AN ASSESSMENT OF KEY SUCCESS FACTORS FOR BIOMETRIC AUTHENTICATION IN KENYAN BANKING SECTOR: A CASE STUDY OF KCB IN THIKA

SHALLOM OKERO NYAMWEYA

ICT-G-4-1249-20

A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF COMPUTING AND INFORMATICS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE OF GRETSA UNIVERSITY

MARCH 2023

DECLARATION

This project is my original work and has not been presented for a degree in any other university.

Signature: _____

Date: 11/12/23

Shallom Okero Nyamweya

ICT-G-4-1249-20

This ~~proposa~~Research has been submitted with my approval as a university supe

Signature: _____

Date: 11-12-2023

Mr. Dennis Wapukha

School of computing and informatics

Gretsa university

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATION AND ACRONYMS

KCB - Kenya Commercial Bank

ICT – Information and Communication Technology

SPSS – Statistical Package for Social Sciences

ID – Identification

PIN – Personal Identification Number

ATM – Automated Teller Machine

FAR- False Accept Rate

FRR- False Reject Rate

RBV-Resource-Based View

TAM- Technology Acceptance Model

ABSTRACT

Biometric authentication has emerged as a promising technology to secure banking operations, reduce fraud, and enhance customer experience. However, the implementation of biometric authentication in the banking sector is not without challenges. This study aims to assess the key success factors for biometric authentication in the Kenyan banking sector in KCB Thika by exploring the factors that influence its adoption, implementation, and effectiveness. The research employs a quantitative research approach, consisting of a survey of banking customer and employees. The study identifies several key success factors for biometric authentication in the banking sector, including user acceptance, technical feasibility, regulatory compliance, cost-effectiveness, system reliability, and scalability. The findings reveal that user acceptance is a critical factor for the successful implementation of biometric authentication in the banking sector. Customers' perceived ease of use, perceived usefulness, and trust in the technology influence their acceptance of biometric authentication. Technical feasibility, including accuracy, speed, and compatibility with existing systems, is also crucial for successful implementation. Moreover, regulatory compliance is a critical factor, given the sensitive nature of banking operations and the potential risks associated with biometric data. The study finds that cost-effectiveness and system reliability are key factors that influence the adoption and sustainability of biometric authentication in the banking sector. Scalability is also an essential factor to consider, as biometric authentication needs to accommodate a growing customer base and increasing transaction volumes. Overall, the study concludes that biometric authentication has the potential to enhance security and improve customer experience in the banking sector. However, its success depends on careful consideration of the factors that influence its adoption, implementation, and effectiveness.

CHAPTER ONE: INTRODUCTION

1.0 INTRODUCTION

With the increasing prevalence of cyber threats and identity theft, the need for secure authentication methods has become more pressing in the banking sector. Biometric authentication has emerged as a promising solution for enhancing security and customer experience in the banking sector. Biometric authentication uses unique biological characteristics such as fingerprints, facial recognition, and voice recognition to verify the identity of the user as per Islam et al (2020). Biometric authentication offers a higher level of security than traditional authentication methods, such as passwords and PINs, as biometric traits are difficult to replicate or falsify as per Liao & Luo (2018). However, despite the potential benefits of biometric authentication, there are still challenges to its adoption and implementation in the banking sector. Therefore, this research aims to assess the key success factors for biometric authentication in the banking sector

1.1 BACKGROUND TO THE STUDY

The use of technology can automate the process of subject identification thereby that would require a more secure form of identification. Biometric identification as per Jain et al (2005) is the process by which a person can be identified by his characteristics.

The banking sector has been one of the early adopters of biometric authentication technologies, with many banks around the world implementing biometric authentication for various transactions, such as opening accounts, making payments, and accessing mobile banking apps as per Dehghantanha et al (2020). Biometric authentication offers several benefits to the banking sector, including enhanced security, improved customer experience, and reduced costs. Biometric authentication can help prevent identity theft, fraud, and cyber-attacks, as biometric traits are unique to each individual and difficult to replicate or falsify as per Kaur & Singh (2021). Biometric authentication can also provide a seamless and convenient customer experience, as users do not need to remember passwords or PINs and can access their accounts using their biometric traits as per Kanoun et al (2020). Biometric authentication can also reduce costs for banks, as it eliminates the need for physical tokens and reduces the risk of password resets and account lockouts as per Boukottaya et al (2020).

However, despite the potential benefits of biometric authentication, there are still challenges to its adoption and implementation in the banking sector. One of the main challenges is the lack of standardization and interoperability of biometric authentication technologies. Different biometric authentication technologies use different algorithms, standards, and protocols, which can lead to compatibility issues and interoperability problems as per Sadiq et al (2020). Another challenge is the lack of trust and confidence in biometric authentication among customers. Many customers are still skeptical about the security and privacy of their biometric data and are concerned about the potential misuse of their biometric traits as per Olawale et al (2021). Moreover, there are also regulatory and legal issues related to the collection, storage, and use of biometric data, which can vary across different jurisdictions and countries as per Zhang et al (2019).

Biometric system can be used in many instances such as; Immigration cards holding both passport number and measures of user's hand as per Wing (2000), Fingerprint taken as a legal requirement for a driver license but not stored anywhere in the license as per Slagle (1999), automatic facial recognition system searching for known card cheats in a casino as per Walter (2000), season tickets to an amusement park linked to the shape of purchaser's finger as per Levin (2001), Home incarceration programs supervised by automatic voice recognition systems as per Markowitz (2016) and confidential delivery of health care through iris recognition as per Perkins (2021)

This technology of biometrics has now started to being implemented in financial institution and banks sector. More and more banks worldwide are opting the use of biometrics to verify consumers in order to access their services. This trend is not limited to banks, other financial outfits are also taking up biometric authentication to identify customers and safeguard resources. Banks have been forced to overhaul their identity procedures due to rising instances of financial fraud, identity theft, and online threats; the solution is the use biometrics in banking and financial services.

Biometrics offers friction less access to banking services. banks in Africa actually a few of them offers biometrics services to their customers especially the most developed ones like South Africa. Most of customers in these countries you find that they are much satisfied that their accounts are secure because there is use of biometrics.

Now narrowing down to our country Kenya, same case as banks in Africa a few of them have biometrics. Considering Kenya Commercial Bank (KCB) in Thika branch where the research

was be based on, customer authentication in computer system is being conducted based on some security measures like the use of paper based identity documents or the government issued photo ID cards, use of passwords, secret codes, and also the use of PIN codes, thus due to advanced technology having deposited money and valuables of people, banks and financial institutes are always on the hit-list of fraudsters and cyber criminals daily.

The approach banks use to identify and authenticate consumers using ID cards has grown riskier. Fraudsters can forge information: names, addresses and unique ID number printed on a card along with the picture, especially in a world full of high-resolution digital cameras and printing machines. With biometrics thus it is nearly impossible to use someone else's identity. For example, a fingerprint does not usually change except for accident or illness but a signature, a behavioral characteristic as per John Chirillo & Scott Blaul (2003), can change as a person ages.

1.2 PROBLEM STATEMENT

With the help of modern technology, criminals and unauthorized individuals can access the personal information of illiterate people physically or online, using that information to make fake passports and national identification documents that allowed them to bypass the security team and gain access to bank accounts.

Since handwritten signatures are unreliable owing to fabrication in a case of simple signatures, there have been numerous examples of theft or fraud in Kenya's various banks, usually involving persons who use them as authentication. Additionally, using passwords and security codes isn't all that common or all that secure because people can forget them, input them incorrectly, or even give their passwords to other unauthorized persons.

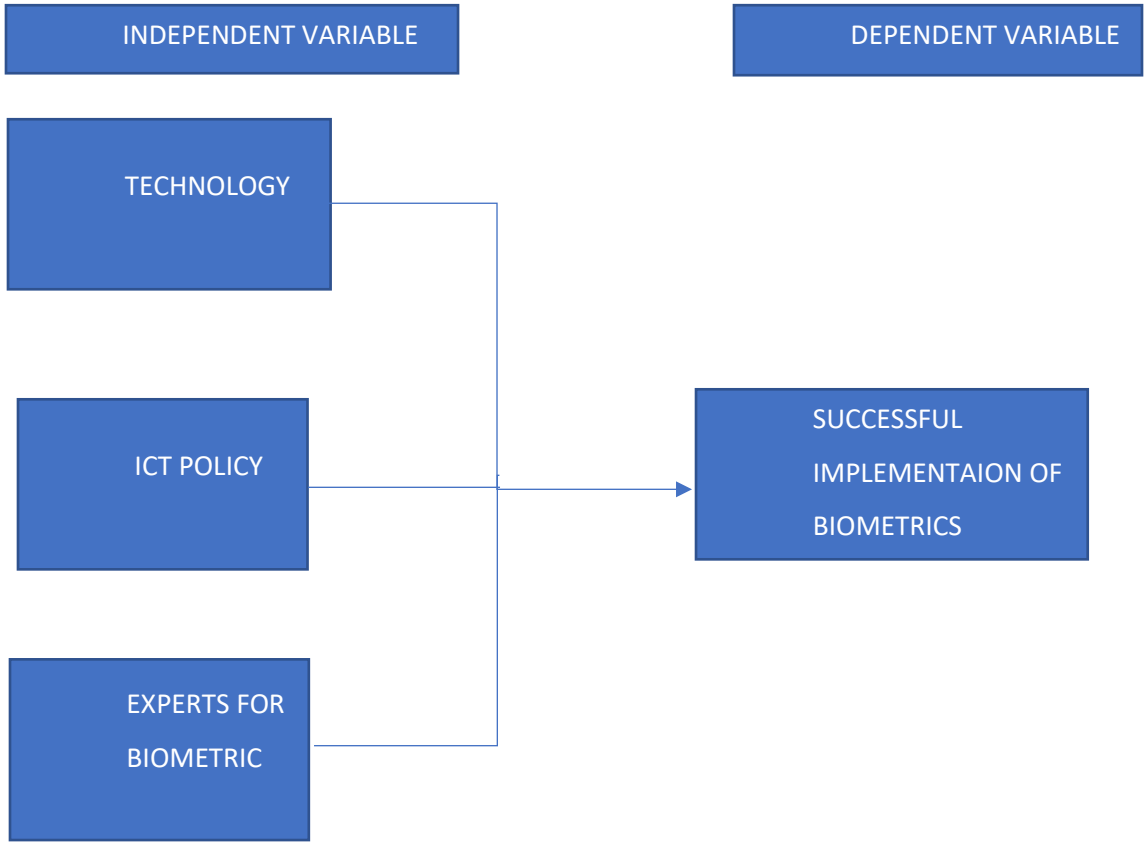
In order to combat the challenges of online and offline fraudulence, banks must find a more secure way to assist their customers so that they do not experience any type of fraud or theft. As a result, biometric authentication such as fingerprint recognition should be deployed and implemented. These methods are more dependable, quick, and secure. Therefore, the study aims to incorporate the crucial success elements in banking institutions.

