ASSESSMENT OF TECHNOLOGICAL RISKS FACING MOBILE BANKING: A CASE OF COMMERCIAL BANKS IN KENYA

NEBABA LUBAYO MONDA

A Project Research submitted in partial fulfilment of the requirements for the award of the degree of Master of Science in applied information technology in the, department of Computer and Information Technology and the School of Science and Technology of Africa Nazarene University

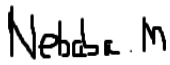
July 2020

DECLARATION

I declare that this document and the research it describes are my original work and that they have not been presented in any other university for academic work.

Name: Nebaba Lubayo Monda

Reg No: 17S03DMIT002



14/09/2020

Student Signature Date (dd/mm/yyyy)

This research was conducted under my supervisor and is submitted with our approval as university supervisors.

Supervisor Name: Dr Amos Gichamba



14/09/2020

University Supervisor signature Date (dd/mm/yyyy)

Supervisor name: Dr Kendi Muchungi



14/09/2020

University Supervisor Signature Date (dd/mm/yyyy)

Africa Nazarene University

Nairobi Kenya

DEDICATION

This work is dedicated to my family and partner Mariam who supported and encouraged me throughout the research work. At times it was energy sapping but without their encouragement and support this piece of work would not have been completed.

ACKNOWLEDGEMENT

All the effort and time I invested in this project would have been in vain were it not for the gift of good health that the Almighty God bequeathed upon me during the period of compiling this research thesis. Not to forget the tolerance my family endured of my absence as I raced against time to complete this thesis.

Much appreciation goes to my thesis Supervisor, Dr. Amos Gichamba and Dr. Kendi Muchungi from whom I received valuable guidance, encouragement, contributions and criticism that helped shape the direction of the research. Behind the scene, there are many unforgettable individuals. From the School of Science and Technology, Dr. J. Obuhuma for his numerous contribution that have formed the backbone of this project thesis.

May the Lord reward you abundantly for all your efforts.

Heartfelt appreciations!

ABSTRACT

Mobile banking technology has been widely adopted amongst all the commercial banks in Kenya. Currently Kenyan banks lose millions of shillings by means of online theft through mobile banking and other platforms. This study therefore intended to address the issues associated with mobile banking and was directed by the following objectives: to understand the mobile banking architecture, to establish the technological risks arising for commercial banks in Kenya as a result of mobile banking, to establish strategies which commercial banks use to mitigate against mobile banking risks, and to propose an integrated risk mitigation framework for use in mitigating against mobile banking risks. The target population was employees within the banking industry from different departments. Purposive sampling was used, which saw 52 staff from 3 commercial banks being sampled. A questionnaire was used as the main research instrument. The collected data was coded into Statistical Package for the Social Sciences (SPSS) version 26 in order to obtain descriptive statistics and correlation analysis. Qualitative data was analysed with the help of NVIVO Version 12 software. The analysed data was presented using charts, figures and tables. The study found that Current Mobile Banking applications leaked protected information while in transit or during communications from mobile phone to the server doing the transaction due to a weakness in the Secure Socket Layer Certificate (SSL). The study also found that banks did not have advanced detection mechanism such as intelligent behaviour monitoring and use of big data analytics technology for fraud detection and behaviour analysis. Lastly the study also found lack of mobile banking risk analysis and mitigation model amongst the 3 selected banks and developed a mobile banking risk mitigation model. The study therefore recommends adoption of the proposed framework which takes into account various best practices from different researchers and practitioners on information security in the context of mobile banking. The study further recommends that banks and other financial institutions should carry out an own assessment and customize the elements of the framework to fit their own organizational contexts.

TABLE OF CONTENT

DECLARATION ..... **i**
DEDICATION ..... **ii**
ACKNOWLEDGEMENT ..... **iii**
ABSTRACT ..... **iv**
DEFINITION OF TERMS ..... **vii**
ACRONYMS ..... **viii**
LIST OF TABLES ..... **x**
LIST OF FIGURES ..... **xii**
CHAPTER ONE **1**
1.1 Introduction 1
1.2 Background to the study 1
1.3 Statement of the Problem 3
1.4 Purpose of the study 4
1.5 Objective of the study 4
1.6 Research Questions 4
1.7 Significance of the Study 5
1.8 Scope of the Study 5
1.9 Delimitations of the Study 6
1.10 Limitations of the Study 6
1.11 Assumptions 6
1.12 Theoretical Framework 6
1.13 Conceptual Framework 9
CHAPTER TWO **10**
2.1 Introduction 10
2.2 Theoretical Review of Literature 10
2.3 Empirical Review 12
2.4 Technological Risks as a Result of Mobile Banking 14
2.5 Strategies and Technological Recommendations for Mitigating Mobile Banking Risks 18
2.6 Summary of Literature Review 21
2.7 Research Gap 21
CHAPTER THREE **23**
3.1 Introduction 23

3.2 Research Design 23
3.3 Research Site 23
3.4 Target Population 25
3.5 Determination of Study Sample 25
3.6 Data Collection 27
3.7 Data Processing and Analysis 28
3.8 Legal and Ethical Consideration 29
CHAPTER FOUR 31
4.1 Introduction 31
4.2 Characteristics of the Respondents 31
4.3 Presentation of Research Analysis and Findings 33
CHAPTER FIVE 60
5.1 Introduction 60
5.2 Discussions 60
5.2.1 Mobile Banking Architecture 60
5.2.2 Technological Risks arising for Kenyan Commercial Banks because of Mobile Banking 61
5.2.3 ICT General Controls Kenyan Commercial Banks use to Mitigate against Mobile Banking Risks 62
5.2.4 Mobile Banking Risk Mitigation Model 63
5.3 Conclusion 70
5.4 Recommendations for Policy and Practice 73
5.5 Areas for Future Research 74
REFERENCES 75
Appendix I: Questionnaire 87
Appendix II: ANU Introduction Letter 93
Appendix III: NACOSTI Research Authorization 94
Appendix IV: NACOSTI Research Permit 95
Appendix V: Project Plan 96
Appendix VI: Budget 97

DEFINITION OF TERMS

Biometric Authentication	The use of a person's unique biological information to verify the person's identity.
Encryption	Prevention of unauthorized access to information by encoding the message.
Poodle	A protocol downgrade that allows exploits on an outdated form of encryption.
Risk	The likelihood of occurrence of an event that has negative effects or damage.

ACRONYMS

AJAX	Asynchronous JavaScript and XML
ANOVA	Analysis of Variance
APK	Android Package
ATM	Automated Teller Machine
E-COMMERCE	Electronic Commerce
EDI	Electronic Data Interchange
HTTP	Hyper Text Transfer Protocol
IB	Internet Banking
ICT	Information Communication Technology
IP	Internet Protocol
IS	Information Security
JDBC	Java Database Connectivity
JMS	Java Message Service
JSON	JavaScript Object Notation
J2ME	Java 2 Platform, Micro Edition
J2EE	Java 2 Platform Enterprise Edition
M-BANKING	Mobile Banking
NFC	Near Field Communication
OTP	One Time Password
PKI	Public Key Infrastructure
PMT	Protection Motivation Theory
PR	Perceived Risk
SACCO	Savings and Credit Cooperative Organization
SIM	Subscriber Identification Module
SMS	Short Message Service

SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
TPR	Theory of Perceived risk
USSD	Unstructured Supplementary Service Data
2FA	Two Factor Authentication

LIST OF TABLES

Table 3-1: Sample Size Distribution 26

Table 4-1: Response Rate Table 31

Table 4-2: Descriptive Statistics of Malware 37

Table 4-3: Means and Standard Deviation on Descriptive statistics on malware 38

Table 4-4: Descriptive Statistics of SSL Vulnerabilities 39

Table 4-5: Means and Standard Deviations on Descriptive Statistics of SSL Vulnerabilties 40

Table 4-6: Descriptive Statistics of Mobile Fraud 43

Table 4-7: Means and Standard Deviations on Descriptive Statistics Of Mobile Fraud Vulnerabilties 44

Table 4-8: Descriptive Statistics of other Information Security Incidents/ Risks 45

Table 4-9: Means and Standard Deviations on information security incident /risk 45

Table 4-10: Number of Information Security risks/incidents 46

Table 4-11: Descriptive statistics of two factor authentication 47

Table 4-12: Means and Standard Deviations of two factor authentication 48

Table 4-13: Descriptive Statistics of encryption 48

Table 4-14: Means and Standard Deviations on Descriptive statistics of encryption 49

Table 4-15: Descriptive statistics of Permission based access 50

Table 4-16: Means and Standard Deviations on Descriptive statistics of Permission Based Access 51

Table 4-17: Descriptive Statistics of the use of Biometrics 52

Table 4-18: Means and Standard Deviation on Descriptive statistics of the use of Biometrics 53

Table 4-19: Descriptive statistics of the use of intelligent behavioural monitoring and analysis technology 54

Table 4-20: Means and Standard Deviations on Descriptive statistics of the use of intelligent behavioural monitoring and analysis technology 55

Table 4-21: Output of Correlation between strategies to mitigate mobile banking risks and occurrence of mobile banking risks 56

Table 4-22: Output of Correlation between strategies to mitigate mobile banking risks and number of mobile banking risks 57

Table 4-23: Output of Correlation between strength of risk mitigation and number of mobile banking risk.....58

Table 5-1: Mobile Validation Scores.....70

LIST OF FIGURES

Figure 1-1:Conceptual framework showing dependent and independent variables...9
Figure 2-1: Determinants of Preventive behaviour/actions.....11
Figure 2-2: Mobile Banking Architecture 13
Figure 2-3: Bank B banking services architecture.....14
Figure 3-1: Banking Tier Rating 24
Figure 3-2: Krejcie and Morgan model 26
Figure 4-1: Years Of Work experience of the Respondents.....32
Figure 4-2: Work Deparment of the respondents 33
Figure 4-3: Education level of the Respondents.....33
Figure 4-4: Mobile BankingArchitecture 34
Figure 4-5: Word Frequency 35
Figure 4-6: SSL Vulnerability of Bank A 41
Figure 4-7: APK Vulnerability of Bank B.....42
Figure 5-1: Risk Mitigation Model Proposed By Luvaga (2014) 64
Figure 5-4: Proposed Mobile Banking Risk Mitigation Model.....66

CHAPTER ONE

INTRODUCTION

1.1 Introduction

This chapter is geared towards highlighting the historical background of the study matter. Additionally, the segment will explain mobile banking and online money transfer challenges. The statement of the problem, purpose, objectives, research issues, meaning, limitations, scope, conceptual and theoretical framework will also be discussed in this chapter.

1.2 Background to the study

Mobile Banking alludes to the utilization of a cell phone or other cell gadget to perform web based financial undertakings while away from your home PC, for example, checking account status, moving assets between accounts, clearing transactions or finding an ATM (Automated Teller Machine) and normally works over all significant networks in Kenya such as Safaricom, Airtel and Telkom through various channels such as USSD (Unstructured Supplementary Service Data), SMS (Short Messaging Service) or mobile applications programmed for phones (Chase, 2020). Recently, we have experienced a revolution in mobile applications which feature strong processors, expanded bandwidth, faster data connections, better user interface and countless applications (Chase, 2020).

Kenya leads in the penetration mobile financial services in Africa with 68% penetration which is higher than that of Sudan, Gabon, and Algeria whose penetration rates are 52%, 50% and 44% respectively (Verkijika, 2020. Only banks can directly offer digital financial services. The report notes that Kenya has a significant impact on a number of factors, such as the penetration of mobile telephones, the development of financial and classical networks, legislation and the willingness of private players to implement new initiatives that drive a

variety of digital finance services compared to Cameroon, where only banks can directly offer digital financial services. There are 203 million worldwide mobile cash accounts, approximately half of which have the largest share of Sub-Saharan Africa with East Africa. The minimum number of mobile money accounts registered in at least 19 African countries is greater than those of bank accounts (Kimutai, 2018).

The adoption of mobile banking has brought about various security challenges which threaten its success. However, the greater efficiency that mobile banking provides for both banks and customers implies that it is an idea whose time has come, and commercial banks have no choice but to make sure it is successful. The customer expects standard banking services on mobile devices too. Kimutai (2018) notes that increasing sales of smart phones will continue to increase transaction volumes from mobile devices. Mobile devices are an evolution that a bank cannot disregard when its rivals are not willing to leave behind.

According to Kimutai (2018), Kenyan banks have lost a total of $860,000 to hackers, with two lenders temporarily halting their mobile and online banking services. One of the banks was hit in June 2018, when hackers tried to move $1 million out of their networks. The bank recouped $630,000. A week later, it was again targeted, another $120,000 hit, only half recovered. "These funds have been routed through the mobile money and online platform which, according to Kimutai (2018), has temporarily halted the services as the bank conducts an audit and update.

The 2014 Kenya Cyber Security Report by Serianu (2014) indicated that most local banks do not have adequate protection from fraud against mobile banking services. In this report, which expounds on the threats posed by the adoption of ICT, organizations have to protect their systems equally against cyber-criminals. Results from a research done on 33 banks showed that only two banks have taken sufficient security measures to secure money for their clients. "Most of the mobile banking apps tested are not highly encrypted and susceptible

to attacks," the report adds. There have been deliberate efforts to identify and combat cybercrime around the globe (Serianu, 2014). Based on a comprehensive study done by Islam (2014) on the security challenges posed by cellular banking in Malaysia between 2008 and 2012, the results showed that the most important threats during that period were unauthorized access, malicious hacking, ransomware, and smartphone viruses.

1.3 Statement of the Problem

Mobile banking technology has been widely adopted amongst all commercial banks in Kenya as a strategic tool for market penetration, without massive investment in physical infrastructure. The technology has been very crucial in serving a significantly large and expanding client base with quick, proficient, and suitable quality services (Ngugi et al., 2020). According to Serianu (2016) the major mobile banking issues stumbled upon were unwarranted external individuals having access to financial institutional data, credential information tapped over insecure wireless networks, unencrypted data and reverse engineering. Virus harbouring cell phones were also one of the key causes that led to hacking in mobile banking platforms. Despite the existence of some of these threats, there are technological security controls, which effectively and substantially mitigate the risk.

In Kenya, a study by Shaukat et al (2020) to evaluate mobile banking, identified system failure or fraud as the main risks facing mobile banking service providers. The variations in the findings indicate that the risks arising from the adoption of mobile banking are dynamic and vary from one. Hence, there is need for clarity on the actual and prevailing mobile banking risks facing the service providers in different contexts. Despite these studies offering a rich information base on the mobile banking risks, there is scarcity of empirical evidence about the prevailing security risks facing mobile banking in commercial banks in Kenya. This denies the banks valuable information for conducting cost benefit analysis for adopting the technology. This study therefore seeks to fill this knowledge gap by examining the current risks facing

mobile banking among the commercial banks in Kenya, recommending various technologies and strategies that would minimize mobile banking risks, while also providing a risk mitigation model that will be beneficial to the banking sector down the line.

1.4 Purpose of the study

To assess the technological risks being faced by mobile banking among the commercial banks in Kenya and develop a risk mitigation model.

1.5 Objective of the study

1.5.1 General Objective

To Assess Mobile Banking risks and Mitigation Strategies being used amongst commercial banks in Kenya.

1.5.2 Specific Objectives

i. To understand the mobile banking architecture and its components.
ii. To establish the technological risks arising for commercial banks in Kenya as a result of mobile banking.
iii. To establish strategies and provide ICT General Controls recommendations which mitigate against mobile banking risks.
iv. To develop a Mobile Banking risk mitigation model for banks in Kenya.

1.6 Research Questions

i. What does a mobile banking platform entail and consist of?
ii. What technological risks arise for Kenyan Commercial Banks because of Mobile Banking?
iii. What ICT General Controls do Kenyan Commercial Banks use to minimize mobile banking risks?
iv. What entails a Mobile Banking risk mitigation model?

1.7 Significance of the Study

The study will be important to financial institutions as it will outline useful information regarding the requirement of mobile banking implementation in relation to technology and risks surface area generated as a result of it. A better understanding of these factors will enable the stakeholders such as Mobile Banking Service Providers and Financial institutions to develop suitable awareness programmes and marketing strategies.

The Information would be valuable to mobile developers involved in the coding and development of the mobile banking application hosted by banks and used by customers, as it will help them understand potential risks brought about by their applications and why bank customers avoid the existing application despite potential marketing ploits to use the system. The study can also be used as a basis to conduct future research regarding how far the mobile banking industry has reached over a given period and its significance, in addition any organization with an aim of entering or penetrating the Kenyan mobile banking industry can get meaningful and valuable insights by extrapolating the results of the study.

This study will identify knowledge gaps while providing suggestions for further research which might be needed. It will also add to the already existing knowledge involving mobile banking technology risk issues which would be useful for the individuals involved decision making while also providing a reference point for future researchers regarding mobile banking and information technology.

1.8 Scope of the Study

The study focused on employees from 3 commercial banks in Kenya which were purposively selected for this study. They included banks from Tier 1, Tier 2 and Tier 3 Category. Scope consisted of Bank A, a Tier 1 Bank, Bank B, a Tier 2 Bank, and Bank C, a Tier 3 Bank. In addition, the study focused on mobile banking risks only, and did not focus on other information security risks facing the banking systems.

1.9 Delimitations of the Study

The scope was limited to the three commercial banks three banks because of time and reachability constraints. It was difficult to reach all the commercial banks in Kenya within a short time. The three banks were representative of all the commercial banks in Kenya because one bank was picked from each tier. The focus on mobile banking risks only was because other information security risks facing commercial banks were not relevant for the study.

1.10 Limitations of the Study

The study was limited by the reluctance of respondents to give full information regarding information security incidents that have occurred in the bank, as well as the existing mitigation measures/controls. The reluctance was due to the fact that banking information is sensitive, and therefore banks may not be willing to make it look like they are exposed, or that customer data has been compromised by cyber attackers. To address this limitation, the study assured the bank management as well as the respondents that the information would be highly anonymized so that no one can relate it to a particular bank.

1.11 Assumptions

Mobile banking is a recent banking development and practice in Kenya although it is widely practiced by customers. Banking and Financial institutions in Kenya are well technologically developed and secure to support mobile banking services.

1.12 Theoretical Framework

1.12.1 Risk Barrier

Forsythe and Shi (2013) stated that the concepts of perceived risk changed from risk of service quality and fraud to risks related to the socio political, mental and physical risks in online transactions as more people engage with online and mobile transactions. According to Ram and Sheth (2010), the risk barrier is the level of risk in innovation. It should be noted that the risk concerned is a consumer's perceived risk and not an innovation characteristic (Fain &

Roberts, 2012); the consumer expects to have a state or loss if the innovation does not achieve the expectations. Ram (2013) suggests that the perceived high risk can play an important role, but he is not, as many other factors contribute, the only driver of innovation resistance. The study conducted by Fain and Roberts (2012) found that the key differentiations between younger and older customers with risk barriers are differences in m-banking resistance factors. In mobile banking, privacy and security, a variety of identified risks exist (Lee & Lin, 2015). It can include PIN codes, personal and financial information. One may be worried, for example, that mobile bank data is being collected or poor battery life, which can disrupt mobile banking, or that the input of false data may be fearful because of small keypads. Moreover, self-efficiency, which refers to one's faith in its ability to use mobile banking, is also seen as a strong obstacle to resistance to innovation (Ellen, Bearden and Sharma, 2011). If you don't feel you 're not comfortable, skilled or able to learn to operate an innovation, your adoption takes place less often. Particularly for mobile banking and mature users, the process needs the input of important information and figures that can increase the doubt about self-efficiency. Considering the theory of Ram (2013) that increased innovation testing can reduce stability, risk can be expected through the proceeding of the service with consultations with bank staff.

