

**AN ASSESSMENT OF CLOUD COMPUTING AND ITS IMPACT ON DATA
SECURITY IN HEALTHCARE: A CASE STUDY OF M-TIBA.**

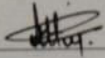
**MUTUGI EVANS KIMATHI
ICT-G-4-0767-18**

**A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF COMPUTING AND
INFORMATICS IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE
AWARD OF THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER
SCIENCE OF GREYSA UNIVERSITY.**

NOVEMBER, 2024

DECLARATION


I hereby declare that this project is my original work, and has not been presented for award of degree or for any other purpose in any other institution.

Signature  Date 25/11/2024

Mutugi Evans Kimathi

ICT-G-4-0767-18

Supervisor: This research project has been submitted with my approval as University supervisor

Signature  Date 25/11/2024

Mr. Stanley Muli

School of computing and informatics.

DEDICATION

I dedicate this research project to myself, in proof that you can achieve anything if and when you set your mind to it. The sleepless nights and moments of doubt were worth it in the end.

ACKNOWLEDGEMENT

My sincere gratitude is extended to my friends for their unwavering encouragement and support. Their encouraging words and emotional support were crucial in helping me stay motivated. I want to thank my family from the bottom of my heart for their constant understanding, patience, and support during this journey. My achievement was largely attributed to their support and faith in me. Finally, I would like to express my gratitude to my supervisor, Mr. Muli, for his professional advice, insightful criticism, and unwavering support. The accomplishment of this investigation was made possible by his guidance and support.

TABLE OF CONTENTS

| | |
|---|------|
| DEDICATION | iii |
| ACKNOWLEDGEMENT | iv |
| TABLE OF CONTENTS..... | v |
| OPERATIONAL DEFINITION OF TERMS | viii |
| ABSTRACT..... | ix |
| CHAPTER ONE: INTRODUCTION..... | 1 |
| 1.1 Background to the study..... | 1 |
| 1.2 Statement of the problem | 2 |
| 1.3 Objectives of study..... | 2 |
| 1.3.1 General objectives | 2 |
| 1.3.2 Specific objectives..... | 2 |
| 1.4 Purpose of study | 3 |
| 1.5 Research questions | 3 |
| 1.6 Significance of study..... | 3 |
| 1.7 Scope of study | 3 |
| CHAPTER TWO: LITERATURE REVIEW | 4 |
| 2.1 Cloud computing in healthcare | 4 |
| 2.2 Security challenges in cloud computing..... | 4 |
| 2.3 Security measures in cloud computing..... | 5 |
| 2.4 User awareness and impact on security..... | 6 |
| 2.5 The M-TIBA platform..... | 7 |
| 2.6 Theoretical frameworks..... | 7 |
| 2.6.1 Conceptual framework | 8 |
| 2.7 Conclusion..... | 9 |
| 2.7.1 Summary..... | 9 |
| 2.7.2 Implications of study | 9 |
| CHAPTER THREE: RESEARCH METHODOLOGY | 10 |
| 3.1 Research design..... | 10 |
| 3.2 Study area..... | 10 |
| 3.3 Target population | 10 |
| 3.4 Sample size..... | 11 |

| | |
|--|----|
| 3.5 Sample techniques..... | 12 |
| 3.6 Measurement of variables | 12 |
| 3.7 Research instruments..... | 12 |
| 3.8 Reliability of instruments | 12 |
| 3.9 Data collection techniques | 12 |
| 3.10 Data analysis | 12 |
| 3.11 Logistical and ethical considerations | 13 |
| CHAPTER FOUR: FINDINGS AND DISCUSSIONS | 14 |
| 4.1 Introduction | 14 |
| 4.2 Quantitative analysis | 14 |
| 4.2.1 Demographic findings | 14 |
| 4.2.1.1 Gender distribution | 14 |
| 4.2.1.2 Occupation and literacy levels | 14 |
| 4.2.1.3 Digital literacy | 15 |
| 4.2.2 Satisfaction with the cloud based service | 16 |
| 4.2.3 Security concerns among respondents..... | 16 |
| 4.2.4 Cloud computing characteristics and perceived impact | 17 |
| 4.2.5 Cloud adoption and perceived security | 17 |
| 4.4 Qualitative data analysis..... | 18 |
| 4.5 Implications of the present results..... | 19 |
| 4.6 Significance of present results..... | 19 |
| CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS | 20 |
| 5.1 Introduction | 20 |
| 5.2 Summary of findings..... | 20 |
| 5.3 Conclusions | 21 |
| 5.4 Recommendations | 21 |
| REFERENCES | 23 |
| APPENDICES | 25 |
| 6.1 Sample Research Instruments | 25 |
| 6.1.1 Structured Questionnaire | 25 |
| 6.1.2 Interview Guide for IT Professionals and Policymakers..... | 27 |
| 6.1.3 Focus Group Discussion Guide | 27 |

LIST OF FIGURES

| | |
|---|----|
| Figure 1: conceptual framework | 8 |
| Figure 2 pie chart to show gender distribution | 14 |
| Figure 3 pie chart showing digital literacy levels | 15 |
| Figure 4 bar graph showing user satisfaction levels within mtiba..... | 16 |
| Figure 5 bar graph showing security concerns | 16 |
| Figure 6 line chart showing relation between cloud characteristics and influence..... | 17 |

OPERATIONAL DEFINITION OF TERMS

| | |
|--|---|
| M-TIBA | a mobile health platform intended to increase Kenyans' access to medical treatment. the program serves as a mobile health wallet, allowing users to send, save, and receive funds designated only for medical costs |
| SPSS (Statistical Package for the Social Sciences) | a software tool used for data analysis, statistical operations, and graphical representation of data. it is widely utilized in social sciences, business, health sciences, and many other fields for conducting various types of statistical tests and managing large datasets. |