1.3 PURPOSE OF THE STUDY

The study seeks to investigate the key success factors for biometric implementation in banking sector.

1.4 CONCEPTUAL FRAMEWORK

The conceptual framework below shows the independent variables: technology, ICT policy and experts for biometrics. The dependent variable is the successful implementation of biometrics. It illustrates how technology, ICT policy and experts for biometrics affects successful implementation of biometrics.



1.5 RESEARCH QUESTION

The following questions were addressed from the research:

i. How does technology affect successful implementation of biometrics at KCB in Thika?
ii. In what way does ICT policies affect successful implementation of biometrics at KCB in Thika?
iii. How does availability of experts for biometric affects implementation of biometrics at KCB in Thika?

1.6 OBJECTIVES OF THE STUDY

1.6.1 GENERAL OBJECTIVE

The general objective is the assessment of key success factors for biometric implementation in banking sector.

1.6.2 SPECIFIC OBJECTIVE

i. To assess how ICT policy affects successful implementation of biometrics at KCB in Thika.
ii. To investigate how technology affects successful implementation of biometrics at KCB in Thika.
iii. To explore experts available for biometrics and how they affect its implementation at KCB in Thika.

1.7 HYPOTHESIS

H_0 : The IT policy affects successful implementation of biometrics at KCB in Thika.

H_1: The technology affects successful implementation of biometrics at KCB in Thika.

H_2: The experts for biometrics affects successful implementation of biometrics at KCB in Thika.

1.8 SIGNIFICANCE OF THE STUDY

This part of research contains the benefits and the beneficiaries of the research and provided new perspectives in approaching identity security issues of customers:

1.8.1 BENEFICIARIES

i. **BANK CUSTOMERS**

Customers of the bank are the most ones who will benefit from biometric implementation. This is because biometrics especially fingerprint has distinctive traits that are specific to an individual, such as ridges, valleys, and minutiae points, making it impossible to duplicate a fingerprint in order to access their personal accounts and information.

ii. **BANK MEMBERS EASE OF OPERATION**

This study will benefit the bank members also in that there will be no much of paperwork. Like the cases of using signatures takes time. PIN authentication in banks might take few seconds or more if you use the wrong one whereas fingerprint recognition is a seamless, near-instant process. This will save a lot of time for both the customers and business involved. Thus, the bank will have more time to serve other customers.

iii. THE BANK

This study will also benefit the bank itself. People in the community will obviously want their personal information and accounts to be secure. They also don't want to be exposed to identity theft so they will opt to choose a bank with biometrics. Thus, KCB in Thika gained more customer through biometric implementation.

iv. FUTURE RESEARCHERS

This study covers information involving biometric authentication as an approach to reduce identity theft levels. Thus, the result of this study can be used for future discussions of capabilities of identity theft in other security levels.

1.8.2 BENEFITS

Biometric authentication has emerged as a powerful tool in enhancing the security of financial transactions, and its implementation in the banking sector has been gaining momentum in recent years. Biometric authentication systems rely on physical traits of individuals, such as fingerprints, facial recognition, and iris scans, to verify their identities. These systems are more secure than traditional password-based systems and have the potential to significantly reduce instances of fraud, identity theft, and other cybercrimes. The significance of this study lies in its potential to provide insights into the implementation of biometric authentication in the banking sector. The study assessed the key factors that influence the successful implementation of biometric authentication systems, including technological, financial, and regulatory factors. By identifying these factors, the study provided useful recommendations for banks looking to implement biometric authentication systems in their operations. The findings of the study can have a positive impact on the banking industry by improving the security of banking transactions, which in turn can increase customer trust and confidence. By implementing biometric authentication systems, banks can provide a more secure environment for customers to carry out financial transactions. This can lead to increased customer satisfaction, loyalty, and retention, which are critical to the success of any business.

Furthermore, the study can contribute to the existing body of knowledge on biometric authentication systems, particularly in the banking sector. The study was of interest to banking professionals, policy-makers, and academic researchers seeking to understand the impact of biometric authentication systems on the banking industry. The results of the study

can serve as a basis for further research in this area and can inform future policy decisions related to the implementation of biometric authentication systems in the banking sector.

1.9 SCOPE OF THE STUDY

The scope of this study is to assess the implementation of biometric authentication systems in the Kenyan banking sector, with a specific focus on Kenya Commercial Bank (KCB) Thika branch. The surveys were be administered to customers and employees of KCB Thika to gather information on their attitudes towards biometric authentication systems, the level of awareness about these systems, and the perceived benefits and drawbacks of using these systems. The surveys was conducted with senior management and IT personnel of KCB Thika to gather information on the technological, financial, and regulatory factors that influence the successful implementation of biometric authentication systems in the banking sector.

1.10 LIMITATION OF THE STUDY

The study had several limitations, including the potential for respondent bias, particularly among customers who were not willing to provide accurate responses due to concerns about privacy and data security. Additionally, the study focused on a single branch of KCB, which may not be representative of the entire Kenyan banking sector. Some respondents did not turn up to be interviewed and considering the sample size so the retrieved information was not that handy. The available biometric devices for the study were less as they are expensive to acquire. However, the study provided valuable insights into the implementation of biometric authentication systems in the Kenyan banking sector and can serve as a basis for further research in this area.

CHAPTER TWO: LITERATURE REVIEW

2.1 INTRODUCTION

Biometrics recognition methods and tools have become trendy for development of useful and widely accepted applications such as security issues, surveillance, forensic investigations, fraudulent transactions, identity access management and access control as per Shaveta & Munish (2020). The banking sector is one of the most critical sectors in any economy. The sector is responsible for the management of financial transactions, which is essential for the smooth functioning of the economy. However, the sector is also vulnerable to fraud, which can have significant implications for the economy. The implementation of biometric authentication systems in the banking sector has gained attention as a potential solution to address the security and privacy concerns associated with traditional password-based systems. In this literature review, we examined the role of information and communication technology (ICT) policies, Technology and Experts in the implementation of biometric authentication systems in the banking sector.

2.2 REVIEW OF THE LITERATURE

In this chapter the researcher brings together and examines the dominant and recurring ideas about home represented in the relevant theoretical and empirical literature as per Shelley (2014). Reviews of published scientific literature are a valuable resource that can underline best practices in biometrics and clarify clinical controversies as per Supriya (2018). Throughout the literature review the researcher will assess how ICT policy affects successful implementation of biometrics, investigate on how the advancement in technology affects successful implementation of biometrics and lastly on how availability of experts affects biometric system implementation.

2.3 TECHNOLOGY AND BIOMETRIC IMPLEMENTATION

The implementation of biometric authentication systems heavily relies on the advancement of technology. Several studies have explored the impact of technology on biometric implementation. For example, Akram et al. (2020) investigated the effect of technology on the adoption of biometric authentication in online banking. The study found that the technological features, such as accuracy, speed, and ease of use, significantly influence the adoption of biometric authentication in online banking.

Moreover, biometric authentication systems heavily rely on software and hardware technologies for their implementation. The software technology used in biometric

authentication systems includes image processing algorithms, machine learning, and artificial intelligence. The hardware technology includes cameras, sensors, and other equipment required for capturing biometric data. The effectiveness of biometric authentication systems largely depends on the quality and reliability of these technologies. A study conducted by Bhatti et al. (2020) investigated the impact of hardware technology on the accuracy of facial recognition-based authentication systems. The study found that the accuracy of the facial recognition system is highly dependent on the quality of the camera used for capturing facial images.

In addition to the hardware and software technologies, the implementation of biometric authentication systems requires the integration of multiple systems and technologies. These include database systems, network infrastructure, and security systems. The integration of these technologies is critical to the success of biometric authentication systems. A study by Azhar et al. (2019) investigated the impact of technology integration on the implementation of biometric authentication systems in mobile banking. The study found that effective technology integration significantly improves the success rate of biometric authentication systems in mobile banking.

This chapter analyses technological innovation and factors to see how far an organization is with current technology and also relate to theft prevention with regard to minor and major burglary as per Kim, Evelien, Hans & Wim (2018). Moreover, it discusses how people view technology as a security measure and their acceptance, expectations, and satisfaction with it. (Kim Van,2018). As per Bhattacharyya et al (2009) information security needs to be given a proper attention considering advancement in technology. Thus, as per Ateba et al (2013) for banks to remain relevant and successful in today's competitive world, they must provide innovative and best secured services to their customers.

With advancement in technology banks and other financial institution have faced many cases of fraud. Like a case when a customer conducts a transaction online, fraudsters initiate attacks into their system so as to acquire information for theft activities. Stopping large amounts of fraudulent transactions and identity theft is another difficulty facing banks. This happens because most of these banks are using outdated security measures such as use of passwords, PINs, signatures and government issued identity cards. Therefore, using digital banking solutions appears to be a perfect mechanism to curb these threats as per Hossein & Mohammadi (2012). Using PIN code to verify someone's identity is not regarded as a best

mechanism against security gaps. Using biometrics, the operator's data and information is securely kept in an encrypted container or sandbox as per Jonson (2019).