1.12.2 Theory of Perceived Risk (TPR)

As defined by Bauer (2014), Perceived risk theory details the relation to consumer behaviours, the benefits in most cases are always hand in hand with risks. According to Ostlund (2014) the perceived risk is considered to be a barrier to new innovation dissemination. The results of Lee (2014) confirmed that a person's decision to use the mobile banking compared to a benefits factor had a stronger effect on perceived risk. In the context of Internet Banking five types of perceived risk were investigated. These include security, confidentiality, financial, social, simplicity and productivity risk (Lee, 2014). According to Sathye (2017) the security risk and the risk of privacy relate to the likelihood of unauthorized access to personal

or financial information by means of network or data transactions attacks or unauthorized access to the account through faux or faulty authentication that compromises the security of internet banking sites. The risk factors related to security and privacy were identified as significant obstacles to the adoption of Mobile Banking (Sathye, 2017). The potential cash loss and uncertainty arising from mistakes in transactions or bank account misuse are related to financial risk (Lee, 2014). Laukkanen and Kiviniemi (2010) state that many customers avoid using Mobile Banking with the worry of losing money when conducting online transactions due to lack of face to face interaction or physical authentication. The risk of time or convenience refers to the risk that a disoriented internet site that is difficult to navigate or delays transaction completion may cause time and discomfort (Lee, 2014). Lastly, Laukkanen and Kiviniemi (2010) define performance risk as the risk that a customer will lose from vulnerabilities of the Internet banking website and the break-out of system servers or interruptions of the Internet.

1.13 Conceptual Framework

In figure 1.1, the independent variables include the ICT General Controls that mitigate mobile banking risks, elements of the mobile banking architecture, and technological risks that arise as a result of mobile banking. The dependent variable is mobile banking risks whose indicators include the type and number of risks occurred, and the strength of mobile risk mitigation.

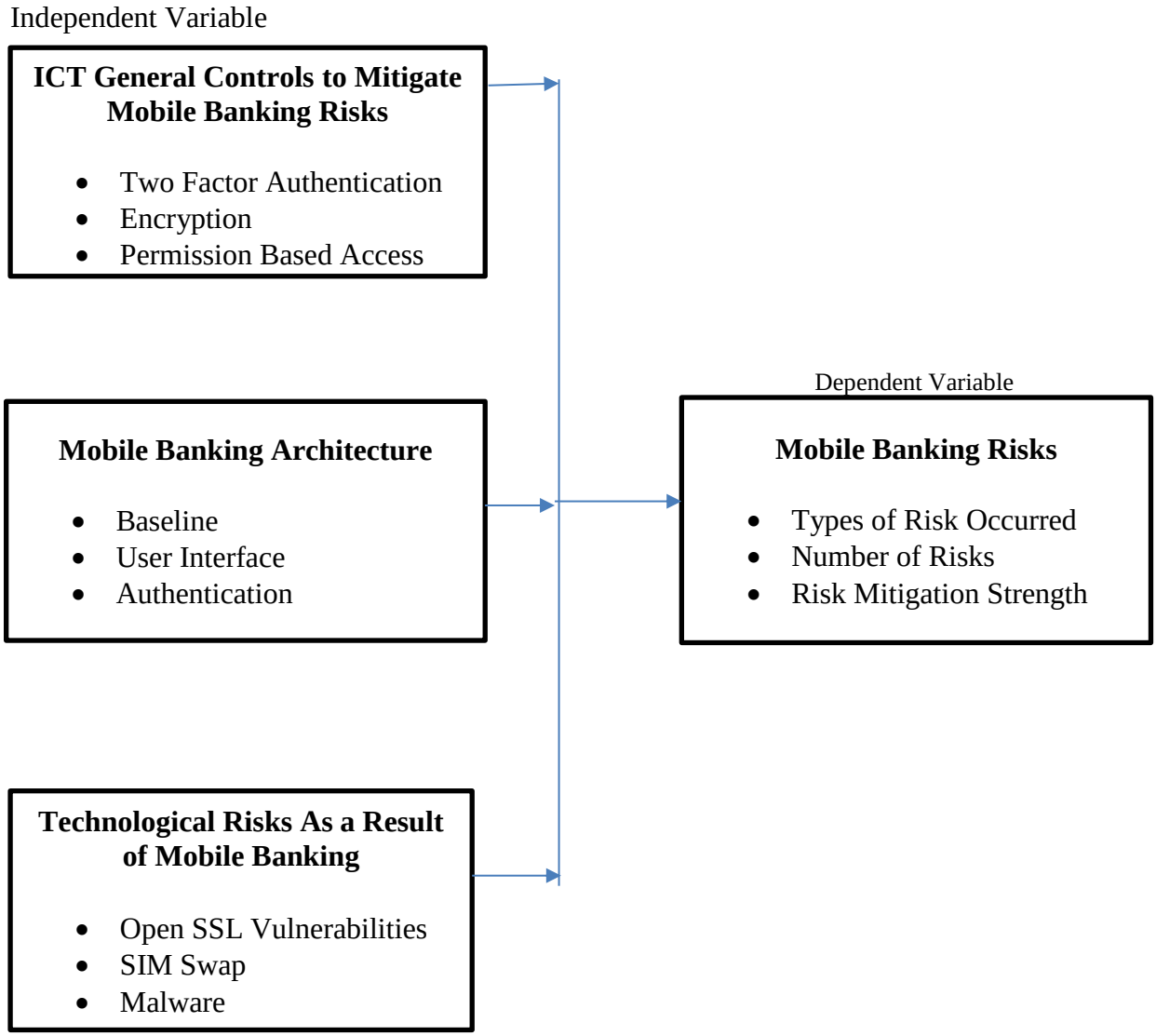


Figure 1-1 Conceptual Framework Diagram

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The segment deals with the theoretical literature and empirical study. The first section examines the architecture of mobile banking. The second section addresses technical challenges resulting from mobile banking use. The final section examines approaches and practical guidelines for reducing the risks of mobile banking.

2.2 Theoretical Review of Literature

2.2.1 Protection Motivation Theory (PMT)

The Protection Motivation Theory was the brainchild of Jansen and Schaik (1975) who posited that self-protective behaviour among individuals or groups is motivated by the fear of the potential consequences of a perceived threat. This process begins with an appraisal of the potential threat which then triggers preventive actions to mitigate or prevent the undesirable consequences, in a process referred to as the coping appraisal process. The Protection Motivation Theory has evolved over time and has been applied by researchers in various fields to provide theoretical justification for preventive behaviour or actions. From the perspective of Information Security (IS), PMT has been applied to explain the behaviour of users, organizations, IS security experts, among others towards information security vulnerabilities such as data breaches, fraud, malware attacks among others. Pal, Herath and Rao (2020) applied the Protection Motivation Theory in their study to explain the protective behaviour of users of mobile devices in the context of the risk of data breach. The study found that self-efficacy and the fear of potential negative consequences of a data breach motivated user of mobile devices to take precautionary measures. Similar facets were identified by Diesch, Pfaff and kramar (2016), In a study on the application of PMT to the security of wireless networks

at homes, Shaukat et al (2020) adopted the Protection Motivation Theory and modelled preventive behaviour as shown in figure 2.1.

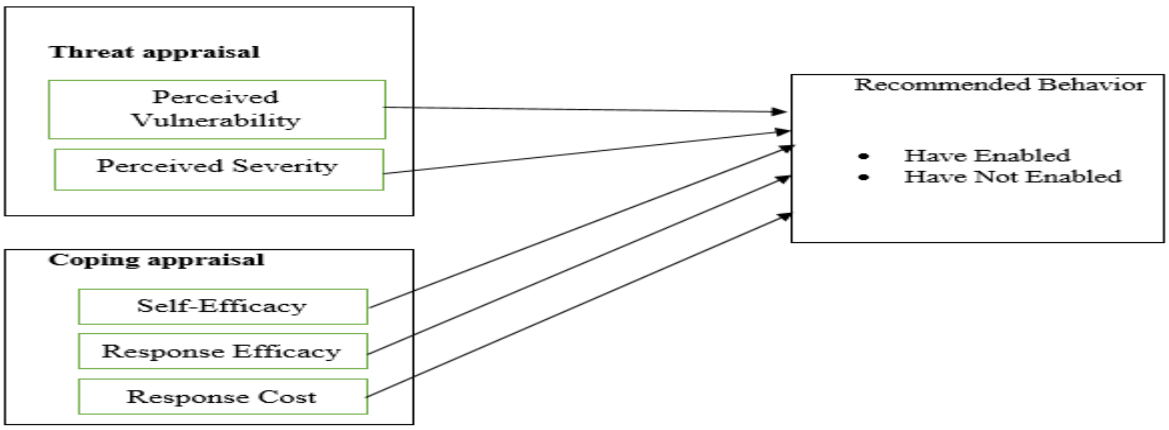


Figure 2-1: Determinants of preventive behaviour/actions, adopted from PMT. Source: Shaukat et al (2020)

In the context of this study, the PMT is indeed applicable and was useful in explaining the various mitigation measures implemented by commercial banks to guard against information security risks associated with mobile banking. The theory also justifies the goal of this study which is to develop a holistic preventive security model that will address the Information Security (I.S) needs of commercial banks especially in the wake of the widespread adoption of mobile banking and the increasing security risks that accompany it. The study also investigates the technological risks facing banks as a result of mobile banking adoption, as part of the threat appraisal process of PMT.

2.2.2 Socio-Technical Systems Theory

The socio-technical systems theory is concerned with the nexus between technological systems and social aspects such as human behaviour. In the context of information security risks, the human aspect is dominantly linked to most of cyber-attacks. According to Mujinga, Eloff and Kroeze (2017), most attacks on organizational information systems take advantage

of the human vulnerabilities of these systems to penetrate the laid down security measures through social engineering and other human-related avenues of attack. It is therefore worth noting that implementing the very best information security measures without taking care of the human aspect of information security makes an organization vulnerable. Therefore, a robust information security system must take into consideration both the technical and human aspects.

The need to have a holistic approach to information security by incorporating both technical and social controls is the basis of the socio-technical systems theory (Paja et al., 2015). Human beings have been described as the weakest link in information security, especially because human behaviour is difficult to predict or control.

2.3 Empirical Review

2.3.1 Mobile Banking Architecture

Jacob (2020) explains that mobile banking combines on-the-go two-way data transmission in payments with banking, and real-time, pervasive access to bank information and services by devices such as smartphones. The EDI technology is used to transfer data in an electronic format without the need for any human input by bank employees. It allows for automatic processing. According to Paladion Networks (2017) the main application in mobile banking within the Bank Network is based on general mobile banking architecture. It contains transaction requests from customers with the core banking systems as displayed in fig 2-2.

The online banking programs on users send the transaction request via an Internet protocol that defines the mobile banking application service to the web server area. The mobile banking software links mobile network providers to a dedicated network to provide the user with proof of the transaction status of the Short Messaging System (SMS). Alternatives to smartphone apps like unstructured extra service (USSD) are used by some internet bank providers. Usually USSD solutions are supported by a dedicated rental connection from mobile network providers on mobile banking servers.

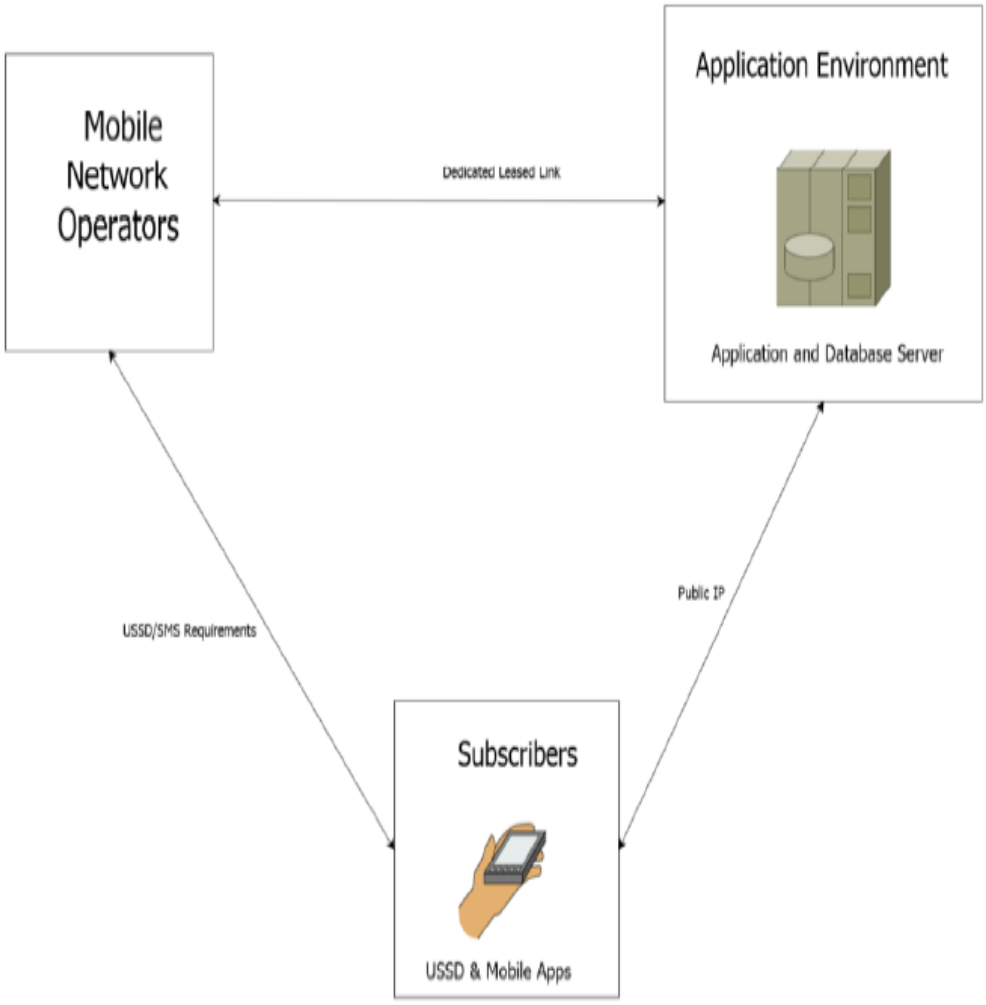


Figure 2-2: Mobile Banking Architecture inspired by (Paladion Networks, 2007)

Bank clients have to activate their mobile bank accounts by requesting the mobile banking apps and the platform service providers to do so. The customers' mobile numbers are currently linked to their active bank accounts. The architecture of Bank's B mobile banking for example has been designed to provide its customers with access by local network operators, such as Liquid Telecommunication limited and Embarq Limited via different channels, including its mobile banking application. As depicted in figure 2-3, once authorized users are connected to the banking platform, they are able to enjoy services offered by the bank.

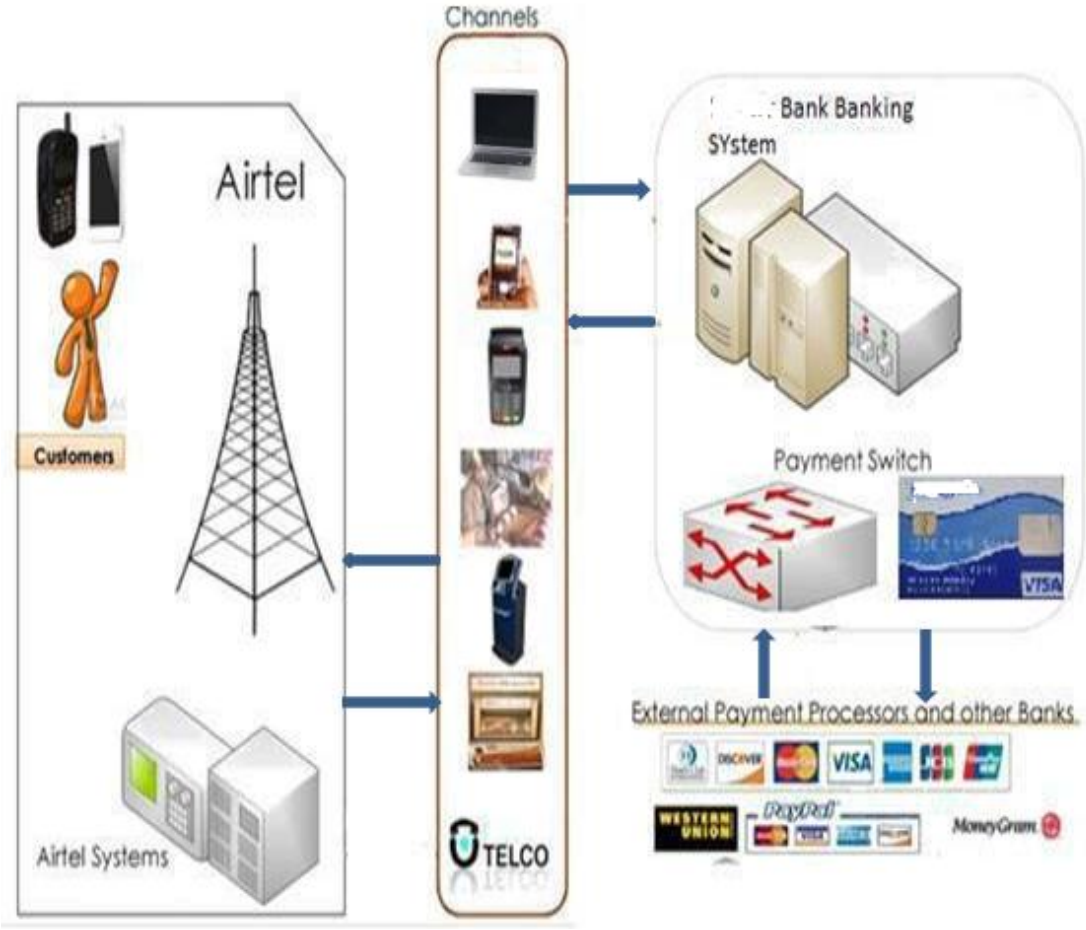


Figure 2-3: Bank B banking services architecture

Secure socket layer Certificates (SSL) are installed on mobile banking websites by some mobile banking providers to ensure that data is transmitted via the platform. Stable Socket Layer Certificates encrypt Internet communications with the user's public / private keys.

2.4 Technological Risks as a Result of Mobile Banking.

2.4.1 OpenSSL Vulnerabilities

The OpenSSL software library uses the secure socket layer (SSL) as described by Chandra, Messier and Viega (2012), and the security layer transport (TLS) security protocols. By its design, OpenSSL provides a secure means of communication over an unsecure medium, because of the need to securely encrypt and decrypt data in transmissions in internet-based

platforms. It is used for secure communications and protection against information leakages in applications. It is often used to validate other parties' identity in applications. In an open source environment, OpenSSL employs the (Transport Layer Security) protocols: SSL and TLS. Chandra et al., (2012) further states that although OpenSSL seeks to ensure that developers and administrators are able to communicate safely and securely in a safe and secure way, in reality the SSL protocol requires an adequate understanding of the principles of security to make proper use of it. As a result, many OpenSSL applications are vulnerable to attacker exploitation. This is mainly because developers, vulnerable third-party libraries and vulnerable security elements are integrated into mobile devices (Chandra, Messier & Viega 2013). This is also due to poor understanding of security principles. Details of another security vulnerabilities have also been released by various researchers, which allow an attacker to attack and extract data from a safe connection. The most frequently described bug is a downgraded legacy Padding Oracle encryption (POODLE) found in SSL release 3. No known bug mediation mechanisms such as the POODLE bug for early SSL releases that are no longer industry standard safety criteria are currently being identified, including updating their applications with Version 1.2 (Chandra, Messier & Viega 2013), Transport Layer Protection (TLS) may indicate vulnerabilities to these unsafe SSL variants.