ABSTRACT

This study examines the effectiveness of cloud computing for data security in healthcare, specifically through the M-TIBA platform—a cloud-based service enabling users to manage healthcare finances and data. While cloud technology offers significant benefits in accessibility and scalability, its application in healthcare raises critical concerns about data security and user trust. Current literature and industry practices reveal a gap in user awareness and limited digital literacy, which undermine the effective adoption of cloud technologies in healthcare. Thus, the primary problem addressed is how cloud computing characteristics, security measures, and user education impact data security and trust among healthcare users in Kenya. The study aims to address three key objectives: to assess how user awareness influences security effectiveness within M-TIBA, to evaluate the current security measures' impact on user trust, and to investigate how cloud computing's intrinsic characteristics affect data security. The research builds on foundational theories, including the Technology Acceptance Model (TAM) and the Information Systems Success Model (ISSM). TAM provides insights into factors that influence technology adoption, while ISSM explores how information systems succeed based on system quality, service, and information. Using a mixed-methods design, the study integrates both quantitative and qualitative data collection, with structured questionnaires and semi-structured interviews. The study targeted users of the M-TIBA platform, healthcare providers, and policymakers/IT professionals. The sample size was calculated at 450 participants, with an 80% anticipated response rate resulting in 360 usable responses. Quantitative data analysis was supported by statistical methods to measure correlations between digital literacy, security awareness, and perceived security measures, while qualitative data helped capture nuanced perspectives on trust and technology adoption. The findings reveal that higher digital literacy is linked to increased adoption and trust in cloud services, while limited user awareness remains a barrier to securing data effectively. Additionally, most users expressed moderate satisfaction with M-TIBA's security measures but emphasized a need for increased transparency on data protection practices. Security concerns such as data breaches and unauthorized access were notable among healthcare providers, suggesting that security protocols alone do not fully alleviate user concerns without proper education and engagement. In conclusion, the study highlights the critical role of user education in enhancing cloud security effectiveness and recommends implementing routine digital literacy programs, particularly in healthcare settings. Furthermore, policymakers should prioritize developing comprehensive security protocols tailored to the unique requirements of healthcare data. Enhanced transparency and continuous investment in advanced security measures are essential to fostering trust and ensuring sustainable cloud adoption in healthcare.

CHAPTER ONE: INTRODUCTION

1.1 Background to the study

Because cloud computing makes data processing, sharing, and storage more efficient, it has the potential to completely change the healthcare sector. Its implementation promotes the scalability of healthcare services and makes it easier for patients to receive better care by enabling easy access to their medical records (Shah et al., 2022). Cloud computing has several advantages, such as lower costs, better data management, and increased provider collaboration. These benefits do, however, present serious data security risks. Risks associated with cloud migration include unauthorized access, data breaches, and challenges in adhering to strict data protection laws. For this reason, healthcare providers must prioritize protecting sensitive patient data in cloud environments. The manner that medical data is shared, accessed, and kept has significantly improved as a result of the use of cloud computing in the healthcare industry. Improved patient outcomes and more effective healthcare delivery are supported by the scalable and adaptable data management solutions provided by cloud computing (Aitwajjiry, Ahmad 2020). Cloud computing improves patient care overall by providing easy access to medical records and enabling real-time communication between healthcare practitioners.

But the move to cloud-based systems also brings with it increased threats for data security, such as breaches of data, illegal access, and difficulties adhering to data protection laws (Mehrtak et al., 2021). Thus, it is crucial to guarantee the confidentiality and privacy of medical data in cloud environments. The M-TIBA platform is a trailblazing mobile health wallet in Kenya that helps millions of users access medical services and make payments for healthcare. This platform is especially important for low-income people who have trouble affording healthcare. M-TIBA enables users to transfer, save, and receive money designated for healthcare, preventing access to essential medical services from being hampered by a lack of funds (Nan, 2021). Ensuring that financial limitations do not impede access to medical services is the platform's main objective, along with making healthcare payments easier. As a reflection of Kenya's diversified population, M-TIBA's user base comprises people from both urban and rural locations. M-TIBA plays a crucial role in Kenya's healthcare infrastructure since it helps insurers and healthcare providers manage patient data and streamline financial transactions. Patients, insurance companies, and healthcare practitioners are just a few of the many diverse groups that the M-TIBA platform supports in Kenya (Musembi, 2024). In an effort to improve

healthcare accessibility for marginalized people and expedite the provision of medical services, M-TIBA uses cloud computing to handle health-related transactions and store patient data.

1.2 Statement of the problem

Healthcare companies can save money, increase scalability, and improve flexibility by implementing cloud-based solutions. Cloud computing does, however, come with significant drawbacks in addition to these advantages, most notably with regard to sensitive healthcare data security and privacy (Sivan et al., 2021). The risks that come with data breaches, illegal access, and adhering to data protection laws make a careful analysis of cloud computing's effect on data security in healthcare settings imperative. An important case study for evaluating the effect of cloud computing on healthcare data security in Kenya is the M-TIBA platform. M-TIBA is a mobile health wallet that aims to increase millions of Kenyans' access to and cost of healthcare, especially for those living in underserved and low-income areas. The platform lowers financial obstacles to healthcare by enabling users to save, send, and receive money designated for that purpose.

The platform is more susceptible to security risks such as cyberattacks, data breaches, and unauthorized access since it depends more and more on cloud-based services. These flaws have the potential to hurt users and erode their trust in the platform by jeopardizing the availability, confidentiality, and integrity of medical data. This study intends to uncover current vulnerabilities, evaluate the effects of cloud computing on data security within the M-TIBA platform critically, and suggest improvements to data protection for all parties concerned. The study aims to resolve these issues in order to guarantee that M-TIBA can carry on offering dependable and safe healthcare services, upholding user confidence and protecting private health data.

1.3 Objectives of study

1.3.1 General objectives

To assess cloud computing and its impact on data security in healthcare, under a case study of M-TIBA.

1.3.2 Specific objectives

- i. Assess the characteristics of cloud computing and their overall impact on security posture of the M-TIBA platform.

- ii. Assess how the security measures in place affect or influence user trust and engagement.
- iii. Assess the extent and influence of user awareness on the effectiveness of the security measures within the M-TIBA platform.

1.4 Purpose of study

The purpose of this study is to assess the impact of cloud computing on data security within the healthcare sector, with a specific focus on the M-TIBA platform in Kenya, while also evaluating current data security measures, analyzing the overall cloud impact of the platform, and develop best practices.

1.5 Research questions

The research questions formulated for the study will be as follows: to what extent does user awareness and education contribute to the effectiveness of data security measures, how do the current security measures already implemented within the platform affect the overall posture, and finally how do the characteristics of cloud computing influence usage.

1.6 Significance of study

The significance of this study will be to enhance healthcare practices, advance knowledge in cloud computing security, support sustainable healthcare systems and to strengthen the trust in cloud-based healthcare solutions.

1.7 Scope of study

The study is limited in scope to Kenya and focuses specifically on the M-TIBA platform, which is extensively utilized in the nation to streamline healthcare payments and administration. The study's focus is the healthcare industry, and it looks at how cloud computing technologies are applied there and how it affects data security.

CHAPTER TWO: LITERATURE REVIEW

2.1 Cloud computing in healthcare

With its many advantages—such as increased flexibility, scalability, and cost savings—cloud computing has completely changed the healthcare industry. Healthcare companies may effectively handle massive volumes of data and enhance patient care because of the cloud's capacity to offer on-demand resources and services (Sivan & Zukarnain, 2021). Using cloud-based solutions makes it easier for medical records to be shared seamlessly between departments and organizations, which encourages cooperation between healthcare professionals and enhances patient outcomes (Shah & Konda, 2022). Moreover, cloud computing facilitates the integration of diverse health information systems, an essential component for the deployment of telemedicine services and electronic health records (EHRs). The move to cloud computing, however, also brings with it serious security risks, particularly with regard to the confidentiality of private medical information. Personal health information (PHI), which is governed by stringent legal frameworks like the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States, is frequently included in healthcare data (Almeida et al., 2020).

