ENHANCING SECURITY OF MPESA TRANSACTIONS BY USE OF VOICE BIOMETRICS

BY

LUCY JEPKEMBOI CHETALAM

Project Submitted to the School of Science and Technology in Partial Fulfilment of for the Degree of Master of Science in Information Systems and Technology

UNITED STATES INTERNATIONAL UNIVERSITY-AFRICA

SPRING 2018
STUDENT’S DECLARATION

I, the undersigned, declare that this is my original work and has not been submitted to any other college, institution, or university other than the United States International University Africa for academic credit.

Signed: __________________________ Date: ______________________________

Lucy Jepkemboi Chetalam (ID Number: 649679)

This project has been presented for examination with my approval as the appointed supervisor.

Signed: __________________________ Date: ______________________________

Mr. Dalton Ndirangu

Signed: __________________________ Date: ______________________________

Dean, School of Science & Technology
COPYRIGHT

All rights reserved. No part of this dissertation report may be photocopied, recorded or otherwise reproduced, stored in retrieval system or transmitted in any electronic or mechanical means without prior permission of USIU-A or the author.

Lucy Chetalam © 2018
ABSTRACT

The main objective of this project is to 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. The voice biometric is a state of the art technology that factors in authentication with better usability with the aim of combating fraud, self-service empowerment and cost savings through proper use of time and saving or reduction of administration costs for companies. The research study addressed the following objectives; to investigate the authentication schemes used by mobile money services; to investigate the major MPESA fraud techniques used in Kenya; to implement and analyse a time efficient, secure mobile-based multi-factor authentication scheme using device specific ID, voice biometric and a PIN for securing MPESA transactions.

A design science research was used 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 population of study were MPESA subscribers around Mirema-USIU area. The sample frame was drawn from the population of study. The research study adopted the purposing sampling techniques to enable selection of respondents who were only relevant to be sampled.

Collection of data was done via online Google Forms questionnaire survey and a descriptive method was used to carry out the data analysis. A total of thirty (32) questionnaires were sent to users via Google Forms online survey and all the questionnaires were duly filled in hence giving a response rate of 100%. The research design adopted quantitative techniques where data was analysed and presented in form of graphs and charts. The research also adopted a qualitative technique, where the individual views from respondents for example, their understanding of voice biometrics.

The findings regarding the first research study objective on investigating the authentication schemes used by mobile money services indicated that majority of respondents, 75% indicated that MPESA 4-digit PIN as a security measure is insufficient and 56.3% think that their PINs can easily be guessed. The study hence identified a big gap in the security of mobile money transactions in terms of using PIN as a security
measure when performing mobile transactions. The study also indicated that majority of the respondents indicated that adding biometrics will improve MPESA security. The findings regarding the second research study objective on investigating the major MPESA fraud techniques used in Kenya revealed that there are different techniques are used by fraudsters these include reversal of transactions, unauthorized sim-swap, identity theft, erroneous transactions, scam messages and insider theft. The research study revealed that MPESA subscribers were aware of the fraud techniques used in their area which was mostly unauthorized SIM-swap and identity theft. A model was developed on the android platform, VMPESA, to address issues regarding objective three, 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 research concluded PIN is not a sufficient security measure when performing mobile transactions and fraudsters are taking advantage of this vulnerability to defraud MPESA subscribers by using techniques such as SIM-swap, reversal transactions and scam messages. Voice biometrics is a factor that can be used to achieve a high degree of benefits and advantages in lowering the risk within mobile financial systems with specific reference to MPESA mobile money transfer system. The study recommended that for mobile money service providers to provide safe and secure transactions, they should concentrate on implementing multi-factor authentication schemes in their system. They should also identify the major weaknesses of the implementing single factor authentication, such as PIN, as a security measure. Mobile money service providers should also be aware that fraudsters are employing new techniques everyday therefore continuous upgrade of the security features is imperative. Safeguarding subscriber personal information and account is extremely important and should be top priority to these organisations. Researchers should do further studies on alternative multifactor authentication schemes which have more functionalities to make the entire process more seamless, convenient for the subscribers and intelligent in nature. Further studies should be done to identify the advance techniques used by fraudsters to acquire subscribers’ personal information.
ACKNOWLEDGEMENT

Much thanks to our Lord God, for the love, life, wisdom and knowledge He has given me and for seeing me through my entire Master’s degree program. Secondly, I acknowledge and appreciate the support and guidance of my project supervisor, Mr. Dalton Ndirangu whose vast experience, knowledge, corrections and insights shaped my academic pursuits and provided guidance to enable completion of this project. Thank you and may God bless you abundantly.
DEDICATION

I dedicated this work to the Almighty God for giving me the strength and wisdom to make it this far. Special thanks to my beloved parents for their unending love and support they have provided me in my entire life, to my dear husband Vincent, my lovely children Ethan Gitau and Eleanor Wangui for your love, patience and understanding.
# TABLE OF CONTENTS

STUDENT’S DECLARATION ........................................................................................................ii
COPYRIGHT .......................................................................................................................... iii
ABSTRACT ............................................................................................................................. iv
ACKNOWLEDGEMENT ......................................................................................................... vi
DEDICATION ......................................................................................................................... vii
TABLE OF CONTENTS ....................................................................................................... viii
LIST OF TABLES .................................................................................................................. xi
LIST OF FIGURES ............................................................................................................... xii
ABBREVIATIONS ................................................................................................................ xiv

## Chapter 1: Introduction ...................................................................................................... 1
1.1 Background of the Problem ............................................................................................ 1
1.2 Statement of the Problem .............................................................................................. 5
1.3 Research Objectives ..................................................................................................... 7
  1.3.1 General Objectives .................................................................................................. 7
  1.3.2 Specific Objectives .................................................................................................. 7
1.4 Significance of the Study .............................................................................................. 7
1.5 Scope of the Study ......................................................................................................... 8
1.6 Definition of Terms ....................................................................................................... 8
1.7 Chapter Summary ......................................................................................................... 9

## Chapter 2: Literature Review ........................................................................................... 10
2.1 Introduction .................................................................................................................. 10
2.2 Investigating Authentication Factors Used By Mobile Money Services ............... 10
  2.2.1 Authentication Factors ........................................................................................... 10
    2.2.1.1 Single Factor Authentication ........................................................................ 11
    2.2.1.2 Two -Factor Authentication ........................................................................ 16
    2.2.1.3 Multifactor Authentication (MFA) ............................................................... 16
2.3 Major MPESA Fraud Techniques Used In Kenya ..................................................... 25
2.4 Impact of Implementing a Voice Biometric Feature on Mobile Transactions ......... 30
2.5 Conceptual Framework ............................................................................................... 32
2.6 Research Gap ............................................................................................................... 34
2.7 Chapter Summary ....................................................................................................... 34
5.4 Major MPESA Fraud Techniques used in Kenya......................................................... 102
5.5 Impact of Implementing Voice Biometrics Feature on Mobile Transactions............. 105
5.6. Chapter Summary ................................................................................................. 109

Chapter 6: Discussion, Conclusion and Recommendation ....................................... 110

6.1 Introduction............................................................................................................. 110
6.2 Summary ............................................................................................................... 110
6.3 Discussions .......................................................................................................... 113
   6.3.1 Authentication Schemes Used by Mobile Money Services......................... 113
   6.3.2 Major MPESA Fraud Techniques used in Kenya....................................... 117
   6.3.3 Impact of Implementing Voice Biometrics Feature on Mobile Transactions118
6.4 Conclusion ............................................................................................................ 121
   6.4.1 Authentication Schemes Used by Mobile Money Services......................... 122
   6.4.2 Major MPESA Fraud Techniques used in Kenya....................................... 122
   6.4.3 Impact of Implementing Voice Biometrics Feature on Mobile Transactions123
6.5 Recommendations ................................................................................................. 123
   6.5.1 Authentication Schemes Used by Mobile Money Services......................... 123
   6.5.2 Major MPESA Fraud Techniques used in Kenya....................................... 123
   6.5.3 Impact of Implementing Voice Biometrics Feature on Mobile Transactions123
   6.5.4 General Recommendation........................................................................... 124

References.................................................................................................................. 126

Appendices ................................................................................................................ 134

Appendix I: Questionnaire ......................................................................................... 134
LIST OF TABLES

Table 2-1: Comparison of Various Biometric Technologies..................................................23
Table 3-2: Population Distribution.........................................................................................36
Table 3-3: Sample Size Distribution.....................................................................................37
Table 4-4: Functional Requirements .....................................................................................45
Table 4-5: Non-Functional Requirements .............................................................................45
Table 4-6: Login Narration..................................................................................................62
Table 4-7: Withdraw Narration.............................................................................................63
Table 4-8: Check Balance Narration......................................................................................64
Table 4-9: Send Money Narration........................................................................................65
Table 4-10: Registration Narration........................................................................................67
Table 4-11: Voice Registration Narration..............................................................................68
Table 4-12: Manage Subscriber Details Narration...............................................................69
Table 4-13: Deposit Narration...............................................................................................71
### LIST OF FIGURES

Figure 1-2: Basic Design Framework.......................................................................................... 32
Figure 2-2: Speaker Identification............................................................................................. 32
Figure 2-3: Speaker Verification................................................................................................. 33
Figure 2-4: Authentication Process ............................................................................................ 33
Figure 3-5: Prototype Model ...................................................................................................... 40
Figure 4-6: Android System Architecture .................................................................................. 47
Figure 4-7: Voice Biometrics Enrollment ................................................................................... 50
Figure 4-8: High Level Platform Architecture .......................................................................... 53
Figure 4-9: Trigger Event Occurs............................................................................................... 54
Figure 4-10: User Authentication System Notified the Voice Biometric Application ............... 54
Figure 4-11: Voice Biometric Application Makes Secure REST Requests to the VBG Voice Biometric Platform .............................................................................................................. 55
Figure 4-12: The Voice Biometric Application Queries the Voice Biometric Platform to Find out What Prompt Should is shown to the User ................................................................................. 56
Figure 4-13: The Voice Biometric Application Queries the Voice Biometric Platform to Find Out What Prompt Should Be Shown to the User ............................................................................ 56
Figure 4-14: IVR Makes Call from Cloud .................................................................................. 57
Figure 4-15: The Voice Biometric Application Queries the Voice Biometric Platform for Status When Necessary .............................................................................................................. 57
Figure 4-16: User Responds to Prompts and Completes the Verification Process .................. 58
Figure 4-17: The Voice Biometric Application Polls and Gets Final Result and Signals Pass/Fail to the User Authentication System .................................................................................. 58
Figure 4-18: Text-dependent Biometric Engine ......................................................................... 59
Figure 4-19: VMPESA - Level 0 DFD........................................................................................ 59
Figure 4-20: VMPESA - Level 1 DFD........................................................................................ 60
Figure 4-22: VM-PESA – Use Case Diagram (Agent) ............................................................... 61
Figure 4-23: Subscriber Login Sequence Diagram ..................................................................... 73
Figure 4-24: Subscriber Transaction Sequence Diagram .......................................................... 74
Figure 4-25: Subscriber Login Activity Diagram ....................................................................... 74
Figure 4-26: VMPESA ERD ...................................................................................................... 75
Figure 4-27: Landing Page ......................................................................................................... 79
Figure 4-28: Agent Transaction Page ......................................................................................... 79
Figure 4-29: Registered Subscriber Enter Phone Number Page.................................................. 80
Figure 5-42: Importance of Information Security and Data Protection ...................................... 91
Figure 5-47: 4-digit Start Key Used when Registering for MPESA ........................................ 94
Figure 5-48: MPESA Secret Word Used when Registering for MPESA .................................. 95
Figure 5-49: MPESA Secret Word Used when Calling MPESA Customer Support .................. 95
Figure 5-51: Easily Guessed MPESA PIN ............................................................................ 96
Figure 5-52: Improve MPESA Security by Adding another Security Feature to the MPESA PIN 97
Figure 5-55: Adding Biometrics Will Improve MPESA Security ............................................ 99
Figure 5-56: Ever Used Voice Biometrics in Any System ....................................................... 99
Figure 5-57: Is Voice Biometrics the Most Secure Type of Security for MPESA .................... 100
Figure 5-58: Easily Use Voice Biometrics When Transacting Using MPESA ....................... 101
Figure 5-59: Voice Biometrics Would Slow Down the MPESA Process ............................ 101
Figure 5-62: MPESA PIN Revelation .................................................................................... 103
Figure 5-63: What Means Did the Fraudster Use ................................................................. 103
Figure 5-64: Fraud Techniques Used in the Area .................................................................. 104
Figure 5-65: Type of Fraud Techniques Used in the Area ..................................................... 104
Figure 5-66: Registering for VMPESA Services .................................................................. 105
Figure 5-67: Assistance to Register Voice on VMPESA .................................................... 106
Figure 5-68: Transaction Duration Using the VMPESA Application .................................... 107
Figure 5-69: Problems When Transacting Using the VMPESA Application ....................... 108
### Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APIs</td>
<td>Application Programming Interfaces</td>
</tr>
<tr>
<td>CER</td>
<td>Crossover Error Rate</td>
</tr>
<tr>
<td>CFK</td>
<td>Consumers Federation of Kenya</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>DFD</td>
<td>Data Flow Diagram</td>
</tr>
<tr>
<td>DVM</td>
<td>Dalvik Virtual Machine</td>
</tr>
<tr>
<td>DNA</td>
<td>Deoxyribonucleic Acid</td>
</tr>
<tr>
<td>ERD</td>
<td>Entity Relationship Diagrams</td>
</tr>
<tr>
<td>FAR</td>
<td>False Acceptance Rate</td>
</tr>
<tr>
<td>FRR</td>
<td>False Rejection Rate</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>HAL</td>
<td>Hardware Abstraction Layer</td>
</tr>
<tr>
<td>IMEI</td>
<td>International Mobile Equipment Identity</td>
</tr>
<tr>
<td>IVR</td>
<td>Interactive Voice Response</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile Station International Subscriber Directory Number</td>
</tr>
<tr>
<td>OTT</td>
<td>Over the Top</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>RAD</td>
<td>Rapid Application Development</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a service</td>
</tr>
<tr>
<td>SDK</td>
<td>Software Development Kit</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>USSD</td>
<td>Unstructured Supplementary Service Data</td>
</tr>
<tr>
<td>VMPESA</td>
<td>Voice Mpesa</td>
</tr>
<tr>
<td>3FA</td>
<td>Three Factor Authentication</td>
</tr>
<tr>
<td>3G</td>
<td>Third Generation</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

1.1 Background of the Problem

MPESA is an important mobile money transfer service in Kenya that was inaugurated on the 6th of March 2007 by Safaricom in collaboration with Vodafone (Vodafone, 2017). It is a messaged based cash transfer service that allows users to deposit, send, and withdraw money using their cell phones (Buku, 2012).

Ten years after the launch of MPESA, mobile money has become ubiquitous in Kenya. Growth was explosive from the start: there were 20,000 active subscribers in the first month (March 2007) and one million active subscribers eight months later. As more subscribers joined Safaricom, it immediately increased its value by launching new products and services, and expanded the ecosystem through diverse partnerships (Safaricom, Celebrating 9 years of changing lives, 2016).

Based on its positive results in Kenya, MPESA has expanded to an international platform, slowly and progressively becoming one of the most used and favourable medium of personal money transfers. Its growth is phenomenal and many stories and testimonials have been documented (Karuri, 2012). MPESA celebrated its 10th anniversary in March 2017, but with these celebrations it noted a challenge; the increase of MPESA fraud cases reported. Fraudsters have found a loop hole in Safaricom’s MPESA services, and have used it to swindle unsuspecting subscribers and MPESA agents by electronically wiping out MPESA accounts leading to insurmountable loses to customers and the organization (Ndung’u, 2012).

Consumers Federation of Kenya (CFK) mentioned that today’s fraudsters use social engineering to achieve their objectives. One way of doing this is by calling their victims pretending to be safaricom customer care, then using automatically generated short codes or passwords to wipe out subscribers MPESA accounts (Kenya, 2017). CFK report further indicates that these fraudsters actually appear to have some experience in customer care (of mobile service providers) hence manage to easily convince the victims. They are very patient and can call the prey repeatedly without switching off their mobile numbers (Kenya, 2017). An article by Dominic Omondi from Standard Group noted that fraudsters are employing smart techniques of obtaining the victim’s personal details and PIN number (Omondi, 2016). The fraudsters then proceed to swap SIM cards hence accessing the customer’s funds in the MPESA account.
This year alone, Safaricom dismissed 52 employees for fraudulent behaviour; this number is 16 more than the 36 it sent home the previous year. The company also mentioned that those who were dismissed were found to have been involved in fraudulent SIM card swaps and violation of rules governing money transfer service MPESA start key issuance (Safaricom, Sustainability Report, 2017). The Telco firm has now dismissed 130 employees since 2014 over fraud and corruption.

To help its customers safeguard themselves from social engineering attacks and the criminal syndicates, Safaricom has taken the initiative to continuously run mass market caravan campaigns and other activations, especially in rural areas. This awareness campaigns are meant to alert and enlighten customers of the common fraud schemes used by crime syndicates, they also offer advice and provide guidance on the steps its subscribers can take to prevent being defrauded (Safaricom, Sustainability Report, 2017). This confirms the fact that MPESA fraudulent activities are on the raise and that its negative impact is affecting both the users and Safaricom as an organization, thus the need to improve the authentication process on MPESA transactions in order to greatly reduce the number of MPESA fraudulent cases.

The introduction and uptake of mobile technology has led to phenomenal growth and impact in developing countries in the past decade. It has been a major catalyst for economic development and social growth creating opportunities to both rural and urban populations. From Al-Jabir’s point of view, mobile technology has also revolutionised the financial sector and has forced financial institutions to change the way they operate and conduct their business (Al-Jabir, 2012). Consequentially, banks and other financial institutions are now offering mobile banking services to keep up with the technological evolution. These services require proper security due to the ubiquity of mobile devices. It is important to secure mobile data from hackers, to prevent attack and theft of data. Authentication is very important because it allows only authorized individuals to gain access to the data (Sameer Hayikader, 2016).

The definition of mobile banking as by Mobile Survey is “using a mobile phone to access your bank or credit union account. This can be done either by accessing your bank or credit union’s web page through the web browser on your mobile phone, via text messaging, or by using an app downloaded to your mobile phone.” It is therefore
important to secure data transmission from mobile phone to prevent hackers from attacking and stealing the data. Authentication is also important which only allows authorized users to have access to the data.

Services offered by mobile banking include 1) person-to-person transfer of money; 2) person-to-business payments for buying a variety of goods or services, and 3) mobile banking which enables customers make payments, deposit and withdraw cash by accessing their bank accounts, (Jenkins, 2008). In addition to this, there are a number of mobile technology benefits that a country can experience, these include; more efficient financial transfers which are conducted by low income traders. Secondly, it aims to provide financial services to the greater population who are unbanked.

Mobile banking service requires the highest level of security since it deals with subscribers personal information and money. This service creates an attractive environment for hackers and fraudsters who target the money transacted through this service. In addition, subscribers can also misuse this service for money laundering and perform illegal transactions. Chrystel Gaber said that, “it is important that mobile services comply with the financial and ICT policies already formulated to enable mitigation of risks involved”. Some of the risks present when providing mobile money services include money laundering, privacy and security, consumer protection, fraud, and credit and liquidity risks.

Fraudsters are continuously looking for new techniques to exploit the mobile money services. It’s a multimillion business and keeps increasing annually. The government, business owners and other stakeholders have an interest in preventing, detecting and mitigating fraud. Everyday innocent Kenyans have fallen victims to criminals and fraudsters targeting the mobile money service. These criminals have identified loopholes in the mobile money services and have gone further to use reverse psychology to perpetuate fraudulent activity against users.

Telkom, Airtel, Safaricom are the main telecommunication operators and provide mobile money services to the citizen of Kenya. These services require users to use their Personal Identification Numbers (PIN) and passwords as a security measure to identify users. This level of authentication is known as single factor authentication.
Praveen Kumar J, noted that users use easy passwords that can be guessed, or similar passwords for different accounts, or store their passwords on devices or write them on a piece of paper. One of the main shortcomings with passwords or PINs is that many users either have no knowledge of making strong and memorable passwords or underrate the need for security (Praveen Kumar J., June 2016). Such management and security challenges may be a weak point for hackers to steal passwords through snooping, shoulder surfing, sniffing, guessing (Aloul, 2009). Research carried out by Syracuse University researchers has proven that hackers can identify PINs by interpreting video of individuals tapping on their phone screens despite the display not being visible. Software that is used to interpret these video depends on “spatio-temporal dynamics” that measures the distance between the fingers and the phone’s screen, and proceeds to guess exact characters the fingers press on the phone’s keypad (Diksha Shukla, 2015).

