
2017

Participant Information Sheet (PIS)

Dear Sir/Madam

My name is Thabani Joyisa. I am a Masters student in the School of Business Science at the University of the Witwatersrand, Johannesburg. My supervisor is Dr. John Mangundu, I am conducting a research study about artificial intelligence in cybersecurity. The study title is Artificial Intelligence for Cybersecurity: Governance Insights from Cybersecurity Experts in the Banking Industry in South Africa.

I am inviting you to take part in an interview. If you decide to take part, your participation in this research study will last about 30 to 45 minutes. The interview will take place at 1 Discovery Place during office hours.

With your permission, I would like to audio record the interview. This data will be stored in a password-protected computer with multi-factor authentication for no longer than 1 year and will be deleted immediately after graduation. Only the researcher will have access to the data.

During the research activity, I will need to ask for some personal information about you, including your name and contact details.

The interview will be confidential and anonymous. When I share the results of the research study, I will not include your name or anything else that could identify you. With your permission, other researchers may use the data collected from this research study, but your name and any personal information will not be used or passed on.

If you decide to take part in the research study, it should be because you want to volunteer. You do not have to take part. You can stop being in the study at any time. You do not have to answer any questions if you do not want to. You will not get any direct benefits if you choose to join the research study. You will not lose any services, benefits or rights you would normally have if you decide not to join. Taking part in the research study will not cost you anything. You will not be paid for being in this research study.

The risks for this research study are no more than what happens in everyday life / some of the questions asked may make you feel sad or upset. If this happens, I will stop the interview and continue another time. If you need some support or counselling services following the interview, these are available free of charge at 1 Discovery Place. The contact details for the counselling service are 080 0320 420 or +27(0)11 529 6291.

This research study will be written up as a research report. The report will be available on the university library website. If you would like to receive a summary of this report, I will be happy to send it to you.

If you have any questions during or afterwards about this research study, feel free to contact me or my supervisor on the details listed below. If you have any concerns or complaints about the ethical procedures of this research study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical), by telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za.

Yours sincerely,
Thabani

Researcher:
Thabani Joyisa, 1285042@students.wits.ac.za, +27(0)84 760 3725

Supervisor:
Dr. John Mangundu, john.mangundu@wits.ac.za, +27(0)11 717 9869

APPENDIX E: LITERATURE REVIEW THEMATICAL ANALYSIS

No	Author(s) / Reference	Year	Sub-Theme	Article Title	Source	Origin	Research Design	Theoretical Framework
1	Roy	2020	Definition of AI, ML, and DL	"Understanding Difference between Artificial Intelligence, Machine Learning and Deep Learning."	Website article	United States of America	N/A	N/A
2	Nikolskaia et al.	2021	AI for cybersecurity	"The Relationship between Cybersecurity and Artificial Intelligence"	IEEE Xplore	Russia	Reviewed existing literature (literature review)	Encompasses various conceptual lenses through which the **relationship between cybersecurity and AI** was examined.
3	Dangi et al.	2023	AI for cybersecurity	"A Review of the use of Artificial Intelligence on Cyber Security and the Fifth-Generation Cyber-attacks and its analysis."	IEEE Xplore	India	Qualitative and descriptive	Draws upon established theories and concepts in cybersecurity and AI. **Systems theory** looks at the interconnectedness of cybersecurity systems and how AI can be integrated into them to enhance security
4	Lourens et al.	2022	AI for cybersecurity	"Integration of AI with Cybersecurity: A detailed Systematic review with the practical issues and challenges"	IEEE Xplore	South Africa	Comprehensive literature review	Multiple frameworks could have been used in this article, however, it appears that the **introduction of AI** was among the frameworks used. This framework looks at the genesis of AI.

5	Vernon	2019	Pioneering robotics and AI in Africa	"Robotics and Artificial Intelligence in Africa [Regional]"	IEEE Xplore	Rwanda	Descriptive and analytical	The article did not explicitly mention a specific theory but it draws upon theories such as **development and innovation theories**.
6	Mamela et al.	2020	Reshaping banking with AI	"Adapting to Artificial Intelligence through Workforce Re-skilling within the Banking Sector in South Africa"	IEEE Xplore	South Africa	Quantitative with non-random convenient sampling technique	The article mentioned **skills and AI tools adaptation** as two of its theoretical and conceptual frameworks
7	Rawat et al.	2022	AI for cybersecurity	"The Empirical Analysis of Artificial Intelligence Approaches for Enhancing Cyber Security for Better Quality"	IEEE Xplore	India	Quantitative	Man-made consciousness and network safety frameworks.
8	Rawat et al.	2021	AI for national security	"Use of Artificial Intelligence in Modern Warfare and National Security"	IEEE Xplore	India	Qualitative	Innovation theory
9	Vast et al.	2021	AI for cybersecurity	"Artificial Intelligence-based Security Orchestration, Automation and Response System"	IEEE Xplore	India	Literature review	**SOAR** – Security Orchestration Automation and Response framework.
10	Nomnga et al.	2021	Safeguarding cyberspace rights	"Advancing Artificial Intelligence to Combat Escalating Cyberspace Human Rights Violations in Africa"	IEEE Xplore	South Africa	Mixed methods (qualitative and quantitative methodologies)	The conceptual model of this paper implements deep learning techniques and natural language processing (NLP) to perform text and sentiment

11	Barletta et al.	2022	Future-proofing cybersecurity	"New perspectives for cyber security in software development: When end-user Development meets Artificial Intelligence"	IEEE Xplore	Italy	Qualitative	AI model to support user development.
12	Tao et al.	2021	Future-proofing cybersecurity	"The Future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey"	EAI.EU	China	Qualitative	Nonlinear control theory is used to ensure device stability when attacks happen.
13	Mariarosaria et al.	2019	Navigating trust	"Trusting artificial intelligence in cybersecurity is a double-edged sword"	Nature Machine Intelligence	United Kingdom	Conceptual and analytical. Draws from existing literature.	The theoretical framework of the article revolves around concepts of trust, reliability, and control in the context of AI technologies and cybersecurity
14	Taddeo	2019	Ethical dilemmas	"Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity"	Springer	United Kingdom	Conceptual and analytical	The article employs a theoretical framework grounded in ethical analyses to critically examine the ethical challenges posed by AI applications in cybersecurity
15	Abraham et al.	2023	Humanising machine intelligence	"Systematic Review on Humanising Machine Intelligence and Artificial Intelligence"	IEEE Xplore	India	Literature review	The article lays out a framework on how to humanise AI from a multilevel perspective.
16	Chaudhary et al.	2020	Challenges explored	"A review of various challenges in cybersecurity using Artificial Intelligence"	IEEE Xplore	India	Quantitative	Machine-learning framework

17	Meek et al.	2016	Ethics and risks in AI advancements	"Managing the ethical and risk implications of rapid advances in artificial intelligence: A literature review"	IEEE Xplore	United States of America	Literature of AI ethics	AI ethics in the subject of Engineering and Technology Management (ETM) and Management of Technology (MOT).
18	Reuters	2023	Disruptive plan	"Elon Musk says he will launch a rival to Microsoft-backed ChatGPT"	Website article	United States of America	N/A	N/A
19	Kshetri	2021	Economic perspective	"Economics of Artificial Intelligence in Cybersecurity"	IEEE Xplore	United States of America	Primarily analytical and descriptive	This article employs a theoretical framework grounded in economic analysis to explore the implications of AI adoption in cybersecurity
20	Lidestri	2018	Unveiling the impact of AI	"The Impact of Artificial Intelligence in Cybersecurity"	ProQuest	United States of America	Comprehensive literature review	Artificial intelligence in cybersecurity
21	Chauhan et al.	2022	AI governance	"Standards, Ethics, Legal Implications & Challenges of Artificial Intelligence"	IEEE Xplore	Norway	Conceptual and analytical	The theoretical framework of the article revolves around the intersection of ethics, law, and technology, particularly focusing on AI
22	Darraj et al.	2019	AI governance	"Artificial Intelligence Cybersecurity Framework: Preparing for the Here and Now with AI."	Research Gate	United States of America	Qualitative	AI cyber security framework for artificial intelligence systems.

23	AlDaajeh, et al.	2024	Strategic Models for Cyber Protection	"Strategic cybersecurity"	Computers & Security	Jordan	Literature Review	Strategic taxonomy for cybersecurity challenges
24	Bailey et al.	2023	Challenges Relating to Ethics and Governance	"Risk and the future of AI: Algorithmic bias, data colonialism, and marginalisation."	Information and Organisation	United States of America	Conceptual and Analytical	Ethical analysis in AI and algorithmic bias
25	Iturbe et al.	2024	AI for cybersecurity	"Unleashing offensive artificial intelligence: Automated attack technique code generation."	Computers & Security	Spain	Empirical	Breach and Attack Simulation (BAS)
26	McIntosh et al.	2023	Challenges Relating to Ethics and Governance	"Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation."	Computers & Security	New Zealand	Case Study	Governance, Risk, and Compliance (GRC) frameworks
27	Mehrizi et al.	2024	Strategic Models for Cyber Protection	"How do organisations learn from information systems incidents? A synthesis of the past, present, and future."	MIS Quarterly	United Kingdom	Systematic Review	Organisational learning frameworks in incident management
28	Shi et al.	2024	AI for cybersecurity	"Research on quality assessment methods for cybersecurity knowledge graphs."	Computers & Security	China	Mixed Methods	Cybersecurity knowledge graphs
29	Wang et al.	2024	AI for cybersecurity	"Data privacy and cybersecurity challenges in digital transformation."	Computers & Security	China	Qualitative	Digital transformation and cybersecurity frameworks

30	Burlina et al.	2021	Challenges Relating to Ethics and Governance	"Mitigating algorithmic bias with synthetic data in AI."	Ophthalmology AI	United States of America	Analytical and Descriptive	Addressing algorithmic bias in AI
31	Kaur et al.	2024	AI for cybersecurity	"AI-based cybersecurity assessment: A review of applications and challenges."	Cybersecurity Insights	India	Literature Review	Systems theory and AI integration in cybersecurity
32	Mersinas et al.	2025	Behavioural dynamics in cybersecurity	"Behavioural dynamics in cybersecurity responses: A study on human factors."	Cybersecurity Psychology	Australia	Empirical	Behavioural dynamics and decision-making frameworks
33	Kuwaiti et al.	2024	Strategic Models for Cyber Protection	"Strategic approaches to addressing AI threats in digital infrastructure."	Digital Resilience Quarterly	United Arab Emirates	Analytical	Strategic frameworks for resilience
34	Lovejoy et al.	2023	AI for cybersecurity	"Implications of generative adversarial networks for cybersecurity: A dual perspective."	Journal of AI Systems	United Kingdom	Analytical	Generative adversarial networks (GANs)
35	Strom et al.	2023	AI for cybersecurity	"MITRE ATT&CK model: Advancing threat intelligence with AI-based tools."	Threat Intelligence Review	United States of America	Analytical	MITRE ATT&CK frameworks
36	Zheng et al.	2021	Challenges Relating to Ethics and Governance	"The ethical and operational impact of AI on cybersecurity policy frameworks."	Policy and Technology	United States of America	Qualitative	Ethical frameworks for operational AI for cybersecurity