As per Chowdhury et al. (2021) impact of machine learning algorithms on the performance of biometric authentication systems. The study found that the use of machine learning algorithms significantly improves the accuracy and efficiency of biometric authentication systems.

Another study by Siddiqui et al. (2020) explored the impact of cloud computing on the implementation of biometric authentication systems in the banking sector. The study found that the use of cloud computing can significantly reduce the implementation costs and enhance the scalability and reliability of biometric authentication systems.

The advancement of technology has also led to the development of new biometric authentication methods such as behavioral biometrics, which uses human behavior patterns such as keystroke dynamics and mouse movements to authenticate users. A study by Wu et al. (2020) investigated the impact of behavioral biometrics on the security of online transactions. The study found that the use of behavioral biometrics can significantly enhance the security of online transactions and reduce the risks of fraud and identity theft.

2.4 ICT POLICY AND BIOMETRIC IMPLEMENTATION

ICT policies provide a framework for the implementation of technology solutions and ensure the protection of user privacy and data security. In the context of biometric authentication systems in the banking sector, ICT policies play a critical role in ensuring that the systems are implemented in compliance with data protection laws and standards.

The implementation of biometric authentication systems in the banking sector requires strict adherence to data protection laws and standards. For example, the European Union's General Data Protection Regulation (GDPR) outlines strict requirements for the collection, processing, and storage of biometric data. The regulation requires that biometric data is processed only for a specific purpose, and individuals must provide explicit consent for their data to be collected and used as per European Union (2018).

ICT policies also provide guidelines on the use of biometric authentication systems in the banking sector. For example, the policies outline the circumstances under which biometric authentication systems can be used, the types of biometric data that can be collected, and how the data should be protected. Moreover, biometric recognition systems are incredibly

complex and also biometric recognition is an inherently probabilistic endeavor as per National Research Council (2015). In spite of all these cases biometrics has provided a way to identify fraudsters, provide better control of access to physical facilities and financial accounts and increase the efficiency of access to services and their utilization as per National Research Council (2015).

Research has also shown that there are cultural and social factors that influence the adoption of biometric authentication systems. For example, some individuals may have concerns about the use of their biometric data, which can lead to a lack of trust in these systems. These concerns may be more prevalent in certain cultures or communities as per Hwang & Kim (2015).

In banks the main objective is to prevent fraudulent transaction as per TV Bakunova (2019) and identity theft thus implementing biometrics such as fingerprint is the crucial solution. With the average banking customer handling a wide range of financial transactions online through desktop and mobile services, the need for easy and safe access to their banking data is becoming a top priority for banking service providers wanting to differentiate themselves from their challengers as per Richman Charles A gidi (2018).

Considering the use policy, this impacts on the customers and also the members. The customers will have to be taught on how to use biometrics. Biometrics is the science of measuring and analyzing person's characteristics. Biometrics is still in the early stages in our country but already a number of technological applications of its principles have been developed and adopted by firms in order to increase security and efficiency of adopters' operation as per Richman Charles Agidi (2018).

Looking at the benefits of biometrics, the ICT policy at KCB in Thika should recommend its implementation. Biometrics includes fingerprints, face recognition, hand geometry, iris observation and signature acknowledgement as per Clodfelter (2010). The biometric recognition system is not going to displace other security measures but it will aid in improving the security aspects of the application where operators' cooperation can be gathered as per Shaveta & Munish (2020) The most appropriate biometric to implement in KCB is the fingerprint as it is cheap and less complex compared to others like voice recognition where someone's voice can change overtime.

2.5 EXPERTS AND BIOMETRICS IMPLEMENTATION

The implementation of biometric authentication systems in the banking sector has been gaining popularity due to the need for enhanced security and customer convenience. The success of these systems is largely dependent on the expertise of the individuals responsible for their implementation

Experts play a crucial role in the successful implementation of biometric authentication systems in the banking sector. These experts have the knowledge and skills required to design, implement, and maintain these systems. They also possess a deep understanding of the regulatory and legal frameworks governing the use of biometric data in the banking sector.

Research has identified several factors that contribute to the success of biometric implementation in the banking sector. One of the key factors is the expertise of the individuals responsible for the implementation. Experts with a deep understanding of the technology, its limitations, and its potential applications can design and implement systems that are reliable, secure, and effective as per Basri & Wahab (2019).

Expertise also plays a critical role in addressing technical challenges associated with the implementation of biometric authentication systems. Experts can identify and mitigate technical challenges such as data quality issues, hardware and software compatibility issues, and system scalability problems as per Li et al (2015).

In any firm experts in specific field is very crucial. As per Helen & Annette (2022) creativity has been found out that it is the crucial attribute for employment in 21st century. A number of people and approaches position expertise as individual knowledge. However, institutions are leveraging expertise cross-departmentally to facilitate effective institutional decision making, policy and practice as per Zachery (2021). When ‘environmentally friendly’ items are added to a group of conventional items, people conclude that the whole group will have a decrement in environmental impact but you will find that the impact increases as per Mattias, Alan, John, Marsh, Patrick (2018).

Sometimes also the experts at particular field can be available but often lack the domain knowledge needed to validate context on specific parts of the software as per as per Tim (2020). Thus, in order for successful biometric implementation at KCB in Thika experts in different fields of biometrics and also with domain knowledge for creativity. Thus, after identifying the experts for biometrics its implementation should be conducted. For successful

implementation of the biometrics, deep artificial neural networks are in high demand as per Shaveta & Munish (2020)

2.6 THEORITICAL FRAMEWORK

Biometric authentication systems are becoming increasingly popular in the banking sector as a means of enhancing security and customer experience. However, the success of biometric implementation projects depends on several key factors, including customer acceptance, ease of use, and organizational capabilities. This literature review explored the theoretical framework for investigating the key success factors of biometric implementation in the banking sector.

2.6.1 TECHNOLOGY ACCEPTANCE MODEL

The Technology Acceptance Model (TAM) is a widely used theoretical framework for investigating the factors that influence the adoption and use of new technologies. According to TAM, the acceptance and use of a technology depend on two main factors: perceived usefulness and perceived ease of use as per Davis. (1989). In the context of biometric implementation in the banking sector, the TAM can be used to investigate the factors that influence customer acceptance and use of biometric authentication systems.

Several studies have used the TAM to investigate the acceptance and use of biometric authentication systems in the banking sector. For example, Karkar et al. (2018) conducted a study to investigate the factors that influence customer acceptance of biometric authentication systems in online banking. The study found that perceived usefulness and perceived ease of use significantly influenced customer acceptance of biometric authentication systems. Similarly, Al-Fawareh et al. (2019) investigated the factors that influence customer acceptance of biometric authentication systems in mobile banking. The study found that perceived usefulness and perceived ease of use were significant predictors of customer acceptance.

2.6.2 RESOURCE-BASED VIEW

The Resource-Based View (RBV) is a theoretical framework that explains how organizations can achieve competitive advantage by leveraging their unique resources and capabilities as per Barney. (1991). In the context of biometric implementation in the banking sector, the RBV can be used to investigate the factors that contribute to the success of biometric implementation projects.

Several studies have used the RBV to investigate the factors that contribute to the success of biometric implementation projects in the banking sector. For example, Yussof et al. (2016) conducted a case study to investigate the factors that contributed to the success of biometric implementation in a Malaysian bank. The study found that the bank's IT infrastructure, skilled personnel, and strategic partnerships were critical resources that contributed to the success of the implementation project. Similarly, Bhuyan and Hazarika (2018) conducted a study to investigate the factors that influence the adoption of biometric authentication systems in Indian banks. The study found that the availability of skilled personnel, IT infrastructure, and organizational support were significant predictors of adoption.

2.7 SUMMARY OF IDENTIFIED GAPS IN THE REVIEWED LITERATURE

After reviewing the literature on the key success factors of biometric implementation in the banking sector, several gaps were identified. The first gap is the limited research on the actual implementation process of biometric authentication systems in the banking sector. Most studies focused on investigating the factors that influence customer acceptance and use of biometric authentication systems rather than the actual implementation process.

The second gap is the limited research on the impact of biometric authentication systems on organizational performance. While several studies investigated the factors that contribute to the success of biometric implementation projects, few studies investigated the actual impact of biometric authentication systems on organizational performance.

The third gap is the limited research on the ethical and legal implications of biometric authentication systems in the banking sector. While biometric authentication systems have the potential to enhance security and customer experience, they also raise ethical and legal concerns, such as privacy and data protection

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 INTRODUCTION

This section presents the overview of the methodology which was employed during the study. In addition to this, the areas of the study and the arguments which support the choice of the area was explained. This chapter covered the research design, study area, target population, sampling techniques & size, data analysis and data collection methods that were used during data collection are provided.

3.2 RESEARCH DESIGN

Research design is a conceptual structure within which the research is conducted and it consists of the collection, measurement and analysis of data which is relevant to the research. It is plan parading the approach and strategy of investigation selected to retrieving valid and first-hand information that achieved the research objectives and research questions. This design focused more on what of the research subject rather than the why of the subject. This research used quantitative research approach, consisting of customer and employees' surveys. The customer surveys were conducted with a sample of bank customers to assess their attitudes towards biometric authentication, their level of trust and confidence in biometric technologies, and their willingness to adopt and use biometric authentication for various banking transactions. The employees' surveys were conducted to assess their knowledge on how to manage biometric devices.

3.3 STUDY AREA

The study was carried out in Kiambu county, Thika town. The research population consisted of the bank members in KCB and the customers who live around Thika. This decision was made since Thika Town is a metropolitan area where the necessary banks and pertinent institutions are located. Still the town has large number of people that are much into technology thus there is a possibility of retrieving all needed and relevant data from these research population. The target audience were requested to participate in the survey by responding to the provided questionnaires.