2.4.2 Sim Swap

Mobile banking applications are usually connected directly to mobile banking servers that can be reached through the internet. Sensitive client banking data is then sent from mobile devices to the mobile banking servers over the internet. This expands the attack surface in banking systems by introducing potential areas of vulnerabilities that can easily be exploited by an unauthorized user and an internal member of staff (Temenos & NetGuardian, 2016). One such attack that can be deployed in such a setup is a man in the middle attack. This is a cyber-attack where a perpetrator positions himself in a conversation between a user and an

application, either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway (Seriano, 2015).

By performing a man in the middle attack over an unsecured/compromised connection between a mobile banking application and the respective financial institution, an attacker can easily be able to retrieve the user's authentication information such as an identification number, phone number and passwords amongst other account details. He can then easily share this with an internal member of staff in the banking institution who has access to the customers' data within the mobile banking system. The insider can then alter the credentials by putting the attacker's phone number as the active phone number of that account number. At this point, the attacker can call the bank's helpline requesting a password reset. This will be sent to the active phone number which now belongs to the attacker. He can then proceed to raid the account before having the insider revert the records back to the correct state. An attack influenced or perpetuated by an insider is very difficult to identify or recover from (Seriano, 2015). This is largely in part due to their knowledge of security and procedures already in place.

Using the acquired credentials and a little social engineering an attack that relies on social interactions between people to trick them into breaking normal security procedures (Rouse, 2016). The attacker can also launch a SIM swap attack on the unsuspecting victim. A SIM swap attack is an attack whereby the attacker uses your identification details and a little social engineering to convince your mobile network provider's agents at various stations and call centres to activate a new SIM that they are in possession of. This deactivates the current SIM card that the unsuspecting victim has causing him to lose phone service (Brignall, 2016). The attacker can then proceed to make PIN change requests and perform account transactions through the mobile banking application on their phones using your mobile phone number and other identification details they already have. All responses from the bank are sent back to the attacker's phone since it currently holds the active SIM card registered to the victim. Given

that the requests are coming from an authorized source (the victim's phone number), the financial institutions cannot flag this as an erroneous transaction attempt. According to Serianu (2015), sensitive and confidential customer banking information is often stolen and sold in the black market. The theft of confidential data from unsafe or compromised connections and other instances of fraud are damaging to a bank's image and reputation even if there was no direct loss of money (Temenos & NetGuardian, 2016). As it stands, fraud and identity theft are a serious concern for financial institutions and mobile banking related fraud can only make things worse.

2.4.3 Malware

Malware attacks have become common as a result of the widespread adoption of mobile banking. In addition, these malwares have become increasingly sophisticated, posing a significant information security risks to commercial banks and users (He, Tian & Shen, 2015). Malware programs take advantage of system vulnerabilities to infiltrate and access sensitive information leading to the leakage of data, manipulation, and financial loss. Common forms of malware experienced in mobile banking include viruses, root kits and Trojans. According to He, Tian & Shen (2015), attackers are continuously making improvements to these malwares in order to outwit the security features implemented by banks. This makes it difficult for banks to completely defend against malware attacks because they are always evolving and gaining more resilience. Viruses attach themselves into other programs and replicates, while Trojans present themselves as useful functions but have a hidden harmful purpose in the computer system. Other forms of malware include spywares, worms, and backdoors (Elhadi et. al, 2012).

2.4.4 Mobile Fraud

Mobile fraud is a major that faces mobile banking and threatens the integrity and security of financial data. Mobile fraud involves the manipulation of the financial systems that support mobile banking, for illegal financial gain. It involves financial deception orchestrated though the mobile banking, and can originate from the customers, agents, service providers, or system administrators (Karanja, 2017). Mobile fraud leads to financial loss for both the bank and the customer. In addition, it leads to loss of consumer trust and confidence in the bank. cases of mobile fraud causes reputational damage to the bank and negatively affects the relationships with customers (Hoffmann & Birnbrich, 2012).

2.5 Strategies and Technological Recommendations for Mitigating Mobile Banking Risks

Advancement in technology should be accompanied by enhancement in information security strategies that ensure that those who use these platforms are not exposed to vulnerabilities (Potnis et al, 2020). Several strategies have been adopted by banks to mitigate the threats associated with mobile banking. The current study explores how two factor authentication, encryption, isolation and permission-based methods have been used by commercial banks in Kenya to control the prevailing mobile banking risks.

2.5.1 Two Factor Authentication

As the use of mobile banking increases, the security and privacy threats of mobile banking through malwares, hacking, unauthorized access and mobile fraud increases. The ordinary approach of using normal passwords may no longer address the emerging risks adequately especially in securing critical applications such as online

and mobile banking, and therefore two-factor authentication helps to enhance the level of security (Bindhu et al., 2014). A study by Han (2015) to review mobile banking security in Oman shows that two factor authentication has proven to be a secure method for customer verification as it requires the customers to produce additional authentication together with their unique login identification and password. The additional information may include onetime passcode issued by onetime passcode token or received by mobile short message services, phone call, card reader or a card with random numbers. Bhindu et al. (2014) notes that this approach to authentication creates an extra level of security through secondary password authentication.

However, Mahesh et al.(2020) point out that increased security through multiple factor authentication could have negative effect on the mobile banking systems efficiency since too much information and predefined security questions and answers that needed to be remembered by customers to verify their entry into system lead to decreased perceived usability (Han, 2015). Moreover, the use of multiple factor verification should not be taken as fool proof since memorable codes can still be intercepted and used by third parties for unauthorized access or fraud. Despite this, the use of multiple factor authentication offers higher security than single login schemes.

2.5.2 Encryption

Confidentiality of data transmitted through the internet can be achieved by cryptography. According to Gangan (2015), data cryptography involves the sending of information in a format that can only be read by the intended recipient. Encryption is a process which transforms the original information into an unrecognizable form while the conversion of encrypted data into its original form is called Decryption (Gangan, 2015). The process of encrypting the data with a secret key before exchange or transmission provide another level of secure communication between the sender and

receiver (Chaki et al., 2020). This hides the confidentiality of the data and improves on the data security. Zhang et al. (2020) explains that the key role of encryption is allowing you to securely protect data that you don't want anyone else to have access to which include individuals like hackers. Encryption is advantageous because it protects the security of sensitive information and conceals its existence. Bracciali et al. (2020) notes that it is possible to have complex algorithms for encryption that enhances the level of security, without reducing the performance of the database.

According to Uddin et al. (2020), the security of transactions of a financial nature over a network and those powered by SIM Toolkit application can be enhanced through a Message Authentication Code which is obtained from a Triple DES (Data Encryption Standard) algorithm accompanying the message that is being transmitted. Ferrag (2020) further notes that SIM Application Toolkit makes it possible for the mobile banking application menu to be stored within the SIM card and then the SIM is encrypted to secure the integrity of the data.

2.5.3 Permission Based Access

Permission based access control has also been adopted by organizations as a measure to mitigate against information security risks. Through permission-based access, organizations determine the users who can access specific aspects or levels of the mobile banking infrastructure, whether it is the user interface, servers, database, or API. These permissions are based on roles that specific users have been assigned (Sanchez et al., 2017). However, the permissions are standardized for all applications, such that actions such as “Create”, “Read”, or “Delete” can only be performed by a user if they have been given that specific permission.

2.6 Summary of Literature Review

In summary, the review of existing literature reveals that the concept of mobile banking has received widespread adoption. In terms of architecture, it is evident that the main components are generally the application environment which entails the mobile banking application and a database, a mobile device which enables the users to access the application, and a network. There seems to be consensus in the literature on what the mobile banking architecture consists of, and how these elements interact in the architecture. Various researchers have also identified the technological risks that accompany the adoption of mobile banking. Sim Swaps, SSL vulnerabilities, leakage of confidential data, mobile fraud and malware attacks have been identified as common security risks facing mobile banking. An important point to note is that the risks facing mobile banking, especially malware, are continuously evolving and developing resilience towards the mitigation measures put in place by banks. This implies that banks have to continuously engage in research, monitoring and to ensure that their defences are up to date and robust enough.

2.7 Research Gap

In response to risks that arise as a result of mobile banking adoption, this study notes that banks are still implementing the mitigation measures in isolation without a holistic framework that takes into consideration aspects such as monitoring and continuous creation education of users. The review of existing theoretical and empirical literature on the existing and emerging risks facing data security in commercial banks point to continued concerted efforts by researchers to develop strategies to counter the dynamic technology-related risks facing commercial banks as a result of the widespread adoption of mobile banking. However, it is worth noting that no stand-alone solution can address the challenging and ever-changing landscape of mobile

banking-related security risks. Most researchers have identified and recommended stand-alone solutions by researching on specific risks or architectural components of mobile baking (Chikomo, Chong, Arnab & Hutchison, 2016; Baraka, Anael & Loserian, 2013; Wambua, 2012). There is need for a holistic framework that addresses all aspects such as continuous risk assessment and review, control of devices, network access controls, data protection and management, control of applications and users, education, as well as emerging approaches such as big data analytics and behavioural analytics. In addition, mobile baking security risks continue to evolve as hackers devise new and sophisticated ways of infiltrating the existing security mechanisms put in place by commercial banks. 'Traditional' security mechanisms may therefore not be enough in countering the dynamic security risks associated with mobile banking. Therefore, this study sought to address these gaps in order to contribute to the body of knowledge and also provide practical recommendations to the banking industry and other stakeholders.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the methodology for the study. Specifically, the chapter discusses the research design, the site of the study, target population, sampling, data collection, data analysis, as well as legal and ethical considerations that the study took into account.

3.2 Research Design

This report adopted a concise analysis strategy to specifically describe the challenges posed by mobile banking in Kenya and the commercial banks' approaches in resolving emerging threats and potential future threats that may arise. The scope of the present study was acceptable as the report aimed to show the situation in the industry exactly as it is. Aggarwal (2012) noted that the method also helps to analyse, interpret, compare and identify trends and relationships correctly in terms of information. Explanatory design was used to guarantee the objectivity of the analysis as it restricts the viewpoints and biases of the researcher in performing the test. The concept is also influential in gathering objective results that can be mathematically evaluated for their validity and reliability.

3.3 Research Site

The research site involved the Nairobi head offices of three banks selected from each of the three tiers, Tier 1, 2 and 3 of Kenyan commercial banks.



Figure 3-1: Bank Tier Ratings adopted from Source: Temenos, & NetGuardian (2016).

TIER 1: This includes the major old banks which have been on the business for decades and which have accrued hundreds of billions of shillings and huge customer base, which would make it nearly unlikely for them to collapse through the financial crisis. These control 49.9% of the market.

TIER 2: is a mid-cap lender. There are approximately 16 banks in the country and together, control 41.7 percent of the banking industry.

TIER 3: consists of 21 small banks controlling 8.4% of the market.

3.4 Target Population

The target population for the study was all the 42 commercial banks in Kenya. This would give a full picture of the exact situation in each bank in relation to mobile banking risks as well as strategies implemented to mitigate risks that arise as a result of mobile banking. However, due to the difficulty of reaching all the banks within a short time, the study selected one bank from each of the three tiers. Selecting a bank from each tier ensured that the unique circumstances or contextual differences of each tier were taken into consideration. Therefore, the three banks were a good representation of the entire banking industry.

3.5 Determination of Study Sample

3.5.1 Sampling Procedure

According to Mugenda and Mugenda (2003), sampling is defined as the selection process of the gathering of participants to be studied, in order to reflect the large population of people chosen. Purposive sampling was adopted for this study. The respondents were selected based on their knowledge of the subject matter of the study, which was ICT and Information Security in the context of mobile banking. The selection of the respondents was done with the help of relations officers in each of the three banks who were well versed with the roles and experience of the respondents. The purposive sample was composed of respondents from ICT, Retail, Operations and customer care departments.

3.5.2 Study Sample Size

A sample is a small group obtained from the accessible population. Each member of the sample is referred to as the subject. Sometimes the term respondent or the interviewer is used (Mugenda & Mugenda, 2003). For the sampling size, Krejcie and Morgan model was used.

$$n = \frac{X^2 * N * P * (1-P)}{(ME^2 * (N-1)) + (X)}$$

Where:

n = sample size

X^2 = Chi –the significance level set at 95% confidence interval which corresponded to value of 3.841

N = Population Size corresponding to value of 60

P = Population Proportion corresponding to value of 0.5

ME = desired Margin of Error (expressed as a proportion) corresponding to value of 0.5

$$n = \frac{3.841(60)(0.5)(0.5)}{((0.05^2)(60-1))+(3.841)(.5)(.5)}$$

$$n = 52$$

Figure 3-2: Krejcie and Morgan Model

Therefore, the sample size was 52 respondents who were purposively selected by virtue of their knowledge of mobile banking operations, ICT, and Information Security in the bank. The respondents were from the ICT, Retail, Operations and customer care departments of the three bank from within the Head offices. Table 3-1 shows the distribution of the samples.

Table 3-1 Sample Size Distribution

Bank	**Sample Size**	**Percentage**
A (Tier 1)	21	40.38
B (Tier 2)	14	26.92
C (Tier 3)	17	32.70
Total	52	100%

3.6 Data Collection

3.6.1 Data Collection Instruments

Primary data was gathered using self-administered questionnaires. In the first section, the questionnaire provided general information to the respondents about the purpose of the study, as well as issues of confidentiality and anonymity. The next four sections were arranged in accordance with the objectives of the study. Three relations officers assisted in administering the questionnaires in each of the selected banks.

3.6.2 Pilot Testing of Research Instruments

A pilot study was conducted prior to the actual collection of data in order to pre-test the questionnaire and identify and correct any errors or ambiguous questions which would have been difficult for the respondents to respond to. The researcher carried out the pilot study involving 5 respondents in one bank that was not part of the final data collection. The pilot study aimed primarily to verify that the questionnaires were appropriate and clear, that the information sought was relevant, and that the language used and the content of the answers were valid.

The results of the pilot study revealed that the respondents were able to answer the questions with ease, and that the responses were in line with the objectives. However, it was noted that some of the questions were too technical for respondents who were not from ICT departments. Respondents from operations and customer service struggled to understand the questions. To correct this, the questionnaire design was amended in such a way that non-ICT respondents were not required to respond to technical questions.

3.6.3 Instrument Reliability

According to Mugenda & Mugenda (2003), reliability of a research instrument refers to its ability to generate consistent results after carrying out several iterations. Reliability is an indicator of the dependability of the instrument in giving accurate findings. The study used the Cronbanch's Apha reliability approach to measure the reliability of the instrument, where a Cronbanch's Apha of 0.7 and above was considered adequate as per the acceptance rules fronted by George & Mallery (2003). The Cronbanch's Apha reliability estimate for the instrument was 0.774, hence the instrument met the minimum reliability requirements.

3.6.4 Instrument Validity

This is the accuracy and importance of research findings. Bryman (2011) explains how most of the data analysis findings reflect the phenomena under review. The questionnaire was subjected to review by information security and mobile banking experts who verified that the instrument adequately addressed the research questions and measured the variables.

3.6.5 Data Collection Procedure

The researcher collected data with the help of engagement officers who were selected from the ICT departments of each of the three banks. Twenty questionnaires were distributed for each engagement officer. The researcher-maintained contact with the relationship officers to follow up on the progress of data collection until completion.

3.7 Data Processing and Analysis

Analysis as described by Bryman and Bell (2015) is a process to organize data into and look for relationships between patterns, categories and descriptive units. Upon completion of the data collection process, the data was collated and checked for completeness in preparation for analysis. In addition, the data was organized into

categories to ease the analysis process and ensure that each objective was addressed at the analysis stage. Quantitative data was analysed with the help of SPSS version 26 software while qualitative data was analysed with the help of NVIVO version 12 software.

Quantitative data was analysed using descriptive statistics and inferential analysis. Descriptive statistics were useful in providing summary statistics to describe various aspects of the data by providing the measures of central tendency and dispersion such as mean, mode, standard deviation and skewness. The method of inferential analysis that was used was correlation analysis. This is because correlation analysis helps in determining the existence, strength and direction of the relationship between the study variables. Qualitative data was loaded into the NVIVO software and coded into Nodes that helped in identifying emerging themes and key words. The findings obtained from the qualitative analysis were useful in augmenting and giving further insights into the findings obtained from the quantitative analysis.

Validation of the proposed model was carried out using the expert panel method, where subjected it to a panel of ICT experts obtained from the banking and reinsurance industry. The panel consisted of three experts from the baking industry, and four from the reinsurance industry who were experienced and well versed with information security and mobile banking.

3.8 Legal and Ethical Consideration

` The study took considerable steps to mitigate any detriment to the respondents. The study made sure that the research does not have a negative effect on the respondents by ensuring that the ethical standards were followed. The researcher therefore only asked relevant questions. Information collected was used for research purposes only as emphasised. In the stud and subsequent report, names of respondents were not

mentioned. In addition, before conducting the study, the researcher sought permission to conduct the study from bank management, and also sought consent from the respondents. All the sources that do not belong to the researcher were also cited appropriately.

CHAPTER FOUR

DATA ANALYSIS AND FINDINGS

4.1 Introduction

This chapter presents interpretations and findings of the study based on the research questions. The first discusses general information. The second section provides findings from what risks arise for commercial banks in Kenya because of mobile banking. The third section discusses findings based on what strategies Kenyan banks employ to mitigate mobile banking risks.

4.2 Characteristics of the Respondents

4.2.1 Response Rate

The study utilized questionnaires with open-ended and closed-ended type of questions to collect data from the respondents. Table 4-1 shows the response rate from the three selected banks.

Table 4-1: Response Rate Table

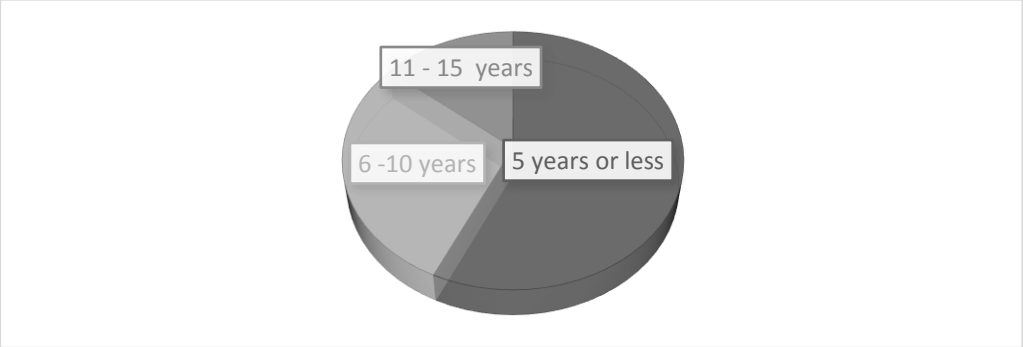
Banks	**Frequency**	**Percent**
Bank A	16	43.24
Bank B	13	35.14
Bank C	8	21.62
Total	**37**	**100**

Out of the 52 questionnaires administered, 37 questionnaires were returned with bank A recording the highest response rate with 43 % compared with bank B which recorded 35 % and Bank C recorded 21 %. The study achieved a response rate of 71%.

This response was excellent as per Mugenda and Mugenda (2003) since it postulates a response rate that is above 70% and is sufficient for analysis.

4.2.2 Work Experience

The study sought to determine work experience of the respondent. The findings revealed that 57 % of the employees have worked in the organization for less than 5 years. 29 % of have worked for 6-10 years and 14 % for 11-15 years as shown in figure 4-1.



n=52

Figure 4-1: Years of work experience of the respondents

4.2.3 Work Department

The study also collected data on the department where the respondent works. The results indicated that the department with the highest number of respondents was ICT which had 24 respondents representing 65% of the total respondents. Operations department had 6 respondents representing 14%, customer care had 5 respondents representing 16 % of the total respondents, while retail department had 2 respondents representing 5% of the total respondents.

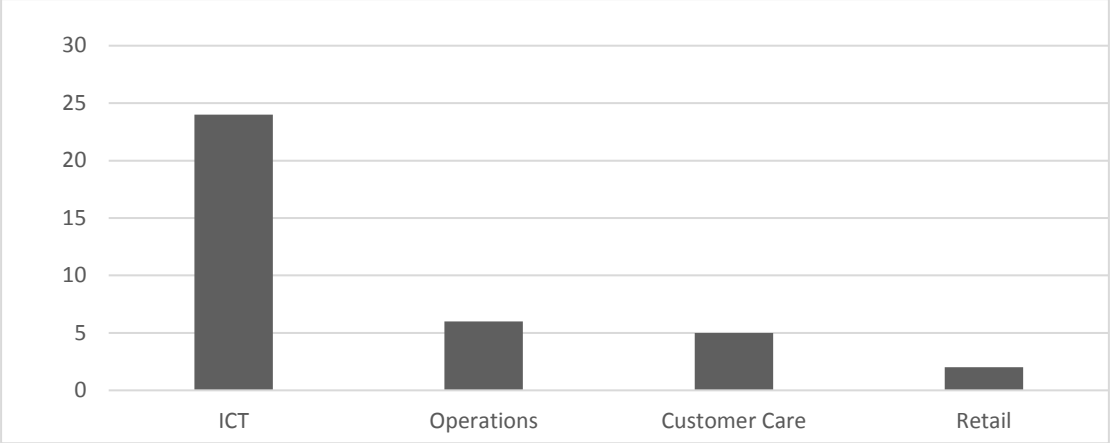


Figure 4-2: Work Department

4.2.4 Education Level

The study sought to determine level of education of the respondents. The study revealed that 51% of the respondents had a bachelor's degree, 35% had a master's degree, 14 % had a diploma and of the respondents 0 had a PHD as shown in figure 4.3. This shows the recruiting policy of banks by going after well-educated individuals.

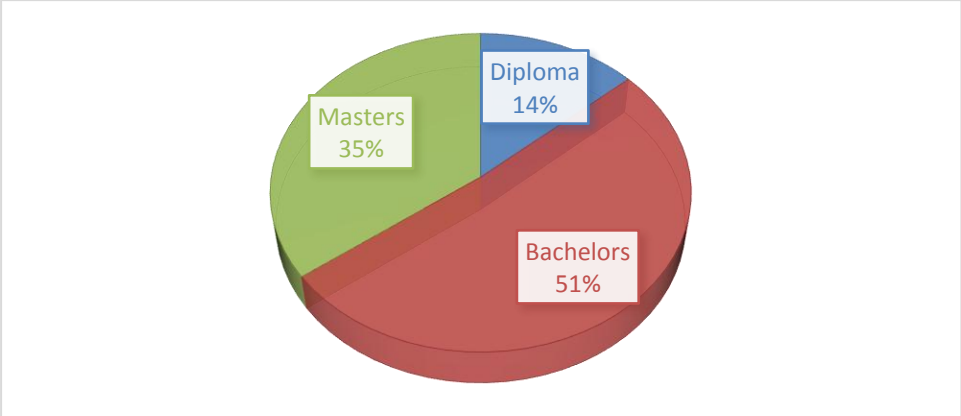


Figure 4-3: Education level of the respondents

4.3 Presentation of Research Analysis and Findings

This section presents the results obtained from the analysis of the data collected for purposes of the study.

4.3.1 Mobile Banking Architecture

The first objective of the study sought to understand the mobile banking architecture. Through the analysis done on data obtained from the respondents in the questionnaires, mobile banking consisted of various layers. Firstly, it consists of authentication level whereby users log in and their credentials are validated through two factor authentication or SMS tokens running on Java Message Service (JMS). Secondly it consists of the baseline service which consists of controller modules, core modules and user interface modules which run the whole mobile banking architecture and lastly it consisted of the User interface level which consists of the interface the Bank customer interacts with while using the mobile banking application applications which consists of services such as payments and withdrawals amongst many others.

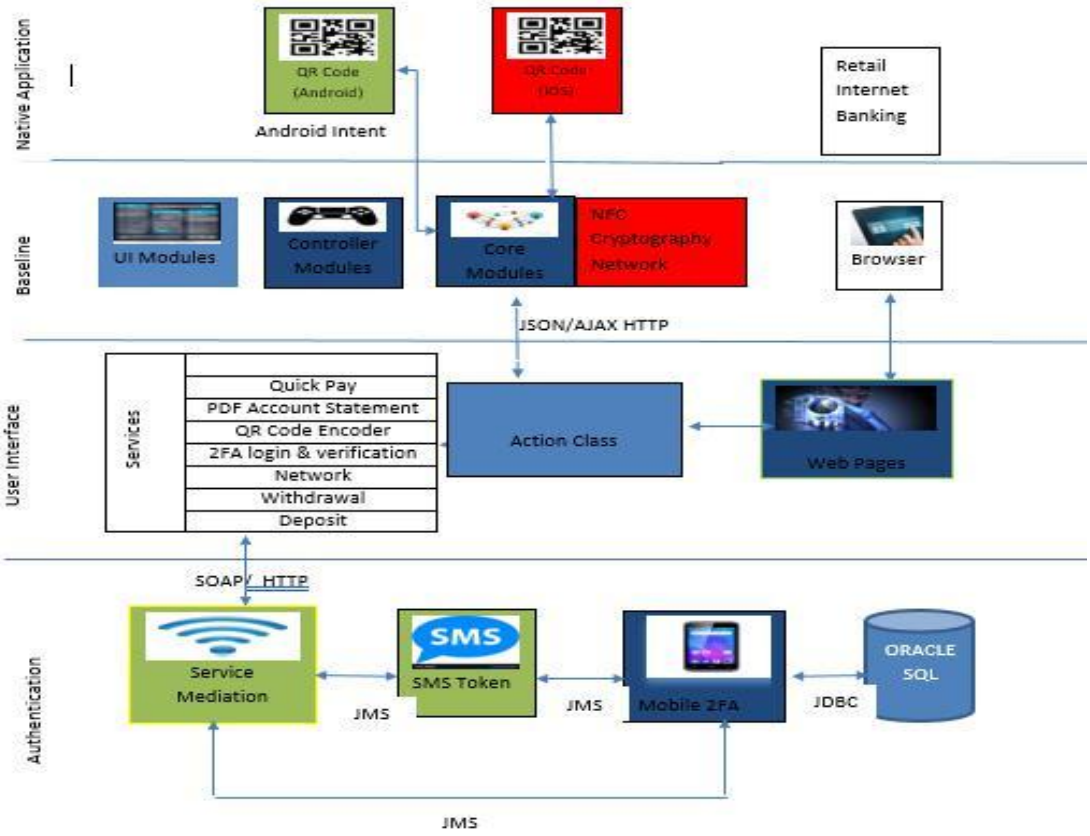


Figure 4-4 Mobile Banking Architecture

From Figure 4-4, the nodes included the type of Middleware API used, authentication mechanism, database hosting the banking platform, and type of micro edition platform supported. The word frequency in Figure 4-5 shows the most common items from the nodes.

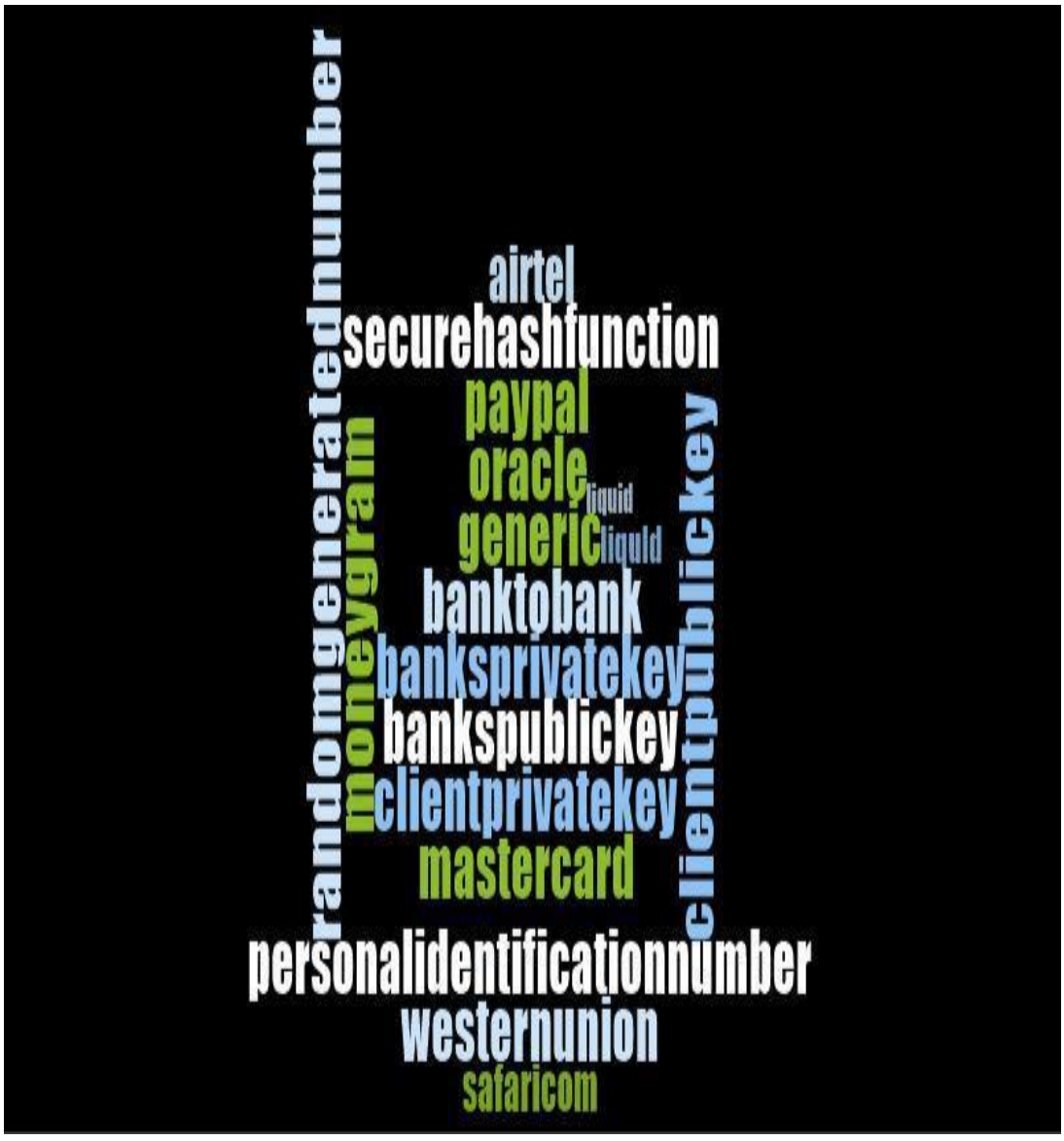


Figure 4-5: Word Frequency

From the word frequency figure 4-5 above, the most common database hosting the banking platform was Oracle, while the most common internet service providers

were Airtel, Safaricom and Liquid Telkom. In terms of the Server-side technology used, Java Http and Generic were used across the banks. The most supported external payment platforms included PayPal, Western Union, and Money Gram. Personal Identification Number, Random Generated Number, Secure Hash Function, Client Public Key, Banks Public Key, and Banks Private Key were the most commonly used authentication mechanisms. Similar findings were noted by Dmitriy et al. (2020), Trustonic Security et al. (2020) and Themistocleous & Papadakee (2013) who studied the mobile banking architecture and the security components embedded in the architecture to secure information.

4.3.2 Technological Risks Arising as a Result of Mobile Banking

The second objective of the study sought to establish the technological risks facing commercial banks in Kenya because of mobile banking. The study used a five-point Likert scale. Respondents were asked to respond to a set of questions that they were rating with the least being absolutely not (1), small degree (2), modest degree (3), large degree (4), very large degree (5).

4.3.2.1 Malware

The study sought so study the risks because of malware-related applications and malware and the findings are presented in Table 4-2 and Table 4-3.

Table 4-2 Descriptive statistics of malware

		1	2	3	4	5
Are there fake similar Mobile Banking Applications	f	9	19	9	0	0
	%	24	52	24	0	0
Have you experienced virus attack on the Mobile Banking Platform	f	19	9	8	0	0
	%	53	25	22	0	0
Have you come across toolkits which enable root level access	f	13	14	10	0	0
	%	38	35	27	0	0
Do Mobile Banking Trojans try exploiting customers accounts	f	0	4	18	8	7
	%	0	11	49	21	19

The study found that 52% of the respondents agreed that to a small degree fake mobile banking application exist, 24% agreed to a modest degree, while 24% absolutely disagreed. The respondents 25% agreed to a small degree of experiencing a virus attack on the mobile banking platform, 22% agreed to a modest degree, while 53% absolutely disagreed. The study also found out that 35% agreed to small degree of coming across toolkits which enabled root level access, 27 % to a modest degree agreed, while 38% absolutely disagreed. Lastly the Study found out that 49% modestly agreed to the existence of mobile banking Trojans which exploited customers' accounts, 21% agreed to a large degree, 19% agreed to a very large degree while 11% agreed to small degree.

Table 4-3: Means and Standard Deviations on Descriptive statistics of malware

	N	Mean	Std Deviation
Are there fake similar mobile banking applications	37	2.73	0.74
Have you experienced Virus Attack on the mobile banking platform	37	1.6	0.78
Have you come across toolkits which enable root level access	37	1.91	0.44
Do Mobile Banking trojan try exploiting customers accounts	37	3.48	0.67

The study found that majority of the respondents agreed that to a small degree that fake mobile banking application existed (M = 2.73, SD = 0.74); having experienced virus attack on the mobile banking platform (M = 1.6, SD = 0.78) and having coming across toolkits which enable root level access (M = 1,91, SD = 0.44). The respondents to a modest degree agreed to mobile banking trojans trying to exploit customers' accounts (M = 3.48, SD = 0.67). The standard deviations were less than 1 implying that the responses given by the respondents had a low variation from the mean value. This implies that the respondents had similar opinions regarding malware. The findings are supported by Luvanga (2014) which identifies malware attacks as one of the main information security risks that continue to evolve and pose a significant threat to organizations.

4.3.2.2 SSL Vulnerabilities

The study sought out to determine risk arising from the SSL Certificate and SSL in general and findings are presented in Table 4-4 and Table 4-5.

Table 4-4 Descriptive statistics of SSL vulnerabilities

		1	2	3	4	5
Have customer account credentials ever being exposed.	f	9	18	8	2	0
	%	24	49	22	5	0
Has the mbanking or internet banking exposed platform ever been exploited due to the ssl issues.	f	4	19	12	2	0
	%	12	51	32	5	0
Are the Banking platform SSL Durability ever tested	f	0	0	4	14	19
	%	0	0	11	38	51

The study found that 49% of the respondents agreed to a small degree of customers account credentials being exposed, 24% absolutely disagreed, 22% to a modest degree agreed, while 5% agreed to a large degree. Respondents 51% agreed to a small degree of the m-banking platform being exploited due to Secure Socket Layer issues, 32 % to a modest degree agreed, 12% absolutely disagreed and 5% agreed to large degree. The finding also indicated that 51% of the respondents agreed to a very a large degree of the Banking platform SSL Durability test taking place, 38% agreed to a large degree and 11% to a modest degree agreed.

Table 4-5: Means and Standard Deviations on Descriptive statistics of SSL vulnerabilities

	N	Mean	Std Deviation
Have customer account credentials ever been exposed	37	2.08	0.786
Has the mobile-banking or internet banking platform ever been exploited due to SSL Issues	37	2.32	0.89
Are the Banking Platform SSL Durability ever tested.	37	3.4	0.91

The findings indicated that the majority of respondents agreed to small degree of having customers account credentials being exposed (M = 2.08, SD = 0.786) and having the mobile banking or internet banking platform being exploited due to SSL Issues (M = 2.32, SD = 0.89). The respondents to a modest degree agreed to the Banking platform SSL Durability being tested (M = 3.4, SD = 0.91). The standard deviation obtained was small (less than 1) showing that the respondents have similar opinions on the extent of Secure Socket Layer Vulnerabilities (SSL). These findings are in line with various researchers such as Wang et al. (2020) who stated SSL vulnerabilities as one of the main information security risks that continue to evolve and pose a significant threat to organizations. Figure 4-6 and 4-7 show how the issues related to SSL vulnerabilities are depicted.

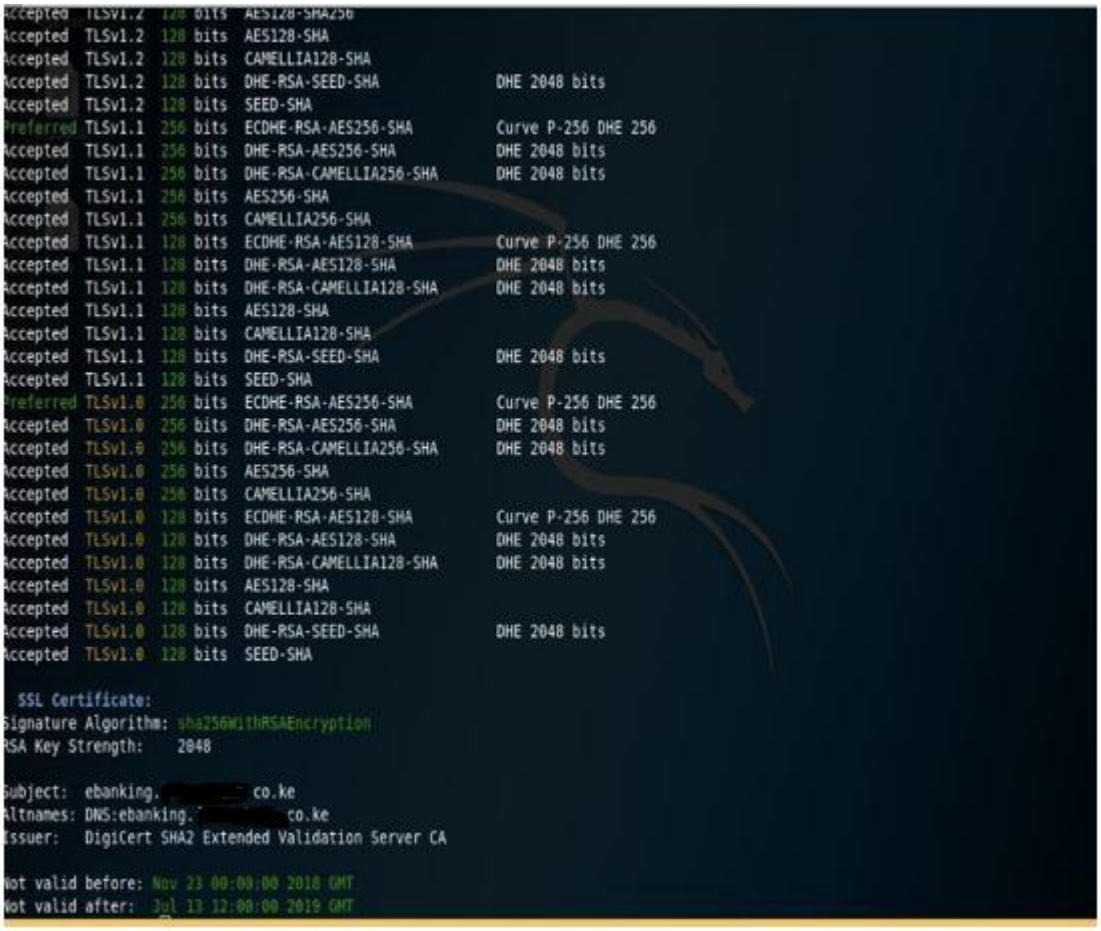


Figure 4-6: SSL Vulnerability of Bank A

Figure 4-6 depicts the current SSL certificate of Bank A. An issue of interest is the Accepted TLSV 1.0 which dates to 1999. An attacker can decrypt data exchanged between two parties by taking advantage of vulnerability in the implementation of the Cipher Block Chaining (CBC) mode in TLS 1.0. The TLS version 1.0 is displayed above currently supported in the Bank B Mobile Banking architecture which is a technological weakness.



Figure 4-7: APK Vulnerability of Bank B

4.3.2.3 Mobile Fraud

The study sought out to determine mobile fraud in commercial banks in Kenya and the findings are presented in Table 4-6 and Table 4-7.

Table 4-6: Descriptive Statistics of Mobile Fraud

		1	2	3	4	5
Criminal fraud by bank clients for financial gain	f	0	0	8	19	19
	%	0	0	22	51	27
Criminal fraud by bank agents for financial gain	f	0	2	18	7	8
	%	0	6	51	20	23
Criminal fraud by system engineers for financial gain	f	0	4	20	6	7
	%	0	11	54	16	19
Criminal deception by business partners for financial gain	f	0	15	16	7	0
	%	0	39	43	18	0

The study found that 51% of the respondents agreed that criminal fraud by bank clients for financial gain occurred to a large degree, 27% agreed to the statement to a very large degree, while 22% to a modest degree agreed. The respondents 51% to a modest degree agreed that criminal fraud by bank agents for financial gain does occur, 20% to a large degree agreed, 23% to a very large degree agreed while 6% agreed to a small degree of its occurrence. The study also found out that 54% of the respondents to a modest degree, agreed that criminal fraud by system engineers for financial gain occurred , 19% to a very large degree agreed, 16 % to a large degree agreed, while 11% to a small degree agreed. Lastly the study found that 43% agreed that criminal deception by business partners for financial gain does occur to a modest degree, 39% agreed to a small degree of its occurrence while 18% agreed to a large degree of its occurrence.

Table 4-7: Means and Standard Deviations on Descriptive Statistics of Mobile Fraud

	N	Mean	Std Deviation
Criminal Fraud by bank clients for financial gain	37	4.05	0.871
Criminal Fraud by bank agents for financial gain	37	3.41	0.87
Criminal Fraud by System engineers for financial gain	37	3.43	0.81
Criminal Deception by Business Partners for financial gain	37	2.05	0.84

The findings indicated that majority of respondents strongly agreed that criminal fraud by bank clients for financial gain occurred (M = 4.05, SD = 0.871). Majority of respondents to a modest degree agreed to Criminal Fraud by bank agents for financial gain occurring (M = 3.41, SD = 0.871); Criminal Fraud by System engineers for Financial gain occurring (M = 3.43, SD = 0.81) and Criminal Deception by Business Partners for financial gain occurring (M = 2.05, SD = 0.84). The standard deviation obtained was small less than 1 showing that the respondents have similar opinions on the extent of Mobile Fraud. The findings are in line with Luvanga (2014) who identified mobile fraud as a key vulnerability.

4.3.2.4 Other Information Security Risks/Incidents

The respondents also indicated the level of occurrence of information leakage, Distributed Denial of Service attacks, and password theft by intruders. The descriptive statistics are given in Table 4-8 and Table 4-9.

Table 4-8: Descriptive Statistics of other Information Security Incidents/Risks

		1	2	3	4	5
Information Leakage	f	0	3	12	15	7
	%	0	8	32.4	40.7	18.9
DDOS Attack	f	0	0	11	14	12
	%	0	0	29.7	37.8	32.5
Password Theft	f	2	4	14	12	5
	%	5.4	10.9	37.8	32.4	13.5

The findings revealed that 40.7 % of the respondents largely agreed that information leakage had occurred as a result of mobile banking, 32.4% agreed to a modest degree, 18.9 % to a very large degree, while 8% agreed to a small degree. Another 37.8% of the respondents agreed to large extent that the mobile banking platforms had been affected by Denial of Service attacks, 32.5 % agreed to a very large degree agree to the statement, while 29.7% agreed to a modest degree. In terms of password theft, the largest percentage of the respondents (37.8%) indicated that password theft had occurred to a modest degree, 32.4 % agreed to a large extent, 13.5% agreed to a very large extent, while 5.4% absolutely disagreed with the statement.

Table 4-9: Means and Standard Deviations on Descriptive Statistics of other Information Security Incidents/Risks

	N	Mean	Std Deviation
Information Leakage	37	3.7	1.32
DDOS Attack	37	4.02	1.87
Password Theft	37	3.86	1.78

The findings of the study indicate that the majority of the respondents to a large extent agreed that information leakage had occurred as a result of mobile banking (M = 3.70, SD = 1.32) and that the mobile banking platforms had been affected by Denial of Service attacks (M = 4.02, SD = 1.87). The respondents also agreed to a modest degree that password theft had occurred to a modest degree (M = 3.86, SD = 1.78).

4.3.2.5 Number of Security Risks/Incidents

Table 4-10 shows the number of mobile banking security risks that occurred in the between 2018 and 2019 based on the data collected by the study.

Table 4-10: Number of Information Security Risks/Incidents

	Bank A	Bank B	Bank C
Information Leakage	7	11	4
Denial of Service Attacks	3	8	14
Mobile Fraud	5	7	2
Customer Impersonation	19	6	2
Malware Attacks	27	11	7
Password Theft	2	1	4
Total	63	44	33

4.3.4 Objective 3: General ICT Controls Kenyan Banks Employ to Mitigate Mobile Banking Risks

The third objective of the study sought to establish General ICT Controls that Kenyan banks employ to mitigate mobile banking risks. The study used a five-point Likert scale. Respondents were asked to respond to a set of questions that

they were rating with the least being Absolutely not (1), Small Degree (2), Modest Degree (3), Large Degree (4), Very Large Degree (5).

4.3.4.1 Two Factor Authentication

The study sought out to determine technological strategies used to mitigate mobile banking risk. The findings are presented in Table 4-11 and Table 4-12.

Table 4-11: Descriptive Statistics of Two Factor Authentication

		1	2	3	4	5
Use of one-time SMS verification codes together with the normal PIN	f	0	0	9	10	18
	%	0	0	24	27	49
Use of random numbers together with the normal PIN	f	10	4	12	14	0
	%	25	10	30	35	

The study found that in regards to two factor authentication, 49% of the respondents agreed to a very large degree that the use of one time SMS verification together with the Normal Pin happens, 27 % agreed to a large degree, while 24% agreed to a modest degree. Respondents 35% agreed that use of random numbers together with the normal pin does occur to a large degree, 30% to a modest degree agreed, 25% absolutely disagreed while 10% agreed to a small degree. These findings are in agreement with those of various researchers including Peake (2017), Bindhu, Chen and Tavares (2014) who noted that the use of two-factor authentication provides an extra layer of protection that makes it difficult for intruders to access the application.

*Table 4-12***:** *Means and Standard Deviations* of Two Factor Authentication

	N	Mean	Std Deviation
Use of one-time SMS Verification codes together with the normal PIN	37	4.24	1.8
Use of Random numbers together with the normal PIN	37	2.97	1.47

The findings indicated that the majority of respondents to a very large degree agreed that use of one-time SMS Verification codes together with the normal PIN occurred (M = 4.24, SD = 1.8). The respondents to a large degree also agreed that use of Random numbers together with the normal PIN occurred. (M = 2.97, SD = 1.47).

4.3.4.2 Encryption

The study also sought to determine the level of use of encryption by the commercial banks. Findings are presented in Table 4-13 and Table 4-14.

Table 4-13 Descriptive Statistics of Encryption

		1	2	3	4	5
Use of SIM application Tool kit for PIN encryption	f	14	8	7	0	8
	%	38	22	18	0	22
Data encryption usage to avoid data misuse	f	0	0	10	8	19
	%	0	0	27	22	51
Data encryption usage achieving higher security	f	0	0	11	18	8
	%	0	0	22	49	29

The study found that 38% absolutely disagreed to the use of sim application tool kit for pin encryption, 22% agreed to a small degree, 22% agreed to a large degree and 18% to a modest degree agreed. Respondents 51% agreed that data encryption usage to avoid data misuse occurred to a very large degree, 27% to a modest degree agreed and 22% agreed to large degree. The study also found that 49% agreed to a large degree that data encryption usage achieving higher security levels occurred, 29 % agreed to a very large degree while 22% modestly agreed. The importance of encryption as identified in the findings, also reflects the works of Chaki et al (2012), Zhang et al(2020), as well as Kaur and Kumari (2014) who posit that when combined with other security measures, encryption plays a pivotal role in securing data from malicious attacks by guarding the confidentiality of the data.

Table 4-14: Means and Standard Deviations on Descriptive Statistics of Encryption

	N	Mean	Std Deviation
Use of SIM Application Tool Kit for PIN encryption	37	2.43	1.2
Data encryption usage to avoid data misuse	37	4.02	1.95
Data encryption usage achieving higher security levels	37	3.98	1.84

The findings indicated that the majority of respondents strongly agreed to Use of SIM Application Tool Kit for PIN encryption occurring (M = 2.43, SD = 1.2). The Respondent also agreed to a very large degree that Data encryption usage to avoid data misuse occurred (M = 4.02, SD = 1.95) and also agreeing to a large degree that Data encryption usage achieving higher security levels occurred (M = 3.98, SD = 1.84).

4.3.4.3 Permission Based Access

The study sought out to determine the level permission and warnings in regard to the application and findings are presented in Table 4-15 and Table 4-16.

Table 4-15 Descriptive Statistics of Permission Based Access

		1	2	3	4	5
Use of time use systems which prompt users to approve permissions as needed by applications at runtime	f	0	4	7	17	9
	%	0	11	19	46	24
Use of systems that warn end users what permission the mobile application will have access to such as user location, private information, depository, hardware and system information amongst	f	0	0	14	16	7
	%	0	0	38	43	19
Use of dangerous warnings introduced at the installation stage of each mobile application	f	0	4	16	12	5
	%	0	11	43	32	14

The study found that 46% of the respondent agreed to a large degree that Use of time use systems which prompt users to approve permissions as needed by applications at runtime occurred, 24% agreed to a very large degree, 19% to a modest degree agreed, while 11% agreed to small degree. Respondents 43% agreed to a large degree that use of systems that warn end users what permission the mobile application will have access to such as user location, private information, depository, hardware and system information amongst others occurred, 38% to a modest degree agreed and 19% agreed to a very large degree.

The study also found that 43% to a modest degree agreed that use of dangerous warnings introduced at the installation stage of each mobile occurred, 32% agreed to a large degree, 14% agreed to a very large degree while 11% agreed to a small degree. Studies by Benabied et al (2013) and Peake (2017) also identified permission-based access as an important component of the mobile banking security system because it prevents unauthorized persons from intruding the system.

Table 4-16: Means and Standard Deviations on Descriptive Statistics of Permission Based Access

	N	Mean	Std Deviation
Use of time use systems which prompt users to approve permissions as needed by applications at runtime	37	3.83	1.69
Use of systems that warn end users what permission the mobile application will have access to such as user location, private information, depository, hardware and system information	37	3.83	1.34
Use of Dangerous warnings Introduced at the installation stage of each mobile application	37	3.49	1.74

The findings indicated that the majority of respondents to a large degree agreed that Use of time use systems which prompt users to approve permissions as needed by applications at runtime occurred(M = 3.83, SD = 1.69) and Use of systems that warn end users what permission the mobile application will have access to such as user location, private information, depository, hardware and system information (M = 3.83, SD = 1.34). The finding also found that majority to a modest degree agreed that use of dangerous warnings introduced at the installation stage of each mobile occurred (M = 3.49, SD = 1.74).

4.3.4.4 Use of Biometrics

The study also sought to establish the level of use of biometrics as a risk mitigation measure in the context of mobile banking. The findings are presented in table 4-17.

Table 4-17: Descriptive Statistics of the use of Biometrics

		1	2	3	4	5
Adoption of physiological characteristics such as face, fingerprint, hand-geometry, ear, iris, retina, palm print for mobile banking customer identification	f	21	8	0	8	0
	%	56.8	21.6	0	21.6	0
Adoption of behavioural traits such as voice, gait, keystroke dynamics for mobile banking customer identification	f	27	10	0	0	0
	%	72.9	27.1	0	0	0
Adoption of multimodal functionality, which combines several biometric recognition methods for mobile banking customer identification	f	0	14	16	7	0
	%	0	37.9	43.2	18.9	0

The study found out that respondents 56.8 % agreed to a large degree that Adoption of physiological characteristics such as face, fingerprint, hand-geometry, ear, iris, retina, palm print for mobile banking customer identification did not occur at all, 21.6% agreed it occurred in little extent, while 21.6 agreed to a large degree of it happening. The respondents 72.9% agreed to a large degree that Adoption of behavioural traits such as voice, gait, keystroke dynamics for mobile banking customer identification did not occur at all while 27.1 % agreed it occurred in small degree.

Lastly, majority of respondents 43.2% to a modest degree agreed that adoption of multimodal functionality, which combines several biometric recognition methods for mobile banking customer identification occurred , 37.9% agreed to small degree of its occurrence and 18.9% agreed to a very great degree of its occurrence. The results of this study are therefore in line with those of He, Tian, & Shen (2015) and Hossain (2020) whose research posits that these emerging approaches to information security risks are the game-changer in modern banking.

Table 4-18: Means and Standard Deviations on Descriptive Statistics of the use of Biometrics

	N	Mean	Std Deviation
Adoption of physiological characteristics such as face, fingerprint , hand-geometry, ear, iris, retina, palm print for mobile banking customer identification	37	1.86	1
Adoption of Behavioural traits such as voice, keystroke dynamics for mobile banking customer identification	37	1.27	0.28
Adoption of multimodal functionality, which combines several biometric recognition methods for mobile banking customer identification	37	2.81	1.78

The findings indicated that the majority of respondents to a large degree agreed that Adoption of physiological characteristics such as face, fingerprint , hand-geometry, ear, iris, retina, palm print for mobile banking customer identification occurred (M = 1.86, SD = 1) and Adoption of Behavioural traits such as voice, keystroke dynamics for mobile banking customer identification occurred (M = 1.27, SD = 0.28). Lastly, majority of respondents to a modest degree agreed that adoption of multimodal

functionality, which combines several biometric recognition methods for mobile banking customer identification occurred (*M* = 2.81, *SD* = 1.78).

4.3.4.5 Use of Behavioural Analysis

The study sought to find out the level of behavioural analysis used within mobile banking as a risk mitigation measure. The findings are presented in Table 4-19 and Table 4-20.

Table 4-19: Descriptive Statistics of the use of Intelligent Behavioural Monitoring and Analysis Technology

		1	2	3	4	5
Use of inductive reasoning for detecting abnormal customer behaviour	f	0	2	10	8	17
	%	0	5.5	27.0	21.6	45.9
Use of cognitive control system to override seemingly obvious but incorrect customer information	f	6	20	11	0	0
	%	16.3	54	29.7	0	0
Use of numerical systems to detect faults in customer behaviour	f	14	16	7	0	0
	%	37.8	43.3	18.9	0	0
Use of artificial intelligence to forecast behaviour	f	9	19	9	0	0
	%	24.3	51.4	24.3	0	0

The findings revealed that 45.9% agreed to a very large degree to use of inductive reasoning for detecting abnormal customer behaviour occurred, 21.6% agreed to a large degree, 27% to a modest degree, while 5.5% agreed to small degree. In addition, 54% of the respondents agreed that use of cognitive control system to override seemingly obvious but incorrect customer information occurred to small degree, 29.7% agreed to modest degree of its occurrence while 16.3% agreed it absolutely did not occur at all.

The findings also revealed that 43.3% agreed that use of numerical systems to detect faults in customer behaviour occurred to a small degree, 37.8% agreed it absolutely did not occur at all, while 18.9 % to a modest degree agreed to its occurrence. The findings also indicated that 51.4% agreed to small degree to use of artificial intelligence to forecast behaviour occurring, 24.3% agreed to a modest degree and 24.3% indicated that it did not occur at all.

Table 4-20: Means and Standard Deviations on Descriptive Statistics of the use of Intelligent Behavioural Monitoring and Analysis Technology

	N	Mean	Std Deviation
Use of Inductive reasoning for detecting abnormal customer behaviour	37	4.08	0.22
Use of Cognitive control system to override seemingly obvious but incorrect customer information	37	2.14	0.91
Use of numerical systems to detect faults in customer behaviour	37	1.81	0.88
Use of artificial intelligence to forecast behaviour	37	2.00	0.10

The findings indicated that the majority of respondents to a very large degree agreed to Use of Inductive reasoning for detecting abnormal customer behaviour (M = 4.08, SD = 0.22); The respondents also agreed to a small degree that use of cognitive control system to override seemingly obvious but incorrect customer information was used (M = 2.14, SD = 0.91); use of numerical systems to detect faults in customer behaviour was also used (M = 1.81, SD = 0.88) and use of artificial intelligence to forecast behaviour occurred (M = 2.00, SD = 0.10). The standard deviations were less than 1 implying that the responses given by the respondents had a low variation from the mean value. This implies that the respondents had similar opinions regarding behavioural analysis within banks. The results of this study are therefore in line with

those of He, Tian, & Shen (2015) and Hossain (2018) whose research posits that these emerging approaches to information security risks are the game-changer in modern banking.

4.3.5 Correlation Analysis

4.3.5.1 Correlation between Strategies to Mitigate Mobile Banking Risks and Occurrence of Mobile Banking risks

Table 4-21: Output of Correlation between Strategies to Mitigate Mobile Banking Risks and Occurrence of Mobile Banking risks

Correlations				
			Strategies_to_Mitigate_Mobile_Banking_Risks	Occurence_of_Mobile_Banking_Risks
Spearman's rho	Strategies_to_Mitigate_Mobile_Banking_Risks	Correlation Coefficient	1.000	-.731**
		Sig. (2-tailed)	.	.001
		N	37	37
	Occurence_of_Mobile_Banking_Risks	Correlation Coefficient	-.731**	1.000
		Sig. (2-tailed)	.001	.
		N	37	37
**. Correlation is significant at the 0.01 level (2-tailed).				

The Spearman's correlation coefficient (rho) between Strategies to Mitigate Mobile Banking Risks and Occurrence of Mobile Banking Risks as shown in table 4.21 above is -0.731 and is statistically significant at 99% level of significance (p-value is 0.001 which is less than 0.01). This implies that there is a negative and statistically significant

relationship between the two variables, and therefore, existence of robust strategies to mitigate against mobile banking risks reduces the likelihood of occurrence of mobile baking information security risks.

4.3.5.2 Correlation between Strategies to Mitigate Mobile Banking Risks and Number of Mobile Banking Risks

Table 4-22: Output of Correlation between Strategies to Mitigate Mobile Banking Risks and Number of Mobile Banking risks

Correlations				
			Strategies_to_Mitigate_Mobile_Banking_Risks	Number of Risks
Spearman's rho	Strategies_to_Mitigate_Mobile_Banking_Risks	Correlation Coefficient	1.000	-.827*
		Sig. (2-tailed)	.	.039
		N	37	37
	Number of Risks	Correlation Coefficient	-.827*	1.000
		Sig. (2-tailed)	.039	.
		N	37	37
*. Correlation is significant at the 0.05 level (2-tailed).				

The Spearman's correlation coefficient (rho) between Strategies to Mitigate Mobile Banking Risks and Number of Mobile Banking Risks as shown in table 4-22 above is -0.827 and is statistically significant at 95% level of significance (p-value is 0.039 which is less than 0.05). This implies that there is a negative and statistically significant

relationship between the two variables, and therefore, the more robust the strategies to mitigate mobile banking risks, the lower the number of risks that occur.

4.3.5.3 Correlation between Strength of Risk Mitigation and Number of Mobile Banking Risks

Table 4-23: Output of Correlation between Strength of Risk Mitigation and Number of Mobile Banking risks

Correlations				
			Risk_Mitigation_Strength	Number of Risks
Spearman's rho	Risk_Mitigation_Strength	Correlation Coefficient	1.000	-.697*
		Sig. (2-tailed)	.	.018
		N	37	37
	Number of Risks	Correlation Coefficient	-.697*	1.000
		Sig. (2-tailed)	.018	.
		N	37	37
*. Correlation is significant at the 0.05 level (2-tailed).				

The Spearman's correlation coefficient (rho) between the Strength of Risk Mitigation and Number of Mobile Banking Risks as shown in table 4-23 above is -0.697 and is statistically significant at 95% level of significance (p-value is 0.018 which is less than 0.05). This implies that there is a negative and statistically significant relationship between the two variables, and therefore, the stronger the level of risk mitigation, the lower the number of risks associated with mobile banking. The results of the correlation analysis indicated that a higher level of robustness in strategies implemented to mitigate against mobile banking risks is associated with a lower likelihood of occurrence of mobile banking risks. The results reflect the findings of Luvaga (2014), Accenture

(2017) and Benabied, (2013) whose studies also revealed a positive link between mobile banking -security vulnerabilities and the presence of a robust security mechanism that address all aspects of mobile banking information security.

CHAPTER FIVE

DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the findings established from the data analysis done and summarizes the findings. Subsequently, the findings are also discussed in full of relevant literature to support the results established. Thus, the chapter entails the discussion and conclusions as well as recommendations for further studies.

5.2 Discussions

5.2.1 Mobile Banking Architecture

The first research question that the study sought to answer was the composition of the mobile banking platform. The study found that the main components that make up the architecture of the platform include a database (Oracle was the most commonly used), a J2ME (Java 2 Platform, Micro Edition) Mobile Information Device Application which resides on the mobile phone, Servlets (Java Http and Generic), a receiver server in the bank, internet, external payment systems, and an authentication mechanism. The findings reflect those of Garg (2012) who conducted a study on mobile banking applications and noted that the application's components include the user interface segment, data access segment, and the domain logic. The general architecture comprises of the mobile application, a J2ME midlet which carries out processing on the client's mobile phone, a J2EE (Java Platform, Enterprise Edition) servlet residing in the bank, authentication system, and a database. Themistocleous and Papadakē (2013) also had similar findings, but went further to categorize these components into seven key areas namely the client's mobile device (Containing the application and midlet), distribution network (Wi-Fi, or mobile data), communication gateway between

the bank and the client e.g SMS and Http Web Servers, the mobile application , integration platforms and finally, the core banking platform where the data resides. The findings also agree with those of Dmitriy et al. (2020) as well as Trustonic Security (2020) who posit that a mobile banking platform comprises of a user, mobile application, authentication mechanism, a network, a receiver server at the bank which processes the request, and a database.

5.2.2 Technological Risks arising for Kenyan Commercial Banks because of Mobile Banking

From the findings, it was evident that commercial banks continued to face significant information security risks as a result of mobile banking. Malwares, SSL vulnerabilities, SIM swap, Virus attacks, and people-related risks continue to threaten the security of information stored by banks. This reflects the findings of Luvaga (2014) and He, Tian, & Shen (2015) who also identified malwares, device vulnerabilities, application vulnerabilities, unsecure networks, phishing, and user vulnerabilities as the main risks that can compromise the security and integrity of data in the mobile banking platform. Unauthorized access to sensitive customer data may have serious consequences which may include financial losses, litigation and loss of customer trust (Peake, 2017).

Benabied et al (2013) notes that when the vulnerabilities are exploited because of weak controls, significant attacks may be launched on the mobile banking platform. In addition to malware, virus attacks, SSL vulnerabilities, fraud, and root-level access, Kaya identified social engineering attacks, distributed denial of service, loss of sensitive data and rootkit attacks as information security risks associated with mobile banking. These also reflect the findings of (Molina-Castillo et al, (2017). SIM swaps, Trojans, skimming, interception of SMS and phishing were noted to be common risks and vulnerabilities in studies conducted by Barclays (2016) and Dagada (2013). The

findings therefore reflect the fact that as reported in the existing literature, mobile banking risks are evident and continue to threaten the security and integrity of data if robust control strategies are not implemented.

5.2.3 ICT General Controls Kenyan Commercial Banks use to Mitigate against Mobile Banking Risks

In terms of controls, the findings indicate that controls such as Personal Identification Numbers, data encryption, access controls, warning systems, biometric systems and SMS verifications were commonly used by banks to prevent or detect unauthorized access to sensitive information. Peake (2017) studied the IS risks facing Kenyan commercial banks mobile banking platforms and identified similar mitigation strategies. In addition, Peake (2017) stressed on the importance of two-factor authentication in preventing unauthorized access, and data isolation in ensuring that sensitive data is not compromised. Bindhu, Chen and Tavares (2014) also concurred with the use of two-factor authentication because it provides an extra layer of protection that makes it difficult for intruders to access the application. Similar to the findings of this study, Luvaga (2014) concludes that traditional security mechanisms only can no longer guarantee the safety and integrity of data in the dynamic mobile banking landscape. The proliferation of devices and the urge by users to jailbreak the devices makes it difficult to address the security risks using normal mechanisms only.

The study further found that there was low adoption of new advanced technologies such as Intelligent Behavioural Monitoring and Analysis, and Advanced Big Data Analytics. These emerging mechanisms can enable organizations to analyse, monitor, predict, and prevent many risks associated with mobile banking (He, Tian, & Shen, 2015). Given the dynamic nature of risks facing the mobile banking platform, banks have an opportunity to leverage on the unique strengths of these technologies in

combination with other technological and non-technological measures to enhance the security of the mobile banking platform.

From the correlation analysis, there was a negative and statistically significant correlation between the level of robustness of risk mitigation strategies and occurrence of mobile banking risks. This implies that when the technological and non-technological strategies are properly implemented, say through a holistic and robust model, the control or mitigation of mobile banking risks is improved, and hence the occurrence of the risks is minimal (Luvaga, 2014; Accenture, 2017; Benabied, , 2013).

5.2.4 Mobile Banking Risk Mitigation Model

The development of the risk mitigation model for mobile banking risks was based on a review of the existing literature. From the existing literature, the study identified the existing models and recommended components of a good risk mitigation model to address the dynamic information security risks facing mobile banking platforms. Luvaga (2014) identified key control mechanisms against the ever-dynamic mobile banking risks. According to his study, mapping out and understanding the specific threat is a key component that helps organizations to prepare, monitor, and stop attacks. This also provides insights and predictive information that helps in mitigating the risk. The study also identified that implementing security layers for defence makes it difficult for attackers to intrude the platform. This multi-layered defence approach could include components such as Intrusion Detection Systems, firewalls, malware detection and protection, continuous monitoring and evaluation, patch management, implementing Public Key Infrastructure (PKI), use of encrypted protocols, securing interactions with the server, authentication mechanisms such as two-factor or one-time code, as well as confidentiality and data integrity controls such as SSL and TLS. Based

on these components, Luvaga (2014) proposed the following model in figure 5-1 below.

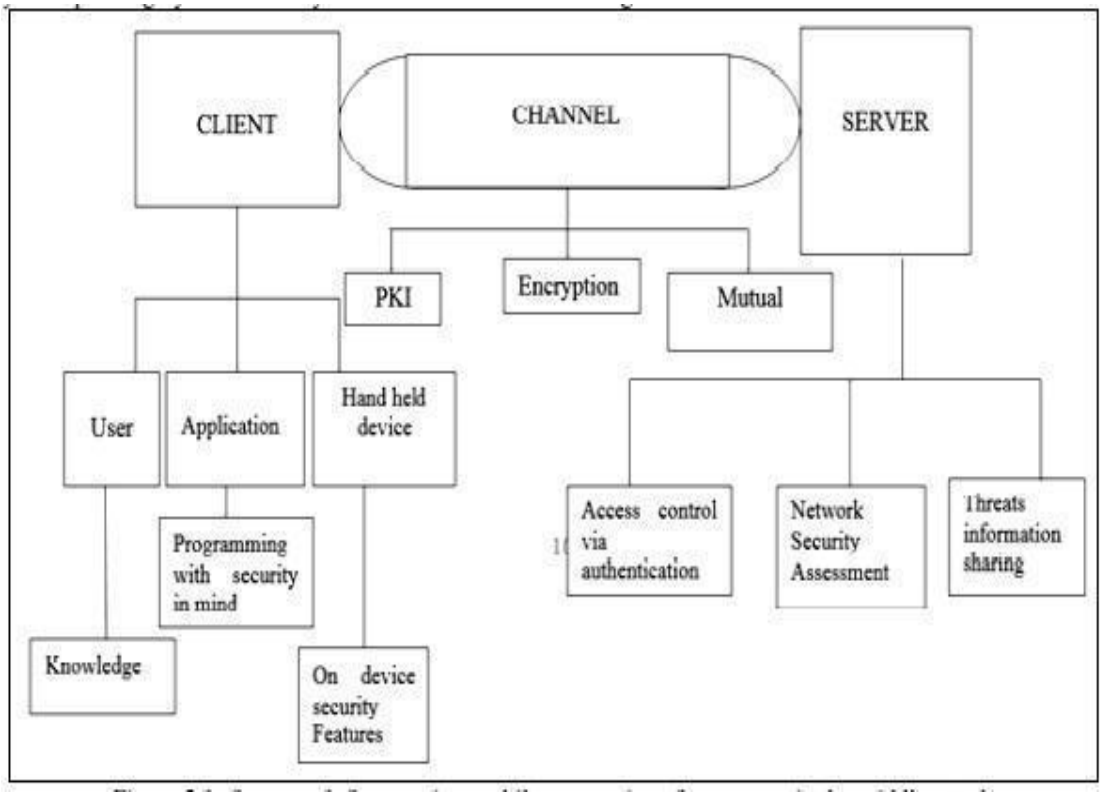


Figure 5-1: Risk Mitigation Model Proposed by Luvaga (2014)

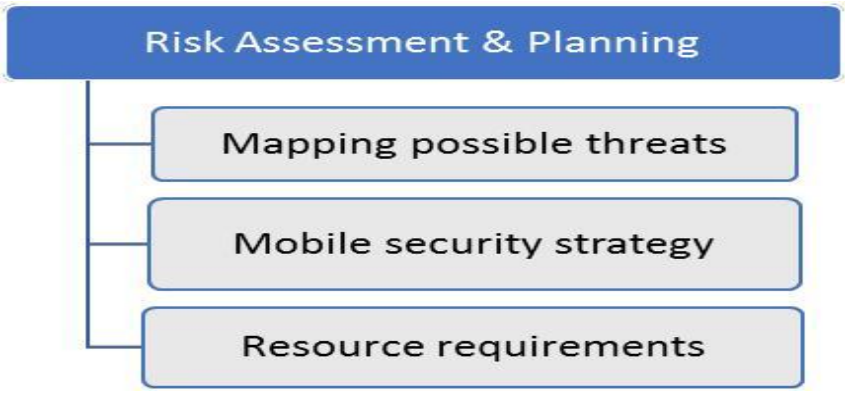
Otonchi and Kakamanshadi (2010) also studied the security of mobile banking and recommended that key components for securing mobile banking included rapid response and recovery systems, firewalls, Intrusion Detection System, encryption and coding, testing integrity of the systems, digital signatures and continuous monitoring. Accenture (2017) also highlighted the key elements that organizations should focus on when implementing security measures for mobile banking platforms. These include the device-related controls, controls on the organization's network, data protection, application controls, managing user access, and implementing strict IS governance and ensuring compliance. It is also important to have an integrated plan for mobile banking security that incorporates the mobile security strategy, resource requirements, and

mapping to business needs. In a study on mobile banking risks facing commercial banks in Kenya, Peake (2017) identified two-factor authentication, cryptography, isolation and permission-based access controls as the main strategies to mitigate against mobile banking security risks.

In a study that examined the security risks and mitigation measures for mobile banking risks, He, Tian, and Shen (2015) categorized their recommendations into best practices for users, application developers and banking institutions. For users, best practices include avoiding jail breaking their phones, avoiding download of mobile banking applications from third parties, use of secured networks, one-time passwords, updating the mobile Operating System (OS) as well as the mobile banking app, and consistent use and update of trusted anti-virus software. Developers and administrators should implement secure transfer protocols, SSL certification and validation, encryption of data, detection and prevention of rooting or jail breaking, security logs and analysis, and removal of older versions of the banking application which may be vulnerable to attacks. Emerging security mechanisms such as biometric identification (facial, voice, and fingerprints), intelligent behavioural monitoring and analysis technology, using big data analytics are also highly recommended to be used in conjunction with the other technological and non-technological strategies.

Having consolidated the components discussed above, this study proposed the following integrated framework which is based on eight pillars namely, Risk assessment and planning, Device controls, Network access controls, Data protection and management, Application controls, Users, Monitoring and Evaluation, and Continuous education/awareness. Figure 5-2 below depicts the model.

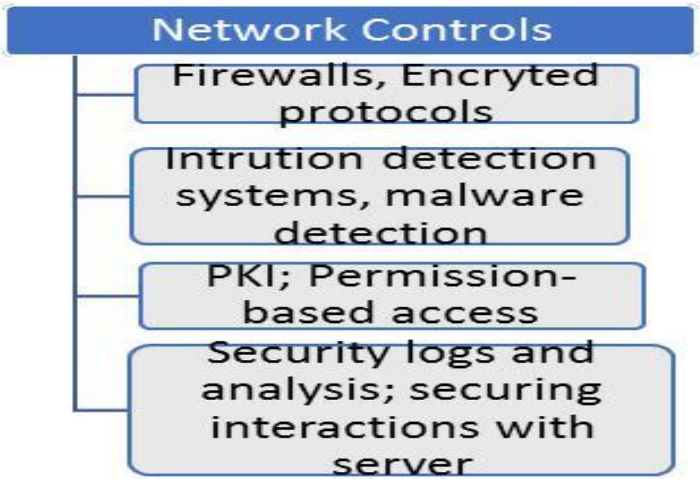
Pillar 1:



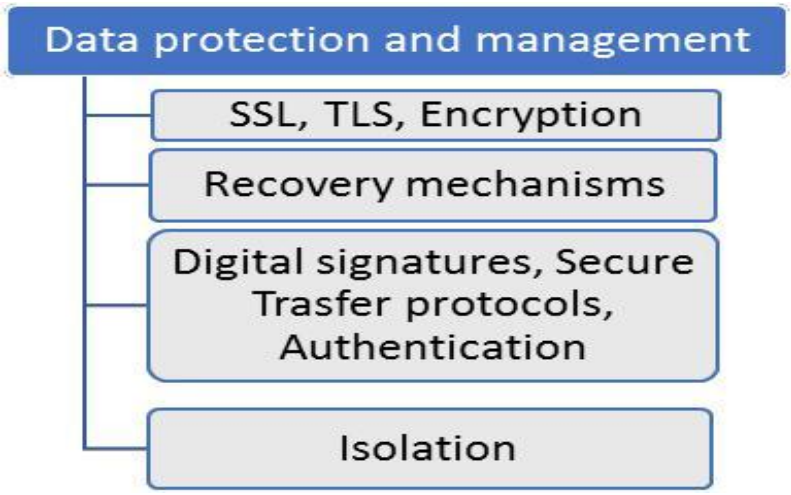
Pillar 2:



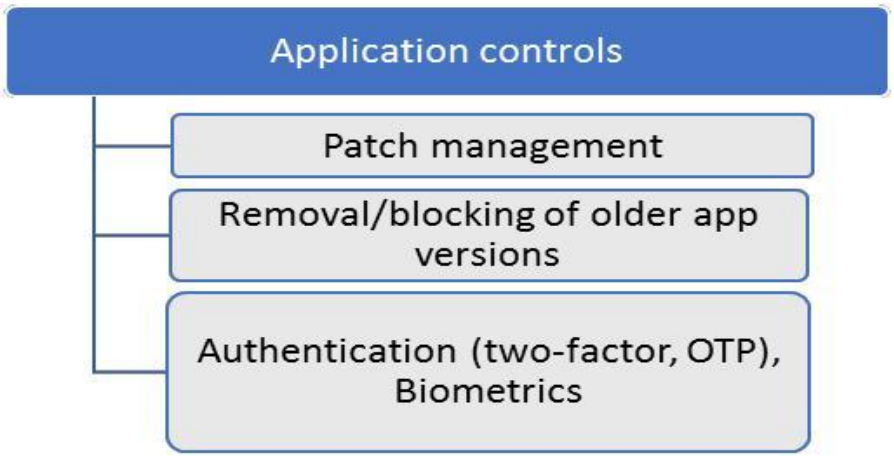
Pillar 3:



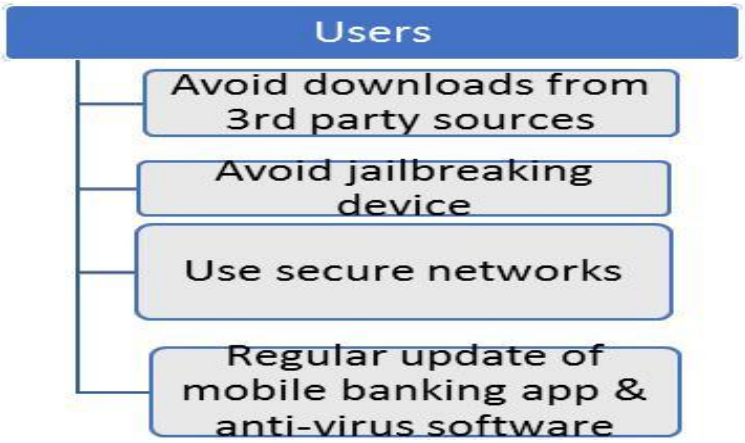
Pillar 4:



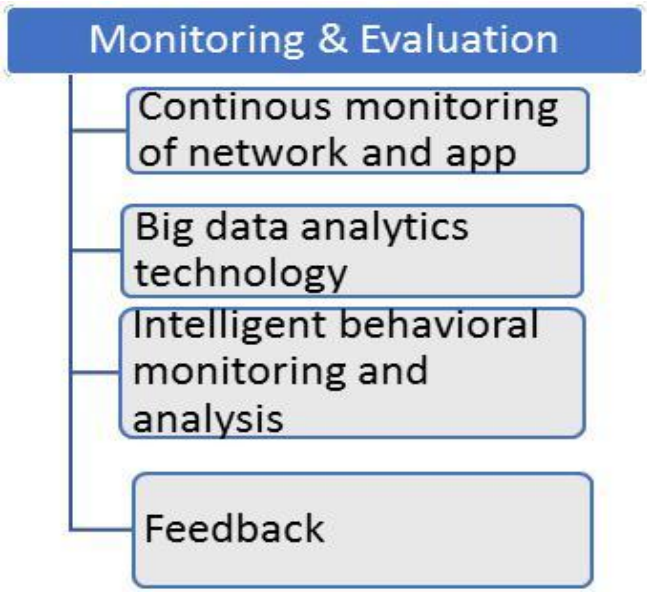
Pillar 5:



Pillar 6:



Pillar 7:



Pillar 8:

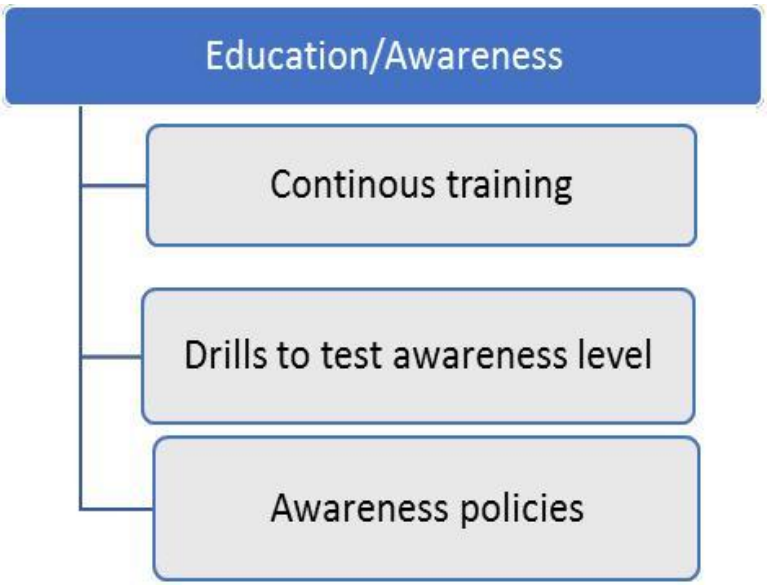


Figure 5-2 Proposed Mobile Banking Risk Mitigation

5.2.4.1 Validation of the Model

In order to validate the model, the study subjected it to a panel of ICT experts obtained from the banking and reinsurance industry. The ICT experts were experienced individuals in the field of information security. The panel consisted of three experts from the baking industry, and four from the reinsurance industry.

In validating the model the study considered the elements of a good mobile banking security model suggested by Luvanda (2014). At the client level, Luvanda (2014) suggested that the model should entail user education in order to create awareness on the possible security risks and how to avoid them at the user level. It should also entail robust application-level security features including authentication mechanisms, transaction limits, and programming that takes security into serious consideration. At the device level, security features such as passwords, firewalls, antivirus protection, and data wiping capability.

The communication channel should also be secured by encrypting data transmitted through the channel. PKI, TSL and SSL should also be adequately and effectively implemented. At the sever level, there should be robust access control mechanisms to prevent unauthorized access. The network should also be effectively managed and continuously monitored. Table 5-1 shows the scores given by the panel of ICT experts.

Table 5-1: Model Validation Scores

Scores out 10								
Focus area	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5	Expert 6	Expert 7	Average
Awareness	9	8	10	9	9	10	8	9
Application-level security	9	7	7	8	9	9	9	8.3
Device-level security	10	8	8	9	8	7	6	8
Communication channel security	5	8	7	7	5	6	5	6.1
Server-level security	10	9	8	9	9	10	10	9.3
Network	10	10	9	10	10	8	9	9.4

From the validation results in table 5-1, it can be concluded that based on the ICT experts' opinions, the model meets the requirements of a good mobile banking security model.

5.3 Conclusion

In the first objective, the study aimed at establishing the components of a mobile banking architecture. Based on the findings, the study concludes that they key components of a mobile banking architecture include a database, Mobile Information Device Application which resides on the user's mobile phone, Servlets, a receiver server in the bank, internet, external payment systems, authentication mechanism, and a network. The study therefore achieved its first objective.

The second objective of the study was to establish the technological risks arising for commercial banks as a result of mobile banking. The findings indicate that commercial banks in Kenya continue to face significant information security risks as a result of the widespread adoption of mobile banking. These risks pose a significant challenge to the security and effectiveness of the mobile banking platform, and therefore demands a robust framework and strategies to mitigate against them. The main risks that had occurred as a result of mobile banking include malwares, mobile fraud, SSL vulnerabilities, SIM swap, Virus attacks, information leakages, DDoS, and people-related risks. The study concluded that these risks continue to pose a significant threat to the mobile banking systems.

The third objective of the study was to establish the ICT General Controls implemented by commercial banks to minimize mobile banking risks. The main strategies included Personal Identification Numbers, data encryption, access controls, warning systems, biometric systems and SMS verifications were commonly used by banks to prevent or detect unauthorized access to sensitive information. In addition, biometrics, big data analytics and behavioural analysis had been implemented, albeit to a small extent. The study noted that the strategies are implemented in peace meal, without a holistic framework or model that takes into account all aspects of mobile banking risks. Therefore, there was need for a risk mitigation model for mobile banking risks that addresses this gap in order to enhance secure adoption of mobile banking technology.

In order to address the existing gap where commercial banks are implementing risk mitigation strategies in piece meal, the study built on existing models as well as the findings from objective one to three, and developed and validated an integrated framework which is based on eight pillars namely, Risk assessment and planning,

Device controls, Network access controls, Data protection and management, Application controls, Users, Monitoring and Evaluation, and Continuous education/awareness. In the risk assessment and planning pillar, the organization conducts a detailed and thorough assessment and evaluation of the risks facing its mobile banking platform, existing gaps in mitigating against these risks, level of awareness among staff and customers on information security, strength of their systems in terms of risk mitigation, among others. The device controls pillar entails all the controls or mitigation measures that are applicable in the user devices. User devices are a major risk area because cyber criminals can easily infiltrate the mobile banking system through the customer devices since these devices are mostly not robust in terms of security measures. In addition, lack of awareness among users makes their devices vulnerable because they do not take adequate measures to mitigate information security risks. Network access controls pillar entails measures that prevent unauthorized access to the network. Data protection and management involves measures that ensure proper management and protection of data in the mobile banking system. Such measures may include separation of sensitive data, encryption, data tracking, and data wiping among other measures. Application controls are measures that prevent unauthorized access at the application level, while the users pillar entails measures that guide the management of users in order to protect the security of the system. The monitoring and evaluation pillar entails activities that ensure that the organization is aware of the state of information security as well as any potential risks at any one time. In addition, it entails continuous research in order to identify and implement new technologies that are more effective in mitigating against the continuously evolving mobile banking information security risks. Last but not least, is the continuous user education pillar. In this pillar, the objective is to ensure that the users of mobile banking are continuously informed

about the mobile banking information security risks and their role in mitigating against these risks. In addition, user education should address new developments in information security so that the latest tactics used by attackers are known to users in advance.

5.4 Recommendations for Policy and Practice

The study therefore recommends adoption of the proposed framework which takes into account various best practices from different researchers and practitioners on information security in the context of mobile banking. The study further recommends that organizations should carry out an own assessment and customize the elements of the framework to fit their own organizational contexts. Organizations should consider a thorough implementation of Risk assessment and planning, device controls, network access controls, data protection and management, application controls, user management, monitoring and evaluation, and continuous education/awareness in one holistic framework in order to ensure that no loopholes or gaps are left in the mobile banking risk mitigation measures.

In terms of policy, the study recommends that policy makers should provide robust industry-wide policy guidance on how to manage information security risks relating to mobile banking. Policy makers should consider developing an industry guide on information security in the context of mobile banking, and consider the framework recommended by this study. This will ensure that there is a standard approach to mobile banking information security which will safeguard the gains made by the banking industry in revolutionizing banking through mobile banking and reaching millions of people. It is important to address these security risks to avoid jeopardizing this revolutionary concept that has been widely adopted in Kenya and around the world.

5.5 Areas for Future Research

The study recommends further studies to be carried out to validate the framework and to improve it even further in order to make it more robust and responsive to emerging risks and dynamics.

REFERENCES

Accenture. (2017) Mobile Banking Applications: Security Challenges for Banks.

Agami, A and Du, T (2017, September 16). Examining young users' security perceptions of mobile banking [News Website]. Retrieved September 16, 2017, from http://www.diva-portal.org/smash/get/diva2:1156302/FULLTEXT01.pdf.

Al-Akhras, T.M., Al-Saiyeed, R., Alian, M. and Qwasmi, D. (2011) Innovative Secure Mobile Banking Services. 195.

Aggarwal, Y. P. (2012). *The Science of Educational Research. A Source Book.* Kurukshetra: Nirmal Book Agency.

Babbie, E. (1990) *Survey Research Methods.* 2nd Edition, Wadsworth, Belmont.

Barclays Corporate Banking research indicates that global financial services players have yet to align on key issues of collaboration, innovation, and cybersecurity. (2016). Banking Newslink, p. Banking Newslink, Mar 17, 2016.

Bauer, R.A. (2014) *Consumer Behaviour as Risk-Taking, Dynamic Marketing for Changing. World. American Marketing Association,* Chicago, 389.

Benabied, S., Zitouni, A., & Djoudi, M. (2013). A Cloud Security Framework Based on Trust Model and Mobile Agent. ArXiv.org, 1-8.

Bindhu, V.,Chen, J., Tavares, J., & SpringerLink. (2014). International Conference on Communication, Computing and Electronics Systems : Proceedings of ICCCES 2019 (1st ed. 2020. ed., Lecture notes in electrical engineering 637).

Bracciali, A., Clark, J., Pintore, F., Rønne, P., Sala, M., & SpringerLink. (2020). Financial Cryptography and Data Security : FC 2019 International Workshops, VOTING and WTSC, St. Kitts, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers (1st ed. 2020. ed., LNCS sublibrary. SL 4, Security and cryptology 11599).

Brignall, M. (2016, April 16). *Sim-swap fraud claims another mobile banking victim* [News Website]. Retrieved April 16, 2016, from

https://www.theguardian.com/money/2016/apr/16/sim-swap-fraud-mobile-banking-fraudsters.

Bryman, A. (2011) *Social research methods*. 3rd Edition, Oxford University Press., New York.

Bryman, A., & Bell, E. (2015). Business research methods. Oxford University Press, USA.

CAK. (2015). *First Quarter Sector Statistics Report for the Financial Year 2015/2016 (July-September 2015*). Nairobi: Communications Authority of Kenya (CA).

Campbell, Kim. (2012). *Collecting Information: Qualitative Research Methods for Solving. Workplace Problems. Technical Communication*. 46.

Chaki, R., Cortesi, A., Saeed, K., Chaki, Nabendu, & SpringerLink. (2012). Advanced Computing and Systems for Security: Volume Ten (1st ed. 2012. ed., Advances in intelligent systems and computing 996).

Chandra, P., Messier, M., & Viega, J. (2013). *Network Security with OpenSSL*. *In* . *Network Security with OpenSSL* (p. 384). O‟Reilly. Retrieved from

http://directory.umm.ac.id/Networking%20Manual/Network%20Security20With20O penSSL%202002.pdf.

Chase, Aaron. (2020). Secure the Smartphone, Secure the Future: Biometrics, Boyd, a Warrant Denial and the Fourth and Fifth Amendments. Hastings Race and Poverty Law Journal, 17(2), 603.

Chikomo, Kelvin & Chong, Ming & Arnab, Alapan & Hutchison, Andrew. (2016). Security of mobile banking.

Ćurguz, Jelena. (2016). Vulnerabilities of the SSL/TLS Protocol. Computer Science & Information Technology. 6. 245-256. 10.5121/csit.2016.60620.

Dagada, Rabelani. (2013). Digital Banking Security, Risk and Crediblity Concerns In South Africa.

Dalpiaz, Fabiano & Paja, Elda & Giorgini, Paolo. (2016). Security Requirements . Engineering: Designing Secure Socio-Technical Systems. 10.1007/978-3-319-. 07452- 8_3

Diesch, R., Pfaff, M., & Krcmar, H. (2016). A comprehensive model of information security factors for decision-makers. *Computers & Security, 92*, Computers & Security, May 2020, Vol.92.

Dmitrienko, A., Liebchen, C., Rossow, C., & Sadeghi, A.-R. (2014). *Security analysis .of mobile two-factor authentication schemes.* Intel® Technology Journal, 18(24),

138-161.

Dmitriy A. Izergin, Mikhail A. Eremeev, Shamil G. Magomedov, & Stanislav I. Smirnov. (2020)Information security evaluation for Android mobile operating system.

Elhadi, A. A., Maarof, M. A., & Barry, B. I. (2013). *Improving the detection of malware behaviour using simplified data dependent API call graph. International Journal of Security and Its Applications*, 7(5), 29-42.

Ellen, Pam & Bearden, William & Sharma, Subhash. (2011). *Resistance to Technological Innovations: An Examination of the Role of Self-Efficacy and Performance Satisfaction. Journal of the Academy of Marketing Science*. 19. 297-307. 10.1007/BF02726504.

Fain, D., & Roberts, M.L. (2012). Technology vs. consumer behaviour: the battle for the financial services customer. Journal of Direct Marketing, 11(1), 44-54.

Farsole, A. A., Kashikar, A. G., & Zunzunwala, A. (2010). *Ethical hacking. International Journal of Computer Applications*, 1(10), 14-20.

Ferrag Mohamed Amine. (2020). Authentication schemes for smart mobile devices: Threat models,countermeasures,and open research issues. Telecommunication. Systems, 73(2), 317-348.

Forsythe, S.M. and Shi, B. (2013) *Consumer Patronage and Risk Perceptions in Internet Shopping. Journal of Business Research*, 56, 867-875. http://dx.doi.org/10.1016/S0148-2963(01)00273-9.

Fred Mukinda (2014) *Easy Cash in Mobile Banking Report 2014*. Retrieved 9 7 2014from https://www.nation.co.ke/news/1056-2444632-md3ystz/index.html

French, A. (2012). A case study on E-Banking security – When security becomes too sophisticated for the user to access their information. *Journal of Internet Banking and Commerce, 17*(2), 1-14.

Gandotra, E., Bansal, D., & Sofat, S. (2014). *Malware analysis and classification: a survey. Journal of Information Security*, 5, 56-64.

Gangan, S. (2015). *A Review of Man-in-the-Middle Attacks*, 12. https://doi.org/arXiv:1504.02115.

Garg, P. (2012). Impact of Digitization on Commercial Banking Services. 71-90.

Giwah, A., Wang, L., Levy, Y., & Hur, I. (2019). Empirical assessment of mobile .. device users' information security behaviour towards data breach. *Journal of Intellectual Capital.*

Han, U. (2015). Information Security Risk Management in Electronic Banking System. 2015 IEEE Conference on Computer Applications(ICCA), 1-6.

Harwell, M. R. (2011). Research design: Qualitative, quantitative, and mixed methods. Conrad, & R. C. Serlin (Eds.), *The Sage handbook for research in education: Pursuing ideas as the keystone of exemplary inquiry* (2nd ed.). Thousand Oark.

Hayikader, S., Hadi, F. N., & Ibrahim, J. (2016). *Issues and security measures of mobile banking Apps. International Journal of Scientific and Research Publications*, 6(1), 36-41.

He, W., Tian, X., & Shen, J. (2015). *Examining Security Risks of Mobile Banking Applications through Blog Mining*. Research Gate, 1-6.

Heggestuen, J. (2014). *The Future of Mobile and Online Banking*: 2014. Retrieved 10 25, 2016, from http://www.businessinsider.com/the-future-.of-mobile-and-onlinebanking-2014-slide-deck-2014-10?op=1.

He, W., Tian, X., & Shen, J. (2015). *Examining Security Risks of Mobile Banking Applications through Blog Mining*. Research Gate, 1-6.

Heggestuen, J. (2014). *The Future of Mobile and Online Banking*: 2014. Retrieved 10 25, 2016, from http://www.businessinsider.com/the-future-.of-mobile-and-onlinebanking-2014-slide-deck-2014-10?op=1.

Hoffmann, A. O., & Birnbrich, C. (2012). The impact of fraud prevention on bank-customer relationships: an empirical investigation in retail banking. International *Journal of Bank Marketing*, 30(5), 390-407.

Hossain, S., Bao, Y., Hasan, N., & Islam, M. (2018). Perception and prediction of intention to use online banking systems: An empirical study using extended TAM. *International Journal of Research in Business and Social Science*, 9(1), 112-126.

Islam, S. (2014). *Systematic literature review: Security challenges of mobile banking and payments system.* International Journal of Science and Technology, 6(7),107116.

Jacob, D. (2020). New SIM-swap hacks highlight carriers' wobbly security. Urgent Communications, Jan 14, 2020.

Jansen, J., & Van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. International Journal of Human Computer Studies, 123, 40-55.

Ju, Y. W., & Lee, B. H. (2013). *The implementation of secure mobile biometric system. International Journal of Bio-Science and Bio-Technology*, 5(4), 53-60.

Karanja, J. (2017) Risks Facing Mobile Banking Retrieved March17, 2017, from https://www.semanticscholar.org/paper/Investigation-into-the-Risks-Facing-Mobile-.Banking%3A-Karanja/63f13395a001d258c349d16c4c8b39348c858b68.

Kaur, A., & Kumari, S. (2014). Secure database encryption in web applications. *International Journal of Advanced Research in Computer and Communication Engineering*, *3*(7), 7606-7608.

Kaya, M. (2013) Trust and Security Risks in Mobile Banking. Retrieved from https://www.academia.edu/6228133/Trust_and_security_risks_in_mobile_ banking.

Kenyan WallStreet, (2017) Mobile Financial services report retrieved April 2017 from https://kenyanwallstreet.com/kenya-tops-africa-use-mobile-financial-services-report/

Kimutai, E. (2018*). Kenyan banks lose $0.86 million to hackers*. Viewed from https://www.ceoafrica.co.ke/two-kenyan-banks-lose-0-86-million-to-hackers-in-a-. month/ *Accessed on*, 29*(07), 2018.*

Kombe, S. K., & Wafula, M. K. (2015). *Effects of internet banking on the financial performance of commercial banks in Kenya a case of Kenya Commercial Bank*. International Journal of Scientific and Research Publications, 5(5), 1-10.

Kumar, R. (2011). *Research methodology: A step-by-step guide for beginners*. Los . Angeles, CA: SAGE.

Laukkanen, & Kiviniemi, (2010). *The role of information in mobile banking resistance*. International Journal of Bank Marketing. 28. 372-388. 10.1108/02652321011064890.

Lee, G. and Lin, H. (2015), "Customer perceptions of e-service quality in online shopping", *International Journal of Retail & Distribution Management*, *Vol.* 33 No. 2, pp. 161-. 176.

Luvanga, A., Kimani, S., & Kimwele, M. (2014). *Lack of awareness by end users on security issues affecting mobile banking: a case study of Kenyan mobile phone end users*. Journal of Information Engineering and Application, 4(5), 19-28.

Mahesh Kumar, & Sanjay Gupta. (2020). Security perception of e-banking users in . India: An analytical hierarchy process. Banks and Bank Systems, 15(1), 11-20.

Mallat, N., Rossi, M. & Tuunainen, V.K., 2004. *Mobile banking services. Communications of the ACM*, 47(5), p.42. Available at: http://portal.acm.org/citation.cfm?doid=986213.986236 [Accessed January 3, 2012.

Manoj, V. B. (2011). SMS based secure mobile banking. *International Journal of Engineering and Technology*, *3*(6), 472-479.

Masamila, B. (2014). *State of mobile banking in Tanzania and . Security Issues.* International Journal of Network Security & Its Applications, 4, 53-64.

Mohan, K. (2016) *5 most-secure smartphones in the world*. Viewed from https://economictimes.indiatimes.com/tech-life/5-most-secure-smartphones-in-the-. world/slideshow/53882978.cms.

Molina-Castillo, F., Lopez-Nicolas, C., & De Reuver, M. (2017). Mobile Payment: The Hiding Impact of Learning Costs on User Intentions. Journal of Theoretical and Applied Electronic Commerce Research, 15(1), 1-12.

Mudiri, J. L. (2012). *Fraud in Mobile Financial Services.* Luknow, India: MicroSave.

Mugenda, A., & Mugenda, O. (2009). *Research Methods: Quantitative and Qualitative Approaches.* Nairobi, KE: ACTS.

Mujinga, M., Eloff, M. & Kroeze, J. (2017). A socio-technical approach to information security.

Musaev, E., & Yousoof, M. (2015). *A review on internet banking security and privacy issues in Oman*. *ICIT 2015 The 7th International Conference on Information Technology*, (pp. 365-369). Oman.

Mutua, J. (2018) *Kenya is mobile cash king but Ghana and Rwanda lead in reach*. Viewed from https://www.businessdailyafrica.com/datahub/Kenya-is-mobile-cash-king-but-Ghana/3815418-5145552-tnc57fz/index.html . *Accessed on,* 2*7(05), 2016.*

Ngugi, D., Sawe, E., Nguyen, D., & Bertsch, A. (2020). Modelling and Measuring Acceptance and Use of Internet Banking: The Systematic Development of an Instrument. Review of Integrative Business and Economics Research, 9(2), 24-45.

NIST. (2014, October 14). *Vulnerability Summary for CVE-2014-3566 [Information Communication Technology*]. Retrieved January 3, 2017, from https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566.

Nordin, F. (2011), *Transcendental marketing: a conceptual framework and empirical examples, Management Decision, Vol.* 47 No. 10, pp. 1652-1664. . https://doi.org/10.1108/00251740911004736.

Nyamtiga, B. W., Sam, A., & Laizer, L. S. (2013). *Enhanced security model for mobile banking systems in Tanzani*a. *International Journal of Technology Enhencements and Emerging Engeering Research, 1*(4), 4-20.

Opili, E., & Muturi, W. (2016). *Factors influencing the use of mobile banking in Kenya, the case of M-Kesho in BUNGOMA County*. International Journal of Management and Commerce Innovations, 3(2), 149-154.

Otair (2012, January) *Mobile Banking Based On Stand-Alone Mobile Application Clients – A Suggested Mobile Banking Solution for Banks In Jordan*. Retrieved from https://www.researchgate.net/publication/296706154_Mobile_Banking_Based_On_StandAlone_MobileApplication_Clients_A_Suggested_Mobile_Banking_SolutionFor_. Banks_In_Jordan-

Ostlund, L. (2014), *Perceived Innovation Attributes as Predictors of Innovativeness*, *Journal of Consumer Research*, **1**, (2), 23-29.

Otonchi & Kakamanshadi (2010) Security of Mobile Banking, Retrieved from https://www.researchgate.net/publication/304737379_Security_of_Mobile_Banking.

Ouko, E. (2013, June). *Mobile Banking Adoption in the Banking Industry on Kenya.* . Retrieved From http://chss.uonbi.ac.ke/sites/default/files/chss/ESTHER%20A.%20OUKO%20ODER. A20D61-71319-2008_0.pdf.

Pal, A., Herath, T., De', R., & Rao, H. (2020). Contextual facilitators and barriers influencing the continued use of mobile payment services in a developing country: Insights from.adopters in India. Information Technology for Development: Data Justice, Micro-. Entrepreneurship, Mobile Money and Financial Inclusion, 26(2), 394-420.

Paladion Networks. (2017, May 23). *Mobile Banking Architecture Information Communication Technology*]. Retrieved December 12, 2016, from http://paladion.net/mobile-banking-architecture/

Pavlovski, Chris. (2013). A Multi-Channel System Architecture for Banking. International Journal of Computer Science, Engineering and Applications. 3. 1-12. 10.5121/ijcsea.2013.3501.

Peake, C. (2017). Banking Hurdles, Five Issues Small Businesses Are Facing. WWD, 18.

Potnis, D., Gaur, A., & Singh, J. (2020). Analysing slow growth of mobile money market in India using a market separation perspective. Information Technology for DevelopmentData Justice, Micro-Entrepeneurship, Mobile Money and Financial Inclusion, 26(2), 369-393.

Ram, S. and Sheth, J. (1989), *Consumer Resistance to Innovations: The Marketing Problem and its solutions, Journal of Consumer Marketing*, *Vol.* 6 No. 2, pp. 5-14. . https://doi.org/10.1108/EUM0000000002542.

Roberts, F. (2012). *Technology vs. consumer behaviour: The battle for the financial services customer*. Viewed from https://onlinelibrary.wiley.com/doi/abs/10.1002/%28SICI%291522-.

Rogers, R. W. (2015). A Protection Motivation Theory of Fear Appeals and Attitude Change, *Journal of Psychology*. 91(1), 93-114.

Rosen, T. v. (2013). *Branchless Banking in Kenya. Does Mobile Banking and Agent Banking have the Potential to lift the Welfare of Low-Come Individuals. Lund University.*

Rossi & Tuunainen, Virpi. (2014). *Mobile Banking Services*. Commun. ACM. 47. 42-46. .10.1145/986213.986236.

Rouse, M. (2016, October). *Phishing [Information Security*. Retrieved January 3, 2017, from http://searchsecurity.techtarget.com/definition/phishing.

Sathye, M. (2017) *Adoption of Internet Banking by Australian Consumers: An Empirical Investigation. International Journal of Bank Marketing*, 17, 324-334. http://dx.doi.org/10.1108/02652329910305689.

Sekaran, U., & Bougie, R. (2010). *Research methods for business: A skill-building approach* (5th ed.). Haddington: John Wiley & Sons.

Seriano (2016) Kenya Cyber security Report 2016 retrieved from https://www.serianu.com/downloads/KenyaCyberSecurityReport2016.pdf.

Seriano (2014) Kenya Cyber Security Report 2014 retrieved from http://www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf.

Shaukat, Haafizah Rameeza, Hashim, Fazirulhisyam, Shaukat, Muhammad Arslan, & Ali Alezabi, Kamal. (2020). Hybrid Multi-Level Detection and Mitigation of Clone Attacks in Mobile Wireless Sensor Network (MWSN). Sensors (Basel, Switzerland), 20(8) Sensors (Basel, Switzerland), 2020, Vol.20(8).

Simpson, J. (2012). The impact of the internet in banking: Observations and evidence from developed and emerging markets. *Telematics and Informatics*, *19*, 315-330.

Singh, A., & Jauhari, U. (2012). *Data security by preprocessing the text with secret hiding*. *Advanced Computing: An International Journal, 3*(3), 63-74.

Soofi, A. A., Khan, M., & Fazal-e-Amin. (2014). *Encryption techniques for cloud data confidentiality*. *International Journal of Grid Distribution Computing*, *7*(4), 11-. 20Temenos, & NetGuardian. (2016). A-Z of Banking Fraud 2016, 39.

Siponen, Mikko & Pahnila, S. & Mahmood, A. (2017). Factors influencing protection motivation and IS security policy compliance. Innovations in Information Technology. 1-5.

Temenos, & NetGuardian. (2016). A-Z of Banking Fraud 2016, 39.

Themistocleous, M., Papadakē, M., & SpringerLink. (2013). Information Systems : 16th.European, Mediterranean, and Middle Eastern Conference, EMCIS 2014, Dubai, United Arab Emirates, December 9–10, 2019, Proceedings (1st ed. 2013. ed., Lecture notes in business information processing 381).

Trustonic Security to be Implemented in LG Mobile Smartphones. (2020). Plus Company .Updates, April 23, 2020.

Venkatesh, V., Brown, S. A., & Bala, H. (Forthcoming 2012-2013). *Bridging the qualitative quantitative divided: Guidlines for conducting mixed methods research in information systems*. *MIS Quarterly, X* (X), pp. 1-34.

Verkijika, S. (2020). An affective response model for understanding the acceptance of mobile payment systems. Electronic Commerce Research and Applications, 39, Electronic Commerce Research and Applications, January 2020, Vol.39.

Uddin, M., Bansal, J., & SpringerLink. (2020). Proceedings of International Joint Conference on Computational Intelligence: IJCCI 2019 (1st ed. 2020. ed., Algorithms for Intelligent Systems).

Wambua, Ardhendu & Venkataramani, Bhama & Ambarkhane, Dilip. (2012). Role of Mobile Banking in Financial Inclusion. SSRN Electronic Journal. . 10.2139/ssrn.2485777.

Wang, Yingjie, Xu, Guangquan, Liu, Xing, Mao, Weixuan, Si, Chengxiang, Pedrycz, Witold, & Wang, Wei. (2020). Identifying vulnerabilities of SSL/TLS certificate verification in Android apps with static and dynamic analysis. The Journal of Systems & Software, 167, The Journal of Systems & Software, September 2020, Vol.167.

Wet, K. D. (2010). The importance of ethical appraisal in social science research: Reviewing a faculty of humanities‟ research ethics committee. *Journal of Academic Ethics, 8*, 301-314. doi: 10.1007/s10805-010-9118-8.

Willy, Baraka. (2013). Enhanced Security Model For Mobile Banking Systems In Tanzania. International Journal of Technology Enhancements and Emerging Engineering Research. Vol 1. 4 - 20.

Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). A Protection Motivation Theory Approach to Home Wireless Security. *Twenty-Sixth International Conference on Information Systems*, National University of Singapore.

Zhang, L., Cui, Y., & Mu, Y. (2020). Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing. IEEE Systems Journal, 14(1), 387-397.

APPENDICES

Appendix I: Questionnaire

The purpose of this questionnaire is to identify the mobile banking risks in Kenya. Kindly, respond by either selecting the response among choices given that best represents to your views or by filling the spaces provided.

1. Name of Bank
   (Optional)……

2. Type of Bank

   Locally controlled (> 50% local ownership) [ ]

   Foreign controlled (> 50% foreign ownership) [ ]

   Government Controlled (>50% government ownership) [ ]

3. Work Experience?

   Less than 5 years [ ] 6-10 years [ ]

   11-15 years [ ] above 15 years [ ]

4. Position in the bank hierarchy?

   Senior Manager [ ] Middle level Manager [ ]

   Other (Specify)……

5. Highest Education Level?

   Certificate [ ] Diploma [ ] Higher national Diploma [ ]

   Bachelors [ ] Masters [ ] PhD [ ]

6. Work Department

   Customer Care [ ] I.T.[ ] Marketing [ ]

   Teller [ ] Retail [ ] Operations [ ]

PART II: MOBILE BANKING RISKS

To what extent do you encounter the following risks as a result of mobile banking. (1- Absolutely Not, 2-Small Degree, 3-Modest Degree, 4-Large Degree, 5-Very Large Degree)

	1	2	3	4	5
Malware					
Are there fake similar Mobile Banking Applications ?					
Have you experienced virus attack on the mobile banking platform ?					
Have you come across toolkits which enable root-level access ?					
Do Mobile banking Trojan try exploiting customers accounts ?					
SSLVulnerabilities					
Have customer account credentials ever being exposed ?					
Has the m-banking or internet banking exposed platform ever been exploited due to the ssl issues ?					
Are the Banking platform SSL Durability ever tested ?					
SIM SWAP					
Criminal fraud by bank clients for financial gain					
Criminal fraud by bank agents for financial gain					
Criminal fraud by system engineers for financial gain					
Criminal deception by business partners for financial gain					

What other measures have been put in place by your organization to safeguard against mobile banking challenges?

STRATEGIES TO MITIGATE PREVAILING MOBILE BANKING THREATS

To what extent does your bank employ the following measures to control the current mobile banking risks. (1- Absolutely Not, 2-Small Degree, 3-Modest Degree, 4-Large Degree, 5- Very Large Degree)

	1	2	3	4	5
Encryption					
SIM Application Tool Kit usage for PIN Encryption					
Data Encryption usage to avoid data misuse					
Data Encryption usage achieving higher security Levels					
Permission Based Access					
Use of time of use systems which prompt users to approve permissions as need by applications at runtime					
Use of systems that warn end users what permissions the applications will have access to such as user location, private information, depository, hardware and system information					
Use of dangerous warnings introduced at the installation stage of each mobile application					
Two Factor Authentication					
Use of one time SMS verification codes together with the normal PIN					
Use of random numbers together with the normal PIN					

What other measures are put in place in your organization to mitigate current mobile banking risks?

STRATEGIES TO MITIGATE FUTURE MOBILE BANKING THREATS

To what extent does your bank employ the following measures to control the current mobile banking risks…?

(1- Not at all, 2-Little extent, 3-Moderate extent, 4-Great extent, 5- Very great extent)

	1	2	3	4	5
Biometric Powered Mobile Bank Applications					
Adoption of physiological characteristics such as face, fingerprint, hand-geometry, ear, iris, retina, palm print for mobile banking customer identification					
Adoption of behavioural traits such as voice, gait, keystroke dynamics for mobile banking customer identification					
Adoption of other features such as gender, weight, height, age for mobile banking customer identification					
Adoption of multimodal functionality, which combines several biometric recognition methods for mobile banking customer identification					
Use of Intelligent Behavioural Monitoring and Analysis Technology					
Use of inductive reasoning for detecting abnormal customer behaviour					
Use of cognitive control system to override seemingly obvious but incorrect customer information					
Use of numerical systems to detect faults in customer behaviour					
Use of artificial intelligence to forecast behaviour					
Use of Advanced Big Data Analytics Technology for Fraud Detection and Behaviour Analysis					
Availability of sufficient huge data storage system					
Availability of high speed data processing and analysis					
Availability of computer systems to handle varied data types					

Mobile Banking architecture questionnaire

1) What Database host the Banking Platform

2) What Provider supports the Institutions

3) What type of Servlet used?

4) Type of Micro Edition Platform Supported

5) External Payment Systems supported

6) Omni channel Banking Support

7) Authentication Mechanism Used

Model Validation Guide

Scores out 10								
Focus area	**Expert 1**	**Expert 2**	**Expert 3**	**Expert 4**	**Expert 5**	**Expert 6**	**Expert 7**	**Average**
Awareness								
Application-level security								
Device-level security								
Communication Channel security								
Server-level security								
Network								

Appendix II: ANU Introduction Letter

AFRICA NAZARENE
UNIVERSITY

January 17, 2019

To Whom It May Concern

Dear Sir/Madam,

RE: PROPOSAL APPROVAL FOR NEBABA MONDA (17S03DMIT002)

The above named is a Master of Applied IT student at Africa Nazarene University. This is to confirm that his research proposal titled **"Investigation into the technological risk facing mobile banking: A case of commercial banks in Kenya"** has been approved for conduct of research, subject to obtaining other permissions and/or clearances that may be required beforehand.

Any support and/or assistance accorded to him will be highly appreciated.

Please feel free to contact me via email on jobuhuma@anu.ac.ke in case of further clarity required.

Yours Sincerely,

AFRICA NAZARENE UNIVERSITY
CHAIRMAN
SIGN:.....
COMPUTER SCIENCE
P. O. Box 53067, NAIROBI.

Obuhuma James
Head of Department, Computer and Information Technology

Appendix III: NACOSTI Research Authorization



NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY AND INNOVATION

Telephone:+254-20-2213471,
2241349,3310571,2219420
Fax:+254-20-318245,318249
Email: dg@nacosti.go.ke
Website : www.nacosti.go.ke
When replying please quote

NACOSTI, Upper Kabete
Off Waiyaki Way
P.O. Box 30623-00100
NAIROBI-KENYA

Ref. No. **NACOSTI/P/19/30643/28064** Date: **15th February, 2019**

Nebaba Lubayo Monda
Africa Nazarene University
P.O. Box 53067-00200
NAIROBI.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on ***"Investigation into the technological risk facing mobile banking: A case of Commercial Banks in Kenya"*** I am pleased to inform you that you have been authorized to undertake research in **Nairobi County** for the period ending **15th February, 2020.**

You are advised to report to **the Chief Executive Officers of selected Commercial Banks, the County Commissioner and the County Director of Education, Nairobi County** before embarking on the research project.

Kindly note that, as an applicant who has been licensed under the Science, Technology and Innovation Act, 2013 to conduct research in Kenya, you shall deposit **a copy** of the final research report to the Commission within **one year** of completion. The soft copy of the same should be submitted through the Online Research Information System.

GODFREY P. KALERWA MSc., MBA, MKIM
FOR: DIRECTOR-GENERAL/CEO

Copy to:

The Chief Executive Officers
Selected Commercial Banks.

The County Commissioner
Nairobi County.

Appendix IV: NACOSTI Research Permit

THIS IS TO CERTIFY THAT:
MR. NEBABA LUBAYO MONDA
of AFRICA NAZARENE UNIVERSITY,
16611-620 Nairobi,has been permitted
to conduct research in *Nairobi County*

on the topic: *INVESTIGATION INTO THE TECHNOLOGICAL RISK FACING MOBILE BANKING: A CASE OF COMMERCIAL BANKS IN KENYA*

for the period ending:
15th February,2020

Permit No : NACOSTI/P/19/30643/28064
Date Of Issue : 15th February,2019
Fee Recieved :Ksh 1000



.....
Applicant's Signature

.....
Director General
National Commission for Science, Technology & Innovation

APPENDIX V: Project Plan

Time Activity	November 2018	December 2018	January 2019	February 2019	March 2019	April -June 2019
Topic Definition						
Chapter one						
Chapter Two						
Chapter Three						
Proposal Presentation						
Data Collection						
Finalization of thesis						

APPENDIX VI: Budget

Activity	Description	Unit Cost	Number of units	Amount
Proposal & Final Thesis	Typing, photocopying, printing and binding		1	30,000
Pilot Survey	Photocopying			3,000
Analysis of data using SPSS	Data Package	10,000	1	10,000
Internet Services	2000 minutes @ 1 sh	2000	1	2,000
Transport	Transport to sites	3,000	1	3,000
Miscellaneous		8,100	1	8,100
Total				56,100