

**A CONCEPTUAL FRAMEWORK FOR MULTI-FACTOR AUTHENTICATION FOR
MOBILE MONEY SYSTEMS IN LESOTHO**

By

NTSEJOA RANYALI

Project submitted in Partial Fulfilment of the requirements of the Degree of
Masters in Computer Systems Management at Botho University in the
Department of Blended Distance Learning and Faculty of Graduate Studies
in Computing

May 2019

TABLE OF CONTENTS

TITLE PAGE	i
TABLE OF CONTENTS	ii
LIST OF TABLES, FIGURES	vi
ACKNOWLEDGEMENTS	viii
PROJECT/DISSERTATION DECLARATION FORM	ix
ABSTRACT	x
LIST OF ABBREVIATIONS	xii
CHAPTER 1: INTRODUCTION	1
1.1 Introduction to the study.....	1
1.2 Background to the study.....	3
1.2.1 Background of EcoCash.....	4
1.2.2 Background of M-Pesa.....	4
1.3 Statement of the Problem.....	5
1.4 Research Objectives.....	7
1.5 Purpose of the study.....	8
CHAPTER 2: REVIEW OF THE LITERATURE	9
2.1 Introduction.....	9
2.2 History of Mobile Money Transfer Services.....	9
2.2.1 History of Mobile Money in Lesotho.....	11
2.3 The use Mobile Money Transfer Services.....	13
2.4 Stakeholders in Mobile Money Transfer Services.....	14
2.5 Registration process of Mobile Money Transfer Services.....	16
2.5.1 Registering for M-Pesa.....	16
2.5.2 Registering for EcoCash.....	17

2.6 Technologies used by Mobile Money Transfer Services.....	17
2.6.1 Subscriber Identification Module (SIM) Toolkit.....	18
2.6.2 Unstructured Supplementary Service Data.....	18
2.6.3 Security flaws in USSD.....	18
2.6.4 Short Messaging Service (SMS) Technologies.....	19
2.6.5 Security Flaws in SMS.....	19
2.7 Security Flaws in SMS.....	20
2.7.1 Single factor authentication.....	21
2.7.2 Weaknesses in the current authentication technique.....	21
2.7.3 Two factor authentication.....	22
2.7.4 Multifactor authentication.....	23
2.7.5 Biometric Technologies.....	23
2.7.5.1 Voice Recognition System.....	24
2.7.5.2 Fingerprint Identification.....	25
2.7.5.3 Hand Geometry.....	25
2.7.5.4 Biometric Face Recognition.....	26
2.7.6 Steps of face recognition system applications.....	27
2.7.7 How Biometrics system operates.....	28
2.7.8 Strengths of Biometric system.....	30
2.7.9 Weaknesses of Biometric Facial Recognition system.....	31
2.7.10 Comparison of Biometrics Methods.....	32
2.8 Relationship with other studies.....	33
2.9 Chapter Summary.....	39

CHAPTER 3: RESEARCH METHODOLOGY AND CONCEPTUAL FRAMEWORK

3.1 Introduction.....	40
3.2 Proposed work.....	40

3.3 Research design.....	41
3.4 Research method.....	42
3.4.1 Justification for the use of quantitative method.....	42
3.5 Sampling.....	43
3.5.1 Study population.....	43
3.5.2 Sampling frame.....	43
3.5.3 Sampling size.....	44
3.5.3.1 Sample size determination.....	44
3.5.3.2 Sample size for M-money users.....	44
3.5.4 Sampling technique.....	45
3.5.4.1 Advantages of Convenience non-probability sampling.....	46
3.5.4.2 Disadvantages of Convenience non-probability sampling.....	46
3.6 Data collection methods.....	47
3.6.1 Pilot Study.....	48
3.6.2 Justification for using questionnaires.....	49
3.6.3 Strengths of using questionnaires as data collection method.....	49
3.6.4 Weaknesses of using Questionnaires as data collection method.....	50
3.7 Ethics consideration.....	51
3.7.1 Informed consent.....	51
3.8 Data analysis method.....	52
3.8.1 Computer-based analysis tools	52
3.8.1.1 SPSS (Originally, Statistical Package for the Social Sciences).....	52
3.8.1.2 Excel.....	53
3.9 Research limitations.....	53
3.10 Conceptual Framework for the study.....	54
3.10.1 The current Model of MMS.....	54
3.10.2 Execution Phase.....	55

3.10.3	Proposed Conceptual framework for multi-factor authentication for M-money systems.....	56
3.10.3.1	Registration Phase.....	56
3.10.3.2	Authentication Phase.....	58
3.11	Chapter summary.....	59

CHAPTER 4: RESEARCH FINDINGS AND DATA ANALYSIS

4.1	Introduction.....	62
4.2	Background of data.....	62
4.3	Demographic Information.....	63
4.4	Rating the Mobile Money Transfer Services.....	68
4.5	Challenges in M-money transfer services.....	74
4.6	Security of M-Money Transfer Services.....	77
4.7	M-money transfer service (M-Pesa/Ecocash) can adopt Biometric Face Recognition (BFR).....	85
4.8	Chapter Summary.....	90

CHAPTER 5: DISCUSSION, CONCLUSION AND RECOMMENDATIONS

5.1	Introduction.....	91
5.2	Discussion.....	91
5.3	Conclusion.....	94
5.4	Recommendations.....	95
5.5	Further Research.....	97

REFERENCES.....	98
------------------------	-----------

APPENDICES.....	104
------------------------	------------

Appendix 1: Questionnaire.....	104
---------------------------------------	------------

LIST OF TABLES, FIGURES

List of tables

Table 1 Characteristic Features of Biometric Technologies	33
Table 2 Age Distribution	63
Table 3 Duration of using M-Money Service	65
Table 4 A cross tabulation of region against type of phone used.....	66

List of figures

Figure 1 Mobile Money Agents (% per district)	13
Figure 2 Different processes in face recognition systems	28
Figure 3 General Biometric System.....	30
Figure 4 Registration Phase in 2FA model.....	34
Figure 5 Execution Phase in 2FA model	35
Figure 6 Protocol for wireless payment: Multifactor secure Web authentication protocol using mobile devices.	36
Figure 7 Random Password Authentication Model	37
Figure 8 Subscriber Transaction Sequence Diagram	38
Figure 9 Registration in current M-money system	55
Figure 10 Execution Phase in Current M-money System.....	56
Figure 11 Flowchart for Registration of the user in the proposed framework	57
Figure 12 Flowchart for Authentication phase for proposed system	59
Figure 13 Respondents by gender	62
Figure 14 Place of residence	64
Figure 15 Number of Users registered for M-money service.....	64
Figure 16 Type of phone used for M-money	66
Figure 17 MMS are reliable and convenient.....	67
Figure 18 MMS are time efficient.....	68
Figure 19 MMS are secure	69
Figure 20 MMS are affordable	69
Figure 21 MMS are easy to use.....	70

Figure 22 MMS service center is easily accessible by phone	71
Figure 23 MMS are quick to address my problems	71
Figure 24 the service meets my expectations	72
Figure 25 I will recommend this service to someone	73
Figure 26 Have you ever had challenges while using the service.....	74
Figure 27 Are your challenges related to this mentioned	75
Figure 28 was your problem solved.....	75
Figure 29 Was your problem solved through any of the following.....	76
Figure 30 Have you ever shared your PIN	77
Figure 31 if yes, do you still think your account is still safe	77
Figure 32 Do you think your PIN can be easily guessable	78
Figure 33 PIN provides enough security	79
Figure 34 Did you ever forget your PIN	79
Figure 35 would you remember your answer to security question set	80
Figure 36 How often do you change your PIN	80
Figure 37 Have you ever been a victim of fraud	81
Figure 38 did it relate to any of the following frauds	82
Figure 39 Were fraudulent activities solved	82
Figure 40 If yes, was it through any of the following	83
Figure 41 Is there a need for an additional method to improve security	83
Figure 42 which biometric are you familiar with	84
Figure 43 It will improve the security of (M-Pesa/EcoCash)	85
Figure 44 It will complicate the current process of doing transactions	86
Figure 45 It will be convenient for the user.....	86
Figure 46 I will be comfortable to always take a picture	87
Figure 47 It will attract more users.....	88
Figure 48 what will prevent you to use this system.....	88

ACKNOWLEDGEMENTS

I would like to thank the Lord almighty for giving me strength and courage to pull through this Masters program. I would also like to express my appreciation to my supervisor, Dr Rajiv Kumar for his guidance and continuous support through out the entire journey. I would also like to show my gratitude to my family for their love and support, and always believing in me and wishing me the best in my studies. A special thanks to all my colleagues and friends, who dedicated their time even on their busy schedule, they have contributed a great deal and I appreciate their support. Lastly I thank everybody who took their time and participated in this study, may the Lord bless you greatly.

PROJECT/DISSERTATION DECLARATION FORM

Name: Ntsejoa Ranyali	
Student ID: 1817506	
Programme of Studies: Msc in Computer Systems Management	
Module Code/Name: G9-PWD-15	
Title of Project/Dissertation: A conceptual framework for Multi-Factor Authentication for Mobile Money Systems in Lesotho	
Name of Supervisor(s): Dr Rajiv Kumar	
Declaration: In accordance with the appropriate regulations, I hereby submit the above dissertation for examination and I declare that: (i) I have read and understood the sections on Plagiarism and Fabrication and Falsification of Results found in the University's "General Information to Students" Handbook (2017) and certify that the dissertation embodies the results of my own work. (ii) I have adhered to the 'Harvard system of referencing' for referencing, quotations and citations in my dissertation. Each contribution to, and quotation in my dissertation from the work of other people has been attributed, and has been cited and referenced. (iii) I have not allowed and will not allow, anyone to copy my work with the intention of passing it off as his or her own work. (iv) I am aware that I may have to forfeit the certificate/diploma/degree in the event that plagiarism has been detected after the award. (v) Notwithstanding the supervision provided to me by the Botho University, I warrant that any alleged act(s) of plagiarism during my stay as registered student of the Botho University is entirely my own responsibility and the Botho University and/or its employees shall under no circumstances whatsoever be under any liability of any kind in respect of the aforesaid act(s) of plagiarism.	
Signature: Ntsejoa Ranyali	Date: May 2019

ABSTRACT

The widespread use of mobile phones has contributed significantly to the emergence of Mobile Money Transfer Services (MMTS) in Lesotho. This invention made a great contribution to the financial sector as it bridged the gap between those who qualify for a bank account and those who have to rely on other financial services except for bank, for their financial needs. The main objective of this research study is to enhance the security of MMTS in Lesotho, and solve its security vulnerability introduced by the current method of authentication they are using. The study proposes a conceptual framework that will mitigate these issues through Multi-factor authentication using Biometric Face Recognition (BFR) technique. BFR will eliminate the chances of a fraudster providing false information to the system, therefore improving the security of the system. The other objectives include, identifying the threats that are introduced by Personal Identification Number (PIN) as a method of authentication that is currently used by MMTS in Lesotho, and how it affects the security of their system. The other specific objective of this research is to investigate and evaluate the security issues of the MMTS in Lesotho.

The idea behind the establishment of MMTS was to overcome challenges of traditional financial systems, where people had to travel long distances to keep, send money and to pay for utilities like electricity. As much as it is making our lives simplified, but its adoption has introduced security issues that were not there before, fraudsters are continuously coming up with new ways to steal money. PIN is the only method of authentication used by customers to access their M-money (Mobile money) accounts in Lesotho, which is also deployed by great number of Mobile Money Operators (MMO) across different countries. This Single-Factor Authentication (SFA) technique has proven to be less secure, easily guessed, shared and forged. The proposed model will verify users through their eight mixed characters PIN that will be masked when entered as well as by comparing them with their digital image stored in the server during the enrolment phase. Biometric face recognition will provide high level of security to M-

money accounts as it will solve the security issues in traditional method that enable the sharing and transfer of PIN or passwords between people.

In this study, closed ended questionnaires were used to investigate the research questions. Convenient non-random technique was used to draw the population sample. The researcher also used quantitative approach which followed descriptive design and made use of Google online questionnaire forms and distributed questionnaire survey method as the main data collection method which had questions related to research objectives. Lesotho is a country divided into ten districts grouped into regions. Respondents were M-Pesa and EcoCash M-money users across these three regions (lowlands, semi-lowlands and highlands) of Lesotho. Completed questionnaires were then later analyzed using tables and graphs.

The findings were done in line with the key objectives of the study, the study was examining the challenges participants were faced with while using the service, 75% of respondents agreed that they had challenges, majority of them said the most challenge they were facing was due to poor network. The study further revealed that a great number of respondents 60.7% indicated that PIN alone does not provide enough security to their accounts. Greater part of respondents said they never forget their M-money account PIN, but if ever they forget their PIN they would not remember the security question they set while they were registering for their accounts, this is proven by 80.4% of respondents

Majority of respondents demonstrated that they have never been victim of frauds in M-money. But the major fraud experienced was when respondents received a fake SMS claiming received monies, and requesting users to resend the money. The fraudsters are reported to be working with Mobile Network Operator's (MNO) employees to get information about users, targeting users with more money into their accounts. Best part of respondents indicated that there is a need for an additional method to enhance the

security of M-money system, and agreed that proposed model will enhance the security of M-Pesa/EcoCash

It was concluded that, the sharing of PIN amongst friends and family members is seen to have been a problem as one of the specific fraud is performed by someone the user has shared their PIN with before, then performing transaction without their knowledge. The study concludes that by implementing Biometric Face Recognition with eight characters PIN that is masked when entered, different threats in M-money will be eliminated. Most respondents have not been victim of frauds in M-money, but the common fraud is users receiving fake SMS claiming to have received money. The study revealed that there is a need for security enhancement in M-money, most respondents demonstrated that even though they are not sure about the convenience of the proposed system, but they agree that the proposed model will improve the security of their M-money accounts.

LIST OF ABBREVIATIONS

- ATM** - Automated Teller Machine
- BFR** - Biometric Face Recognition
- CBL** - Central Bank of Lesotho
- ETL** - Econet Telecom Lesotho
- GoL** - Government of Lesotho
- GSM** - Global System for Mobile Communication
- KYC** - Know Your Customer
- LCA** - Lesotho Communications Authority
- LMPS** - Lesotho Mounted Police Service
- MMS** - Mobile Money Services
- MMTS** - Mobile Money Transfer Services
- MMO** - Mobile Money Operators
- MNP** - Mobile Network Providers
- MMS** - Mobile Money Systems
- MFA** - Multi-Factor Authentication
- NBFIs** - Non Banking Financial Institutions
- PIN** - Personal Identification Number
- SFA** - Single-Factor Authentication
- SMSC** - Short Message System
- SMS** - Short Message System
- SPSS** - Statistical Package for the Social Sciences
- SIM** - Subscriber Identity Module Toolkit

TFA/2FA - Two-Factor Authentication

USSD - Unstructured Supplementary Service Data

VCL - Vodacom Lesotho

2G - Second generation

CHAPTER 1: INTRODUCTION

1.1 Introduction to the study

“M-money refers to electronically stored monetary value that is available to a user to conduct transactions through a mobile device, issued upon receipt of funds, accepted as a means of payment by persons other than the issuer, and redeemable for cash. M-money services are a subset of electronic money services, which may be delivered via mobile phones, prepaid cards, or other means”, (GSMA, 2016). On the contrary, Jefferis and Manje (2014) emphasise that “M-money in Lesotho includes various components that facilitate the delivery of payments to the banked and non-banked population through mobile phones or other similar electronic means. M-money offers major advantages as a financial services distribution channel. Lesotho has experienced a rapid uptake of mobile money since its introduction in 2012. As primarily a payments mechanism, M-money can help facilitate other financial services such as loan repayments and insurance premiums, but can also act as a savings mechanism. Possibly the greatest advantage of M-money is its wide distribution network. As M-money is serviced by agents rather than physical branches (like with banks) there are far more touch points at which M-money customers can access services”.

The MMS has faced out the old, slow, less secure and inconvenient cash transactions with a more secure, cheaper and convenient way of mobile system. Most people in the rural areas of Lesotho do not have the formal bank accounts, therefore they rely on old fashioned way where they had to travel long distances or catch a bus to send money or to buy electricity. The introduction of MMS provides with a possible answer for sending and accessing other financial services that were not possible before, now they can be accessed at their finger tip. According to (GSMA, 2017), “As of December 2016 there were 140 live M-money services in 39 countries, delivering financial inclusion to the unbanked populations in the Sub-Saharan African. Of which Lesotho had 1.4 million unique subscribers and 62% mobile penetration”.

The widespread adoption of M-money services highly contributed to increased challenges affecting both users and agents while using the system. “In the past Mobile Network Providers (MNP)s were mainly dealing with voice and data services which are not as sensitive as financial transactions. M-money services were introduced by MNOs without having sufficient expertise and experience in providing banking services”, (Mtaho and Mselle (2014)). The issue of security is of paramount importance in MPS, users need to be confident that whatever transaction they perform, they are always secure. The services that are provided to users through MMS includes sending and receiving of money across the country and internationally, paying for utilities like, electricity, water bill, television channels and insurance. This system uses the following technologies which have been proved not to be entirely secure, Short Message System (SMS) and Unstructured Supplementary Service Data (USSD) and Subscriber Identity Module (SIM) Toolkit.

The system depends on one method of authentication which requires the M-money account holder to enter PIN which is a four-digit number known by the user for authenticating the user. The two MNO providing this service in Lesotho deploys this SFA method. “More often than not, static or single password (one-factor) authentication mechanisms are susceptible to brute-force attacks resulting to unauthorized access, given enough attempts and time. Authentication based on one factor does not provide adequate security because the static password does not change between subsequent logons or is rarely altered”, (Amwoyo, 2014). The security of the user account completely depends on the confidentiality of the PIN and it does not provide with any form of identity check (Only PIN is entered). “PINs used are only four digits in length, thus they are likely to be easily guessed and forged. PINs are sent in plain text and are not masked while entered, which makes it visible for anyone nearby”, (Mtaho, 2015). A more effective and secure MFA technique will be proposed to prevent the current security issues in MMS.

According to (GSMA, 2017) “The number of smart-phone connections in Sub-Saharan Africa has doubled over the past two years to nearly 200 million, accounting for a

quarter of mobile connections in 2016. Smart-phone growth has been driven by increasing affordability: sub-\$100 smart-phones, mostly from Asian manufacturers such as Gionee and Tecno, are now commonplace across the region, while many first-time smart-phone users that cannot afford a new device rely on second-hand devices passed down by a relative or purchased at a reduced price from the budding recycled smart-phone market.” Lesotho Communications Authority ((LCA) 2017) reports that “In 2016, 78.7% of the Lesotho residents own a mobile phone. The survey shows that 95% of these mobile phone owners are prepaid subscribers.” Therefore, it is sufficient enough to introduce a Biometric Face Recognition as Multifactor authentication method that will enhance the security of MMS. “MFA is an approach to authentication which requires the presentation of two or more of the three authentication factors: a knowledge factor (something only the user knows), a possession factor (something only the user has), and an inherence factor (something only the user is). After presentation, each factor must be validated by the other party for authentication to occur”, (Amwoyo, 2014).

1.2 Background to the study

In developing countries, due to financial constraints, and other necessary requirements by banks, most people do not qualify to have a bank account, they have to opt for other financial means to send or receive money. Therefore, the introduction of M-money services made it possible for anyone who has a cell phone, regardless of their living standard to perform digital transactions. The use of M-money services proves to have contributed to the economy of most developing countries. “African M-money story is known to have started in Kenya in 2007 when Safaricom launched its M-Pesa solution for peer to peer money transfer. Before that due to a low rate of banking, sending money to a relative was an issue”, (mns-consulting (2017)). Lesotho has seen the establishment of M-money services in 2012 when Econet Telecom launched their EcoCash, then 2013 when Vodacom launched their M-Pesa. These two MMO have been approved and regulated by Central Bank of Lesotho (CBL), which drive to achieve a greater penetration of financial services in the country.

1.2.1 Background of EcoCash

EcoCash launched 2012 by Lesotho's second biggest network operator Econet Telecom Lesotho (ETL) M-money transfer service that allows Econet subscribers to send and receive money on their mobile phones. It is a service that was established in Zimbabwe in 2011 by one of the biggest MNO Econet wireless. It started as M-money service that allows users to send and receive money, as it grew in addition to customers to sending and receiving money, they can also pay facilities like electricity, water bill, insurance and school fees. The services had grown to customers buying goods at different shops and receiving money from other countries (international cross border remittances) and transferring mobile from bank account into Eco-cash. In 2015, this MNO had 318,786 customers and 1480 agents across the country.

1.2.2 Background of M-Pesa

M-Pesa is a mobile phone-based money transfer and micro-financing services provided by Vodacom Lesotho (VCL). It was established in Lesotho in July 2013. It has been adopted from Kenya's biggest network Safaricom and it is currently utilized in all Vodafone and Vodacom's operations world-wide. It has significantly grown from offering basic services such as sending, receiving money and buying airtime to paying school fees, and many other facilities that includes paying for electricity, water bill, insurance and television channels. Companies can also use M-Pesa to pay salaries or send funds to their beneficiaries cost effectively and efficiently. This service provides users with a more secure way of keeping money as it made it possible to convert their cash into M-money, and securing them against possible theft. In Lesotho this service has rapidly grown since 2013, where two years after the launch it had over 745,242 registered users and 1, 999 Agents. In 2017, the number of agents increased 2, 500. Currently this MMO provides services to over 900, 550 users and 4, 969 agents.

“Since the introduction of M-money in September 2012, the growth in the number of users and usage has been substantial. As at June 2014, Econet’s EcoCash had signed up around 157,723 customers by the end of 2013 representing 31% of its cell-phone subscriber base. After twelve months of operation, Vodacom M-Pesa had signed up 421,851 customers representing 33% of its cell-phone subscriber base. Uptake has been far faster than original expectations, and was partially driven by the fact that Vodacom had offered generous incentives (in the form of an airtime bonus) for signing up. However, the majority of M-money subscribers do not use the system; both networks estimate that between one-third and one-quarter of M-money customers are active. This suggests that between 145,000 and 190,000 Basotho actively used M-money, constituting 12-17% of the adult population”, (Jefferis & Manje (2014)).

1.3 Statement of the Problem

The idea behind the establishment of MMS was to overcome challenges of traditional financial systems, where people had to travel long distances to keep, send money and to pay for utilities like electricity. As much as it is making our lives simplified, but its adoption has introduced security issues that were not there before, fraudsters are continuously coming up with new ways to steal money. “The weakest link in the mobile money chain is at the point of registration,” (Chetalam, 2018). Any user can get a SIM toolkit at any nearest MNO store for free and register for M-money account at their own convenient time. During the registration process he/she will be required to enter information (Names, Passport number) and answer a secret question. There is no form of verification done after the user registers to check if those names are valid. That means one person can have multiple accounts with false names and false passport numbers or even other people’s names. Chetalam (2018) indicates that in Kenya “An ID (or passport) is required when registering for MPESA and it is then used for any MPESA transaction. Users are required to produce their national identification card when transacting money from MPESA agents”. This is not the case with both Lesotho’s MNO, which help to address the issue of fake accounts.

Lesotho Mounted Police Service (LMPS) indicates that there are a number of cases being reported where employees of MNOs will check user's accounts with more money. Send the information to the fraudster who will then send a fake SMS to that user, claiming to have deposited a certain amount into their account, the SMS will state how much the user had, and how much is the new balance, so that when the user checks the SMS it will truly correspond to whatever information she/he is being given. Then later on the user will receive a phone call asking them to resend (reverse) the money because it was mistakenly sent to them. After the realization of this fraud by the MNO, they made numerous attempts to notify users about such a scam, but fraudsters are still using this technique and finding new ways to steal from customers.

Even though the MNO added an extra functionality to include the names of the recipient when the user is sending money, but some users do not check whether the mobile number they entered corresponds with the account holder's names provided, therefore, they send money to the wrong recipient (registered and unregistered) or to inactive subscriber number. Recovering the money is not an easy task it requires the sender to ask the MNO to intervene, and sometimes it is impossible to recover the money. This case is similar to the one where a user is withdrawing money from an agent, they enter the wrong till number and before confirming withdrawal, they do not ask the agent name, to avoid withdrawing money where they did not intend to. "Despite this procedure of confirming the number against the name of the recipient, several cases of transferring money to unintended recipient have been reported. Inaccurate data entry is the main cause of transferring money to unintended recipient. Some of the reasons that contribute to this problem include poor sender concentration when carrying out the transaction, user illiteracy and unfamiliarity with mobile phone. In the current M-Pesa system, once the recipient receives money in his/her account, he/she can directly withdraw it without even knowing the sender. This is possible because in M-Pesa system once you receive the money no any security word is needed to authenticate you as the right recipient of that money. These weaknesses affect security of money transfer service in M-Pesa system", (Mtaho and Mselle (2014)).

The greatest security challenge facing users and agents of M-money services is associated with PIN. “M-Pesa PIN is a four-digit number. Moreover, the PIN never expires and is written in plain text during the transaction. Such PIN therefore does not follow effective password management policies. Due to these weaknesses’ customer PIN can easily be guessed, smudged or snooped by unauthorized users”, (Mtaho and Mselle, 2014). Users are constantly reminded not to share their PIN with anyone, in most cases people are lazy to live the comfort of their home to go to the nearest agent to withdraw money, and they usually send their family members or friends, and then share their PIN with them. Then in a later stage, that person can access the account and perform any transaction they want. Entering the correct PIN does not fully guarantee that the person using the account is really the owner.

“Usually M-money business is done by agent separately or together with other services. Agent offices may have several staff who serves for distinct services in the same office or shop. In case a dishonest staff who is not serving for MMSs knows the M-money PIN of another staff who serves for MMSs, unauthorized transaction may be committed”, (Mtaho and Mselle, 2014). There can also be a case of a dishonest staff that might steal agent phone and transfer funds to his/her friends or family mobile accounts, so that she uses it for her own purpose. “The environments in which MMSs are carried are also subjected to security risks. Some agents have permanent offices, other agents in town centers have no offices. They just stay along the road or near bus stands. Such environments make MMS vulnerable to theft or unauthorized access attacks. Unless strong authentication methods are used, security of MMSs will always remain at risk”, (Mtaho and Mselle, 2014).

1.4 Research Objectives

The study seeks to achieve the following key objectives:

- The main objective of is to propose a conceptual frame-work that will assist with higher level of secure authentication process (Multi-factor authentication method)

using Biometric Face Recognition.

- The study will further analyse the current security challenges introduced by use of PIN as the only authentication method used by MMS.
- The other objective of this research is to investigate and evaluate the security issues of the Mobile Money Systems (MMS) in Lesotho.

1.5 Purpose of the Study

The purpose of this study is to investigate the current security issues of the MMS in Lesotho, and provide a more effective solution that will make the system more reliable and secure. It further identifies the threats that are introduced by method of authentication that is currently used by both EcoCash and M-Pesa, and how it affects the security of their system. SFA is proven to be less secure method of authentication therefore; this paper will provide a conceptual framework that will assist the technical teams of both companies put in practice an authentication technique to mitigate these issues using BFR (Multi-factor authentication) Method. BFR will eliminate the chances of a fraudster providing false information to the system, therefore increasing the security of the system. The study will definitely solve the current security issues and provide users and agents with a broad knowledge on how to effectively secure their M-money accounts.