The above research clearly demonstrates that passwords and PIN is no longer sufficient security measure. A stronger more secure feature is the Three Factor Authentication (3FA). 3FA has three key features: Firstly, what the subscriber knows for example password or PIN code. Secondly, what the subscriber has for example electronic card or IMEI Number. Lastly, the characteristics of the paying client for example behavioural or biometric feature (voice). User authentication by use of PIN is the most basic scheme that is used for information assurance and security that has the lowest cost. PIN can be changed by the subscriber (mobile) once he/she gets access to the account. IMEI number is used to identify the mobile phones uniquely. However, many network and security features are enabled by knowing the current device being used by a subscriber (Prof. Krishna P. Tayade, 2015). Voice biometric authentication plays a main role in 3- factor authentication by digitizing an individual’s speech to generate a stored model voice print or template (GlobalSecurity.org, 2017).

Safaricom has invested heavily in customer awareness by engaging in radio, television advertising. In addition to this, Safaricom has a dedicated page on their website that provides tips to MPESA subscribers on how to avoid being party to MPESA fraud and scams. The company has also improved in MPESA services by adding the ‘Hakikisha’ feature. This service is for all MPESA subscribers that enable users of this service to verify and confirm the name of the individual they are sending money to before
completing the transaction. In addition to this, subscribers who are withdrawing cash from their MPESA account can also confirm the name of the agent (Safaricom, Hakikisha, 2016). The company has recently a voice biometric system that is coded “Jitambulishe” which enables an easier access for services such as PUK requests and resetting MPESA pins through enabling a vocal password to be established. The use of a vocal password limits access to confidential passwords in print therefore limiting fraud and enhanced authentication (Ngao, 2018).

As much as this information is available, innocent subscribers are still falling victims of MPESA fraud.

Despite the security measures, campaigns and policies put in place, the level of mobile money fraud and hacking is still high and continues to rise. This begs the question, is there enough security for mobile subscribers when performing transactions?

This study focused on integrating voice biometric solution during authentication of MPESA transactions that will significantly reduce the fraud incidences. It has also highlighted the challenges faced by subscribers of MPESA while transacting and aimed at improving the authentication process of MPESA by incorporating (3FA) Three Factor Authentication feature in a mobile application. The challenges with the current MPESA authentication were first determined. The next step identified the major fraud techniques used. A mobile based application with a voice authentication system was developed to improve on the existing authentication feature. This approach identified MPESA users who tested the application, collection of data, designing and development of the Voice Biometric Mobile Application and its deployment, and finally analysis of the authentication accuracy and the time taken to validate users.

This research adds new knowledge of incorporating voice biometrics as an authentication security feature as an enhancement to MPESA services.

1.2 Statement of the Problem

MPESA is a value added service that Safaricom developed that aimed to solve the problem of sending money. Value-added services have ranged from media transfers, accessing the internet, playing games and now, as a mobile banking platform. But the
change from traditional ways of sending and storing cash to mobile banking has introduced new security issues (Macharia, Fraudsters eye mobile money, 2011).

According to a report by Serianu - 2016, as result of Mobile money revolution in Africa, fraud has increased. Another result of this revolution is mobile money service has extended its services to be integrated with other financial platforms such as insurance, banking, and e-commerce. The report notes that unfortunately most mobile money applications do not have basic security controls for example encryption of data (Serianu, Africa Cyber Security Report, 2016).

The weakest link in the mobile money chain is at the point of registration. This is where double authentication is needed to verify customers’ phone numbers match the mobile money account. Despite this measure, the system needs continuous and consistent monitoring, as fraudsters are always searching for ways to exploit the system.

A report by Kenya Bankers Association (KBA) and Anti-fraud Police Unit disclosed that most fraud cases happen in close collaboration with staff and noted that identity theft as a rising trend. One Kenyan bank reported how criminals would forge customers' IDs and proceed to approach bank staff, requesting personal details to be changed (Macharia, 2011).

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 helps agents confirm the transaction through a message code received on their phone, correlating the users ID and the transaction details. Despite this identification system, fraudsters still find a way to defraud unsuspecting MPESA customers by sending fake messages or lottery wins to random customers (Macharia, 2011).

One of the con schemes (as I had mentioned earlier on) involves the fraudsters posing as customer care agents from leading telecoms. They proceed to ask questions to verify the owner of the line. Most of the questions begin with one's identification number followed by many other questions that target to acquire a subscriber's mobile money account PIN. These fraudsters or con men are swift are masters of psychology. They already know the kind of questions one would ask and they are prepared with answers (Nampa-Xinhua, 2016).
1.3 Research Objectives

1.3.1 General Objectives
The objective of this research study was to improve MPESA authentication by use of voice biometric mobile application.

1.3.2 Specific Objectives
The research encompasses a study and implementation of a mobile-based multi-factor authentication to be specific voice biometric authentication scheme for MPESA. Specific objectives are:

i. To investigate authentication schemes used by mobile money services.

ii. To investigate the major MPESA fraud techniques used in Kenya.

iii. To implement and analyze a time efficient, secure mobile-based multi-factor authentication scheme using device specific ID, voice biometric and a PIN for securing MPESA transactions.

1.4 Significance of the Study
This research study has highlighted the weaknesses involved when implementing a PIN based authentication feature in MPESA. In addition to this, it has clearly shown the importance of using voice biometrics in MPESA as an important security feature of MPESA to ensure mobile subscriber private information and MPESA account remain secure. Use biological characteristics offer unique and accurate identification methods. These features ensure only the authorized person gets access as a result you get high level of security. Biometrics also creates a clear, definable audit trail of transactions.

The study’s practical knowledge generated will be very helpful to the management and technical team financial institutions who offer mobile money services to their customers. This information will be used to develop effective strategies and techniques of protecting customer information while performing financial transactions using their mobile phones. The study will be of great benefit to the following:

1.4.1 Financial and Microfinance Institutions
Financial institutions will find this research study very important by learning how to improve on services offered to their customers by providing safe and secure mobile transactions. They will be able to gain competitive advantage by first enabling customers’ access their monies through their phones and secondly securing the financial transactions by use of voice biometrics.
As noted by Wang et al. (2012), the increase of smartphones usage would lead to the increased usage of financial transactions. This follows the trend of shifting financial transactions from the computer or banking hall to the mobile phone. The consumer expects the mobile device to have enough security or to inform them of any potential harm of an application (Banuri et al., 2012).

Research carried out in South Korea, investigating the increased usage of the smartphone, noted that trust and security impacted the use of mobile phones to conduct banking transactions and the paper identified the following security threats; hacking, malicious code, stolen ID/passcode and fraudulent SSL digital certificate (Kim, 2013). Some of the advantages that users of these services stand to gain from include convenience. Currently customers are subjected to frequent renewal of complex passwords and this causes some inconvenience in terms of remembering and creating a new complex password every time.

1.4.2 Scholars and Researchers
This research study will make a significant contribution to the existing knowledge regarding implementation of voice biometrics on mobile applications that perform financial transactions.

1.5 Scope of the Study
The scope of this study is limited to authentication process of MPESA. The system is a mobile application with a voice biometric feature aimed to simulate the MPESA process.

1.6 Definition of Terms

1.6.1 PIN
Personal Identification Number is an identifying number used to authenticate the originator of the transaction by use of a secret code, which is known to the originator of the transaction and is in some way verifiable by electronic equipment under control of the institution that controls the funds (Stein, 1989).

1.6.2 MPESA
(M for mobile, Pesa, Swahili for money) is a mobile phone-based money transfer and micro financing service, launched in 2007 by Vodafone for Safaricom and Vodacom, the largest mobile network operators in Kenya and Tanzania. MPESA allows users to exchange cash for "e-float" on their phones, to send e-float to other cellular phone users, and to exchange e-float back into cash (Mbiti, 2011).
1.6.3 IMEI
International Mobile Equipment Identifier (IMEI) is a 15-digit number that uniquely identifies an individual wireless device. The IMEI is automatically transmitted by the phone when the network asks for it. A network operator might request the IMEI to determine if a device is in disrepair, stolen or to gather statistics on fraud or faults (Factor, 2018).

1.7 Chapter Summary
This chapter highlighted the significance of MPESA to Safaricom mobile subscribers and identified the major fraud techniques fraudsters use to defraud MPESA subscribers. The research has also highlighted that fraudsters are always devising new ways to con people and are now using social engineering to con subscribers.

This resulted in designing and development of a mobile application that has a voice biometric feature that will improve the security of customer information during transactions. Chapter two contains the research literature review which gives evidence to support the system to be developed.
Chapter 2: Literature Review

2.1. Introduction
This chapter in the project looks at the specific objectives regarding improving of MPESA authentication using voice biometrics. The chapter also presents a literature review of whether employing the use voice biometrics significantly increases the overall security of mobile money transactions. It also looks at the existing MPESA authentication techniques and identifies the potential fraud techniques used by fraudsters in Kenya. This chapter also discusses a conceptual model of mobile registration using device specific ID, voice biometric and a PIN for securing MPESA transactions. The chapter draws further conclusions and summaries about the objectives discussed.

2.2. Investigating Authentication Factors Used by Mobile Money Services

2.2.1. Authentication Factors
This chapter looks at the specific objectives regarding improving of MPESA authentication using voice biometrics. The chapter also presents a literature review of whether employing the use voice biometrics significantly increases the overall security of mobile money transactions. It also looks at the existing MPESA authentication techniques and identifies the potential fraud techniques used by fraudsters in Kenya. This chapter also discusses a conceptual model or basic design framework of mobile registration using device specific ID, voice biometric and a PIN for securing MPESA transactions. The chapter draws further conclusions and summaries about the objectives discussed.

According to Richardson (2008) although all authentication methods or factors are used in authentication process, biometric authentication methods offer more benefits over other methods. So far users and agents of MPESA in Kenya are authenticated by using PIN. A PIN is used to uniquely authenticate either an agent or customer whenever he/she wants to carry out any mobile money transaction. However, the unique “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 (Tipton, 2004). A robust authentication method is therefore needed to prevent unauthorized access of mobile money account.
2.2.1.1. **Single Factor Authentication**

Rouse (2015) mentions that single-factor or one step authentication can be defined as a process of ensuring access to a given system that uses only a single category of specific credentials to identify the user. An example that fits is the signature. It is considered as the simplest form of identification and an assumption is that the presentation of the sign will match the actual identity. This description highlights Single factor authentication (SFA). The risk identified in such a scenario is that if some other party has access to the sign or assumption then the purpose of the SFA becomes null and void.

The largest mobile network operator in Kenya is Safaricom (Mas, 2010) and MPESA security is based on Single Factor Authentication whereby the user’s phone number is used as the ID and 4-Digit PIN is used as the security feature.

**MPESA TECHNOLOGY**

Unstructured Supplementary Service Data (USSD), Short Message Service (SMS) and Subscriber Identity Module (SIM) Toolkit-STK are three popular access technologies used in MMS in East Africa (Mauree, 2013). USSD is a protocol used in Global System for Mobile Communications (GSM) for supporting communication between mobile phones and service provider computers. USSD enables a real-time “session” to be initiated between the mobile user and the USSD application platform. When the service is invoked, it permits data to be sent back and forth between the mobile user and the USSD application platform until the USSD service is completed (Janagoudar, 2011). Once the session terminates the USSD application platform may be configured to allow an SMS to be sent to the user via Short Message Service Center (SMSC) in a GSM network. Safaricom chose to use the SIM Toolkit (STK) with SMS delivery. With STK the user has an application on the SIM card which is accessed from the phone’s menu (Group W. B., 2009).

Safaricom website gives steps which a user can register and use MPESA services. This is as follows.

i. **Registering New MPESA Customer**

A new Safaricom user who wishes to use the MPESA services is required to provide the following:-

- A Safaricom handset number
- First, last name
• Date of one’s birth
• An original document (identification document)

The following original identification documents are required for MPESA registration:

• Kenyan Personal National ID
• Passport or Military ID
• Alien ID

The next step is to activate the MPESA account.

ii. MPESA Account Activation

Once registration is complete, the Agent and the newly registered user will receive a message from MPESA confirming that the registration has been successful. The registered user will also receive a 4-digit Start Key issuing following instructions:

• Under Safaricom main menu select MPESA
• Select ‘Activate’ in English or ‘Wezesha’ in Swahili
• Input ‘Start Key’ (4-digit code received through MPESA)
• Formulate new PIN (a preferred/chosen 4-digit code which will be the new PIN)
• Confirm PIN through entering four digit code again
• Input ID number (same one that the agent inputted upon registration)

MPESA will send a menu to the registered user’s phone with a ‘Secret Word’, press OK on receipt.

iii. MPESA PIN

The MPESA PIN is mainly used when transacting, sending / withdrawing money from the MPESA accounts when using MPESA menu in one’s Safaricom SIM. The newly registered user is expected to personally keep the PIN secret.

iv. MPESA Secret Word

MPESA secret word is sent to a newly registered user immediately after registration. This word is used for identification when a registered user calls the MPESA Support (call-line 234). Registered users are not expected to share the secret code with anyone except the Safaricom user or client support staff. The above steps clearly show that MPESA security is based on Single Factor authentication whereby the user’s phone number is used as the ID and 4-Digit PIN is used as the security feature
a) Challenges of Single Factor Authentication

The main trouble associated with codes or passwords is the fact that many users don’t understand the way to make memorable and strong passwords or they underestimate the importance of security. Some of these passwords may be compromised or cracked within seconds making the codes ineffective similar to having no password at all. Besides those avenues remaining in need of being guarded against comprise, passwords should be less identifiable or predictable especially to machines. Test of codes or password-entropy simulates or predicts difficulty in cracking a specific password through guessing, forced cracking, dictionary-attacks or any other common means (Rouse, single-factor authentication (SFA), 2015). Passwords may still be cracked through brute force, dictionary as well as rainbow table attacks once a hacker or attacker gets the password to the database that is used or resides in a protected computer. Administrators should also do their role to protect codes / passwords against dictionary attacks. A good example may be through adding various random characters against the special numbers or characters in the password encryption thus making them less vulnerable or less prone to dictionary-based attacks, also known as password salting. The current speeds in CPUs today may facilitate such attacks. Brute-force attacks are a real or major threat that relates to passwords. Massive parallel general purpose graphics processing (GPGPU) password-cracking as well as rainbow tables have made it actually possible for unauthorized users to produce excess of 500,000,000 codes per second. Another threat in password-based validation or authentication systems can be termed as social engineering. Other threats to passwords, for instance Trojans may find access through email messages. Concisely, passwords are some of the most vulnerable or broken forms of authentication (Rouse, TechTarget, 2017).

There are several security challenges raised by the use of USSD technology in mobile money services. PIN passes through USSD technology to the server in plain text this makes system vulnerable to attackers who can use network sniffers applications like Wire-shark can intercept it. Also, the service provider can read the sent PIN (Kelvin Chikomo, 2006). To add to this USSD technology is vulnerable to malware attacks. Attackers have discovered techniques to capture USSD codes and exploit Android devices (Dobie, 2012). Some of Android applications can directly pass a USSD code to the dialer and proceed to execute USSD code without prompting the user (Guo, 2004).
These vulnerabilities on USSD technology can be used by attackers to access information stored in the SIM.

Mobile phones are now being used to store sensitive information such as bank details, confidential personal and business information, PINs. In addition, they are also used to conduct several transactions such as bill payments (Lipa na MPESA, pay bill) money transfer, online purchase. Also smart phones are also expensive devices. Due to these attributes, smart phones have therefore become the target of attacks. A report by computer crime and security survey 2009 indicated that, 42% of the respondents experienced “laptop and mobile hardware loss or theft” and 12% of these cases led to data breaches (Richardson, CSI Computer Crime and Security, 2008). Mobile phone devices are also prone to virus attacks. According to the report by NISA user’s lack of proper information and awareness on smartphone might lead the user to install applications from non-trusted sources (Mudiri, 2013). These applications might have malware that can change private information in the phone or send personal information to other devices. The information sent by malware can later be used by an attacker to conduct fraud in MPESA. Moreover, mobile phone has several security features that have not been activated by the manufacturer. It is upon the user of the phone to activate these security features for example allowing of encryption of the data. If such features are not enabled, the online interception of the sensitive stored data such user’s PIN is possible by the third party.

The customer who owns a mobile money account is accountable for maintaining security of his/her account. The manner in which mobile phones, SIM card and PIN are handled by the customer may affect security of the electronic money stored in mobile money account. For example, over trust of customer to mobile money agents such as telling them the PIN when the customer wants to withdraw money from mobile money account can lead to security breach. Sharing of mobile phones among family members and co-workers also may lead to unauthorized access of the mobile money account. The habit of charging many mobile phones at one place such as at the agent’s office also adds more security risks, as it provides a room for a dishonest agent to access someone’s mobile money account without being permitted by the owner.

In order for a person to use mobile money account he/she must be registered using customer ID card. Types of identifications that are allowed include valid passport, employment ID, and an introduction letter from the village or ward executive officer.
According to (A. Basigie . Mtaho, 2014), registration process in MMSs creates more security vulnerabilities in many ways. For example, so far it is not possible to verify whether the ID card used for registering a mobile money customer was fake or real because mobile money agents have no special tools to verify those IDs. They just rely on inspecting the physical document without contacting the legitimate authority that provided it. This means that there is a possibility for a person to register with incorrect personal particular and perform any unauthorized transactions later without being identified (A. Basigie . Mtaho, 2014).

Usually mobile money business is done by agent separately or together with other services. Agent offices may have several staffs who serve for distinct services in the same office or shop. In case a dishonest staff who is not serving for MMSs knows the mobile money PIN of another staff who serves for MMSs, unauthorized transaction may be committed. The environments in which MMSs are carried are also subjected to security risks. For example, while some agents have permanent offices, other agents in town centres 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.

The current MMA method makes use of PIN to prove if the subscriber who performs a particular transaction is an authorized user. All MMSs such as money transfer; cash withdrawal and airtime purchase requires the use of PIN. The PIN used is too short (only 4 digits) which makes it easy for people to guess. Yet, such PIN is unmasked (written in clear text) therefore becomes more vulnerable for a snooping attack. The same PIN is used for authenticating a user for all MMSs. Sharing of PIN among users or family members also add more security risks. Studies Tipton (2004) have reported that most users use their date of births as PINs. Such tendency leads to a critical security vulnerability as date of birth can be known from different sources, such as a co-worker, family member, relative, various record management systems etc. Also, currently there is no specific protection when user’s mobile phone is stolen by fraudsters who can successfully figure out the user’s PIN (Dobie, 2012).
2.2.1.2. Two -Factor Authentication
Two step factor authentication code in systems is a user friendly way and requires memory of both passwords. The aim of cyber security is to maintain integrity, availability thus the privacy of information entrusted in systems can be obtained through using such an authentication technique.
Two step-factor authentications have reduced cases of fraud however, not completely. It only acts as an extra added layer in security for the single-step factor authentication. In addition, it is through the information security steps that two methods of identification are simultaneously combined for increasing the authenticity in the identification of user. 2FA requires specific two authentication factors:

(i) Something that a user knows, e.g. an alphanumeric password
(ii) Something that a user knows and which he/she can click, example: graphical password

2.2.1.3. Multifactor Authentication (MFA)
The main aim of Multifactor Authentication is to make it difficult or harder for unauthorized users to gain access to a system. Multifactor authentication process is whereby two or more different aspects are used complementarily to authenticate (Alireza Pirayesh Sabzevar, 2008). We looked at how biometrics can be used in Multifactor Authentication.

i. Biometrics
Biometrics refers to the automated methods in recognizing people based on physiological as well as behavioral characteristics. As per Coats et al (2007), physiological features are very unique identifiers as no two persons have similar biometric measurements.
Physiological biometrics defines the use of physical features for instance fingerprints, hand, iris or face in recognition. On the other hand, behavioral biometric defines the use of a behavioral feature, which may be the voice, keystroke or signature.
According to the definition by Russ, authentication defines the process involved in reliably verifying peoples’ identity or that of a specific individual or item.(Russ, 2000) It is explained as the process used in determining whether something or someone is who, what it has been declared. Woodward also defines biometric authentication as the automated method used in determining the identity that is of an actual living person based on phenotypic characteristics. (Woodward et al 2001). Biometric system can be some verification (authentication) platform which equates to an identification system.
Identification is defined as confirmation of a person’s identity using a username that is an identifier.