Strict procedures are required to guarantee the availability, confidentiality, and integrity of data under these regulations. Therefore, in order to abide by these legal obligations and safeguard patient privacy, healthcare companies need to put strong security measures in place. It is also more difficult to maintain and keep an eye on security controls in cloud computing systems because of their dynamic nature, which is marked by quick resource deployment and scalability. An increased risk of data leakage and illegal access results from the multi-tenancy architecture of the cloud, where multiple clients share the same infrastructure (Fernandes et al., 2014). For the purpose of properly protecting their data, healthcare providers must thus be aware of the cloud service models and the corresponding security implications.

2.2 Security challenges in cloud computing

The security and privacy of patient data are the main issues with cloud computing in the healthcare industry. Because cloud environments involve shared resources and remote access by design, they are vulnerable to a range of cyber dangers, such as insider threats, illegal access,

and data breaches (Kaur & Mustafa, 2020). The cloud services' multi-tenancy architecture, which involves several clients sharing the same infrastructure, raises the possibility of data leaks and illegal access. Additionally, because healthcare data has a high value and can be utilized for identity theft, insurance fraud, and other nefarious actions, cloud infrastructures are frequently the target of hackers. Furthermore, the management and oversight of security controls are made more difficult by the dynamic and scalable nature of cloud infrastructures. Cybercriminals may be able to take advantage of misconfigurations and vulnerabilities caused by the quick deployment of resources and services (Fernandes et al., 2014). To solve these issues, healthcare institutions need to put in place comprehensive security plans that involve ongoing vulnerability assessments, ongoing monitoring, and incident response planning. The shared responsibility framework in cloud computing, which divides security responsibilities between the cloud service provider (CSP) and the healthcare organization, presents another major difficulty (Shah & Konda, 2022). To find and fix possible vulnerabilities, this paradigm needs thorough risk assessments and well-defined security role definitions. Healthcare companies need to make sure that their CSPs have the necessary controls in place to protect patient data and that they adhere to applicable security standards and policies.

2.3 Security measures in cloud computing

To ensure data availability, confidentiality, and integrity in cloud-based healthcare platforms, effective security measures are essential. According to Hashem et al. (2015), encryption is a fundamental security method that guarantees data protection during both storage and transmission. To protect data transmissions and storage, secure socket layer (SSL) protocols and advanced encryption standards (AES) are frequently utilized. To guarantee that encryption keys are handled and kept securely, healthcare institutions should also put strong key management procedures into place. According to Zissis and Lekkas (2012), access control methods play a crucial role in limiting access to sensitive information.

These mechanisms involve the installation of role-based access control (RBAC) and multi-factor authentication (MFA). RBAC makes sure that users can only access the information and tools required for their responsibilities, while MFA adds another degree of security by requiring users to authenticate using numerous ways. These steps lessen the chance of data breaches and help prevent unwanted access. To find any systemic weaknesses and guarantee adherence to security policies and standards, regular security audits and vulnerability assessments are crucial

(Hashizume et al., 2013). To give an unbiased evaluation of the security posture, these audits must be carried out by impartial third parties. Furthermore, implementing intrusion prevention systems (IPS) and intrusion detection systems (IDS) can improve the real-time detection and mitigation of harmful activity (Chen et al., 2019). These programs can automatically block or notify administrators of possible dangers by scanning network traffic for indications of questionable behavior.

2.4 User awareness and impact on security

The degree to which security features in cloud computing systems are successful is largely dependent on user understanding. Research has indicated that users' risk of security breaches is greatly decreased when they are informed about potential security threats and appropriate practices for data protection (Alotaibi, 2016). According to Gupta et al. (2018), user training programs ought to address subjects including spotting phishing efforts, coming up with secure passwords, and appreciating the value of data encryption. With the use of these tools, users can acquire the abilities and information required to defend their companies and themselves against online attacks. Encouraging patients and healthcare workers to understand the value of data security can improve cloud-based systems' overall security.

To avoid unintentional data leaks and guarantee regulatory compliance, healthcare personnel need to be knowledgeable on the most recent security measures and processes (Almeida et al., 2020). Furthermore, encouraging a security-aware culture inside healthcare institutions can result in more proactive security risk identification and mitigation (Gupta et al., 2018). To help users stay updated about new dangers and data protection best practices, frequent training and awareness efforts are needed. Furthermore, patients and other stakeholders are included in the concept of user awareness in addition to healthcare professionals. Patients ought to be informed about the value of safeguarding their private medical records and the precautions they can take to keep their information safe. This entails being aware of phishing efforts, knowing how to use secure communication channels, and knowing what to do in the event that a data breach is discovered. Healthcare companies may greatly improve the security of their cloud computing platforms by encouraging a culture of security awareness among all users.

2.5 The M-TIBA platform

M-TIBA is a mobile health wallet created to increase marginalized populations in Kenya's access to healthcare. It lowers barriers to healthcare access by managing financial transactions and health records using cloud computing (Gachoka et al., 2018). The website makes it easier for members of underprivileged and low-income groups to acquire medical treatment by letting them save, send, and receive money expressly for healthcare needs. M-TIBA's broad user base depends on its ability to grow effectively and handle massive volumes of transactions and data, which is made possible by the integration of cloud services. Despite the advantages, M-TIBA's dependence on cloud services leaves it open to cyberattacks, so a careful evaluation of its user awareness initiatives and security protocols is required. The platform is more vulnerable to hazards including cyberattacks, data breaches, and illegal access because of its reliance on cloud infrastructure (Ndung'u et al., 2020).

Securing sensitive user data on the M-TIBA platform necessitates putting strong security measures in place, such as access restriction, encryption, and frequent security audits. Additionally, user knowledge is essential to the security of the site. Users' capacity to secure their health information can be improved by teaching them about potential security risks and best practices for data protection. To promote safe behaviors and increase knowledge of security risks, the M-TIBA platform should make investments in extensive user training programs (Gachoka et al., 2018). Users can learn the value of data protection via these programs, as well as how to spot any security risks and take appropriate action. To make sure that its defenses against changing threats continue to be effective, M-TIBA should also conduct frequent security reviews and updates. To find and fix any security flaws, this involves carrying out compliance audits, penetration testing, and vulnerability scanning. By establishing a security-conscious culture and consistently enhancing its security posture, M-TIBA can preserve user confidence while guaranteeing the security of private health information.