3.4 TARGET POPULATION

As per Saunders et al. (2019), Population is the group of goods or objects that the researcher is interested in, from which data is acquired to address a management issue. It covers all cases of individuals or things that fit a certain specification. In order to assess key success factors for biometric implementation at KCB in Thika, the target population for the study was 3000

respondents, which included customers of the bank, the system engineers, telecommunication engineers, business system analysts, other employees, card fraud experts and biometric authentication system experts located in Thika town. As per Creswell, Romm and Ngulube (2014) Face-to-face interviews take a lot of time. Thus, in qualitative research, 6 to 12 individuals are sufficient for in-person interviews, while 6 to 20 participants are appropriate for focus groups. The individuals chosen for this study were technically knowledgeable about how financial technologies and telecommunications infrastructure operate. Consequently, the chosen subjects held the information needed to address the issue.

3.5 SAMPLING TECHNIQUE

The target population consisted of huge number of respondents therefore getting all of them to participate in this study is not possible as per Fisher et al (2010), as a result information must be gained through study of some samples of it. Convenience random sampling was used on customers who comes often to the bank to access their bank accounts. To choose bank personnel, particularly those in the ICT department and those who manage the information security system, random purposive sampling was employed. However, each applicant had an equal chance of getting chosen. In order to meet the objective of the study the researcher made judgement through observation, concentrating on outlook appearance of potential and willing respondents.

3.6 SAMPLE SIZE

The sample size that used in this study was 352 respondents located in Thika town from the target population. As per Mugenda A & O, Mugenda (2008)

$$n = \frac{N}{1 + N(e)^2}$$

Whereby;

N	population
n	Sample size
1	constant
e	Degree of freedom

Table 1: Sample size formula

$$n = \frac{3000}{1+3000(0.05*0.05)}$$

n= 352 respondents

NO	CATEGORY OF RESPONDENTS	NO OF RESPONDENTS
1	Bank customers	285
2	System engineers	3
3	Telecommunication engineers	4
4	Business system analyst	5
5	Card fraud experts	5
6	Biometric authentication system experts	5
7	Other employees	45

Table 2: catergory of respondents

The bank customer represented about 80% of the respondents because they are the most ones that are affected by fraudsters through identity theft and fraudulent transactions. The bank employees were about 15% of respondents because the group constitutes of leadership of the organization. Lastly the biometric experts were only 5% because they are not available easily and they contribute to success factors of biometric implementation.

3.7 MEASUREMENT OF VARIABLES

VARIABLE	INDICATORS	MEASUREMENT SCALE	QUESTION NUMBER
technology	• Advancement in technology • Risk of the technology	Nominal scale	1
ICT policy	• software usage policy • cost implication of adopting the technology	ordinal scale	2
Experts for biometrics	• lack of experts	interval scale	3
Successful implementation of biometrics	• reduced cases of fraudulent transaction and identity theft	ordinal scale	4

Table 3: Measearement of variables

3.8 RESEARCH INSTRUMENTS

Research instruments are critical tools that help researchers collect data and information necessary to achieve their research objectives. Therefore, one research instrument was used in carrying out the study (surveys)

Surveys: Surveys are one of the most common research instruments used in investigating the key success factors of biometric implementation in the banking sector. Surveys were used to collect data on customer perceptions and experiences with biometric authentication systems in the banking sector. The survey questions can be designed to elicit responses on the ease of use, security, and overall satisfaction with biometric authentication.

3.9 VALIDITY OF MEASUREMENTS

The validity of measurements used in the implementation of biometric authentication in the banking sector is of critical importance in ensuring the accuracy and effectiveness of such systems. Biometric authentication systems rely on the measurement and comparison of unique physical or behavioral characteristics of an individual, such as fingerprints or facial recognition, to identify and authenticate them. Therefore, it is essential to assess the validity of the measurements used to ensure that they accurately measure what they are intended to measure.

Construct validity is of particular importance in the context of implementing biometric authentication systems in the banking sector. Construct validity refers to the degree to which a measurement accurately represents the underlying construct that it is intended to measure. In the case of biometric authentication systems, the underlying construct is the individual's unique physical or behavioral characteristics that are being measured to identify and authenticate them.

Studies have been conducted to examine the construct validity of biometric measurements used in the banking sector. A study conducted by Al-Sherbaz et al. (2018) found that biometric measurements, specifically fingerprint and facial recognition, have high construct validity in identifying and authenticating bank customers. The study concluded that biometric authentication systems using these measurements are reliable and accurate, providing an effective means of securing customer data and financial transactions.

Another study conducted by Kumar and Kumar (2018) also examined the construct validity of biometric measurements in the banking sector. The study found that biometric measurements, specifically iris recognition, have high construct validity in identifying and authenticating bank customers. The study concluded that biometric authentication systems using iris recognition provide a secure and reliable means of authentication in the banking sector

3.10 REALIBILITY OF MEASUREMENTS

Reliability is the degree to which research instruments yields correct results or data after repeated trials. It is concerned with consistency of responses with which repeated measures produce the same results across time and across observers as per Sekaran & Bogie (2010) three criteria are used in measuring reliability; test-retest reliability and the alternatives ones form and internal consistency reliability. A 97% confidence interval was set during planning stage in order to achieve acceptance level of reliability. An experiment was conducted in order to evaluate the instrument's financial performance. Using a test-retest methodology, the questions were asked to the participants in the same spot. No matter the initial research tools, the same subjects were given an online survey two weeks later, and the results were compared.

3.11 DATA COLLECTON TECHNIQUES

The researcher collected data by administering questionnaires which is a technique of data in which each person is asked to respond to same set of questions in an order. Another technique

is interviews which involves face to face conversation with the respondents where the researcher seeks simple well understood answers.

Considering the state of the study, questionnaires which includes open-ended were used for both the bank customers and bank employees because their sample size is too large for direct interaction. This helped for faster collection of data and get an in-depth understanding on the challenges they are facing from fraudsters.

The interviews are more adjustable, versatile, and may readily help the research dig deeper into the goal of the study. The data collection techniques were implemented at KCB in Thika using surveys with bank managers and biometric experts.

3.12 DATA ANALYSIS

Data that was collected from different sources was processed and analyzed for further discussion. Data analysis was conducted using both qualitative and quantitative methods. The quantitative data from the bank employees and customer surveys was analyzed using descriptive statistics and regression analysis to examine the relationships between different variables, such as trust, attitudes, and willingness to adopt biometric authentication.

Appropriate computer software was used to analyze the data. Quantitative data collected using open-ended questions were analyzed using statistical methods. Both excel and statistical package for social science (SPSS) computer was used to analyze descriptive statistics to obtain percentages, means and frequencies to see the effectiveness of implementation of biometric systems. Qualitative data collected was arranged into groups and categories. It was possible to spot and examine patterns in the data. Regarding to the findings from the questionnaire and data entry, the data was kept in the format which yields the best SPSS outputs.

3.13 LOGISTICAL AND ETHICAL CONSIDERATION

Research ethics are the codes of behavior adopted by a group suggesting what member of a group thought to do under a given circumstances. The researcher ensured confidentiality of the information from the respondents by respecting their rights, race and conditions. The researcher ensured that the study was used for academic purpose and not any other purposes. Logical consideration refers to the rule that no logically valid. Conclusion can contain what is not given in the premises. Participation in this research work was voluntary and participants were allowed to withdraw upon finishing the questionnaires

CHAPTER FOUR: DATA PRESENTATION, INTERPRETATION AND DISCUSSION

4.1: INTRODUCTION

This chapter is concerned with data representation of the findings obtained throughout the study. This finding involved gathering and compiling of data that was collected using questionnaires presented to respondents. Considering the research questions in chapter one, this study looked into how end users felt about the viability of using biometric authentication technologies as preventative measures to reduce card fraud, forgery and fraudulent transactions.

4.2 DEMOGRAPHIC INFORMATION

This coverage entails highlighting specific characteristics of each respondent, including level of education, age, gender and duration in the institution. The findings on the demographic data were used to determine if a responder was suitable for participation in the study since they would have had the opportunity to interact with the variables being examined.

4.2.1 RESPONSE RATE

The target population that comprised of bank employees, system engineers, telecommunication engineers, card fraud experts, other employees, business system analyst and biometric experts in KCB in Thika were given 352 questionnaires. Out of those 352 questionnaires, 281 were completed and returned for analysis which translates to a response rate of 79.83%. This response rate served as a representative sample for the study, so it was sufficient to draw conclusions. As per Mugenda and Mugenda (2009), a response rate of 50% is adequate for analysis and reporting; a rate of 60% is good and a response rate of 70% and over is excellent. The response rate is demonstrated in the figure below.

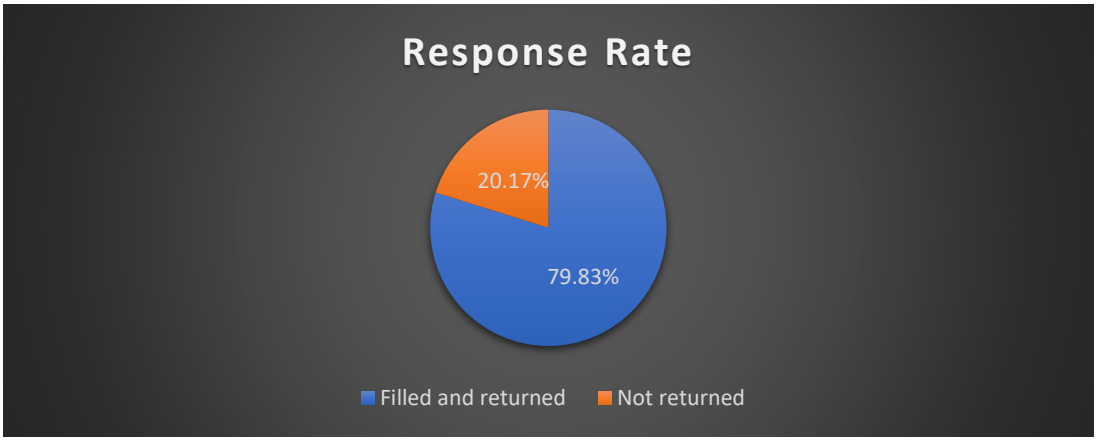


Figure 1:Response rate

4.2.2 GENDER SPECIFIC

The study sought to examine the gender distribution of respondents. According to the data gathered 65% of the respondents were male while 35% were female, which indicates males forms the largest group of the respondents as shown in the table below.