CHAPTER 2: REVIEW OF THE LITERATURE

2.1 Introduction

This chapter begins by discussing the history of mobile money services, and continues to look at the use M-money service with the current authentication technique, different roles played by each stakeholder as well as how users register and the technologies deployed by MMS. The study will also discuss the different authentication techniques that can be employed in MMS. These techniques include SFA which is the current and only authentication method deployed by all MNO in Lesotho, Two-Factor Authentication (TFA/2FA) and MFA. With supporting literature, then recommend MFA using Biometric Face Recognition as a method that will provide with improved security to the MNO in Lesotho. It will conclude by examining the related work of the research study.

2.2 History of Mobile Money Transfer Services

Prior to the introduction of M-money services, the unbanked had to rely on unsafe, time-consuming and unreliable means to send their families in remote area money, they would put money in an envelope give it to someone who is travelling to home by a bus to deliver it to their place. It will take days before the money is received and sometimes the money will not be received at all. This was the reality for most people more than a decade ago, (GSMA, 2017) indicates that even though much information is not available detailing how many people were unbanked in 2006, but in “2009 the Financial Access Initiative undertook a comprehensive analysis, estimating that 2.5 billion adults in the world were unbanked. However, more than one billion people in low and middle-income countries already had access to a mobile phone.”

Lack of infrastructure, the money required to open and sustain a bank account, the distance one has to travel to access banking services, as well as documents required by the bank, are the main contributing factors to high rate of unbanked in developing countries, (Subia and Martinez, 2014). The unsafe conditions surrounding the use of

traditional financial services lead to the establishment of M-money platform in 2001 to provide solution and chance for a great number of unbanked to finally be included in formal financial services. East Asia and Pacific region managed to launch six mobile money services in four countries in 2006, which did not do well, reports shows that, only 8.8% of the 6.6 million registered for mobile services and were at list using the service to send or receive money within 90 days. The widespread use of M-money came after the successful launch of M-Pesa by Kenya in 2007, it was only then that its potential worth was noticed, (GSMA, 2017).

“Mobile money services started in Kenya in 2007 through M-PESA (M for mobile, pesa for money in Swahili), a popular mobile money service offered by a local mobile network operator, Safaricom. Since then, the mobile money industry has rapidly expanded, particularly in developing economies in Africa and South Asia such as India, Bangladesh, and Pakistan”, (Subia and Martinez, 2014). The world now celebrates more than a decade of a great success of mobile money services. A MNO that started as a text and voice based service provider then expands its services to allowing remote subscribers to send and receive money to and from their families without a need of a bank account. “In 2018, the scale of M-money continues to grow, with more than 866 million registered accounts in 90 countries and \$1.3 billion transacted every day, this is 20% increase from 2017 Globally, around 1.7 billion people still lack access to safe, reliable and convenient financial services. However, 31 emerging markets have seen an impressive increase in financial inclusion rates, which can be attributed to simultaneous growth in active mobile money use”, (GSMA, 2019).

After realising the successful implementation of M-money M-Pesa by Kenya, a lot of MNOs were keen to employ the same service in their practice. Tanzania was the second country to launch M-Pesa in April 2008 just a year after Kenya, which did not see the same rapid adaptation as Kenya. “The slow M-Pesa uptake in Tanzania was due to the fact that Vodacom may not have carefully judged the unique country context prior to implementing it in Tanzania. Therefore, it could not contextualize advertising to suit the level of financial literacy in the country for customers to understand the product.

In Zimbabwe, EcoCash was launched by Econet Services on the 30th September 2011. The service achieved great success to the extent that it reached an agent network of 4,000 agents, 2.3 million customer registrations (which is equivalent to 31% of the country's adult population) just within 18 months after launch, with 1 million of them active as well as an annualized transaction volume valued at 22% of the country's GDP", (Sekantsi and Motelle, 2016).

2.2.1 History of Mobile Money in Lesotho

The successful deployment of Kenya's mobile money M-Pesa has lead to launch of similar model of mobile money services in different developing countries. M-Pesa had a positive impact towards most people's lives, by enabling millions of people who had no hope towards a formal banking system to be able to access and perform financial services at the comfort of their home. M-Pesa promise its clients a more effective, cheap, reliable and secure means of dealing with their financial services. "In the same manner, ETL and VCL in Lesotho launched M-money services in an effort to narrow financial exclusion and drive economic development in Lesotho", (Sekantsi and Motelle, 2016).

Since the introduction of M-money services in 2012, there has been a significant growth in the number of registered users. In their comprehensive study, Sekantsi and Motelle (2016) indicate that "based on 2006 population census figure of 1,880,661 inhabitants, the number of registered M-money customers increased from 10% in June 2013 to approximately 57% of the population in December 2015. On the other hand, the number of agents increased exponentially from 337 in June 2013 to 3654 in December 2015. As a proportion of MNO subscribers, the two MNOs achieved approximately 48% market penetration in December 2015."

The growth of M-money services have been attributed to its growing market penetration, the increased number of transactions that have been seen particularly in customers

withdrawing from their M-money accounts, sending of money and buying of airtime. Sekantsi and Motelle (2016) further point out that by “December 2015, M-money has processed a total of 751,743 airtime purchases, 243,169 customer cash withdrawals, 321,768 bill payments and 221,257 domestic money transfers. However, its use case in the processing of salaries has remained significantly limited despite its potential to reduce the hurdles of salaries processing of contract and casual workers by different organizations in the country including the Government of Lesotho (GoL). The high uptake and usage of M-money is also consistent with the growth of trust account balances of the two MNOs”. Regardless of endless efforts by both MNOs to invest in M-money by proving positive impact that can be brought by this service as well as teaching them how the service work, Lesotho has seen a slow growth in M-money services, mainly in the urban area where one will assume the high number in mobile phone penetration will mean a better chance for the service to perform better.

The high increase in the number of agents in across the country, but especially in Maseru where 40 percent of the registered agents were located while 60 percent in other nine districts. This was still a challenge facing this service as registered users in other areas could not efficiently utilize the service because they had no active agents where they could deposit or withdraw money. CBL (2016) point out that “in December 2016, the registered M-money customers (end users) were recorded at 1 137 903 throughout the country compared to 1 064 025 that were registered in December 2015. This amounts to 6.9 percent growth from December 2015. This was attributed to new agent registrations that were done by the MNOs following the public outreach activities undertaken.” Figure 1 below demonstrates the number in percentage of M-money agents registered per district by December 2016.

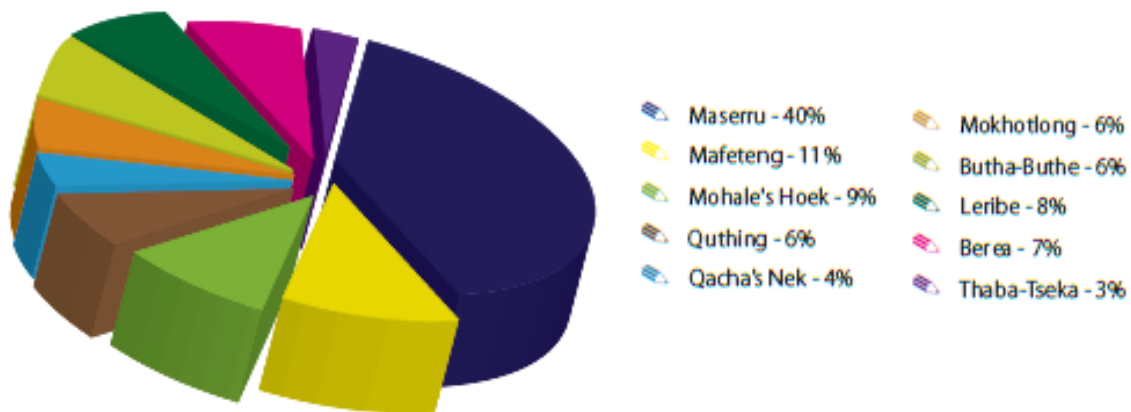


Figure 1 Mobile Money Agents (% per district) (Source: Central Bank of Lesotho, 2016)

The most imperative benefit that Lesotho gain from M-money services is that it continue to bridge the financial inclusion gap due to the increased number of registered active agents that the country have seen by the end of 2016, and the high number of transactions which is showing a positive growth. “Another challenge facing M- money, as a tool for increasing financial inclusion, is that the number of active M-money customers (users) still remains very low relative to the total number of registered users. In this regard, a large M-money market share in Lesotho still remained untapped during in the period ending December 2016”, (CBL, 2016).

2.3 The Use Mobile Money Transfer Services

The emergence of M-money services in developing countries contributed towards bridging the gap between banked and unbanked, geographically excluded can now perform their financial services with more convenient and ease. Its widespread use has attributed to users securely sending and receiving money from the comfort of their home. “The two mobile money providers (Vodacom M-Pesa and Econet EcoCash) allow subscribers to send money deposited in their M-money account to any other individual, who can then withdraw this as cash from M-money agent. No registration or bank account is required to receive money. For regulatory reasons, all e-value balances on the M-Money system have to be matched exactly by a deposit by the MNO in a trust account at a licensed bank”, (Jefferis & Manje, 2014).

In the early days of M-money services in Lesotho, users could only load money into their accounts (cash-in) from MNO agent, send money to any MNO subscriber, whether registered for the service or not, receive money, cash withdrawals (Cash-out) and buy airtime. The services offered grew from these simple but convenient transactions to allowing users to purchase electricity, paying for utilities like water bill, insurance, school fees and television bill directly from their mobile phones. “Both mobile money providers offer bulk payment disbursements for customers such as businesses. Paying salaries through mobile money enables the safety of paying workers’ salaries into accounts, as opposed to paying in cash, without requiring them to have a bank account, which they may struggle to access”, (Jefferis & Manje, 2014). Even though the registration of M-money account is free, but users are charged a certain amount of fee set by MNO for every transaction they perform, the fee is deducted from user’s M-money account immediately after a completion of a transaction. The user will receive SMS notification of the remaining balance.

2.4 Stakeholders in Mobile Money Transfer Services

For M-money services to work effectively and deliver services to users there are number of stakeholders involved including MNOs (Vodacom and Econet), trustee banks (Standard Lesotho Bank), agents, merchants, regulators and users. “The MNO plays the dominant role in the partnership, contracting a network of agents to interface with customers and operating the telecommunications infrastructure for effecting transactions and storing virtual money”, (Gutierrez and Choi, 2014). Both Econet and Vodacom use Standard Lesotho Bank as their trustee bank, which hold the collective of all sums corresponding to electronic money in user’s M-money account. “This achieves two objectives. First, customers have the security that all money deposited onto the system is backed by bank money, and hence funds on an M-money platform should be as secure as funds deposited in a bank. Second, it prevents the MNO from deploying

M-money balances to other, potentially more risky purposes. It also aims to ring-fence the funds backing the M-money balances from the MNO's other financial balances and business operations", (Andrews, Jefferis, Murgatroyd, and Webb, 2013).

"Both Econet and Vodacom have appointed agent networks to handle cash-in and cash-out transactions for their M-money offerings. Agent networks comprise both agents and super-agents, with the latter acting as the intermediary between the agent and the MNO", (Jefferis & Manje, 2014). "The CBL has appropriately left the management of agent networks to the MNOs, rather than imposing strict regulation. The MNOs have clear business interests in ensuring that the agent network functions efficiently, that agents are knowledgeable and can educate customers, and that agents are honest. Hence there is an incentive for the MNOs to manage, invest in, train and discipline agents as necessary, which minimises the need for close regulation. Nevertheless, the CBL will need to monitor the functioning of the agent network and of the MNOs management of it", (Andrews et al, 2013).

"Users are the primary consumers of the ecosystem and they perform transaction using their mobile devices running a communication protocol application which the processing servers can understand", (Victor, 2014). In every country, there should be an organized body that will oversee safe and steady environment for use of M-money services, and define guidelines that all MNO should follow. "The regulatory system for the Lesotho financial system is based around the CBL and the Lesotho Communications Authority (LCA), which regulates telecommunications services. The CBL is responsible for regulating banks and Non-Banking Financial Institutions (NBFIs) including mobile money transfer operators, etc.), as well as the payments system and capital markets", (Jefferis & Manje 2014). On the other hand, "The merchants represent entities or institutions (such as vendors, utilities etc) that are frequent recipients of fund transfers. Their integration into the mobile money application interface greatly simplifies the payment process by creating a direct channel", (Victor, 2014).

2.5 Registration process of Mobile Money Transfer Services

Registering for M-money account requires a person to be a either ETL or VCL subscriber, and have an active SIM card. To start the registration, process the user will dial a USSD code to interact with the menu. This is an easy and straight forward process that does not require a user to visit M-money offices to be enrolled. To prevent the challenge of money-laundering through the MMS, CBL under M-money guidelines introduced know your customer (KYC) requirements which will enable different tiers of users to be enrolled based on Least, Partial and Full KYC.

“The tier with Least KYC requires only simple registration (with no verification), and has daily and monthly transactions limits of M2, 500 (\$171.06) and M10, 000 (\$684.23) respectively”, (Andrews et al, 2013). “This tiering enables M-Money accounts with low-value transaction limits to be opened easily by customers, without imposing onerous requirements for proof of identity and address. Essentially, accounts in the Least KYC category below can be opened simply by using a mobile phone handset, on a self-declaration basis. Therefore, even customers without ready access to proof of identity (such as a passport) or an address can open M-Money account”, (Jefferis & Manje, 2014). The partial KYC require partial verification of documents to be provided with Daily limit of M5, 000 (\$342.11) and Monthly limit of M15, 000 (\$1026.34). With full KYC, the user will be fully verified against official documents, with Daily limit of M7, 500 (\$478.96) and monthly limit of M20, 000 (\$1368.46). Andrews et al (2013) emphasise that “With the introduction of national identification (ID) cards KYC procedures will become much easier as eventually all or most adults will have an ID card that will prove identity”.

2.5.1 Registering for M-Pesa

Registering for M-Pesa the user dial USSD *111# to access the phone menu, the system will prompt the user to select option to access M-Pesa services, then select register, where they will need to enter their details which include first name, surname,

date of birth with the following format (DDMMYYYY), village name and preferred language where the user will select between English and Sesotho which are the two official languages in Lesotho. After entering these particulars, the user will receive an SMS which will inform the user to dial *111# in order to register PIN, the user will start by selecting the security question and then answer that question, which will help the user to reset their PIN in case they forget it. Then the user will be prompted to enter a four digit PIN and confirm it. The user will receive an SMS to confirm that their M-Pesa account has been activated, (Vodacom Lesotho, 2019a).

2.5.2 Registering for EcoCash

To register, the user must be an Econet subscriber that is Buddie, Libertie or Business Parta subscriber. The user will Dial *100# to access phone menu, which will prompt the user to select EcoCash services then register, where they will enter their Identification number (Passport or National ID), first name and surname. Similar to M-Pesa, the user will receive an SMS but with temporary PIN that will be changed in the first login, the SMS ask the user to dial *100# to register PIN. The PIN registration procedure in EcoCash is the same as in M-Pesa but here there is no security question set, the user only enters four-digit PIN and the confirm it. The user is sent and SMS to confirming EcoCash account is active, (Econet Lesotho, 2019a).

2.6 Technologies used by Mobile Money Transfer Services

“Global system for mobile communication (GSM) network is used widely in networking mobile connections. Its initial design was for use in voice communications but as the usage of mobile phone increases, additional means of data transmissions begin to be used; the most popular of which being SIM ToolKit, USSD and SMS”, (Nyamtiga, Sam and Laizer, 2013).

2.6.1 Subscriber Identification Module (SIM) Toolkit

“The SIM Application Toolkit consists of a set of commands programmed into the SIM which define how the SIM should interact directly with the outside world and initiates commands independently of the handset and the network. SIM card stores the necessary international mobile subscriber identity information required to authenticate and identify a user within a telecoms network. After registering and creating an account, the customer’s personal information is associated with their mobile phone number at the processing server. This record constitutes a M-money account commonly referred to as an e-wallet or e-money account”, (Victor, 2014).

2.6.2 Unstructured Supplementary Service Data (USSD)

For the user to access M-money services menu, they utilize USSD code. “USSD is a session-based, real-time communication technology for supplementary services. USSD is used in sending messages across a GSM network between a mobile client and an application server. It operates much like SMS but its session-based and interactive nature distinguishes the two. Unlike SMS, it does not operate by store-and-forward and its turnaround response time is much shorter for interactive applications than it is for SMS. This makes USSD much faster and very cost effective as it involves simple operations that are also handset independent (old handsets to most recent smart-phones can all access the service). USSD applications are characterized by menu-driven and interactive services and a request is invoked by dialling a number that is composed of asterisks (*) and hashes (#)”, (Nyamtiga, Sam and Laizer, 2013). For the user to access their M-money account using M-Pesa, they dial (*111#) while accessing EcoCash the user dial (*100#).

2.6.3 Security flaws in USSD

“Despite the convenience offered by USSD to customers in accessing banking services; the technology is not without its associated security risks. When compared to SMS, USSD is considered to be relatively more secure because no copy of the message is

stored on customer's phone or at the SMS Center (SMSC). A single session is established between the mobile terminal and the application server, and at the USSD gateway the message is encrypted preventing data to be misused between the gateway and the server. The big risk lies on the fact that data carried within the communication channel is not itself encrypted. If GSM encryption is broken, this data can be then be accessed. The A5 encryption that is used in GSM has been reverse engineered and thus leaving USSD data vulnerable to attacks because messages are not encrypted on the GSM backbone. Moreover, GSM encryption is only applied between the mobile terminal and the base station; across the rest of the operator's network, the message is in plaintext", (Nyamtiga, Sam and Laizer, 2013). On the other hand, Desai (2011) emphasize that "USSD content error-handling may reveal sensitive information about customer data, USSD application and the service provider's sensitive data."

2.6.4 Short Messaging Service (SMS) Technologies

"SMS refers to a wireless, radio-based service for transferring short alphanumeric messages among mobile phones on the GSM networks. It was introduced in the wireless networks and was included in the GSM standards in 1991. It is a two way transmission service that makes use an SMSC that acts as a store-and-forward unit for messages. The sender can receive a notification for a success or failure of the transmission thus providing a guaranteed delivery to the receiver", (Nyamtiga, Sam and Laizer, 2013).

2.6.5 Security flaws in SMS

"Despite being useful in conveying information to many recipients at minimal costs, the security afforded by SMS is not sufficient for financial transactions. The security issues that exist in the GSM are mainly the cryptographic issues related to encryption and authentication algorithms, this is because neither encryption nor integrity check mechanisms are enforced during its transmission across the GSM. Moreover, its nature

of operation to store-and-forward makes things even worse because of the number of locations where the SMS data is available to others in clear format”, (Nyamtiga, Sam and Laizer, 2013). In his comprehensive study, Chong (2006) also indicate that “there is security vulnerability at the SMSC. When an SMS message is received at the SMSC, the message gets queued up at the storage buffer. The attacker can exploit this vulnerability by flooding the buffer queue with multiple meaningless messages to a target mobile number. This type of flooding can cause the SMSC to reject incoming messages for the victim because the storage space is limited in the buffer queue”.

2.7 Authentication techniques

Before the user can access and use M-money services, they are supposed to enter their authentication particulars that they provided during the registration process, then this details which in this case is a PIN will be validated by the MNO's server against the one stored while the user was registering. “The strength of the authentication depends on the password selection strategies used”, Chong (2006). “Authentication is the use of one or more mechanisms to prove that you are who you claim to be. Once the identity of the human or machine is validated, access is granted”, Aloul, Zahidi and El-Hajj (2009). “Initially, only one factor was utilized to authenticate the subject. By that time, SFA was mostly adopted by the community due to its simplicity and user friendliness”, (Ometov, Bezzateev, Mäkitalo, Andreev, Mikkonen and Koucheryavy, 2018). Three universally recognized authentication factors exist today”, Aloul, Zahidi and El-Hajj (2009). Ometov et al (2018) define these factors as

- i. **“Knowledge factor:** something the user knows, such as a password or, simply, a secret;
- ii. **Ownership factor:** something the user has, such as cards, smart-phones, or other tokens;
- iii. **Biometric factor:** something the user is, i.e., biometric data or behaviour pattern.”

2.7.1 Single factor authentication

The current authentication method that is used by both EcoCash and M-Pesa is single factor authentication, whereby the user is required to enter PIN in order to access the M-money system, and this method is proven to be less secure. “Most systems today rely on static passwords to verify the user’s identity. However, such passwords come with major management security concerns. Users tend to use easy-to-guess passwords, use the same password in multiple accounts, write the passwords or store them on their machines, etc. Furthermore, hackers have the option of using many techniques to steal passwords such as shoulder surfing, snooping, sniffing, guessing”, Aloul, Zahidi and El-Hajj (2009). On the other hand, Amwoyo (2014) emphasize that “Most online systems use static password which is susceptible to brute force attack. This method does not provide adequate security since the static password remains the same with subsequent logons unless a user manually changes it”. Ometov et al (2018) state that “it was realized that authentication with just a single factor is not reliable to provide adequate protection due to a number of security threats.”

“Single factor authentication, e.g. passwords, is no longer considered secure in the internet and banking world”, (Aloul, Zahidi and El-Hajj, 2009). “SFA is defined as using a single attribute to give or deny access to a service. The service can be accessed through a web interface or over a mobile device. The SFA scheme uses one set of credentials to identify and give access to the entity requesting the services. The most common SFA is uses of password or PIN to access privileged services. Password/PIN security depends on the safety and integrity of the administration as well as its internal security mechanisms in setting up and managing user details for access” (Handson, 2016).

2.7.2 Weaknesses in the current authentication technique

There are a number of security issues that are introduced by using only the PIN as a method of authenticating users. Other agents operate on the streets of towns, this

environment is not safe as it is just an open space where people will be passing, so since PIN is just a four-digit number that is not even masked when entered it introduces threats to the system as people nearby may see what numbers are entered. Yet again the system allows the user to use one PIN for as long as they want, it does not expire. “Additionally, the security policies in the application servers leave some vulnerability which can be exploited to perform attacks on the system. Periodic changes of PIN are not enforced, and the use of a system’s default PIN is allowed in some systems”, (Nyamtiga, Sam and Laizer, 2013).

Change in the structure of PIN will enhance the security of M-money services, it should have a combination of upper-case letters and small case letters, symbols and numbers, the system should prompt the user to enter a password of this format and if it does not meet these requirements, deny it. The password should also expire after a certain period of time. According to Handson (2016) “Complex passwords do not abstract users from having their passwords cracked by brute force, dictionary and rainbow table attacks, but makes it a bit harder. If a hacker accesses the password database, then the whole password security is compromised. However, administrators can configure their password system providers to create and append random characters to the hashes of password encryption. This can help against dictionary-based attacks and social engineering such as phishing. Use of passwords alone will not be adequate, other schemes such as biometric authentication distributes credential storage and passwords that expire quickly can provide strong alternatives”.

2.7.3 Two factor authentication

“Two factor authentications (TFA, T-FA or 2FA) is a mechanism which implements two of the above-mentioned factors and is therefore considered stronger and more secure than the traditionally implemented one factor authentication system. Withdrawing money from an ATM machine utilizes two factor authentications; the user must possess the ATM card, i.e. what you have, and must know a unique Personal Identification Number (PIN), i.e. what you know”, (Aloul, Zahidi and El-Hajj, 2009). “Without the corroborating

verification of both of these factors, authentication does not succeed. This scenario illustrates the basic concept of most two-factor authentication systems: the combination of a knowledge factor and a possession factor”, (Amwoyo, 2014). “Passwords are known to be one of the easiest targets of hackers. Therefore, most organizations are looking for more secure methods to protect their customers and employees”, (Aloul, Zahidi and El-Hajj, 2009).

2.7.4 Multifactor authentication

“MFA was proposed to provide a higher level of safety and facilitate continuous protection of computing devices as well as other critical services from unauthorized access by using more than two categories of credentials. For the most part, MFA is based on biometrics, which is automated recognition of individuals based on their behavioural and biological characteristics. This step offered an improved level of security as the users were required to present the evidence of their identity, which relies on two or more different factors”, Ometov et al (2018). “Biometrics are known to be very secure and are used in special organizations, but they are not used much in secure online transactions or ATM machines given the expensive hardware that is needed to identify the subject and the maintenance costs”, (Aloul, Zahidi and El-Hajj, 2009). “Today, MFA is expected to be utilized in scenarios where safety requirements are higher than usual. Moreover, a recent survey discovered that 30 percent of enterprises planned to implement the MFA solution in 2017, with 51 percent claiming that they already utilize MFA, and 38 percent saying that they utilize it in some areas of operation. This evidence supports the MFA as an extremely promising direction of the authentication evolution”, Ometov et al (2018).

2.7.5 Biometric Technologies

According to Tripathi (2011), “Biometric technologies are defined as, automated methods of verifying or recognizing the identity of a living person based on a

physiological or behavioural characteristic. The term automated methods refers to three basic methods in concern with biometric devices: firstly, a mechanism to scan and capture a digital or analog image of a living personal characteristic, secondly, compression, processing and comparison of the image to a database of stored images; and lastly Interface with applications systems". In their study, Mali and Bhattacharya (2013) emphasize that "currently biometrics is one of the biggest tendencies in human identification. Biometrics is claimed to be better than current and established authentication methods, such as PINs, passwords, smart cards. Key advantages of using a biometric feature are: availability (always), uniqueness (to each person), not transferable (to other parties), not forgettable, not subject to theft, not guessable".

"This identification method is preferred over traditional method for several reasons, including the person to be identified is required to be physically present at the point of identification and/or identification based on biometric techniques obviates the need to remember a password or carry a token. By replacing PINs, biometric techniques can potentially prevent unauthorized access to or fraudulent use of different devices. PINs and passwords may be forgotten and token-based identification methods such as passports and driver's licenses may be forged, stolen, or lost. Thus, biometric systems of identification are enjoying a new interest. Various types of biometric systems are being used for real-time identification", (Tripathi, 2011). These biometric identification technologies include hand geometry, fingerprint, speech, iris voice recognition, facial recognition. Widely used technologies include facial and fingerprint.

2.7.5.1 Voice Recognition System

In their inclusive study Najih, Al-Haddad, Ramli, Hashim and Nematollahi (2016) state that "voice is the most important form of human communication as it reveals valuable information about a person. Voice recognition is a kind of speech recognition system with voice identification which involves identifying an unknown voice by using a population of known voices. This system also has voice verification, as the most popular type of general biometric verification method which aims to verify the identity of a given

voice from a population of known voices”. Delac and Grgic (2004) proceeds by saying “The features of an individual's voice are based on physical characteristics such as vocal tracts, mouth, nasal cavities and lips that are used in creating a sound. These characteristics of human speech are invariant for an individual, but the behavioral part changes over time due to age, medical conditions and emotional state.” This technology offers a number of benefits, “speech is easy to be produced, captured and transmitted as it has a lower cost compared to other biometric recognition techniques. Secondly, the speech is non-invasive and does not need direct contact with or to be perceived by an individual. Thirdly, speech can reveal emotion which is hidden from other biometric recognition techniques such as iris printing and fingerprinting”, (Najih et al, 2016).