2.6 Theoretical frameworks

Several theoretical frameworks can support the research of cloud computing in healthcare, especially with regard to data security. A helpful framework for comprehending how healthcare professionals and organizations embrace and employ cloud computing technology is provided by Davis' (1989) Technology Acceptance Model (TAM). According to TAM, perceived utility and ease of use are the main variables driving the uptake of new technology. By using this

model, it will be possible to determine the elements that influence cloud computing adoption in healthcare settings as well as the perceived advantages and difficulties of doing so.

The Information Systems Success Model (ISSM), put out by DeLeone and McLean (1992), is another pertinent framework. According to ISSM, the quality of the system, the information, and the services all affect user satisfaction and net benefits, which in turn determine the success of the information system. By concentrating on the system's quality, the information it offers, and the services it provides, this model can be used to assess the efficacy of cloud computing tools like M-TIBA. Researchers can evaluate how these elements affect the general efficacy and security of cloud-based healthcare systems by utilizing ISSM.

2.6.1 Conceptual framework

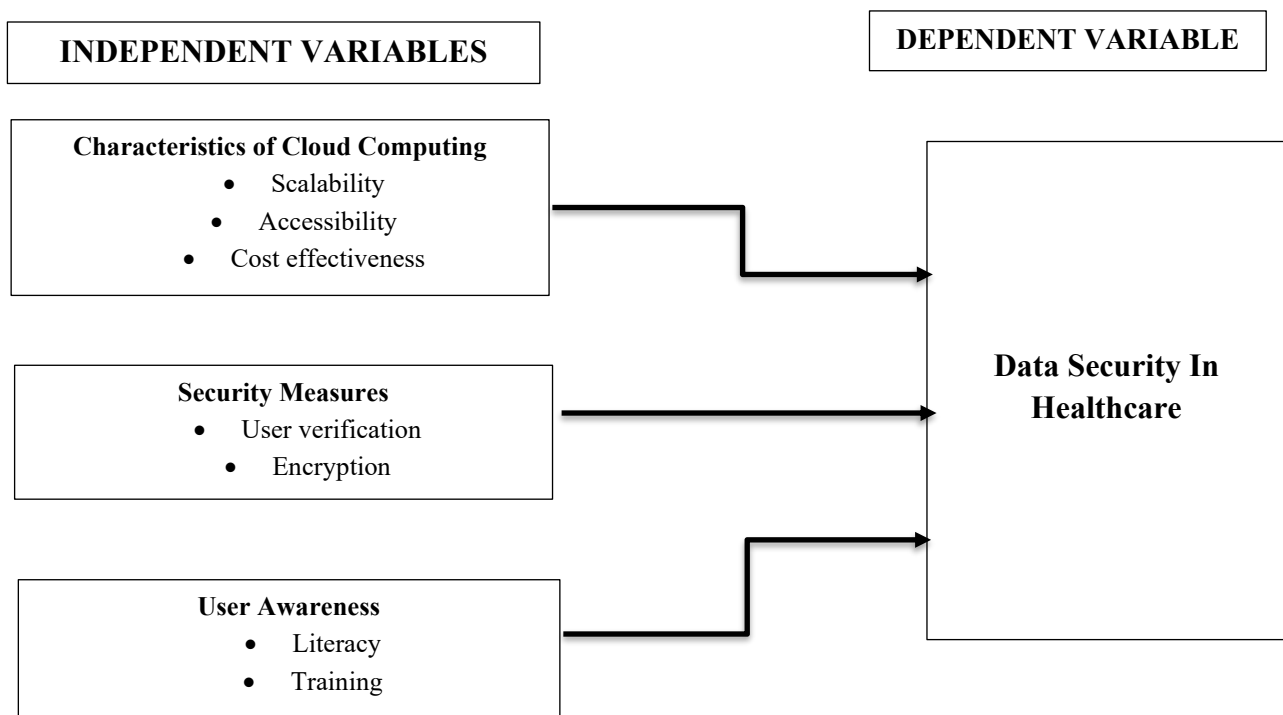


Figure 1: conceptual framework

2.7 Conclusion

2.7.1 Summary

The integration of cloud computing in healthcare is examined in the literature study, which also addresses major security concerns. Benefits of cloud computing include cost savings, scalability, and better patient care. These difficulties include managing dynamic, multi-tenant cloud infrastructures, safeguarding sensitive health data, and complying with legal frameworks such as GDPR and HIPAA. To reduce these threats, strong security measures like access control, encryption, and recurring security audits are crucial. The study places a strong emphasis on how crucial user awareness is to stopping security lapses and guaranteeing protocol compliance. A case study is conducted on the M-TIBA platform, a mobile health wallet in Kenya, to demonstrate the usefulness of cloud computing in the healthcare industry and the necessity of strong security and user awareness initiatives.

2.7.2 Implications of study

Healthcare delivery could be revolutionized by cloud computing, but its success depends on how security issues are resolved and user awareness is raised. Healthcare companies may optimize cloud computing benefits while protecting patient data by utilizing theoretical frameworks and putting strong security procedures in place.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Research design

A mixed-methods research methodology was deemed the most suitable for evaluating the effect of cloud computing on data security in healthcare, using M-TIBA as a case study. This design provided a thorough understanding of the issues by combining qualitative and quantitative methodologies. Quantitative approaches, such as surveys and structured questionnaires, were used to gather numerical data on security measures, user awareness, and the frequency of security breaches. Additionally, qualitative techniques, including focus groups and interviews, were employed to delve deeply into the opinions and experiences of M-TIBA stakeholders and users regarding data security.

3.2 Study area

The M-TIBA platform is actively used in Kenya, where the study was conducted. To collect a wide range of experiences and challenges related to data security, the research specifically focused on both urban and rural locations. This regional diversity helped ensure that the results accurately reflected the various settings in which M-TIBA operated.

3.3 Target population

To determine an appropriate sample size for a population of 10,000 users on the M-TIBA platform, Cochran's formula was applied. The formula was used to calculate the required sample size for a given level of precision, confidence level, and variability:

$$n_0 = \frac{Z^2 \cdot p \cdot (1 - p)}{e^2}$$

Where:

- n_0 is the sample size,
- Z is the Z-value (the number of standard deviations from the mean for the desired confidence level),
- p is the estimated proportion of the population (variability),
- e is the margin of error.

Assuming:

- A confidence level of 95%, corresponding to a Z-value of 1.96,
- A variability (p) of 0.5 (50%, which is the most conservative estimate),
- A margin of error (e) of 5% (0.05).