GENDER SPECIFIC	FREQUENCY	PERCENTAGE
Male	183	65%
Female	98	35%
Total	96	100%

Table 4:gender response rate

4.2.3 DURATION IN THE INSTITUTION

In order to assess the precision biometric authentication, the researcher sought to find out the duration spent by employees and the customer in KCB in Thika. 12 respondents have worked there for less than a year, 50 respondents have worked with KCB for a period of between two and five years, 40 have worked between six to ten years, while the other 179 have served in KCB for more than 10 years as illustrated below.

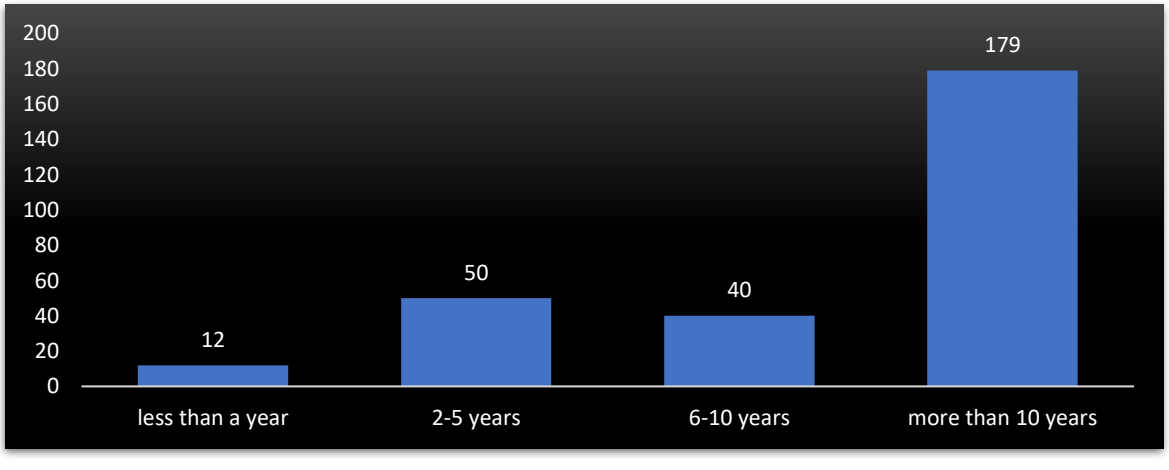


Figure 2:duration in institution

4.2.3 LEVEL OF EDUCATION

One important factor in the success of the research was the respondents' level of education, which the researcher used to determine the respondents' educational accomplishments.

Level of education	Frequency	percentage
Certificate	20	7.12%
Diploma	60	21.35%
Bachelor's degree	189	67.26%
Master's degree	10	3.56%
PHD	2	0.71%
TOTAL	281	100%

Table 5:Level of Education

We can see from (*table 5*) that most of the respondents managed to attain a bachelor's degree, which gives a go ahead that the respondents were able to understand and respond to the questions presented in the questionnaire

4.3 TECHNOLOGY AND BIOMETRIC IMPLEMENTATION

The study aimed to determine how technology can affect successful implementation of biometrics in KCB in Thika. The respondents' familiarity with interaction with biometric technologies were examined.

4.3.1 Respondents' Views on Technology and Biometrics Implementation

The respondents were asked the effect of technology on successful implementation of biometrics. They were questioned regarding the appropriate biometric traits to use for each of the physical and behavioral characteristics. It was used to gain a better understanding of the technologies that participants liked and disliked. The findings are represented in the figure below.

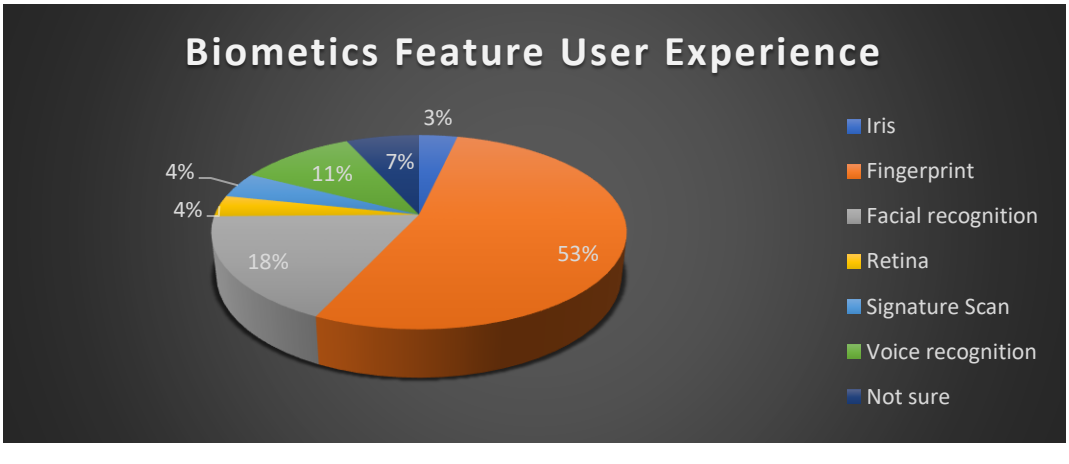


Figure 3:biometric feature user experience

53% of the respondents which was the majority were familiar with the use of fingerprint followed by those who were enormous with facial recognition which had 18%. Given their prevalence in personal electronics and our daily lives, this is hardly surprising. Both of these technologies have been utilized to safeguard portable electronic gadgets and are becoming more and more prevalent in our daily lives. For instance, fingerprint and facial recognition are currently commonly used in the vast majority of widely used personal devices such as smartphones and tablets, therefore this utilization is expected. 11% of the respondents were vast with voice recognition which is not surprising because in personal lives there exists gadgets that use this technology such as cars, houses and smartphones. 4% of the respondents were familiar with retina and signature scan. 3% of the respondents were vast in iris recognition. Lastly 7% of the respondents were not familiar with the use of biometrics in their daily lives. Which implies that fingerprint technology has been in use for many years and is a common method of identification for many individuals. Therefore, customers are likely to be more comfortable with using this technology than other biometric technologies, such as facial recognition or iris scanning, which may be perceived as intrusive or unfamiliar. The familiarity of fingerprint technology can lead to increased adoption rates, making it easier for banks to integrate this technology into their operations

4.3.2 User willingness vs non-user unwillingness to biometric technology usage

To assess the degree of general user willingness vs. non-user unwillingness in the use of biometric technologies, a t-test was run in SPSS. Statistical measurement of two intact groups using an independent samples t-test is appropriate to evaluate the variance amongst the two groups as per Shalah. K (2014). Results showed a statistically significant difference between non-user unwillingness and user willingness. Users' willingness to utilize biometric technology was on average 4.97, while non-users' unwillingness to use it was on average 3.73. The outcome indicates that users and non-users willingly assessed their overall satisfaction with the use of biometrics at essentially different levels.

Comparison sample	**Mean**				
User willingness vs non user willingness to use biometric technologies	Willingness (184)	Unwillingness (97)	Mean difference	t-value	sig
	4.39	3.33	1.06	7.610	0.00

Table 6:independent samples for t-test results

4.4 ICT POLICY AND BIOMETRIC IMPLEMENTATION

The study aimed as to determine the effect of the ICT policy on successful implementation of biometrics in KCB in Thika.

4.4.1 IMPACT OF ICT POLICY ON BIOMETRIC IMPLEMENTATION

The study aimed to find out the impact of ICT policy on biometric implementation at KCB in Thika. They were tested using the following elements;

Statements	N	Mean	Standard Deviation
ICT policies and guidelines should require banks to provide customers with control over their biometric data, including the ability to delete it	281	4.48	0.761
Effective ICT policies and guidelines can help ensure the ethical and responsible use of biometric authentication in banks	281	4.59	0.631
I will feel comfortable recommending biometric technology in my organization	281	3.28	0.453
I am willing to use biometrics technology to protect sensitive information	281	4.39	0.433
It will be a good idea to replace passwords and ID cards with biometric technology	281	4.18	0.391
I have privacy concerns using biometric technology	281	1.74	0.435
Biometric technologies are available in a reasonable cost with respect to its outcomes	281	3.13	0.338
Using biometric technology increases security level of individual data in banks	281	3.99	0.882

Table 7:impact of ICT policy on biometric implementation

The findings suggested that most of the respondents indicated that ICT policies and guidelines should require banks to provide customers with control over their biometric data, including the ability to delete it with a mean of 4.48 and standard deviation of 0.761. The findings also established that most respondents indicated that Effective ICT policies and guidelines can help ensure the ethical and responsible use of biometric authentication in banks with a mean of 4.59 and standard deviation of 0.631. The findings also established that most of the respondents indicated they will feel comfortable recommending biometric technology in the organization with a mean of 3.28 and standard deviation of 0.453. The findings suggested that most of the respondents indicated that they are willing to use biometrics technology to protect sensitive information with a mean of 4.39 and standard deviation of 0.433. The findings suggested that most of the respondents indicated that it will be a good idea to replace passwords and ID cards with biometric technology with a mean of 4.18 and standard deviation of 0.391. The findings

suggested that most of the respondents indicated they don't have privacy concerns using biometric technology with a mean of 1.74 and standard deviation of 0.435. The findings suggested that most of the respondents indicated that biometric technologies are available in a reasonable cost with respect to its outcomes with a mean of 3.13 and standard deviation of 0.338. The findings suggested that most of the respondents indicated that using biometric technology increases security level of individual data in banks with a mean of 3.99 and standard deviation of 0.882

4.4.2 Respondents' Views on ICT policy and Biometrics Implementation

The following statements were asked using a five-point Likert scale ranging from strongly agree to strongly disagree.

Statements	Strongly Agree	Agree	Neutral	Disagree	Strongly disagree
ICT policies and guidelines should require banks to provide customers with control over their biometric data, including the ability to delete it	50%	30%	10%	5%	5%
Effective ICT policies and guidelines can help ensure the ethical and responsible use of biometric authentication in banks	50%	20%	20%	5%	5%
I will feel comfortable recommending biometric technology in my organization	27%	23%	40%	8%	2%
I am willing to use biometrics technology to protect sensitive information	40%	50%	8%	1%	1%
It will be a good idea to replace passwords and ID cards with biometric technology	40%	40%	10%	5%	5%
I have privacy concerns using biometric technology	10%	3%	17%	10%	60%
Biometric technologies are available in a reasonable cost with respect to its outcomes	10%	20%	60%	5%	5%
Using biometric technology increases security level of individual data in banks	30%	40%	20%	7%	3%

Table 8:Respondents' view on impact of ICT policy on biometric implementation

80% of the respondents indicated that ICT policies and guidelines should require banks to provide customers with control over their biometric data, including the ability to delete it which is necessary below everyone has a right to his or her personal information. Also 70% of the respondents stated that effective ICT policies and guidelines can help ensure the ethical and responsible use of biometric authentication in banks

50% of the respondents indicated that they will feel comfortable implementing biometric technology in KCB in Thika while 40% of them were neutral. Our inference from these

responses is that there is a need to raise awareness of the benefits of biometric technology over traditional IT security methods. 80% of the respondents indicated that they are willing to use biometric technology to protect sensitive information. It has been determined that people would value implementing biometric technology in the future to safeguard sensitive data within their organizations as no one wants to be impersonated by fraudsters. 80% of the respondents also indicated that it will be a good idea to replace passwords and ID cards with biometric technology because it involves personal presence during verification process.

The majority 70% of the respondents stated that they don't have privacy concerns with biometric technology. This appears to suggest that people are aware of biometrics systems and willing to accept them. while 13% of them indicated that they have privacy concerns as privacy of personal data is very crucial. For instance, the DNA information can reveal a person's health and exposure to disease. 30% of the respondents indicated that biometric technologies are available in a reasonable cost with respect to its outcomes while 60% of them were neutral, our conclusion is that respondents lack understanding about the implementation costs of biometrics technology in relation to its results, and that this ignorance of costs may have an impact on respondents' views about the deployment of biometrics in bank institutions.

70% of the respondents indicated that using biometric technology increases security level of individual data in banks, this evident because biometrics use Two-factor authentication which is a combination of fingerprint and strong password. Two factor authentication prevents password theft and card theft. Because of this, a hacker may find it tough to steal or hack the biometrics of the database.

Which implies that development of a clear and comprehensive ICT policy is crucial for the successful implementation of biometric technology in banks. The ICT policy should outline the framework for the adoption, implementation, and maintenance of biometric technology in banks. Therefore, banks should develop and implement an ICT policy that addresses the key success factors of biometric implementation. And also, ICT policy should prioritize the protection of customer data and privacy. The ICT policy should ensure that biometric data is collected, stored, and used in compliance with relevant regulations and guidelines. Therefore, banks should prioritize the protection of customer data and privacy in their ICT policy.

4.5 EXPERTS AND BIOMETRIC IMPLEMENTATION

The study aimed as to determine the effect of experts on successful implementation of biometrics in KCB in Thika.

4.5.1 IMPACT OF EXPERTS ON BIOMETRIC IMPLEMENTATION

Statements	N	Mean	Standard Deviation
Experts can help ensure that biometric authentication in banking is accessible and user-friendly for customers.	281	4.28	0.721
Lack of expertise in biometric technology hinders effective implementation in banking.	281	3.59	0.431
Experts can help identify and address security and privacy concerns related to biometric authentication in banking	281	4.28	0.653
I know how to use biometrics	281	4.75	0.433
I find it simple to learn how to use biometric technologies.	281	4.18	0.391
My organization needs biometric technologies to avoid fraudulent transaction	281	4.74	0.735
Both technical staff and administration need to spread awareness for biometric technology in banks	281	4.13	0.638
I believe by attending any biometric technology conference will enhance my profounder understanding of the technology	281	3.99	0.882
Biometric enable me to have more convenience in the workplace	281	3.55	0.431
Biometric technologies can be easily compromised	281	1.89	0.465
The maintenance cost is lower with biometric technology compared to traditional security methods	281	3.46	0.568

Table 9:impact of experts on biometric implementation

The study aimed to find out the impact of experts on biometric implementation at KCB in Thika. They were tested using the following elements; The findings established that most of the respondents indicated experts can help ensure that biometric authentication in banking is accessible and user-friendly for customers with a mean of 4.28 and standard deviation of 0.721. The findings suggested that most of the respondents indicated that lack of expertise in biometric technology hinders effective implementation in banking with a mean of 3.59 and

standard deviation of 0.431. The findings suggested that most of the respondents indicated experts can help identify and address security and privacy concerns related to biometric authentication in banking with a mean of 4.28 and standard deviation of 0.653. The findings suggested that most of the respondents indicated the organization needs biometric technologies to avoid fraudulent transaction with a mean of 4.74 and standard deviation of 0.745. The findings established that most of the respondents indicated that both technical staff and administration need to spread awareness for biometric technology in banks with a mean of 4.13 and standard deviation of 0.638. The findings established that most of the respondents indicated that they believe by attending any biometric technology conference will enhance their profounder understanding of the technology with a mean of 3.99 and standard deviation 0.882. The findings established that most of the respondents indicated that biometric technologies cannot be easily compromised with a mean of 1.89 and standard deviation of 0.465. The findings also established that most of the respondents indicated that maintenance cost is lower with biometric technology compared to traditional security methods with a mean of 3.46 and standard deviation of 0.568

4.5.2 Respondents' Views on Experts and Biometrics Implementation

The following statements were asked using a five-point Likert scale ranging from strongly agree to strongly disagree.

Statements	Strongly Agree	Agree	Neutral	Disagree	Strongly disagree
Experts can help ensure that biometric authentication in banking is accessible and user-friendly for customers.	50%	20%	20%	5%	5%
Lack of expertise in biometric technology hinders effective implementation in banking.	20%	30%	40%	5%	5%
Experts can help identify and address security and privacy concerns related to biometric authentication in banking	40%	30%	20%	8%	2%
I know how to use biometrics	30%	50%	10%	5%	5%
I find it simple to learn how to use biometric technologies.	20%	40%	30%	8%	2%
My organization needs biometric technologies to avoid fraudulent transaction	20%	30%	1%	20%	29%
Both technical staff and administration need to spread awareness for biometric technology in banks	50%	20%	20%	8%	2%
I believe by attending any biometric technology conference will enhance my profounder understanding of the technology	80%	20%	0%	0%	0%
Biometric enable me to have more convenience in the workplace	10%	60%	20%	5%	5%
Biometric technologies can be easily compromised	10%	5%	25%	30%	30%
The maintenance cost is lower with biometric technology compared to traditional security methods	10%	20%	50%	14%	6%

Table 10:Respondents' view on experts and biometric implementation

70% of the respondents indicated that experts can help ensure that biometric authentication in banking is accessible and user-friendly for customers. Which is not familiar because experts have deep understanding of the regulatory and legal frameworks governing the use of biometric data in the banking sector. 50% of the respondents indicated that Lack of expertise in biometric technology hinders effective implementation in banking while 40% of them indicated that they were not sure.

80% of the participants indicated they know how to use biometric technology. This is evident because nowadays people own gadgets like smartphones and tablets that use biometric

technology especially use of fingerprint and voice recognition to secure their devices. The majority 60% of the respondents stated that they find it simple to learn how to use biometric technology

50% of the respondents indicated that KCB in Thika need to deploy use of biometric technology to prevent fraudulent transaction, while 49% which is almost half of the respondents denied. Our conclusion is that although while the majority of respondents (50%) feel that biometric technology should be used in their business, this could be because they have faith in the current system but see the need for more secure technology to entirely prevent fraudulent transaction and identity theft. Also, 49% of the respondents believes that their current system is secure enough and capable of preventing fraudulent transaction and identity theft. This may be due to a lack of knowledge about the key benefits of biometric technology or a reluctance to implement changes in the system.

70% of the respondents indicated that both technical staff and administration need to spread awareness for biometric technology in banks, which is necessary so as the customers can find it easy to use the biometric devices without any assistant which in turn saves time. All the respondents indicated that they believe by attending any biometric technology conference will enhance their profounder understanding of the technology which is basically normal because it is basic knowledge. 70% of the respondents stated that they have more confident while using biometrics in the banks as the confidential information is hidden in the database only the biometric devices are visible by the third party. This draws a conclusion that biometrics are more secure.

15% of the respondents stated that biometrics can be easily comprised while 60% of them indicated that they cannot be compromised which is not surprising as most of the respondents indicated that biometrics are more secure as two factor authentication. The remaining 25% were not sure. 30% of the respondents indicated that the maintenance cost is lower with biometric technology compared to traditional security methods while 50% of the were not sure. Our conclusion is that many of respondents are unaware of the maintenance costs associated with biometric technology in comparison to maintenance costs associated with traditional IT security approaches. From the standpoint of a provider, this would suggest that there is a need to raise awareness about the financial benefits of maintaining biometric technology as opposed to conventional IT security measures.

Which implies that having a team of experts who are knowledgeable about biometric technology is crucial for the successful implementation of biometric technology in banks. Experts can help banks identify the appropriate biometric technology, evaluate the benefits and costs of biometric technology, and ensure that the technology is implemented in compliance with relevant regulations and guidelines. Therefore, banks should prioritize the recruitment of experts who are knowledgeable about biometric technology.

4.6 Correlation between Technology, ICT policy and Experts on Biometrics Implementation

The research's first objective was to determine how technology affects successful implementation of biometrics an KCB in Thika. The findings showed that technology is positively correlated with success factors in biometric implementation in banks as shown in the table below.

The research's second objective was to determine how ICT policy affects successful implementation of biometrics an KCB in Thika. The findings showed that ICT policy is positively correlated with success factors in biometric implementation in banks as shown in the table below.

The research's third objective was to determine how experts affects successful implementation of biometrics at KCB in Thika. The findings suggested a positive correlation between the two variables. Thus, higher numbers of experts are associated with higher numbers of key success factors in biometric implementation in banks. As shown in table below

Correlations

		Technology	ICT policy	Experts	Success factors of biometric implementation
Technology	Pearson Correlation	1	.988**	.817**	.842**
	Sig. (2-tailed)		.000	.000	.000
	N	281	281	281	281
ICT policy	Pearson Correlation	.988**	1	.827**	.853**
	Sig. (2-tailed)	.000		.000	.000
	N	281	281	281	281
Experts	Pearson Correlation	.817**	.827**	1	.970**
	Sig. (2-tailed)	.000	.000		.000
	N	281	281	281	281
Success factors of biometric implementation	Pearson Correlation	.842**	.853**	.970**	1
	Sig. (2-tailed)	.000	.000	.000	.000
	N	281	281	281	281

**. Correlation is significant at the 0.01 level (2-tailed).

Table 11:Correlation between Technology, ICT policy and Experts on Biometrics Implementation

4.7 Regression between Technology, ICT policy and Experts on Biometrics Implementation

As shown in the table below the R square=0.949, which suggests that there is a higher relationship between the variables

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.974[a]	.949	.948	.07867

a. Predictors: (Constant), Experts, Technology, ICT policy

Table 12:Regression between Technology, ICT policy and Experts on Biometrics Implementation

4.8 ANOVA between Technology, ICT policy and Experts on Biometrics Implementation

According to ANOVA table below it shows that linear regression is significantly strong. A small p-value (0.00) suggest that the effect of the grouping variable on the dependent variable is strong and statistically significant

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	31.873	3	10.624	1716.710	.000[b]
	Residual	1.714	277	.006		
	Total	33.587	280			

a. Dependent Variable: Success factors of biometric implementation

b. Predictors: (Constant), Experts, Technology, ICT policy

***Table 13**:ANOVA between Technology, ICT policy and Experts on Biometrics Implementation*

4.9 Coefficient between Technology, ICT policy and Experts on Biometrics Implementation

According to the coefficient table below, it suggests that an increase in ICT policy use is associated with an increase in success factors such as data protection laws and standards by (0.333).

Also, according to the coefficient table below, it suggests that an increase in technology use is associated with an increase in success factors such as accuracy, reliability, user acceptance, and perceived usefulness by (0.780).

According to the coefficient table below, it suggests that an increase in Experts is associated with an increase in success factors such as deep understanding of the regulatory and legal frameworks governing the use of biometric data in the banking sector by (0.667).

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	1.405	.060		12.456	.000
	ICT policy	.333	.075	.347	4.448	.000
	Technology	.780	.070	.000	16.687	.000
	Experts	.667	.031	.652	21.833	.000

a. Dependent Variable: Success factors of biometric implementation

***Table 14**:Coefficient between Technology, ICT policy and Experts on Biometrics Implementation*

4.10 HYPOTHESIS TESTING

This research had three null hypothesis that were to be tested. Data collected was analyzed using SPSS and excel.

Concerning the impact of technology and key success factors of biometric implementation at KCB in Thika the data revealed that there is strong relationship (p=0.00) between technology and biometric implementation. In that an increase in technology leads to an increase in key success factors of biometric implementation at KCB in Thika. Thus, the null hypothesis was excluded.

On the impact of ICT policy and key success factors of biometric implementation at KCB in Thika the data revealed that there is strong relationship (p=0.00) between technology and biometric implementation. In that an increase in ICT policy leads to an increase in key success factors of biometric implementation at KCB in Thika. Therefore, the null hypothesis was rejected.

On the impact of Experts and key success factors of biometric implementation at KCB in Thika the data revealed that there is strong relationship (p=0.00) between technology and biometric implementation. In that an increase in Experts leads to an increase in key success factors of biometric implementation at KCB in Thika. Therefore, the null hypothesis was rejected.

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 INTRODUCTION

The banking sector is one of the industries that have been quick to adopt biometric technology for identification and authentication purposes. Biometric technology provides a secure and reliable way for banks to verify the identity of their customers and protect them from identity theft and fraud. This chapter reviews summary, conclusions and recommendations for further research based on the findings.

5.2 SUMMARY

The general objective of the study was to assess the key success factors for biometric implementation at KCB in Thika. Moreover, there were specific objectives of the study which were to determine the impact of technology, ICT policy, and experts on successful implementation of biometrics at KCB in Thika.

The literature review showed that the adoption of biometric technology in the banking sector has been successful in improving security and customer experience. Biometric authentication has been shown to be more secure and reliable than traditional methods such as passwords, PINs, and tokens. Biometric technology has also been shown to reduce the risk of fraud and identity theft by making it harder for criminals to impersonate someone else. The use of biometric technology in banking has also improved customer experience by reducing the time it takes to verify customer identities and access their accounts.

The survey conducted among bank customers and employees provided valuable insights into the implementation of biometric technology in the banking sector. The survey showed that customers are generally comfortable with using biometric technology in banking, and most of them find it convenient and secure. However, some customers have privacy concerns, and they prefer not to use biometric technology. The survey also showed that employees are generally supportive of the implementation of biometric technology, and they believe it can improve security and efficiency in banking. Using Statistical Package for Social Sciences (SPSS), quantitative data were analyzed using descriptive statistics which included tables, graphs, frequency distributions, and percentages. The research's findings, conclusions, and recommendations were based on the data that were analyzed.

Concerning the impact of technology and key success factors of biometric implementation at KCB in Thika the data revealed that there is strong relationship (p=0.00) between technology and biometric implementation. In that an increase in technology leads to an increase in key success factors of biometric implementation at KCB in Thika. Thus, the null hypothesis was excluded.

On the impact of ICT policy and key success factors of biometric implementation at KCB in Thika the data revealed that there is strong relationship (p=0.00) between technology and biometric implementation. In that an increase in ICT policy leads to an increase in key success factors of biometric implementation at KCB in Thika. Therefore, the null hypothesis was rejected.

On the impact of Experts and key success factors of biometric implementation at KCB in Thika the data revealed that there is strong relationship (p=0.00) between technology and biometric implementation. In that an increase in Experts leads to an increase in key success factors of biometric implementation at KCB in Thika. Therefore, the null hypothesis was rejected.

The analysis of the implementation of biometric technology in the banking sector showed that it is effective in improving security and efficiency. Biometric technology has reduced fraud and increased customer satisfaction.

5.3 CONCLUSIONS

In conclusion, the implementation of biometric authentication in the banking sector has several benefits, including improved security, reduced fraud, and improved customer experience. However, the technology must be carefully implemented and monitored to ensure its accuracy, effectiveness, and privacy and security of customer data. Validity considerations for measurements used in biometric authentication implementation are crucial in determining the success of the technology.

Key success factors for biometric implementation in the banking sector, including technology selection, integration with existing systems, regulatory compliance, user education and awareness, and continuous monitoring and evaluation, should be addressed to ensure the effectiveness and acceptance of the technology.

Based on the findings of the study the following conclusions were drawn:

i There was a strong relationship between Technology and biometric implementation which suggests that, an increase in technology leads to an increase in key success factors for biometric implementation at KCB at Thika such as accuracy, reliability, user acceptance, and perceived usefulness

ii Secondly there was a strong relationship between ICT policy and biometric implementation which suggests that, an increase in ICT policy leads to an increase in key success factors for biometric implementation at KCB at Thika such as data protection laws and standards

iii Lastly there was a strong relationship between Experts and biometric implementation which suggests that, an increase in experts leads to an increase in key success factors for biometric implementation at KCB at Thika such as deep understanding of the regulatory and legal frameworks governing the use of biometric data in the banking sector

5.4 RECOMMENDATIONS

Based on the findings of this study, it was discovered that technology has statistically significant impact of the key success factors of biometric implementation at KCB in Thika. The study encourages the organization to increase their technology so as to increase in success factors such as accuracy, reliability, user acceptance, and perceived usefulness. Also, the study found out that an increase in the number of experts leads to an increase in key success factors of biometric implementation thus KCB should increase the number of experts in biometric as they have a deep understanding of the regulatory and legal frameworks governing the use of biometric data in the banking sector. Lastly the study discovered that an increase in ICT policy leads to increase in key success factors in banks. Banks should conduct regular audits to ensure that the biometric technology they implement is functioning effectively and is not vulnerable to hacking or other security breaches.

By following these recommendations, banks can successfully implement biometric technology in their operations and reap the benefits of improved security and efficiency. The successful implementation of biometric technology in the banking sector will enhance customer satisfaction and strengthen trust in the banking system. Regularly monitor and

evaluate the performance and effectiveness of the biometric authentication system to identify and address any issues or shortcomings.

5.4.1 RECCOMENDATIONS FOR FURTHER RESEARCH

Biometric technology has gained significant attention in the banking sector as a potential solution for enhancing security and customer experience. However, while some studies have explored the key success factors of biometric implementation in the banking sector, there is still a need for further research in this area. Here are some recommendations for future research on this topic:

1. Comparative studies: Future research can focus on comparative studies of the different biometric technologies available for implementation in the banking sector. This could involve a comprehensive analysis of the advantages and disadvantages of each technology, along with an evaluation of their effectiveness in terms of improving security and customer experience.
2. Customer acceptance: Another area for further research is the level of customer acceptance of biometric authentication in the banking sector. Research can explore the factors that influence customer acceptance, such as trust in the technology, ease of use, and perceived benefits.
3. Regulatory and legal considerations: Finally, future research can explore the regulatory and legal considerations associated with biometric authentication in the banking sector. This can involve an analysis of the relevant laws and regulations, as well as an evaluation of the potential legal implications of biometric authentication systems.

Overall, further research in these areas can provide valuable insights into the key success factors of biometric implementation in the banking sector and help organizations to make informed decisions regarding the adoption of this technology.

REFERENCES

Agidi,R.C.,2018, 'using biometric in solving terrorism and crime activities in Nigeria', *Techsplend Journal of technology* 1(12), 91-105.

Akram, M. W., Saleem, Y., & Bhatti, N. K. (2020). *Determinants of adopting biometric authentication for online banking*: A developing country perspective. Journal of Retailing and Consumer Services, 53, 1-9.

Alastair Johnson, 'how biometrics(and blockchain) could save bricks and mortar retails'. *Biometric technology today* 2019 (3), 8-10, 2019

Al-Fawareh, H.M., Al-Jaghoub, S.M., Al-Qirim, N.A. (2019*). Investigating the factors affecting the acceptance of biometric authentication in mobile banking applications: An empirical study*. Journal of Enterprise Information Management, 32(1), 44-62.

Alfred C Weaver. 'Biometric Authentication': *computer* 39 (2), 96-97, 2006

Ateba, B.B., Maredza, A., Ohei,K.,Deka, P. & Schutte, D.,2015, 'Marketing mix: its role in customer satisfaction in the South African banking retailing', *Banks and bank systems (open-access) 10(1), 82-91*

Azhar, M. S., Qureshi, A. M., Ahsan, M. N., Ali, S., & Younis, Z. (2019). *An investigation of biometric authentication success factors for mobile banking: Integrating technology readiness and trust*. International Journal of Information Management, 44, 120-130.

Barney, J.B. (1991). *Firm resources and sustained competitive advantage*. Journal of Management, 17(1), 99-120.

Basri, S., & Wahab, A. (2019). *Adoption of biometric technology in banking industry: A review of challenges, opportunities and future directions*. International Journal of Information Management, 46, 63-71.

Bhatti, N. K., Akram, M. W., & Saleem, Y. (2020). *Investigating the impact of hardware technology on the accuracy of facial recognition-based authentication systems*. Journal of Retailing and Consumer Services, 54, 1-9.

Bhuyan, R., Hazarika, N.K. (2018). *Adoption of biometric authentication system in Indian banking sector*: An empirical study. International Journal of Information Management, 39, 13-23.

Boukottaya, A., Bouabdallah, A., & Loukil, T. (2020). *Biometric authentication in the context of mobile banking: challenges and solutions.* International Journal of Network Security, 22(1), 106-115.

Chowdhury, A., Islam, M. S., Islam, S., & Hossain, M. A. (2021). *The impact of machine learning algorithms on biometric authentication system performance*: A review. IEEE Access, 9, 17748-17764.

Clodfelter, R., 2010, 'Biometric technologies in retailing: Will consumers accept fingerprint authentication?' *Journal of Retailing and Consumer Services* 17(2010), 181–188.

Coetzee, J., 2018, 'Strategic implications of Fintech on South African banks', *South African journal of economical and management science* 21 (1), 2455

Davis, F.D. (1989). P*erceived usefulness, perceived ease of use, and user acceptance of information technology*. MIS Quarterly, 13(3), 319-340.

Dehghantanha, A., Parizi, R. M., Conti, M., & Dargahi, T. (2020). *A survey on biometric authentication in the era of machine learning*. ACM Computing Surveys, 53(4), 1-36.

European Union. (2018). *General Data Protection Regulation. Retrieved from* https://eur-lex.europa.eu/eli/reg/2016/679/oj

Hossein,S.S. & Mohammadi, S., 2012, 'review banking on biometric in the world's banks and introducing a biometric model for iran's banking system', *Joutnal of basic and applied scientific research* 2(9), 9152-9160

Hwang, H. G., & Kim, S. S. (2015). *An empirical analysis of factors affecting biometric technology adoption in banking*. Journal of Business Research, 68(3), 553-560.

Islam, M. A., Asaduzzaman, M., Sadiq, A. S., & Alshaikhli, I. F. (2020). *Biometric authentication: Recent advances, challenges and solutions.* Future Generation Computer Systems, 105, 871-887.

Kanoun, O., Bouslimi, R., & Khammassi, N. (2020). *Biometric authentication in mobile banking applications: state of the art and research challenges*. Journal of Ambient Intelligence and Humanized Computing, 11(8), 3519-3530.

Karkar, R., Abdallah, S., Al-Tamimi, A., & Al-Ali, A. (2018). *Factors influencing customers' acceptance of biometric authentication in online banking*. Journal of Retailing and Consumer Services, 43, 139-148.

Kaur, S., & Singh, S. (2021). *Biometric authentication for mobile banking: a review of challenges and solutions*. Wireless Personal Communications, 118(2), 1093-1123.

Kim Van Hoorde, Evelien De pauw, Hans Vermeersch, Wim Hardyns., 'the influence of technological innovations on the theft prevention': perspectives of citizens and experts. *Socially responsible innovation in security,* 44-62, 2018

Lee, T., 2016, Biometrics and disability rights: *legal compliance in biometric identification programs*, U.III. JL Tech. & Pol'y,p. 209.

Li, Y., Li, J., Lu, R., & Lin, X. (2015). *An efficient privacy-preserving biometric identification scheme for cloud-based mobile health services*. Journal of Medical Systems, 39(12), 186.

Liao, S., & Luo, C. (2018). *Biometric authentication in mobile banking: trends, challenges, and future directions*. Journal of Computer Science and Technology, 33(1), 1-22.

Maguire, M., 2009, ' The birth of biometric security', *Anthropolgy Today* 25(2), 9-14.

Mugenda A. O, Mugenda (2008). *Research methods, qualitative and quantitative approach*

Olawale, O. A., Khan, S. U., Gani, A., & Alazab, M. (2021). *A systematic review of biometric authentication in mobile banking applications*. Computers & Security, 105, 102202.

Sadiq, A. S., Asaduzzaman, M., Islam, M. A., & Al-Amin, M. M. (2020). *Biometric authentication for mobile banking applications: current state and future directions*. Journal of Ambient Intelligence and Humanized Computing, 11(10), 4355-4375.

Saunders, M., Lewis, P., Thornhill, A. & Bristow, A., 2019, *Research methods for business students*,12th edn., Pearson Publishers, Harlow, UK, viewed 03 October2019,

Siddiqui, F. I., Saifullah, A., & Hussain, J. (2020). Cloud-based biometric authentication in banking: Issues and challenges. Journal of Information Security and Applications, 50, 102412.

Supriya Gupta, Prabhakar Rajiah, Erik H middlebrooks, Dhirai baruah, Brett W Carter. *Academic radiology* 25(11), 1481-1490, 2018

Wu, J., Chen, Y., & Ji, X. (2020). *Behavioral biometrics-based authentication in mobile payments: An empirical investigation.* Journal of Business Research, 120,10234

Yussof, S.A.M., Hussin, B., Zakaria, N., & Shamsudin, M.N. (2016). *Critical success factors for biometric implementation in Malaysian banks*: A case study. Journal of Financial Crime, 23(4), 971-983.

APPENDICES

APPENDIX 1: RESEARCH WORK PLAN

Month\Activity	May	June	Aug-Nov	Jan-Feb	March
Topic and proposal preparation	Done				
Proposal writing and Defense		Done			
Data Collection			Done		
Data analysis				Done	
Conclusions and the final defense					Done

Table 15: Research Work Plan

APPENDIX 2: RESEARCH BUDGET

Activity	**Cost (Ksh)**
Questionnaire development	3000
Data collection	2000
Printing, binding, and photocopying	1800
Total	6800

Table 16: Research Budget

APPENDIX 3: QUESTIONNAIRE

A questionnaire has been generated by me, Shallom Okero Nyamweya as part of my study to test the key success factors for biometric implementation at KCB in Thika. Kindly give your opinion to the best of your knowledge

Please read the inquiries and provide your responses by checking the appropriate boxes or filling in the blanks.

SECTION I

1. What is your gender?

Male [ ] Female [ ] Prefer not to say [ ]

2. How long have you been employed or been a customer in this company?

i Not more than a year [ ]
ii 2- 5 years [ ]
iii 6 – 10 years [ ]
iv More than 10 years [ ]

3. What is your level of education?

i Certificate [ ]
ii Diploma [ ]
iii Bachelor's degree [ ]
iv Master's degree [ ]
v PHD [ ]

SECTION II: TECHNOLOGY

Please indicate by checking the box which shows the biometric technology that you are familiar with.

i. Fingerprint recognition [ ]
ii. Facial recognition [ ]
iii. Voice recognition [ ]
iv. Signature scanning [ ]

v. Iris recognition [ ]

vi. Retina scanning [ ]

vii. Not sure [ ]

SECTION III: ICT POLICY

Please indicate how much you agree or disagree with each of the following statements. (1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree).

Statements	**1**	**2**	**3**	**4**	**5**
ICT policies and guidelines should require banks to provide customers with control over their biometric data, including the ability to delete it					
Effective ICT policies and guidelines can help ensure the ethical and responsible use of biometric authentication in banks					
I will feel comfortable recommending biometric technology in my organization					
I am willing to use biometrics technology to protect sensitive information					
It will be a good idea to replace passwords and ID cards with biometric technology					
I have privacy concerns using biometric technology					
Biometric technologies are available in a reasonable cost with respect to its outcomes					
Using biometric technology increases security level of individual data in banks					

SECTION IV: EXPERTS

Statements	1	2	3	4	5
Experts can help ensure that biometric authentication in banking is accessible and user-friendly for customers.					
Lack of expertise in biometric technology hinders effective implementation in banking.					
Experts can help identify and address security and privacy concerns related to biometric authentication in banking					
I know how to use biometrics					
I find it simple to learn how to use biometric technologies.					
My organization needs biometric technologies to avoid fraudulent transaction					
Both technical staff and administration need to spread awareness for biometric technology in banks					
I believe by attending any biometric technology conference will enhance my profounder understanding of the technology					
Biometric enable me to have more convenience in the workplace					
Biometric technologies can be easily compromised					
The maintenance cost is lower with biometric technology compared to traditional security methods					