Verification is the confirmation or no confirmation of identity when using a specific verifier such as a password. In biometrics, the process of verification involves authentication of users in conjunction or complementarily with credit or smart cards or usernames.

Biometric authentication satisfies regulatory definition of multi-step factor authentication. Users can biometrically authenticate through fingerprint, voiceprint and iris checks using the provided equipment and then they enter a password/PIN to open a credential vault. However, this form of authentication is only suitable in certain applications, the solution can become unacceptably time consuming and comparatively costly when large numbers of clients are involved.

Additionally, it is highly vulnerable to a recurrent attack: once biometric information becomes compromised, it can be easily be re-used unless the user is completely protected and guarded. Voice Biometrics has distinct advantage through which it can question user to quote random phrases, thereby significantly reducing risk of successful recurrent attack. Finally, there is a great resistance to the use of biometric authentication. Users resist the action of having their personal phenotypic traits captured as well as recorded to be used in authentication.

Concisely, selection then the successful deployment of a biometric system requires precise consideration of a number of factors. In many biometric equipment or identifiers, the biometric information is factored into algorithm or mathematic information. Devices scan the physical features, copy specific critical information, then stores output in a string of data. Comparison is made between data strings and sufficient commonality constitutes affirmation then a match is given. It can be appreciated that the choice of the level of information to match and what level of accuracy, governs accuracy/speed ratio of biometric device.

All biometric equipment, therefore, does not provide absurd guarantees of specific identity, but rather chances or probabilities may provide misleading outputs. If the biometric system is used against many users - perhaps all customers of a certain bank - the error level may make a system unreasonable to use. Biometric data may be copied and may not be easily altered. This aspect is a key disadvantage because, if discovered, compromised information cannot be corrected.
A user may easily change the password; however, users cannot alter their fingerprints. A bio-identifier may also be feigned or faked. An example: fingerprints may be captured via sticky tapes and fake gelatin prints made. Simple photos eye-retinas may be presented. More expensive sensors should be capable of distinguishing live original and fake replicas, although such devices cannot be practical in mass distribution. It is possible that; as biometric identifier equipment become widespread, better or sophisticated techniques in hacking will be developed.

Historically, fingerprints identifications have been the most accurate method in authentication. Other biometric ways such as eye-retinal scans may be promising, although they have become easily ‘spoof-able’ in their practice. Two-tiered or Hybrid authentication methods are a good compelling solution, like private keys which are encrypted through fingerprint within a USB equipment or device.

Criticism in biometrics authentication is that although it’s easy to determine strength of password by its length, composition and therefore the more time available to brute-force, the strength in a biometric may be difficult to measure. There is no guarantee that simple attacks shall not be created tomorrow, for instance by using local-homemade components to make artificial fingers from fingerprints that qualify to be authenticated by a machine or fingerprint reader. This aspect has raised some concern in some government security agencies where knowledge of strength held by a security mechanism is more imperative than a mechanism which may be better but whose full strength might not be quantifiable.

There are new specific types of biometrics developed which have been presented and proposed which are expected to have different types of identification at the preliminary or formative levels. (Pankati S, 2018) These new biometrics include: brainwave, DNA id, body odor id, vascular pattern match, gait recognition, fingernail bed match, ear pattern match, hand grip recognition, body salinity id, infrared fingertip imaging as well as pattern matching.

Ideally the current biometrics set ups should not only identify imposters and enhance security authentication, they should also keep a record of transactions effected through the used biometrics features. This aspect shall reveal the source as well as the evidence to prosecute and enhance security levels (Jaiswal, 2018).

ii. Voice Biometric

Human beings are naturally characterized by unique human voices and the unique ability to identify the different kind of voices and sounds from individuals. The written version
of a human voice printed is also known as a spectrogram or a voice print or voice gram or spectral waterfall or a sonogram. The technology of linking the unique human voice by the person’s id data or the claimed id is known as voice biometrics. Voice biometrics employs the technology of pattern matching system software which selects the key aspects unique to one’s voice and creates an id which helps identify the individual based on sound. The voice biometric application can be linked to the speaker recognition systems which recognize a voice and match it up with what is in the database through the automated speaker recognition process.

Voice identification refers to the process used in matching voice samples to specific as well as unique digital voice prints recorded before as a means used in identity authentication. Speech recognizers analyze huge samples of voice data which contain words spoken by different people of various ages, gender and racial origins as well as geographic and social backgrounds. The system formulates digital representations that have very high chance of accurate interpretation. Each voice is specifically constructed on physiological as well as behavioral characteristics. Physiological aspects include the size, shape of each individual’s mouth, throat, the larynx, the nasal cavity, the weight amongst other factors; these features cause the natural pitch, the tone and the timbre. Behavioral aspects are those that are formed based on linguistics, education or influence, geography and cause speech cadence, the inflection, the accent, and the dialect (Inc., 2016).

Voice biometrics inculcates technology which uses uniqueness of voice to identify people. Since the voice print is unique in every individual as well as non-replicable, biometrics can be a more effective, secure means of identification and authentication.

According to results of a survey by Unisys, biometric measures ranked through consumer preference are: one, voice recognition: (32%), two, fingerprints: (27%), three, facial scan: (20%), four, hand geometry: (12%), five iris scan: (10%). This ranking confirms that people prefer the aspects of convenience as well as familiarity in choosing a type of biometric application.

Voice biometric is more convenient to apply or use remotely and it leverages equipment which is ubiquitously available in a person’s voice. It is flexible, that is, can be useful whether one is using smart-phones, landline phone or flip-phones. When it is about security administration, applications in voice biometrics become a powerful limitation to fraud as well as corruption.
Voice biometrics has become one of the most sought after forms of secure authentication. Different companies in light of the current technological age have become under threat due to the technological threats which comprises entity and user information. Therefore there has been the need to safeguard against these threats from ‘spoofers ‘and hackers through enhanced technological identification. This aspect has been underscored through specific means for instance through the use of random repeat sentences or random repeat numbers which the hackers cannot have access to. These hackers only have access to recorded sound information.

Interactive voice response (IVR) is classical example of the application of voice biometrics. The different service providers’ record and store voice prints which has been an upgrade from the previous use of pin numbers which has been riddled with imposters who find access to pin numbers and defraud different entities or user accounts. Many financial companies use the voice biometric feature to leverage against various credit lines accessed through phone banking and teleshopping as some of the examples.

Interference

The voice biometric applications may be affected during the recording time by different background or environmental noises which affect the quality of sound. Variations in sound quality may also be due to health, injury or age related aspects or even user behaviour. The use of voice biometrics currently has a low market penetration and small market share because of the areas where it is used. This aspect highlights the different strengths of voice biometric systems. High robust biometric systems are not subject to considerable or significant changes over time and therefore high degree of robustness. A biometric system based on low degree of robustness is subject to small changes over time. Distinctiveness is a feature that differentiates or distinguishes variations in the voices recorded therefore defining the best or most unique identifier. There is a difference between identification and verification which is essentially the main purpose of biometrics in general. Identification questions seek a general answer for instance when trying to identify a new person. On the other hand verification questions try to identify if the person speaking is a particular person.

Licensing for the voice biometrics software has been projected to increase from 49 M in 2015 to 565.8 M in 2024 as per a report produced by a market research agency Tractica . The use of voice biometrics has been projected to increase over time with specific uses being mostly expected in mobile devices which shall the speaker recognition equipment
and a higher technological adoption. Other areas where voice biometrics shall be imperative shall be in hospitals for patient medical forms /records access, wearable devices identification, IT systems authentication especially for Governments, mobile money agencies, call centres and even car control systems amongst many other applications. In this research project the focus is narrowed down to voice biometric application within the context of Safaricom Company in Kenya, MPESA functionality and how incorporation of the voice biometric is expected to have improved overall processes of authentication.

Voice biometrics has to be automatic as the system has the capability to distinguish between minute variations that may sound identical to a person or other sounds that may sound identical if listened to by human ears. Application of voice biometrics has been on the rise following various institutions expressing their interest in protecting themselves against id theft, fraud and general unauthorized access. The maximum utility of voice biometrics however is achieved through the use of the voice feature in remote identification which is completely un-intrusive (Thakkar, 2018).

The application of the three factor authentication (3FA) which involves one the use of a card or token then a pin number normally and then the use of a biometric feature such as voice constitute the best form of authentication. The use of such an integrated system heightens the security of any entity that employs the combined security features.

“Say Pay Code” is a password that users use once for secure binding of user financials with the user to enhance authentication of mobile transactions; this has been the basis for Say Pay company that has made voice biometrics applicable in the mobile transactions. The “say pay code” is used for transacting security protocols as a voice biometric authentication (PYMNTS, 2016).

Safaricom Company LTD has recently introduced a voice biometric system that is coded “Jitambulishe” which enables an easier access for services such as PUK requests and resetting MPESA pins through enabling a vocal password to be established. The use of a vocal password limits access to confidential passwords in print therefore limiting fraud and enhanced authentication (Ngao, 2018). Safaricom new roll out program uses a voice biometric application for authentication purposes for specific functionalities such as pin resetting and generating the new PUK which are currently the only functions for voice biometrics in the firm’s portfolio. The firm’s voice recordings are not stored and customer care agents are used to verify users via phone conversations. A more recent development
is the development of an interactive voice response particularly for the visually impaired under MPESA with some enabled MPESA functionalities such as MPESA balance queries (Oloo, 2018).

- **Advantages of Voice Biometrics**

  There are numerous advantages of implementing voice authentication. The cost of implementing voice biometrics is low because there is no special hardware required. A simple telephone or microphone is needed to authenticate using her voice. Despite its simplicity, the use of remote identification and voice feature simultaneously may be quite costly. Remote identification biometrics that have been used before constitute fingerprints, iris and even facial recognition. Most of these biometric features require the use of a special set up which becomes a limitation in away. Myers (2004) also agrees that other biometric authentication methods like fingerprinting and retinal scans require special devices (Myers, 2004). Ideally the most preferable authentication measure that does not require any special apparatus or set up is voice biometric. The automated speaker recognizer through phone lines or mobile handsets does the job of recording the voice and matching it to the database which then provides the match. The user may not require any sound equipment such as microphones and this voice feature is efficient to the extent of the user becoming oblivious to his or her voice being processed. This aspect enables the voice biometric to be one of the most secure means of authentication which bars out ‘spoofer’ or hackers who may want to hack the database to acquire the recorded voice prints (Thakkar, 2018). A voice-authentication in built application in software is relatively easy to use coupled by the natural determination in people in trying to identify someone via voice first assuming the person is making a phone call. Voice authentication is also highly popular amongst users.

  The most important feature of voice biometrics as mentioned by Myers is that the biometric allows remote identification which makes it unique among all the other biometrics. (Myers, 2004). The voice biometric for instance provides the convenience of remote transaction of bank transactions which is enabled through a voice authentication rather than the traditional way of having to be manually present within the bank premises for fingerprint authentication.

  The time taken to enroll in a voice authentication system is quite short. The process of enrollment requires a user to utter either random or specific words that make up a sentence or numbers which are used to create a voice print which is recorded and stored
for purposes of future matching. Quality is usually the basis for the capture of a good voice print which usually takes about 2 to 8 seconds. (Myers, 2004).

Another advantage is the authentication process is very fast. Authentication is performed in approximately 0.5 seconds. Authenticating a user is a process of comparing a voiceprint that was made at enrolment to a sample issued when user needs to access a system.

Another benefit is the storage size or space of voiceprint is rather small. This allows it to be stored anywhere, this includes; smart cards, disks, databases and even cell phones.

- **Disadvantages of Voice Biometrics**

According to research done at the Sans Institute, voice biometrics is not listed as the best authentication application therefore there has to be some reinforcement of the integrated application with other forms of authentication to have a high level authentication system. There is more security when the voice biometric is applied simultaneously to PIN requirements for instance thus illustrating one of the shortcomings. The human voice gets ragged over time due to various factors which limits the longevity of voice samples collected. This aspect highlights a disadvantage which characterizes voice biometrics.

The table below shows a comparison of the current biometric technologies in a variety of categories.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Fingerprint</th>
<th>Hand Geometry</th>
<th>Retina</th>
<th>Iris</th>
<th>Face</th>
<th>Signature</th>
<th>Voice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ease of Use</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Error incidence</td>
<td>Dryness, dirt, age</td>
<td>Hand injury, age</td>
<td>Glasses</td>
<td>Poor Lighting</td>
<td>Lighting, age, glasses, hair</td>
<td>Changing signatures</td>
<td>Noise, colds, weather</td>
</tr>
<tr>
<td>Accuracy</td>
<td>High</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Cost</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>User acceptance</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Required security level</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Very High</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Long-term stability</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Source: (Myers, 2004)

**Table 2-1: Comparison of Various Biometric Technologies**
• **Accuracy of Voice Biometrics**

Speech is a complex signal that has many possible variations of that signal for the same individual. These variations reduce the accuracy of speech recognition (Nicolas Scheffer, 2013). Accuracy in voice authentication is variant based on several factors. Difference in telephones or handsets may be problematic. For instance registration for voice biometric through a handset may be different than is a landline issued thus becoming a problem. Other factors may include illness, age that affects voice, background noises which may interfere with the quality of the recording. Fingerprint biometric is also affected due to factors such as skin peeling off due to various reasons for instance the kind of work one does or may even be affected adversely by aging thus causing a problem. Accuracy of biometrics based on the following subsets:

- Failure to correctly enroll – the user’s registration in system is not completed successfully.
- False to be accepted – the user becomes authenticated irregularly.
- False rejection – the user is not verified or authenticated when he or she is supposed to.

Systems which analyze biometric information should balance the *false acceptance rate* and the *false rejection rate*. Emphasizing on requirements for specific match may lower the *false acceptance rate* (FAR), but likely to raise *false rejection rate* (FRR). A plot for FAR and FRR against one other similar to a demand and supply curve, the point where they intersect is the *crossover error rate* (CER). Therefore, the lower CER, the more efficient the biometric system application.

Source: (Silverman, 2018)

Figure 2-1: Crossover Error Rate Attempts to Combine Two Measures of Biometric Accuracy

24
2.3. Major MPESA Fraud Techniques Used In Kenya

A report by Serianu highlighted that the estimated cost of cybercrime in Kenya has soared to $175 million and this cost will continue to grow as more business automate their processes. The report continues to mention that mobile transfer of money in Kenya has experienced many attacks as a function of social engineering, the spread of malware and account personifications. As alternative channels for bank heists, hackers are exploiting weak security controls in mobile money systems or platforms to wreak havoc through stealing millions.

The Kenya Cyber Security Report also mentions that there is a rise of malware targeting mobile and banking infrastructure. The report notes that there are many types of malware in internal systems including: Trojans for instance, Dridex, Zeus malware and attackers are using these forms of programs to compromise as well as access very sensitive information in the network. Unfortunately, statistics largely remain vague as companies are slow to reveal extent to which the attackers have caused damage (Serianu, The Kenya Cyber Security Report, 2016).

Research by Amwoyo (2014) provides information that local software engineers are developing solutions and requesting for Application Programming Interfaces (APIs) to enable the solutions transact securely with Mobile Money Transfer Systems and Commercial Banks so as to reduce lead times. The research also notes that most of the local Mobile Money Transfer Systems do not have standardized and documented APIs for integration. This is hampering the growth of local online businesses. He continues to mention that with the rise of SaaS business model, there is a need to address secure logins. In addition, authentications schemes need to be aligned with the current devices that are accessing the online portals (like tablets and smart phones), hence a paradigm shift from traditional two factor authentications. More so, there is a need to transact securely using emerging and widely accepted innovations like MPESA Mobile Money Transfer System. (Amwoyo, 2014).

Amwoyo continues to analyze static or single step password (one-factor) verification and authentication mechanisms and notes that this scheme is prone to brute-force attacks resulting to unauthorized access, assuming unlimited attempts and the subsequent time. Finally, authentication that is based on one step factor does not ensure adequate security as the static password doesn’t really change in between subsequent logins or is seldom
altered. The risk may be largely reduced by continually altering the password, as provided by the One-Time Password (OTP) two-step factor authentication system (Amwoyo, 2014).

According to Communications Commission of Kenya (CCK) report, 75% of Kenyan population has access to mobile phones therefore it is necessary to provide phone based multi-factor authentication so as to keep up with technological trends like Cloud Computing Software as a Service (SaaS) business models.

Mobile money fraud is not only affecting users of MPESA. It is global problem. In Ghana, the Ghana Chamber of Telecommunications reported that in April 2017, mobile money companies in Ghana which include, MTN, Airtel Money, TigoCash, and Vodafone Cash noted 388 cash fraud cases in the 2016 financial year against 278 cases recorded in 2015. Various amounts of money were stolen by fraudsters; majority of those cases were reported to law enforcement for additional investigations and a few have been fruitful/successful given that suspects were tried as well as convicted in relation to the fraudulent actions (Kunateh, 2017).

Although mobile money companies did not state the amounts of money stolen by fraudsters, majority of cases were reported to law enforcement for further inquiry and investigation. Some fraudsters who were involved in some of the cases were prosecuted.

In lieu of these activities, the telecom industry experts warned about the rise of mobile money theft; mobile cash fraud that is rampant in Kenya, Tanzania and Uganda is on the rise in Ghana and it was expected to increase because of identifiable loopholes within the national identification, authentication system, ignorance and greed among others (Kunateh, 2017).

2.3.1. Ways of Attacking System

Amwoyo (2014) highlights the techniques which fraudsters use to attack the system includes;

i. **An Attacker Can Determine the Shared Secret**

A good example is by attacking an authenticator or management system, using reverse-engineering of the possession factor or intercepting secret codes during authentication. In case of a lock and key system, the lock may be picked. In a properly secured mobile money platform for example, the database containing shared secret codes can be compromised by SQL injection. An example is the *Man-in-the-Middle Attack*. 
a. **Man-In-The-Middle Attack**

The attacker may access the specific authentication process then masquerade as main authenticator to a party with authentication, in a man-in-the-middle attack. In the other case: lock and key, the attacker may interpose a fake or dummy lock which shall allow them make a copy of key then later on, utilize the copy in accessing the real lock. In the case that explains the computer system, the hacker can for instance interpose some counterfeit authentication platform to intercept communications and channel information between legitimate user and the actual authenticator.

The man-in-the-middle attack in cryptography or computer security represents a form of eavesdropping in which an attacker makes sole connections with victims and communicates messages in between them, convincing them to believe they are conversing directly to one another over private network connection, when in actual sense, the whole conversation is managed by a schemer. The attacker is able to access all messages between two victims as well as create new ones, that is usually straightforward in most circumstances.

ii. **An Attacker may steal Possession Factor.**

In reference to the case of lock and key, an attacker may steal the key then use it just before the actual owner notices the lock changed and the loss incurred. In the case of a mobile phone, the attacker can steal the mobile phone and perform MPESA transactions without the owner noticing and has the device cancelled.

iii. **An Attacker May Copy Possession Factor if it is Inadequately Safeguarded**

An attacker may make an impression of the physical key then go ahead to duplicate it; in the situation of a case of MPESA, possession factor is represented by the PIN. Fraudsters acquire subscribers’ PINs then carry out SIM swaps then carry out MPESA transactions.

2.3.2. **Types of Mobile Money Fraud**

a) **Phishing**

A phishing-attack is when an attacker claims to be someone or something, like an authority, in order to earn a victim’s trust. If the victim trust the attacker enough he or she may give away sensitive information, pay counterfeited invoices or do anything else that the attackers asks for (Frida K., 2016).

This method is a likely avenue for online fraud but is also common in mobile cash fraud. Particulars include the use of handset messages, emails and correspondence via phones trying to trick users of their money through issuing out the secret codes, PINS and
personal information. The customer may also transfer virtual money himself under false promises or schemes. This may also happen with agents/retailer who own trust accounts and perform cash in/cash out transactions (H., 2016).

i. Types of Phishing

▪ Scam Messages/Reversal of Erroneous Transactions:
The fraudsters send communications to users under false pretenses for the user to send money to the phone numbers used to contact them. The fraudsters use different SIM cards or even fake emails or fake handset messages informing the client or user of an MPESA transaction to their phones as a wrongful remittance of cash to the user. Once the client or user gets the information, he or she quickly responds by resending the amount of money to the source, losing out, which is very common to users who are ignorant of the risks of fraud. (Enebeli, 2017)

A cooked message may also be used to perpetrate the fraud through messages formulated to persuade the user to change their PIN by sending the old PIN and the new PIN to the source. Therefore, if the user falls for it, he or she is defrauded of their money. (Enebeli, 2017).

▪ Emotional Delusional SMS:
The fraudster may opt to send a handset message similar to that of the service provider then contact the user posing as a misguided person who had sent money accidentally with a request for the user for to resend the money to a specific number. The fraudster may even pose as a stresses emotional person for the user to easily send the money back without checking the authenticity of the handset message sent to him or her therefore being defrauded. (Enebeli, 2017).

▪ Anonymous Calls from Fraudsters:
The user or client may receive some money from the fraudster as bait. The fraudster then calls and poses as someone who sent money accidentally instead of buying airtime. In light of this explanation some users do not cross check the money or airtime and quickly send money to the source. (Enebeli, 2017).

▪ False Promotion
The false promotions are carried out by tricksters who pose as a staff for telecommunication companies in the lottery business. These fraudsters call a mobile money user under the false pretense and claim that the user has won some prize in light of the intense promotions that have been made by various mobile networks that are in
competition. The fraudsters however request for an advance fee to facilitate the process of the lottery from the user. Users who not aware of the trick usually fall prey and usually remit money to the alleged telecommunications staff therefore being defrauded.

b) Split Transactions
Fraudulent customer care agents send client transactions in small amounts of money in order to have a higher volume of transactions therefore more commissions. The process of breaking transactions in this manner deliberately amounts to fraud on the part of the agent.

c) Commission Frauds by Agents
Agents introduce fake accounts to gain higher registration commissions (Deloitte, 2015).

d) Unauthorized SIM Swap
A fraudster can attempt to use someone else’s wallet account through measures such as pretending to be someone else using fake identity documents. Once the fraudster assumes the wrong identity, he or she swaps SIM cards. Since most of the wallets are linked to MSISDN, the fraudster gains access to wallet of the subscriber and can embezzle the funds. This could be a serious concern for OTT players as they do not have control on SIM swap since they do not own the network (Deloitte, 2015).

e) Identity Theft
Identity theft is usually an inside job activity through unscrupulous employees gaining unauthorized access to mobile money data that belongs to users and then irregularly misappropriating their funds. This form of fraud largely involves the use of client mobile money data for wrongful financial gains on the part of the fraudster.
Identity theft may also be carried out by cybercriminals who may use personal information left online to set up new accounts. The new accounts set up using client information may then be used for various irregular transactions unknown to the original user and this has been on the rise in the recent past (Serianu, 2016).

f) Insider Threat
Research by Serianu indicates that over 80% of fraud within remote systems has been carried out through facilitation by insiders and employees in 2016. The report continues to mention that many cases are based on privileged access and the major reasons for fraud include revenge, financial gains amongst other reasons. Additionally, 50% of the direct cybercrime costs are due to insider threats to the organizations. Organisations have lost
large amounts of money to the tune of billions of shilling as a result of employee fraud within the companies or institutions both in the private and public sector. (Serianu, 2016).

g) **Counterfeit know your customer (KYC)**

The provision of fake documentation in the ‘know your customer’ process has created an avenue for fraudulent persons to access premium mobile wallets therefore being able to defraud quite considerable amounts of cash. This aspect also facilitates the money laundering process therefore denting the economy through mobile money. (Deloitte, 2015).

### 2.4. Impact of Implementing a Voice Biometric Feature on Mobile Transactions

Research data commissioned by Visa and as well as Populas in 2016 provides that, two-thirds of all Europeans are committed and ready to use different biometrics for the purpose of secure transactions or payments. Business Insider periodical predicts that 99% of U.S. handsets (Smartphone) shall be fully biometrics-enabled by the year 2021 (Brown, 2017).

Jonathan Vaux, the Executive Director: Innovation Partnerships mentioned that biometric authentication has created a lot of excitement in transactions space and has also offered a chance to streamline as well as improve customer experience.

Success or failure of biometric systems determines the impacts they have on delivery of service. Biometrics is associated with operational efficiencies for identification and verification procedures (Schneider and Price, 2001). According to Bataller (2011), biometrics application enables self-service as well as automated authentication, thus increasing operational efficiency and assuring security.

By the year 2019, biometrics shall be expected to be a $25 billion market industry, constituted of excess of 500 million biometric equipment scanners in operational use globally, according to the information provided by Marc Goodman, an Interpol and FBI advisor (Sottile, 2016). Eighty percent of the users who expressed some preference claimed they opine that biometric authentication is actually more secure compared to traditional passwords, as per *OnePoll/Gigya* survey (Gigya, 2016).

Driving the accelerated growth is need for combating security breaches manifested by identity theft including the rising number in fraud cases. Researchers attached to the Biometric Research Group (BRG) are also of the opinion that biometrics have potential to lowering operational risks in the banking industry by a 20% minimum within the next 10
years. This statistic means that people can put their trust in remote transactions which includes MPESA transactions done through mobile devices.

Biometrics can lead to improved security for the mobile subscribers which are critical to ensure safe transactions. It also has the potential to improve customer service and enhance customer satisfaction across industries (Wirtz and Hercleous, 2006). Efficiency in service contributes to improved customer satisfaction (Jain et al., 2000).

On the other hand, if the processes to use biometrics are lengthy or erroneous due to system inefficiencies, MPESA services can be negatively affected. This would lead to reluctance in use of the MPESA service culminating to abandonment of the system where mobile subscribers would prefer the traditional methods or alternative services of sending money.

Mobile money fraud is one of the main reasons for biometrics in MPESA. Biometrics is capable of reducing fraud by verifying the identity of mobile subscribers thus reducing the possibilities of fraud. It can also prevent MPESA agents and Safaricom internal staff from committing fraudulent activities.

The use of biometric systems has effects on the cost of service delivery. With efficient and more secure system, the MPESA usage will increase with the decrease in the MPESA fraud cases reported. Enhancing MPESA services through the use of biometrics means money is not lost to fraud. This contributes to the reduction of service delivery cost. Use of alternative security features and unreliable biometric system on the other hand means frequent servicing and supporting the system, thus increasing system support cost. The costs could also be increased in cases where Safaricom engages with third party on advertisements informing the public on MPESA Security features and PIN awareness.
2.5. Conceptual Framework

To have a secure MPESA solution, a number of variables will be built into the application including PIN, device specific token (IMEI), and user voice profile. These variables will be used by mobile subscribers directly or indirectly. The security of the proposed solution will be influenced by the ease of use, complexity of the authentication factors, communication channels and the cryptographic scheme used.

![Diagram of MPESA Application Authentication Process]

**Figure 1-2: Basic Design Framework**

The MPESA authentication process involves extracting the mobile subscriber’s voice sample during registration followed by comparison against voice samples. The user’s voice profile is identified using a speak recognition system. All the speaker recognition equipment is comprised of two major modules (refer to Fig 2-3, Fig 2-4): feature extraction as well as matching. Feature extraction refers to extraction of small data amounts from voice signal which can be later used for representation of each speaker. Feature matching entails the actual process or procedure for identification of unknown speaker through comparison of the extracted specifics from his/her input voice with the voice inputs from sets of other known speakers.

![Diagram of Speaker Identification Process]

**Figure 2-2: Speaker Identification**
All the recognition systems serve two alternative phases. The first phase is referred to as enrolment sessions or the training phase, the second is referred to as operation sessions or the testing phase. Under the training phase, registered speakers need to provide samples or parts of their speech in order for the system to build a reference model unique for that speaker. In the case of speaker verification/authentication systems, additionally, a speaker-specific baseline or threshold is determined mathematically out of training samples. During testing (operational) phase (see Figure 2-5), input speech is linked or matched up with recorded reference models and the recognition decision can be made.

Biometric identification has the functionality of comparing a person’s biometric templates to a set of many recorded profiles then finds the most identical match. Authentication on the flip side involves ‘one-tone’ matching of person’s live reading and the stored profile (Ruggles, 2002). Identification provides answers the question “Who is this person?” while authentication seeks to answer the question, “Is this person who he or she claims to be?” Authentication is typically meant for the positive recognition, whereby the objective is to bar other people from making use of that identity (Jain et al., 2004). Figure 2-5 below illustrates the authentication process.

**Figure 2-3: Speaker Verification**

**Figure 2-4: Authentication Process**
2.6. Research Gap

The literature review clearly shows that with the increase of mobile money usage, there is need to improve the authentication process. The literature review, research has pointed out that PIN as a form security is weak and vulnerable to fraudsters and many Kenyans are victims of MPESA fraud. MPESA PIN and secret word is one of the security features offered by Safaricom. Research has also shown that there is need to increase security by adding layers of security through multifactor authentication. Research has also shown voice biometrics technology has become an imperative tool for effective functionality and secure keeping of customer identification, stronger authentication and fraud mitigation. However, voice biometrics authentication is not currently being used in Kenya for authenticating MPESA transaction by users.

2.7. Chapter Summary

This chapter has covered literature review and the recent studies done on authentication schemes used by mobile money services and MPESA. The following topics were covered the major MPESA fraud techniques used in Kenya, the impact of implementing a voice biometric feature on mobile transactions as well as the specific conceptual framework. The following chapter (chapter three) covers the research methodology, population, design, research procedure, data collection, implementation approach and lastly data analysis methods.
Chapter 3: Research Methodology

3.1. Introduction
The chapter discussed about the research methods which were used in carrying out the study. This included the research design, target population, sampling procedure, methods of data collection, research procedures, implementation approach, data analysis and chapter summary.

3.2. Research Design
The study employed a design science research. The design science research is fundamentally a problem-solving research. It seeks to create innovations that define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, and use of information systems can be effectively and efficiently accomplished (Alan Hevner, 2010).

The research study design 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.

3.3. Population and Sampling Design
3.3.1. Target Population
According to Avwokeni (2006), the definition of ‘population of study’ is a set of all participants that qualify for a study. Ngechu (2004) also defines population as a set of people, elements, services, and events that are being investigated. Population in statistics is the specific population about which information is desired. The main purpose of doing research is to infer research objectives from a sample to a larger population. The process of inference is achieved by use of statistical techniques based on probability theory.

The population of concern in this study was the mobile money users within Mirema-USIU area. The target population for this study were users of mobile money services specifically users who had registered and were using the MPESA mobile money transfer services provided by Safaricom. The total number of the target population was 209.
### Table 3-2: Population Distribution

<table>
<thead>
<tr>
<th>Classification</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fahari Apartments residents</td>
<td>90</td>
</tr>
<tr>
<td>North-View Apartments residents</td>
<td>32</td>
</tr>
<tr>
<td>Esanto Apartments</td>
<td>87</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>209</strong></td>
</tr>
</tbody>
</table>

#### 3.3.2. Sampling Design

A sample design is the framework that serves as the foundation for the selection of a survey sample. Moreover, survey researchers are focused in acquiring some type of information through a survey for some population of interest. It is a technique used by the researchers to get a sample from the population to ensure precise accuracy of the information, Crosby (2001). According to Strydom and De Vos (1998), sampling employs the selection of individuals from a population in a manner that gives an equal chance of selection for each of the individuals in the respective population. Sampling enables drawing of inferences regarding a specified population; hence a sample represents a population in the study. Mugenda (2003) noted that sampling involves selecting a subset of individuals from the chosen population with the aim of estimating the characteristics of the entire population.

#### 3.3.2.1. Sample Frame

A sampling frame is a list of things that you draw a sample from (Carl-Erik S., 2015). A sample frame as defined by Jeovanym (2015) is a group of individuals who can be selected from the target population given the sampling process used in the study. The sampling frame has significant implications on the cost and the quality of any survey. The study drew the sample from MPESA subscribers within Mirema-USIU area.

#### 3.3.2.2. Sampling Technique

Sampling Technique is defined as a process done when researchers aim to draw conclusions for the entire population after conducting a study on a sample taken from the same population. The sampling technique used was non-probability sampling also called as judgment or non-random sampling. It was used since it was the best technique to identify respondents who had valuable information contributing to the research. In non-probability sampling, the population does not have an equal chance of being selected; instead, selection is determined according to some factor (Trochim, 2004). The selection
of the sample was made based on subjective judgment of the investigator in this case the target sample was MPESA subscribers around Mirema-USIU area.

### 3.3.2.3. Sampling Size

According to Polit (2001), sample is a proportion of a population. According to Lind (2008), a sample is a subgroup of the population. The use of a sample enable a researcher save a lot of time and money, and get more detailed information (Bluman, 2009). A sample reflects the population as a whole i.e. it a true representative of the population. Out of the whole population, a sample was selected to be a true representation of the population. The sample size in a research was the number of observations to include in a statistical sample. The sample size is critical in achieving the objective of making an inference about a population from a given sample. Holloway and Wheeler (2002) agree that sample size does not influence the quality of the study and continue to note that there are no guidelines in determining the size. According to Mugenda and Mugenda (2008), a sample should comprise between 10-30% of the population, and a good population sample should be at least 10% and not more than 30% of the entire population. Questionnaires were administered to 32 respondents to determine the data in the research.

#### Table 3-3: Sample Size Distribution

<table>
<thead>
<tr>
<th>Classification</th>
<th>Number in Population</th>
<th>Target Number in Sample</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fahari Apartments residents</strong></td>
<td>90</td>
<td>18</td>
</tr>
<tr>
<td><strong>North-View Apartments residents</strong></td>
<td>32</td>
<td>12</td>
</tr>
<tr>
<td><strong>Esanto Apartments</strong></td>
<td>87</td>
<td>2</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>209</strong></td>
<td><strong>32</strong></td>
</tr>
</tbody>
</table>

### 3.4. Data Collection Methods

Data collection methods presents the researchers with various optional techniques that they can use to obtain relevant data that fits and can be used or applied their area of study. The study used primary data which was collected from respondents, who interacted with the MPESA model application, using both open and closed ended questionnaires. The application installed on a test phone, hence allowing users to interact with it while performing the MPESA transactions. The questionnaire was developed from the objectives of the research and contained both open-ended and closed-ended questions.
The answers to the open-ended questions were to be provided by the respondents. A five-point Likert scale and ranking was used regarding the closed ended questions. A five-point Likert scale ranges from (1) to (5) representing strongly agree and strongly disagree respectively, (2) and (4) represent moderately agree and disagree while (3), represented neutral. The questionnaire had clear instructions for the respondents and assurance of confidentiality. The questionnaire was divided into two sections two sections. One section required the respondents’ personal information, the other section contained questions with concerning the security features of MPESA. Both sections had questions with a direct significance for statistical analysis regarding the area of study.

3.5. Research Procedures

Before administering the questionnaire a pretest was carried out. Five questionnaires were pre-tested and reviewed for precision, completeness, accuracy and clarity of interview questions. This step is critical because it assisted the researcher in deciding whether the questionnaire was well understood by the intended respondents. In addition to this, it helped to determine the time required in answering the questions and finally in establishing whether the researcher could obtain the intended information from the questions asked. Findings received from the pre-test were incorporated into the questionnaire before administering the final copy to the intended respondents for their responses.

The research was carried out by administering online questionnaires to MPESA subscribers. The questionnaires were sent via email to various MPESA subscribers. The respondents were first introduced to the research at to enable them get an understanding of the topic and the expectations required. An introductory cover letter from the University attached also aimed to gain the respondents trust and participation. The respondents were also enabled to interact with the MPESA model application with the enhanced voice biometric security feature.

The questionnaires also had a brief description of the research and assured respondents of confidentiality.

3.6. Implementation Approach

According to Russo (1995), system development methodologies are promoted as a means of improving the management and control of the software development process, structuring and simplifying the process, and standardizing the development process and product by specifying activities to be done and techniques to be used. Different types of
system development methodologies are used in designing information system. Depending upon the actual requirement of the system, different approaches for data processing are adopted. The following are examples of the various system development methodologies: The Waterfall Model, Prototyping Model, Incremental Process Model, Spiral Model, Rapid Application Development (RAD) Model, Iterative Enhancement Model, Evolutionary Process Model, and the Unified Process Model (Aggarwal & Singh, 2007). The implementation approach that this research study adopted was the Prototyping Model as illustrated in figure 6 below. The Prototyping Model is a method in which a working sample is built, tested, and then reworked as necessary until an acceptable prototype is finally achieved. This method is best to use when some of the system requirements have been identified. It’s an iterative, trial-and-error process that continually adds onto the sample built. In software development, prototypes are used to emulate a model of the proposed system. The prototype will enable development to uncover any underlying issues and address them early enough before the main application is developed and released. The prototype then acts as a base for replication and further development based on lessons learned (Hackney & Elizabeth, 2015).

This research study developed a model of the MPESA application on the android platform. The first prototype was developed which incorporated the most important functionality that is the voice biometric during authentication. The next cycle involved incorporating the PIN validation.
Pros of Prototyping process model

There is reduction in time and cost. Requirements and specifications are determined early therefore resulting in faster and cheaper software products. In addition to this, there is improved and increased user involvement.

![Prototype Model Diagram](image)

Source: (NIVT, 2010)

**Figure 3-5: Prototype Model**

### 3.7. Data Analysis Method

The process of analysing, cleaning, transforming, and modelling data collected is called data analysis (Wagner, Halley & Zaino 2011). The purpose of analysing data is to obtain usable and useful information. This research adopted quantitative data analysis. In quantitative data analysis, raw information was transformed into meaningful data through the application of rational and critical thinking (Dudovskiy, 2017).

Reliability of the questionnaires was tested using the Cronbach’s alpha method. Psychomerika (1951) defines Cronbach’s alpha as a measure of the internal consistency of a test or scale; it is expressed as a number between 0 and 1. Data collected was checked for accuracy and completeness. The results of the data are represented in form of charts, tables with percentages and frequency distributions. These features enabled clear understanding and interpretation of the data collected. Data analysis was performed using the IBM SPSS tool. Findings were presented using charts, graphs, and tables.
3.8. Chapter Summary

This chapter covered the research methodology, population and design, data collection, research procedure, implementation approach, and data analysis methods in relation to the research specific objectives. In addition, this chapter attempted to define the target populations, sample size and technique used while carrying out the research. Lastly, the data collected was analysed using SPSS and findings represented in form of charts, tables and figures. These findings were also followed by a detailed explanation of the diagrams.

The next chapter presents the data analysis and interpretation of findings.
Chapter 4: System Implementation

4.1. Introduction

A software development methodology is a set of rules and guidelines that are used in the process of researching, planning, designing, developing, testing, setup and maintaining a software product. The methodology includes core values that are upheld by the project team and tools used in the planning, development and implementation process (Mihai, 2014). Software engineering involves the initial system’s requirements engineering process, software design, to the management and maintenance of the deployed system as noted by Sommerville (2009). Sommerville continued to note that system implementation is a very critical stage within the process of software development. System implementation involves the creation of an executable version of the software system. Implementation of the system may at times involve the use of programs in low-level or high-level programming languages, or the adoption of off-the-shelf, generic software systems, to meet the respective user’s or organizations requirements. Software designs give a description of the software structure to be developed and implemented. It comprises of data structures and models, system components, interface involved within the various components, at times the algorithms applied (Sommerville, 2009).

To meet the objective of developing a voice biometric system model to improve on the security of MPESA, VMPESA System was designed, developed, and implemented using Android technology. The system design and development of VMPESA System involved various steps that will be discussed in detail in this chapter. These steps include: carrying out of system feasibility studies, requirements engineering, system analysis and design, system development and implementation, and eventually system deployment on the Google Play Store Cloud Services.

Development of the model was done using open-source software. The tools used include android studio, MySQL database, Notepad ++. According to StatCounter, the mobile operating system market share in Kenya as of May 2018 indicates that android operating system has a percentage of 81.17% (StatCounter, 2018). This fact determined the mobile operating system to use.
4.1.1. System Design Methodology

a) System Feasibility

Feasibility study is described as a short and focused study that is supposed to take place during the early stages of the requirements engineering process (Sommerville, 2009). This process should answer the following questions:

a) Is the system under development able to reduce subscriber’s exposure to fraud?

b) Can the system be developed and implemented within the given budget and schedule using the currently available technology i.e. reduce costs for authentication?

c) Can the system improve customer experience?

If the above questions are met with respect to the system been developed, then that means the developers can go ahead and implement it (Sommerville, 2009). VMPESA System was developed to meet the objective of coming up with a voice biometric system model to improve on the security of MPESA transactions. It was developed with the aim of reducing fraud cases involving SIM swapping and identity theft. The system was also developed within budget and schedule to meet user requirements. The system also improved customer experience; hence it met the feasibility study.

b) System Specification

<table>
<thead>
<tr>
<th>Hardware Specifications</th>
<th>Software Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor: Intel Core i5/i7</td>
<td>Operating System: Android OS, windows 10</td>
</tr>
<tr>
<td>RAM: 8 GB</td>
<td>Language: JAVA, PHP</td>
</tr>
<tr>
<td>Hard Disk: 500 GB</td>
<td>Database: MYSQL</td>
</tr>
<tr>
<td>Monitor: 17 Inch Color</td>
<td>IDE: Android Studio 2017</td>
</tr>
<tr>
<td>Peripheral’s: Mouse&amp;Keyboard</td>
<td>EDITOR: Notepad++</td>
</tr>
</tbody>
</table>

c) System Configuration

The android application configuration in this study covered various modules and components that were developed. These modules are separate implementation of components that when put together they form the entire system.
• **Registration module**
  This module is concerned with enabling subscribers to register to use the system. It also enables them to access the system by accessing and using the system using their respective credentials.
    - **Personal details**
      This module is concerned with capturing the subscriber’s personal details. These details include names, date of birth, phone number and identification number.
    - **Voice sample submission**
      This module is concerned with recording and submitting subscriber’s voice samples to the Voice Biometrics Platform.

• **Transaction module**
  This module is concerned with allowing users of the system to transact of the platform. The transactions include: Deposits, Withdrawals, Send Money and Check Balance.
    - **Deposit**
      • This module is concerned with allowing authorized users to deposit money to subscriber accounts.
        - **Send Money**
          • This module is concerned with allowing subscribers to send money to other subscribers’ accounts.
        - **Withdrawal**
          • This module is concerned with allowing authorized users to withdraw money from their accounts.
          - **Pin verification**
            • This module is concerned with verifying subscriber’s PIN when performing transactions. All users are issued with a PIN number during registration.
          - **Voice verification**
            • This module is concerned with verifying subscriber’s voice when performing transactions. Subscribers submit voice samples during registration.
d) System Services
This section outlines the various functional and non-functional requirements of VMPESA mobile application.

Table 4-4: Functional Requirements

<table>
<thead>
<tr>
<th>Functional Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VMPESA Access</strong></td>
<td>The system shall enable a user to access the VMPESA application once installed on the mobile phone.</td>
</tr>
<tr>
<td><strong>Register personal details</strong></td>
<td>The system shall enable new user personal details to be registered on to the system using the registration functionality. The system shall generate a 4-digit PIN that will be used when performing transactions.</td>
</tr>
<tr>
<td><strong>Voice Sample Recording</strong></td>
<td>The system shall enable users to record and submit three voice samples. The application will also allow users to re-submit audio samples.</td>
</tr>
<tr>
<td><strong>Withdrawals</strong></td>
<td>The system shall allow the registered users to perform withdrawals based on their available balance.</td>
</tr>
<tr>
<td><strong>Deposit</strong></td>
<td>The system shall allow the authorized agents to perform deposits.</td>
</tr>
<tr>
<td><strong>Send Money</strong></td>
<td>The system shall allow users to send money to other registered users.</td>
</tr>
<tr>
<td><strong>Balance Check</strong></td>
<td>The system shall enable the users check their available account balance.</td>
</tr>
<tr>
<td><strong>Voice verification</strong></td>
<td>The system will perform voice verification before a transaction is completed.</td>
</tr>
</tbody>
</table>

Table 4-5: Non-Functional Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td>The system shall ensure the security of its user’s credentials. This system has many security measures to protect user’s credentials at various levels such as:</td>
</tr>
<tr>
<td></td>
<td><strong>Database Level:</strong> The database is password protected. PINs are</td>
</tr>
</tbody>
</table>
encrypted, and every user credentials have a security stamp.

**Application Level**: The system has an API Key and Access Tokens to protect any unauthorized users from accessing it. The application generates a random transaction identifier used for each transaction.

<table>
<thead>
<tr>
<th>Response Time</th>
<th>Response time with respect to user requests should be within 1 to 3 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput</td>
<td>The system shall allow many users to access it concurrently.</td>
</tr>
<tr>
<td>Reliability</td>
<td>The system shall be 99% operational.</td>
</tr>
<tr>
<td>Accuracy</td>
<td>The system shall present accurate data to the users to maintain its credibility and that of the users as well.</td>
</tr>
<tr>
<td>Access Reliability</td>
<td>The system shall be accessible 99% of the time.</td>
</tr>
<tr>
<td>Availability</td>
<td>The system shall be available to users 24 hours a day/7 day a week.</td>
</tr>
<tr>
<td>Portability</td>
<td>The system shall support various android versions available.</td>
</tr>
<tr>
<td>Usability</td>
<td>The system shall be usable in various ways including: user friendly interface, help and navigation links ease to use with minimal training.</td>
</tr>
<tr>
<td>Friendliness</td>
<td>The system shall be very friendly with a very attractive user interface.</td>
</tr>
<tr>
<td>Scalability</td>
<td>The system shall be developed in such a way to allow expansion in the future to handle more users and functionality.</td>
</tr>
</tbody>
</table>

### 4.2. System Analysis

#### 4.2.1. Android Architecture

Figure below describes the current Android Architecture. The Linux kernel operates as the hardware abstraction layer (HAL) and provides device driver, memory management, process management, as well as networking functionalities. The library layer is interfaced through Java. This is the layer in which the Android specific libc (Bionic) is located. The surface manager handles the user interface windows. The Android runtime layer holds the Dalvik Virtual Machine (DVM) and the core libraries (such as Java or IO). Most of the functionalities available in Android are provided via the core libraries (Shibly, 2016).
Android operating system is one of the most widely used mobile Operating System these days (Android, 2012). Android mobile operating system is based on the Linux kernel and is developed by Google. Some of the key features of Android operating system are: Application Framework, Dalvik virtual machine, Integrated browser, Optimized Graphics, SQLite, Media Support, GSM Technology, Bluetooth, Edge, 3G, Wi-Fi, Camera and GPS (Android, 2012). To help the developers for better software development Android provides Android Software development kit (SDK). It provides Java programming Language for application development (Android, 2012). The Android software development kit includes a debugger, libraries, a handset emulator based on QEMU (Quick Emulator), documentation, sample code, and tutorials (wikipedia, 2018).

Main components of Android Operating system Architecture or Software Stack are Linux. kernel, native libraries, Android Runtime, Application Framework and Applications.
a) **Linux Kernel**

Linux Kernel (Linux 2.6) is at the bottom layer of the software stack. Whole Android Operating System is built on this layer with some changes made by the Google. Like main Operating System it provides the following functionalities: Process management, Memory Management, device management (ex. camera, keypad, display). Android operating system interacts with the hardware of the device with this layer (Tutorialspoint, 2018). This layer also contains many important hardware device drivers. Linux kernel is also responsible for managing virtual memory, networking, drivers, and power management.

b) **Native Libraries Layer**

On the top of the Linux Kernel layer is Android's native libraries. This layer enables the device to handle different types of data. Data is specific to hardware. All these libraries are written in c or c++ language. These libraries are called through java interface. Some important native libraries are: Surface Manager: it is used to manage display of device. Surface Manager used for composing windows on the screen. SQLite: SQLite is the database used in android for data storage. It is relational database and available to all applications. WebKit: It is the browser engine used to display HTML content. Media framework: Media framework provides playbacks and recording of various audio, video and picture formats (for example MP3, AAC, AMR, JPG, MPEG4, H.264, and PNG). Free Type: Bitmap and Font Rendering. OpenGL | ES: Used to render 2D or 3D graphics content to the screen. libc: It contains System related C libraries [5].

c) **Android Runtime**

Prior to Android version 5.0 (API level 21), Dalvik was the Android runtime (Developers, 2018). Android Runtime consists of Dalvik Virtual machine and Core Java libraries. It is located on the same level as the library layer (Singh, 2014)[5]. Dalvik Virtual Machine is a type of Java Virtual Machine used for running applications on Android device. The Dalvik VM enables every Android application to run in its own process, with its own instance of the Dalvik virtual machine. The Dalvik VM allows multiple instance of Virtual machine to be created simultaneously providing security, isolation, memory management and threading support [8]. Unlike Java VM which is process-based, Dalvik Virtual Machine is registerbase. Dalvik Virtual Machine run .dex files which are created from .class file by dx tool. Dx tool is included in Android SDK. DVM is optimized for
low processing power and low memory environments. DVM is developed by Dan Bornstein from Google (Singh, 2014).

d) Application Framework

The Application Framework layer provides many higher-level services or major APIs to applications in the form of Java classes. Application developers are allowed to create Android apps by simplifying the reuse of core, modular system components and services (Developers, 2018). These are the blocks with which developer's applications directly interact. Important blocks of Application framework are:

- View System It is used to build an app’s UI, including lists, grids, text boxes, buttons, and even an embeddable web browser.
- Resource Manager provides access to non-code resources such as localized strings, graphics, and layout files.
- Notification Manager enables all apps to display custom alerts in the status bar.
- Activity Manager manages the lifecycle of apps and provides a common navigation back stack.
- Content Providers enable apps to access data from other apps to share their own data (Developers, 2018).
- Telephony Manager: it manages all voice call related functionalities.
- Location Manager: It is used for Location management, using GPS or cell tower.
- Resource Manager: Manage the various types of resources used in Application (Singh, 2014).

e) Application Layer

The Applications Layer is the top layer in the Android architecture. Some applications come preinstalled with every device, such as: SMS client app, Dialler, Web browser and Contact manager. A developer can write his own application and can replace it with the existing application (Singh, 2014).

Android applications are bundled into an Android package (.apk) via the Android Asset Packaging Tool (AAPT). To streamline the development process, Google provides the Android Development Tools (ADT). The ADT streamlines the conversion from class to dex files, and creates the .apk during deployment. In a very simplified manner, Android applications are in general composed of:

- Activities (needed to create a screen for a user application – classes with a UI).
- Intents it is used to transfer control from one activity to another.
- Services these are classes without a UI, so they can be executed in the background.
- Content Providers allows the application to share information with other applications (Shibly, 2016).
4.2.2 Voice Biometrics Technology

a. First, Get Audio

Voice Biometric systems analyse voice recordings; therefore, the first step in implementation is knowing how you will get voice samples of the person for whom you are creating a voiceprint. You need a way to capture audio of the person you want to authenticate and/or identify such that you have only that voice and not a mix of that voice and other voices or sounds. For the purpose of this research the audio captured through a microphone and record in a format suitable for the voice biometric engine.

b. Enrollment

This is the process of determining what you will be asking the person of interest to do in order to capture that person’s voice and send to the Voice Biometric engine in order to make a voiceprint. The figure 4-7 below shows the enrolment process.

![Voice Biometrics Enrollment Diagram](source)

Figure 4-7: Voice Biometrics Enrollment

Source: (East, 2012)

Once enrolled, you can then authenticate the user by capturing a new voice sample that is compared against the voiceprint from enrollment. A comparison can be done of that new sample against all other voiceprints in the database to determine the identity of the speaker.

Different categories of enrollment include:

i. Passive Method

A passive enrollment means that the person speaking does not have to take any action specific to enrolling. The audio is captured from a person’s conversation. One benefit of this passive approach is that you do not need to train the speaker or ask her to do anything extra in order to enroll her voiceprint.
The downside of this approach is that you are relying on whatever the speaker happens to be saying as the audio data for the voiceprint. Not controlling the content of what is spoken creates inefficiencies. The first inefficiency relates to the fact that creating a viable voiceprint requires sampling enough unique spoken sounds from a person, what we call “phonetic diversity.”

A second inefficiency comes from managing audio files. This can be a complex programming task that links multiple systems together to keep track of people and their matching audio and the part of the audio used for enrollment. The impacts are higher cost and longer time to implement.

ii. Active Method

The active method requires knowing participation of the person whose voice you are capturing. The downside of requiring participation is that the speaking party has to follow instructions and behave in an expected manner. Furthermore, active participation requires the speaker to devote time to the process, especially for enrollment.

The active use case has distinct advantages. First, because the nature of what is spoken is known in advance, the voice biometric engine can be more efficient. It turns out that speaking numbers presents distinct advantages for a voice biometric system because it is easy to validate the content in many languages, the amount of speech is relatively short, and numbers are easy for people to remember.

A second advantage of the active use case is awareness. By simply having the threat of a voice biometric system, the rate of fraud decreases. Some people will of course try to crack the voice biometric, but our customers tell us that the overall attempts at cheating decline significantly.

A third advantage is operational simplicity. In a passive system discussed earlier, where the person can speak anything, acquiring enough audio and managing audio data adds complexity. With an active use case, on the other hand, the speech samples are immediate and short and require no separate storage or management.

Active Method Options

- Static Passphrase (Text):

The user speaks the same thing (“static”); that is a phrase of text. The person speaks this phrase three times or so to enroll and one time to verify. This is simple and easy.
A weakness of this approach is the ease at which a third party could record the person speaking and then use the recording to authenticate. This is a genuine concern with the quality of recording devices and a determined fraudster.

- **Static Passphrase (Number):**
  This means speaking the same number each time. Numbers tend to be easier to remember and in many cases a person already has at least one long digit string memorized. You require the person to speak the number string three times for enrollment and one time for verification.

Like Static Text, this type of voiceprint is more vulnerable to recording by a fraudster, so its recommendation is to combine its use with other techniques -- such as outbound telephone calls to a trusted phone number.

- **RandomPIN™:**
  To thwart a fraudster who tries to make a recording of a person’s voice, you can require the person to speak a random number rather than a fixed phrase.

With the RandomPIN™ use case, a person is required to speak a set of six digit strings that has been crafted for phonetic diversity, each five numbers long, for enrollment. To verify, you ask for a single five-digit string that is different every time. You could use a four-digit string, which is easier for people to remember when speaking back. And to make the system more secure with a four-digit string, you can ask for a four-digit random string two times, thus collecting eight digits, a good approach if the user is an infrequent user but the security level needs to be high.

- **Languages supported**
  Voice Biometrics technology uses the way people make sounds as a way to reveal unique characteristics. Because the voice biometric engine measures how rather than what you are speaking, it does not care about language. However, to tune the voice biometric engine to get the best results means taking into account that different languages use different sounds.
4.2.3 Voice Biometric API
The Voice Biometrics Group uses the VMM-2 voice biometric engine. The VMM-2 provides a comprehensive set of features: voice enrollment, voice verification, 1: N identification and classification (gender), with multiple feature sets, multiple algorithms. In addition to this VMM-2’s Algorithm Fusion technology optimizes and combines algorithms for each use case and then wraps the engine technology within service oriented architecture (Group, 2018). The figure 4-8 below demonstrates the high level architecture of the voice biometrics API. It comprises of a telephone network, internet connection, load balancer, APIs, and databases.

Figure 4-8: High Level Platform Architecture
Source: Voice Biometrics Group (Group, 2018)
4.2.4 Voice Biometrics Configuration
This section describes how the voice biometrics is configured and the various processes involved. The figure 4-9 below demonstrates how the application triggers the Voice Biometrics API. The user of the application accesses the application within the IT environment.

Figure 4-9: Trigger Event Occurs
Source: Voice Biometrics Group (Group, 2018)

Figure 4-10 below shows the next step where the user authentication system notifies the Voice Biometric Application.

Figure 4-10: User Authentication System Notified the Voice Biometric Application
Source: Voice Biometrics Group (Group, 2018)
The next step as shown in figure 4-11 below involves the Voice Biometric Application making a request to VBG Voice Biometrics Platform to perform an authentication, sending over userid, phone number, call type and type parameters. The VMPESA application sends the required parameters with the audio sample to the VBG Voice Biometric Platform to perform authentication.

Figure 4-11: Voice Biometric Application Makes Secure REST Requests to the VBG Voice Biometric Platform

Source: Voice Biometrics Group (Group, 2018)
Figure 4-12 below describes how a Voice Biometrics Application queries a VBG Voice Biometric Platform to find out which prompt should be shown on the user’s screen and then displays on the screen. The VMPESA application queries the Voice Biometric Platform to find out what prompt should be shown to the user’s mobile phone. This prompt is what the subscriber is expected to read out aloud.

Figure 4-12: The Voice Biometric Application Queries the Voice Biometric Platform to Find out What Prompt Should is shown to the User
Source: Voice Biometrics Group (Group, 2018)

Figure 4-13 below shows how the VBG IVR Application Server makes a request to VBG VoIP IVR to start a call. This applies to the VBG IVR system implementation.

Figure 4-13: The Voice Biometric Application Queries the Voice Biometric Platform to Find Out What Prompt Should Be Shown to the User
Source: Voice Biometrics Group (Group, 2018)
Figure 4-14 below demonstrates how an IVR makes a call from the cloud. Assumptions made are; The Voice Biometric Application has already called the VBG REST API to create a userid for each person in the system; each user has already enrolled in the Voice Biometric System.

![Diagram](image1)

Figure 4-14: IVR Makes Call from Cloud
Source: Voice Biometrics Group (Group, 2018)

The figure 4-15 below shows that the Voice Biometric Application polls the Voice Biometric Platform for status using transactions read GET request, changing the prompt on the screen if retry was necessary. Assumptions made are; The Voice Biometric Application has already called the VBG REST API to create a userid for each person in the system; each user has already enrolled in the Voice Biometric System.

![Diagram](image2)

Figure 4-15: The Voice Biometric Application Queries the Voice Biometric Platform for Status When Necessary
Source: Voice Biometrics Group (Group, 2018)
Figure 4-16 below shows the user responds to the prompt and completes the verification process using standard interaction with up to two retries. Assumptions made are: The Voice Biometric Application has already called the VBG REST API to create a userid for each person in the system; each user has already enrolled in the Voice Biometric System.

Figure 4-16: User Responds to Prompts and Completes the Verification Process  
Source: Voice Biometrics Group (Group, 2018)

Figure 4-17 below demonstrates that the Voice Biometric Application pooling gets the final result and signals pass or fail to the User Authentication System. Assumptions made are: The Voice Biometric Application has already called the VBG REST API to create a userid for each person in the system; each user has already enrolled in the Voice Biometric System.

Figure 4-17: The Voice Biometric Application Polls and Gets Final Result and Signals Pass/Fail to the User Authentication System  
Source: Voice Biometrics Group (Group, 2018)
Figure 4-18 below clearly shows the overall process of a text-dependent voice biometric engine that performs verification on the user pass phrase.

![Text-dependent Biometric Engine](Source: NAUNCE (Naunce, 2017))

### 4.3 Modeling and Design

#### 4.3.1 VMPESA - Level 0 DFD

![VMPESA - Level 0 DFD](Figure 4-19: VMPESA - Level 0 DFD)
The figure 4-19 above demonstrates the context diagram of the VMPESA Application. According to Alexander & Sweet (2011), a context diagram is a representation of the external entities interacting with an application system. This diagram shows a system inputs and outputs regarding its external factors. In the above context diagram, all the VMPESA application allows registered subscribers to access the system by using their mobile number. The system can accept or reject their login process depending with their respective input credentials. Subscribers can perform transactions i.e. withdrawals, send money and check balance on the VMPESA application. VMPESA agents can register new subscribers, perform deposits and manage existing registered subscriber accounts.

4.3.2 VMPESA - Level 1 DFD

![Figure 4-20: VMPESA - Level 1 DFD](image-url)
The Figure 4-20 above demonstrates the VMPESA Application Level 1 DFD diagram. According to Sommerville (2009), the main use of Data-Flow Diagrams (DFD) is to demonstrate the flow of data through the various process steps in an application. The figure 15 above demonstrates how data flows in the VMPESA application, among the various processes as illustrated.

4.3.3 VMPESA Use Case Diagram

![Use Case Diagram (Subscriber)](image1.png)

Figure 4-21: VM-PESA – Use Case Diagrams (Subscriber)

![Use Case Diagram (Agent)](image2.png)

Figure 4-21: VM-PESA – Use Case Diagram (Agent)
### 4.3.3.1 VMPESA Use Case Narration

#### I. Login Narration

**Table 4-6: Login Narration**

<table>
<thead>
<tr>
<th>Use Case Name</th>
<th>VMPESA Access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
<td>This use case describes the processes taken by registered subscribers to access the VMPESA mobile application.</td>
</tr>
<tr>
<td><strong>Actors</strong></td>
<td>a) VMPESA subscriber</td>
</tr>
<tr>
<td><strong>Pre-Condition</strong></td>
<td>Users must be registered to the application.</td>
</tr>
<tr>
<td></td>
<td>User must have the application installed on their phone</td>
</tr>
<tr>
<td><strong>Post-Condition</strong></td>
<td>An actor has access to the system if the use case is carried out successfully.</td>
</tr>
<tr>
<td></td>
<td>The state of the system remains unchanged in case the use case was not carried out successfully.</td>
</tr>
<tr>
<td><strong>Basic Flow</strong></td>
<td>The use case begins when an actor wishes to access the VMPESA Application system.</td>
</tr>
<tr>
<td></td>
<td>a) The actor is prompted to enter their respective logon credentials (their cell phone number).</td>
</tr>
<tr>
<td></td>
<td>b) The actor responds by entering their respective logon credentials.</td>
</tr>
<tr>
<td></td>
<td>c) VMPESA application authenticates the user’s credentials against the Users datastore.</td>
</tr>
<tr>
<td></td>
<td>d) Authentic credentials allow a user to be logged on to the system.</td>
</tr>
<tr>
<td><strong>Alternate Flow</strong></td>
<td>Invalid/Unauthentic User logon credentials:</td>
</tr>
<tr>
<td></td>
<td>a) An error message is displayed warning the user of wrong logon credentials that they might have provided.</td>
</tr>
<tr>
<td></td>
<td>b) An actor can decide to logon to the system again or cancel the entire process.</td>
</tr>
<tr>
<td></td>
<td>c) The use case then ends.</td>
</tr>
</tbody>
</table>
| **Empty input fields Error:** | a) An error message is displayed in the case where a
### II. Withdraw Narration

**Table 4-7: Withdraw Narration**

<table>
<thead>
<tr>
<th><strong>Use Case Name</strong></th>
<th><strong>Withdrawal on VMPESA</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
<td>This use case describes the processes taken by registered subscribers to withdraw money the VMPESA mobile application.</td>
</tr>
<tr>
<td><strong>Actors</strong></td>
<td>b) VMPESA subscriber</td>
</tr>
<tr>
<td><strong>Pre-Condition</strong></td>
<td>Users must be registered to the application.</td>
</tr>
<tr>
<td></td>
<td>User must have the application installed on their phone</td>
</tr>
<tr>
<td><strong>Post-Condition</strong></td>
<td>An actor is able to withdraw money from the system if the use case is carried out successfully.</td>
</tr>
<tr>
<td></td>
<td>A successful transaction message is sent to the actor.</td>
</tr>
<tr>
<td></td>
<td>The state of the system remains unchanged in case the use case was not carried out successfully.</td>
</tr>
<tr>
<td><strong>Basic Flow</strong></td>
<td>The use case begins when an actor wishes to access the VMPESA Application system.</td>
</tr>
<tr>
<td></td>
<td>e) The actor is prompted to enter their respective logon credentials (their cell phone number).</td>
</tr>
<tr>
<td></td>
<td>f) VMPESA application authenticates the user’s credentials against the Users datastore.</td>
</tr>
<tr>
<td></td>
<td>g) Authentic credentials allow a user to access the system.</td>
</tr>
<tr>
<td></td>
<td>h) The system displays the withdrawal option to the subscriber</td>
</tr>
<tr>
<td></td>
<td>i) Once the withdrawal option is selected, the subscriber is required to enter the agent number</td>
</tr>
<tr>
<td></td>
<td>j) The user then enters the amount</td>
</tr>
<tr>
<td></td>
<td>k) The user then enters PIN</td>
</tr>
</tbody>
</table>
l) The user is then prompted to readout a displayed text.

**Alternate Flow**

**Insufficient funds:**

d) An error message is displayed informing the user of lack of funds

**Incorrect PIN or inaccurate voice print**

a) An error message is displayed informing the user of incorrect PIN or voice sample

b) The use case then ends.

**Empty input fields Error:**

b) An error message is displayed in the case where a user failed to fill in the input fields.

**Special Requirements**

An actor should contact VMPESA agent to be registered.

An actor should have a voice sample submitted during registration.

**Use Case Relationship**

None

### III. Check Balance Narration

Table 4-8: Check Balance Narration

<table>
<thead>
<tr>
<th>Use Case Name</th>
<th>Check Balance on VMPESA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
<td>This use case describes the processes taken by registered subscribers to check their account balance using the VMPESA mobile application.</td>
</tr>
<tr>
<td><strong>Actors</strong></td>
<td>c) VMPESA subscriber</td>
</tr>
<tr>
<td><strong>Pre-Condition</strong></td>
<td>Users must be registered to the application. User must have the application installed on their phone</td>
</tr>
<tr>
<td><strong>Post-Condition</strong></td>
<td>An actor is able to get account balance from the system if the use case is carried out successfully. A successful balance message is displayed to the actor. The state of the system remains unchanged in case the use case was not carried out successfully.</td>
</tr>
<tr>
<td><strong>Basic Flow</strong></td>
<td>The use case begins when an actor wishes to access the</td>
</tr>
</tbody>
</table>
VMPESA Application system.

m) The actor is prompted to enter their respective logon credentials (their cell phone number).

n) VMPESA application authenticates the user’s credentials against the Users datastore.

o) Authentic credentials allow a user to access the system.

p) The system displays the balance option to the subscriber

q) Once the balance option is selected, the subscriber is required to enter the PIN number

r) The user is then prompted to readout a displayed text.

Alternate Flow

Incorrect PIN or inaccurate voice print

c) An error message is displayed informing the user of incorrect PIN or voice sample

d) The use case then ends.

Empty input fields Error:

c) An error message is displayed in the case where a user failed to fill in the input fields.

Special Requirements

An actor should contact VMPESA agent to be registered.

An actor should have a voice sample submitted during registration.

Use Case Relationship

None

IV. Send Money Narration

Table 4-9: Send Money Narration

<table>
<thead>
<tr>
<th>Use Case Name</th>
<th>Send Money on VMPESA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>This use case describes the processes taken by registered subscribers to send money the VMPESA mobile application.</td>
</tr>
<tr>
<td>Actors</td>
<td>d) VMPESA subscriber</td>
</tr>
<tr>
<td>Pre-Condition</td>
<td>Users must be registered to the application.</td>
</tr>
</tbody>
</table>

65
<table>
<thead>
<tr>
<th><strong>User must have the application installed on their phone</strong></th>
</tr>
</thead>
</table>

**Post-Condition**
- An actor is able to send money from the system if the use case is carried out successfully.
- A successful transaction message is sent to the actor.
- The state of the system remains unchanged in case the use case was not carried out successfully.

**Basic Flow**
- The use case begins when an actor wishes to access the VMPESA Application system.
  - s) The actor is prompted to enter their respective logon credentials (their cell phone number).
  - t) VMPESA application authenticates the user’s credentials against the Users datastore.
  - u) Authentic credentials allow a user to access the system.
  - v) The system displays the send money option to the subscriber
  - w) The subscriber is required to enter the receiver’s phone number
  - x) The user then enters the amount
  - y) The user then enters PIN
  - z) The user is then prompted to readout a displayed text.

**Alternate Flow**

**Insufficient funds:**
- e) An error message is displayed informing the user of lack of funds

**Incorrect PIN or inaccurate voice print**
- e) An error message is displayed informing the user of incorrect PIN or voice sample
- f) The use case then ends.

**Empty input fields Error:**
- d) An error message is displayed in the case where a user failed to fill in the input fields.
Special Requirements

|        | An actor should contact VMPESA agent to be registered. An actor should have a voice sample submitted during registration. |

Use Case Relationship

|        | None |

V. Registration Narration

a. Personal Details Registration

Table 4-10: Registration Narration

<table>
<thead>
<tr>
<th>Use Case Name</th>
<th>Personal Details Registration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>This use case enables an actor to register a subscriber personal details</td>
</tr>
<tr>
<td>Actors</td>
<td>a) VMPESA agent</td>
</tr>
<tr>
<td></td>
<td>b) VMPESA subscriber</td>
</tr>
<tr>
<td>Pre-Condition</td>
<td>User must have the application installed on their phone. User must be an agent</td>
</tr>
<tr>
<td>Post-Condition</td>
<td>VMPESA subscriber personal details are successfully captured. The state of the system remains unchanged in case the use case was not carried out successfully</td>
</tr>
</tbody>
</table>
| Basic Flow    | This use case begins when an actor wishes to register a subscriber’s personal details.  
1) The system requests an actor to specify the action they wish to carry out.  
2) One of the sub flows executes upon been chosen by the actor.  
   • If he/she clicks on registration, the sub-flow executes.  
   a) Register Subscriber  
   • The system requests the actor, in this case an agent, to enter the subscriber’s details.  
   • Upon provision of these details, a subscriber is added on to the system. |
Upon confirmation, the subscriber added to the system.

Alternate Flow

*Subscriber was not found Subscriber already registered*

- An error message is displayed in case the subscriber is already registered
- The actor cancels the operation ending this use case.

*Cancelled/Failed Update*

- In case the actor cancels the registration, the process terminates, and the basic flow started from the beginning.
- If case the system displays a registration failed error message, the process is terminated, and basic flow started from the beginning.

<table>
<thead>
<tr>
<th>Special Requirements</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Use Case Relationship</em></td>
<td>None</td>
</tr>
</tbody>
</table>

**b. Voice Registration Narration**

**Table 4-11: Voice Registration Narration**

<table>
<thead>
<tr>
<th>Use Case Name</th>
<th>Voice Registration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
<td>This use case enables an actor to register a subscriber voice sample</td>
</tr>
</tbody>
</table>
| **Actors** | c) VMPESA agent  
d) VMPESA subscriber |
| **Pre-Condition** | User must have the application installed on their phone.  
User must be an agent |
| **Post-Condition** | VMPESA subscriber voice samples are successfully submitted.  
The state of the system remains unchanged in case the use case was not carried out successfully. |
| **Basic Flow** | This use case begins when an actor wishes to register a subscriber’s voice samples.  
3) The system requests an actor to specify the action |
they wish to carry out.

4) One of the sub-flows executes upon being chosen by the actor.
   - If he/she clicks on registration, the sub-flow executes.

b) **Subscriber’s Voice Sample Submission**
   - The system requests the actor, in this case an agent, to enter the subscriber’s details.
   - Upon provision of these details, a subscriber is added on to the system.
   - Upon confirmation of successful personal details registration, the subscriber is then prompted to submit three voice samples.

<table>
<thead>
<tr>
<th>Alternate Flow</th>
<th>Inaccurate voice sample</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• An error message is displayed in case the subscribe voice sample does not meet the required standards.</td>
</tr>
<tr>
<td></td>
<td>• The actor cancels the operation ending this use case.</td>
</tr>
</tbody>
</table>

**Cancelled/Failed Update**

- In case the actor cancels the voice submission step, the process terminates, and the basic flow started from the beginning.
- If case the system displays a failed error message, the process is terminated, and basic flow started from the beginning.

### Special Requirements

None

### Use Case Relationship

None

### VI. Manage Subscriber Details Narration

**Table 4-12: Manage Subscriber Details Narration**

<table>
<thead>
<tr>
<th>Use Case Name</th>
<th>Manage Subscriber Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
<td>This use case enables an actor to manage subscriber details. The actions involved include add, update, delete a</td>
</tr>
<tr>
<td>Actors</td>
<td>e) VMPESA agent</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Pre-Condition</td>
<td>An actor must be logged on to the system before this use case is carried out.</td>
</tr>
<tr>
<td>Post-Condition</td>
<td>Subscriber details are updated or deleted if the use case was carried out successfully. The state of the system remains unchanged in case the use case was not carried out successfully.</td>
</tr>
<tr>
<td>Basic Flow</td>
<td>This use case begins when an actor wishes to update or delete a patient’s details.</td>
</tr>
<tr>
<td></td>
<td>5) The system requests an actor to specify the action they wish to carry out.</td>
</tr>
<tr>
<td></td>
<td>6) One of the sub flows executes upon been chosen by the actor.</td>
</tr>
<tr>
<td></td>
<td>• If he/she clicks on update a subscriber button, the sub flow executes.</td>
</tr>
<tr>
<td></td>
<td>• If he/she clicks on delete a subscriber button, the sub flow executes.</td>
</tr>
<tr>
<td></td>
<td>c) Update subscriber</td>
</tr>
<tr>
<td></td>
<td>• The system requests an actor to enter the phone number of the specific subscriber they wish to update.</td>
</tr>
<tr>
<td></td>
<td>• The system retrieves the respective subscriber’s details.</td>
</tr>
<tr>
<td></td>
<td>• An actor makes the desired changes in the various input fields they choose.</td>
</tr>
<tr>
<td></td>
<td>• Once the actor is done, the subscriber’s details are successfully updated.</td>
</tr>
<tr>
<td></td>
<td>d) Delete subscriber</td>
</tr>
<tr>
<td></td>
<td>• The system requests the actor to enter the phone number of the specific subscriber wish to delete.</td>
</tr>
</tbody>
</table>
The system fetches the selected subscriber’s details.
- The system displays an alert message for the actor to confirm the chosen action.
- Upon confirmation, the subscriber is deleted from the system.

Alternate Flow

Subscriber was not found
- An error message is displayed in case the subscriber was not found in the system in any one of the sub flows.
- The actor cancels the operation ending this use case.

Cancelled/Failed Update
- In case the actor cancels the update subscriber sub flow, the process terminates, and the basic flow started from the beginning.
- If case the system displays an update failed error message, the process is terminated, and basic flow started from the beginning.

Cancelled Delete
If in the delete subscriber sub flow the actor decides to cancel the process, it’s then terminated, and the basic flow started from the beginning.

Special Requirements
None

Use Case
The database must be queried.

VII. Deposit Narration

Table 4-13: Deposit Narration

<table>
<thead>
<tr>
<th>Use Case Name</th>
<th>Deposit Money On VMPESA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>This use case describes the processes taken by agents to deposit money to registered subscribers on the</td>
</tr>
</tbody>
</table>
**VMPESA mobile application.**

<table>
<thead>
<tr>
<th><strong>Actors</strong></th>
<th>e) VMPESA agent</th>
</tr>
</thead>
</table>

| **Pre-Condition** | User must have the application installed on their phone.  
User must be an agent |
|-------------------|---------------------------------------------------------------|

| **Post-Condition** | An actor is able to deposit money to a registered subscriber if the use case is carried out successfully.  
A successful transaction message is sent to the actor.  
The state of the system remains unchanged in case the use case was not carried out successfully. |
|--------------------|-----------------------------------------------------------------|

| **Basic Flow** | The use case begins when an actor wishes to access the VMPESA Application system.  
   aa) The system displays the deposit money option to the subscriber  
   bb) Once the deposit money option is selected, the agent is required to enter the registered subscriber’s phone number  
   cc) The user then enters the amount  
   dd) The user then enters PIN  
   ee) The user is then prompted to readout a displayed text. |
|-----------------|-----------------------------------------------------------------|

| **Alternate Flow** | **Insufficient funds:**  
f) An error message is displayed informing the user of lack of funds  
**Incorrect PIN or inaccurate voice print**  
g) An error message is displayed informing the user of incorrect PIN or voice sample  
h) The use case then ends.  
**Empty input fields Error:**  
e) An error message is displayed in the case where a user failed to fill in the input fields. |
|-------------------|-----------------------------------------------------------------|

| **Special Requirements** | An actor should contact VMPESA agent to be |
An actor should have a voice sample submitted during registration.

### Use Case Relationship

| Use Case Relationship | None |

#### 4.3.3.2 Sequence Diagrams

**a) Subscriber Login Sequence Diagram**

![Subscriber Login Sequence Diagram](image)

Figure 4-22: Subscriber Login Sequence Diagram
b) Subscriber Transaction Sequence Diagram

![Subscriber Transaction Sequence Diagram](image)

Figure 4-23: Subscriber Transaction Sequence Diagram

4.3.3.3 Activity Diagrams

a) Login Activity Diagram

![Login Activity Diagram](image)

Figure 4-24: Subscriber Login Activity Diagram
4.3.3.4 Conceptual Design

The diagram below displays an ERD of the VMPESA Application.

Figure 4-25: VMPESA ERD
4.3.3.5 Logical Design (Relational Database Schema)

### Users Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int(11)</td>
</tr>
<tr>
<td>unique_id</td>
<td>varchar(23)</td>
</tr>
<tr>
<td>fname</td>
<td>varchar(50)</td>
</tr>
<tr>
<td>lname</td>
<td>varchar(50)</td>
</tr>
<tr>
<td>dob</td>
<td>date</td>
</tr>
<tr>
<td>idnumber</td>
<td>varchar(8)</td>
</tr>
<tr>
<td>cellnumber</td>
<td>varchar(14)</td>
</tr>
<tr>
<td>email</td>
<td>varchar(100)</td>
</tr>
<tr>
<td>amount</td>
<td>int(11)</td>
</tr>
<tr>
<td>status</td>
<td>tinyint(1)</td>
</tr>
<tr>
<td>encrypted_password</td>
<td>varchar(80)</td>
</tr>
<tr>
<td>salt</td>
<td>varchar(10)</td>
</tr>
<tr>
<td>created_at</td>
<td>datetime</td>
</tr>
<tr>
<td>updated_at</td>
<td>datetime</td>
</tr>
</tbody>
</table>

### Template Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int(11)</td>
</tr>
<tr>
<td>responsecode</td>
<td>int(11)</td>
</tr>
<tr>
<td>success</td>
<td>varchar(128)</td>
</tr>
<tr>
<td>transactionid</td>
<td>int(11)</td>
</tr>
<tr>
<td>created_at</td>
<td>datetime</td>
</tr>
<tr>
<td>updated_at</td>
<td>datetime</td>
</tr>
</tbody>
</table>

### Sample Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int(11)</td>
</tr>
<tr>
<td>responsecode</td>
<td>int(11)</td>
</tr>
<tr>
<td>nextdisplayprompt</td>
<td>varchar(128)</td>
</tr>
<tr>
<td>nextprompt</td>
<td>varchar(128)</td>
</tr>
<tr>
<td>probability</td>
<td>int(11)</td>
</tr>
<tr>
<td>recognizedprompt</td>
<td>varchar(128)</td>
</tr>
<tr>
<td>score</td>
<td>int(11)</td>
</tr>
<tr>
<td>success</td>
<td>varchar(128)</td>
</tr>
<tr>
<td>transactionid</td>
<td>int(11)</td>
</tr>
<tr>
<td>usabletime</td>
<td>double</td>
</tr>
<tr>
<td>created_at</td>
<td>datetime</td>
</tr>
<tr>
<td>updated_at</td>
<td>datetime</td>
</tr>
</tbody>
</table>

### Credit Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int(11)</td>
</tr>
<tr>
<td>amount</td>
<td>int(11)</td>
</tr>
<tr>
<td>cellnumber</td>
<td>varchar(14)</td>
</tr>
<tr>
<td>balance</td>
<td>int(128)</td>
</tr>
<tr>
<td>created_at</td>
<td>datetime</td>
</tr>
<tr>
<td>updated_at</td>
<td>datetime</td>
</tr>
</tbody>
</table>
Debits Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int(11)</td>
</tr>
<tr>
<td>amount</td>
<td>int(11)</td>
</tr>
<tr>
<td>cellnumber</td>
<td>varchar(14)</td>
</tr>
<tr>
<td>balance</td>
<td>int(11)</td>
</tr>
<tr>
<td>created_at</td>
<td>datetime</td>
</tr>
<tr>
<td>updated_at</td>
<td>timestamp</td>
</tr>
</tbody>
</table>

Account Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int(11)</td>
</tr>
<tr>
<td>type</td>
<td>varchar(64)</td>
</tr>
<tr>
<td>balance</td>
<td>int(25)</td>
</tr>
<tr>
<td>userid</td>
<td>int(11)</td>
</tr>
</tbody>
</table>

Statement Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int(11)</td>
</tr>
<tr>
<td>amount</td>
<td>int(11)</td>
</tr>
<tr>
<td>balance</td>
<td>int(11)</td>
</tr>
<tr>
<td>date</td>
<td>datetime</td>
</tr>
<tr>
<td>status</td>
<td>varchar(64)</td>
</tr>
</tbody>
</table>

4.4 Proof of Concept

Figure 4-26: Landing Page

Figure 4-27: Agent Transaction Page
Figure 4-28: Registered Subscriber Enter Phone Number Page

Figure 4-29: Subscriber Registration Page

Figure 4-30: Subscriber Registration Page

Figure 4-31: Voice Verification Page
Figure 4-32: Voice Enrollment Page

Figure 4-33: Enter Amount Page

Figure 4-34: Enter PIN Page
### 4.4.1 System Testing

**a) Registration Test Case**

<table>
<thead>
<tr>
<th>Test Case ID: 1</th>
<th>Test Designed by: Lucy Cleatham</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Case Priority: High</td>
<td>Test Design Date: 08.01.2018</td>
</tr>
<tr>
<td>Test Module: Subscriber Registration</td>
<td>Test Execution Date: 09.01.2018</td>
</tr>
<tr>
<td>Test Title: Subscriber Registration Test</td>
<td>Test Executed by: Lucy Cleatham</td>
</tr>
<tr>
<td>Test Description: Test the subscriber registration page</td>
<td>Dependencies: None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test Steps</th>
<th>Test Data</th>
<th>Expected Result</th>
<th>Actual Result</th>
<th>Status (Pass/Fail)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Navigate to Deposit &amp; Registration Page</td>
<td>User should be able to Navigate to Deposit &amp; Registration Page</td>
<td>User is able to Navigate to Deposit &amp; Registration Page</td>
<td>Pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Access the Registration Page</td>
<td>User should be able to Access the Registration Page</td>
<td>User is able to Access the Registration Page</td>
<td>pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Provide a First Name John</td>
<td>User should be able to add John as First name</td>
<td>User is able to add John as First name</td>
<td>Pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Provide a Last Name Doe</td>
<td>User should be able to add Doe as last name</td>
<td>User is able to add Doe as last name</td>
<td>pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Provide a Date of Birth 12-12-1988</td>
<td>User should be able to add date of birth</td>
<td>User is able to add date of birth</td>
<td>pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Provide an ID number 23423456</td>
<td>User should be able to add ID</td>
<td>User is able to add ID</td>
<td>Pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Provide a Safaricom Number 0720123456</td>
<td>User should be able to add Safaricom number</td>
<td>User is able to add Safaricom number</td>
<td>pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Provide a Valid email address <a href="mailto:john@gmail.com">john@gmail.com</a></td>
<td>User should be able to provide a valid email address</td>
<td>User is able to provide a valid email address</td>
<td>pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Click on the Register Voice Button</td>
<td>User should be able to click on Register Voice Button</td>
<td>User is able to click on Register Voice Button</td>
<td>Pass</td>
<td>The voice registration page is displayed</td>
<td></td>
</tr>
</tbody>
</table>
### Voice Sample submission Test Case

<table>
<thead>
<tr>
<th>Test Case ID: 2</th>
<th>Test Designed by: Lucy Chetalam</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Case Priority: High</td>
<td>Test Design Date: 08.01.2018</td>
</tr>
<tr>
<td>Test Module: Voice Sample submission/Enrollment</td>
<td>Test Execution Date: 10.01.2018</td>
</tr>
<tr>
<td>Test Title: Voice Sample submission Test Case</td>
<td>Test Executed by: Lucy Chetalam</td>
</tr>
</tbody>
</table>

**Test Description:** Test the subscriber voice submission page

**Preconditions:** User must have the mobile application installed

**Dependencies:** None

<table>
<thead>
<tr>
<th>Test Steps</th>
<th>Test Data</th>
<th>Expected Result</th>
<th>Actual Result</th>
<th>Status (Pass/Fail)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Navigate to Voice Submission page</td>
<td>User should be able to Navigate to Voice Submission page</td>
<td>User is able to Navigate to Voice Submission page</td>
<td>Pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Click on Record button</td>
<td>User should be able to Click on Record button</td>
<td>User is able to Click on Record button</td>
<td>pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Click on Stop button</td>
<td>User should be able to Click on Stop button</td>
<td>User is able to Click on Stop button</td>
<td>Pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Submit three voice samples</td>
<td>User should be able to Submit three voice samples</td>
<td>User is able to Submit three voice samples</td>
<td>pass</td>
<td>User is automatically navigated to transaction page</td>
<td></td>
</tr>
</tbody>
</table>
## c) Withdrawal Test Case

<table>
<thead>
<tr>
<th>Test Steps</th>
<th>Test Data</th>
<th>Expected Result</th>
<th>Actual Result</th>
<th>Status (Pass/Fail)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Navigate to Transaction page</td>
<td>User should be able to Navigate to Transaction page</td>
<td>User is able to Navigate to Transaction page</td>
<td>Pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Click on Withdraw button</td>
<td>User should be able to Click on Withdraw button</td>
<td>User is able to Click on Withdraw button</td>
<td>pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Provide an Agent Number</td>
<td>User should be able to Provide an Agent Number</td>
<td>User is able to Provide an Agent Number</td>
<td>Pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Provide an Amount</td>
<td>400 12000</td>
<td>User should be able to Provide an Amount</td>
<td>User is able to Provide an Amount</td>
<td>pass</td>
<td>For 12000, insufficient funds message displayed</td>
</tr>
<tr>
<td>5. Provide PIN</td>
<td>1234 9876</td>
<td>User should be able to Provide PIN</td>
<td>User is able to Provide PIN</td>
<td>pass</td>
<td>For *9876 'invalid PIN' displayed</td>
</tr>
<tr>
<td>6. Click on Withdraw button</td>
<td>User should be able to Click on Withdraw button</td>
<td>User is able to Click on Withdraw button</td>
<td>pass</td>
<td>Confirmatio n Message displayed</td>
<td></td>
</tr>
<tr>
<td>7. Navigate to voice verification page</td>
<td>User should be able to Navigate to voice verification page</td>
<td>User is able to Navigate to voice verification page</td>
<td>Pass</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## d) Deposit Test Case

<table>
<thead>
<tr>
<th>Test Steps</th>
<th>Test Data</th>
<th>Expected Result</th>
<th>Actual Result</th>
<th>Status (Pass/Fail)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Navigate to Deposit &amp; Registration Page</td>
<td>User should be able to Navigate to Deposit &amp; Registration Page</td>
<td>User is able to Navigate to Deposit &amp; Registration Page</td>
<td>Pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Access the Deposit Page</td>
<td>User should be able to Access the Deposit Page</td>
<td>User is able to Access the Deposit Page</td>
<td>pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Provide a valid phone number</td>
<td>0720123456</td>
<td>User should be able to Provide a valid phone number</td>
<td>User is able to add John as First name Provide a valid phone number</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>4. Provide amount</td>
<td>200</td>
<td>User should be able to Provide amount</td>
<td>User is able to Provide amount</td>
<td>pass</td>
<td></td>
</tr>
<tr>
<td>5. Click on the ok Button</td>
<td>User should be able to click on ok Button</td>
<td>User is able to click on ok Button</td>
<td>Pass</td>
<td>Successful deposit message is displayed</td>
<td></td>
</tr>
</tbody>
</table>

Preconditions: User must have the mobile application installed.
### e) Voice validation test case

<table>
<thead>
<tr>
<th>Test Steps</th>
<th>Test Data</th>
<th>Expected Result</th>
<th>Actual Result</th>
<th>Status (Pass/ Fail)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to voice verification page</td>
<td>User should be able to Navigate to voice verification page</td>
<td>User is able to Navigate to voice verification page</td>
<td>Pass</td>
<td>Accessed after performing a transaction. Either send money, check balance or withdraw.</td>
</tr>
<tr>
<td>2.</td>
<td>View the displayed text</td>
<td>User should be able to View the displayed text</td>
<td>User is able to View the displayed text</td>
<td>pass</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Click on Record button</td>
<td>User should be able to Click on Record button</td>
<td>User is able to Click on Record button</td>
<td>pass</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Click on Submit button</td>
<td>User should be able to Click on Submit button</td>
<td>User is able to Click on Submit button</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>View verification result</td>
<td>User should be able to View verification result</td>
<td>User is able to View verification result</td>
<td>Pass</td>
<td>User is automatically navigated to Transaction Page</td>
</tr>
</tbody>
</table>
4.5 Chapter Summary

This chapter described the various processes that were involved in implementing the VMPESA application. The methodology adopted to design and develop the system was an incremental delivery process. This chapter also included the feasibility study approach adopted, the system configuration, and system services which covered both functional and non-functional requirements. The system analysis and design section covered the architecture of the VMPESA application, its context diagram, level 1 DFD diagram, and use case diagrams. The conceptual design showcased the systems database diagrams, ERD and relational database schemas. The proof of concept section covered various screen shots of VMPESA application working prototype, and finally the system testing section discussed several test cases that were carried out on the system.
Chapter 5: Results and Findings

5.1. Introduction
This chapter presents the findings and results of the research study. The chapter focuses on the data collected from various respondents who filled in the online questionnaires to help the researcher answer the various objectives outlined in chapter one. The first section covers the descriptive analysis of respondent’s general information. The subsequent sections present results about the research objectives. The research study had a sample size of 32 respondents. The questionnaires that were issued to the respondents were 32 in total, and they were filled in correctly, hence resulting in a 100 % response rate.

5.2. The Respondents Demographic Information
The demographic information that was obtained from the respondents included their gender, age, occupation and type of phone owned. Regarding these demographic information, the following is a presentation of their respective results.

5.2.1. Respondents Classification by Gender
The chart in Figure 5-35 indicates that the male respondents were 65.6%, while the female respondents were 34.4%. The study clearly indicates that most respondents were male.

![Figure 5-35: Respondents by Gender]
5.2.2. Respondents Classification by Age Group

Figure 5-36 below shows the respondents’ distribution by age groups. The results show that respondents in age group 25-44 years had the highest percentage with 75%, followed by 21.9% respondents in age group 18 - 24 years and finally 3.1% in the age group 45-64 years.

Figure 5-36: Respondents Age Group Distribution Pie Chart

5.2.3. Respondents Classification by Locality

Figure 5-37 below shows the respondents’ distribution by locality, where one lives. The results show that 78.1% of the respondents live within Nairobi. The remaining 21.9% live outside Nairobi.

Figure 5-37: Respondents Classification by Locality Pie Chart
5.2.4. Respondents Classification by Place of Work

Figure 5-38 below shows the respondents’ distribution by place of work. The results show that 56.3% of the respondents work in the public sector. 12.5% of the respondents are involved with academia or research. 12.5% of the respondents are self-employed. 5.6% of the respondents are unemployed. 5.6% of the respondents work in the NGO. 5.6% of the respondents work in a government institution.

![Figure 5-38: Respondents Classification by Place of Work Pie Chart](image)

5.2.3. Respondents Classification by Type of Phone Owned

Figure 5-39 below shows the respondents’ distribution by type of phone owned. The results show that 87.5% of the respondents operate an android phone. The remaining 12.5% operate an iPhone. There were no respondents operating a blackberry or a windows phone.

![Figure 5-39: Respondents Classification by Type of Phone Owned Pie Chart](image)
5.3. Authentication Schemes Used by Mobile Money Services

5.3.1 Number of MPESA Transactions per Day

Objective one of the research study aimed at investigating authentication schemes used by mobile money services in Kenya. The research sought to identify the number of MPESA transactions per day for each subscriber. The result findings in figure 5-40 indicated that 65.6% of the respondents mentioned that they transact less than times a day whereas 31.3% of respondents mentioned that they transact less than 10 times a day. 3.1% of respondents mentioned that they transact less than 15 times a day.

![Figure 5-40: Respondents Number of MPESA Transactions per Day](image)

5.3.2 Importance of Information Security and Data Protection

The research sought to establish how subscribers valued their data on mobile phones and importance of information security. According to figure 5-41 below, 59.4% of the respondents considered data protection and information security extremely important, followed by 31.3% of the respondents considered that it was important, while 9.4% of the respondents considered it slightly important.

![Figure 5-41: Importance of Information Security and Data Protection](image)
5.3.3 Techniques Trusted for Securing your Smartphone and Protecting MPESA Data

The research sought to establish techniques the subscribers trusted for securing their smartphone and protecting MPESA data. From figure 5-42 below, most of the respondents indicated that trusted PIN and password as a way of securing and protecting their MPESA data. The findings also showed that most respondents indicated that they trusted PIN and fingerprint as a way of securing and protecting their MPESA data.

![Figure 5-42: Techniques Trusted for Securing your Smartphone and Protecting MPESA Data](image)
5.3.4 Is MPESA 4-digit PIN as a Security Measure Sufficient

The research sought to establish if MPESA 4-digit PIN as a security measure is sufficient. Figure 5-43 below indicate that 75% of the respondents considered MPESA 4-digit PIN as a security measure not sufficient whereas 25% of the respondents considered MPESA 4-digit PIN as a security measure as sufficient security measure.

![Figure 5-43: Is MPESA 4-digit PIN as a Security Measure Sufficient](image)

5.3.5 Security Features that MPESA Can Adopt

The research sought to find out if subscribers are aware of any security features that MPESA can adopt. Figure 5-44 below indicates that 68.8% of the respondents reported that MPESA can adopt security features whereas 18.8% of the respondents reported that they were not aware that MPESA can adopt security features. The remaining 12.5% reported that they were not sure.

![Figure 5-44: Security Features that MPESA Can Adopt](image)
5.3.6 Authentication Document Used When Transacting With MPESA

The research sought to find the authentication documents subscribers used when transacting with MPESA. Figure 5-45 below indicates that most respondents used the national identification card.

![Figure 5-45: Authentication Documents Used when Transacting with MPESA](image)

5.3.7 4-digit Start Key Used when Registering for MPESA

The research sought to find out if subscribers remembered the 4-digit Start Key that was sent to them when registering for MPESA. Figure 5-46 below shows that 87.5% of the respondents indicated that they did not remember the 4-digit Start Key used when they registered for MPESA while 12.5% of the respondents indicated that they remembered their 4-digit Start Key that they received when registering for MPESA.

![Figure 5-46: 4-digit Start Key Used when Registering for MPESA](image)
5.3.8 MPESA Secret Word Used when Registering for MPESA

The research sought to find out if subscribers remembered the MPESA secret word that was sent when registering for MPESA. Figure 5-47 below shows that 84.4% of the respondents indicated that they did not remember MPESA secret word used when they registered for MPESA while 15.6% of the respondents indicated that they remembered their MPESA secret word that they received when registering for MPESA.

Figure 5-47: MPESA Secret Word Used when Registering for MPESA

MPESA Secret Word Used when Calling MPESA Customer Support

The research sought to find out if subscribers used MPESA secret word that was sent when calling MPESA customer care support. Figure 5-48 below shows that 84.4% of the respondents indicated that they did not use MPESA secret word used when they contacted MPESA Customer Support. 15.6% of the respondents indicated that they used MPESA secret word used when they contacted MPESA Customer Support.

Figure 5-48: MPESA Secret Word Used when Calling MPESA Customer Support
5.3.9 **Share MPESA PIN or MPESA Secret Word**
The research sought to find out if subscribers shared their MPESA PIN or MPESA secret word. Figure 5-49 below indicates that 62.5% of the respondents mentioned that they did not share their MPESA PIN or MPESA secret word whereas 37.5% of the respondents mentioned that they shared their MPESA PIN or MPESA secret word.

![Figure 5-49: Shared MPESA PIN or MPESA Secret Word](image)

5.3.10 **Easily Guessed MPESA PIN**
The research sought to find out if subscribers thought that their MPESA PIN could be easily guessed. Figure 5-50 indicated that 56.3% of the respondents thought that their MPESA PIN can be easily guessed and 43.8% of the respondents thought that their MPESA PIN cannot be easily guessed.

![Figure 5-50: Easily Guessed MPESA PIN](image)
5.3.11 Improve MPESA Security by Adding another Security Feature to MPESA PIN

The research sought to find out if subscribers thought that adding another security feature to the MPESA PIN could improve MPESA security. Figure 5-51 indicates that 90.6% of the respondents mentioned that they thought that MPESA security could be improved by adding another security feature to the MPESA PIN whereas 3.1% of the respondents mentioned that they did not think that their MPESA could be improved by adding another security feature to the MPESA PIN. 6.3% of the respondents mentioned that they were not sure that their MPESA could be improved by adding another security feature to the MPESA PIN.

Figure 5-51: Improve MPESA Security by Adding another Security Feature to the MPESA PIN
5.3.12 Combination of Authentication Systems to be used as an Additional MPESA Security

The research sought to find out which combination of authentication systems the subscriber was willing to use as an additional MPESA security. Figure 5-52 below shows that 56.3% of the respondents indicated that they preferred adding fingerprint as combination of authentication systems as an additional MPESA security.

Figure 5-52: Combination of Authentication Systems to be used as an Additional MPESA Security

5.3.13 Type of Biometrics Used Before

The research sought to find out which type of biometrics the subscribers have used before. Figure 5-53 below shows that 93.8% of the respondents indicated that they had used fingerprint as a biometric. 15.6% of the respondents indicated that they had used the iris as a biometric. Voice biometric had a percentage of 18.8%; Face biometric had a percentage of 12.5% as indicated by respondents.

Figure 5-53: Type of Biometric Used Before

98
5.3.14 Adding Biometrics Will Improve MPESA Security

The research sought to find out if subscribers thought that adding biometrics will improve MPESA security. Figure 5-54 indicates that 84.4% of the respondents mentioned that adding biometrics will improve MPESA security, 12.5% of the respondents mentioned that not sure that adding biometrics will improve MPESA security and finally 3.1% of the respondents mentioned that they did not think that adding biometrics will improve MPESA security.

![Figure 5-294: Adding Biometrics Will Improve MPESA Security](image)

5.3.15 Ever Used Voice Biometrics in Any System

The research sought to find out if the subscribers have ever used voice biometrics in any system. Figure 5-55 indicates that 68.8% of the respondents noted that they had never used voice biometrics in any system whereas 31.3% of the respondents noted that they had used voice biometrics.

![Figure 5-305: Ever Used Voice Biometrics in Any System](image)
5.3.16 Is Voice Biometrics the Most Secure Type of Security for MPESA

The research sought to find out if the subscribers thought that voice biometrics is the most secure type of security for MPESA. Figure 5-56 below shows that 43.8% of the respondents indicated that they did not think voice biometrics is the most secure type of security for MPESA, 28.1% of the respondents indicated that they were not sure if voice biometrics is the most secure type of security for MPESA and 28.1% of the respondents indicated that they were sure that voice biometrics is the MOST secure type of security for MPESA.

Figure 5-56: Is Voice Biometrics the Most Secure Type of Security for MPESA
5.3.17   Easily Use Voice Biometrics when Transacting Using MPESA

The research sought to find out if the subscribers would easily use voice biometrics when transacting using MPESA. Figure 5-57 below shows that 46.9% of the respondents indicated that they would easily use voice biometrics when transacting using MPESA. 37.5% of the respondents indicated that they would not easily use voice biometrics when transacting using MPESA and 15.6% respondents indicated that they were not sure if they would use voice biometrics when transacting using MPESA.

![Easily Use Voice Biometrics When Transacting Using MPESA](image1)

**Figure 5-317: Easily Use Voice Biometrics When Transacting Using MPESA**

5.3.18   Voice Biometrics Would Slow Down the MPESA Process

The research sought to find out if the subscribers thought the use of voice biometrics would slow down the MPESA process. Figure 5-58 below shows that 31.3% of the respondents noted that the use of voice biometrics would slow down the MPESA process. 43.8% of the respondents noted that they did not think use of voice biometrics would slow down the MPESA process and 25% noted that they were not sure if the use of voice biometrics would slow down the MPESA process.

![Voice Biometrics Would Slow Down the MPESA Process](image2)

**Figure 5-328: Voice Biometrics Would Slow Down the MPESA Process**
5.3.19 Preference of Using PIN and Voice Security Together
The research sought to find out if the subscribers would prefer using PIN and Voice security together. Figure 5-59 below shows that 62.5% of the respondents indicated that they would prefer using PIN and Voice security together. 31.3% of the respondents indicated that they would not use PIN and Voice security together.

![Preference of Using PIN and Voice Security Together](image)

**Figure 5-59: Preference of Using PIN and Voice Security Together**

5.4. Major MPESA Fraud Techniques used in Kenya

5.4.1 Victim of MPESA Fraud
The research sought to find out if the subscribers have been victims of MPESA fraud. Figure 5-60 below shows that 62.5% of the respondents mentioned that they have never been victims of MPESA fraud whereas 37.5% of the respondents mentioned that they have ever been victims of MPESA fraud.

![Victim of MPESA Fraud](image)

**Figure 5-60: Victim of MPESA Fraud**
5.4.2 MPESA PIN Revelation
The research sought to find out if the defrauded subscribers revealed their PIN numbers. Figure 5-61 below shows that 96.9% of the respondents mentioned that they did not reveal their PIN numbers whereas 3.1% of the respondents mentioned that they revealed their MPESA PIN.

![Figure 5-61: MPESA PIN Revelation](image)

5.4.3 What Means Did the Fraudster Use
The research sought to find out what means the fraudster used. Figure 5-62 indicates that 41.2% of the respondents mentioned that the fraudsters used SMS messages. 41.2% of the respondents mentioned that the fraudsters used phone calls. 5.9% of the respondents mentioned that the fraudsters stole their phones.

![Figure 5-62: What Means Did the Fraudster Use](image)
5.4.4 Fraud Techniques Used in the Area

The research sought to find out if the respondents were aware of the fraud techniques used in their area. Figure 5-63 indicates that 80% of the respondents mentioned that they were aware of the fraud techniques used in their area. 20% of the respondents mentioned that they were not aware of the fraud techniques used in their area. Figure 5-64 indicates that respondents noted that reversal of erroneous transactions and scam messages were mostly used by fraudsters.

Figure 5-63: Fraud Techniques Used in the Area

Figure 5-64: Type of Fraud Techniques Used in the Area
5.5. Impact of Implementing Voice Biometrics Feature on Mobile Transactions

5.5.1 Registering for VMPESA Services

Objective three of the research study aimed at implementing a time efficient, secure mobile-based multi-factor authentication application using device specific ID, voice biometric and a PIN for securing MPESA transactions. The research sort to find out how long respondents took to register for VMPESA services. Figure 5-65 revealed that 31.3% of respondents mentioned that they took less than 10 minutes, 31.3% of respondents mentioned that they took less than 5 minutes, 21.9% of respondents mentioned that they took less than 2 minutes and 15.6% of respondents mentioned that they took more than 10 minutes.

![Figure 5-65: Registering for VMPESA Services](image)

Figure 5-65: Registering for VMPESA Services
5.5.2 Assistance to Register Voice on VMPESA

The research sort to find out if respondents received assistance on how to register your voice on VMPESA. Figure 5-66 below revealed that 59.4% of respondents mentioned that they received assistance on how to register your voice on VMPESA while 40.6% of respondents mentioned that they did not received assistance on how to register your voice on VMPESA.

Figure 5-66: Assistance to Register Voice on VMPESA
5.5.3 Transaction Duration Using the VMPESA Application

The research sought to find out how fast it took to perform a transaction using the VMPESA application. Figure 5-67 revealed that 50% of respondents mentioned that they took less than five minutes to perform a transaction using the VMPESA application, 9.4% of respondents mentioned that they took more than ten minutes to perform a transaction using the VMPESA application, 25% of respondents mentioned that they took less than two minutes to perform a transaction using the VMPESA application and 15.6% of respondents mentioned that they took less than ten minutes to perform a transaction using the VMPESA application.

![Figure 5-67: Transaction Duration Using the VMPESA Application](image)

Figure 5-67: Transaction Duration Using the VMPESA Application
5.5.4 Problems When Transacting Using the VMPESA Application

The research sought to find out if respondents encountered any problem when transacting using the VMPESA application. Figure 5-68 revealed that 67.7% of respondents indicated that they did not encounter any problem when transacting using the VMPESA application, 19.4% of respondents indicated that they were not sure if they encountered any problem when transacting using the VMPESA application and 12.9% of respondents indicated that they encountered problems when transacting using the VMPESA application.

Figure 5-68: Problems When Transacting Using the VMPESA Application

5.5.5 Successful Transactions on the VMPESA Application

The research sought to find out if the transactions were successful on the VMPESA application. Figure 5-69 below revealed that 77.3% of respondents indicated that their transactions were successful on the VMPESA application while 22.7% of respondents indicated that their transactions were not successful on the VMPESA application.

Figure 5-69: Successful Transactions on the VMPESA Application
5.6. Chapter Summary
This chapter did a presentation of findings regarding improving MPESA authentication by implementing a voice biometric feature as an additional security feature. The study investigated 32 subscribers with an emphasis on subscribers within USIU-Mirema area. The presentation of the findings was done in accordance with the research study’s objectives. About the authentication schemes used by mobile money services, 75% of the respondents think that PIN as a security feature is not sufficient as evidenced in figure 5-43. In addition to this 87.5% of the respondents did not remember the 4-digit Start Key used when they registered for MPESA as evidenced in figure 5-46. The findings also indicate that 84.4% of the respondents did not remember MPESA secret word used when they registered for MPESA evidenced in figure 5-47. Information security and data protection extremely important as indicated by 59.4% of the respondents, as evidenced in figure 5-41. As evidenced in figure 5-50, 56.3% of the respondents think that their MPESA PIN can be easily guessed. About the major MPESA fraud techniques used in Kenya, figure 5-60 indicates that 62.5% of the respondents have never been victims of MPESA fraud whereas 37.5% of the respondents have ever been victims of MPESA fraud as evidenced in figure 5-60. In addition to this, a large percentage of respondents did not share their MPESA pin, figure 5-49. About the fraud techniques, 41.2% of the respondents mentioned that the fraudsters used SMS messages used as indicated in figure 5-62. About developing an application that is time efficient, secure using device specific ID, voice biometric and a PIN for securing MPESA transactions, this was an improvement to the existing security measure implemented for MPESA authentication.
Chapter 6: Discussion, Conclusion and Recommendation

6.1. Introduction

This part of the project systemically outlines the study findings based on the research conducted on the basis of the research questions set out and the responses garnered from all the respective respondents. The analysis under chapter six presents the data collected, statistical analysis of the data collected, general and specific comparison with the literature review and previous research on the same, the findings, the extent to which the research gaps have been filled, a comprehensive summary, discussion on the results obtained, establishment of the right conclusions and the proposed relevant recommendation on the application of the voice biometrics to MPESA.

Chapter six highlights how the benefits of incorporating the voice biometric system in MPESA functionalities outweigh the costs and how this would be a positive milestone for Safaricom Company in terms of being the best service provider. It is also a fundamental part of the project where we align the project objectives and the results or findings. The findings enable an exhaustive discussion and the relevance of the literature review in terms of similarities and differences which is backed by significant extrapolation of statistical results based on the same data collected. Therefore chapter six provides a reasonable assurance on the meaning of the findings or data collected in relation to already conducted research.

6.2. Summary

The main objective of this project is to 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. The voice biometric is a state of the art technology that factors in authentication with better usability with the aim of combating fraud, self-service empowerment and cost savings through proper use of time and saving or reduction of administration costs for companies. The research study addressed the following objectives: To investigate the authentication schemes used by mobile money services; to investigate the major MPESA fraud techniques used in Kenya; to implement and analyse a time efficient, secure mobile-based multi-factor authentication scheme using device specific ID, voice biometric and a PIN for securing MPESA transactions.

Research has enabled the acquisition of information that most companies are in the frontline in adopting the voice biometric applications for various advantages. One of
the advantages is that voice is ideally the only landline biometric identifier. Another advantage is that voice is a permanent natural state which cannot be lost like passwords or pins thus underlining the advantage of longevity. Therefore, there it becomes simple to pinpoint any issues and link it to the parties responsible. In addition to this, unique voiceprints rule out the possibility of impersonation of people for whatever reasons. This aspect increases the level of security for private information and accounts. Users who opt for voice biometrics do not require software or devices are required for the implementation of the voice biometric application for participation (authentication process). This point underlines the convenience for the end user who is the main beneficiary of the accurate authentication process.

Subscribers also benefit by saving time through reduced call centre questions in trying to verify the specific parties or individuals. The call centre can easily identify an individual through the use of voice biometric application. In addition to this, the time agents spend when talking to callers from different areas is greatly minimized therefore reducing the overall overheads the company incurs ultimately resulting to higher margins. Lastly, voice biometric application enables the set up for upgrade and the incorporation of additional layers of controls and securities in companies thus increasing the overall security of information. This aspect is a fundamental role of voice biometrics in filling research gaps where previous research did not provide information on a system that would enable multifunctional security protocols through multi layers in addition to the normal traditional layer (enhanced security) (Bakanay, 2018).

However the specific objectives for this project are:

To investigate the authentication schemes used by mobile money services: This objective illustrates the authentication processes adopted by MPESA which have been compromised so far by a considerable extent through fraudulent activity and compromised unique ID systems. The research explains the scope as well as the strength of the authentication and the proposed introduction of a better, more secure and reliable authentication system. The current MPESA system functionality is based on PIN which is essentially a single factor authentication system. The proposed voice biometric adds an additional authentication which is the voice profile thus realizing a three factor authentication system which is more efficient, reliable, accurate and has a higher degree of authenticity in the mobile transfer system.
To investigate the major MPESA fraud techniques: The second objective is to highlight the various kinds of fraud mobile MPESA users are exposed to thus underscoring the essence of strong controls. The mobile money users have become victims of extortion, money laundry, ID theft, phishing, psychological games with the intent to defraud amongst many other kinds of fraud mentioned. Chapter six explains the various kinds of fraud based on the data collected and provides a conclusive element of control that shall be established within the voice biometric system or application proposed. The incorporation of voice biometric in the MPESA functionality enables the unique voice identification for a transaction to be completed regardless of the previous single factor authentication. Therefore there is more control instituted which is based on very specific sound technology in terms of the psychological and behavioural aspects of sound. The aim is to reduce the risk of the possibility of the occurrence of fraud to a minimum level which ensures the safety of MPESA accounts as well as the safety of private personal information.

To implement the multifactor authentication (3FA) scheme: The third objective focuses on implementation of the integrated three factor authentication which is a combined element. The question of how to incorporate the voice biometric into the authentication process therefore arises. The mobile subscriber shall be required to record a unique statement in a number of times maybe three to have the system create an algorithm that works on identifying the best probability of identification of voice given the different environments, the different types of interference, the age factor and all the possible factors that may contribute to the variation in voice or sound as heard by the voice recognition system. The voice of the individual should therefore fit within a given range or standard deviation from the original voice recorded for the biometric system to accept the identification and the enabling of MPESA transactions. This objective illustrates the intelligence aspect of the voice biometric system which is expected to be efficient.

To analyse the use of system in terms of the purpose, accuracy and efficiency: the final objective of this study is to analyse the impact of the incorporation of the voice biometric system in the MPESA functionality within a specific time frame. The integrated 3FA system is able to increase the enhance efficiency of MPESA function and increase the business for the service provider through higher approval of satisfied clients who shall increase their use of the MPESA application. The 3FA system increase the reliance of
clients on MPESA with more authenticity of the system, enhanced purpose of MPESA, more accuracy through subsequent voice authentication and overall more efficiency. There is also the benefit of reduced risk of fraud within MPESA system whether it is fraud through internally hatched plans or externally hatched plans. The element of getting compromised is highly reduced through the 3FA authentication system.

6.3. Discussions

This part of the project tries to correlate the findings obtained from the research and responses from respondents to the specific objectives and ultimately correlation with the main objective of improving the MPESA authentication through the use of a voice biometric system.

6.3.1. Authentication Schemes Used by Mobile Money Services

The research findings indicated that most respondents 65.6% transacted less than 5 times a day followed by 31.3% of respondents indicated that they transacted less than 10 times a day and finally 3.1% indicated that they transacted less than 15 times a day. As per the data collected, majority of the respondents have a relatively moderate frequency of MPESA transactions per day. The data researched shows that an increase in new users daily which is consistent with the growth in the transaction volume data provided for by Safaricom Company. Research shows that one out of 10 transactions globally is made in Kenya with a major portion of those transactions being those of MPESA. The number of transactions done via mobile phone has surged to an average rate of 28.65% annually with most of these transactions credited to loans, dividends and money sourced or channelled to Diaspora. Safaricom through MPESA is the mainly player here with the rapid increase in subscribers since its inception in 2007. A classic example is the volume of money as of December 2016 (sh 316.77 Billion) as portion of the $22 Billion wired across the world December 2016 which essentially constituted 14.4 % of the global money volume remitted during that period in time (David, 2017). These facts match the information submitted by most of the respondents about having numerous transactions in one day given there has been no significant reduction in the number of MPESA users.

Data protection and information security is very important. The research study indicated that 59.4% of the respondents considered data protection and information security extremely important, followed by 31.3% who considered that it was important, while 9.4% of the respondents considered slightly important. Majority of the respondents in the
study consider data protection and privacy as something very instrumental in achieving their goals and objectives. A recent study postulates that even cyber security professional have some concerns about mobile money payments and the security of personal information. The ISACA’S 2015 mobile payment security study provides information that up to 87 % of respondents expected an increase in the level of mobile data breaches within 12 months. Out of the respondents surveyed under this study 42% of those using mobile payments felt their information was not secured and had concerns. Security and privacy are major priorities for the service providers as the clients have their personal information shared. The observation from this study matches the results in the study: majority of the respondents consider data protection to be great importance.

The research revealed that a significant proportion trust the use of biometrics to being incorporated in MPESA transactions in the order of password, fingerprint, face, voice and ear recognition. Majority of the respondents in the study trust the password and the fingerprint forms of identification. Iris recognition and the ear recognition also have significant proportion of people who prefer them as methods of the best form of authentication. The respondents fully trust these features for authentication because of the unique ability of each feature for authentication purposes. Iris scanner and recognition is a more recent technology with its incorporation in authentication being incorporated into some of the latest technological products such as Samsung S8 by Samsung Company. The firm is adopting an integrated approach of adopting iris, fingerprint and facial features in identification systems which indicates the efficiency of integrated authentication systems. In reference to mobile payments system MPESA, a significant proportion of the respondents trust the incorporation of an ear recognition system, voice biometric or an iris recognition system in the authentication of transactions. A recent study indicated that 74% of the respondents said that the use of biometrics was much easier and better than the use of passwords. The use of an integrated system of authentication is however more preferable for this study.

The research study indicated that 75% of the respondents considered MPESA 4-digit PIN as a security measure not sufficient while 25% of the respondents considered MPESA 4-digit PIN as a security measure as sufficient security measure. Majority of the respondents also are of the opinion that the 4 digit pin is not enough in the verification process which provides the necessity of having a higher level of authentication as defined.
and enabled by biometrics applications. In the research findings, 68.8% of the respondents indicated that they were aware that MPESA can adopt security features, 18.8% of the respondents were not aware that MPESA can adopt security features and the remaining percentages of 12.5 % were not sure. Majority of the respondents would prefer to have additional security features in their mobile handsets while transacting via MPESA. This aspects stems from the need to have a higher level of personal data protection (privacy concerns) as well as to, limit the loss of money through fraud and exposure to risk. The general observation is that there has been a wave of loss of money due to exposure to risk and increased personal information exposure enabled through technological developments creating an increased demand for more security through more appropriate authentication measures (ResearchGate , 2012).

The research study indicated that 87.5% of the respondents did not remember the 4-digit Start Key used when they registered for MPESA while 12.5% of the respondents remembered their 4-digit Start Key that they received when registering for MPESA. The research study indicated that 84.4% of the respondents did not use MPESA secret word used when they contacted MPESA Customer Support while 15.6% of the respondents used MPESA secret word used when they contacted MPESA Customer Support. Majority of the respondents who filled out of the questionnaires do not remember their start keys or the secret word they used during registration of MPESA. Majority of these respondents also have not shared out their start keys or secret words. This aspect therefore highlights the problem of limited control as to the authentication and verification of individual information. The situation described above highlights the ease with which such information can be acquired even if it is not shared, once a hacker has access to the individual registration details then the individual MPESA account becomes compromised assuming the PIN or password information is also obtained (Techweez, 2018).

The research findings indicated that most respondents 62.5% did not share their MPESA PIN or MPESA secret word while 37.5% of the respondents shared your MPESA PIN or MPESA secret word. The research study indicated that 56.3% of the respondents think that their MPESA PIN can be easily guessed whereas 43.8% of the respondents think that their MPESA PIN cannot be easily guessed. Majority of the respondents think that the MPESA pin may be easily guessed. This data shows the inherent risk that is posed to this section of respondents especially with the advent of technological applications that can easily enable stealing of passwords or pins.
The research study indicated that 90.6% of the respondents think that their MPESA security can be improved by adding another security feature to the MPESA PIN, 3.1% of the respondents do not think that their MPESA can be improved by adding another security feature to the MPESA PIN and 6.3% of the respondents were not sure. Majority of the respondents are of the view that addition of another security feature shall be imperative as to the enhancement of security of their information and account balances through a higher level of authentication. The application of an integrated system, in this case the 3FA authentication fits the preferred option (Berkeley Solutions, 2016).

The research study indicated that 56.3% of the respondents prefer adding fingerprint as combination of authentication systems as an additional MPESA security. Most of the respondents have a preference for the combination of a fingerprint recognition biometric system and the use of a pin. The use of pin and fingerprint recognition ideally refers to the 3FA system which enhances security of MPESA transactions and personal information. The major disadvantages that occur from the use of a voice biometric recognition system is possibility of system rejection as once the voice biometric senses and records the voice, it cannot revert the process. This aspect was noted by most of the respondents who feared their voices could change due to an illness or change of environment that had various sources of interference. The respondents also felt the passwords could be hacked with the advent of technological advances and prior experiences (Thakkar, 2018).

The research findings indicated that most respondents 93.8% indicated to have used fingerprint as a biometric, 15.6% of the respondents indicated to have used the iris as biometric, face biometric had a percentage of 12.5% and voice biometric had a percentage of 18.8 %. Most of the respondents had some clue about biometrics mostly about fingerprint registration (923.8%) and had only heard about the other biometric applications but had not experienced other these biometric applications.

The research study indicated that 84.4% of the respondents think that adding biometrics will improve MPESA security, 12.5% of the respondents were not sure that adding biometrics will improve MPESA security and 3.1% of the respondents did not think that adding biometrics will improve MPESA security. Most of the respondents had a strong opinion that the inclusion of biometrics in MPESA especially voice biometrics would go a long way in increasing the security of MPESA transactions.

The research study indicated that 68.8% of the respondents have never used voice biometrics in any system while 31.3% of the respondents have ever used voice biometrics
in any system. Most of the respondents had not used any kind of biometrics but had only heard about them and that some could be used with or without a Smartphone. Most of the information regarding biometrics was about authentication and security of mobile payments or transactions. (ID Experts, 2016)

The research study indicated that 43.8% of the respondents do not think voice biometrics is the MOST secure type of security for MPESA, 28.1% of the respondents were not sure if voice biometrics is the MOST secure type of security for MPESA and 28.1% of the respondents were sure if voice biometrics is the MOST secure type of security for MPESA. Most of the respondents think that the use of biometrics is not one of the most secure ways of increasing security within the MPESA platform (PYMNTS, 2016).

The research study indicated that 46.9% would not easily use voice biometrics when transacting using MPESA, 37.5% of the respondents would easily use voice biometrics when transacting using MPESA and 15.6% were not sure if they would use voice biometrics when transacting using MPESA. