2024

The Effect of emerging digital security solutions on fraud risk management in the banking sector in Kenya.

Matheri, Judy
Strathmore Business School
Strathmore University

The Effect of Emerging Digital Security Solutions on Fraud Risk Management in the Banking Sector in Kenya

Judy Matheri

Admission No. 028008

Submitted in partial fulfillment of the requirements for the Degree of Masters of Business Administration at Strathmore University

Strathmore Business School

Strathmore University

Nairobi, Kenya

May 2024

ABSTRACT

Banks and other financial institutions increasingly leverage emerging and innovative digital solutions to fight fraud. While this trend is common, the impact of some of these solutions in enhancing financial fraud detection and prevention remains unexplored in the scientific research community. This study explored the effect of emerging digital security solutions on fraud risk management in Kenya's banking sector. The independent variable, emerging digital security solutions, was depicted by biometrics technology, artificial intelligence, and data analytics, with fraud risk management being the dependent variable. The fraud triangle theory and fraud diamond theory made for the theoretical framework. The research study followed a positivism research paradigm and adopted descriptive research for research design. The units of analysis constituted 42 commercial banks in Kenya, from which a sample of 126 IT, compliance and risk management professionals were selected using a stratified sampling technique. Primary data was collected using structured questionnaires and analyzed using descriptive statistics, correlational and multiple regression analysis. Findings show that biometrics do not have a significant effect on fraud management. AI and data analytics were found to significantly affect fraud risk management in the banking sector. Therefore, this research advises banking institutions to invest more in and integrate these two emerging digital security solutions into their anti-fraud frameworks. This research also recommends expanding research to study the effect of other emerging digital solutions.

DECLARATION

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other university. To the best of my knowledge and belief, this thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

Judy Njeri Matheri

Admin no 028008

Signature: …… Date: …31st May 2024……

APPROVAL

The thesis of Judy has been reviewed and approved for examination by:

Supervisor: Dr. Erastus Mbithi

Strathmore Business School

Signature: …  …….. Date…31st May 2024…….....

TABLE OF CONTENTS

ABSTRACT **1**

DECLARATION **2**

LIST OF TABLES **8**

LIST OF FIGURES **9**

LIST OF ABBREVIATIONS **10**

ACKNOWLEDGEMENT **11**

CHAPTER ONE **12**

INTRODUCTION **12**

1.1 Background of the Study 12

1.1.1 Emerging Digital Security Solutions 13

1.1.2 Fraud Risk Management 14

1.1.3 Banking Sector in Kenya 15

1.2 Statement of the Problem 17

1.3 Objective of the Study 18

1.3.1 General Objective 18

1.3.2 Specific Objectives 18

1.4 Research Questions 19

1.5 Scope of the Study 19

1.6 Significance of the Study 19

1.7 Chapter Summary 20

CHAPTER TWO **22**

LITERATURE REVIEW 22

2.1 Introduction 22

2.2 Theoretical Framework 22

2.2.1 The Fraud Triangle Theory 22

2.2.2 Fraud Diamond Theory 23

2.3 Empirical Review 23

2.3.1 Biometrics and Fraud Risk Management 24

2.3.2 AI and Fraud Risk Management 26

2.3.3 Data Analytics and Fraud Risk Management 28

2.4 Literature Review Summary and Knowledge Gap 30

2.5 Conceptual Framework 34

2.6 Operationalization of Variables 35

2.7 Chapter Summary 37

CHAPTER THREE 38

RESEARCH METHODOLOGY 38

3.1 Introduction 38

3.2 Research Philosophy 38

3.3 Research Design 39

3.4 Population and Sampling 39

3.4.1 Population 39

3.4.2 Sampling 39

3.4.2.1 Sampling Frame 39

3.4.2.2 Sampling Technique 39
3.5 Data Collection 40
3.6 Data Analysis 40
3.6.1 Descriptive Statistics 41
3.6.2 Correlation Analysis 41
3.6.3 Regression Analysis 41
3.7 Research Quality 42
3.7.1 Reliability 42
3.7.2 Validity 43
3.8 Ethical Considerations 43
3.9 Chapter Summary 43
CHAPTER FOUR 45
PRESENTATION OF FINDINGS 45
4.1 Introduction 45
4.2 Response Rate 45
4.3 Background Information 45
4.4 Reliability Tests 46
4.5 Descriptive Statistics 47
4.5.1 Fraud Risk Management 47
4.5.2 Biometric Technology 49
4.5.3 Artificial Intelligence 50
4.5.4 Data Analytics 51

4.6 Inferential Statistics 53
4.6.1 Normality Test 53
4.6.2 Correlational Analysis 54
4.6.2.1 Biometric Technology and Fraud Risk Management 54
4.6.2.2 Artificial Intelligence and Fraud Risk Management 55
4.6.2.3 Data Analytics and Fraud Risk Management 55
4.6.3 Diagnostic Tests 56
4.6.3.1 Test for Heteroscedasticity 56
4.6.3.2 Test for Normality 57
4.6.3.3 Test for Autocorrelation 58
4.6.3.4 Test for Multicollinearity 59
4.6.4 Regression Analysis 59
4.7 Chapter Summary 62
CHAPTER FIVE 63
SUMMARY, DISCUSSION, CONCLUSION, AND RECOMMENDATIONS 63
5.1 Introduction 63
5.2 Summary of the Study 63
5.3 Discussion 64
5.3.1 Biometric Technology and Fraud Risk Management 64
5.3.2 Artificial Intelligence and Fraud Risk Management 65
5.3.3 Data Analytics and Fraud Risk Management 66
5.4 Conclusion 67

5.5 Recommendations 67

5.6 Limitations of the Study 68

5.7 Areas for Further Research 68

REFERENCES 70

APPENDICES 82

Appendix 1: Letter of Invitation to Participants 82

Appendix 2: Participants Information Sheet and Consent Form 83

Appendix 3: Commercial Banks in Kenya 86

Appendix 4: Research Instrument 88

Appendix 5: Research Budget 93

LIST OF TABLES

Table 2. 1: Summary of Literature and Knowledge Gaps 30

Table 2. 2: Operationalization of Variables 36

Table 3. 1: Unit of Analysis ..... **Error! Bookmark not defined.**

Table 4. 1: Response Rate 45

Table 4. 2: Background Information of the Respondents (n=97) 46

Table 4. 3: Reliability Tests 47

Table 4. 4: Fraud Risk Management 47

Table 4. 5: Biometric Technology 49

Table 4. 6: Artificial Intelligence 50

Table 4. 7: Data Analytics 51

Table 4. 8: One-Sample Shapiro-Wilk Test 53

Table 4. 9: Biometric Technology and Fraud Risk Management 54

Table 4. 10: Artificial Intelligence and Fraud Risk Management 55

Table 4. 11: Data Analytics and Fraud Risk Management 55

Table 4. 12: Durbin-Watson Test 58

Table 4. 13: Test for Multicollinearity 59

Table 4. 14: Model Summary[b] 60

Table 4. 15: ANOVA[a] 60

Table 4. 16: Coefficients[a] 61

LIST OF FIGURES

Figure 2. 1: Conceptual Framework 35

Figure 4. 1: Residual Plots for Fraud Risk Management 57

Figure 4. 2: Test for Normality 58

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AML	Anti-Money Laundering
ATO	Account Takeover
BFIU	Banking Fraud Investigation Unit
CBK	Central Bank of Kenya
GDP	Gross Domestic Product
IAM	Identity and Access Management
KBA	Kenya Bankers Association
KCB	Kenya Commercial Bank
KYC	Know Your Customer
MFA	Multi-Factor Authentication
ML	Machine Learning
NACOSTI	National Commission for Science, Technology, and Innovation
NPL	Natural Language Processing
OLAP	Online Analytical Processing
OTP	One-Time Password
PAM	Privileged Access Management
SLR	Systematic Review of Literature
SPSS	Statistical Package for the Social Sciences
TAM	Technology Adoption Model
TRA	Theory of Reasoned Action

ACKNOWLEDGEMENT

First and foremost, I would like to express my deepest gratitude to The Almighty God for His guidance, strength, and blessings throughout my academic endeavors. Without His divine providence and grace, this achievement would not have been possible.

I am deeply grateful to my family, friends and work colleagues for their unwavering support. Your encouragement and support were essential in helping me navigate the challenges of graduate school.

To my supervisor, Dr. Erastus Mbithi, whose expertise, guidance and support were invaluable throughout the course of my research and the writing of this thesis. Your encouragement and constructive feedback pushed me to achieve more than I thought possible.

Lastly, a special thanks to my fellow graduate students at Strathmore Business School. You made this journey a truly enjoyable and enriching experience!

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Fraud refers to "the deliberate misrepresentation of the truth to deceive a particular entity or person for unfair, wrongful gain at their own expense" (Kingsley, 2015). It is a serious concern that continues "to ravage the global economy as a whole and the banking industry in particular" (Xin et al., 2021). Banking fraud can take many forms, with the most common being "scams, debit and credit card theft, online fraud, identity theft, data theft, digital payment fraud, digital wallet fraud, money laundering, insider fraud, loan scams, forged documents, and social engineering" (Enofe et al., 2017; Malik, 2018). "It negatively affects the profitability, economic growth, and social welfare of the firms" (Simbolon et al., 2018). Its severe effects may be felt by declining bank profitability, reputation, competitive advantage, and economic downturn.

A 2022 report by KMPG shows that banking fraud is rampant and shows no signs of slowing. For instance, fraud cases against financial institutions in the United Kingdom were the highest in 2022 at £305.2m, a 4,333% jump from the same period in the previous year. Another report cited by Hasham et al. (2019) of McKinsey & Company demonstrates that "fraud and financial crime are trillion-dollar industries, with private companies spending in the region of $8.2 billion in anti-money laundering controls alone in 2017."

Technology remains a tremendous ally in fostering innovation, growth and improving competitiveness across all sectors, including the banking industry (Winasis et al., 2020). Technology is fast-evolving, and recent information and communication technology (ICT) advancements have seen commercial banks and other financial institutions embrace digital transformation (Filotto et al., 2021). Winasis et al. (2020) and Yanagawa (2018) point out that the integration of digital technologies and innovative solutions into banking services is driven by the need for operational efficiency, superior customer experience, and adaptation to the ever-evolving market landscape. The proliferation of "big data, 5G, blockchain, artificial intelligence (AI), and other digital technologies have seen new financial services such as online loan issuance, online

account managers, intelligent wealth management, and more become a reality" (Li et al., 2020; Zhu & Jin, 2023; Tang & Yang, 2022).

The unprecedented shift to digital banking platforms is revolutionizing fraud in the banking sector. As Aschi et al. (2022) claim, fraudulent activities have evolved from small-scale criminals attempting to steal modest amounts of money to major and internationally connected networks of criminal groups using sophisticated tools and colluding with corrupt bank staff to steal substantial amounts of money. The digitization of the banking industry has grown tremendously over the decades, and so have the opportunities for fraudsters to exploit. Zabala Aguayo and Ślusarczyk (2020), whose views are consistent with those of Revathi (2019), contend that the increasing concerns surrounding banking fraud, among other financial crimes, "align closely with the escalating adoption of digital solutions in the sector."

In response to the growing prevalence of digital banking fraud, banks and other financial institutions are turning to cybersecurity solutions as a pivotal safeguard against clever, innovative, and opportunistic digital fraudsters (Ghelani et al., 2022). A significant number of banks are adopting tools such as "AI, machine learning (ML) big data analytics, blockchain technology, data loss prevention solutions, e-crime intelligence tools," and network insight products (Manoj, 2021; Ghelani et al., 2022; Camillo, 2017; Maharjan & Chatterjee, 2019). The traditional approaches to fraud management, such as internal and external audits, whistle-blower programs, law enforcement investigations, know-your-customer (KYC) policies, and fraud awareness training, are becoming incapable of producing meaningful results by the day. This study was done to determine the effect of these emerging digital security solutions on fraud risk management in Kenya's banking sector.

1.1.1 Emerging Digital Security Solutions

The complexities of fraud management in the banking sector have seen new technologies valued more and integrated deeply into the overall risk management and compliance framework to identify, prevent, and mitigate fraudulent activities (Ghelani et al., 2022). These emerging technologies complement existing fraud management practices such as KYC, fraud risk governance policies, employee training and education, anti-money laundering (AML) procedures, and ensuring compliance (Bhasin, 2016; Halbouni et al., 2016). The commitment to and

investment in data security solutions goes beyond streamlining fraud management; it also demonstrates an organization's stance on integrity (Bhasin, 2016). The common examples of these technologies include AI, data analytics, ML, digital forensic systems, privileged access management (PAM), zero trust architecture, multifactor authentication (MFA), centralized identity and access management (IAM), blockchain technology, data loss prevention solutions, e-crime intelligence tools, and network insight, and biometrics.

Recent technological trends demonstrate that AI tools are proving to be a formidable force in the fight against digital bank fraud. AI technology, particularly ML and deep learning has become instrumental in detecting and preventing fraudulent activities through pattern and anomaly recognition, behavioural analysis, predictive analytics, and eliminating false positives (Bao et al., 2022). As Bao et al. (2022), Psychoula et al. (2021), and Raman et al. (2023) explain, fusing AI, ML, and data analytics tools into fraud detection systems goes a long way in automating and scaling fraud management processes and making them more accurate, efficient, consistent, faster, and effective.

Digital forensics focuses on identifying, collecting, processing, analyzing, and reporting digital evidence to investigate or prevent crime, making it an essential element of fraud management in digital banking (Dzomira, 2014). The common digital forensic systems “include media management analysis, media analysis, operating system analysis, executable analysis, image and video analysis, and memory analysis” (Dzomira, 2014). In their investigation, Mir et al. (2016) found that adopting seamless digital forensic solutions is instrumental in determining the extent of fraud, identifying perpetrators, and providing crucial evidence for legal proceedings. On the other hand, biometric technology has proven its capability in fraud management but remains underwhelmingly adopted in the banking sector (Hill, 2018). Biometric technologies such as facial recognition or voice verification are crucial in verifying customers" identities. They are becoming a must-have for fraud prevention in banking (Hill, 2018).

1.1.2 Fraud Risk Management

A fraud risk is a potential incident or event that, when it occurs, could have an adverse effect on the viability and sustainability of any organization (Sinha, 2021). The “damage caused by fraud can extend beyond financial losses and regulatory implications; it can also lead to significant

adverse business impact, undermining the relationships, reputation, and brands essential for an organization's growth and success" (Sinha, 2021; Adebayo et al., 2022). The purpose of "fraud risk management is to prevent such outcomes from happening. Fraud risk management is the practice of continuously identifying, analyzing, evaluating, and prioritizing fraud risk accompanied" by a coordinated application of measures to prevent, minimize, and mitigate the impact of unfortunate fraudulent incidents (Rosliana et al., 2022; Sinha, 2021; Mwangi & Ndegwa, 2020). As a highly targeted sector by digital fraudsters, banking is in dire need of a robust fraud risk management framework.

The concept of fraud risk management is broad and complex, meaning no "one-size-fits-all" strategy can be implemented to mitigate fraud. Specific strategies vary between organizations. However, all the strategies fall into the following phases of "fraud risk management: fraud risk assessment, fraud risk governance, fraud risk prevention, fraud risk detection, and monitoring and reporting" (Rosliana et al., 2022; Sinha, 2021). Fraud can happen internally or externally, which is why organizations must have all the necessary tools and a strong governance structure. In Kenya, measures adopted by financial institutions to combat fraud include involving law enforcement agencies such as the Banking Fraud Investigation Unit (BFIU), internal controls, KYC policies, deterrence security controls such as AML regulations, staff training, employee screening, internal and external audits, becoming compliant, and investigations (Lokadio, 2018; Mwangi & Ndegwa, 2020).

1.1.3 Banking Sector in Kenya

The Kenyan banking industry remains resilient despite the prevailing macroeconomic conditions in the country and across the globe (Agusto & Co., 2023). It plays a crucial role in the country's economy, which remains the largest in the East African region, with an estimated GDP of Ksh. 9.9 trillion in the 2022 fiscal year (Abuga et al., 2023). The total assets of the sector in 2022 was Ksh. 6.5 trillion, translating to 66% of the GDP in the same period (Abuga et al., 2023). Kenya's banking sector "comprises 46 commercial banks with branches, agencies, and other outlets throughout the country; one mortgage finance company; nine representative offices of foreign banks; 14 microfinance institutions; 79 foreign exchange (forex) bureaus; and 200 licensed deposit-taking savings and credit cooperative organizations (SACCOs)" (Langat et al., 2021; Muriithi, 2022).

The primary classification of these banks is by ownership, nature, and assets. As pointed out above, most of the banks belong to local individuals/companies, while the rest are foreigners. The classification, by nature, includes “commercial banks and non-bank institutions” (Muriithi, 2022). The third classification is recognized by “the Central Bank of Kenya (CBK) and includes Tier 1 (large banks with at least a hundred billion assets), Tier 2 (medium-sized banks), and Tier 3, consisting of small banks” (Muriithi, 2022). Kenya's banking sector is “dominated by a few commercial banks: Equity Bank, Absa Bank, Diamond Trust Bank, Kenya Commercial Bank (KCB), Standard Chartered Bank, Cooperative Bank, and NCBA” (Muriithi, 2022). At least ten banks in Kenya, including KCB, Equity, and NCBA, have subsidiaries in the East African Community.