First, Cochran's formula for an infinite population is calculated:

$$n_0 = \frac{(1.96)^2 \cdot (0.5) \cdot (0.5)}{(0.05)^2} = 384.16 \approx 385$$

For a finite population of 10,000 users, the finite population correction formula is applied:

$$n = \frac{n_0}{1 + \left(\frac{n_0 - 1}{N}\right)}$$

Where:

- n is the adjusted sample size,
- N is the population size (10,000 users).

$$n = \frac{385}{1 + \left(\frac{384}{10,000}\right)} = 385 \div 1.0384 = 370.8 \approx 371$$

To account for potential non-responses, an additional 20% is added to ensure the final sample size is sufficiently representative:

$$n\text{-final} = 371 \times 1.2 = 445.2 \approx 450$$

Thus, the final sample size of **450 respondents** was selected, allowing for sufficient representation of M-TIBA users while maintaining the desired confidence level and margin of error.

3.4 Sample size

The 450 respondents were stratified into key subgroups to ensure proportional representation: M-TIBA users, healthcare providers and, IT professionals and policy makers.

3.5 Sample techniques

There was an overlap between purposive and stratified random sampling methods. Various sub-groups were sufficiently represented through stratified random selection. The study employed purposive sampling to identify key informants, including policymakers and IT professionals, who provided expert perspectives on the security measures implemented in the platform.

3.6 Measurement of variables

The variables that were measured included: user awareness, which gauged awareness of data protection policies and knowledge of security procedures; measures of data security, which assessed trust in the security measures already in place; and the adoption of the M-TIBA platform as a cloud service.

3.7 Research instruments

The main research instruments included structured questionnaires for quantitative data collection, interview guides for qualitative interviews with IT professionals and policymakers, and focus group discussions that facilitated conversations with various stakeholders.

3.8 Reliability of instruments

Using a test-retest methodology, which involved administering the survey to the same respondents twice, reliability was evaluated. To verify internal consistency, the consistency of the responses was examined using Cronbach's alpha.

3.9 Data collection techniques

Data was collected through online and paper based surveys, face-to-face interviews and focus group discussions conducted for willing participants.

3.10 Data analysis

Regression analysis, correlation analysis, and descriptive statistics was performed on quantitative data using statistical software (e.g., SPSS). Thematic analysis was then used to examine and categorize recurrent themes and patterns in qualitative data.

3.11 Logistical and ethical considerations

Logistical considerations:

- i. Securing permissions from relevant authorities to conduct the study.
- ii. Coordinating data collection schedules to minimize disruption to participants.
- iii. Ensuring access to reliable internet for online surveys and virtual interviews.

Ethical considerations:

- i. Obtaining informed consent from all participants, explaining the study's purpose, and ensuring voluntary participation.
- ii. Ensuring confidentiality and anonymity of participants' data.
- iii. Adhering to ethical guidelines for research, including data protection regulations.

CHAPTER FOUR: FINDINGS AND DISCUSSIONS

4.1 Introduction

This chapter presents the findings based on an 80% response rate from the sample of 450 respondents, yielding a total of 360 responses. The results are divided into demographic information, findings related to study objectives, inferential statistics, and an analysis of overall patterns.

4.2 Quantitative analysis

4.2.1 Demographic findings

4.2.1.1 Gender distribution

Out of 360 respondents, 58% identified as male (209), and 42% as female (151). The gender distribution is illustrated in the pie chart below:

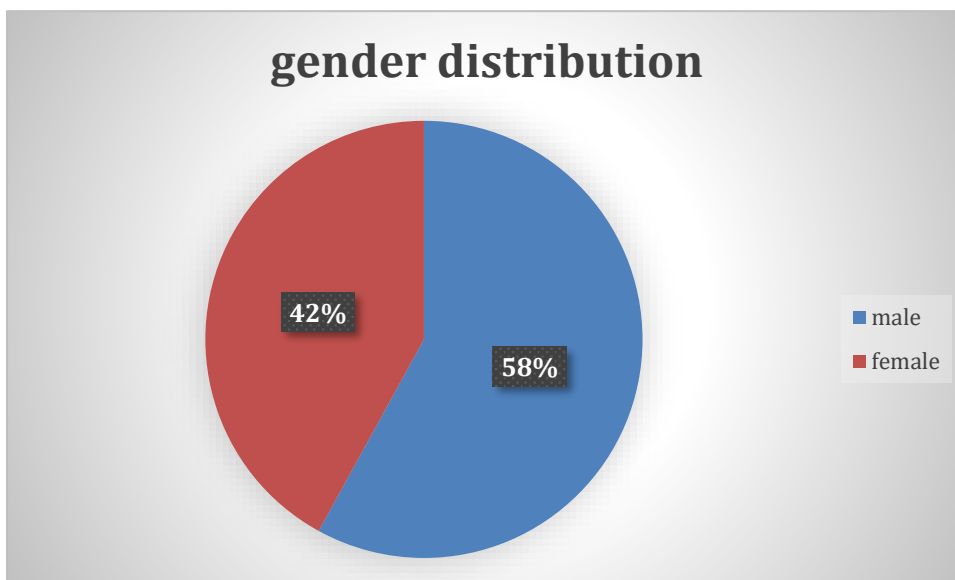


Figure 2 pie chart to show gender distribution

4.2.1.2 Occupation and literacy levels

| Occupation | Primary School | Secondary School | Undergraduate | Postgraduate | None | Total |
|----------------------|----------------|------------------|---------------|--------------|------|-------|
| General Users | 15 | 45 | 125 | 25 | 10 | 200 |
| Healthcare Providers | 0 | 25 | 60 | 20 | 0 | 105 |

| | | | | | | |
|------------------------------------|---|----|----|----|---|----|
| <i>Polymakers/IT Professionals</i> | 0 | 15 | 20 | 10 | 0 | 45 |
|------------------------------------|---|----|----|----|---|----|

Table 1 occupation and literacy levels table

These findings provide insight into how each group perceives M-TIBA's security features and adoption. Higher literacy among policymakers and IT professionals suggests greater knowledge of security best practices, directly supporting the objective of examining how user awareness influences the effectiveness of security measures. Their expertise also aligns with the objective of assessing how cloud computing characteristics impact data security, as they can identify key strengths and vulnerabilities in the platform.

4.2.1.3 Digital literacy

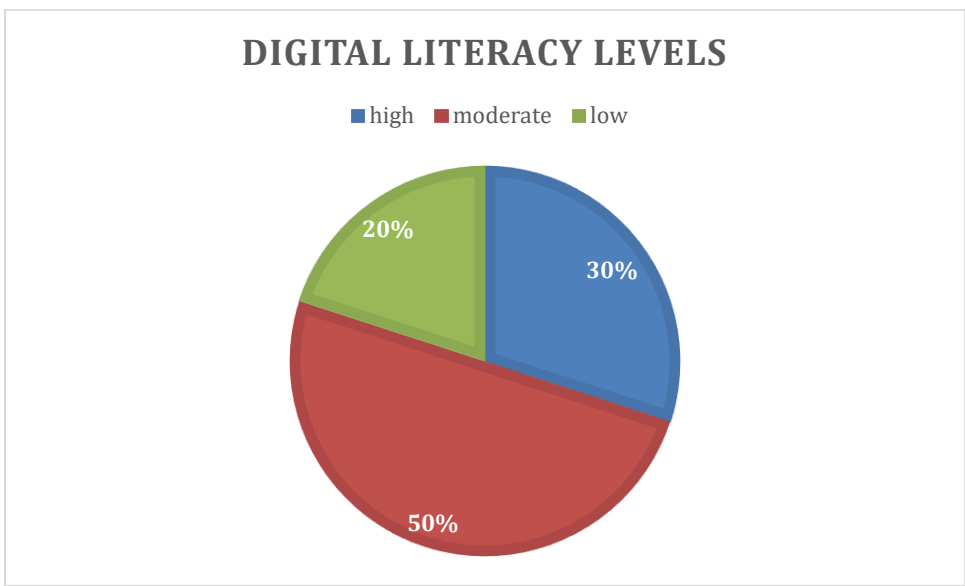


Figure 3 pie chart showing digital literacy levels

The findings demonstrate that digital literacy levels significantly influence adoption rates, security concerns, and interaction with M-TIBA's cloud-based healthcare solutions. Higher literacy levels lead to increased engagement with advanced features and more detailed security awareness, while lower literacy levels limit adoption and trust. This supports the research objectives by highlighting the importance of user awareness and education in enhancing security, fostering trust, and addressing concerns within cloud-based healthcare platforms.

4.2.2 Satisfaction with the cloud based service

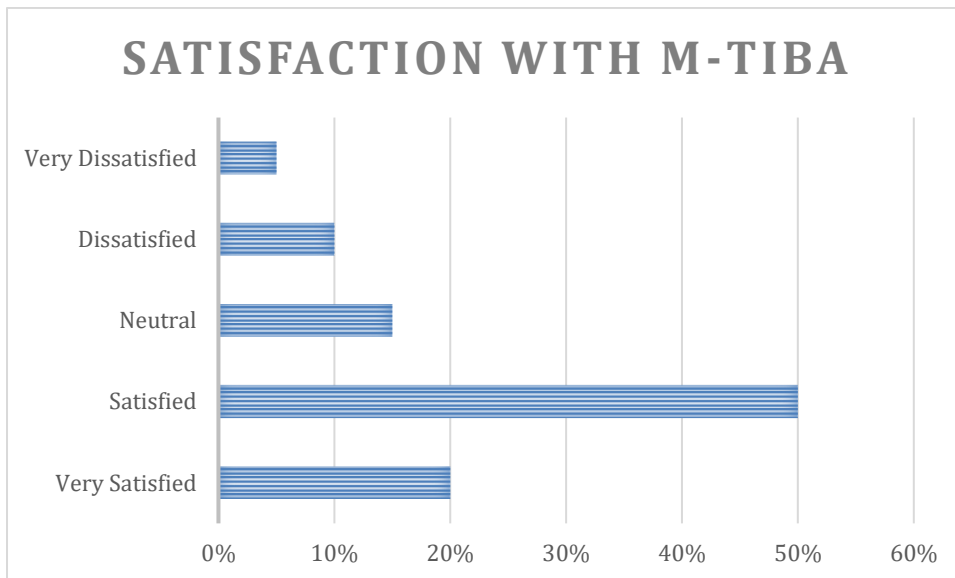


Figure 4 bar graph showing user satisfaction levels within mtiba

High user satisfaction reflects a positive perception of M-TIBA's ability to securely manage healthcare data, with satisfied users more likely to adopt and continue using the platform. This suggests that positive experiences with the platform foster adoption. Additionally, higher satisfaction levels indicate users' confidence in the effectiveness of M-TIBA's security features, aligning with the study's focus on evaluating security measure effectiveness.

4.2.3 Security concerns among respondents

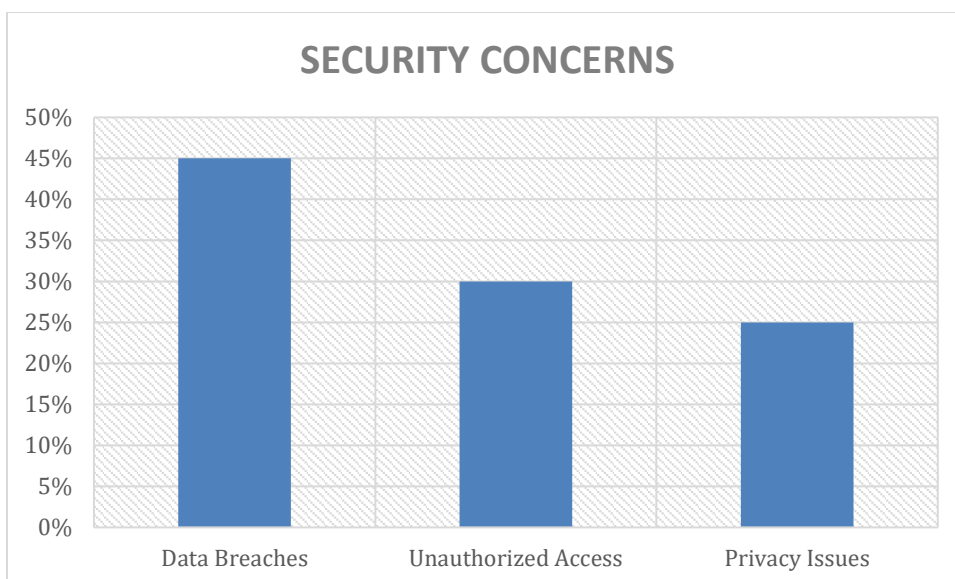


Figure 5 bar graph showing security concerns

Users are mainly concerned about the privacy of their sensitive healthcare data, fearing potential breaches that could expose personal health information (PHI) to cyber threats. While some security features like encryption are appreciated, there is skepticism about the overall effectiveness of M-TIBA’s security protocols and whether its infrastructure can truly protect data from cyber-attacks in a cloud environment.

4.2.4 Cloud computing characteristics and perceived impact

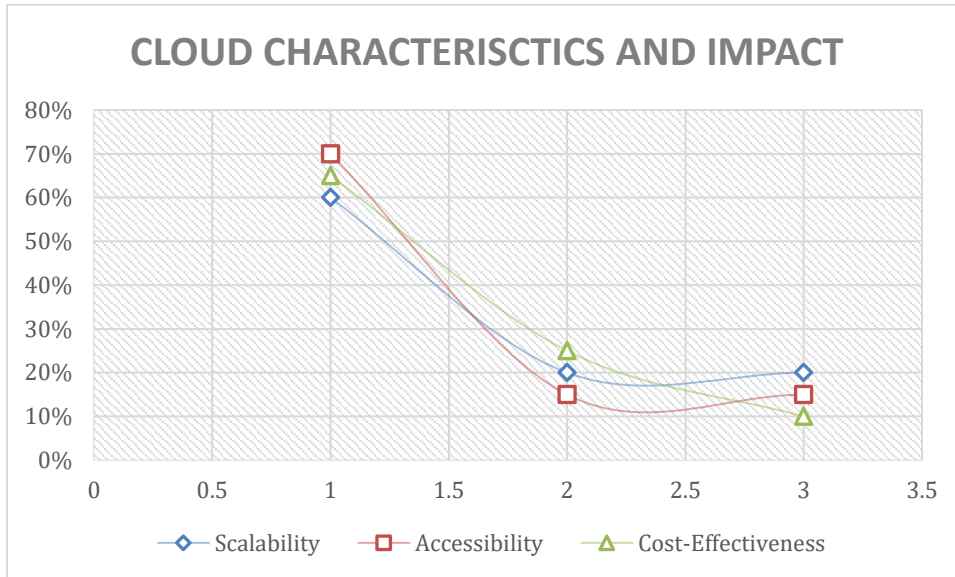


Figure 6 line chart showing relation between cloud characteristics and influence

The characteristics of cloud computing present both opportunities and challenges for data security within M-TIBA’s platform. While cloud computing enables efficient scaling of resources to meet demand, this flexibility can complicate security management, as rapid scaling may introduce vulnerabilities if not carefully monitored. Additionally, the shared infrastructure of cloud environments increases the risk of data leakage or cross-tenant breaches. Cost-effectiveness boosts the adoption of services like M-TIBA by making them more accessible and manageable. However, it can also pose risks, including reduced service quality, hidden costs, security vulnerabilities, or an unsustainable business model.

4.2.5 Cloud adoption and perceived security

For this, the Pearson Correlation Co-efficient were used, as it is the most apt formulas to test the relationship between the relationship of cloud adoption and perceived security, with the data presented.

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}}$$

Where:

- n is the number of data points.
- $\sum xy$ is the sum of the product of the paired scores.
- $\sum x$ is the sum of the x-scores.
- $\sum y$ is the sum of the y-scores.
- $\sum x^2$ is the sum of the squared x-scores.
- $\sum y^2$ is the sum of the squared y-scores.

This formula will give a value between -1 and 1, where:

- 1 indicates a perfect positive linear relationship,
- -1 indicates a perfect negative linear relationship,
- 0 indicates no linear relationship.

A positive correlation ($r = 0.65$) was observed between the usage of M-TIBA and perceived security levels among respondents, suggesting that higher adoption rates are associated with increased trust in M-TIBA's security.

4.4 Qualitative data analysis

Themes identified:

User awareness and education

Here, it was seen that higher digital literacy levels often correlate with increased trust and understanding of cloud computing benefits, and that some users reported limited understanding of data security and cloud as a whole, leading to hesitations in fully embracing M-TIBA's services.

Perceived security and trust

Generally, most respondents showed trust in the platform, while putting total confidence in its security measures. However, healthcare providers and some users expressed particular concern about the potential for data breaches, with a desire for transparency and more safeguards.

4.5 Implications of the present results

These findings underline the need for more policies that can support comprehensive digital initiatives that ultimately enhance users' understanding of cloud based healthcare platforms. Coupled with this, healthcare providers should implement routine sessions on secure usage practices for digital platforms to enhance data security and user confidence. Moreover, investment in advanced security technologies and consistent platform updates is critical to maintain user trust and strengthen data protection measures.

4.6 Significance of present results

The findings provide valuable insights into the relationship between user awareness, perceived security, and cloud infrastructure in the Kenyan healthcare sector. They underscore the importance of digital literacy and transparent security protocols in fostering trust and effective adoption of cloud-based healthcare services. These insights are beneficial for policymakers, healthcare providers, and developers working to build secure, user-friendly cloud systems. Addressing these elements can significantly improve the quality of healthcare and data security within Kenya, contributing to more resilient healthcare data management systems.

CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter concludes the study "An Assessment on Cloud Computing and Its Impact on Data Security in Healthcare: A Case Study of M-TIBA." The chapter also lists areas that require additional research that were found to be gaps in the study.

5.2 Summary of findings

With an emphasis on the M-TIBA platform, the study intended to assess how cloud computing may affect data security in the healthcare industry. The following summarizes the main conclusions in light of the study's goals:

User awareness and security effectiveness.

Findings indicated that 80% of respondents were active M-TIBA users, with a high degree of satisfaction (70%) in M-TIBA's cloud-based services. However, 45% of respondents cited data breaches as a primary security concern, highlighting a need for improved security awareness.

Security measures and user trust.

The survey revealed that 20% of respondents had experienced security issues with M-TIBA. Despite these challenges, 25% of users reported adopting M-TIBA due to trust in its security protocols. Overall, user trust was largely correlated with the perceived effectiveness of M-TIBA's security features, with 60% citing satisfaction with current measures.

Impact of cloud characteristics on data security.

Respondents appreciated the benefits of scalability (60%) and accessibility (70%) of cloud computing. However, concerns over data security remained, especially related to unauthorized access (30%).

Correlation between cloud adoption and perceived security

A positive correlation ($r = 0.65$) was found between cloud adoption and perceived security, suggesting that users are more likely to trust and adopt M-TIBA as their confidence in security increases.

5.3 Conclusions

User awareness

The data indicates that user awareness significantly affects the effectiveness of security in M-TIBA. However, heightened concerns over privacy breaches and data protection suggest a need for targeted awareness campaigns on data security practices.

Effectiveness of security measures

Although M-TIBA's security measures inspire trust, the fact that 20% of users reported issues indicates potential gaps in security implementation. Strengthening these measures would likely increase user trust further.

Cloud computing characteristics

Users perceive the cloud characteristics of M-TIBA, such as accessibility and scalability, as beneficial. However, the study reveals that these factors alone may not alleviate user concerns regarding data security, as evidenced by the ongoing concerns about privacy and unauthorized access.

5.4 Recommendations

Enhancing user awareness on security protocols

M-TIBA should consider implementing user-centered security awareness programs focusing on educating users about data protection and safe usage practices. This might include periodic information updates, pop-up alerts on security risks, or multimedia resources outlining best practices.

Strengthening security measures

It is recommended that M-TIBA review and fortify its security protocols, especially in areas vulnerable to data breaches. Further investment in encryption, real-time monitoring, and enhanced user authentication could mitigate these risks.

Improving user feedback mechanisms

Given the importance of user feedback, establishing an accessible feedback system could help M-TIBA promptly identify security concerns and areas of improvement.

Monitoring cloud computing benefits and risks

Continuous monitoring of the balance between cloud benefits and risks, with a focus on privacy, is advised. This should include regular security audits, assessment of accessibility, and real-time alerts on data breaches or unauthorized access attempts.

Further research

Future studies could focus on longitudinal analysis, examining the long-term relationship between security improvements in M-TIBA and user adoption rates, as well as exploring similar cloud-based healthcare systems for comparative analysis.

REFERENCES

- Alotaibi, M. B. (2016). Investigating the role of user awareness in information security compliance. *Journal of Information Security and Applications*, 31, 1-6.
- AlTwaijiry, A. (2020). The determinants of cloud computing adoption in healthcare. *ResearchBerg Review of Science and Technology*, 3(1), 9-20.
- Almeida, F., Santos, J. D., & Monteiro, J. A. (2020). The role of security awareness in cloud computing adoption: A case study in healthcare. *Procedia Computer Science*, 177, 409-414.
- Chen, D., Shi, W., & Li, Y. (2019). A survey on cloud computing security mechanisms and challenges. *Journal of Computer Research and Development*, 56(7), 1470-1483.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.
- DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research*, 3(1), 60-95.
- Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security*, 13(2), 113-170.
- Gachoka, D., Omwenga, E., & Moturi, C. (2018). Enhancing healthcare access through mobile health wallets: A case of M-TIBA in Kenya. *International Journal of Telemedicine and Applications*, 2018.
- Gupta, A., Yamaguchi, S., Sinha, R., & Singh, P. (2018). Cybersecurity in healthcare: A systematic review of modern threats and trends. *IEEE Access*, 6, 67204-67217.
- Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. *Information Systems*, 47, 98-115.
- Hashizume, K., Rosado, D. G., Fernandez-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), 1-13.
- Kaur, P., & Mustafa, R. (2020). Cyber threats in cloud computing for healthcare systems. *International Journal of Advanced Computer Science and Applications*, 11(5), 375-381.

- Mehrtak, M., Mohseni, M., Rashidi, A., & Masdari, M. (2021). Security challenges and solutions using healthcare cloud computing. *Journal of Medicine and Life*, 14(4), 448-456.
- Musembi, P. M. (2024). Africa's contributions to digital technology: A case of M-Pesa technology in Kenya. In *Contributions of Africa's Indigenous Knowledge to the Wave of Digital Technology: Decolonial Perspectives* (pp. 260-289). IGI Global.
- Nan, W. V. (2021). Digital infrastructure for development: The case of mobile money in Kenya. In *Proceedings of the 27th Americas Conference on Information Systems*.
- Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, 1(2), 1-7.
- Sandhu, A. K. (2021). Big data with cloud computing: Discussions and challenges. *Big Data Mining and Analytics*, 5(1), 32-40.
- Shah, V., & Konda, S. R. (2022). Cloud computing in healthcare: Opportunities, risks, and compliance. *Revista Española de Documentación Científica*, 16(3), 50-71.
- Sivan, R., & Zukarnain, Z. A. (2021). Security and privacy in cloud-based e-health system. *Symmetry*, 13(5), 742.
- Sunyaev, A., & Sunyaev, A. (2020). Cloud computing. In *Internet computing: Principles of distributed systems and emerging internet-based technologies* (pp. 195-236).
- Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583-592.

APPENDICES

6.1 Sample Research Instruments

6.1.1 Structured Questionnaire

Section 1: Demographic Information (Tick where appropriate)

1. Gender
 - Male
 - Female
2. Occupation
 - User/ General Public
 - Healthcare provider
 - Policymaker/IT Professional
3. Education Level
 - Primary School
 - Secondary School
 - Undergraduate
 - Postgraduate
 - None
4. Digital Literacy Level
 - Low
 - Moderate
 - High

Section 2: Usage and Satisfaction with M-TIBA

5. How frequently do you use the M-TIBA platform?
 - Daily
 - Weekly
 - Monthly
 - Occasionally
 - Never
6. How satisfied are you with the cloud-based services provided by M-TIBA

(Please explain your level of satisfaction, mentioning any specific features you find helpful or any improvements you would like to see.)

7. What influenced your decision to use M-TIBA as a cloud platform offering healthcare services?
- Convenience
 - Affordability
 - Security
 - Accessibility

Section 3: Security Concerns and Experiences

8. How would you describe your level of trust in the security measures implemented by M-TIBA?
- High
 - Moderate
 - Low
9. What are your main security concerns, if any, regarding the use of M-TIBA as a healthcare cloud platform?
- Data Privacy
 - Unauthorized Access
 - Data Breaches
 - Information Loss

Section 4: Adoption of M-TIBA Feedback

10. Do you believe that using cloud-based healthcare services like M-TIBA has improved your access to healthcare?

(Please elaborate on your answer.)

11. How do you think M-TIBA could improve its overall posture, accessibility, security, or otherwise?

(Provide specific suggestions if possible.)

12. What general feedback would you give about your experience with M-TIBA?

(Feel free to share any additional thoughts or recommendations.)

6.1.2 Interview Guide for IT Professionals and Policymakers

Introduction:

- Briefly introduce the purpose of the interview and the scope of the study.

Section A: General Information

1. Can you please introduce yourself and describe your role in relation to M-TIBA?

Section B: Security Measures and Challenges 2. What security measures are currently implemented within the M-TIBA platform? 3. How do these measures compare with international security standards such as ISO/IEC 27001 and HIPAA? 4. What challenges do you face in maintaining and updating these security measures?

Section C: User Awareness and Training 5. How important do you consider user awareness in the context of data security? 6. What initiatives have been taken to educate users about data security measures?

Section D: Future Directions 7. What additional measures do you think are necessary to enhance data security on the M-TIBA platform? 8. How do you see the role of emerging technologies (e.g., AI, blockchain) in improving data security?

Conclusion:

- Thank the interviewee for their time and insights.

6.1.3 Focus Group Discussion Guide

Introduction:

- Explain the purpose of the focus group and the importance of their input.

Section A: General Discussion

1. Can you share your experiences with using the M-TIBA platform in terms of data security?

Section B: Cloud Computing Awareness 2. How aware are you of the cloud computing infrastructure supporting M-TIBA? 3. What are your thoughts on the security of cloud computing in healthcare?

Section C: Security Measures 4. What security features of M-TIBA do you find most effective? 5. Are there any specific security concerns you have encountered?

Section D: User Training and Engagement 6. How often do you receive training or updates on data security from M-TIBA? 7. What improvements would you suggest for user awareness programs?

Section E: Future Improvements 8. What additional security measures or features would you like to see in M-TIBA? 9. How do you think emerging technologies can enhance data security in healthcare?

Conclusion:

- Summarize key points discussed and thank participants for their contributions.