2.7.5.2 Fingerprint Identification

“Fingerprint identification is the method of identification using the impressions made by the minute ridge formations or patterns found on the fingertips. No two persons have exactly the same arrangement of ridge patterns (even identical twins), and the patterns of any one individual remain unchanged throughout life”, (Tripathi, 2011). “Fingerprints were used for personal identification for many centuries and the matching accuracy was very high. Patterns have been extracted by creating an inked impression of the fingertip on paper. Today, compact sensors provide digital images of these patterns. Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse. Since the finger actually touches the scanning device, the surface can become oily and cloudy after repeated use and reduce the sensitivity and reliability of optical scanners”, (Delac and Grgic, 2004).

2.7.5.3 Hand Geometry

Tripathi (2011) indicates that “When measuring hand geometry biometrics, three-dimensional image of the hand is taken and the shape and length of fingers and knuckles are measured. Hand geometry has been in use for many years in various

applications, predominantly for access control. The technology does not achieve the highest levels of accuracy but it is convenient and fast use. On the capture process a user places a hand on the reader, aligning fingers with specially positioned guides. Cameras, positioned on above and on the side of hand capture images from which measurements are taken at selected points". On the other hand, Delac and Grgic (2004), "The technique is very simple, relatively easy to use and inexpensive. Dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy. Since hand geometry is not very distinctive it cannot be used for identification of an individual from a large population, but rather in a verification mode. Further, hand geometry information may not be invariant during the growth period of children."

2.7.5.4 Biometric Face Recognition

According to Naeem, Qureshi and Azam (2015) "A facial recognition methodology is a way to automatically verify person by matching his digital image with the database of images. Nowadays the security of person, information or assets is becoming more difficult and important. The crimes like credit card misuse and computer hacking or security breach in organizations are increasing day by day. The face recognition technology is a branch of biometrics through which the humans are identified." Najih et al (2017) further emphasize that "Face recognition is one of the most outstanding abilities of human vision, and is probably the biometric method easier to understand. This is the reason that the features of individual face are considered in security and access control systems. However, many vulnerability slots available in network systems must be protected. For the eight vulnerability slots that have been investigated in a biometric system, the most important slots to be secured are located at transmission and recording steps."

"Face recognition technologies analyse the unique shape, pattern and positioning of facial features. The face is natural biometric because it is a key component in the way we humans remember and recognize each other. Face recognition is very complex

technology and largely software based. Artificial intelligence is used to simulate human interpretation of faces. The problem with human face is that people do change over time; wrinkles, beard, glasses and position of the head can affect the performance considerably. To increase the accuracy and adapt to these changes some kind of machine learning has to be implemented. There are essentially two methods of capture: using video or thermal imaging. Video is more common as standard video cameras can be used. The precise position and angle of the head and surrounding lightning conditions may affect the system's performance", (Tripathi, 2011).

"In real world condition, a face recognition system has complexity due to image processing problems can be considered as a complex system with huge effects of occlusion, illumination and imaging condition on the live images. Face recognition systems should be applied face recognition as well as face detection. Face detection uses detection applications to find the position of the face in the image. The recognition section applies recognition algorithms to classify given images and recognize the new face image. These face images usually have some known properties like; same resolution and are consist of same facial feature components. The standard face recognition algorithms have been used in order to detect eyes, eyebrows, nose and mouth", (Najih et al, 2016).

2.7.6 Steps of face recognition system applications (Najih et al, 2016)

"First, the image should be captured by the camera for face recognition purpose. The second step in a face recognition system is face detection from the acquired image of the previous step. In the third step, face recognition system illustrates the results according the result of the recognition algorithms which is the identity of the input image. The final step is a person verification or identity as a result of the face recognition system. The input face image, which is recognition system, is in digital form. When the face image is captured, the feature should be extracted from it. This Feature extraction of facial image which can be divided into two main categories: appearance knowledge-based approaches. Basically, knowledge-based approaches are based on

the specific features of the face. However, an appearance-based approach has been applied the whole feature in the facial image”, (Najih et al, 2016).

“Face recognition can be classified into two main groups, including static and video image. Although some biometric systems use behavior pattern, face recognition verifies a person based on physiological characteristics. Face recognition is a non-invasive method which does not need direct contact for user friendly. Three processes are considered for face recognition systems. First, the availability of the face in image or video must be detected which is known as face detection. Second, the feature should be extracted from the image which is called feature extraction process. Third, this feature should be compared with face model, which is already trained; it is known as face recognition process”, (Najih et al, 2016). Figure 2 below illustrates all this process.

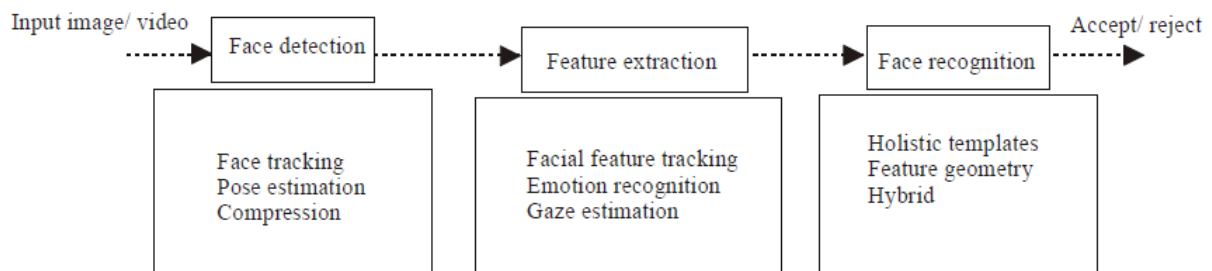


Figure 2 Different processes in face recognition systems, (Najih et al, 2016)

2.7.7 How Biometrics system operates (Tripathi, 2011)

There is a standard operation between most biometric systems, before the user can use the system; they have to be registered into the system. “Enrollment is the process by which a user’s biometric data is initially acquired, accessed, processed, and stored in the form of a template for ongoing use in a biometric system. Subsequent verification and identification attempts are conducted against the template(s) generated during enrollment. Secondly, the presentation phase is a process by which user provides biometric data to an acquisition device-the hardware used to collect biometric data.

Depending on the biometric system, presentation may require looking in the direction of a camera, placing a finger on a platen, or reciting pass phrase”, (Tripathi, 2011).

Tripathi (2011) defines the third phase being the biometric data, where “users provide in an unprocessed image or recording of a characteristic. The unprocessed data is also referred to as raw biometric data or as a biometric sample. Raw biometric data cannot be used to perform biometric matches. Instead, biometric data provided by the user during enrollment and verification is used to generate biometric templates, and in almost every system is discarded thereafter. Thus, biometric systems do not store biometric data-systems use data for template creation. Enrollment requires the creation of an identifier such as a username or ID. This identifier is normally generated by the user or administrator during entry of personal data. When the user returns to verify, he or she enters the identifier, and then provides biometric data. Once biometric data has been acquired, biometric templates can be created by a process of feature extraction”.

The last phase is “feature extraction which is the automated process of locating and encoding distinctive characteristics from biometric data in order to generate a template as called feature extraction. Feature extraction takes place during enrollment and verification-any time a template is created. The feature extraction process includes filtering and optimization of images and data in order to accurately locate features. For example, voice-scan technologies generally filter certain frequencies and patterns, and finger-scan technologies often thin ridges present in a fingerprint image to the width of a single pixel. Since quality of feature extraction directly affects a system’s ability to generate templates, it is extremely important to the performance of a biometric system”, (Tripathi, 2011). The figure 3 below demonstrates how biometric system operates.

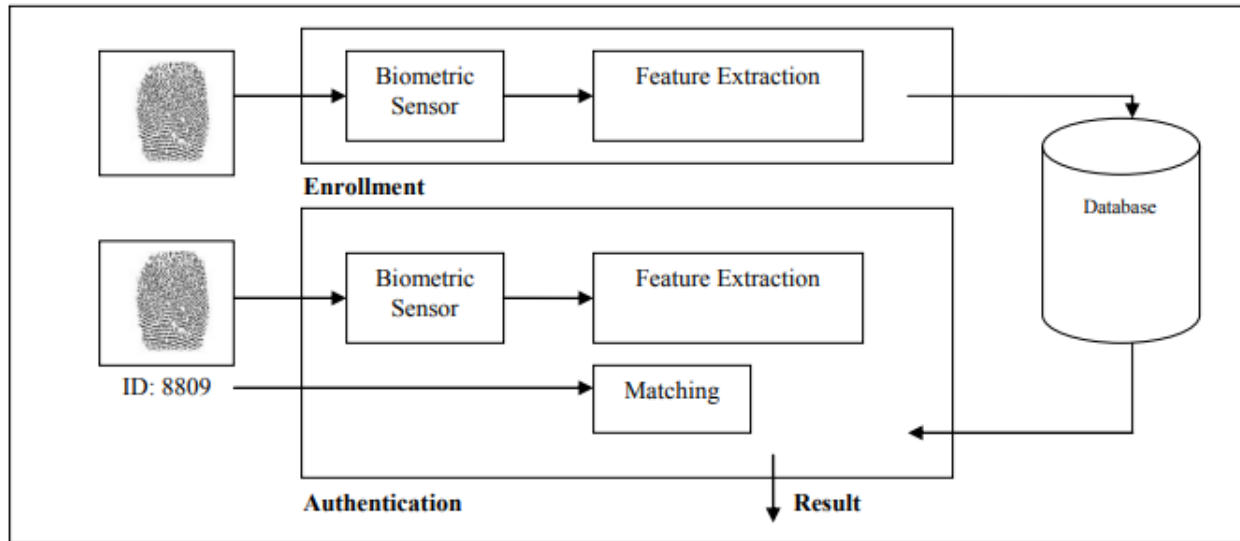


Figure 3 General Biometric System, (Tripathi, 2011)

2.7.8 Strengths of Biometric system

The introduction of Biometric technologies is believed to have introduced more benefits that were not available in the traditional authentication techniques, in some systems, they have completely replaced the present techniques while in others they have supplemented them, (Prabhakar and Pankanti, 2003). Tripathi (2011) indicates that “Biometric traits cannot be lost or forgotten (while passwords can), they cannot be easily copied, be transferred from one person to another, while passwords can be easily shared on cracker’s sites. Using biometrics, the person to be authenticated should be present at that particular moment”. Mali and Bhattacharya (2013) add by saying “biometrics of the person is the key so you need never remember your card or key again. Each body part is unique and Biometrics uses your unique identity to enable a purchase activate something or unlock something.” Bansal and Chawla (2013) state that “Badge or password-based authentication procedures are too simple to hack but biometrics represents a convincing substitute; face recognition represents a better negotiation between what’s publicly acceptable and what’s trustworthy, even when functioning under inhibited environment”.

2.7.9 Weaknesses of Biometric Facial Recognition system

There are few challenges that are available in Facial recognition that are associated to factors that include, “Biometric information may be mechanically copied and cannot be easily changed. This is perceived as a key disadvantage since, if discovered, the compromised data cannot be changed. A user can easily change his/her password; however, a user cannot change their image stored in a database”, (Amwoyo, 2014). Prabhakar and Pankanti (2003) further emphasize that “A user has only a limited number of biometrics, one face, 10 fingers, and so on and they are not easy to replace. Also, because different applications might use the same biometric, a thief who acquires a person’s biometric in one application could also use it in others”. Kumar and Badyal (2014) say “Different cameras carry different lenses which again has a great impact on the picture being captured as different lens have different power. So, any change in the camera or the lenses adds to the difficulty.”

Another challenge associated with facial recognition relates to pose, “Due to variation in pose relative to camera certain features especially eyes may appear partially or fully obstructed or closed”, (Bansal and Chawla, 2013). “Face recognition has low accuracy compared to the proven performance of finger print and iris recognition. Both these methods are way more precise than face recognition and are therefore given preference”, (Kumar and Badyal 2014). “A serious drawback is that many systems are usually less efficient if facial expressions vary. Even a big grin/laugh can render the system’s performance less effectively. So significantly North America now permits only neutral facial expressions on passport photos”, (Saini and Rana, 2014). Additionally, “Impersonating somebody else is not a difficult task anymore. It can be easily achieved in today’s time. This imitation if perfectly done by the attacker can easily con the system. This is called FALSE ACCEPT. A little expression or accessory can change the whole look of a person. This leads to unnecessary dismissal of the same face. This is called FACE REJECT”, (Kumar and Badyal, 2014).

Amwoyo (2014) states that “adding a second factor to the authentication process typically leads to increase in costs for implementation and maintenance. In addition to deployment costs, two-factor authentication often carries significant additional support costs.” Tripathi (2011) also indicates that “While there are several models of biometric systems available in the \$100 range, a majority of technologies are still closer to the \$500 mark. Unless biometrics can get below the cost of password administration costs, business will get below the cost of password administration costs, business will not choose to implement.” Gine, Goldberg, Sankaranarayanan, Sheerin and Yang (2012) say “The estimates are sparse and detailed cost benefits analyses have not been systematically conducted. However, the costs of using different types of biometric technology starting from basic fingerprinting techniques to voice and iris recognition software can be prohibitively expensive.”

Prabhakar and Pankanti (2003) suggest “integrating cryptographic techniques along with biometric matchers, instead of storing the original biometric signal in the system database during enrollment, the system could store only its noninvertible transformed version (for example, a hash). During recognition, the biometric sensor would transform the signal using the same noninvertible transform and perform matching in the transformed space. Different applications can use different noninvertible transforms (or different parameters of the same transform), so a template would be usable only by the application that created it. In fact, the user herself could provide the transform’s parameters in terms of a password or PIN. If a hacker ever compromises such a biometric template, the system can issue a new one using a different transform or different parameters. A simple and effective method of creating an easily revocable biometric template is to encrypt the biometric template with the user’s password.”

2.7.10 Comparison of Biometrics Methods

Different applications use different biometric methods, and a certain method may perform better in an application than the other, therefore all methods have their strong and weak points, depending on which applications they are used in. None of the

biometric methods can be efficient in all conditions. “We match a specific biometric to an application depending on the application’s operational mode and the biometric characteristic’s properties. For example, both the fingerprint and iris-based techniques are more accurate than the voice-based technique. However, in a tele-banking application, the voice-based technique might be preferable because the bank could integrate it seamlessly into the existing telephone system”, (Kumar and Badyal, 2014). In Table 1 below, different factors are used to compare various biometric methods.

Table 1 “Characteristic Features of Biometric Technologies”, (Tripathi, 2011).

Characteristics	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Easy of Use	high	high	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Lighting	Lighting, age, glasses, hair	Changing signature	Noise, colds
Accuracy	High	High	Very high	Very high	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	high
Long Term Stability	High	Medium	high	high	Medium	Medium	Medium

2.8 Relationship with other studies

There have been a great number of cases that have been reported that threatens the security of mobile money services, some of these vulnerabilities are related to the use of PIN as the only authentication method in mobile money system. Mtaho (2015) emphasise that “the uniqueness aspect of the PIN is artificially set because the PIN can be compromised. For example, the customer’s PIN can be known by unauthorized user and hence be used for fraudulent purposes. A robust authentication method is therefore needed to prevent unauthorized access of mobile money account. Biometric authentication methods offer more benefits over other methods.” In his study, Mtaho (2015) recommends “two-factor authentication model for all mobile money systems in

Tanzania, that uses both PIN and fingerprint recognition technology.”

MTAHO 2FA MODEL

“In the proposed model, first, the user will be required to enroll his PIN and fingerprint and save that information in the MNO’s server for future authentication. During the authentication phase, first the user will be authenticated by using the traditional model (PIN). Upon successfully authentication of the PIN, user will again be authenticated by FRT. User enrolls his phone number and his PIN, which are saved in the MNO/s server. After that, user is required to enroll his fingerprint, which is scanned and saved as a template in the MNO server”, Mtaho (2015). The enrollment process in 2FA model is illustrated in figure 4 below.

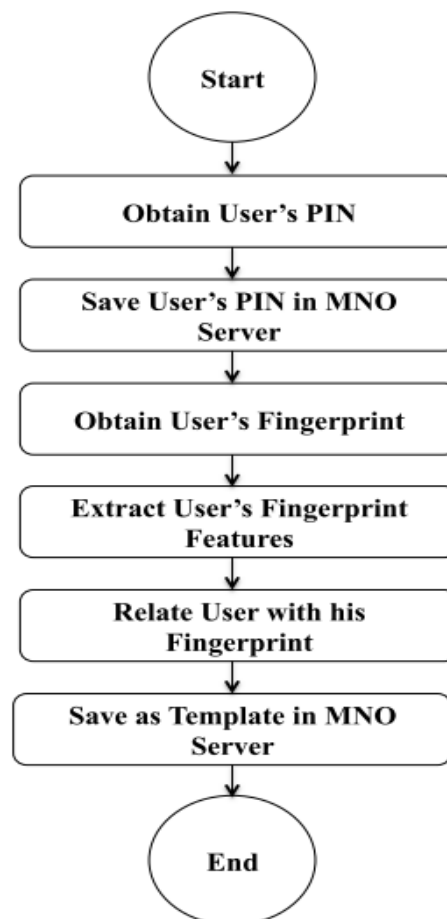


Figure 4 Registration Phase in 2FA model

After the successful enrollment of the user is the execution phase where the user will enter traditional PIN and scan his fingerprint. “The fingerprint is then scanned by the Smartphone’s fingerprint recognition software and matched with the fingerprint template saved during enrollment phase. If the fingerprint matches, user will be given access to the MMSs menu. If the fingerprint does not match, access to the MMSs menu will be denied”, Mtaho (2015). This process is demonstrated in figure 5 below.

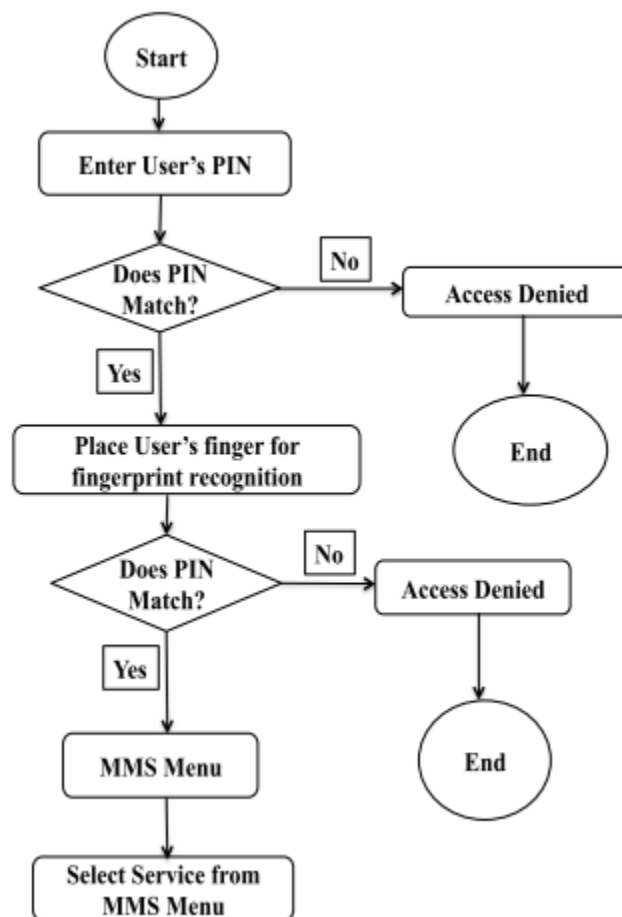


Figure 5 Execution Phase in 2FA model

According to Tiwari, Sanyal, Abraham, Knagskog and Sanyal (2007) “The current online payment systems do not provide adequate user authentication. Thus, it is possible for an unscrupulous user to enter credit card number or account details stolen from valid

users. Financial agencies consider single-factor authentication to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties using web browsers or cell phones/PDA's. They invented a Multifactor Authentication technique to secure web transactions and to increase faith of users on mobile financial transactions, which uses a novel approach to create an authentication system based on TIC's (Transaction Identification code) and SMS to enforce an extra security level for the traditional login in a username/password context. TIC's are user specific unique transaction identification codes which are issued by banks or financial institutions to the user. This code is similar to One Time Password (OTP) and a code is used only once. It further suggests an encryption/decryption technique that would be used to keep TIC's as secret codes on cell phones/PDA's. The user can easily pick up a TIC (from the stored list of TIC's) to initiate secure web transaction using cell phones/PDA's, instead of typing a complicated TIC code in each transaction." The figure 6 below depicts their model.

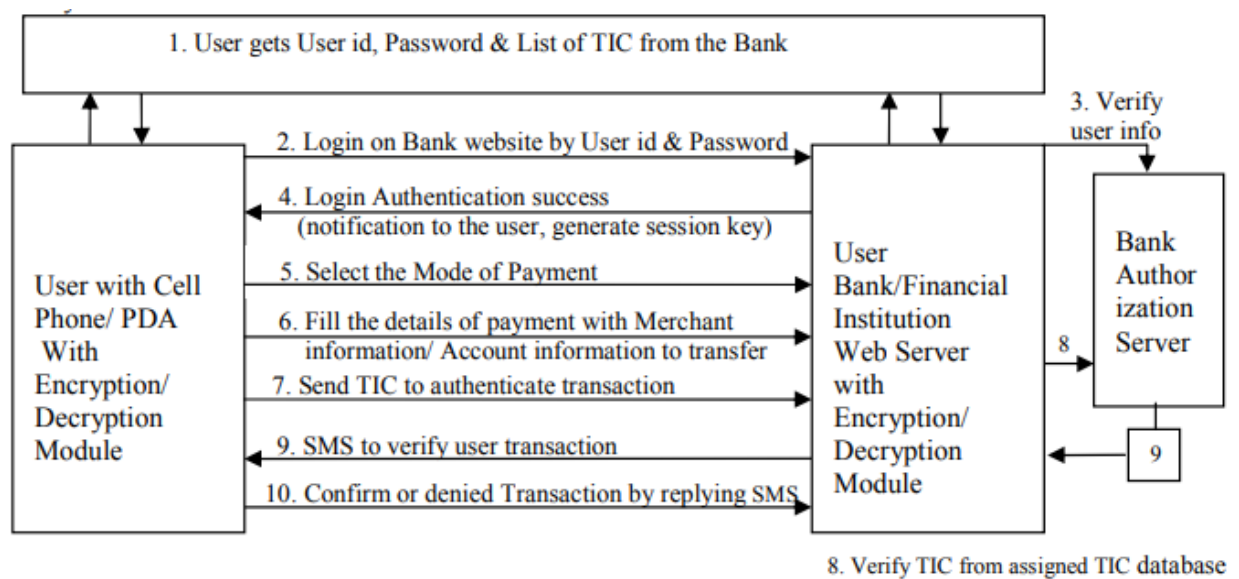


Figure 6 "Protocol for wireless payment: Multifactor secure Web authentication protocol using mobile devices", Tiwari (2007).

In his study Amwoyo (2014) state that "Most Online Systems use Static Password or Single (One-Factor) Authentication, which is susceptible to brute force attack. One-Factor Authentication does not provide adequate security since the static password

remains the same with subsequent logons unless a user manually changes it. It is necessary to mitigate some of the Mobile OTP weaknesses by providing an alternative Multi-Factor Authentication mechanism (which is widely accepted in the cloud computing technology) so as to reduce risks associated with MOTP Authentication. With the wide acceptance of Mobile Money Payment System and subsequent exponential growth of the same in the local market, an alternative E-commerce model needs to be developed to take advantage of the same. Online solutions that are increasingly accessed using mobile devices must be secured against all forms of risks including authentication among others. More so, the solutions require a medium of receiving money for goods and services offered hence the necessity of integration. His project is a roadmap for the creation of secure, local e-commerce solutions using time and session constrained Random Password Multi-Factor Authentication is illustrated through a figure 7 below.”

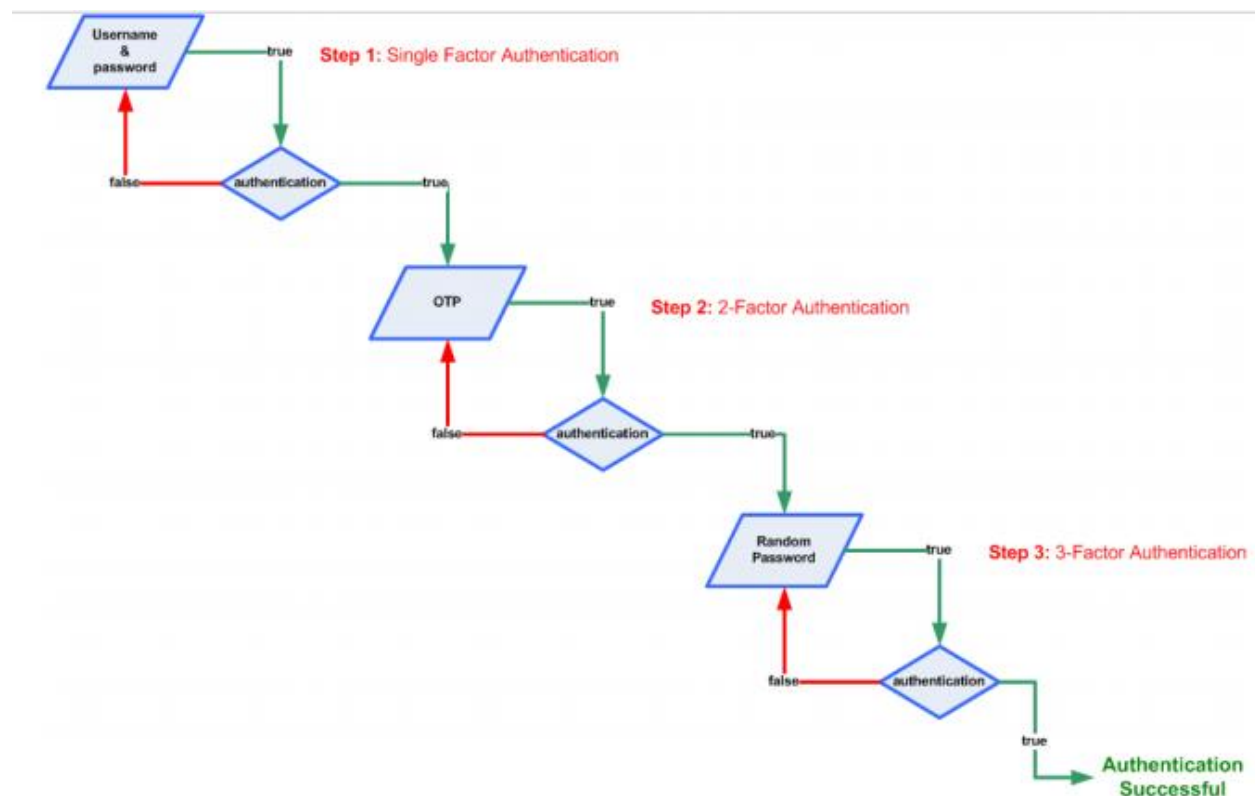


Figure 7 Random Password Authentication Model

Chetalam (2018) proposed “a design science research that aimed at coming up with a voice biometric MPESA model which was developed and implemented to address the main problem of fraudulent MPESA transaction performed using SIM-swap method. The project will improve the MPESA authentication process through the incorporation of a voice biometric functionality that enables the remote control of the individual MPESA accounts by MPESA subscribers with higher efficiency, accuracy and a higher level of authentication. A model was developed on the android platform, VMPEA, to address issues which aimed at implementing a secure mobile-based multi-factor authentication scheme using device specific ID, voice biometric and a PIN for securing MPESA transactions.” The entity relation diagram for the model is illustrated in figure 8 below.

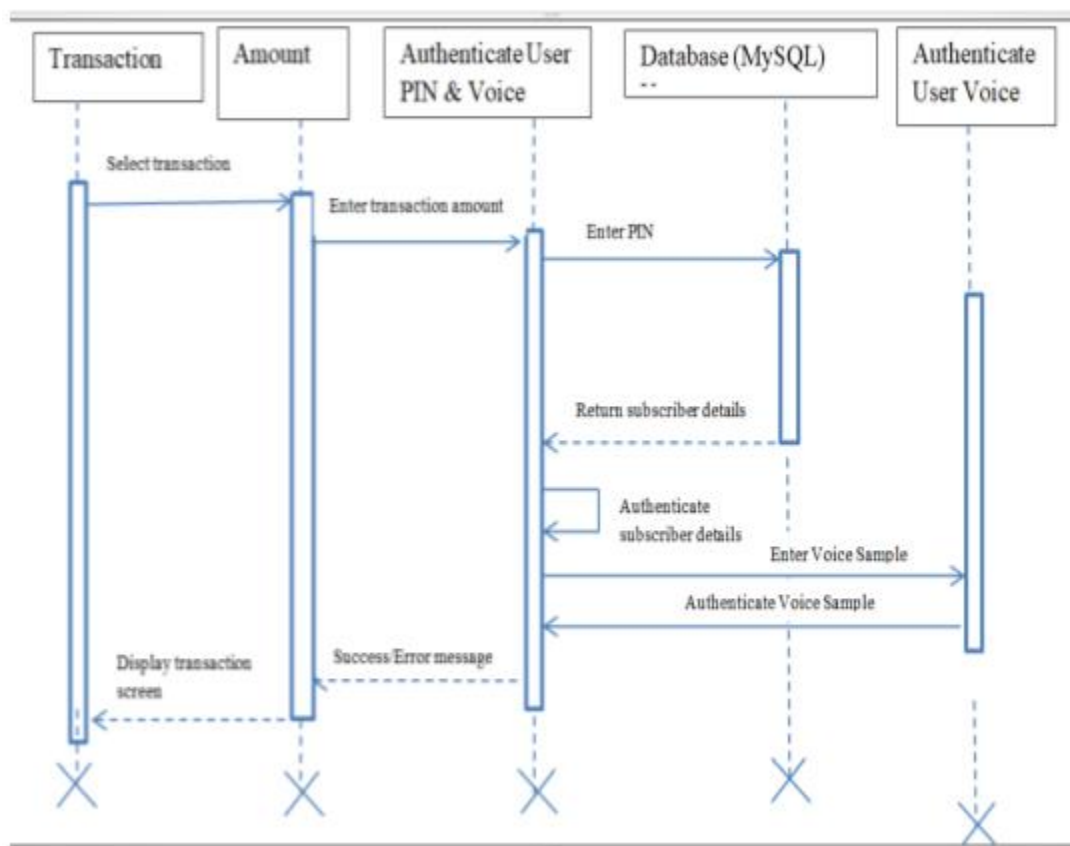


Figure 8 Subscriber Transaction Sequence Diagram

Most of the studies present two factor authentications methods using the combination of single factor authentication (something you know), password or PIN and two-factor authentication which requires (what you are) like biometric voice or fingerprint. This research study will present a conceptual model for improving the security of M-money systems in Lesotho by introducing a more secure and effective multi-factor authentication method that will require the use of something only the user have, mobile phone, something only the user know, 8 character PIN (with upper and lower case letters, numbers and symbol) which will be masked when entered and will expire after every two months and something only the user is, which is biometric face recognition.

2.9 Chapter Summary

Literature has proven that there is numerous security issues that are introduced by the use of PIN as the only authentication method to access M-money services, therefore, the use of Biometric will enhance its security, reducing the challenges that are introduced by MNO employees working with fraudsters to do SIM swaps, targeting accounts with more money. Reliability of M-money account will attract more customers to want to be part of it, and that means the growth in amount of money to be transacted. Using Biometric face recognition will provide with a higher level of identification because the user will need to be physically available than that one of traditional authentication method where any one can enter the PIN and as long as the PIN is correct, the user is authenticated.

CHAPTER 3: RESEARCH METHODOLOGY AND CONCEPTUAL FRAMEWORK

3.1 Introduction

In the preceding chapter, the literature on different biometric methods techniques that can be deployed in M-money systems as well as their strengths and limitations were discussed. Additionally, biometric methods, as well as the literature that proves that BFR technique can enhance the security of M-money systems in Lesotho were discussed. The current chapter will define the method that was used in undertaking the proposed study, as well as justification of using such method. This chapter will start by explaining the proposed work, research design, research method, explaining why it was chosen. It further continues by explaining the sampling technique used its strengths and weaknesses, target population, sampling frame, size, ethics consideration, data collection method, analysis method and why this method was used. It will conclude by defining the research limitations and outlining the proposed conceptual framework for the study. The overall idea of this chapter is to provide motive behind using the selected research method.

3.2 Proposed work

The purpose of this study is to investigate the current security issues of the MMS in Lesotho, and provide a more effective solution that will make the system more reliable and secure. It further identifies the threats that are introduced by method of authentication that is currently used by both EcoCash and M-Pesa, and how it affects the security of their system. Single-Factor Authentication is proven to be less secure method of authentication therefore; this paper will propose a conceptual framework that will assist the technical teams of both companies put in practice an authentication technique to mitigate these issues using BFC method. BFC will eliminate the chances of a fraudster providing false information to the system, therefore increasing the security of the system. The study will definitely solve the current security issues and provide users

and agents with a broad knowledge on how to effectively secure their M-money accounts.

3.3 Research design

“A research design is a procedural plan that is adopted by the researcher to answer questions validly, objectively, accurately and economically. A research design will therefore answer questions that would determine the path the researcher is proposing to take for their research journey. Through a research design decided for the study and communicate to others decisions regarding what study design the researcher is proposing to use, how information is going to be collected from respondents, how they are going to be selected, how the information to be collect is going to be analyzed and how the researcher is going to communicate their findings”, (Kumar, 2011).

In this study, questionnaires were used to investigate the current security measures on M-Pesa and EcoCash, mainly the usage of PIN as the only form of authenticating users while accessing the systems. It will also get respondent's perspective on the proposed BFR as an additional authentication technique to enhance the security of M-Pesa and EcoCash. Convenient non-random technique was used in the study to draw the sample. The researcher also used quantitative approach. Data was collected by both primary and secondary source. Primary data was collected by distributing the questionnaire to respondents to be filled, and through Google online questionnaire forms. Respondents were M-Pesa/EcoCash M-money users across three regions of Lesotho. Secondary data was collected through books, journals and other important written reports. Later the completed questionnaires were then analyzed using tables and graphs.

3.4 Research method

The research method that was used in undertaking this study is quantitative research which can either follow descriptive design, the method that usually measure subjects once or experimental design which measure subjects before and after the study. Therefore, this study adopted descriptive design and used Google online questionnaire forms and distributed questionnaire survey method as the main data collection method which had closed ended questions related to research objectives. This method was selected because of the huge and scattered number of M-money users and agents across Lesotho. Before the questionnaires were distributed, a pilot questionnaire survey was conducted and random sample was selected for that purpose. It was through this pilot study that the questionnaire was correctly measured and finalized.

3.4.1 Justification for the use of quantitative method

“The quantitative findings are likely to be generalized to a whole population or a sub-population because it involves the larger sample which is randomly selected. Besides sampling, data analysis is less time consuming as it uses the statistical software such as SPSS”, (Rahman, 2016). It is also stated that “this method allows one to measure the responses of a number of participants to a limited set of questions, thereby facilitating comparison and statistical aggregation of the data. The results of closed-ended questionnaires help the researchers to identify a general pattern of participants’ reactions to a treatment or programme. Quantitative methods and procedures allow the researchers to obtain a broad and generalized set of findings and present them succinctly and parsimoniously. Quantitative methods can provide parsimonious statistical data through mean achievement scores and hours of instruction”, (Yilmaz, 2013).

3.5 Sampling

Sampling is defined as “the process of selecting a few (a sample) from a bigger group (the sampling population) to become the basis for estimating or predicting the prevalence of an unknown piece of information, situation or outcome regarding the bigger group”, (Kumar, 2011). The study proposed an additional authentication method on top of the one that is currently being used by M-money systems in Lesotho. The sample data collected from randomly selected M-money users and agents was used as a basis to reflect the feasibility of the proposed authentication method. The main aim of the sample was to determine the availability of continuous, unbiased, and random data from different sources of M-money users and agents. Consequently, the sample was the foundation to investigate the constraint of the proposed multifactor authentication method in M-money systems.

3.5.1 Study population

The population sample for this study was selected from M-money users of M-Pesa and EcoCash in Lesotho distributed over three regions, lowlands (Maseru, Berea), semi lowlands (Mafeteng, Leribe, Mohale’shoek, Butha-buthe) and highlands (Quthing, Qacha, Thaba-tseka, Mokhotlong). This three regions are different in relation to the widespread use of M-money services, the lowlands has the higher number of active M-money users and agents, followed by semi-lowlands, then highlands with the lowest number, due to different challenges they are faced with, including, a smaller number of agents, or having to travel a long distance to deposit or withdraw money from an agent. Some users use both M-money services, and some agents provide services for both M-Pesa and EcoCash.

3.5.2 Sampling frame

For this research study, population sample was the representation of the population from randomly selected M-money users and agents of both M-Pesa and EcoCash living in urban areas, semi-urban and rural area of Lesotho.

3.5.3 Sampling size

3.5.3.1 Sample size determination

The following process consisting of four steps was followed to determine the appropriate sample size for this research:

1. Defining the approximate margin of error accepted.
2. Defining the confidence level needed for the study.
3. Defining population size for the study.
4. Defining response distribution

3.5.3.2 Sample size for M-money users

The population size of registered M-money users in Lesotho according to International Monetary Fund (2018) statistics were approximately 1, 680, 000 users which was 60% of Lesotho's population. The margin of error accepted for the survey feedback was typically 5%, applying common confidence level choice of 90%, response distribution of 50%, the sample size required for this research was determined to be 271 M-money users.

The sample size n and margin of error E are given by formula below:

$$\begin{aligned}x &= Z(c/100)^2 r(100-r) \\n &= N x / ((N-1)E^2 + x) \\E &= \text{Sqrt} [(N - n)x / n(N-1)]\end{aligned}$$

Where N is the population size, r is the fraction of responses that the researcher was interested in, and $Z(c/100)$ is the critical value for the confidence level c .¹⁹

3.5.4 Sampling technique

“The purpose of sampling in quantitative research is to draw inferences about the group from which you have selected the sample”, (Kumar, 2011). In his study, (Kothari, 2004) indicates that “samples can be either probability samples or non-probability samples. With probability samples each element has a known probability of being included in the sample but the non-probability samples do not allow the researcher to determine this probability”. The study adopted convenience non-probability sampling technique.

According to Kothari (2004) “non-probability sampling is that sampling procedure which does not afford any basis for estimating the probability that each item in the population has of being included in the sample. In this type of sampling, items for the sample are selected deliberately by the researcher; his choice concerning the items remains supreme. In other words, under non-probability sampling the organizers of the inquiry purposively choose the particular units of the universe for constituting a sample on the basis that the small mass that they so select out of a huge one will be typical or representative of the whole”. On the other hand, Kumar (2011) indicates that “non-probability sampling designs are used when the number of elements in a population is either unknown or cannot be individually identified. In such situations the selection of elements is dependent upon other considerations”.

“Convenience sampling (also known as Haphazard Sampling or Accidental Sampling) is a type of non-probability or non-random sampling where members of the target population that meet certain practical criteria, such as easy accessibility, geographical proximity, availability at a given time, or the willingness to participate are included for the purpose of the study”, (Etikan, Musa, Alkassim, 2016). Due to limited time frame and unavailability of funds to the researcher, this method was the best option as it allowed the researcher to collect data from various respondents in various places. The researcher chooses those respondents that were available at the time the questionnaires were distributed, at that particular location. “In contrast, in probability sampling, each element in the population has a known nonzero chance of being selected through the use of a random selection procedure”, (Michael, 2011). This

technique has limitations, as data gathered from it cannot be generalized to represent the population of M-money users and agents of M-Pesa and Ecocash.

3.5.4.1 Advantages of Convenience non-probability sampling

“Non-probability sampling is less expensive than probability sampling and can often be implemented more quickly”, (Michael, 2011). “It is useful especially when randomization is impossible like when the population is very large. It can be useful when the researcher has limited resources, time and workforce. It can also be used when the research does not aim to generate results that will be used to create generalizations pertaining to the entire population. Therefore, there is a need to use non-probability sampling techniques”, (Etikan et al, 2016). This method is more flexible as it permits the researcher to choose the participant that is available at his convenient location or time.

3.5.4.2 Disadvantages of Convenience non-probability sampling

According to Kothari (2004) “In convenience sampling design, personal element has a great chance of entering into the selection of the sample. The investigator may select a sample which shall yield results favourable to his point of view and if that happens, the entire inquiry may get vitiated. Thus, there is always the danger of bias entering into this type of sampling technique. Sampling error in this type of sampling cannot be estimated and the element of bias, great or small is always there”. Etikan et al (2016) further emphasize that this “sampling technique has a lot of limitations due to the subjective nature in choosing the sample and thus it is not good representative of the population. Non-probability sampling is a sampling technique where the samples are gathered in a process that does not give all the participants or units in the population equal chances of being included. Convenience sampling is that it is likely to be biased. Because of the high self-selection possibility in non-probability sampling, the effect of outliers can be more devastating in this kind of subject selection. Outliers are cases whom consider as not belonging to the data. In a convenience sample, on the contrary, neither biases nor their probabilities are quantified. In fact, the researcher does not know how well a

convenience sample will represent the population regarding the traits or mechanism under research. What makes convenience samples so unpredictable is their vulnerability to severe hidden biases”.

3.6 Data collection methods

“In dealing with any real-life problem it is often found that data at hand are inadequate, and hence, it becomes necessary to collect data that are appropriate. There are several ways of collecting the appropriate data which differ considerably in context of money costs, time and other resources at the disposal of the researcher. The primary data are those which are collected afresh and for the first time, and thus happen to be original in character. The secondary data, on the other hand, are those which have already been collected by someone else and which have already been passed through the statistical process. There are several methods of collecting primary data, particularly in surveys observation method, interview method, through questionnaires, through schedules, and other methods”, (Kothari, 2004). In this study, data was collected through closed ended questionnaires, “a closed ended questionnaire is a written list of questions, the answers are set out in the questionnaire and the respondent ticks the category that best describes their answer”, (Kumar, 2011).

The questionnaire survey method was significant data collection method taking into account the number of users and agents that needed to be surveyed and how isolated they were. While taking into consideration the limitation of resources the researcher is faced with, this method of data collection was the best option as it allowed data to be collected through Google online questionnaires forms and some were distributed and collected. Kothari (2004) indicates that “before using this method, it is always advisable to conduct pilot study (Pilot Survey) which is said to be the rehearsal of the main survey and it brings to the light the weaknesses (if any) of the questionnaires and also of the survey techniques. From the experience gained in this way, improvement can be effected”. The target population for the study was 271, questionnaires were send out and collected from 250, and 21 participants were invited to fill Google online

questionnaire, and 7 questionnaires were completed online, 219 were collected from potential participants and only 168 questionnaires considered to be usable which constitutes 61.9% response rate, amongst 51 questionnaires that were considered unusable, some of the sections or questions were left unattended. The questionnaire was accompanied by a formal letter indicating the purpose of the study and consent form that participants had to fill before they could attempt the questionnaire to ensure that they are aware of the purpose of the research study before they were involved in the study.

3.6.1 Pilot Study

Before the distribution of the main questionnaire a pilot study was conducted to verify and ensure that the questionnaire was clear and reliable. The comments and critics that were received were helpful enough to ensure that the main questionnaire was valid, comprehensive and precise, and whether it will ensure that dependable data will be collected. "Pilot would provide a chance to clarify any confusing questions to respondent and remove any redundant. In general, pilot should provide clear answers that should be understood as intended", (Mohamed, 2014). Pilot questionnaire survey for the pilot study consisted of the letter detailing background information about the study, questionnaire consent form, as well as four section drafted questionnaire. In this pilot study, 30 questionnaires were distributed. Given the small number of the sample for the pilot study, data collected was only used to modify the methods of collecting research data and research-related amendment to the main questionnaire.

The first drafts of the questionnaires were piloted with M-money users of M-Pesa/EcoCash around the district of Maseru. They were asked if they are willing to participate in a questionnaire pilot study. Those who were willing were given the drafted questionnaire and it was agreed that the researcher will come and collect them the following day. Participants were required to indicate how long it took them to complete the whole questionnaire and point out the challenges they had, or to comment on the

overall questionnaire. When the drafted questionnaires were collected the following day, respondents also had face-to-face interaction with the researcher, where they further voiced out their suggestion.

3.6.2 Justification for using questionnaires

The questionnaire enables respondents to select an answer from a list of options, each questionnaire should also try to answer the overall objective of the study which will be the representation of the whole population, and be able to show the responder's perspective of using PIN and BFR technique as the two methods of authenticating users when accessing their M-money accounts. It is indicated that using questionnaires “response choices can clarify the question’s meaning for respondents, again less articulate or less literate respondents are not at a disadvantage, as it provides guide or options where the respondent can choose answers from”, (Copeland, 2017). “Timeliness is another significant benefit of this type of survey instrument. Because the questionnaire can be hosted online or sent electronically via email, responses can be collected, tabulated and evaluated more quickly. Survey questionnaire reduce bias. Because there are no survey takers speaking with respondents to impart verbal or body language cues, some element of bias is reduced through an online survey. Therefore, results obtained are considered to be more objective and scientific”, (Elizabeth, 2013).

3.6.3 Strengths of using questionnaires as data collection method

Kothari (2004) emphasize that “there is low cost even when the universe is large and is widely spread geographically”. Kumar (2011) adds by saying “as you do not interview respondents, you save time, and human and financial resources. The use of a questionnaire, therefore, is comparatively convenient and inexpensive. Particularly when it is administered collectively to a study population, it is an extremely inexpensive method of data collection”. Kothari (2004) further indicates that when using questionnaires, “respondents have adequate time to give well thought out answers, again large samples can be made use of and thus the results can be made more

dependable and reliable”. Lastly, Kumar (2011) state that “it offers greater anonymity as there is no face-to-face interaction between respondents and interviewer, this method provides greater anonymity. In some situations where sensitive questions are asked it helps to increase the likelihood of obtaining accurate information”.

3.6.4 Weaknesses of using Questionnaires as data collection method

“One main disadvantage is that application is limited to a study population that can read and write. It cannot be used on a population that is illiterate, very young, very old or handicapped. Questionnaires are notorious for their low response rates; that is, people fail to return them. If you plan to use a questionnaire, keep in mind that because not everyone will return their questionnaire, your sample size will in effect be reduced. The response rate depends upon a number of factors: the interest of the sample in the topic of the study, the layout and length of the questionnaire the quality of the letter explaining the purpose and relevance of the study and the methodology used to deliver the questionnaire”, (Kumar, 2011).

“There is inbuilt inflexibility because of the difficulty of amending the approach once questionnaires have been dispatched”, Kothari (2004). On the other hand, (Kumar, 2011) says “if, for any reason, respondents do not understand some questions, there is almost no opportunity for them to have the meaning clarified unless they get in touch with the researcher (which does not happen often). If different respondents interpret questions differently, this will affect the quality of the information provided. As respondents can read all the questions before answering (which usually happens), the way they answer a particular question may be affected by their knowledge of other questions”. Kothari (2004) further says “There is also the possibility of ambiguous replies or omission of replies altogether to certain questions; interpretation of omissions is difficult”.

3.7 Ethics consideration

According to Kumar (2011), “there are certain behaviours in research such as causing harm to individuals, breaching confidentiality, using information improperly and introducing bias that are considered unethical in any profession. First the researcher should obtain the respondents’ informed consent. Informed consent implies that subjects are made adequately aware of the type of information the researcher want from them, why the information is being sought, what purpose it will be put to, how they are expected to participate in the study, and how it will directly or indirectly affect them. It is important that the consent should also be voluntary and without pressure of any kind.”

This study considered certain ethical guidelines to ensure that correspondents are aware of what the study is about. As it was mentioned earlier, all participants reported their written acceptance regarding their participation in the research, through a signed consent and briefing letter. Next to this, participants were fully informed regarding the objectives of the study, while they were reassured that their answers were treated as confidential and used only for academic purposes and only for the purposes of the particular research”.

3.7.1 Informed consent

Participants in the questionnaire were briefed fully on the purpose and conduct of the research. It was made very clear to them that participation was voluntary and they could withdraw from the project at any stage without penalty. The rationale behind this study was explained. Data collection and analysis were described clearly to them so that they knew what they were doing.” It was also emphasized that report on the results of this research their identity will remain anonymous. Participants were informed that there was no harm in participating in this research than that ordinarily encountered in daily life.

When all participants agreed that they understood everything clearly, they were asked to give their consent to participate in this study by signing a written consent form”.

3.8 Data analysis method

According to Kothari (2004) “analysis means the computation of certain indices or measures along with searching for patterns of relationship that exist among the data groups. Analysis, particularly in case of survey or experimental data, involves estimating the values of unknown parameters of the population and testing of hypotheses for drawing inferences. Analysis may, therefore, be categorized as descriptive analysis and inferential analysis (Inferential analysis is often known as statistical analysis). Descriptive analysis is largely the study of distributions of one variable”.

After the data have been collected, the researcher turns to the task of analysing them. Most of the questions involved indicating an answer by ticking a box, this generated ordinal data. The coding of all the information on the questionnaire was done by assigning numbers to the answers indicated in all sections of the questionnaire. Establishing these codes on the distributed questionnaire was helpful at data entry time, after the responses on the questionnaire were coded then they were captured in Microsoft Excel and then imported in SPSS (Originally, Statistical Package for the Social Sciences) for analysis. It is important to ensure that data that has been entered corresponds to the data on the questionnaires that means going back to the questionnaires to confirm data entered. The study used SPSS to analyse data, and charts, tables and graphs were used.

3.8.1 Computer-based analysis tools

3.8.1.1 SPSS (Originally, Statistical Package for the Social Sciences)

“SPSS is a computer application that provides statistical analysis of data. It allows for in-depth data access and preparation, analytical reporting, graphics and modeling. SPSS was released in its first version in 1968. SPSS is menu-driven. That means users can execute statistical analyses, simple or complex, by clicking a series of pull-down menus

and selecting the desired pre-programmed commands. However, many researchers or analysts may use certain statistical procedures that are not pre-programmed into SPSS. As a result, SPSS allows users to create custom programs or to link together multiple pre-programmed operations to be applied in sequence”, (Mohamed, 2014).

3.8.1.2 Excel

In this study, Microsoft Excel was also used for data analysis. Kanal and Raman (2016) indicate that “Microsoft Excel provides for analyzing of data with the help of a special tool called analysis toolpak. The analysis toolpak is an excel add-in that provides for statistical, financial and engineering analysis upon the data. The data and criteria is provided for each of the analysis options that we have under the analysis toolpak option. It involves the use of macro functions to perform operations and produce outputs in the form of tables or charts. Firstly, to use the analysis toolpak, it needs to be loaded into excel”.

3.9 Research limitations

The limited resources that were available to the researcher were contributing factors to the effectiveness of this research study. The questionnaires were distributed to a widespread population within a limited time frame, and funds were not available for transportation and food. The researcher had to take money from own pocket, and was not adequate therefore some remote highlands places were not able to be reached. The reliability and validity of the study may depend on the authenticity of information provided by the respondents. The findings from this study can not be generalised, data was based only on sample population.

3.10 Conceptual Framework for the study

The proposed model is based on Two-Factor Authentication model (2FA) by Mtaho (2015), the model combines the current approach of using PIN and adds another layer of security that uses fingerprint recognition technology, it comprises of two phases, the enrollment and authentication phase. The model might be useful as the research try to propose a multifactor model that will strengthen the authentication process of a MMS. Nonetheless, this framework does not solve the security issues that are introduced by the current authentication process of using PIN, but rather add extra layer of security on top of the existing one. The proposed conceptual will utilize some of the components from above model, it will solve the security issues that are introduced by PIN and BFR will be used as added layer that will enhance security of MMS.

3.10.1 The current Model of MMS

In the current model before the user can use M-money services they have to be enrolled, this process require the user to provide the system with their details (name, surname and ID), then register a PIN, this details are saved in the server, and compared against the one the user will enter during the authentication phase. Figure 9 below illustrates registration phase in current system.

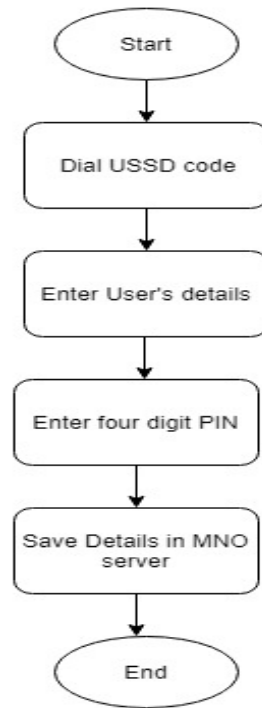


Figure 9 Registration in current M-money system

3.10.2 Execution Phase

“During the execution phase, in order to access MMS, user must initiate transaction by dialing a USSD code, selects a service from available service options, enters PIN and submit the request to the appropriate MNO’s application server. The application server then authenticates the PIN, if the PIN is correct the requested service will be provided, otherwise the user will be given the opportunity to retry for the maximum of three trials. The major drawback of this model is that if unauthorized user knows the customer’s PIN and gets access to someone’s SIM card, a fraudulent transaction can be committed from customer’s mobile money account”, Mtaho (2015). Figure 10 below illustrates the execution phase of this model.

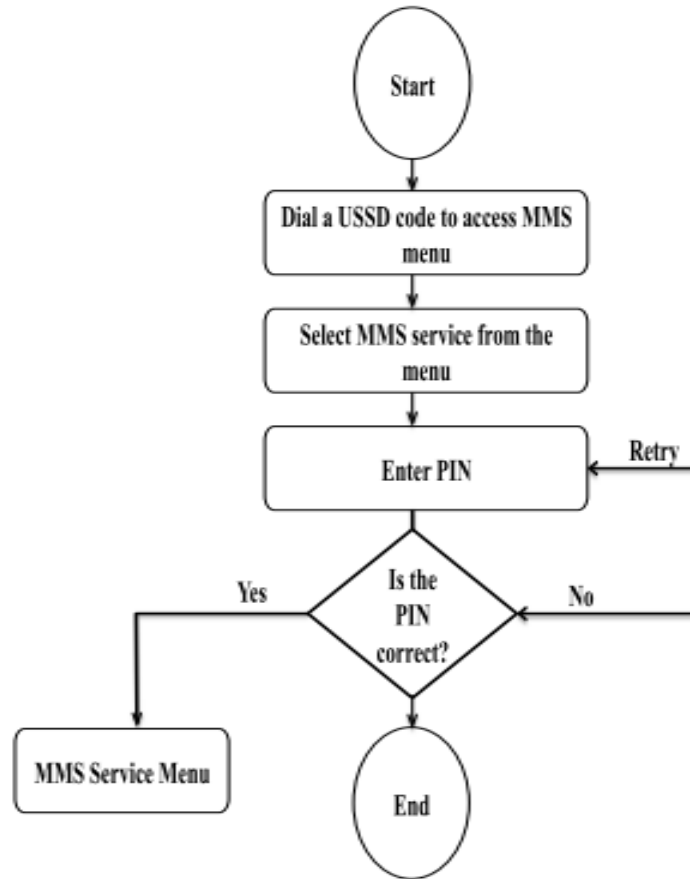


Figure 10 Execution Phase in Current M-money System (Mtaho, 2015)

3.10.3 Proposed Conceptual framework for multi-factor authentication for M-money systems

3.10.3.1 Registration Phase

The proposed model will require the user to be registered and then authenticated. The registration process enables the user to use the system and will require the user to enter their personal details which includes name, surname, date of birth and Identification (ID) number. The user will then register PIN, as opposed to the current authentication process that use four digit PIN, the proposed model will increase the field of characters and prompt the user to enter 8 characters long PIN (combination of uppercase or small letters, numbers and symbols). As the user enters the characters they will be masked, the masking of characters is to prevent others from seeing what is

being entered. To further enhance the security of the system, the server will enforce the user to change their PIN after every two months. Hashing algorithm will be used to run PIN through, this hash algorithm will produce a unique value based on entered PIN, then store that value in a server instead of PIN. After the PIN registration, the user will capture biometric data face image which will be stored in a biometric database server, biometric cryptosystems will be used to secure biometric data, by converting the data into biometric template which will be stored and retrieved for authenticating the user. The proposed model presumes a smart-phone with a front camera is used. This feature is illustrated in figure 11 below.

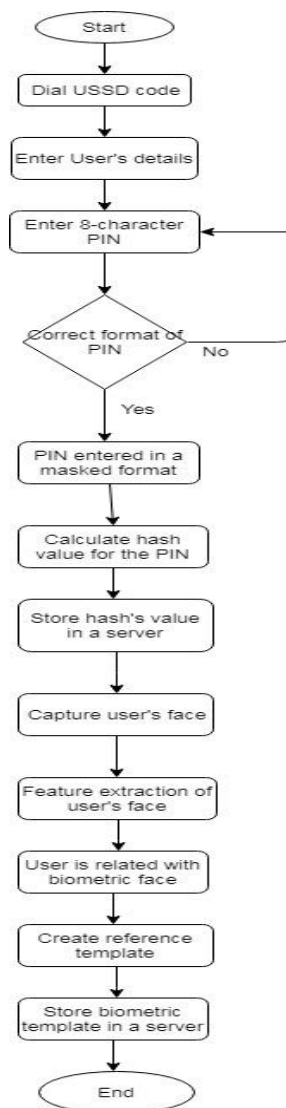


Figure 11 Flowchart for Registration of the user in the proposed framework

3.10.3.2 Authentication Phase

As opposed to current model where users dial *100# for ETL subscribers and *111# for VCL subscribers to access M-money menu and select the service they want before they enter their PIN, the proposed model will require the user to enter their 8-character PIN that will be masked as entered and capture their biometric face before they can user can access M-money services menu. The PIN that is entered will be verified against the one stored in the server during the registration phase, if correct the user is prompted to take a picture, that will be compared against the template stored in the biometric server during the registration phase. If either PIN or biometric data provided by the user does not match with the ones stored in the server, the user will be prompted to re-enter both PIN and biometric data for the second time, the third time access will be denied and account will be blocked. This authentication phase is depicted in figure 12 below. After the authentication phase the user can perform different transactions which include sending money, depositing money, paying bills, buying airtime and withdrawing money.

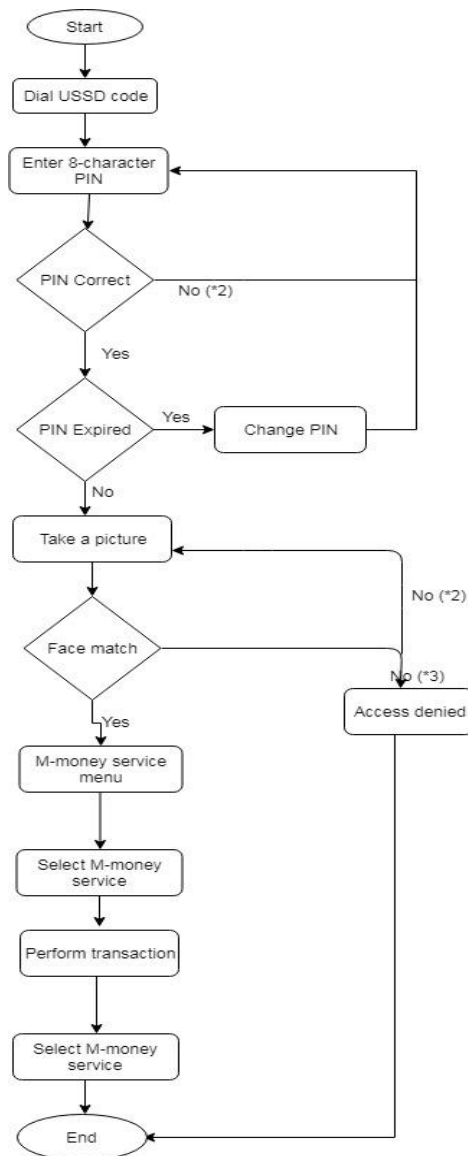


Figure 12 Flowchart for Authentication phase for proposed system

3.11 Chapter summary

The chapter discussed the method that was used in undertaking the proposed study, as well as justification of using such method. The chapter commenced by explaining the proposed work, research design, research method and explaining why that method was chosen. It further explained the sampling technique used its strengths and weaknesses, target population, sampling frame, size, ethics consideration, data collection method, analysis method and why this method was used. It concluded by pointing out the

research limitations, the overall idea of this chapter was to provide motive behind using the selected research method.

CHAPTER 4: RESEARCH FINDINGS AND DATA ANALYSIS

4.1 Introduction

This chapter will present results and analyse data collected from a number of participants who contributed in a self administered questionnaires as well as emailed questionnaires. The target population for the study was 271, questionnaires were send out and collected from 250, and 21 participants were invited to fill Google online questionnaire, and 7 questionnaires were completed online, 219 were received from potential participants and only 168 questionnaires considered to be usable which constitutes 61.9% response rate, amongst 51 questionnaires that were considered unusable, some of the sections or questions were left unattended.

The chapter will provide analysis and findings of participant's responses based on four sections; the first section presents demographic data like gender, age, region, the M-money the participant uses as well as the duration of use. The second section comprises of rating the M-money services in terms security, affordability as well as other factors. The third section will represent the challenges in M-money and how the participant solved the problems. Last section discussed the security of M-money services and how the proposed model will improve the security of the system. Tables, pie charts, bar charts were utilized to analyse data.

4.2 Background of data

Total of 271 participants were targeted across the country of Lesotho, only 168 responded within a given time frame and were satisfactorily completed. The results are presented as follows in the subsequent sections. The first section represents demographic data, which includes gender, age group, region, M-money transfer service, duration and the type of phone the subscriber use for M-money services. The following section will include data that will rate their M-money service in terms of reliability and convenience, affordability, time efficiency and ease of use. The third section will represent challenges in M-money services, it will comprise of challenges facing users, how were their problems solved. The last section will include data about security of M-

money, security of PIN, frauds in M-money, and the efficiency of biometric face recognition.

4.3 Demographic Information

Demographic data includes gender, age group, region, M-money transfer service, duration and the type of phone the subscriber use for M-money services. The following is the representation of demographic data.

4.3.1 Classification of respondents by gender

Respondents were asked to indicate their gender, figure 13 shows 57% of respondents being males and 43% being females and none of the respondents preferred not to specify their gender. This demonstrates that a good number of respondents were therefore males.

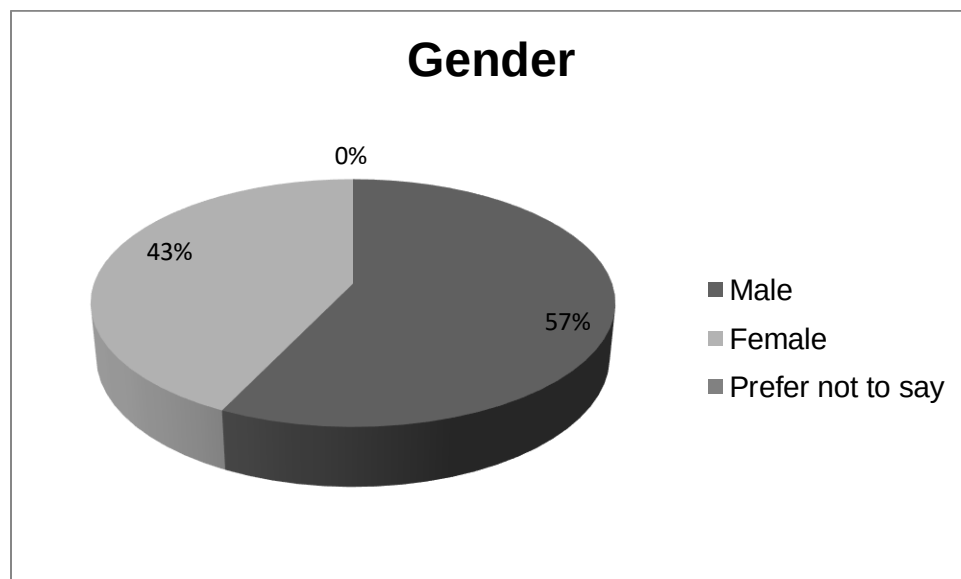


Figure 13 Respondents by gender

4.3.2 Classification of respondents by age

Table 2 below demonstrates respondent's distribution by age, subscribers are allowed to register for M-money from the age of 16. The results indicates that a great number of

respondents were group 25-33 with the highest percentage of 39.9%, with group 16-24 being the second with 20.8%, followed by group 34-42 with 19%, group 43-51 with 14.9% and lastly group 52 and above with 5.4%.

Table 2 Age Distribution

Age	Frequency	Percentage
16-24	35	20.8
25-33	67	39.9
34-42	32	19
43-51	25	14.9
52 & above	9	5.4
TOTAL	168	100

4.3.3 Classification by region

Through figure 14 the study confirm a high percentage of respondents were from the lowlands with 55%, followed by 28% of respondents living in semi lowlands and lastly highlands with 17%. This indicates that there are more people having mobile phones and more people using the M-money services in the lowlands due to its higher population as well as high availability of agents in this region, than both semi lowlands and highlands region.

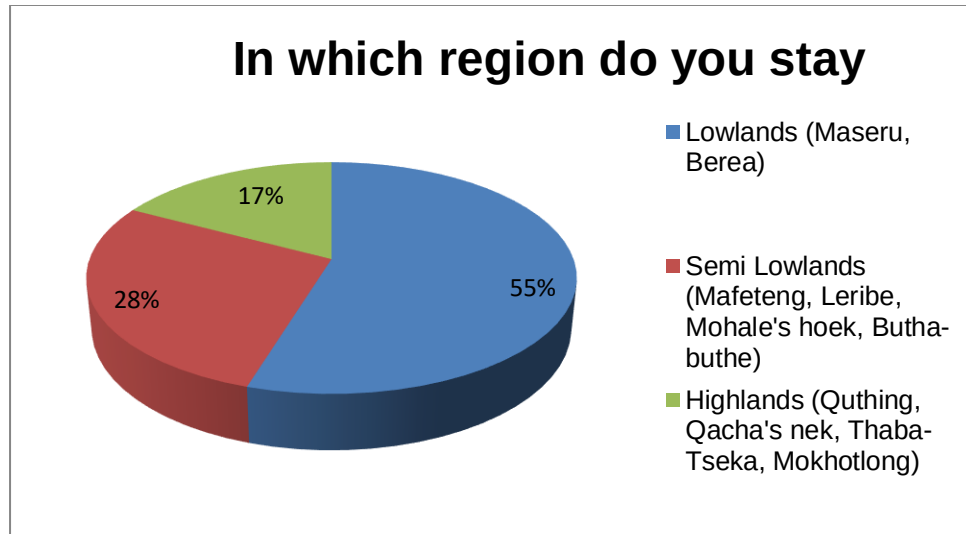


Figure 14 Place of residence

4.3.4 Classification by M-money transfer service

As demonstrated in figure 15 the study revealed that most respondents were users of M-Pesa only with the highest percentage of 57%, while 26% is the users of EcoCash only and 17% use both M-Pesa and EcoCash.

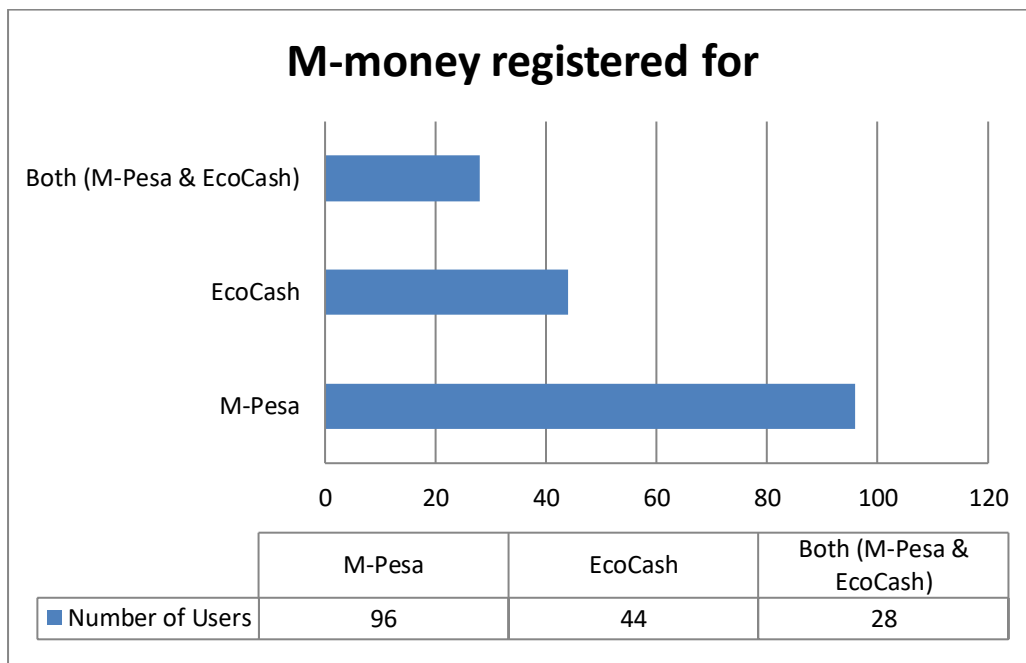


Figure 15 Number of Users registered for M-money service

4.3.5 Classification of how long respondents have been using M-money service

Respondents were asked to specify how long they have been using their M-money service for, through frequency distribution in table 3 it is evident enough that most respondents have been using this service fall within group 3-4 years with 52%, followed by group 5-7 years with 24%, the third group being 1-2 years with 17% and lastly 7% of the respondents have been using the service for a period less than a year.

Table 3 Duration of using M-Money Service

Duration of Use	Number of Users	Percentage
less than a year	11	7
1-2 years	29	17
3-4 years	88	52
5-7 years	40	24
Total	168	100

4.3.6 Classification by Mobile phone used for M-money services

As shown in figure 16 below the study revealed that 51% of the respondents use second generation (2G) phones to access their M-money services, while 42% use Smartphone, 4% using tablet and 3% used all of them. This shows that majority of the respondents' still use 2G phones.

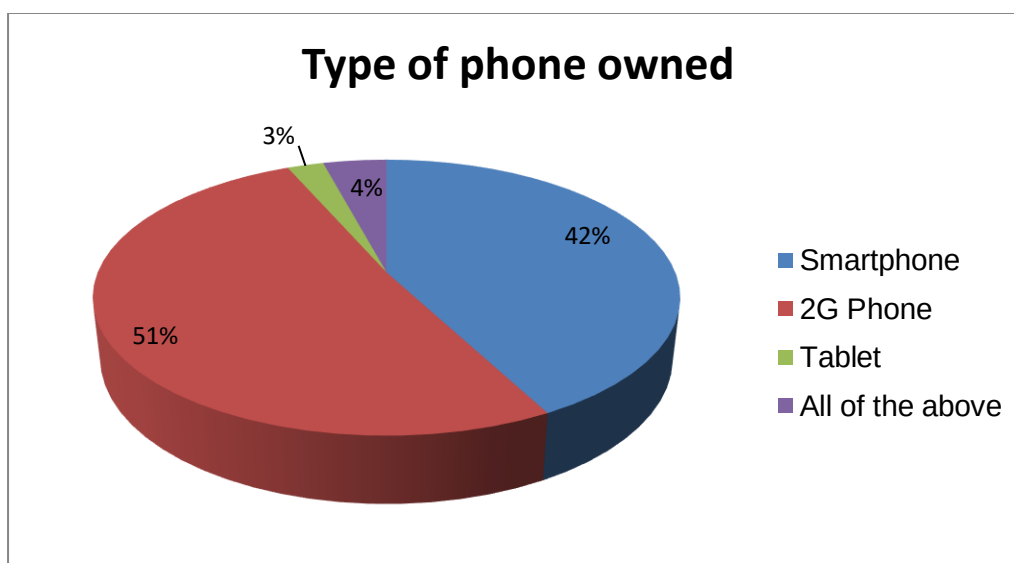


Figure 16 Type of phone used for M-money

4.3.7 A Cross tabulation of region against type of mobile phone used for M-money services

Table 4 illustrates that majority of respondents who use second generation (2G) phones for their M-money services are from the highlands with 55.8%, this can be attributed by the fact that most people cannot afford more expensive phones. High usage of Smartphone is seen in the lowlands with 57.7%, because of their engagement in social media and they are more advanced in technology. The use of tablets is seen equally in the lowlands and in the semi lowlands with 50.0% in both regions.

Table 4 A cross tabulation of region against type of phone used

Region	Type of Phone used				Total
	2G Phone	Smartphone	Tablet	All kinds of phones	
Lowlands (Maseru, Berea)	14.0%	57.7%	50.0%	71.4%	0.48
Semi Lowlands (Mafeteng, Leribe, Mohale's hoek, Butha-	30.2%	25.4%	50.0%	28.6%	0.34

buthe)					
Highlands (Quthing, Qacha's nek, Thaba-Tseka, Mokhotlong)	55.8%	16.9%	0.0%	0.0%	0.18
Total	100.0%	100.0%	100.0%	100.0%	100.0%

4.4. Rating the Mobile Money Transfer Services

In this section respondents were asked to rate the services of their M-money by using five points likert scale rating from 1 strongly agree to 5 strongly disagree. In this section nine items were measure using this scale.

4.4.1 Mobile Money Systems (MMS) are reliable and convenient

In figure 17 respondents demonstrated their level of agreement based on whether they consider their MMS reliable and convenient. 46.4% agree, 38.7% uncertain, 14.9% strongly agree, with no participants indicating that they disagree or they strongly disagree. Therefore, best part of users believed that MMS are reliable and convenient.

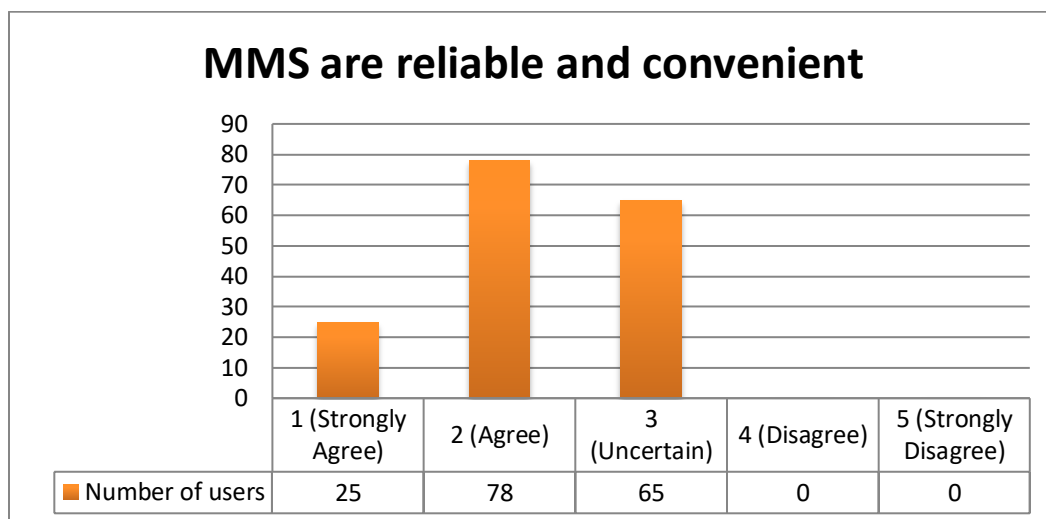


Figure 17 MMS are reliable and convenient

4. 4.2 MMS are time efficient

Figure 18 below illustrate the level of agreement of participants, based on whether they regard their MMS time efficient, 56.5% of participants are uncertain, while 25% agree, and 18.5% strongly agree. With no participants disagree or strongly disagree, therefore the study concludes that majority of participants are uncertain that MMS are time efficient.

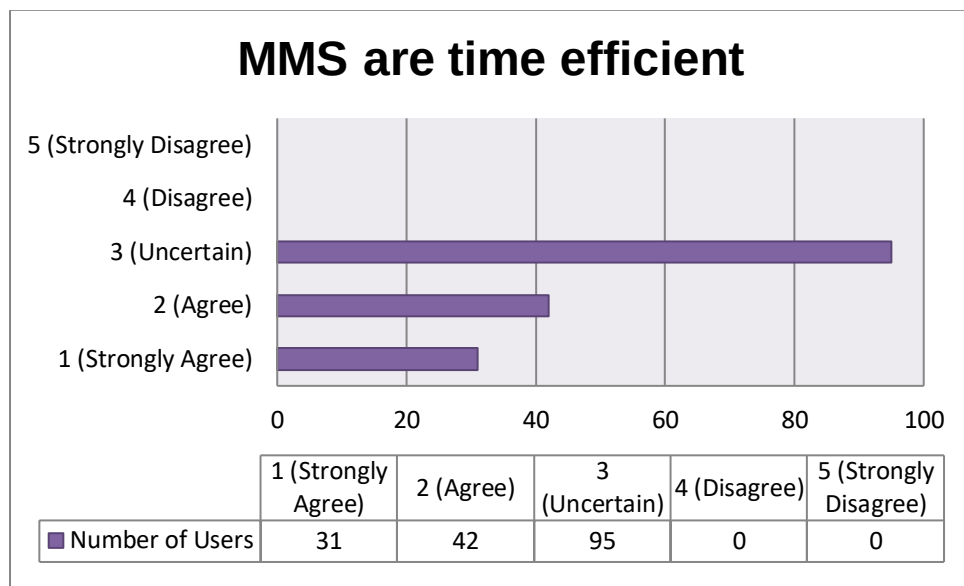


Figure 18 MMS are time efficient

4. 4. 3 MMS are secure

As illustrated in figure 19 below, respondents show their agreement level based on the statement that said MMS are secure, 51.8% of respondents are uncertain, 32.1% agree, 11.9% disagree, 3% strongly agree, strongly disagree 1.2%. As a result, majority of respondents are doubtful that MMS are secure.

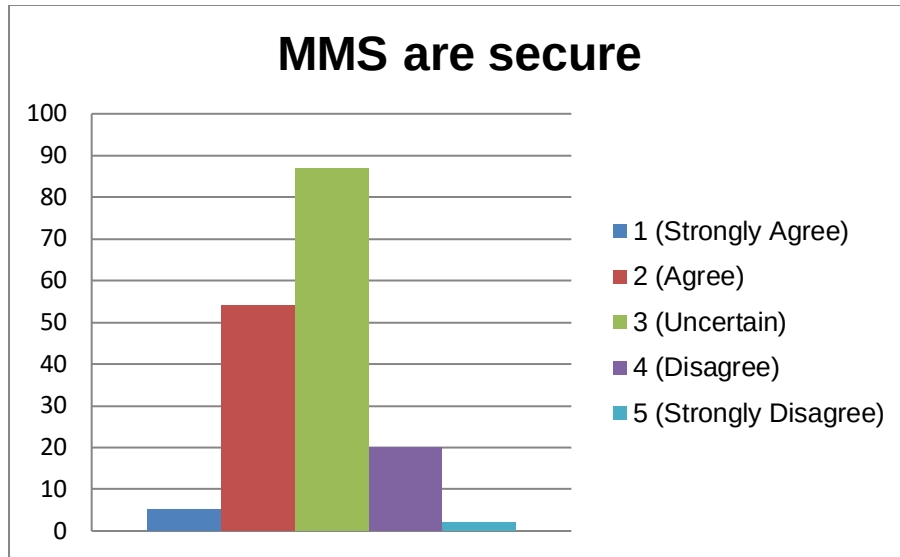


Figure 19 MMS are secure

4. 4. 4 MMS are affordable

Figure 20 below demonstrates agreement level of participants based on the statement that MMS are affordable. A great number of respondents strongly agree with the statement with 46.4%, 35.1% agree, 13.1% uncertain, 5.4% disagree. With no representation of strongly disagree, thus, this is evident that MMS are affordable.

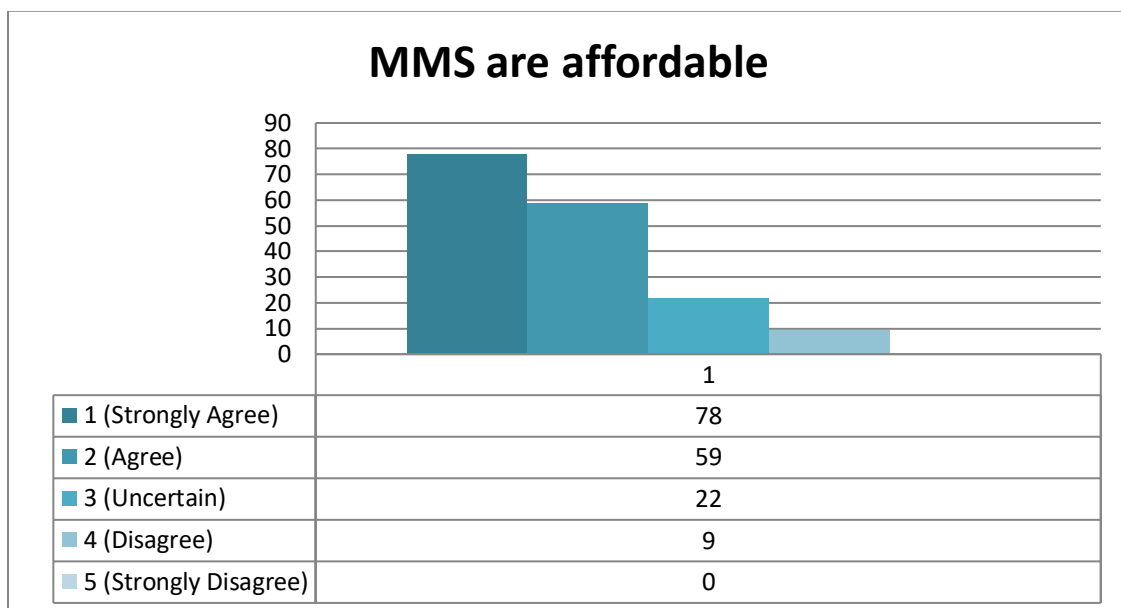


Figure 20 MMS are affordable

4. 4. 5 MMS are easy to use

Figure 21 below shows agreement level of respondents to the statement that said MMS are easy to use, with 50% participates agree, 34.5% strongly agree, 10.1% uncertain, 4.2% disagree, 1.2% strongly disagree. Therefore, data shows that MMS are easy to use.

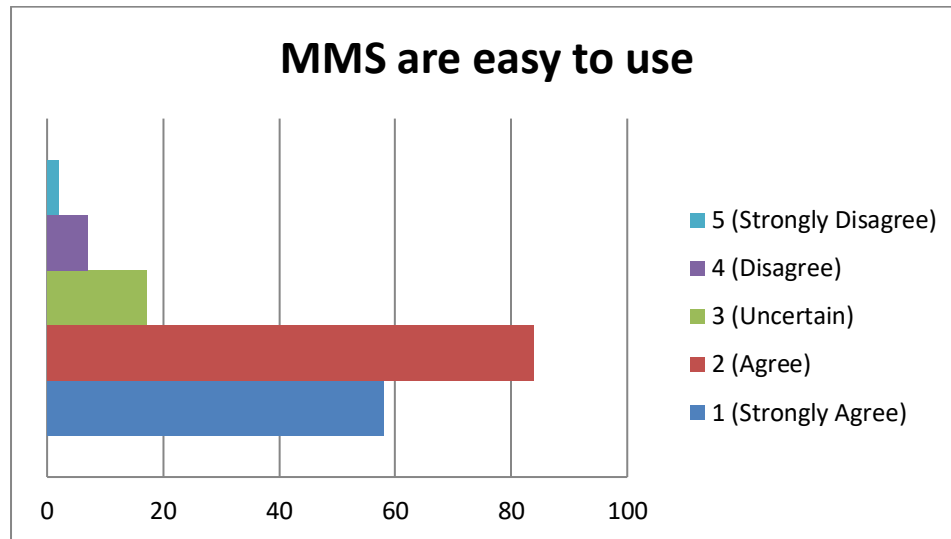


Figure 21 MMS are easy to use

4. 4. 6 MMS service center is easily accessible by phone

In figure 22 below respondents are asked to show their agreement level to show whether their M-money service center is easily accessible to answer their queries relating to the service, 46.4% agree, 32.7% strongly agree, 17.9% uncertain, 3% disagree, with no representation of strongly disagree. For that reason, this is proving that MMS service center is easily accessible to assist users.

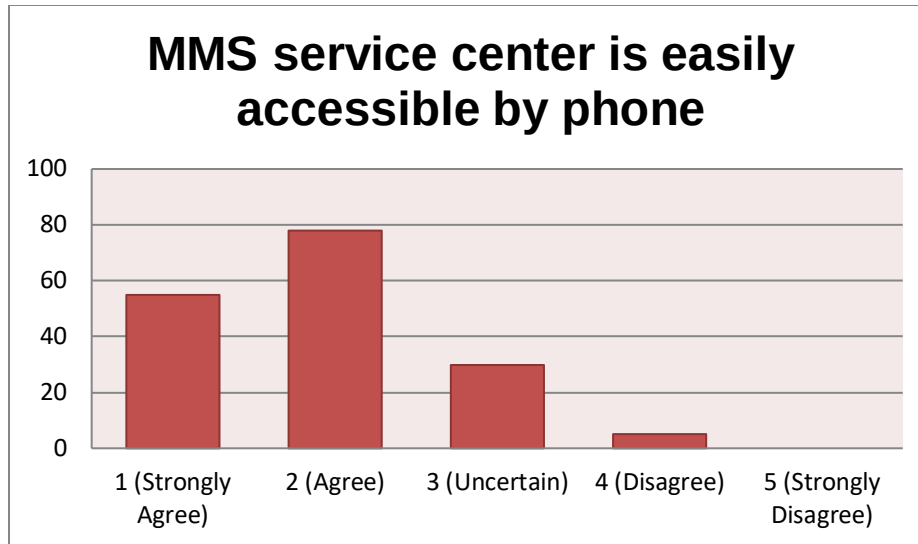


Figure 22 MMS service center is easily accessible by phone

4. 4. 7 The customer service representative was quick to solve my problem or answer my question

Figure 23 below respondents show that whenever they have challenges relating to the service, their problems are quickly addressed. This is demonstrated due to a higher number of participants who agree with this statement, 41.1% agree, 35.7% strongly agree, 16.7% uncertain, 3.6% strongly disagree and 3% disagree. This showed that service center representatives always attend to customers concerns.

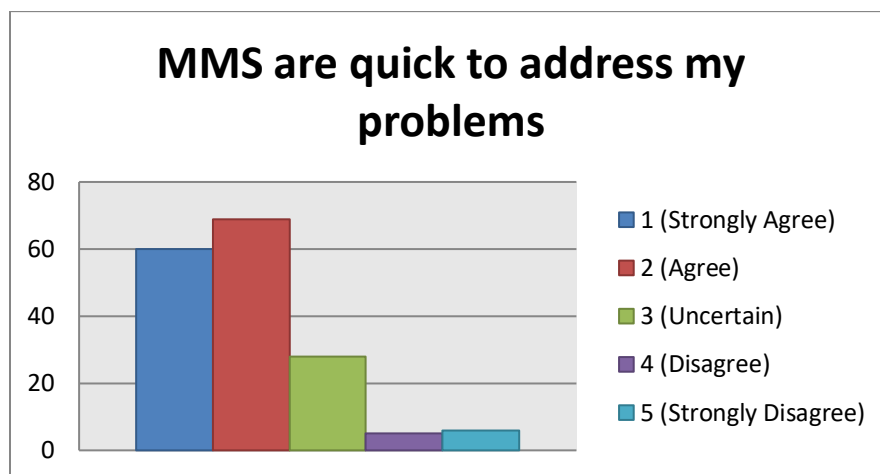


Figure 23 MMS are quick to address my problems

4. 4. 8 The service generally meets my expectations

Figure 24 below, participants indicated by showing their agreement level to the statement that whether the service meets that expectations, 47% agree, 33.9% uncertain, 12.5% strongly agree, 6.5% disagree. This is clear that this service meets expectations of most customers.

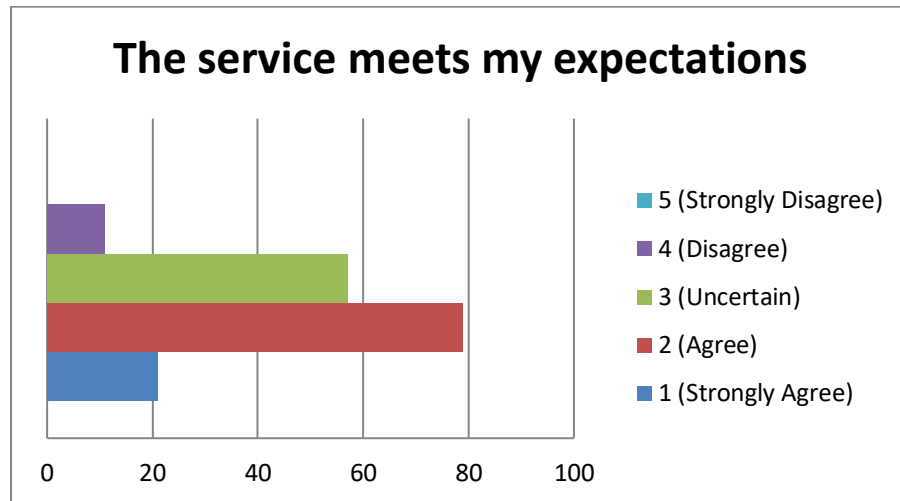


Figure 24 the service meets my expectations

4. 4. 9 I would recommend this service to someone I know

In figure 25 below respondents were asked to specify whether they would recommend the service to someone else, by specifying their agreement level, majority of respondents agree with 43.5%, 36.9% strongly agree, 16.1% uncertain, 3.6% disagree, with no representation of strongly disagree.



Figure 25 I will recommend this service to someone

4.4.10 Summary of M-money service rating

This section was asking respondents to rate their M-money service, 46.4% of respondents said MMS are reliable and convenient, while 56.5% of participants are uncertain that MMS are time efficient. 51.8% of respondents are uncertain that MMS are secure, while 46.4% strongly agree with the statement that MMS are affordable. MMS are easy to use, with 50% participants agree to this statement, M-money service center is easily accessible to answer their queries relating to the service 46.4% agree. 41.1% of participants agree that service center representatives always attend to customers concerns and overall 47% agree that the service meets their expectations; lastly, 43.5% agree they would recommend the service to someone else.

4.5 Challenges in M-money transfer services

One of the objectives of the research study was to investigate the challenges that users of this system are faced with, therefore the research will also find out through this section if there were solutions to these problems and how the problems were solved.

4.5.1 Have you ever had challenges while using this service (M-Pesa/EcoCash)

Figure 26 below finds out if respondents ever had challenges while using the system, 75% of respondents says yes, while 25% says no. This is evident enough that most users experience challenges while using the system.

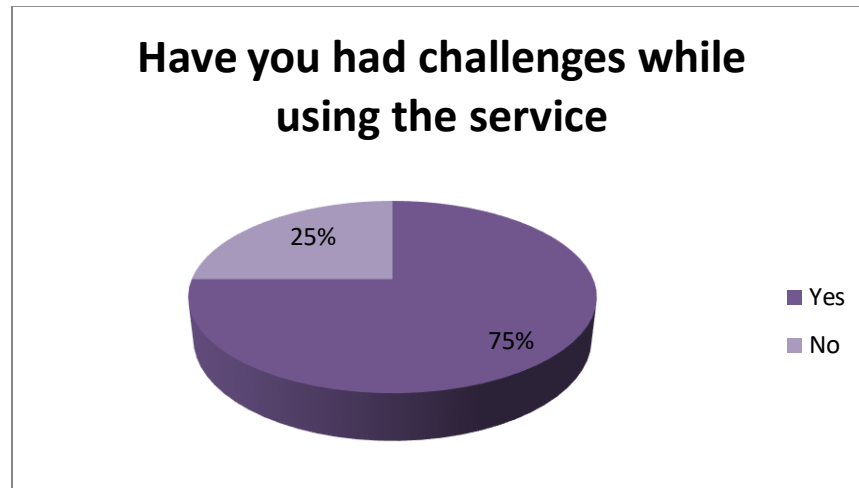


Figure 26 Have you ever had challenges while using the service

4.5.2 If you had challenges are they related to the following?

Figure 27 below demonstrates that amongst the challenges that users were faced with, most of these challenges were due to poor network with 38.9%, followed by challenge of inability of agents to provide money with 22.2%, 18.3% said it is due to unavailability of agents, 9.5% said sending money to wrong recipient and 4% of respondents said the system is too complicated. The data revealed that the most challenge facing users is due to poor network connection.

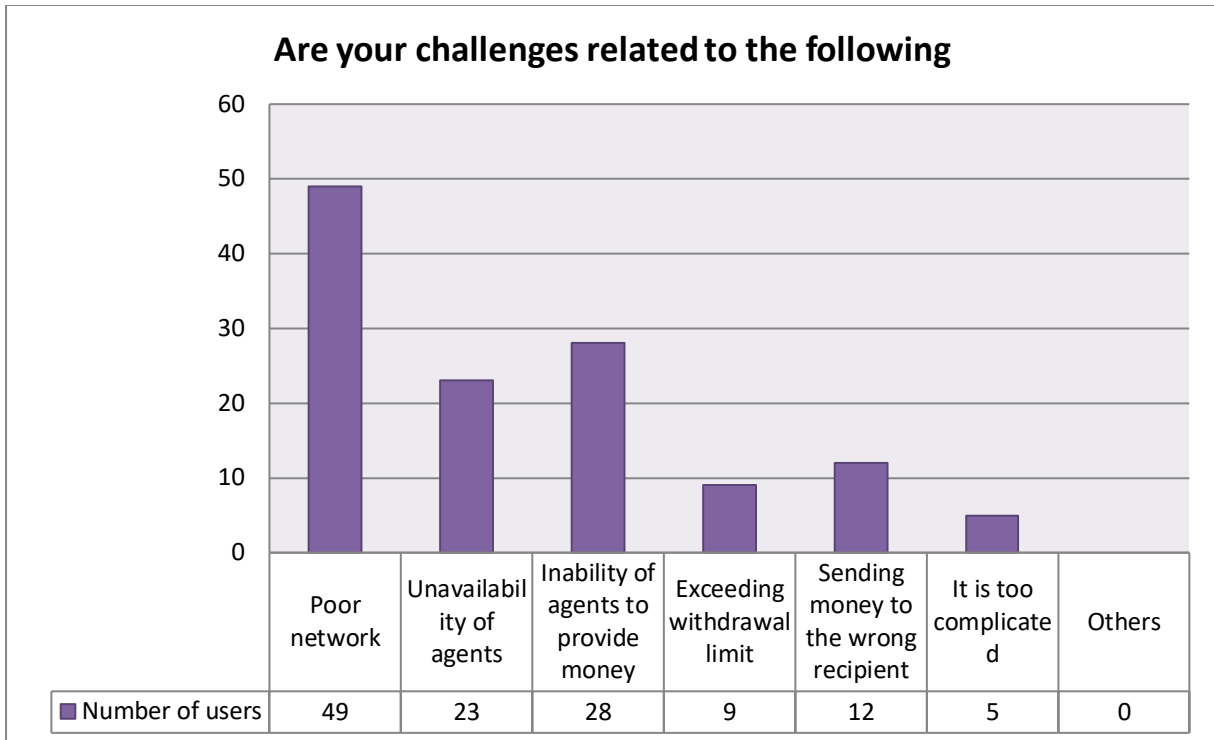


Figure 27 Are your challenges related to this mentioned

4.5.3 Was your problem solved?

Respondents were asked if the problems that they were faced with were solved, 88.9% of respondents say yes they were solved, while 11.1% say no they were not solved.

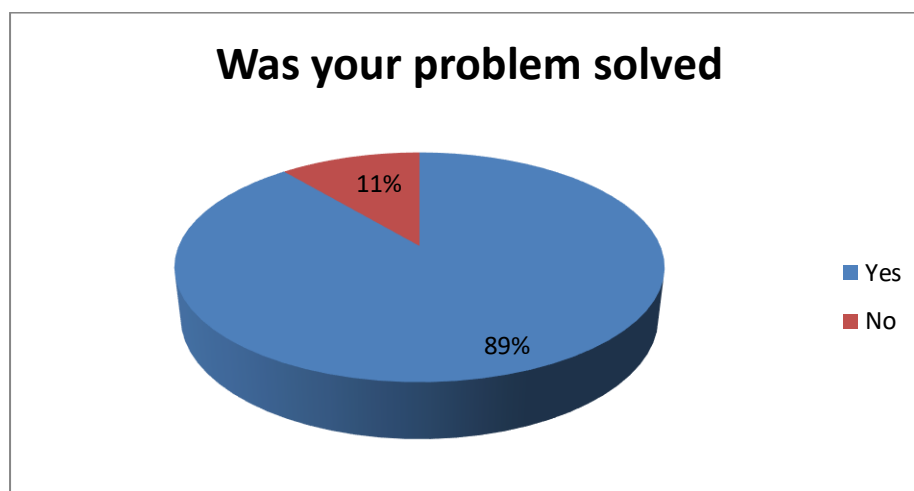


Figure 28 was your problem solved

4.5.4 Was your problem solved through any of the following?

The study further finds out how were the problems facing users were solved, 38.4% say the customer service representative was quick to assist them, while 28.6% had to visit the nearest branch, 27.7% say they looked for alternative agents, 5.4% moved to a location with better cell phone reception. This showed that MNO through their customer representatives are quick to respond to customer's problems.

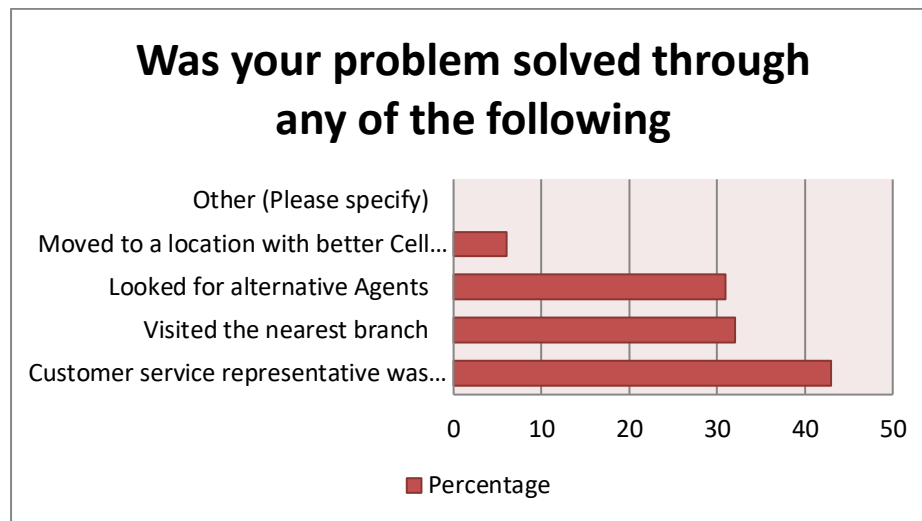


Figure 29 Was your problem solved through any of the following

4.6 Security of M-Money Transfer Services

This section asked respondents about the strength of security of the current authentication method used by MMS, in the following statements participants responded with a yes or no, to indicate their agreement or disagreement to the statement.

4.6.1 Have you ever shared your PIN with anyone?

As demonstrated in figure 30 below, respondents were asked to indicate whether they have shared their PIN with anyone, 60.1% of respondents said no, while 39.9% said yes. This indicated that majority of respondents are aware that not sharing their PIN secure their M-money account.

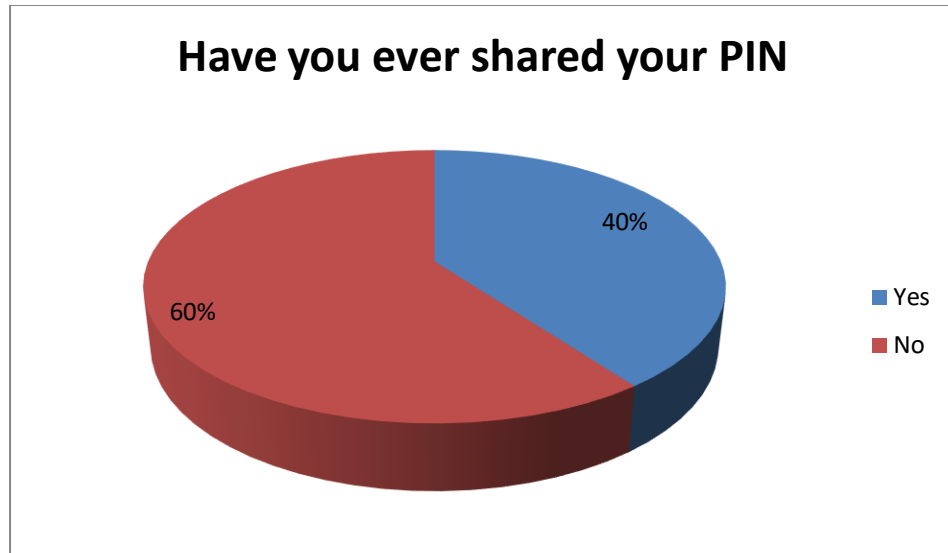


Figure 30 Have you ever shared your PIN

4.6.2 If yes, do you still think your account is still safe?

Respondents that said they have shared their PIN were further asked to specify if they think their account is still safe after sharing their it, in figure 31 below 58.2% of respondents said yes, while 41.8% said no. This maybe is due to respondents trusting the individuals that they have shared their PIN with.

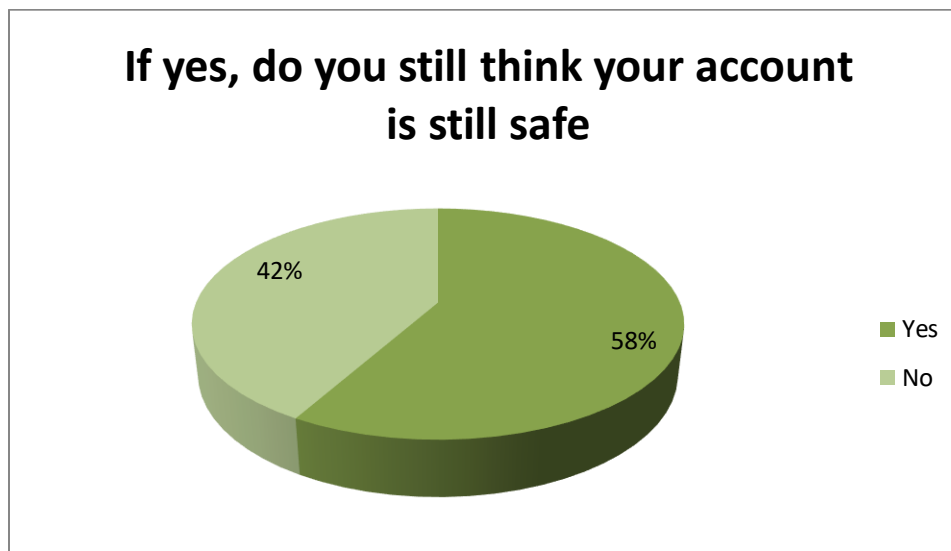


Figure 31 if yes, do you still think your account is still safe

4.6.3 Do you think your PIN can be easily guessable?

In figure 32 below respondents were asked to specify if they think their PIN can be easily guessed, since PIN is a four digit number, most users' tend to use their year of birth as PIN which can be easily guessed. 64.9% said no, while 35.1% said yes, this means most respondents do considers the fact that by using an easy guessable PIN they are putting their accounts at risk.

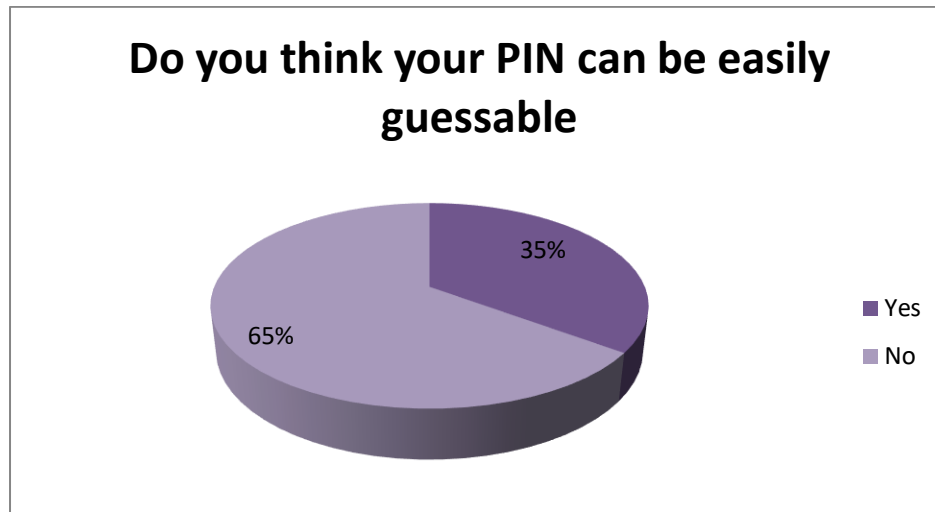


Figure 32 Do you think your PIN can be easily guessable

4.6.4 Do you think your PIN is provides enough security for your account?

In figure 33 below respondents indicates whether they consider PIN secure enough for their M-money accounts, 60.7% said no, while 39.3% said yes. A great number of respondents indicated that PIN alone does not provide enough security to their accounts, therefore, enhancement is necessary.

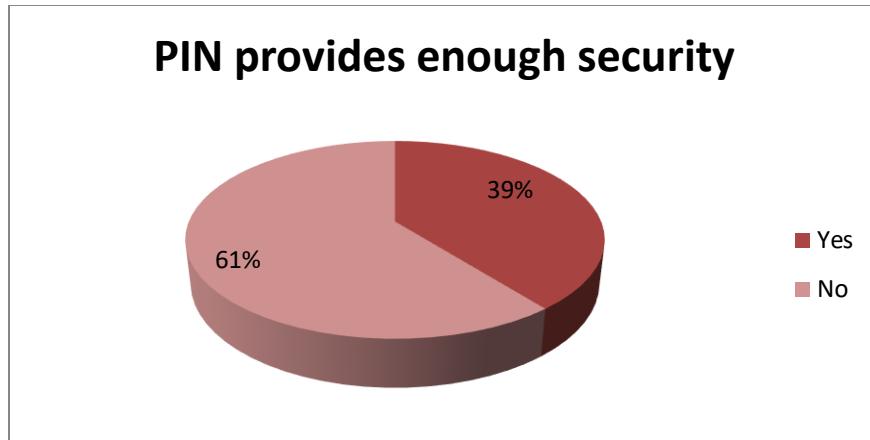


Figure 33 PIN provides enough security

4.6.5 Did you ever forget your PIN?

In figure 34 below respondents indicated whether they ever forget their M-money account PIN, 66.7% said no, while 33.3% said yes. This shows that the four digits PIN is not easily forgettable.

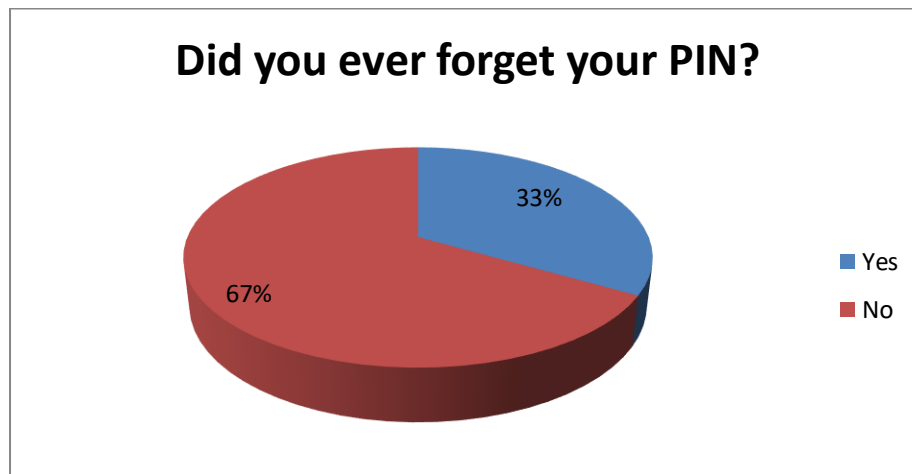


Figure 34 Did you ever forget your PIN

4.6.6 If you ever forget your PIN, would you still remember the answer to the security question you set while you were registering your PIN?

Respondents indicated in figure 35 below that if ever they forget their PIN they would not remember the security question they set while they were registering for their accounts, this is proven by 80.4% of respondents who say no and 19.6% who said yes.

This proves that majority of respondents do not remember their security question and this is no longer sufficient.

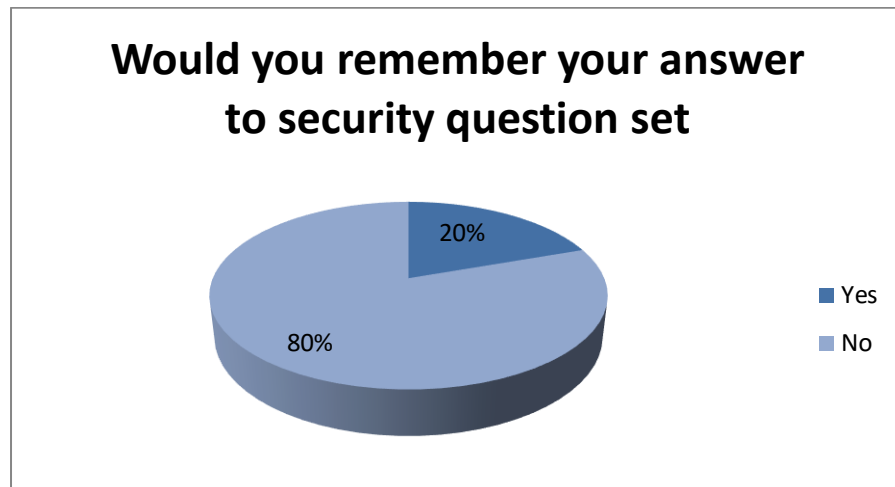


Figure 35 would you remember your answer to security question set

4.6.7 How often do you change your PIN?

In figure 36 below respondents indicated how often they change their M-money accounts PIN, 56% of respondents said they never changed their PIN, while 34.5% say very rarely and 9.5% say occasionally. With no representation of frequently or very frequently, this is evident that majority of respondents are not aware of the significant value of periodically changing their PIN.

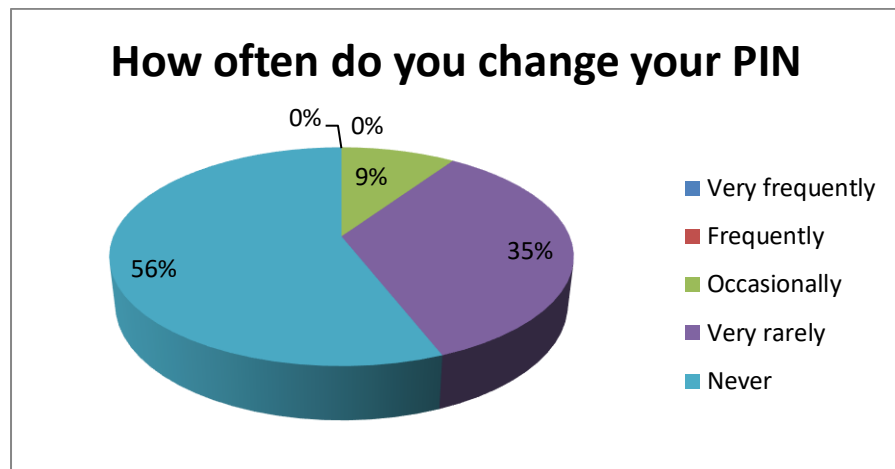


Figure 36 How often do you change your PIN

4.6.8 Have you ever been a victim of fraud in M-money services or someone you know?

In figure 37 below demonstrates that 83.9% of respondents have not been victim of frauds in M-money, while 16.1% say yes they have been victims. This shows that even though there are numbers of cases reported of fraudsters stealing from users, most respondents were not yet victims.



Figure 37 Have you ever been a victim of fraud

4.6.9 If yes, did it relate to any of the following frauds?

In figure 38 respondents are asked to specify the kind of fraud they have been a victim of, 44.4% of respondents said they received a fake SMS claiming received monies, 33.3% someone who knows their PIN performing a transaction without their knowledge, 14.8% said unauthorized SIM swap, 7.4% stolen/lost phone and transaction was performed, with no representation of other forms of frauds which were not specified.

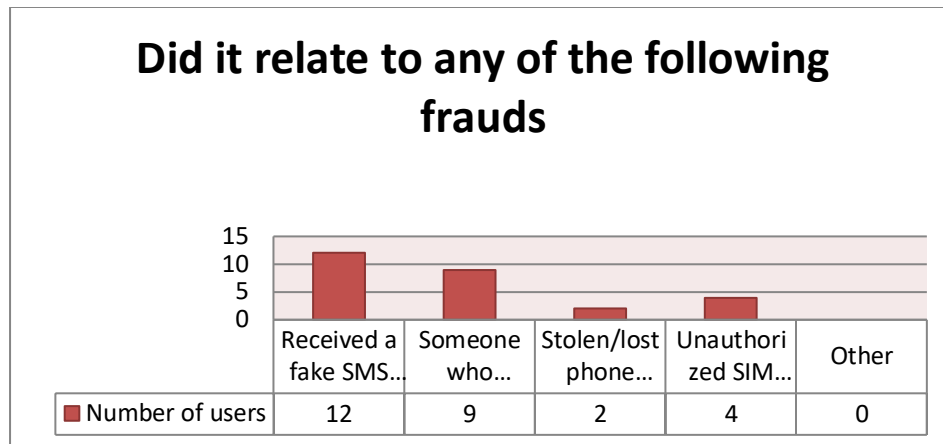


Figure 38 did it relate to any of the following frauds

4.6.10 Were any of the fraudulent activities above solved?

In figure 39 below indicates that 70.4% of the frauds that users had experienced were solved, while 29.6% were not solved. This showed that at list most fraudulent cases are being found solutions for.

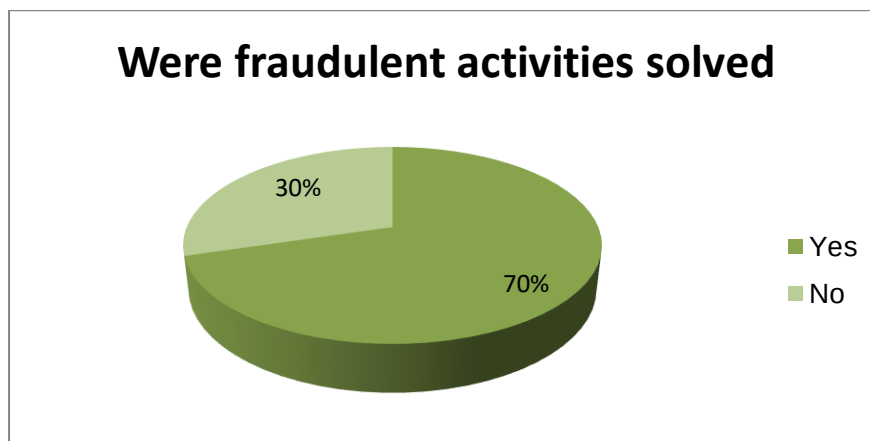


Figure 39 Were fraudulent activities solved

4.6.11 If yes, was it through any of the following?

In figure 40 below, respondents indicated how above fraudulent activities solved, 63.2% of respondents said Mobile Money Operator (Vodacom/Econet) intervened, while 36.8% said they reported the matter to the police, with no representation of other solutions from respondents. This shows that MNO are working tirelessly to maintain the reputation of their system.

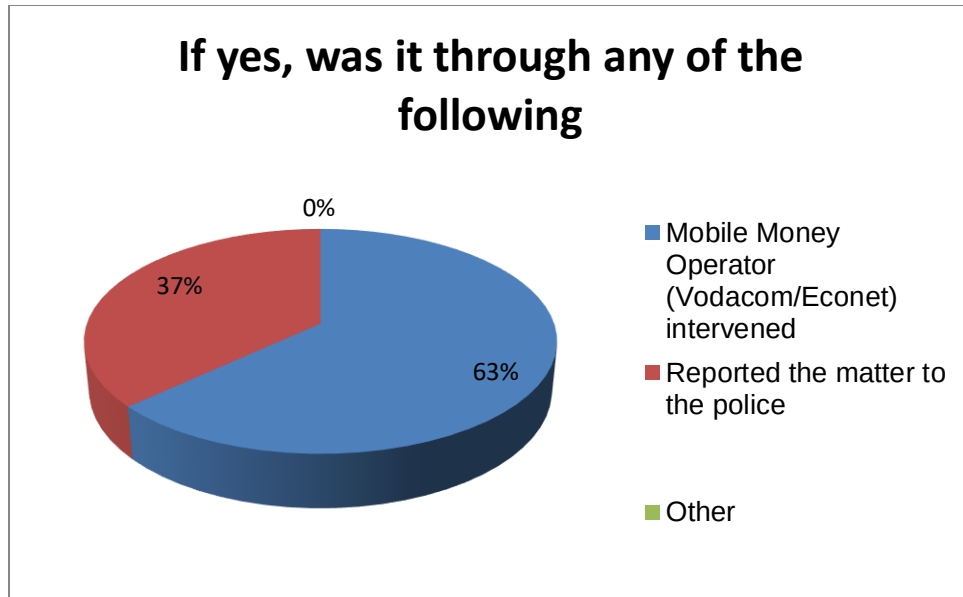


Figure 40 If yes, was it through any of the following

4.6.12 Is there a need for an additional method to improve the security of these systems?

As shown in figure 41 below, respondents indicated that there is a need for an additional method to enhance the security of M-money system, 63.7% said yes, while 36.3 said no, this is evident that there is a need for security enhancement and users are no longer feeling secure with the current authentication method.

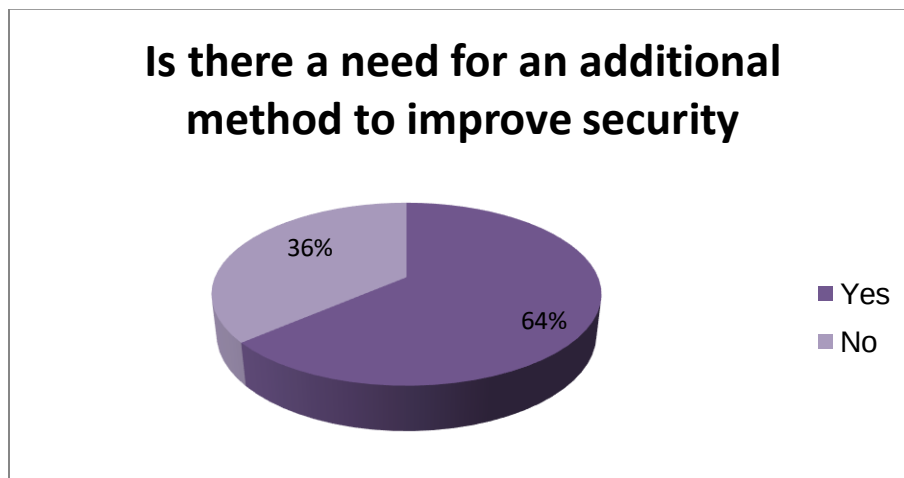


Figure 41 Is there a need for an additional method to improve security

4.6.13 Are you familiar with any of the following biometric authentication techniques?

Figure 42 below demonstrates the biometric factors that respondents are familiar with, most respondents are familiar with biometric fingerprint with 28.6%, followed by 27.4% face recognition, 21.4% voice, 15.5% said they are not familiar with any biometric factor and lastly 7.1% is familiar with hand geometry. Majority of respondents are familiar with fingerprint biometric and face recognition, therefore, it will be easier for them to use the proposed system.

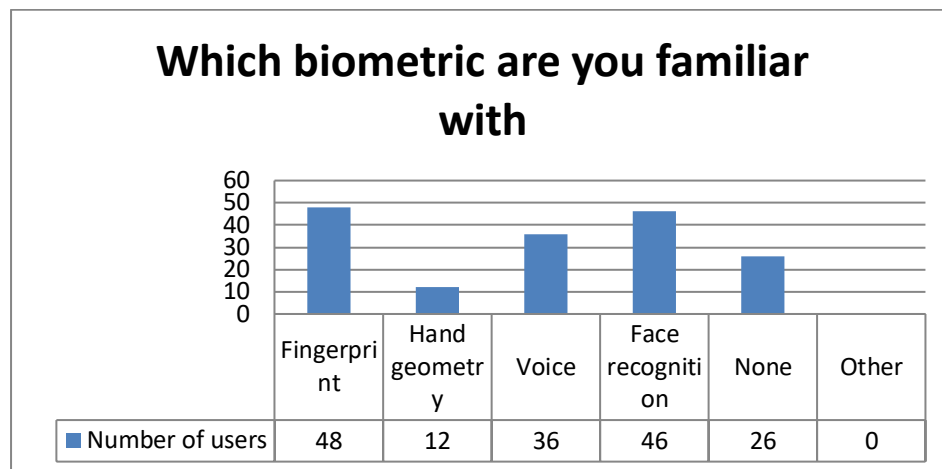


Figure 42 which biometric are you familiar with

4.7 M-money transfer service (M-Pesa/Ecocash) can adopt Biometric Face Recognition (BFR), Please rate this authentication process.

The main objective of the research study is to propose an additional authentication factor that will implement Biometric Face Recognition, in this section respondents are asked to rate this proposed model. Respondents used a likert scale to rate five items that range between 1 strongly agree to 5 strongly disagree, to show their level of agreement to the statements given.

4.7.1 It will improve the security of (M-Pesa/EcoCash)

As demonstrated in figure 43 below, respondents were asked to indicate their agreement level if the proposed model will enhance the security of M-Pesa/EcoCash, 48.8% strongly agree with the statement, 33.9% agree, 10.7% uncertain, 4.2% disagree, 2.4% strongly disagree. Majority of respondents demonstrated that this additional method will enhance the security of MMS.

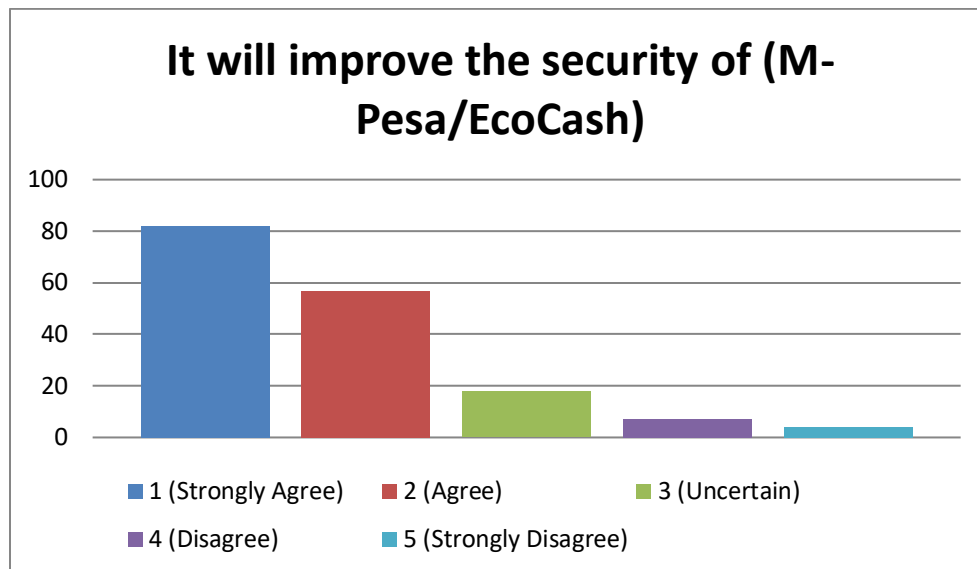


Figure 43 It will improve the security of (M-Pesa/EcoCash)

4.7.2 It will complicate the current process of doing transactions

Figure 44 below indicates respondents agreement level to the statement that the proposed method will complicate the current process of performing transactions, 34.5% of respondents agree, 28.6% disagree, 14.9% strongly agree, 11.3% uncertain, 10.7% strongly disagree. This indicated that majority of users do think the proposed method will complicated the way of doing transactions.

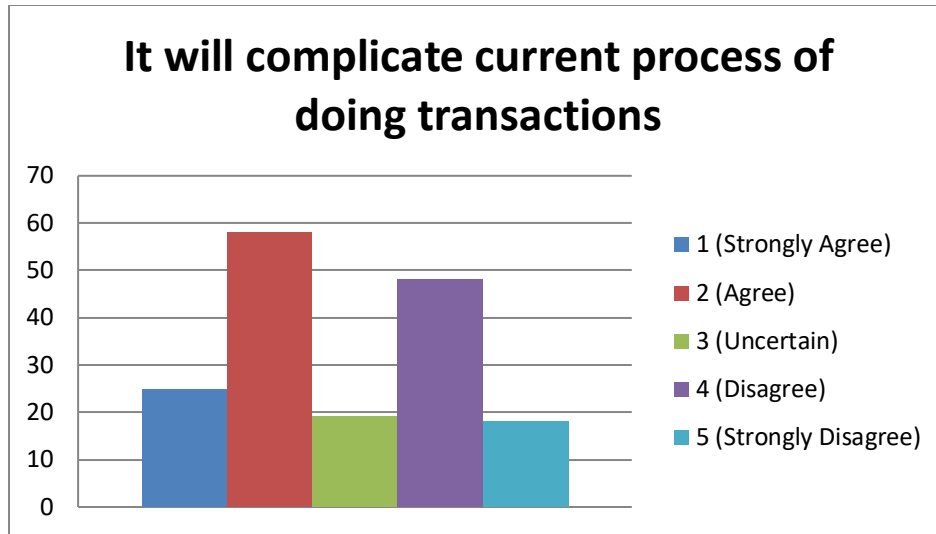


Figure 44 It will complicate the current process of doing transactions

4.7.3 It will be convenient for the user

As demonstrated in figure 45 below respondents indicated their agreement level to the statement that this additional method will be convenient to the user, 32.7% of respondents were uncertain, 29.2% agree, 24.4% strongly agree, 10.1% disagree, 3.6% strongly disagree. Majority of respondents were unsure that the proposed model will be convenient for the user.

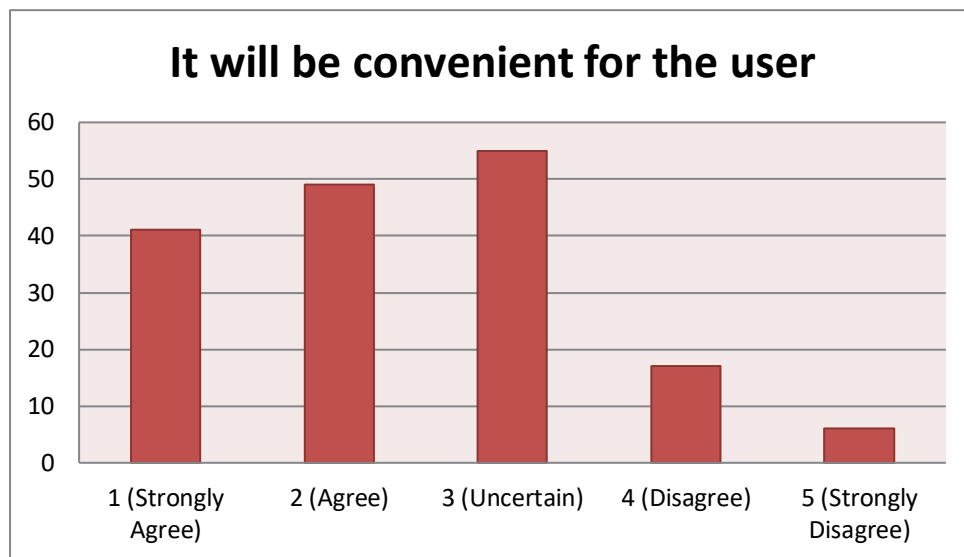


Figure 45 It will be convenient for the user

4.7.4 I will be comfortable to always take a picture with every (M-Pesa/EcoCash) transaction I make

Respondents were asked to indicate their agreement level to the statement that they will be comfortable to always take a picture with every transaction they make. In figure 46 below demonstrate that most respondents with 38.1% were uncertain, 31.5% agree, 20.8% strongly agree, 9.5% disagree, with no representation of strongly disagree. This showed that respondents were unsure whether they will be comfortable to take a picture every time they carry out the transaction.

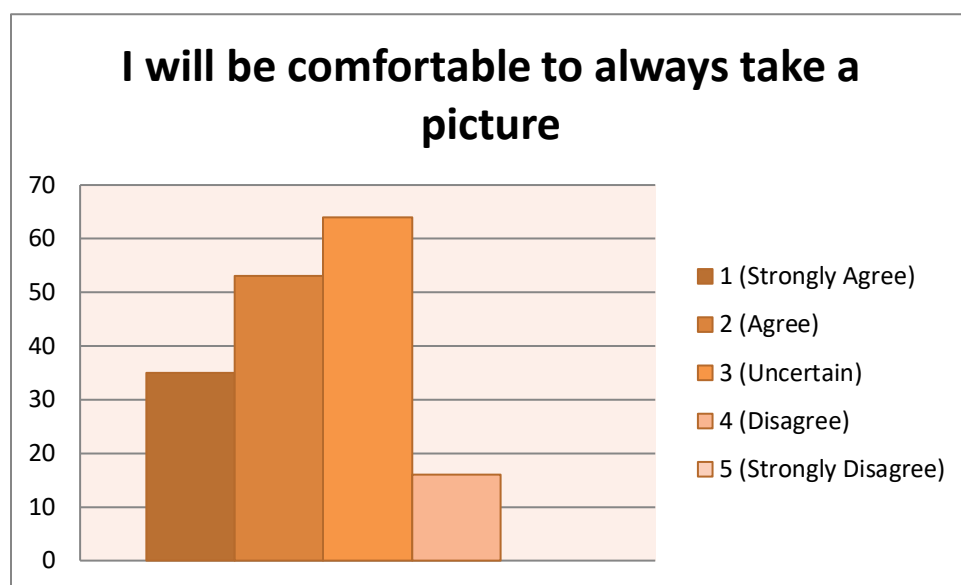


Figure 46 I will be comfortable to always take a picture

4.7.5 This feature will attract more people to use (M-Pesa/EcoCash)

In figure 47 below respondents indicated their agreement level to the statement that, this feature will attract more people to use M-Pesa/EcoCash, 32.7% were uncertain, 28.6% strongly agree, 25% agree, 7.1% disagree, and 6.5% strongly disagree. This is clear that most respondents are unsure that the feature will attract more users to use the system.

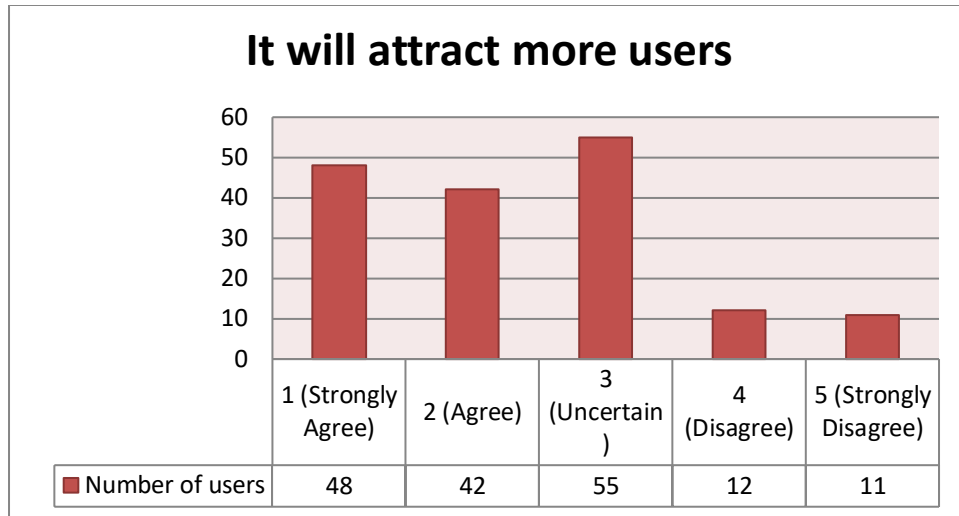


Figure 47 It will attract more users

4.7.6 What are the challenges that will prevent you from using the above system?

As shown in figure below, the study find out challenges that will prevent the respondent from using the proposed system, 48.8% of respondents said there is nothing that will prevent them, 21.4% said it is too complicated, 13.7% said they do not have a smart phone, 8.9% said they are concerned about their privacy, 7.1% said it is not secure. This showed that if the proposed system is put into practice, more users will want to use it, this is due to a higher number of respondents who indicated that there are no challenges that will prevent them from using the system.

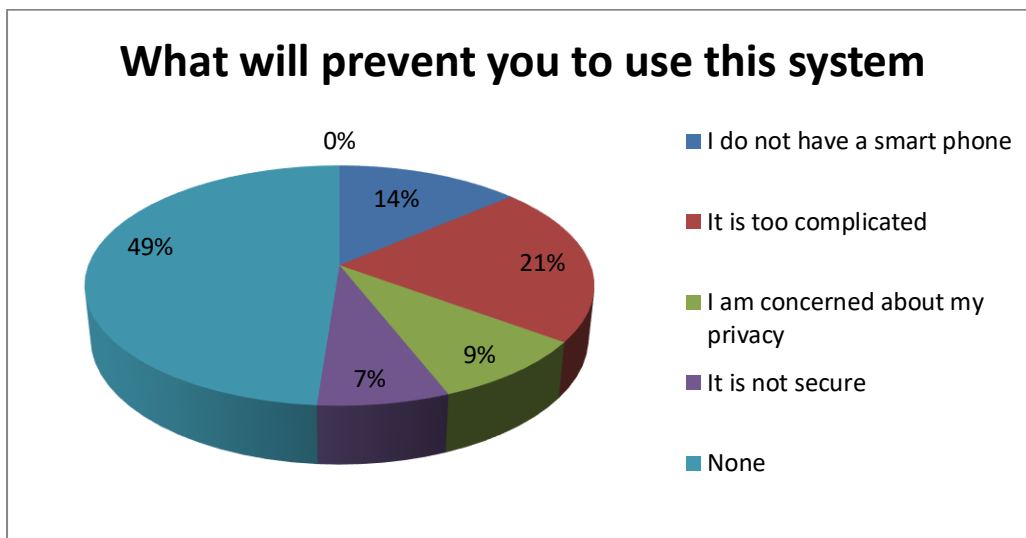


Figure 48 what will prevent you to use this system

4.8 Chapter Summary

The chapter presented findings from 168 respondents, and investigated the significance of introducing Multifactor authentication technique as a way of enhancing the security of Mobile Money Transfer Services in Lesotho. The study revealed that a great number of participants were males, with 57% response rate, and most of them range within age 25-33 with 39.9%. Data also demonstrates that 55% of participants were residing in the lowlands with 57% using only M-Pesa as their M-money service, a great number of them having used this service within a range of 3-4 years with 52%, and 51% use 2G phones.

The findings were done in line with the key objectives of the study, the study was examining the challenges participants were faced with while using the service, 75% of respondents agreed that they had challenges, 38.9% of them said the most challenge they were facing was due to poor network, a great number of respondents which constitute 88.9% indicated that yes their problems were solved and 38.4% of them said the customer service representative was quick to assist them with the challenges they meet.

Respondents were also asked to specify whether they have shared their PIN with anyone, 60.1% of respondents said no they had never shared their PIN. Respondents that said they have shared their PIN were further asked to specify if they think their account is still safe after sharing their it 58.2% of respondents said yes, this can be the level of trust between them and the people they shared their PIN with. 64.9% said no they do not think their PIN can be easily guessed. A great number of respondents 60.7% indicated that PIN alone does not provide enough security to their accounts. Greater part of respondents said they never forget their M-money account PIN, but if ever they forget their PIN they would not remember the security question they set while they were registering for their accounts, this is proven by 80.4% of respondents. Respondents further indicated how often they change their M-money accounts PIN, 56% of respondents said they never changed their PIN. This further put their accounts at risk.

Majority of respondents demonstrated that they have never been victim of frauds in M-money. But the major fraud experienced was when respondents received a fake SMS claiming received monies, and requesting users to reverse the money. 70.4% of the frauds that users had experienced were solved, 63.2% of respondents said Mobile Money Operator (Vodacom/Econet) intervened. Best part of respondents indicated that there is a need for an additional method to enhance the security of M-money system, and agreed that proposed model will enhance the security of M-Pesa/EcoCash. Respondents used the likert scale to rank the security of the proposed model and 48.8% of respondents said there is nothing that will prevent them from using the proposed system.

CHAPTER 5: DISCUSSION, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

The current chapter will discuss the major findings for this research study based on the research questions and data gathered from the participants. The study will further offer some recommendations based on the literature gathered as well as the gap seen during the analysis of data in the previous chapter. The summary of future research will also be outlined, stating clearly the direction in which other researchers should take in the future. The study will also provide reasons why MNO in Lesotho should implement the proposed method, stating how it will benefit its subscribers. The chapter will also allow the study objectives to be aligned with the research findings, looking at the variation and relationship between the literature as well as the discussions based on the data gathered from respondents.

5.2 Discussion

The main objective of this research study is to enhance the security of Mobile Money Transfer Services in Lesotho, and solve its security vulnerability introduced by the method of authentication they are using. The study proposes a conceptual framework that will assist the technical teams of both companies put in practice an authentication technique to mitigate these issues through Multi-factor authentication using Biometric Face Recognition technique. BFR will eliminate the chances of a fraudster providing false information to the system, therefore increasing the security of the system. The proposed model will verify users through their eight mixed character PIN that will be masked when entered as well as by comparing them with their digital image stored in the server during the enrolment phase.

Therefore, the use of biometric will enhance its security, reducing the challenges that are introduced by MNO employees working with fraudsters to do unauthorised SIM swaps, targeting accounts with more money. Reliability of M-money account will attract

more customers to want to be part of it, and that means the growth in amount of money to be transacted. Using Biometric face recognition will provide with a higher level of identification because the user will need to be physically available than that one of traditional authentication method where any one can enter the PIN and as long as the PIN is correct, the user is authenticated.

Biometric face recognition will provide high level of security to M-money accounts as it will solve the security issues in traditional method that enable the sharing and transfer of PIN or passwords between people. With this technique the verification factor is unique feature to every other user, and unlike a four-digit PIN that is currently being used that can be forgotten or that can be guessed because users do not want to set complicated numbers that are not easy to remember, this biometric factor is a feature that is always there with the user and it cannot be stolen or forged. Since this feature allows real-time identification of users, it will definitely solve put a stop to unauthorised access to accounts and stop the common fraudulent activities outside and inside the MNOs. The system will have features that will detect difference between a live captured picture and printed or recorded picture.

The research study revealed that majority of respondent are mostly familiar with biometric fingerprint technique, followed by biometric face recognition, this assisted the researcher to realise which biometric is widely used and which one the user would be comfortable to use. It was also observed in the literature that there was a need for enhancing the security of M-money systems. Therefore, the majority of respondents indicated that there was a need to improve the security of M-Pesa/EcoCash, although a great number of them felt that this model will complicate the current process of carry out transaction. Most of them were uncertain whether the proposed model will be convenient to the user and whether they will feel at ease to always take a picture with every transaction they make. In general, there seemed to be no reason that will prevent majority of them to use the proposed model.

Most companies are enjoying the benefit that is given by implementing the biometric

systems, because of the security they provide. But the greatest challenge of implementing and maintaining this system comes with increased costs. Another challenge with biometric face recognition is that a user only has one biometric face that can be used by different system, if it is compromised an attacker can use it to gain access in other systems and it cannot be changed or replaced easily. Because different lenses do not have the same power, if a different lenses of cameras are used, they could have a high effect on the picture captured, therefore, user might be denied access. Another major setback seen with the use of biometric face is that as the person gets older, their face features do change, so this affects the performance of the system. However the benefits of implementing this system prevail over its costs and shortcomings.

The specific objective identifies the threats that are introduced by method of authentication that is currently used by both EcoCash and M-Pesa, and how it affects the security of their system. Both M-Pesa/EcoCash uses only PIN to allow users to access their M-money accounts, this single factor technique is proven to be less secure method of authentication. Because PIN is just a four digits number that is not even masked when entered it introduces threats to the system as people nearby may see what numbers are entered. Yet again the system allows the user to use one PIN for as long as they want, it does not expire. Majority of respondents 60.7% said PIN does not provide enough security for their M-money accounts, this was also proven by the literature review. Although majority of the respondents indicated that they never forget their PIN, but majority of them 80.4% of them indicated that they would no longer remember the answer to the security question set while they were registering.

Users are constantly reminded not to share their PIN with anyone, in most cases people are lazy to live the comfort of their home to go to the nearest agent to withdraw money, and they usually send their family members or friends, and then share their PIN with them. Then in a later stage, that person can access the account and perform any transaction without the user's permission. Entering the correct PIN does not fully guarantee that the person using the account is really the owner. The study further

revealed that a great number of users never changed their PIN, this introduces more threats to the system.

The other specific objective of this research is to investigate and evaluate the security issues of the M-Pesa/EcoCash in Lesotho, and provide a more effective solution that will make the system more reliable and secure. The study points out that majority of respondents are being fraud, they usually receive a fake SMS claiming to have received monies. The fraudsters are reported to be working with MNO's employees to get information about users, targeting users with more money into their accounts. The SMS details are usually correct showing the false new balance of the user. After the SMS, the fraudster calls the user to re-send the money back to them because they mistakenly send it to them. This fraud is highly common and even though MNOs are making numerous attempts to notify users about them, fraudsters are still using this technique.

5.3 Conclusions

Through the literature review and research findings, the current authentication method deployed by both M-Pesa and EcoCash is proven not to be sufficient enough for securing user's M-money accounts. There were major security issues that were observed with a four digit PIN, it is not masked when entered therefore, people nearby might see what is entered. It can be easily guessed as most people use their year of birth as their PIN, the sharing of PIN amongst friends and family members is seen to have been a problem as one of the specific fraud is performed by someone the user has shared their PIN with before, then performing transaction without their knowledge. By implementing Biometric Face Recognition with eight characters PIN that is masked when entered, different threats in M-money can be eliminated.

Most respondents have not been victim of frauds in M-money, but the common fraud is users receiving fake SMS claiming to have received money, another fraud is of someone who user have shared their PIN with performing transaction without permission. The other reported frauds that are not commonly performed but do exist are

unauthorized SIM swap and stolen phone with transaction performed. The study revealed through the finding that even though frauds do exist in M-money Lesotho, most respondents were not yet victims of. Users should feel comfortable and secure while using any system, especially if it involves money, therefore, MNOs should go extra mile to ensure the security of their systems. Deploying Multi-Factor Authentication system (MFA) will protect user's valuable information.

The study revealed that there is a need for security enhancement in M-money, most respondents demonstrated that even though they are not sure about the convenience of the proposed system, but they agree that the proposed model will improve the security of their M-money accounts. Eight characters (combination of uppercase and small letters, numbers and symbols) PIN that will be masked when entered, will solve the issues in four digits PIN currently used. Supplemented with Biometric Face Recognition will prevent any unauthorised entry into the system. The study further indicated that majority of respondents no longer remember their answer to the security question set during enrolment, therefore, the proposed model will save the MNOs money by reducing a need to hire service center representatives that assist users to reset their PIN whenever they forget them.

5.4 Recommendations

Mobile Network Operators should implement policies that will minimise and prevent their employees from engaging in fraudulent activities. They should also engage in nationwide campaigns that will make aware their customers of the different techniques fraudsters use, and how they should safeguard their M-money accounts. They can also implement a model that will detect and prevent fraud, and by introducing Biometric Face Recognition method, they can trace and store biometrics of the suspects in the system, and the system will detect and report whenever they try to execute their frauds. To secure biometric data stored in a server, cryptographic techniques should be integrated, by storing a template which is the transformed version of actual biometric data provided during the registration stage.

During the registration process in the current system, the user is required to enter their details (Names, Passport number) and answer a secret question. There is no form of verification done after the user registers to check if those names are valid. That means one person can have multiple accounts with false names and false passport number or even use other people's names. The M-money system could be linked to the national identity system in order to verify the details of the user entered during enrolment phase. That means the system will deny any false information or stolen identity, because the details would have to match with the ones stored in the national identity system against the one the user will be entering.

The study indicated that respondents are faced with challenges while using the system, with the major challenge being poor network. MNO should put into place resources that will improve their network performance. The study also revealed that there is a low usage of M-money in the highlands, and respondents indicated to have a challenge of unavailability of agents as well as inability of agents to provide the required money. MNO should check the ability of agents to sustain their liquidity before they could allow them to provide this service to its clients. MNOs should also consider how they can increase the number of agents in the highlands. Exceeding withdrawal limit is another challenge facing users, most of them are not aware of the different levels that are available while registering for M-money, the level that the user registers for, determine how much money can withdraw per day and per month. MNOs should make aware their customers of this levels and why they exist.

The current M-money system requires the user to enter PIN at the end of the transaction and if the user had made the wrong choice of the service it does not have the back or home option the user has to cancel and start afresh, and this is inconvenient to the user and it consumes time. They should modify the system to request the PIN when the user wants to view the M-money services, and then include a back option or home option.

5.5 Further Research

To increase the accuracy of biometric face recognition system and adapt to the changes of human face, some kind of machine learning has to be implemented. Researchers should do further research on how to enhance the security in face recognition system, through its algorithms and machine learning.

A research study should be conducted focusing on different frauds techniques that are used to steal subscriber's money and models that Mobile Network Operators in Lesotho can use to detect and minimise fraud in M-money.

REFERENCES

1. Aloul, F., Zahidi, S. and El-Hajj, W., 2009, Two Factor Authentication Using Mobile Phones
2. Amwoyo, K., 2014, Multi-Factor Authentication and Secure Integration of Mobile Payments
3. Andrews, A.M., Jefferis, K., Murgatroyd, P. and Webb, D., 2013, Lesotho: Financial Sector Development Strategy, accessed on 27/03/2019, from https://www.centralbank.org.ls/images/Financial_Stability/Financial_Inclusion/Lesotho%20FSDS%20%20-%20Nov%202013.pdf
4. Bansal, K. A. and Chawla, P., 2013, Face Recognition Techniques: A Review, International Journal of Engineering Research and Applications
5. Chong, K. M., 2006, Security of Mobile Banking: Secure SMS Banking
6. Copeland, 2017, The Pros and Cons of Open and Closed Questions, accessed on 02/04/2019, from <https://www.interpnet.com/NAI/docs/CIT/Copeland-Questions.pdf>
7. Coppolino, L., D'Antonio, S., Formicola, V., Massei, C., Romano, L., 2015a. Use of the Dempster-Shafer Theory for Fraud Detection: The Mobile Money Transfer Case Study, in: Intelligent Distributed Computing VIII. Springer, pp. 465–474.
8. Chetalam, J. L., 2018, ENHANCING SECURITY OF MPESA TRANSACTIONS BY USE OF VOICE BIOMETRICS
9. Debois, S. 2019, 10 Advantages and Disadvantages of Questionnaires, accessed on 02/04/2019, from <https://surveyanyplace.com/questionnaire-pros-and-cons/>
10. Delac, K. and Grgic, M., 2004, A SURVEY OF BIOMETRIC RECOGNITION METHODS, 46th International Symposium Electronics in Marine.
11. Desai, S., 2011, MITIGATING SECURITY RISKS IN USSD-BASED MOBILE PAYMENT APPLICATIONS
12. Econet Telecom Lesotho, 2019a, ECOCASH SPACHE-FONO - HOW TO REGISTER, accessed on 27/03/2019, from

https://www.etl.co.ls/index.php?option=com_content&view=article&id=62:ecocas-h-spache-fono-register&catid=25:services&Itemid=198

13. Elizabeth, 2013, Ten advantages of implementing a survey questionnaire, accessed on 02/04/2019, from
<https://novisurvey.net/blog/ten-advantages-of-implementing-a-survey-questionnaire.aspx>
14. Etikan, I., Musa, A. S., Alkassim, S. R., 2016, Comparison of Convenience Sampling and Purposive Sampling, American Journal of Theoretical and Applied Statistics, 5 (1)
15. Gine, X., Goldberg, J., Sankaranarayanan, S., Sheerin, P. and Yang, D., 2012, Use of biometric technology in developing countries
16. Gombiro, C., Jantjies, M. and Mavetera, N., 2015, A CONCEPTUAL FRAMEWORK FOR DETECTING FINANCIAL CRIME IN MOBILE MONEY TRANSACTIONS, Journal of Governance and Regulation, 4 (4)
17. GSMA, 2018, The Mobile Economy 2018, retrieved on 04/03/2019
<https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf>
18. GSMA, 2017, The Mobile Economy Sub-Saharan Africa 2017, accessed on 26/02/2019, from
<https://www.gsmaintelligence.com/research/?file=7bf3592e6d750144e58d9dcfac6adfab&download>
19. GSMA, 2016, Safeguarding Mobile Money: How providers and regulators can ensure that customer funds are protected, Accessed on 04/03/2019, from
https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/01/2016_GSMA_Safeguarding-Mobile-Money_How-providers-and-regulators-can-ensure-that-customer-funds-are-protected.pdf
20. Gutierrez, E. and Choi, T., 2014, Mobile Money Services Development: The Cases of the Republic of Korea and Uganda, accessed on 19/03/2019, from
https://www.researchgate.net/publication/263809182_Mobile_Money_Services_Development_The_Cases_of_the_Republic_of_Korea_and_Uganda

21. Handson, B. Z. O., 2016, Mobile – Based Multi-Factor Authentication Scheme for Mobile Banking
22. International Monetary Fund, 2018, Kingdom of Lesotho: Selected Issues; IMF Country Report No. 18/59, accessed on 02/04/2018, from <https://www.tralac.org/images/docs/12810/lesotho-selected-issues-paper-imf-country-report-no-18-59-february-2018.pdf>
23. Jefferis, K. & Manje, L., 2014, MAP-Lesotho Demand, Supply, Policy and Regulation Diagnostic Report, accessed on 29/03/2019, from http://finmark.org.za/wp-content/uploads/2018/09/MAP-Lesotho_Diagnostic-report_final_2014_rev.pdf
24. Kanal, A. and Raman, A., 2016, DATA ANALYSIS and BUSINESS MODELLING in Microsoft Excel using Analysis ToolPak, International Journal of Computer Science and Information Technologies, 7 (5)
25. Kothari, R. C., 2004, Research Methodology Methods and Techniques
26. Kumar, N. N. and Badyal, S., 2014, A Comprehensive Study of Drawbacks of Existing Face Recognition Techniques and Suggesting Improved Methods of Face Recognition, International Journal of Enhanced Research in Science Technology & Engineering, 3 (4)
27. Kumar, R., 2011, Research methodology; a step-by-step guide for beginners, 3rd ed
28. Lesotho Communications Authority (LCA), 2017, THE STATE OF ICT IN LESOTHO (2016), Commissioned by the Lesotho Communications Authority and The International Telecommunication Union
29. Mali, K. and Bhattacharya, S., 2013, Comparative Study of Different Biometric Features, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013
30. Michael, P. B., 2011, Nonprobability Sampling, Encyclopedia of Survey Research Methods
31. Mohamed, A., 2014, CHAPTER 3-METHODOLOGY-TECHNOLOGY TRANSFER-THESIS, accessed on 04/04/2019, from <https://www.researchgate.net/publication/261473688>

32. Mtaho, B. A., 2015, Improving Mobile Money Security with Two-Factor Authentication, International Journal of Computer Applications, 109 (7)
33. Mtaho, A. B. and Mselle, L., 2014, Securing Mobile Money Services in Tanzania: International journal of Computer Science & Network Solutions, A Case of Vodacom M-Pesa, 2 (5)
34. mns-consulting, 2017, Mobile Money: an Africa success story, accessed on 26/02/2019, from <http://mns-consulting.com/wp-content/uploads/2017/10/MNS-Mobile-Money-whitepaper.pdf>
35. Najih, A., Al-Haddad, S. A. R., Ramli, R. A., Hashim, S. J. and Nematollahi, A. M., 2016, An Overview of Multimodal Biometric Approaches Based on Digital Image Watermarking, Research Journal of Applied Sciences, Engineering and Technology, 13 (6)
36. Najih, A., Al-Haddad, S. A. R., Ramli, R. A., Hashim, S. J. and Khmag, A., 2017, Face Selection for Digital Image Watermarking, International Journal of Applied Engineering Research, 12 (5)
37. Naeem, M., Qureshi, I. and Azam, F., 2015, Face recognition techniques and approaches: a survey, Sci.Int.(Lahore), 27(1)
38. Nyamtiga, W. B., Sam, A. and Laizer, S. L., 2013, Security Perspectives for USSD Versus SMS In Conducting Mobile Transactions: A Case Study of Tanzania, INTERNATIONAL JOURNAL OF TECHNOLOGY ENHANCEMENTS AND EMERGING ENGINEERING RESEARCH, 1 (3)
39. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y., 2018, Multi-Factor Authentication: A Survey.
40. Prabhakar, S. and Pankanti, 2003, Biometric Recognition: Security and Privacy Concerns, IEEE Security and Privacy Magazine
41. Rahman, S., 2016, The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language "Testing and Assessment" Research: A Literature Review, accessed on 02/04/2019, from: https://www.researchgate.net/publication/309889936_The_Advantages_and_Dis

advantages_of_Using_Qualitative_and_Quantitative_Approaches_and_Methods_in_Language_Testing_and_Assessment_Research_A_Literature_Review

42. Realini, C., 2011. Securing Mobile Money to Deliver on the Promise. Lydian J.
43. Saini, R. and Rana, N., 2014, COMPARISON OF VARIOUS BIOMETRIC METHODS, International Journal of Advances in Science and Technology, 2 (1)
44. Sekantsi, P. L., and Motelle, I. S., 2016, THE FINANCIAL INCLUSION CONUNDRUM IN LESOTHO: IS MOBILE MONEY THE MISSING PIECE IN THE PUZZLE? Central Bank of Lesotho, Working Paper No.02/16, accessed on 26/03/2019, from https://www.centralbank.org.ls/images/Publications/Research/Papers/Working/THE_FINANCIAL_INCLUSION_CONUNDRUM_IN_LESOTHO.pdf
45. Showkat, N., 2017, Non-Probability and Probability Sampling, accessed on 04/04/2019, from https://www.researchgate.net/publication/319066480_Non-Probability_and_Probability_Sampling
46. Tiwari, A., Sanyal, S., Abraham, A., Knagskog, J. S. and Sanyal, S., 2007, A MULTI-FACTOR SECURITY PROTOCOL FOR WIRELESS PAYMENT-SECURE WEB AUTHENTICATION USING MOBILE DEVICES
47. Tripathi, K. P., 2011, A Comparative Study of Biometric Technologies with Reference to Human Interface, International Journal of Computer Applications
48. Victor, D., 2014, Evolution of Mobile Money Technologies in Developing Countries on the User-centric Evolution of Mobile Money Technologies in Developing Nations: Successes and Lessons. Accessed on 19/03/19, from: https://www.researchgate.net/publication/271854366_Evolution_of_Mobile_Money_Technologies_in_Developing_Countries_On_the_User-centric_Evolution_of_Mobile_Money_Technologies_in_Developing_Nations_Successes_and_Lessons
49. Vodacom Lesotho, 2019a, Guide to Vodacom M-Pesa, Registering for M-Pesa, accessed on 27/03/2019, from <https://www.vodacom.co.ls/ls-personal/m-pesa/guide-to-vodacom-m-pesa/getting-started-with-m-pesa/registering>

APPENDICES

Appendix 1: Questionnaire



Consent for Participation in Questionnaire

I.....volunteer to participate in a research project conducted by.....from Botho University Botswana . I understand that this questionnaire has been designed to investigate the current security measures on Mobile Money Systems (MMS) in Lesotho (M-Pesa/EcoCash), mainly the usage of Personal Identification Number (PIN) as the only method to allow users to access their mobile money accounts.

1. I understand that even if I agree to participate now, I can withdraw at any time or refuse to answer any question without any consequences of any kind.
2. I understand that I will not benefit directly from participating in this research and I will not be paid for my participation.
3. I understand that all information I provide for this study will be treated confidentially and I will spend approximately 15 minutes to complete the questionnaire.
4. I understand that in any report on the results of this research my identity will remain anonymous.
5. I also understand that there are no risks involved in participating in this activity, beyond those risks experienced in everyday life.
6. I have read the information above. By signing below and returning this form, I am consenting to participate in this questionnaire project.

Signature of participant

Date

I believe the participant is giving informed consent to participate in this study

Signature of researcher

Date



Dear Respondent

The purpose of this research project is to investigate the current security measures on Mobile Money Systems in Lesotho (Vodacom M-Pesa and Econet Ecocash), mainly the usage of Personal Identification Number (PIN) as the only form of authenticating users while accessing the systems. The study will then recommend Biometric Face Recognition (BFR) as an additional authentication technique to enhance the security of M-Pesa and Ecocash.

This research is conducted by Ntsejoa Ranyali, enrolled in Msc in Computer Systems Management at Botho University Botswana. Please provide your views on this survey because your contribution is highly significant as you are identified because of your involvement in using either or both M-Pesa and EcoCash.

Please note that the information that you will provide will be kept private and confidential and will only be used for the purpose of this study and may be shared with Botho University. Your participation is fully voluntary and if for any reason you would rather not answer a question just skip it.

Thank you for your time.

Yours faithfully

.....

Ntsejoa Ranyali

SECTION A (General Information)

Please indicate your answer by placing a tick in the appropriate category

1. Gender

Male ☐

Female ☐

Prefer not to say ☐

2. Age Group

16-24..... ☐

25-33..... ☐

34-42..... ☐

43-51..... ☐

52 & above..... ☐

3. In which Lesotho region do you live?

Lowlands (*Maseru, Berea*)..... ☐

Semi Lowlands (*Mafeteng, Leribe, Mohale'shoek, Butha-buthe*)..... ☐

Highlands (*Quthing, Qacha, Thaba-tseka, Mokhotlong*)..... ☐

4. Which Mobile Money Service (MMS) are you registered for?

M-Pesa..... ☐

EcoCash..... ☐

Both..... ☐

5. How long have you been using this service?

Less than a year..... ☐

1-2 years..... ☐

3-4 years..... ☐

5-7 years..... ☐

6. Which mobile phone do you use for your MM services?

2G phone (Masechocha).....	☐
Smartphone.....	☐
Tablet.....	☐
All of the above.....	☐

SECTION B (Mobile Money Services)

Please tick the box that best matches your views for each of the following statements in relation to the service of your Mobile Money System (M-Pesa/ EcoCash)

1	Strongly Agree	2	Agree	3	Uncertain	4	Disagree	5	Strongly Disagree
----------	-----------------------	----------	--------------	----------	------------------	----------	-----------------	----------	--------------------------

	1	2	3	4	5
a) MMS are reliable and convenient					
b) MMS are time efficient					
c) MMS are secure					
d) MMS are affordable					
e) MMS are easy to use					
f) MMS service center is easily accessible by phone					
g) The customer service representative was quick to solve my problem or answer my question					
h) The service generally meets my expectations					
i) I would recommend this service to someone I know					

SECTION C (Challenges in M-Pesa/EcoCash)

1. Have you ever had challenges while using M-Pesa/EcoCash, if no please proceed to SECTION D

Yes ☐

No ☐

2. If yes, are they related to the following?

Poor network..... ☐

Unavailability of agents..... ☐

Inability of agents to provide money..... ☐

Exceeding withdrawal limit..... ☐

Sending money to the wrong recipient..... ☐

It is too complicated..... ☐

Other (**Please specify**).....

3. Was your problem solved?

Yes ☐

No ☐

4. Was it solved through any of the following?

Customer service representative was quick to assist me..... ☐

Visited the nearest branch..... ☐

Looked for alternative Agents..... ☐

Moved to a location with better Cell phone reception..... ☐

Other (**Please specify**).....

SECTION D (Security of M-Pesa/EcoCash)

1.

	YES	NO
a) Have you ever shared your PIN with anyone?	☐	☐
b) If yes, do you still think your account is still safe?	☐	☐
c) Do you think your PIN can be easily guessable?	☐	☐
d) Do you think your PIN provides enough security for your account?	☐	☐
e) Did you ever forget your PIN?	☐	☐
f) If you ever forget your PIN, would you still remember the answer to the security question you set while you were registering your PIN?	☐	☐

2. How often do you change your PIN?

Very frequently.....☐

Frequently.....☐

Occasionally.....☐

Very rarely.....☐

Never.....☐

3. Have you ever been a victim of fraud in M-Pesa/EcoCash, or someone you know?

If no please proceed to Question 7.

Yes ☐ No ☐

4. Did it relate to any of the following frauds

Received a fake SMS claiming received monies.....☐

Someone who knows your PIN performing a transaction without your knowledge.....☐

Stolen/lost phone and transaction was performed.....☐

Unauthorized SIM swap..... ☐

Other (**Please specify**).....

5. Were any of the above solved?

Yes ☐

No ☐

6. If yes, was it through any of the following?

Mobile Money Operator (Vodacom/Econet) intervened..... ☐

Reported the matter to the police..... ☐

Other (**Please specify**).....

7. PIN is the only method that is used by (M-Pesa/Ecocash) to allow users to access their accounts. Is there a need for an additional method to improve the security of these systems?

Yes ☐

No ☐

8. Are you familiar with any of the following biometric authentication techniques?

Fingerprint..... ☐

Hand geometry..... ☐

Voice..... ☐

Face recognition..... ☐

None..... ☐

Other (**Please specify**).....

9. M-Pesa/Ecocash can adopt Biometric Face Recognition (BFR) method which identify and authenticate the user from a digital image. The user will enter PIN and take a Picture so that they can be granted access to their accounts.

Please rate the above authentication process

☐ 1 Strongly Agree
 ☐ 2 Agree
 ☐ 3 Uncertain
 ☐ 4 Disagree
 ☐ 5 Strongly Disagree

	1	2	3	4	5
a) It will improve the security of (M-Pesa/EcoCash)					
b) It will complicate the current process of doing transactions					
c) It will be convenient for the user					
d) I will be comfortable to always take a picture with every (M-Pesa/EcoCash) transaction I make					
e) This feature will attract more people to use (M-Pesa/EcoCash)					

10. What are the challenges that will prevent you from using the above system?

I do not have a smart phone.....☐
 It is too complicated.....☐
 I am concerned about my privacy.....☐
 It is not secure.....☐
 None.....☐
 Other (Please specify).....

Thank You!