Tier 1, 2 & 3 are terms used to describe the financial strength of commercial banks in the context of capital adequacy. The classifications are based on their books, profits and savings, assets and liabilities, market size, and the number of branches. “The Kenyan banking industry is governed by the Banking Act, the Companies Act, the Central Bank of Kenya Act, and prudential guidelines issued by CBK” (Langat et al., 2021). “The banks have come together under the Kenya Bankers Association (KBA), which serves as a lobby for the banking sector's interests. The KBA serves as a forum to address issues affecting members” (Langat et al., 2021).

Kenya’s banking sector is experiencing an unprecedented pace of digital transformation driven by the need for convenience and contactless banking. For instance, a survey by KBA shows that 58.4% of customers preferred mobile banking as a transaction in 2022, up from 52% in 2020. At the same time, the preference for ATM channels was only 9.7% in 2022 compared to 12% in 2020. The “preference for digital banking options is also driven by the increased internet penetration and access to internet-enabled devices” (KBA, 2022). The growth of digital banking has been accompanied by a sudden increase in financial fraud cases. A report on the East African suggests that “Kenya’s financial services sector players top the global list of institutions that have become a prime target of tech-savvy fraudsters preying on unsuspecting customers” (Anyanzwa, 2021). Kenyan banks lose up to Ksh13 billion ($121.49 million) to fraudsters every year.

1.2 Statement of the Problem

Banking systems in Kenya are rapidly moving online, and so is fraud, making the financial services sector a global prime target for tech-savvy fraudsters. As demonstrated by Anyanzwa (2021), "With the advent of digitization and automation of financial systems, financial crimes have become more electronically sophisticated and impersonal," with Kenyan banks losing up to $121.49 million a year.

Rohali et al. (2022) and Harun (2023) found that security and fraud protection are crucial determinants for customers when choosing a bank today. The number of institutions that have adopted and derived meaningful value from emerging anti-fraud technologies is low. Only 61% of organizations have implemented enhanced internal control by leveraging advanced solutions, with the majority of them being "communications monitoring (57%), transaction testing/monitoring (55%), anomaly detection (41%), contract review (35%), data visualization (35%), pattern recognition (29%), predictive analytics (23%), and AI (14%)" (PwC, 2021). As shown above, innovative solutions such as biometrics, AI and ML, and data analytics remain underexploited (PwC, 2021).

Empirical data is important in making critical decisions, such as implementing new digital security solutions to combat fraud. A framework for quality information helps guide decisions about what new technologies to adopt, when and how, their roles and effectiveness, and more, especially considering that combatting banking fraud is a continuous process that requires organizations to adapt and be steps ahead of the innovative nature of fraudsters. Whereas the current body of empirical literature suggests emerging security solutions have a positive impact on fraud management, the difference in opinions regarding specific technologies is apparent among researchers.

A multitude of studies demonstrate the positive effect of emerging technologies on fraud risk management (Bhasin & Rajesh, 2022; Ngava, 2015; Bhasin, 2016; Aschi et al., 2022; Hussaini et al., 2021; Victory et al., 2022; Kiragu, 2013; Fatoki, 2023; Okoye & Ndah, 2019; Chukwuma et al., 2022). Another set of empirical studies argues otherwise, suggesting that emerging digital

security solutions translate negatively on fraud management (Josyula et al., 2023; Rad, 2021; Tropina, 2016; Khailtash & Lindqvist, 2022).

Another set of empirical studies argue otherwise. For instance, Tropina (2016) noted that while technology continues to be embraced in identifying, assessing, and responding to fraud, it is also emerging as a powerful tool for perpetuating financial fraud. For example, "blockchain, AI, robotic process automation (RPA), and data analytics may provide new opportunities for fraudsters to take advantage of companies or consumers" (Rad, 2021). Also, Rad (2021) warns of technology being a double-edged sword for financial fraud risk management, citing that the adoption of digital solutions continues to attract new sets of fraudsters.

In another study, Josyula et al. (2021) found that "AI has not yet attained the efficiency regarding financial fraud risk management. It is still reliant on human intervention, making it prone to bias and unable to handle non-routine risk environments. "Khailtash and Lindqvist (2022) found that adopting AI resulted in new technological and regulatory risks for companies.

Researchers have varying opinions on the effect of emerging security solutions on fraud risk management. As a result, there is a lack of consensus on the impact of emerging technologies such as AI, data analytics, and biometrics on fraud risk management. In addition, there is insufficient empirical evidence contextualizing the phenomenon in Kenya's banking sector. This study addresses the gap.

1.3 Objective of the Study

The study was guided by one general objective and three specific objectives as outlined below:

1.3.1 General Objective

To investigate the effect of emerging digital security solutions on fraud risk management in Kenya's banking sector.

1.3.2 Specific Objectives

i. To examine the effect biometrics have on fraud risk management in Kenya's banking sector

ii. To determine the effect AI solutions have on fraud risk management in Kenya's banking sector
iii. To examine the effect data analytics have on fraud risk management in Kenya's banking sector

1.4 Research Questions

i. How does biometric technology affect fraud risk management in Kenya's banking sector?
ii. What effect does the AI solutions have on fraud risk management in Kenya's banking sector?
iii. How do data analytics affect fraud risk management in Kenya's banking sector?

1.5 Scope of the Study

The study aimed to determine the effect of emerging digital security solutions on fraud risk management in Kenya's banking sector. Biometrics technology, AI technology and data analytics served as the independent variables and fraud risk management as the dependent variable. The scope of the study was limited to the banking sector in Kenya. More specifically, the study surveyed commercial banks in Kenya. These banks formed the unit of analysis for the study from whom the respondents were drawn.

1.6 Significance of the Study

The outcome of this study, as well as its recommendations, are valuable in various ways. For instance, the key stakeholders in Kenya's banking sector will benefit tremendously from the study. In particular, commercial banks will find this research valuable as the findings and recommendations will help the banks integrate ultramodern technologies into their risk management frameworks as part of their strategies to combat fraud more effectively.

The outcome of the study, as well as its recommendations, provides valuable insights to inform the policymaking process in the country around the creation and adoption of innovative technologies to fight incidences of fraud. The information from the study would help regulators

understand the role of emerging technologies in confronting fraudulent crimes. As a result, it serves to inform the formulation of industry-wide policies for fighting financial fraud.

This research also benefits the scientific research community. It achieves this by addressing the existing knowledge gap on the effect of emerging technologies on fraud risk management in the banking sector. Researchers, scholars, and academicians interested in the topic would gain quality and up-to-date information on the phenomenon. In addition, it would help future researchers develop literature, formulate research hypotheses, and guide the entire research process.

The general public, including consumers, can benefit from the knowledge created by this research. The information provided can help them understand the role and impact of emerging technologies in combatting fraud. Such information can help them make wise decisions on what banks to engage with when it comes to fraud risk management.

Therefore, this research study has a diverse range of target audiences and multiple uses depending on the audience, as described above. Effective dissemination of the findings is ensured to enhance the intended uses of the study. Write-ups and publications in the correct format, language and tone are maintained.

1.7 Chapter Summary

Banks and other financial institutions are increasingly leveraging emerging and innovative solutions in the digital space to fight fraud. While this trend is common, the effect of some of these solutions in enhancing financial fraud detection and prevention remains unexplored in the scientific research community.

The study aimed to determine the effect of emerging digital security solutions on fraud risk management in Kenya's banking sector. Following an extensive review of existing studies on this topic, research gaps were identified, which led to the formulation of the problem statement. Researchers have varying opinions on the effect of emerging security solutions on fraud risk management. Several studies demonstrate the positive effect of emerging technologies on fraud risk management. On the other hand, other studies argue that emerging technologies are a powerful tool for perpetuating financial fraud, and other studies cite that some technologies still have a high

reliance on human intervention, hence making then none effective when it comes to fraud risk management. As a result, there was a lack of consensus on the effect of emerging technologies such as AI, data analytics, and biometrics on fraud risk management. The study aimed to address this gap.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

In this chapter, the theoretical underpinning of the study will be provided and an in-depth review of literature relevant to the topic. More specifically, the section covers theories that were made for the theoretical framework, empirical literature review, literature gap, conceptual framework and how variables were operationalized.

2.2 Theoretical Framework

The "theoretical framework plays a fundamental role in providing a foundational structure that can hold or support the theory of a research study" (Kivunja, 2018). It is necessary "to explain a phenomenon, draw conclusions, and make predictions in research studies" (Kivunja, 2018). The theories that underpinned the study are discussed in detail below.

2.2.1 The Fraud Triangle Theory

The "fraud triangle theory was developed in 1953 by an American criminologist, sociologist, and penologist, Donald R. Cressey" (Mansor & Abdullahi, 2015). It proposes that "individuals are motivated to commit fraud when three conditions are fulfilled: some kind of pressure, perceived opportunity and rationalization for fraud" Mansor and Abdullahi (2015). For instance, according to Cressey, pressure is "the incentive that could motivate an individual to commit fraud", and it can range from personal financial issues to the work environment (Sujeewa et al., 2018). The perceived opportunity, as Cressey illustrated, "constitutes two components: general information and technical skill" (Sujeewa et al., 2018). On the final piece of the fraud triangle, rationalization, according to Sujeewa et al. (2018), the majority of people will not choose to engage in fraud unless they can justify why the illegal behaviour is intelligible.

Cressey's fraud triangle theory is a popular framework in fraud literature and serves as the basis for most discussions of broader white-collar crimes. Puspasari (2015) found that the theory was relevant and useful in the prevention of fraud in Indonesia's government. It helps map out "*who*

could be the perpetrators of fraud, *why* they commit fraud, and *how* to prevent fraud" Puspasari (2015). Similarly, Rahman and Jie (2024) found the fraud triangle model instrumental in detecting fraud in China. A major critique of the theory is that it reduces the "complex nature of fraud to just three factors: pressure, opportunity, and rationalization, ignoring the diversity of criminogenic influences" inherent in fraudulent activities (Lokanan, 2015). Nonetheless, since the focus area for this research is fraud risk management, the theory was relevant to this study.

2.2.2 Fraud Diamond Theory

The "fraud diamond theory was presented by David Wolfe and Dana Hermanson in 2004, and it is considered an expanded version of the fraud triangle theory" (Sujeewa et al., 2018). The theory proposes that "while pressure, perceived opportunity, and rationalization influence may exist for one to commit fraud, fraud is unlikely unless the element of capability (capacity) exists" (Sujeewa et al., 2018). In other words, as Wolfe and Hermanson emphasized, pressure, opportunity, and rationalization are not enough unless an individual has the skills and abilities to commit fraud. As Sujeewa et al. (2018) write, "Wolfe and Hermanson believe that the fraud triangle could be enhanced to improve both fraud prevention and detection by considering a fourth element."

The theory is also popular in fraud literature, and it has extensive applications in formulating frameworks for detecting and preventing fraud. Gbegi and Adebisi's (2013) research is a classic example of its application in the corporate environment. According to the researchers, the theory can provide a sufficient framework for forensic accounts to investigate fraud. The model can help determine motivations for fraud, map out the opportunities for fraud, such as lack of proper controls, and identify fraudsters based on capabilities. However, although "an extension of the fraud triangle theory, the four diamonds theory also limits fraud to just four elements, which may not always be the case" (Sorunke, 2016). Nevertheless, it was useful in determining the effect of emerging digital security solutions in fraud risk management.

2.3 Empirical Review

An empirical review of literature is the systematic analysis and evaluation of previous research studies on the topic under investigation. It aims to provide an overview of current knowledge on the phenomenon and identify relevant theories, research methods, and gaps in the existing research

that can be applied to the study. This section reviews previous studies on the effect of emerging digital security solutions on fraud risk management in the banking sector to identify knowledge gaps in the current body of empirical work.

2.3.1 Biometrics and Fraud Risk Management

A study that looks into the relationship between biometrics and fraud management was conducted by Gisairo (2016), who sought to determine "the effectiveness of biometrics technology in curbing fraud in medical insurance firms in Kenya". Adopting a cross-sectional descriptive design, this study was also based on primary data gathered from the representatives of the selected 18 medical insurance firms using questionnaires and secondary data from the Insurance Fraud Investigation Unit (IFIU) database. Correlational and regression analyses were used to analyze data. Gisairo (2016) found that "the value of reported fraud cases significantly increased with the value of claims authenticated via biometric technology". In other words, biometrics technology was effective in fighting fraud. However, the context of this study was the medical insurance sector, meaning its conclusion cannot be accurately inferred from Kenya's banking system. It is a limitation that the current study sought to address.

In a similar investigation but in the banking sector, Banga and Pillai (2021) sought to examine "the impact of behavioural biometrics on mobile banking systems". The "technology acceptance model (TAM) and theory of reasoned action (TRA) models were made for the study's theoretical framework, and a qualitative research design was adopted where data was collected from previous literature and analyzed using a systematic review of the literature technique" (Banga & Pillai, 2021). The study found that behavioural biometrics significantly impacted mobile banking systems. However, the degree of significance varied with specific techniques of behavioural biometrics. Fingerprint, retina scan, and DNA scans had the highest impact, with face recognition and voice recognition having the lowest impact. The limitation of the study is that it was based on secondary data, which is why the present study was based on primary data.

Adopting a similar approach as Banga and Pillai (2021), Singh et al. (2019) investigated the effect of using biometrics on the prevention of payment card fraud. To achieve this objective, the study was an SRL with a qualitative research design where data was obtained from scholarly materials from reputable online databases. Thematic analysis technique was used to analyze data. It was

observed that biometric technology was effective in preventing payment card fraud. Singh et al. (2019) further proposed a novel approach to preventing card fraud using biometrics. The approach involves integrating physiological and behavioural biometrics on existing card security systems to ensure the presence of cardholders at the time of processing transactions to mitigate fraud. The study was, however, limited to secondary data, a limitation the current study sought to address by collecting primary data.

In Russia, Bakunova et al. (2019) sought to examine "the effectiveness of biometrics as a method of information security in the banking sector digitization." The principles of the qualitative research design were applied, and the researcher analyzed reports from the Central Bank, researched financial technology development, and researched biometric technology in the financial market. The study employed mathematical, statistical, and synthesis and analysis methods for data collection and analysis. The study's outcome suggests that the application of biometrics in information systems narrows the scope of activity from criminal actors, thereby positively affecting the fight against fraud in the banking sector. The study was limited to Russia's banking sector and based on secondary data. The current study was based on primary data collected in Kenya's banking sector.

Elsewhere in Nigeria, Talabi et al. (2021) sought to analyze the "cybersecurity and related risk management challenges in identity systems by undertaking a comparative analysis of different biometric traits." The study followed the principles of general deterrence, TAM, planned behaviour theory, and protection motivation theories for the theoretical framework. The methodology employed to complete the study were descriptive, analytical, and empirical techniques. Primary data was collected from a sample recruited from various organizations using biometrics in their information security. The study found that a multimodal identification and authentication system combining different elements of biometrics significantly impacted the effectiveness of the cybersecurity risk management framework. The gap identified in the study is that it was limited to Nigeria and covered cybersecurity risk management as the outcome variable. The present study was conducted in Kenya's banking sector, covering fraud risk management as the outcome variable.

2.3.2 AI and Fraud Risk Management

In their investigation, Josyula et al. (2023) sought to "determine whether AI is an efficient financial fraud risk management technology". The study employed "an integrative literature review approach, exploring previous empirical and theoretical literature on the topic" (Josyula et al., 2023). Data was comprehensively gathered from peer-reviewed materials from Google Scholar, Research Gate, Proquest, PubMed, Springer, Emerald, Science Direct, and other reputable online databases. It was discovered that "AI had not yet attained efficiency for financial fraud risk management; the findings further illustrated that the technology was still overly reliant on human intervention, thus prone to bias and unable to handle non-routine emergency risk environments" (Josyula et al., 2023). The limitation identified in the study is that it was based on secondary data and adopted a qualitative design. The present study followed a quantitative design based on primary data.

Unlike Josyula et al.'s (2023) research, Khailtash and Lindqvist (2022) adopted a quantitative study approach to "investigate the impact of AI on risk management approaches in the banking sector." Dynamic risk management and multi-level perspectives were used for the study's theoretical framework, and descriptive research was followed for the research design. Data was collected from 12 respondents recruited through a purposive sampling technique, and semi-structured questionnaires were used to collect data. A thematic model was used for data analysis, where themes in the research instrument were identified and categorized. The study found that adopting AI led to a set of new organizational and regulatory risks, prompting users to revise how they classified risks. The study was limited to the banking sector in Stockholm, Sweden, meaning its results cannot be inferred from Kenya's banks, a limitation the present study sought to address by studying Commercial banks in Kenya.

Also, using a quantitative approach in the United Arab Emirates (UAE), Abdulrahman (2019) "conducted a study to examine the impact of AI" in detecting fraud. "A descriptive research design was adopted to complete the study based on both qualitative and quantitative data from a sample of 200 respondents recruited from the UAE banking sector" (Abdulrahman, 2019). These respondents represented professionals working in the fraud detection department and were selected using "simple random sampling and 10 data scientists from the same sector; the data collected was

analyzed using the deductive data analysis approach" (Abdulrahman, 2019). The study found that AI-based tools had a significant impact on fraud detection. The outcome of the study is instrumental in understanding the topic. However, it was geographically limited to UAE's banking sector, meaning its conclusion cannot be inferred from Kenya's banking sector, the area the present study sought to cover.

Adopting a meta-analysis approach similar to Josyula et al. (2023), Sood et al. (2023) conducted an elaborate study to analyze "the role of AI in detecting and preventing financial fraud using natural language processing (NLP)". 241 peer-reviewed materials sourced from the Scopus database and published within the last two decades at the time of the study were systematically reviewed and analyzed. The VOS viewer tool and K-means clustering were used for author-coauthor network collaboration and to identify the critical research domain, respectively. The outcome of the study suggests that NLP was instrumental in identifying unusual or out-of-the-ordinary transactions that may indicate fraud. The study focused solely on NLP as an element of AI, a limitation the present study sought to address by exploring AI as a whole.

Elsewhere in India, a study more similar to Sood et al. (2023) but focused on ML, a subset of AI, was conducted by Shah (2022), who sought to "examine the extent to which it is efficient in detecting financial fraud using mobile transaction metadata". The analysis adopted the Naïve Bayes model, a mathematical formula for determining conditional probability. "The Paysim Synthetic dataset of mobile money transactions was also employed, and data was analyzed using the Confusion Matrix" (Shah, 2022). The study found that with a success rate of 99.6%, ML was extremely efficient at detecting financial fraud in mobile transactions. However, the study was based in India, and its context was not the banking sector; it focused on mobile transactions. The present study was based in Kenya and will cover the banking sector.

In a separate investigation, Tiwari (2023) sought to determine "the application of AI and ML in the financial industry and its effects on risk management and fraud detection". The study adopted a meta-analysis research design as the methodology to fulfil the objective. Ten peer-reviewed articles were identified and selected from JSTOR, ProQuest, and Google Scholar. These articles were analyzed using a thematic analysis model. The researcher made four observations: AI-based systems improved the efficiency and effectiveness of fraud detection, AI-based systems improved

risk management, AI and ML improved the performance of financial institutions, and AI and ML significantly improved fraud detection and risk management. The study provided useful insights into the topic but was limited in that it was based on secondary data. The present study was based on primary data.

2.3.3 Data Analytics and Fraud Risk Management

Tang and Karim (2019) aimed to examine "the application of big data analytics to the brainstorming session in the current auditing standards." In particular, the researchers determined the role of data analytics in financial fraud detection for auditors. The study adopted the systematic literature review (SLR) approach, where scholarly articles were selected and analyzed. Tang and Karim (2019) found that "integrating big data analytics into brainstorming sessions can broaden the information size, strengthen the results from analytical procedures, and facilitate auditors" communication." The study was limited to auditing practice, implying that it cannot be inferred from Kenya's banking. A study that focuses on the banking sector is warranted, and the present study sought to address this limitation.

Still in the auditing sector as Tang and Karim (2019), but from a government's perspective, in another study, Koreff et al. (2021) explored "how government-related audit data analytic tools promote the abuse of power by auditors, enabling politically sensitive processes that encourage industry-wise normalization of behaviour." The study adopted a positivist cross-sectional case study design. A sample of 40 individuals representing C-level executives, high-ranking clinical personnel, directors, and consultants in America's healthcare sector. The interviews were pilot-coded and assigned descriptive labels to ensure the themes focused on the use of audit data analytics. The outcome of the study showed that "people raised several concerns about the use of data analytics by government auditors" (Koreff et al., 2021). The evidence of the use of rule-based, anomaly, and network models is shown, and even those models yield false positives. The study shows the potentiality of data analytics being exploited for the wrong reasons.

Deviating from the direction of Tang and Karim (2019) and Koreff et al.'s (2021) studies, Novita and Anissa (2022) examined "the role of data analytics in detecting fraud in the public sector in Indonesia. The study followed the principles of fraud triangle theory for the theoretical framework and adopted a descriptive research design." The study employed non-probability sampling to

recruit a sample of 33 examiners and auditors in the State Finance Auditor I to VII and the Main Investigation Auditor for the study. Questionnaires were used as research instruments, and data was analyzed using quantitative statistical techniques (correlation and inferential analyses) via STATA version 14. Novita and Anissa (2022) found that "data analytics has a positive and significant effect on the indications of fraud for public sector examiners and auditors." The limitation of the study is that it was based in Indonesia and contextualized to the government sector. The conclusions made cannot be generalized to the banking sector, which the present study sought to cover.

Handoko and Rosita (2022) embarked on a study examining "the effect of scepticism and big data analytics on financial fraud detection as moderated by forensic accounting". This was a "quantitative study in which the hypothesis between the independent (scepticism and big data analytics), moderating (forensic accounting), and dependent (financial fraud detection) variables was tested" (Handoko & Rosita, 2022). Questionnaires were the instrument of data collection and correlational and inferential statistics adopted for data analysis. The results of the study showed that "professional scepticism and big data analytics have a significant impact on financial fraud detection; forensic accounting moderate both professional scepticism and big data analytics" (Handoko & Rosita, 2022). The study was limited in conceptual framework, area of coverage, and context. The proposed study will address these limitations by focusing on the effect of data analytics on fraud risk management in the banking sector.

Elsewhere in Germany, Trierweiler (2019) conducted a study to "evaluate the use of big data analytics and its role in facilitating compliance and fraud prevention." The study adopted a multi-step empirical design with a mixed methods approach. Directors, fraud managers, and compliance managers were recruited from IT-related departments among companies in the German-speaking areas. Interviews and questionnaires were employed as data collection methods from the recruited subjects, and they were analyzed using qualitative content and quantitative content analysis techniques. The researcher observed a smaller distribution of IT and analytical tools for fraud detection and prevention in the surveyed organizations. However, the few that adopted these solutions benefited significantly in becoming compliant and curbing fraud.

2.4 Literature Review Summary and Knowledge Gap

Table 2.1 summarizes the reviewed empirical literature and knowledge gaps identified from the analyzed studies. Also provided is a brief description of how the study proposes to fill these knowledge gaps.

Table 2. 1: Summary of Literature and Knowledge Gaps

Author	Objective	Findings	Knowledge gap	Type of Gap	Focus of this study
Gisairo (2016)	To determine the effectiveness of biometrics in curbing fraud in Kenya's medical insurance firms.	The results show that increasing use of the authentication capabilities of the biometrics technology saw a significant rise in the value of reported fraud cases.	The study was limited to medical insurance firms	Contextual	The study was based on data collected from commercial banks
Tang & Karim (2019)	To analyze the role and implications of big data analytics on the detection of financial fraud from an auditor's perspective.	It was discovered that when big data analytics is integrated into auditors' brainstorming sessions, information size is broadened, communication is facilitated, and results of analytical procedures are strengthened.	This was an SRL study limited to auditing practice, implying that the findings cannot be inferred to the banking sector.	Scope, Methodology	The present study focused on the banking sector.

Author	Objective	Findings	Knowledge gap	Type of Gap	Focus of this study
Bakunova et al. (2019)	To evaluate the role of biometric technology as an information security solution for the digitization of the banking sector.	The technology was found to help curb fraud in banking when used as an information security solution.	This is a qualitative study limited to Russia's banking sector and based on secondary data.	Scope, Methodology	The current study was based on primary data collected in Kenya's banking sector.
Trierweiler (2019)	To analyze how using big data analytics helps facilitate fraud prevention and compliance.	The researcher found that increased use of big data analytics facilitates fraud prevention and compliance significantly.	The study was conducted in Germany and did not focus on the banking sector	Scope	The study was conducted in Kenya and focused on the banking sector.
Talabi et al. (2021)	To examine the effect of using authentication based on biometric multimodal in cybersecurity risk management in identity systems.	A multimodal identification and authentication system that combines different elements of biometrics had a significant impact on the effectiveness of the cybersecurity risk	The gap identified in the study is that it was limited to Nigeria and covered cybersecurity risk management as the outcome variable.	Scope, conceptual	The present study was conducted in Kenya's banking sector and covered fraud risk management as the outcome variable.

Author	Objective	Findings	Knowledge gap	Type of Gap	Focus of this study
		management framework.			
Banga & Pillai (2021)	To analyze how behavioural biometrics influences mobile banking systems.	Behavioural biometrics was a significant factor in the mobile banking system.	The study was based on secondary data.	Scope, Methodology	The study utilized primary data.
Koreff et al. (2021)	To assess the use and influence of data analytics in auditing healthcare fraud.	The study observed that government auditors raised multiple concerns over the use of data analytics. Models used yielded false positives.	The study was conducted in the healthcare sector. Failed to highlight the relationship between data analytics and fraud risk management	Contextual	The study focused on data analytics and fraud risk management in Kenya's banking sector.
Novita & Anissa (2022)	To explore data analytics and its role in indicating fraud in the government sector.	A positive and significant correlation was observed between data analytics and the indications of fraud.	The limitation of the study is that it was based in Indonesia and contextualized to the government sector. The conclusions made cannot be generalized to the banking sector.	Scope, contextual	The present study focused on the banking sector in Kenya.

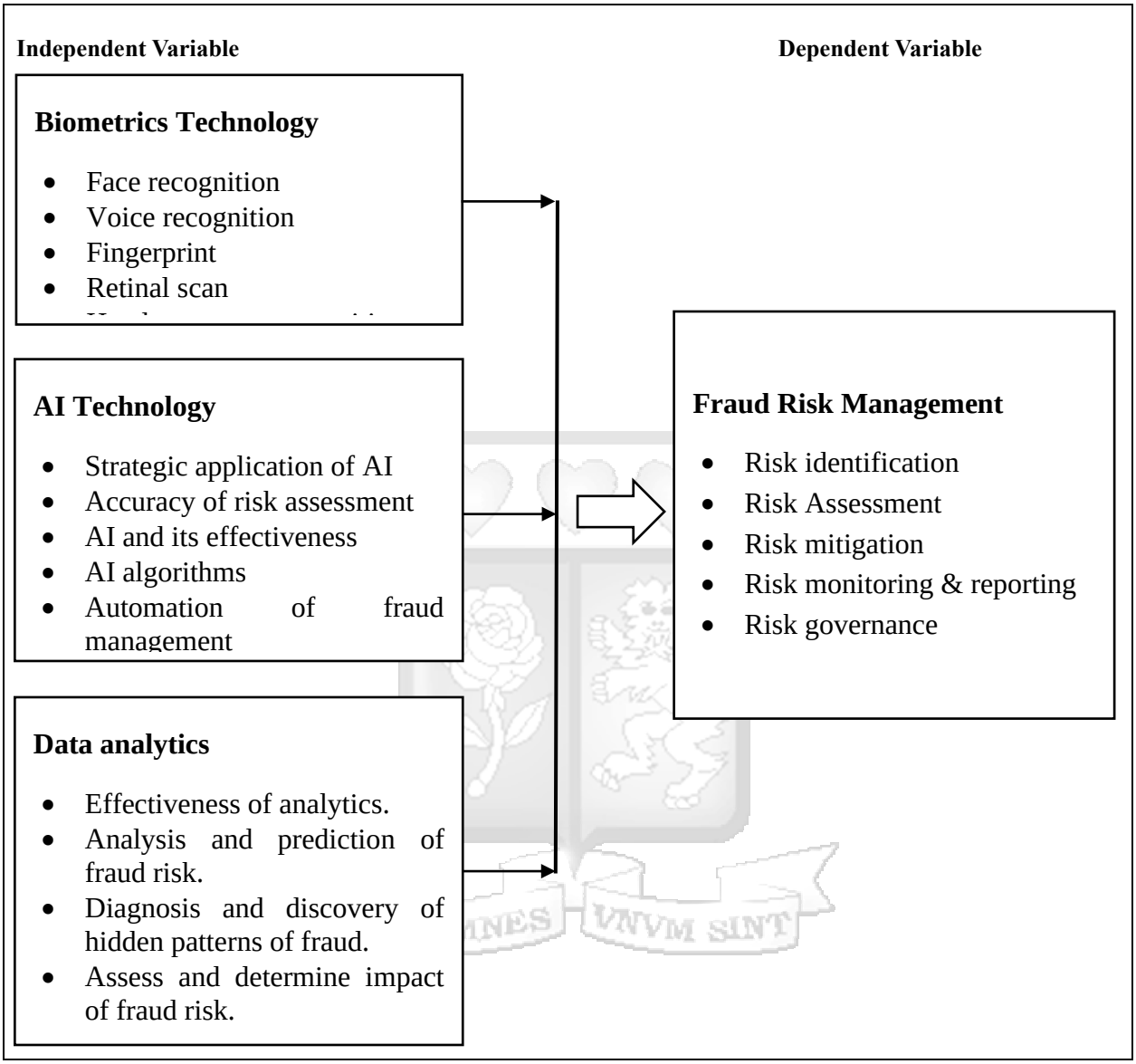
Author	Objective	Findings	Knowledge gap	Type of Gap	Focus of this study
Handoko & Rosita (2022)	To analyze scepticism and data analytics and determine their influence on the detection of financial fraud, forensic accounting serves as the moderating variable.	Financial fraud detection was found to be strongly and positively impacted by big data analytics and professional scepticism. Also, it was observed that data analytics and professional scepticism were moderated by forensic accounting.	The study was limited in conceptual framework, area of coverage, and context.	Conceptual, scope, contextual	The proposed study focused on the effect of data analytics on fraud risk management in the banking sector.
Sood et al. (2023)	To test how AI helps detect and prevent financial fraud using NLP.	NLP was instrumental in identifying unusual or out-of-the-ordinary transactions that may indicate fraud	The study focused solely on NLP as an element of AI and used a meta-analysis design.	Conceptual, methodology	The present study addressed this by exploring AI as a whole
Josyula et al. (2023)	To determine the efficiency of AI in financial fraud risk management.	It was discovered that AI has yet to attain efficiency in applications in financial fraud risk management.	It was based on secondary data and adopted a qualitative design	Methodology	The proposed study followed a quantitative design and was based on primary data.

Author	Objective	Findings	Knowledge gap	Type of Gap	Focus of this study
Tiwari (2023)	To analyze how the use of AI and ML influences fraud detection and risk management in the financial industry.	AI improved the efficiency and effectiveness of fraud detection, improved risk management, improved the performance of financial institutions, and significantly improved fraud detection and risk management.	The study was limited in that it was based on secondary data	Methodology	The present study was based on primary data

2.5 Conceptual Framework

A "conceptual framework, or conceptual model, is a visual representation of the expected relationship between variables in a study" (Varpio et al., 2020). By highlighting the relationship between variables, the conceptual framework "defines the relevant research objectives for the research process and maps out how they come together to draw coherent conclusions" (Varpio et al., 2020). In this survey, emerging digital security solutions were the independent variable and were represented by biometrics, AI, and data analytics, whereas fraud risk management was the dependent variable, as shown in Figure 2.1.

Figure 2. 1: Conceptual Framework



2.6 Operationalization of Variables

Whereas "the conceptual framework illustrates the relationship between variables in a study, the operationalization of variables describes how the variables will be defined and measured" (Edmonds & Gudmestad, 2018). It involves turning abstract concepts of the variables into measurable or quantifiable indicators. According to Edmonds and Gudmestad (2018), variables need to be operationalized in a way that permits their accurate measurement. The variables, indicators, and scale of measurements are illustrated in Table 2.2.

Table 2. 2: Operationalization of Variables

Variables	Indicators	Measurement (scale)	Source
Dependent Variable			
Fraud Risk Management	• Risk identification • Risk Assessment • Risk mitigation • Risk monitoring & reporting • Risk governance	5-Point Likert Scale	(Mwangi & Ndegwa, 2020; Sinha, 2021; Chen et al., 2015)
Independent Variables			
Biometrics Technology	• Face recognition • Voice recognition • Fingerprint • Retinal scan • Hand geometry recognition	5-Point Likert Scale	(Goode, 2018; Gupta & Varma, 2019)
AI Technology	• Strategic application of AI • Accuracy of risk assessment • AI and its effectiveness • AI algorithms • Automation of fraud management	5-Point Likert Scale	(Choi & Lee, 2018; Bao et al., 2022)
Data Analytics	• Effectiveness of analytics. • Analysis & prediction of fraud risk. • Diagnosis & discovery of hidden patterns of fraud. • Assess & determine the impact of fraud risk. • Data integration.	5-Point Likert Scale	(Kambatla et al., 2014; Moreira et al., 2018; Runkler, 2020)

2.7 Chapter Summary

In this section of the study, peer-reviewed articles on the effect of emerging digital security solutions on fraud risk management were identified, reviewed, and analyzed. The review was broken down into the established objectives of the study: the effect of biometrics technology, AI, and data analytics on fraud risk management. These empirical studies were reviewed through the lenses of the fraud triangle and fraud diamond theories, which will make for this study's theoretical framework. Emerging digital security solutions and fraud risk management remain inconsistent in the reviewed literature, with conceptual, research design, and scope limitations evident in some of these studies.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter details the specific procedures and techniques for collecting, processing, and analyzing data on the topic. The chapter focuses on the "how" the study was carried out. This section discusses the philosophy and design of the study adopted, how data was collected and analyzed, and the target population and sampling methods. Also discussed are the enhanced research quality and ethical standards.

3.2 Research Philosophy

Edson et al. (2016) define “a research philosophy as a set of beliefs, assumptions, and principles that guide the design and execution of a research study.” This research study adopted the positivism paradigm of research. Park et al. (2020) indicate that “positivism is rooted in the belief that knowledge can be obtained through objective observations and measurements”. In simpler terms, the philosophy assumes that “answers to the research questions can be obtained by systematically measuring and analyzing data, particularly statistical or numerical data” (Park et al., 2020). Therefore, according to the principles of the positivist worldview, as Park et al. (2020) further demonstrate, “only the factual knowledge gained through objective observation, including measurement, is trustworthy”.

The positivist research paradigm stresses the importance of conducting quantitative research in a setting where variables can be controlled and measured (Edson et al., 2016). So, it typically manifests in research methodologies that utilize quantitative data. Since positivism emphasizes objective measurement and reason, a research study that adheres to this school of thought produces objective findings since it is free from human misinterpretation or prejudice (Edson et al., 2016; Park et al., 2020). In this case, positivism, as a research philosophy, was instrumental in collecting and analyzing quantitative data in an objective manner which was instrumental in quantifying the extent to which emerging technologies' affect fraud risk management in Kenya's banking sector.

3.3 Research Design

A "research design is the blueprint of a scientific study that outlines the methodologies, tools, and techniques for conducting the study" (Abbott & McKinney, 2013). In simpler terms, it is the strategy employed to answer the research questions using empirical data. There are "several research designs, including quantitative, qualitative, experimental, correlational, explanatory, diagnostic, and descriptive" (Abbott & McKinney, 2013). A cross-sectional descriptive research design was adopted in this study. This design aims to observe and measure a phenomenon without attempting to infer the causal or other hypothesis. The design was suitable for exploring the effect of emerging digital security tools on fraud risk management in the banking sector.

3.4 Population and Sampling

3.4.1 Population

In scientific research, "a population is a group of individuals, items, entities, or objects that have similar characteristics. Population is the entire group a researcher intends to draw conclusions about" (Ishak & Abu Bakar, 2014). The population for the study constituted the cohort of the "42 registered commercial banks in Kenya" (Appendix). More specifically, the study targeted management-level employees with knowledge of, interaction with, and experience with emerging digital security solutions.

3.4.2 Sampling

3.4.2.1 Sampling Frame

According to Ishak and Abu Bakar (2014), "a sampling frame is the source material or device from which a sample is drawn". Put simply, it is the population of interest for a research study. In this case, the subset of the target population where the sample for the study was selected includes the risk management, IT, and compliance departments of the 42 commercial banks in Kenya.

3.4.2.2 Sampling Technique

The study utilized a stratified sampling technique to select and recruit respondents. Acharya et al. (2013) define stratified sampling as "a probability sampling method in which a population is

divided into different strata and randomly selected". In this case, a stratum is a mini-representation of the population. As such, the population was divided into three strata per commercial bank, with each stratum representing the risk management, IT, and compliance departments. One respondent was selected randomly from each of the 126 strata. Therefore, the sample size for the study was 126 risk management, IT, and compliance professionals from 42 commercial banks in Kenya.

3.5 Data Collection

Data should be "collected and measured systematically, enabling a researcher to sufficiently respond to research questions, test hypotheses, and evaluate the study's outcome. Appropriate and accurate data collection methods and processes are essential to achieve the above" (Mazhar et al., 2021). For this reason, the study adopted a survey method for data collection in which structured questionnaires were employed as a data collection instrument. These questionnaires were distributed online using Google Forms. Links to the pre-populated online questionnaires were sent to the target respondents via email and text.

As a data collection tool, "a structured questionnaire comprises a set of standardized and close-ended questions with a specific scheme and sequencing, allowing for limited, quick, and quantitative responses" (Roopa & Rani, 2012). The questionnaire design constituted sections with sets of questions that aim to answer the research objectives/questions. Variables were measured using a Likert five-point scale "where 1=strongly disagree, 2 = disagree, 3 = neither agree nor disagree, 4 = agree, and 5 = strongly agree" (Appendix 1). The filled questionnaires were collected and prepared for analysis.

3.6 Data Analysis

Data analysis is "the systematic processing of applying statistical tools and techniques to process raw data and turn it into meaningful information" (George & Mallery, 2018). The completed questionnaires were collected, sorted, and checked for accuracy and consistency. They were then cleaned for errors and omissions to ensure data eligibility for analysis. Once the eligibility of data was ascertained, the data was coded, categorized, and input into computer software, Microsoft

Excel and SPSS for analysis. Descriptive, correlational, and multiple regression statistics were adopted for analysis.

3.6.1 Descriptive Statistics

Descriptive statistics seeks to summarize the characteristics of a given data set. It summarizes, organizes, and presents data logically, meaningfully, and efficiently. The measures of central tendency, frequency, variability, and distribution, as well as statistical techniques of descriptive statistics, were instrumental in summarizing respondents' demographic profiles. Besides summarizing the sample, descriptive statistics were useful in summarizing responses from the research participants in which "mean, mode, and standard deviation" were used (George & Mallery, 2018).

3.6.2 Correlation Analysis

Correlation analysis, "also bivariate analysis, is used to determine whether a relationship exists between variables and determine the magnitude of the relationship" (Sheard, 2018). This statistical method was used for Objectives 1, 2, and 3. Here, correlation statistics were used to test how each independent variable correlates with the dependent variable. The presence of linear regression is denoted by correlation coefficient values that fall within the -1 to +1 range (Sheard, 2018). As Sheard (2018) further points out, "a negative coefficient shows the presence of a negative correlation, a positive coefficient shows a positive correlation and 0 means there is no correlation between the variables".

3.6.3 Regression Analysis

Correlation analysis analyzes the presence of correlation between two variables, and "regression analysis analyzes the relationship between a single dependent variable and several independent variables" (Mertens, 2017; Sheard, 2018). It was used to determine the functional relationship between the predictor variables (biometrics, AI, and data analytics) and the dependent variables (fraud risk management).

However, before performing the regression analysis, the study performed diagnostic tests to check for the appropriateness of the regression model. These tests included the test for normality,

heteroscedasticity, autocorrelation, and multicollinearity. They were performed to check for assumptions of normal distribution, presence of homoskedasticity, lack of autocorrelation between the independent variables, and absence of multicollinearity, respectively.

The regression equation used includes:

$$Y = \alpha + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon$$

Where;

Y = Fraud risk management

α = Constant

β= Beta coefficients

X_1= Biometrics technology

X_2= Artificial intelligence (AI)

X_3= Data analytics

ε = error term

3.7 Research Quality

Aksnes et al. (2019) mention that "the whole point of research is to produce reliable data that yields rigorous and reproducible research results". Therefore, researchers have the responsibility of delivering good quality research conducted with a rigorous scientific approach that is trustworthy and credible. To achieve this, certain standards must be followed.

3.7.1 Reliability

Reliability "refers to the ability of a research study to be consistent or produce the same results over and over. For the purpose of ensuring the reliability of the current research, a pilot study was conducted" on individuals with similar characteristics as the target population to ascertain the reliability of the research instrument (Roberts & Priest, 2006). The pilot study was done at NCBA bank and targeted ten individuals who fit the profile of the target population. The data was then

subjected to Cronbach's Alpha scale to check for internal consistency and modified accordingly to ensure an acceptable level of internal consistency. The value falls within the accepted 0.7 and 0.90 range of Cronbach's Alpha values.

3.7.2 Validity

Validity refers to “the appropriateness of measures used, the accuracy of the analysis, and the ability to generalize the findings of a research study” (Roberts & Priest, 2006). A valid research study conveys data that accurately reflects the genuine feedback of the respondents. The validity of the study was enhanced by verifying the research instrument to ensure it collected data that represents the true views of the participants. Validity is either internal or external. Internal validity was ascertained by designing the questionnaires around the research questions. The design of the questionnaires was also aided with the support of assigned supervisor to ensure internal validity was enhanced. External validity was reinforced by informing participants of the anonymity of their participation in the survey to minimize response bias.

3.8 Ethical Considerations

Besides quality standards, a research study must adhere to the established ethical principles for scientific inquiry. Before embarking on data collection, ethical approval was obtained from the “Strathmore University Institutional Scientific and Ethical Review Committee” (SU-ISERC). Once secured, a license for scientific research was obtained from “the National Commission for Science, Technology, and Innovation” (NACOSTI) to maintain the study's credibility. The study also adhered to the principles of informed consent, privacy and confidentiality. Prospective respondents were provided consent forms before agreeing to participate in the study and were assured of their voluntary participation. They were free to withdraw from the study at any point if they felt so. They remained anonymous as the study did not collect personally identifiable data.

3.9 Chapter Summary

This section of the study describes the methodologies that were employed to fulfil the purpose of the study. As described in this chapter, the study followed a positivist research paradigm and adopted a descriptive cross-sectional research design. The target population of the study

constituted employees of the 42 registered commercial banks in Kenya, from whom a sample of 126 was recruited using a cluster sampling technique. Primary data was collected from the sample using structured questionnaires. Descriptive, correlational, and multiple regression statistics were employed for data analysis, and findings were presented using tables and figures. Quality and ethical standards were observed in completing the study.

CHAPTER FOUR

PRESENTATION OF FINDINGS

4.1 Introduction

This research aimed to determine the effect of emerging digital security solutions on fraud risk management in Kenya's banking sector. This chapter presents and interprets data collected by means of questionnaires and analyzes them using quantitative statistical techniques. Findings are presented using tables and figures.

4.2 Response Rate

A sample of 126 respondents was selected and furnished with the survey questionnaires to fill out. Out of the 126 questionnaires distributed, 97 were completed and returned on time for the analysis, translating to a 76.98% response rate. According to Fosnacht et al.'s (2017) standards for a sufficient response rate for academic research, with a 76.98%, this research met the threshold. The questionnaires were sorted, organized, and checked for errors and missing responses. All the questionnaires were eligible for analysis.

Table 4. 1: Response Rate

Category	Frequency	Percentage
Responded	97	76.98%
Non-response	29	23.02%
Total	**126**	**100.0%**

4.3 Background Information

The survey sought to gather background information on the target respondents. According to the findings, the majority of the respondents were male (66.0%), implying that most people working in the risk management, IT, and compliance departments were male; most were aged 31-40 years (37.1%); were undergraduates (62.9%), and had 5-10 years of experience in their organizations

(41.2%), suggesting that they had sufficient experience to participate in the survey. Also, most of them (55.7%) stated that their organizations performed fraud risk management reviews monthly.

Table 4. 2: Background Information of the Respondents (n=97)

Characteristics	Distribution	Frequency	Percentage
Gender	Male	64	66.0%
	Female	33	34.0%
Age (years)	<30	22	22.7%
	31-40	36	37.1%
	41-50	31	32.0%
	50>	8	8.2%
Level of education	Diploma	4	4.1%
	Undergraduate	61	62.9%
	Postgraduate	32	33.0%
Experience (years)	<5	35	36.1%
	5-10	40	41.2%
	10-15	14	14.4%
	15>	8	8.2%
Frequency of fraud risk management	Monthly	54	55.7%
	Quarterly	43	44.3%

4.4 Reliability Tests

The research performed the Cronbach's Alpha test to determine the reliability of the research study. It is a standard requirement that a reliable research study should attain a minimum Cronbach's Alpha coefficient value of 0.7. All the constructs have a relatively high internal

consistency, as shown in Table 4.3. Therefore, the reliability of this research is substantiated by the derived Cronbach's Alpha value.

Table 4. 3: Reliability Tests

Constructs	Cronbach's Alpha	N of Items
Fraud risk management	.749	5
Biometric technology	.841	5
Artificial intelligence	.812	5
Data analytics	.913	5

4.5 Descriptive Statistics

The study performed descriptive statistics – measures of central tendency, frequency, and distribution – to summarize, organize, and describe the main qualities of data. The findings are presented below:

4.5.1 Fraud Risk Management

The survey sought to gather data on fraud risk management practices among commercial banks in Kenya. Respondents were required to indicate the extent to which they agreed or disagreed with the statements about fraud risk management practices in their respective banks on a five-point Likert scale where 1=strongly disagree; 2=disagree; 3=neutral; 4=agree; 5=strongly agree. Table 4.4 shows the summary of the main characteristics of the responses.

Table 4. 4: Fraud Risk Management

	1 f (%)	2 f (%)	3 f (%)	4 f (%)	5 f (%)	Mean	SD
In my view, this bank uses ultramodern fraud risk detection mechanisms to	1 (1.0)	2 (2.1)	12 (12.4)	20 (20.6)	62 (63.9)	4.443	.8657

monitor transactions and root out fraudulent activities.							
I am of the opinion that this bank leverages innovative tools to assess fraud exposure and its associated risks.	0 (0.0)	7 (7.2)	8 (8.2)	16 (16.5)	66 (68.0)	4.454	.9244
I believe that this bank reviews and updates its internal fraud risk controls regularly to adapt to the changing threat landscape.	1 (1.0)	1 (1.0)	5 (5.2)	30 (30.9)	59 (60.8)	4.464	1.922
I can say that this bank employs a robust and streamlined anti-fraud technology that detects, flags, and reports anomalies in real time.	4 (4.1)	0 (0.0)	11 (11.3)	56 (57.7)	26 (26.8)	4.031	.8715
In addition to anti-fraud technology, I think this bank has a solid structure of rules, practices, and processes for effective fraud risk management.	0 (0.0)	4 (4.1)	4 (4.1)	44 (45.4)	45 (46.4)	4.340	.7484
Overall Mean						**4.346**	**1.066**

Findings presented above show a mean value of 4.346 at a 1.066 standard deviation, showing that data points were somewhat dispersed from the mean. This implies that respondents generally agreed that banks in Kenya practice fraud risk management. They were in agreement with the notions that commercial banks in Kenya use ultramodern fraud risk detection mechanisms (M=4.443, SD=.8657), leverage innovative tools to assess fraud exposure (M=4.454, SD=.9244), review and update their internal fraud risk controls regularly to adapt to the changing fraud risk landscape (M=4.464, SD=1.922), employ robust and streamlined anti-fraud technology (M=4.031, SD=.8715), and have solid structures of rules, practices, and procedures for effective risk management (M=4.340, SD=.7484).

4.5.2 Biometric Technology

The survey sought to gather data on the usage of biometric technologies to control fraud in banks. Respondents were required to indicate the extent to which they agreed or disagreed with the statements about the usage of biometric technologies in their respective banks on a five-point Likert scale where 1=strongly disagree; 2=disagree; 3=neutral; 4=agree; 5=strongly agree. Table 4.5 shows the summary of the main characteristics of the responses.

Table 4. 5: Biometric Technology

	1	2	3	4	5	Mean	SD
	f (%)	f (%)	f (%)	f (%)	f (%)		
I believe that this bank utilizes facial recognition systems to authenticate users and customers.	30 (30.9)	2 (2.1)	40 (41.2)	8 (8.2)	17 (17.5)	2.794	1.421
In my view, this bank incorporates fingerprint scanning tools to supplement or replace traditional authentication methods such as PINs.	14 (14.4)	4 (4.1)	22 (22.7)	52 (53.6)	5 (5.2)	3.309	1.131
I think that voice recognition is a critical part of this bank's biometric authentication technology for fraud management.	14 (14.4)	10 (10.3)	13 (13.4)	56 (57.7)	4 (4.1)	3.268	1.168
It is my opinion that this bank makes use of digital signatures to verify the identity of a customer and maintain the integrity of transactions.	18 (18.6)	22 (22.7)	44 (45.4)	4 (4.1)	9 (9.3)	2.693	1.121
I am of the view that this bank utilizes hand geometry recognition to enhance security and prevent fraud.	27 (27.8)	18 (18.6)	10 (10.3)	42 (43.3)	0 (0.0)	2.691	1.286

Overall Mean	**2.938**	**1.225**

The mean score for the biometric variable was 2.938 at a 1.225 standard deviation, implying that data points were dispersed from the mean value. This means that the respondents were in disagreement with the view regarding the usage of biometric technology in banks to control fraud. This is confirmed by the disagreements about using facial recognition for authentication (M=2.794, SD=1.421), use of digital signatures (M=2.693, SD=1.121), and usage of hand geometry (M=2.691, SD=1.286). However, they remained neutral on the use of fingerprint scanning tools to supplement traditional authentication methods (M=3.309, SD=1.131) and the use of voice recognition for authentication (M=3.268, SD=1.168).

4.5.3 Artificial Intelligence (AI)

The survey sought to gather data on the usage of AI to control fraud in banks. Respondents were required to indicate the extent to which they agreed or disagreed with the statements about the usage of AI in their respective banks on a five-point Likert scale where 1=strongly disagree; 2=disagree; 3=neutral; 4=agree; 5=strongly agree. Table 4.6 shows the summary of the main characteristics of the responses.

Table 4. 6: Artificial Intelligence

	1	**2**	**3**	**4**	**5**	**Mean**	**SD**
	f (%)	**f (%)**	**f (%)**	**f (%)**	**f (%)**		
I am of the view that the application of AI technology in this bank is important to the fight against financial fraud.	8 (8.2)	2 (2.1)	8 (8.2)	26 (26.8)	53 (54.6)	4.175	1.199
I think that the use of AI in this bank provides a more accurate assessment of fraud risks and accelerates the response to fraud.	8 (8.2)	2 (2.1)	20 (20.6)	56 (57.7)	11 (11.3)	3.619	1.005

In my opinion, the overall effectiveness of this bank's fraud management improves with the increased investment in AI.	0 (0.0)	14 (14.4)	4 (4.1)	65 (67.0)	14 (14.4)	3.814	.8579
I believe the AI-based fraud detection system, which relies on powerful algorithms, enables better fraud management in this bank.	0 (0.0)	10 (10.3)	7 (7.2)	58 (59.8)	22 (22.7)	3.948	.8462
It is my view that AI has helped automate processes for predicting, detecting, and preventing fraud in transactions.	2 (2.1)	4 (4.1)	16 (16.5)	59 (60.8)	16 (16.5)	3.856	.8164
Overall Mean						**3.882**	**.9448**

The overall mean for the AI variable was 3.882 at a .9448 standard deviation, which indicates that data points were close to the mean value. Therefore, respondents were, in general, neutral on the usage of AI for fraud control among banks in Kenya. This is proven by their neutrality on the usage of AI providing a more accurate assessment of fraud risk (M=3.619, SD=1.005), the effectiveness of fraud management improving with increased investment in AI (M=3.814, SD=.8579), AI-based fraud detection system enabling better fraud management (M=3.948, SD=.8462), and AI helping automate fraud management processes (M=3.856, SD=.8164). However, they agreed with the idea that the application of AI is important to the fight against financial fraud (M=4.175, SD=1.199).

4.5.4 Data Analytics

The survey sought to gather data on the usage of data analytics to control fraud in banks. Respondents were required to indicate the extent to which they agreed or disagreed with the statements about the usage of data analytics in their respective banks on a five-point Likert scale where 1=strongly disagree; 2=disagree; 3=neutral; 4=agree; 5=strongly agree. Table 4.7 shows the summary of the main characteristics of the responses.

Table 4. 7: Data Analytics

	1 f (%)	2 f (%)	3 f (%)	4 f (%)	5 f (%)	Mean	SD
From my observation, integrating data analytics into fraud management increases the effectiveness of fraud control.	4 (4.1)	0 (0.0)	4 (4.1)	52 (53.6)	37 (38.1)	4.216	.8687
I believe that the predictive capability of data analytics makes it possible to foresee fraudulent activities and take appropriate actions.	3 (3.1)	0 (0.0)	14 (14.4)	49 (50.5)	31 (32.0)	4.082	.8620
The idea that data analytics tools can help assess fraud risks and determine their effect is great for this bank and its mission to combat fraud.	3 (3.1)	0 (0.0)	13 (13.4)	51 (52.6)	30 (30.9)	4.082	.8499
I would say that without data analytics, it would be difficult to uncover and act on the hidden patterns of financial fraud on digital platforms.	2 (2.1)	0 (0.0)	31 (32.0)	40 (41.2)	24 (24.7)	3.866	.8615
I believe data analytics enables the anti-fraud team to integrate data into a single platform for a more efficient fraud management process.	0 (0.0)	4 (4.1)	30 (30.9)	40 (41.2)	23 (23.7)	3.845	.8334
Overall Mean						**4.019**	**.8551**

The overall mean score for the data analytics variable was 4.019 at a .8551 standard deviation, suggesting that data points were close to the mean. The finding implies that respondents were, in general, in agreement with the usage of data analytic solutions for fraud control in Kenyan banks. They agreed that integrating data analytics into fraud management increases the effectiveness of fraud control (M=4.216, SD=.8687), the predictive capability of data analytics makes it possible to foresee fraudulent activities and take appropriate actions (M=4.082, SD=.8620), and data analytics tools can help assess fraud risks and determine their effect which is great for banks to

combat fraud (M=4.082, SD=.8499). However, they remained neutral on the idea that the absence of data analytics would make it difficult to uncover and act on the hidden patterns of financial fraud on digital platforms (M=3.866, SD=.8615) and data analytics enabling the anti-fraud team to integrate data into a single platform for a more efficient fraud management process (M=3.845, SD=.8334).

4.6 Inferential Statistics

The analysis advanced to inferential statistics after understanding the main qualities of data as described above. The purpose of inferential statistics was to use the sample data to draw conclusions, and make estimations, generalizations, or inferences about the target population. A normality test was first performed to determine whether to proceed with parametric or nonparametric for the inferential statistics.

4.6.1 Normality Test

The study performed Shapiro-Wilk (S-W), an appropriate normality test for the sample size (i.e., <100), to check whether data followed a normal distribution. This is because parametric tests are applied when data is normally distributed; otherwise, nonparametric tests apply. All the constructs were not normally distributed (sig.<.05), as shown in Table 4.8. Instead, the constructs were skewed, as proven by the tailedness of the distribution (skewness and kurtosis). As such, the analysis proceeded with nonparametric tests.

Table 4. 8: One-Sample Shapiro-Wilk Test

	N	Mean	Std. Deviation	Skewness	Kurtosis	K-S	Asmp. Sig.
Fraud risk management	97	4.3912	.66264	-2.125	6.256	.774	.000
Biometric technology	97	2.9381	.96193	-.794	-.691	.840	.000
Artificial intelligence	97	3.8825	.72154	-1.551	1.572	.757	.000
Data analytics	97	4.0186	.73659	-1.164	3.680	.808	.000

4.6.2 Correlational Analysis

The research conducted Spearman's rank correlation to determine the direction and strength of correlation between the individual independent variables (biometric technology, AI, and data analytics) and the dependent variable (fraud risk management). In other words, the analysis sought to determine if the association is positive or negative and very strong, strong, moderate, weak, or no correlation at all.

4.6.2.1 Biometric Technology and Fraud Risk Management

The study performed Spearman's rank correlation to determine the association between biometric technology and fraud risk management in commercial banks in Kenya. Table 4.9 illustrates the direction and strength of the correlation and whether the correlation is significant.

Table 4. 9: Biometric Technology and Fraud Risk Management

			Fraud risk management	Biometric technology
Spearman's rho	Fraud risk management	Correlation Coefficient	1.000	.110
		Sig. (2-tailed)	.	.282
		N	97	97
	Biometric technology	Correlation Coefficient	.110	1.000
		Sig. (2-tailed)	.282	.
		N	97	97

A weak, nonsignificant correlation between risk management and biometric technology (r=.110, p>.05) was discovered. This means that an increase in the use of biometric technology by a unit would increase fraud risk control by 11.0% as a result. However, since the correlation is not significant, this research failed to reject the null hypothesis at a 95% level of confidence and a 5% level of significance.

4.6.2.2 Artificial Intelligence and Fraud Risk Management

The study performed Spearman's rank correlation to determine the association between AI and fraud risk management in commercial banks in Kenya. Table 4.10 illustrates the direction and strength of the correlation and whether the correlation is significant.

Table 4. 10: Artificial Intelligence and Fraud Risk Management

			Fraud risk management	Artificial intelligence
Spearman's rho	Fraud risk management	Correlation Coefficient	1.000	.456**
		Sig. (2-tailed)	.	.000
		N	97	97
	Artificial intelligence	Correlation Coefficient	.456**	1.000
		Sig. (2-tailed)	.000	.
		N	97	97

**. Correlation is significant at the 0.05 level (2-tailed).

The study found a moderate, significant positive correlation between AI and fraud risk management (r=.456, p<.05). This means that an increase in the investment and use of AI by a unit would improve fraud risk control by 45.6%. Since the correlation is significant, this research rejected the null hypothesis at a 95% confidence level and 5% level of significance.

4.6.2.3 Data Analytics and Fraud Risk Management

The study performed Spearman's rank correlation to determine the association between data analytics and fraud risk management in commercial banks in Kenya. Table 4.11 illustrates the direction and strength of the correlation and whether the correlation is significant.

Table 4. 11: Data Analytics and Fraud Risk Management

			Fraud risk management	Data analytics
Spearman's rho	Fraud risk management	Correlation Coefficient	1.000	.207**
		Sig. (2-tailed)	.	.003
		N	97	97
	Data analytics	Correlation Coefficient	.207**	1.000
		Sig. (2-tailed)	.003	.
		N	97	97

**. Correlation is significant at the 0.05 level (2-tailed).

A weak, significant positive correlation between data analytics and fraud risk management (r=.207, p<.05) was discovered. This means that increasing the investment and use of data analytics by 1% would increase fraud control by 20.7%. Therefore, since the association is significant, this research rejected the null hypothesis at a 95% confidence level and 5% level of significance.

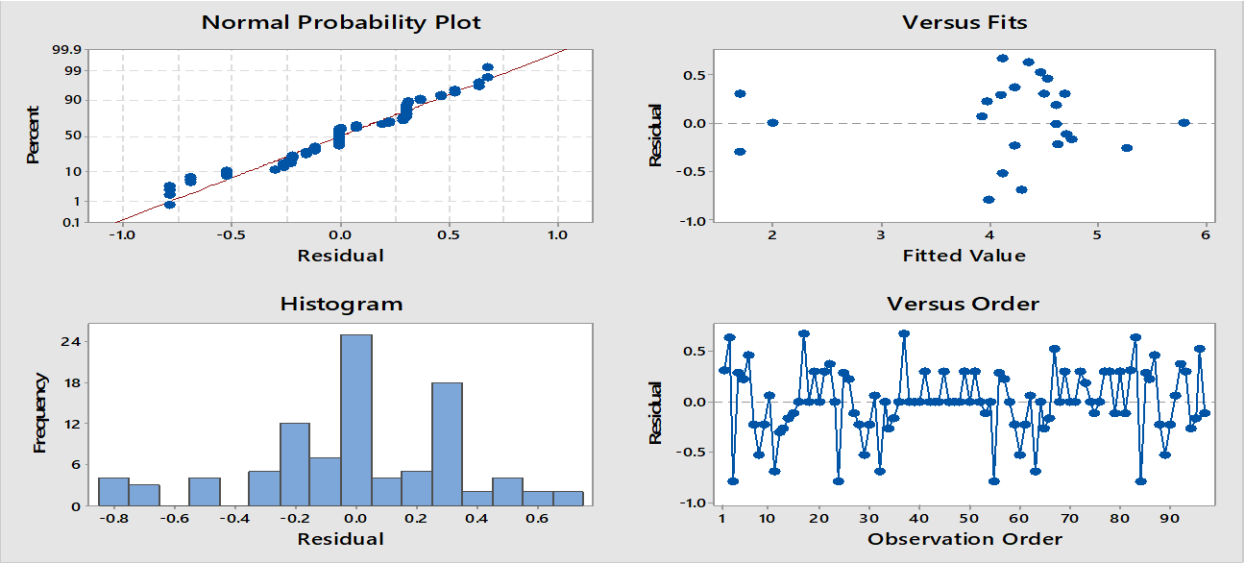
4.6.3 Diagnostic Tests

The study carried out some diagnostic tests to determine the appropriateness of the regression analysis. In other words, before proceeding to regression analysis, diagnostic tests were crucial to test whether the underlying assumptions of the regression model were satisfied (Bollen et al., 2016). This is because when any of these assumptions are violated, the validity of the regression estimates is violated (Bollen et al., 2016; Darlington & Hayes, 2016). The tests performed were test for heteroscedasticity, test for normality, test for autocorrelation, and test for multicollinearity, as shown below:

4.6.3.1 Test for Heteroscedasticity

The first assumption of the regression model is that the variance of the residuals or error terms is constant along the values of the dependent variable, a state known as homoscedasticity or homogeneity of variances. To check whether this assumption was held, scatter plots of the residuals were generated, and the results are shown in Figure 4.1.

Figure 4. 1: Residual Plots for Fraud Risk Management

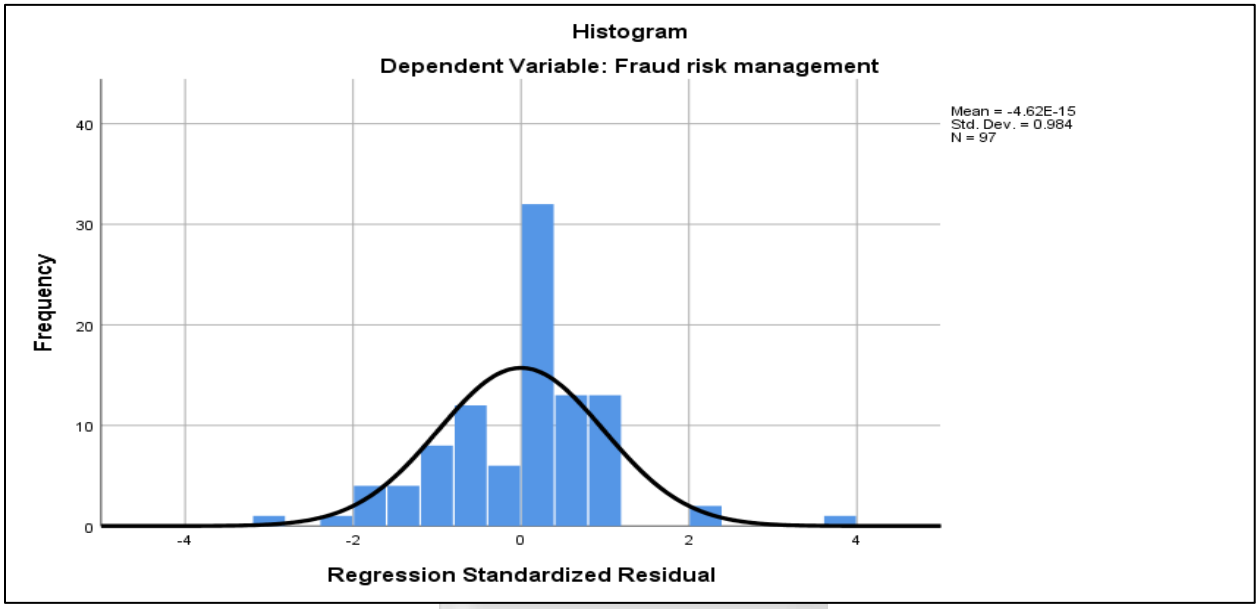


The probability-probability (p-p) plot in the top left shows a perfect straight line, confirming that the distribution is a perfect match. In other words, heteroscedasticity was not a concern. This is further confirmed by a flatter line in the top-right plot, evenly distributed residuals in the bottom-left plot, and variance being normally distributed in the histogram.

4.6.3.2 Test for Normality

The second assumption of regression analysis maintains that the residuals or errors follow a normal distribution. A P-P plot was generated to examine the normality of the residuals, as shown in Figure 4.1. The visual representation of the normality shows that the residuals are slightly skewed. Fortunately, they do not significantly deviate from normal distribution. Therefore, this distribution satisfies the normality assumption.

Figure 4. 2: Test for Normality



4.6.3.3 Test for Autocorrelation

Another assumption of the regression model is that error terms or disturbances are identical and independently distributed in a way that the correlation between the successive error components is zero. Durbin-Watson (D-W) statistics were performed to detect the autocorrelation. Usually, the test produces a value ranging from 0 to 4. A value ranging from 1.5 to 2.5 denotes the absence of autocorrelation; a value below 1.5 indicates positive autocorrelation, and a value above 2.5 indicates negative autocorrelation. In this case, this assumption was not violated since as shown in Table 4.12.

Table 4. 12: Durbin-Watson Test

D-stat	2.015
p-value	.000
Alpha	.05

From the table above, the DW statistic was 2.015, which confirms that the autocorrelation assumption was not violated. This is further confirmed by the level of significance being less than the alpha level ($p<.05$).

4.6.3.4 Test for Multicollinearity

The final assumption of the regression model is that the independent variables are not correlated. The variance inflation factor (VIF) test was performed to detect multicollinearity and its statistical significance. The rule of thumb is that the presence of multicollinearity is not statistically significant if the VIF value is less than 10. As illustrated in Table 4.13, the independent variables were not correlated. Therefore, this assumption was not violated.

Table 4. 13: Test for Multicollinearity

Model		Collinearity Statistics	
		Tolerance	**VIF**
1	(Constance)		
	Biometric technology	.433	2.309
	Artificial intelligence	.483	2.069
	Data analytics	.523	1.911

a. Dependent Variable: Fraud risk management

4.6.4 Regression Analysis

The analysis proceeded to regression analysis once it was ascertained that the assumptions underlying the regression model were satisfied. Regression analysis was necessitated by the need to determine the functional relationship between a single dependent variable (in this case, fraud risk management) and several independent variables (i.e., biometric technology, AI, and data analytics. The findings are presented below:

A model summary of the regression was generated to test the degree to which the variation of the independent variables affects the dependent variable. The model summary confirms that a portion

of the variance (R Square = .281) of fraud risk control is attributed to the three emerging digital security solutions. In other words, biometric technologies, AI, and data analytics collectively explain 28.1% of fraud risk control among commercial banks in Kenya.

Table 4. 14: Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.530[a]	.281	.258	.41284

a. Predictors: (Constant), Biometric technology, artificial intelligence, data analytics
b. Dependent Variable: Fraud risk management

The Analysis of Variance (ANOVA) was performed to determine the level of variability within the regression model and also the significance of the model. The results of the analysis are shown in Table 4.15. The results confirm that the relationship between the dependent variable and the dependent variables is proven by (F (3,96) = 12.103, P<0.05). Therefore, this research concludes that emerging digital security solutions are reliable predictors of fraud risk control among commercial banks in Kenya.

Table 4. 15: ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.836	3	3.945	12.103	.000[b]
	Residual	30.317	93	.326		
	Total	42.153	96			

a. Dependent Variable: fraud risk management
b. Predictors: (Constant), Biometric technology, Artificial intelligence, Data analytics

The standardized or beta coefficients (the β parameters) were generated to determine the strength and direction of each of the independent variables in the regression model. This was done to determine the quantitative effect of each of the independent variables on the dependent variable.

In other words, the extent to which the change in each independent variable must be multiplied to give a corresponding change in the dependent variable. The findings are shown in Table 4.16.

Table 4. 16: Coefficients[a]

Model		Unstandardized Coefficients			
		β	**Std. Error**	**t**	**Sig.**
1	(Constant)	1.964	.470	4.179	.000
	Biometric technology	.035	.092	.375	.709
	Artificial intelligence	.340	.116	2.926	.004
	Data analytics	.250	.109	2.289	.024

a. Dependent Variable: Fraud risk management

Biometric technology, AI, and data analytics all have positive effects on fraud risk control. However, the effect of biometric technology is nonsignificant (β = .035, t = .375, p>.05) whereas the effect of AI (β = .340, t = 2.926, p<.05) and data analytics (β = .250, t = 2.289, p<.05) are statistically significant. Therefore, the final equation for the regression equation is as follows:

$$Fraud\ risk\ management\ =\ 1.964\ +\ .340X_1 + .250X_2 + \varepsilon$$

Where;

X_1= AI

X_2= Data analytics

ε= error term

From the regression equation above, when the values of AI and data analytics are all equal to 0 (zero), fraud risk control is only 1.964. This means that in the absence of biometric technologies, AI solutions, and data analytic tools, commercial banks would only be able to control financial fraud risk up to 1.964.

4.7 Chapter Summary

The findings of the study have been presented using tables and figures in this chapter. It has been observed that respondents were in agreement regarding the adoption of fraud risk management practices and, the use of data analytics, remained neutral on the use of AI but disagreed on the use of biometrics for fraud control. Inferential statistics confirm that both AI and data analytics are significant predictors of the effectiveness of fraud control in the banking sector, whereas biometric technology is not a significant predictor.

CHAPTER FIVE

SUMMARY, DISCUSSION, CONCLUSION, AND RECOMMENDATIONS

5.1 Introduction

This section of the paper provides a summary of the study accompanied by an in-depth discussion of the findings. The chapter also offers the conclusion of the research study, presents its theoretical and practical implications, brings up the limitations encountered, and proposes areas for further research.

5.2 Summary of the Study

This research aimed to determine the effect of emerging digital security solutions on fraud risk management in Kenya's banking sector. Digital emerging solutions constituted the independent variable and were represented by biometric technology, AI, and data analytics, while fraud risk management was the dependent variable. The study was underpinned by the fraud triangle theory and fraud diamond theory and adopted a positivist research paradigm. The study targeted a cohort of 42 commercial banks in Kenya. A stratified sampling technique was used to select a sample of 126 IT, risk management, and compliance professionals from these institutions. Data was collected from the respondents using structured questionnaires.

A sum of 126 questionnaires were distributed, but 97 of them were filled out and returned on time for analysis. Therefore, this research attained a sufficient response rate of 76.98%. The analysis of the demographic data of the participants revealed that most of them were male, aged 31-40 years and 41-45 years, had a bachelor's degree, and had experience of 5-10 years in their respective banking institutions. Most of them also mentioned that their banks perform fraud risk management reviews quarterly. Descriptive statistics revealed that respondents were in agreement that banks in Kenya practice fraud risk management (M=4.346, SD=1.066) and the usage of data analytics for fraud control (M=4.019, SD=.8551), remained neutral on the usage of AI (M=3.882, SD=.9448), and disputed the use of biometric technology for fraud control (M=2.938, SD=1.225).

Findings from correlation analysis confirm that biometric technology has a weak, nonsignificant positive correlation with fraud management (r=.110, p>.05), AI has a strong, significant positive

correlation with fraud management (r=.456, p<.05), and data analytics has a weak, significant positive correlation with fraud risk management (r=.207, p<.05). Findings from regression analysis show that biometric technology, AI, and data analytics explain 28.1% of fraud risk management and that the three emerging digital security solutions are reliable predictors of fraud risk control in Kenya's banking sector (F (3,96) =12.103, P<0.05). Regression analysis also suggests that the effect of biometric technology on fraud risk management is positive but nonsignificant (β=.035, t=.375, p>.05), while the effect of AI (β=.340, t=2.926, p<.05) and data analytics (β=.250, t=2.289, p<.05) are statistically significant.

5.3 Discussion

This section of the paper describes, analyzes, and interprets the findings, accompanied by an explanation of their significance and how they relate to the research questions. The discussion is broken down into the specific objectives of the study.

5.3.1 Biometric Technology and Fraud Risk Management

The first specific objective of this research study was to determine the effect of biometric technology on fraud risk management in Kenya's banking sector. Descriptive statistics show that the use of biometric technology for fraud management in Kenya's banking sector is underwhelming. According to the respondents, the adoption and use of facial recognition, digital signatures, and hand geometry is below expectations. There is also plenty of room for improvement regarding the use of fingerprint scanning and voice recognition for fraud control. In support of this observation, Cirera et al. (2022) outline the following as possible reasons for the slow adoption of biometric technology: lack of demand, lack of capabilities, poor infrastructure, financial constraints, and government regulations.

Inferential statistics show that biometric technology has a positive, nonsignificant impact on fraud risk control. Therefore, this research failed to reject the null hypothesis. As far as biometric technology is concerned, this research is in support of the fraud triangle and fraud diamond theories. This is in the sense that the nonsignificant effect of biometric technology creates the necessary conditions for people to commit fraud – some kind of pressure, perceived opportunity, rationalization for fraud, and capability – as proposed by the fraud triangle and fraud diamond

theories. More specifically, the underwhelming ability of biometric technologies to effect fraud risk control creates opportunities for users and customers to engage in fraudulent activities.

The finding also corroborates findings from previous literature, including Tang and Karim's (2019) and Koreff et al.'s (2021) research that discovered issues with the use of biometric technology. According to Koreff et al. (2021), the integration of data analytics into government-related audits promotes the abuse of power by auditors, resulting in industry-wide unethical behaviours. Trawnih et al. (2023) provide evidence suggesting that the perceived risks of biometric technology could be the hindrance behind their perceived value. According to scholars, the vast majority of users believe the use of certain biometric systems, such as eye recognition, hand geometry, DNA matching, etc., is invasive and associated with physical risks.

5.3.2 Artificial Intelligence and Fraud Risk Management

The second objective of the study was to determine the effect of AI on fraud risk management in Kenya's banking sector. Descriptive statistics show that the investment in and application of AI is crucial in the fight against financial fraud in the banking sector. This observation is proven true by Theuri and Olukuru (2022), who point out that, led by KBA, commercial banks in Kenya have an aggressive agenda against fraud and money laundering that involves increased spending on new tech solutions such as AI. Descriptive statistics further reveal it is not well known whether AI solutions provide a more accurate assessment of and faster response to fraud, the effectiveness of fraud control improves with increased AI usage, and whether AI automating processes for detecting and responding to fraud.

Inferential statistics confirm that AI has a significant positive effect on fraud risk control in Kenya's banking sector. Put simply, the adoption and use of AI tools improve the fight against financial fraud in Kenya's banking industry. Therefore, this research rejected the null hypothesis. It also does not support the fraud triangle theory and fraud diamond theory. This is because the effectiveness of AI in curbing financial fraud eliminates the necessary conditions for fraud, such as pressure, perceived opportunity, rationalization for fraud, and capability, as suggested by the theoretical models. In particular, AI's ability to identify and respond to fraud risks automatically and in real time deters fraudsters from engaging in financial fraud.

The findings are also consistent with those of Abdulrahman (2019), Sood et al. (2023), Shah (2022), and Tiwari (2023), who found that AI significantly improved fraud detection and risk management. AI is a powerful, innovative solution that offers unmatched capabilities to banks and other financial institutions looking to protect their assets and customers (Sood et al., 2023; Tiwari, 2023). AI solutions can analyze a vast amounts of data in real-time, detect anomalous patterns, adapt to changing threats, identify unusual or out-of-the-ordinary transactions, etc., all of which are geared towards improving fraud detection and prevention strategies (Sood et al., 2023; Hassan et al., 2023; Soviany, 2018). In support of this research's findings, Muhammad and Abbas (2023) contend that AI and its recent breakthroughs make it the most powerful tool for fighting financial fraud.

5.3.3 Data Analytics and Fraud Risk Management

The final objective of the study was to examine the effect of data analytics on fraud risk management in Kenya's banking sector. The general sentiment among respondents is that data analytics use is widespread in the fight against financial fraud in the banking sector. For instance, commercial banks are known to integrate data analytics into fraud control systems, use data analytics tools to foresee unusual transactions, and use data analytic tools to assess fraud risks and determine their effect. However, it is still unsure whether data analytics makes it easier to uncover and respond to hidden patterns of fraud on digital platforms and its ability to integrate data into a single platform for efficient fraud control.

Findings from inferential statistics demonstrate that data analytics has a significant positive effect on fraud risk management. In other words, the use of data analytics improves financial fraud control in Kenyan banks. Therefore, this research rejected the null hypothesis. It also failed to support the fraud triangle and fraud diamond theories. Since the use of data analytics strengthens fraud risk management, it eliminates the necessary conditions for people to commit fraud. These conditions, as proposed by the fraud triangle and fraud diamond theories, include pressure, perceived opportunity, rationalization for fraud, and capability. More specifically, data analytics solutions get rid of the opportunity to engage in fraud and quash people's ability to commit fraud.

Findings also align with previous literature (Trierweiler, 2019; Handoko & Rosita, 2022; Novita & Anissa; Tang & Karim, 2019). The effectiveness of data analytics in the fight against fraud is

realized in its role in anti-fraud systems. According to Handoko and Rosita (2022) and Tang and Karim (2019), data analytics leverages vast amounts of data generated by day-to-day operations and explores patterns and trends of fraudulent behaviour to enable anti-fraud teams to strengthen their security measures. Handoko and Rosita (2022) add that when integrated with other advanced tools, such as AI and ML, data analytics can monitor transactions and identify anomalies, identify coordinated fraud rings, and automate fraud control processes.

5.4 Conclusion

This research aimed to examine the effect of emerging digital security solutions on fraud management in Kenya's banking sector. The need for this research was warranted by the observation that many banks and other financial institutions are undergoing digital transformation in response to the pressure of becoming more efficient and competitive. This means heavy reliance on IT systems to support business processes. Therefore, as banks continue to embrace digitization, the relevance and importance of emerging digital security solutions grows. This research sought to assess how these solutions effect fraud management. The results of the study show that biometric technology has a positive nonsignificant effect, while AI and data analytics have a significant positive effect on fraud risk management. Therefore, this research concludes that AI and data analytics significantly improve fraud risk management in Kenya's banking industry.

5.5 Recommendations

This study extends the financial fraud research by highlighting the effect of emerging digital security solutions on fraud management in the banking sector. As such, the theoretical implication of this research is that it suggests that emerging digital security solutions, in particular, AI and data analytics, help improve the fight against financial fraud in Kenya's banking sector. Based on this finding, it is recommended that investing in, adopting, and integrating digital security solutions into anti-fraud security measures helps curb fraud. This research confirms that these solutions, more specifically AI and data analytics, play a crucial role in improving the effectiveness of fraud risk control in Kenya's banking sector.

Based on the findings, this research also recommends that banking institutions should prioritize investing in both AI and data analytics solutions. This research demonstrates that AI and analytics have strong effect on fraud risk management. This implies that they are the most important digital security solution for fraud control in banking, an observation that has been supported by multiple other studies. Therefore, as banks advance to become more digitized, AI and data analytics can be a powerful ally in the fight against financial fraud, which is increasingly becoming more widespread.

At the policy level, this research recommends formulating government policies aimed at encouraging banks to embrace digital security solutions. Government regulations and the lack of capabilities have been identified as major barriers to the adoption of the use of innovative solutions. Some of these solutions, such as biometrics and AI, are highly regulated, which limits their adoption. The policy response should involve easing the regulatory framework to facilitate the adoption of these solutions. Also, many banking institutions find it a challenge to adopt emerging innovations because of inadequate expertise. It is time for the government to transform the education sector by introducing programs geared towards creating a skilled workforce for these technologies.

5.6 Limitations of the Study

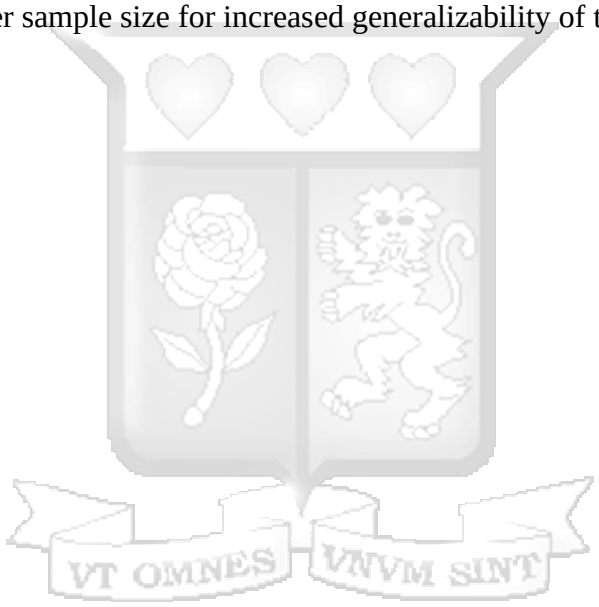
The study focused on employees at managerial levels within critical banking departments, including compliance, risk management, and IT. Due to their demanding roles and busy schedules, engaging them in the study was a challenge. Achieving a sufficient response rate involved a repetitive and meticulous process of scheduling, rescheduling, and canceling meetings.

5.7 Areas for Further Research

Findings from this research suggest that biometric technology, AI, and data analytics explain 28.1% of fraud risk management, implying that the rest of the percentage is attributed to digital security solutions not covered in this research. Digital security is a broad field, encompassing different types of solutions—for example, blockchain technology, centralized identity and access management (IAM), zero trust architecture, digital forensic systems, ML, multifactor

authentication (MFA), e-crime intelligence tools, etc. Future researchers should focus on these technologies and determine how they influence fraud risk management in banking institutions in Kenya.

In addition, the focus of this research was to report the effect of digital security solutions on fraud management. It has achieved this goal by demonstrating that AI and data analytics significantly improve the effectiveness of anti-fraud systems. However, it fails to describe the innerworkings of these technologies on fraud risk management. Therefore, future researchers should aim to analyze the exact ways these solutions work to achieve better anti-fraud campaigns. In other words, provide explanations for the significant effect of AI and data analytics. Lastly, future research studies should incorporate a larger sample size for increased generalizability of the findings.



REFERENCES

Abbott, M. L., & McKinney, J. (2013). *Understanding and applying research design*. John Wiley & Sons.

Abdulrahman, M. A. (2019). The impact of Artificial Intelligence (AI) in detecting fraud in the UAE. *Education in Medicine Journal*, *10*, 1-19.

Abuga, K., Wamugo, L., & Makori, D. (2023). Liquidity Capacity and Financial Performance of Commercial Banks in Kenya. *International Journal of Finance and Accounting*, *8*(1), 76-96.

Acharya, A. S., Prakash, A., Saxena, P., & Nigam, A. (2013). Sampling: Why and how of it. *Indian Journal of Medical Specialties*, *4*(2), 330-333.

Adebayo, A. O., Olagunju, A., & Bankole, O. E. (2022). Fraud risk management and fraud reduction: Evidence from the Nigerian oil and gas sector. *Malaysian Management Journal*, *26*, 145-168.

Agusto & Co. (2023). The Kenya Banking Industry Report 2023. Available at https://www.agustoresearch.com/report/2023-kenya-banking-industry-report/

Aksnes, D. W., Langfeldt, L., & Wouters, P. (2019). Citations, citation indicators, and research quality: An overview of basic concepts and theories. *Sage Open*, *9*(1), 2158244019829575.

Anyanzwa, J. (2021). Kenya's financial services firms are prime targets for fraudsters. The East African. https://www.theeastafrican.co.ke/tea/business/kenya-identity-fraud-financial-services-industry-3441762

Arim, A., & Wamema, J. (2022). Towards an Improved Framework for E-Risk Management for Digital Financial Services (DFS) in Ugandan Banks: A Case of Bank of Africa (Uganda) Limited. *Journal of Information and Organizational Sciences*, *46*(1), 103-127.

Aschi, M., Bonura, S., Masi, N., Messina, D., & Profeta, D. (2022). Cybersecurity and fraud detection in financial transactions. In *Big Data and Artificial Intelligence in Digital Finance: Increasing Personalization and Trust in Digital Finance using Big Data and AI* (pp. 269-278). Cham: Springer International Publishing.

Bakunova, T. V., Trofimova, E. A., & Lapteva, E. V. (2019, December). Biometrics as a method of information security in the banking sector digitalization. In *International Scientific and Practical Conference on Digital Economy (ISCDE 2019)* (pp. 929-934). Atlantis Press.

Banga, L., & Pillai, S. (2021, July). Impact of behavioural biometrics on the mobile banking system. In *Journal of Physics: Conference Series* (Vol. 1964, No. 6, p. 062109). IOP Publishing.

Bao, Y., Hilary, G., & Ke, B. (2022). Artificial intelligence and fraud detection. *Innovative Technology at the Interface of Finance and Operations: Volume I*, 223-247.

Bhasin, M. L. (2016). The role of technology in combatting bank frauds: perspectives and prospects. *Ecoforum Journal*, *5*(2).

Bhasin, N. K., & Rajesh, A. (2022). The role of emerging banking technologies for risk management and mitigation to reduce non-performing assets and bank fraud in the Indian Banking System. *International Journal of e-Collaboration (IJeC)*, *18*(1), 1-25.

Bollen, K. A., Biemer, P. P., Karr, A. F., Tueller, S., & Berzofsky, M. E. (2016). Are survey weights needed? A review of diagnostic tests in regression analysis. *Annual Review of Statistics and Its Application*, *3*, 375-392.

Camillo, M. (2017). Cybersecurity: Risks and management of risks for global banks and financial institutions. *Journal of Risk Management in Financial Institutions*, *10*(2), 196-200.

Chen, J., Tao, Y., Wang, H., & Chen, T. (2015). Big data-based fraud risk management at Alibaba. *The Journal of Finance and Data Science*, *1*(1), 1-10.

Chitavi, M., Cohen, L., & Hagist, S. C. (2021). Kenya Is Becoming a Global Hub of FinTech Innovation. *Harvard Business Review*, *21*.

Choi, D., & Lee, K. (2018). An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation. *Security and Communication Networks*, *2018*.

Chukwuma, O., Okolie, P., & Eneh, A. (2022). Impact of cyber security and forensic accounting techniques on fraud detection in Nigeria. *International Journal of Multidisciplinary Research and Growth Evaluation. 3*, 585-595.

Cirera, X., Comin, D., Cruz, M., Lee, K. M., Martinez, P., & Martins-Neto, A. (2022). Firm-level Adoption of Technologies in Kenya.

Darlington, R. B., & Hayes, A. F. (2016). *Regression analysis and linear models: Concepts, applications, and implementation*. Guilford Publications.

Dzomira, S. (2014). Digital Forensic Technologies as E-Fraud Risk mitigation Tools in the Banking industry: Evidence from Zimbabwe. *Risk governance and control: financial markets and institutions*.

Edmonds, A., & Gudmestad, A. (2018). Operationalizing variables. *Critical reflections on data in second language acquisition*, *51*(2).

Edson, M. C., Henning, P. B., & Sankaran, S. (Eds.). (2016). *A guide to systems research: Philosophy, processes and practice* (Vol. 10). Springer.

Enofe, A. O., Abilogun, T. O., Omoolorun, A. J., & Elaiho, E. M. (2017). Bank fraud and preventive measures in Nigeria: An empirical review. *International Journal of Academic Research in Business and Social Sciences*, *7*(7), 40-51.

Fatoki, J. O. (2023). The influence of cyber security on financial fraud in the Nigerian banking industry.

Federal Trade Commission. (2022). New data shows FTC received 2.8 million fraud reports from consumers in 2021.

Filotto, U., Caratelli, M., & Fornezza, F. (2021). Shaping the digital transformation of the retail banking industry. Empirical evidence from Italy. *European Management Journal*, *39*(3), 366-375.

Gbegi, D. O., & Adebisi, J. F. (2013). The New Fraud Diamond Model- How can it help forensic accountants in fraud investigation in Nigeria? *European Journal of Accounting Auditing and Fiancé Research*, *1*(4), 129-138.

George, D., & Mallery, P. (2018). Descriptive statistics. In *IBM SPSS Statistics 25 Step by Step* (pp. 126-134). Routledge.

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints*.

Gisairo, B. (2016). *Effectiveness of use of biometric technology to curb fraud in medical insurance in Kenya* (Doctoral dissertation, Doctoral dissertation).

Goode, A. (2018). Biometrics for banking: best practices and barriers to adoption. *Biometric Technology Today*, *2018*(10), 5-7.

Granić, A. (2023). Technology acceptance and adoption in education. In *Handbook of open, distance and digital education* (pp. 183-197). Singapore: Springer Nature Singapore.

Gupta, R., & Varma, S. (2019). A structural equation model to assess behavioural intention to use biometric-enabled e-banking services in India. *International Journal of Business Information Systems*, *31*(4), 555-572.

Halbouni, S. S., Obeid, N., & Garbou, A. (2016). Corporate governance and information technology in fraud prevention and detection: Evidence from the UAE. *Managerial Auditing Journal*, *31*(6/7), 589-628.

Handoko, B. L., & Rosita, A. (2022, April). The Effect of Skepticism, Big Data Analytics to Financial Fraud Detection Moderated by Forensic Accounting. In *Proceedings of the 6th International Conference on E-Commerce, E-Business and E-Government* (pp. 123-130).

Harun, M. A. (2023). Customers' choice of the bank during the Covid-19 pandemic: the moderating effect of different banks in Bangladesh. *South Asian Journal of Marketing*, *4*(1), 33-50.

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. *McKinsey & Company*, *2019*.

Hassan, M., Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk

management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, *6*(1), 110-132.

Hill, C. (2018). Biometrics becoming a must-have for fraud prevention. *Biometric Technology Today*, *2018*(1), 9-11.

Hussaini, I., Aliyu, Y., & Bashir, A. B. (2021). Effect of Information and Communication on Fraud Prevention and Detection in Deposit Money Banks in Nigeria. *UMYU Journal of Accounting and Finance Research*, *1*(2), 21-30.

Ishak, N. M., & Abu Bakar, A. Y. (2014). Developing Sampling Frame for Case Study: Challenges and Conditions. *World journal of education*, *4*(3), 29-35.

Josyula, H. P., Vishnubhotla, D., & Onyando, P. O. (2023). Is artificial intelligence an efficient technology for financial fraud risk management? *International Journal of Managerial Studies and Research (IJMSR)*, *11*(6), 11-16.

Kambatla, K., Kollias, G., Kumar, V., & Grama, A. (2014). Trends in big data analytics. Journal of parallel and distributed computing, 74(7), 2561-2573.

Kangogo, S. (2020). *Influence of fraud prevention and detection techniques on fraud and moderating effect of firm revenue in Kenyan State Corporations* (Doctoral dissertation, Strathmore University).

Kenya Bankers Association. (2021). Survey: mobile apps top bank customers' digital banking feature preferences. https://www.kba.co.ke/survey-mobile-apps-top-bank-customers-digital-banking-feature-preferences/

Khailtash, D., & Lindqvist, P. (2022). The Impact of AI on Banks' Risk Management Approach: A qualitative study on the effects of AI in the banking sector from a holistic perspective.

Kiragu, D. N. U. (2013). Technology adoption and occupational fraud risk: Empirical evidence from commercial banks in Kenya.

Kivunja, C. (2018). Distinguishing between theory, theoretical framework, and conceptual framework: A systematic review of lessons from the field. *International journal of higher education*, *7*(6), 44-53.

KMPG, (2022). Rampant fraud shows no sign of slowing, putting sustained pressure on UK courts.

Koreff, J., Weisner, M., & Sutton, S. G. (2021). Data analytics (AB) use in healthcare fraud audits. *International Journal of Accounting Information Systems*, *42*, 100523.

Kumar, M. (2023). Technology Acceptance Model: A Review. *Journal of Advanced Research in Information Technology, Systems and Management*, *7*(1), 4-7.

Langat, D.K., Bonuke, R., & Kibet, Y.K. (2021). Mobile Banking Service Quality, Customer Perceived Value and Customer Retention in the Kenyan Banking Industry.Getugi, J. C., Osoro, C., & Kihara, A. (2023). Mobile Banking and Technical Efficiency of Commercial Banks in Kenya. *Journal of Accounting*, *6*(1), 1-20.

Li, K., Kim, D. J., Lang, K. R., Kauffman, R. J., & Naldi, M. (2020). How should we understand the digital economy in Asia? Critical assessment and research agenda. *Electronic commerce research and applications*, *44*, 101004.

Lokadio, S. (2018). Strategic approaches adopted to combat fraud at Kenya Commercial Banks. (Doctoral dissertation, University of Nairobi).

Lokanan, M. E. (2015, September). Challenges to the fraud triangle: Questions on its usefulness. In *Accounting Forum* (Vol. 39, No. 3, pp. 201-224). No longer published by Elsevier.

Maharjan, R., & Chatterjee, J. M. (2019). Framework for Minimizing Cyber Security Issues in the Banking Sector of Nepal. *LBEF Research Journal of Science, Technology and Management*, *1*(1), 82-98.

Maina, B. W. (2016). *The Effects of Financial Fraud and Liquidity on Financial Performance of Insurance Companies in Kenya* (Doctoral dissertation, University of Nairobi).

Malik, A. A. (2018). Bank Frauds Using Digital Devices and the Role of Business Ethics. *International Journal for Electronic Crime Investigation*, *2*(4), 7-7.

Mangala, D., & Soni, L. (2023). A systematic literature review on frauds in the banking sector. *Journal of Financial Crime*, *30*(1), 285-301.

Manoj, K. S. (2021). Banks" Holistic Approach to Cyber Security: Tools to Mitigate Cyber Risk. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, *12*(1), 902-910.

Mansor, N., & Abdullahi, R. (2015). Fraud triangle theory and fraud diamond theory. Understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Science*, *1*(4), 38-45.

Marangunić, N., & Granić, A. (2015). Technology acceptance model: a literature review from 1986 to 2013. *Universal access in the information society*, *14*, 81-95.

Mazhar, S. A., Anjum, R., Anwar, A. I., & Khan, A. A. (2021). Methods of data collection: A fundamental tool of research. *Journal of Integrated Community Health (ISSN 2319-9113)*, *10*(1), 6-10.

Mertens, W. (2017). *Quantitative data analysis*. Springer.

Mir, S. S., Shoaib, U., & Sarfraz, M. S. (2016). Analysis of digital forensic investigation models. *Int. J. Comput. Sci. Inform. Secur*, *14*(11).

Mishra, D., Akman, I., & Mishra, A. (2014). Theory of reasoned action application for green information technology acceptance. *Computers in human behavior*, *36*, 29-40.

Mongwe, W. T., & Malan, K. M. (2020). A survey of automated financial statement fraud detection with relevance to the South African context. *South African Computer Journal*, *32*(1), 74-112.

Moreira, J., Carvalho, A., & Horvath, T. (2018). A general introduction to data analytics. John Wiley & Sons.

Muhammad, F. & Abbas, M. (2023). Artificial intelligence for fraud detection and prevention. https://www.researchgate.net/publication/375671860_Artificial_Intelligence_for_fraud_detection_and_prevention

Muriithi, R. G. (2022). Distressed Debt Management & Lessons Learnt Through Case Management: Banking Industry in Kenya. *European Journal of Business and Management Research*, *7*(1), 134-146.

Mwangi, S.W., & Ndegwa, J.N. (2020). The Influence of Fraud Risk Management on Fraud Occurrence in Kenyan Listed Companies. International Journal of Finance & Banking Studies, 9, 147-160.

Mwithi, J. M., & Kamau, J. N. (2015). Strategies adopted by commercial banks in Kenya to combat fraud: A survey of selected commercial banks in Kenya. *International Journal of Current Business and Social Sciences, 1*(3), 1-18.

Ngava, A. M. (2015). *A study on the influence of Information Communication Technology (ICT) adoption on bank fraud in Kenya* (Doctoral dissertation, Strathmore University).

Novita, N., & Anissa, A. I. N. A. (2022). The role of data analytics for detecting indications of fraud in the public sector. *International Journal of Research in Business and Social Science (2147-4478), 11*(7), 218-225.

Nurjannah, S. (2023). Digital Transformation In The Banking Industry Challenges And Opportunities. *International Journal of Accounting, Management and Economics*, *1*(01).

Okoye, E., & Ndah, E. N. (2019). Forensic accounting and fraud prevention in manufacturing companies in Nigeria. *International Journal of Innovative Finance and Economics Research*, *7*(1), 107-116.

Olongo, F. O. (2013). *The effects of financial fraud and liquidity on the financial performance of commercial banks in Kenya* (Doctoral dissertation, University of Nairobi).

Park, Y. S., Konge, L., & Artino Jr, A. R. (2020). The positivism paradigm of research. *Academic medicine*, *95*(5), 690-694.

Psychoula, I., Gutmann, A., Mainali, P., Lee, S. H., Dunphy, P., & Petitcolas, F. (2021). Explainable machine learning for fraud detection. *Computer*, *54*(10), 49-59.

Puspasari, N. (2015). Fraud theory evolution and its relevance to fraud prevention in the village government in Indonesia. *Asia Pacific Fraud Journal*, *1*(2), 177-188.

PwC. (2021). Fraud and Economic Crime – opportunity in the face of adversity: *PwC Kenya Economic Crime and Fraud Survey*.

Rad, A. (2021). Technology is a double-edged sword for financial fraud risk management. The Asian Banker.

Rahman, M. J., & Jie, X. (2024). Fraud detection using fraud triangle theory: evidence from China. *Journal of Financial Crime*, *31*(1), 101-118.

Raman, R., Tiwari, M., Buddhi, D., Trivedi, S., Bothe, S., & Ponnusamy, R. (2023, May). Cyber Security Fraud Detection Using Machine Learning Approach. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 1037-1042). IEEE.

Revathi, P. (2019). Digital banking challenges and opportunities in India. *EPRA International Journal of Economic and Business Review*, *7*(12), 20-23.

Roberts, P., & Priest, H. (2006). Reliability and validity in research. *Nursing Standard*, *20*(44), 41-46.

Rohali, Y., Basri, Y. Z., Ismail, R., & Septian, R. A. D. (2022). Factors affecting the decision-making of Indonesian sharia banking companies. *ADI Journal on Recent Innovation*, *4*(1), 13-25.

Roopa, S., & Rani, M. S. (2012). Questionnaire designing for a survey. *Journal of Indian Orthodontic Society*, *46*(4_suppl1), 273-277.

Rosliana, R., Elliany, E., & Handayani, W. (2022). Implementation of Fraud Risk Management to Minimize Fraud Risk in Wanda Putra Kencana Surabaya. *International Journal of Social Science, Education, Communication and Economics (SINOMICS JOURNAL)*, *1*(5), 667-680.

Runkler, T. A. (2020). Data analytics. Wiesbaden: Springer Fachmedien Wiesbaden.

Shah, V. (2022). How efficient is Machine Learning in detecting financial fraud using mobile transaction metadata? *Journal of Student Research*, *11*(3).

Sheard, J. (2018). Quantitative data analysis. In *Research Methods: Information, Systems, and Contexts, Second Edition* (pp. 429-452). Elsevier.

Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking information resource cybersecurity system modelling. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(2), 80.

Singh, A., Srivastava, R., & Singh, Y. N. (2019). Prevention of payment card fraud using biometrics. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*, 516-525.

Singh, D., & Reddy, C. K. (2015). A survey on platforms for big data analytics. Journal of big data, 2(1), 1-20.

Sinha, A.K. (2021). Fraud Risk Management in Banks.

Soni, V. D. (2019). Role of artificial intelligence in combating cyber threats in banking. *International Engineering Journal For Research & Development*, *4*(1), 7-7.

Sood, P., Sharma, C., Nijjer, S., & Sakhuja, S. (2023). Review the role of artificial intelligence in detecting and preventing financial fraud using natural language processing. *International Journal of System Assurance Engineering and Management*, 1-16.

Soviany, C. (2018). The benefits of using artificial intelligence in payment fraud detection: A case study. *Journal of Payments Strategy & Systems*, *12*(2), 102-110.

Sujeewa, G. M. M., Yajid, M. S. A., Azam, S. M. F., & Dharmaratne, I. (2018). The new fraud triangle theory-integrating ethical values of employees. *International Journal of Business, Economics and Law*, *16*(5), 52-57.

Talabi, A.A., Longe, O.B., Muhammad, A.A., & Olusanya, K. (2021). Cybersecurity Risk Management in Identity Systems using Biometric-based Multimodal Authentication. *Proceedings of the 28th iSTEAMS Multidisciplinary & Inter-tertiary Research Conference.*

Tang, J., & Karim, K. E. (2019). Financial fraud detection and big data analytics–implications on auditors' use of fraud brainstorming session. *Managerial Auditing Journal*, *34*(3), 324-337.

Tang, W., & Yang, S. (2022). Digital transformation and firm performance in the context of sustainability: Mediating effects based on behavioural integration. *Journal of Environmental and Public Health*, *2022*.

Theuri, J., & Olukuru, J. (2022). *The impact of Artificial Intelligence and how it is shaping banking* (No. 61). KBA Centre for Research on Financial Markets and Policy Working Paper Series.

Tiwari, R. (2023). The Application of AI And Machine Learning in the Financial Industry and its Effects on Risk Management and Fraud Detection. *International Journal of Scientific Research in Engineering and Management (IJSREM), 7*(1)

Trawnih, A. A., Al-Adwan, A. S., Yaseen, H., & Al-Rahmi, W. M. (2023). Determining perceptions of banking customers regarding fingerprint ATMs. *Information Development*. https://doi.org/10.1177/02666669231194360

Trierweiler, M. (2019). Evaluation the use of big data analytics to facilitate compliance and fraud prevention: an empirical study about usefulness and usage of big data analytics to prevent occupational fraud in German-speaking companies/submitted by Michaela Trierweiler (Doctoral dissertation, Universität Linz).

Tropina, T. (2016). Do digital technologies facilitate illicit financial flows?

Varpio, L., Paradis, E., Uijtdehaage, S., & Young, M. (2020). The distinctions between theory, theoretical framework, and conceptual framework. *Academic Medicine, 95*(7), 989-994.

Victory, C. O., Promise, E., & Mike, C. N. (2022). Impact of Cyber-Security on Fraud Prevention in Nigerian Commercial Banks. *Jurnal Akuntansi, Keuangan, dan Manajemen*, *4*(1), 15-27.

Winasis, S., Riyanto, S., & Ariyanto, E. (2020). Digital transformation in the Indonesian banking industry: Impact on employee engagement. *International Journal of Innovation, Creativity and Change*, *12*(4), 528-543.

Xin, Q., Zhou, J., & Hu, F. (2018). The economic consequences of financial fraud: evidence from the product market in China. *China Journal of Accounting Studies*, *6*(1), 1-23.

Yanagawa, E. (2018). Digital transformation in Japan's banking industry. *Journal of Payments Strategy & Systems*, *12*(4), 351-364.

Zabala Aguayo, F., & Ślusarczyk, B. (2020). Risks of banking services" digitalization: The practice of diversification and sustainable development goals. *Sustainability*, *12*(10), 4040.

Zhu, Y., & Jin, S. (2023). COVID-19, Digital Transformation of Banks, and Operational Capabilities of Commercial Banks. *Sustainability*, *15*(11), 8783.

APPENDICES

Appendix 1: Letter of Invitation to Participants

Judy Njeri Matheri

MBA Student

Strathmore University Business School

To whom it may concern,

RE: REQUEST FOR PARTICIPATION IN AN ACADEMIC RESEARCH

I am pursuing a Master's Degree in Business Administration at the Strathmore University Business School. I am conducting a study on the effect of emerging digital security solutions on fraud risk management in Kenya's banking sector.

You have been selected as one of the potential respondents to this study. Therefore, I request your kind participation by completing the attached questionnaire. The information you will provide will be treated with strict confidence and will only be used for this research and academic purposes. Your anonymity is also assured.

Thank you in advance.

Best regards,

Judy Njeri Matheri

Appendix 2: Participants Information Sheet and Consent Form

TITLE OF THE PROPOSED STUDY

The effect of emerging digital security solutions on fraud risk management in the banking sector in Kenya.

SECTION 1: INFORMATION SHEET

Principal Investigator: Judy Njeri Matheri

Institutional Affiliation: Strathmore Business School (SBS)

Mobile: +254 722968607

Email: judymatheri@yahoo.com

Supervisor: Benjamin Mutuku Kyalo

Email: bkyalo@strathmore.edu

Institutional Affiliation: Strathmore Business School (SBS)

SECTION 2: INFORMATION SHEET – THE STUDY

2.1. Why is this study being carried out?

This study is being carried out in fulfilment of the requirement for the award of a Master in Business Administration at Strathmore Business School.

It aims to determine the effect of emerging digital security solutions on fraud risk management in the banking sector in Kenya.

2.2. Do I have to take part?

No. Taking part in this study is entirely optional, and the decision rests only with you. If you decide to take part, you will be asked to complete a questionnaire to get information on the influence of job satisfaction factors among nurses on patient safety in Nairobi County. The questionnaire will be well-structured and simple to understand and complete. Further explanation will be provided where necessary.

Please note you are free to decline to take part in the study from this study at any time without giving any reasons.

2.3. Who is eligible to take part in this study?

Practitioners in Kenya's 42 registered commercial banks. In particular, information technology (IT), compliance and risk management professionals of these banks are eligible to participate in the study.

2.4. Who is not eligible to take part in this study?

- Practitioners not in the IT, compliance, and risk management departments of the 42 registered commercial banks in Kenya.
- Practitioners who have not consented to the study
- Incapacitated persons.
- Any person who is under 18 years of age (Minors).

2.5. What will taking part in this study involve for me?

You will be approached and requested to take part in the study. If you are satisfied that you fully understand the goals behind this study, you will be asked to sign the informed consent form (this form), which will then be taken through a questionnaire to complete.

2.6. Are there any risks or dangers in taking part in this study?

There are no risks in taking part in this study. All the information you provide will be treated as confidential and will not be used in any way without your express permission.

2.7. Are there any benefits of taking part in this study?

The information will be used to improve the knowledge of fraud risk management in the banking sector. The completion of the study will be instrumental in confronting financial fraud.

2.8. What will happen to me if I refuse to take part in this study?

Participation in this study is entirely voluntary. Even if you decide to take part at first but later change your mind, you are free to withdraw at any time without explanation.

2.9. Who will have access to my information during this research?

Access to all the information obtained during this research will be restricted. All research records will be stored in securely locked cabinets. That information may be transcribed into our database, but this will be sufficiently encrypted and password-protected. Only the people who are closely concerned with this study will have access to your information. All your information will be treated as private and confidential.

2.10. Who can I contact in case I have further questions?

You can contact me, the Principal Investigator, Judy Njeri Matheri, at Strathmore Business School by email at judymatheri@yahoo.com or by calling **+2547 22968607,** and a summary report of the findings will be shared via email.

You can also contact my supervisor, **Benjamin Mutuku Kyalo**, at the Strathmore Business School, Nairobi, or by e-mail (bkyalo@strathmore.edu).

If you want to ask someone independent anything about this research, please contact:

The Secretary

Strathmore University Institutional Ethics Review Board,

P. O. BOX 59857, 00200,

Nairobi.

Email: ethicsreview@strathmore.edu

I, _____, confirm that all the issues confirm that all the issues about this study have been clarified. I further affirm that I have asked all the questions that I needed to ask, and all of them have been answered to my satisfaction. I have read and understood the questions. I have been provided with the contacts of the person and institution that I need to contact in case issues arise and I need further clarification.

Please tick the boxes that apply to you;

Participation in the research study

☐ I AGREE to take part in this research

☐ I DON'T AGREE to take part in this research

Storage of information on the completed questionnaire

☐ I AGREE to have my completed questionnaire stored for future data analysis

☐ I DON'T AGREE to have my completed questionnaire stored for future data analysis

Participant's signature: _____ Date: ____/ _____/ _____ (DD/MM/YY)

Participant's name: _____ Time: ____: _____ (HH/Mins)

(please print name)

I, JUDY NJERI MATHERI, certify that I have followed the SOP for this study, have explained the study information to the study participant named above, and that s/he has understood the nature and the purpose of the study and consented to the participation in the study. S/he has been given the opportunity to ask questions which have been answered satisfactorily.

Investigator's signature: Date: __12__/ __03___/ __2024___

Investigator's name: __Judy Njeri Matheri__ Time: ____: _____ (HH/Mins)

Appendix 3: Commercial Banks in Kenya

1. African Banking Corporation Limited
2. Bank of Africa Kenya Limited
3. Bank of Baroda (K) Limited
4. Bank of India
5. Barclays Bank of Kenya Limited
6. Stanbic Bank Kenya Limited
7. Charterhouse Bank Limited
8. Chase Bank (K) Limited
9. Citibank N.A. Kenya
10. Commercial Bank of Africa Limited
11. Consolidated Bank of Kenya Limited
12. Co-operative Bank of Kenya Limited
13. Credit Bank Limited
14. Development Bank of Kenya Limited
15. Diamond Trust Bank Kenya Limited
16. Ecobank Kenya Limited
17. Spire Bank Ltd
18. Equity Bank Kenya Limited
19. Family Bank Limited
20. Fidelity Bank Limited
21. First Community Bank Limited
22. Guaranty Trust Bank (K) Ltd
23. Giro Commercial Bank Limited
24. Guardian Bank Limited
25. Gulf African Bank Limited

26 Habib Bank A.G Zurich

27 Habib Bank Limited

28 Imperial Bank Limited

29 I&M Bank Limited

30 Jamii Bora Bank Limited

31 KCB Bank Kenya Limited

32 Middle East Bank (K) Limited

33 National Bank of Kenya Limited

34 NIC Bank Limited

35 M-Oriental Bank Limited

36 Paramount Bank Limited

37 Prime Bank Limited

38 Sidian Bank Limited

39 Standard Chartered Bank Kenya Limited

40 Trans-National Bank Limited

41 UBA Kenya Bank Limited

42 Victoria Commercial Bank Limited

(CBK, 2016)

Appendix 4: Research Instrument

This questionnaire aims to collect data on the effect of emerging digital security solutions on fraud risk management in the banking sector in Kenya. I am conducting this survey as part of the fulfilment of the degree of Masters of Business Administration (MBA) at Strathmore University. Therefore, it is purely for academic purposes. Your participation is voluntary, and the responses you provide will remain confidential. The survey shall not collect any personally identifiable information.

Please read each question carefully and answer by ticking against the most appropriate answer.

SECTION A: BACKGROUND INFORMATION

1. Please indicate your gender.

☐ Male ☐ Female

2. Which of the following age groups do you fall into?

☐ Less than 30 years ☐ 31-40 years

☐ 41-50 years ☐ Above 50 years

3. What is the highest degree or level of school you have completed?

☐ Diploma ☐ Undergraduate

☐ Postgraduate ☐ Other

4. How long have you worked in this organization?

☐ Less than 5 years ☐ 5-10 years

☐ 11-15 years ☐ More than 15 years

5. How regularly are the fraud risk management reviews held by the Board or management in your organization?

☐ Monthly ☐ Quarterly

☐ Semi-annually ☐ Annually

6. Name of the commercial bank (optional) _____

SECTION B: RISK MANAGEMENT PRACTICES

This section relates to your response regarding fraud risk management practices in your organization. Please indicate the extent to which you agree or disagree with each statement by placing an "X" on the column that best matches your response.

	1	2	3	4	5
In my view, our organization uses ultramodern fraud risk detection mechanisms to monitor transactions and root out fraudulent activities on an ongoing basis.					
I am of the strong opinion that our organization leverages innovative tools to assess fraud exposure and its associated risks to strengthen existing controls.					
I believe my organization reviews and updates its internal fraud risk controls regularly to adapt to changing business needs, threat landscape, and emerging technologies.					
Our organization employs a robust and streamlined anti-fraud technology that detects anomalies and flags, and reports them in real time.					
Besides investing in anti-fraud technology, our organization has a solid structure of rules, practices, and processes for effective fraud risk management.					

Note: 1=Strongly Disagree; 2=Disagree; 3=Neither Agree nor Disagree; 4=Agree; and 5=Strongly Agree.

SECTION C: BIOMETRICS TECHNOLOGY

This section relates to your response regarding the usage of biometrics technology to control fraud risk in your organization. Please indicate the extent to which you agree or disagree with each statement by placing an "X" on the column that best matches your response.

	1	2	3	4	5
I have seen and tested this organization's application of face recognition technology for financial fraud, and I think it is a great solution for fraud risk prevention.					
Having been exposed to voice recognition, I think it is a more convenient and efficient solution for authenticating users and combating fraud.					
I would encourage the organization to expand the use of fingerprints for user identification because I believe it is effective in fraud prevention.					
Retinal scanning is a useful biometric technique for organizations that helps with countering financial fraud more effectively.					
I think it is a great idea to use hand geometry recognition to control financial fraud in the organization.					

Note: 1=Strongly Disagree; 2=Disagree; 3=Neither Agree nor Disagree; 4=Agree; and 5=Strongly Agree.

SECTION D: ARTIFICIAL INTELLIGENCE

This section relates to your response regarding the use of artificial intelligence (AI) to control fraud risk in your organization. Please indicate the extent to which you agree or disagree with each statement by placing an "X" on the column that best matches your response.

	1	2	3	4	5
I am of the view that the application of artificial intelligence technology in the organization is important to the fight against financial fraud.					

I think that the artificial intelligence solution the organization uses provides a more accurate assessment of fraud risks and accelerates the response to fraudulent activities.					
In my opinion, the overall effectiveness of the organization's fraud risk management improves with the increased use of artificial intelligence.					
I believe the AI-based fraud detection system, which relies on powerful algorithms, enables better fraud risk management in the organization.					
It is my view that artificial intelligence has been a major part of automating processes for predicting potential risks and detecting, and preventing fraud in banking transactions, app usage, payment methods, and other financial activities.					

Note: 1=Strongly Disagree; 2=Disagree; 3=Neither Agree nor Disagree; 4=Agree; and 5=Strongly Agree.

SECTION E: DATA ANALYTICS

This section relates to your response regarding the use of data analytics to control fraud risk in your organization. Please indicate the extent to which you agree or disagree with each statement by placing an "X" on the column that best matches your response.

	1	2	3	4	5
From my observation, integrating data analytics into fraud management mechanisms ensures a satisfactory level of effectiveness in controlling fraud.					
I believe that data analytics and its predictive modelling capability make it easier to predict possible fraudulent activities and take appropriate responsive actions.					

The idea that data analytics tools can help assess fraud risks and determine their impact is great for the organization and its mission to combat fraud.					
I have seen the application of data analytics, and I would say that without it, it would be difficult to uncover and act on the hidden patterns of financial fraud on digital platforms.					
Data analytics enables risk management personnel to integrate data from various sources into a single platform that simplifies the fraud risk management process.					

Note: 1=Strongly Disagree; 2=Disagree; 3=Neither Agree nor Disagree; 4=Agree; and 5=Strongly Agree.

Thank You for Your Participation

Appendix 5: Research Budget

BUDGET SUMMARY

Research Topic: The Effect of Emerging Digital Security Solutions on Fraud Risk Management in the Banking Sector in Kenya.

Project Duration: 8th April – 12th April 2024.

Cost		**Total cost (KES)**
Fees		**1,000**
Project personnel expenses	**60,000**	
Data collection and analysis	**61,000**	**121,000**
Miscellaneous		**10,000**
	Total	**132,000**

BUDGET BREAKDOWN

Fees

	Role	**Total Cost (KES)**
Research license	National Commission for Science, Technology, and Innovation (NACOSTI) research license.	**1,000**

Project Personnel Expenses

	Role	**Days**	**Rate**	**Total Cost (KES)**
Principal Investigator	Project planning and workshops, seminars, tours, etc.			**25,000**
	Report preparation and manuscript publication			**15,000**

	Meetings and evaluations	10	2,000	**20,000**
			Subtotal	**60,000**

Data Collection and Analysis

	Role	**Days**	**Rate**	**Total Cost (KES)**
Travelling expenses	Research instrument distribution	2	6,500	**13,000**
	Collection of completed research instruments	2	6,500	**13,000**
	Travel to and from the university.			**10,000**
Cost of materials, services, and expendables	Telephone and Internet services			**5,500**
	Consultancy services			**8,000**
	Stationery			**5,000**
	Printing and photocopying			**6,500**
			Subtotal	**61,000**

Miscellaneous

	Role	**Total Cost (KES)**
Other costs	Unplanned costs and provision for cost variance	**10,000**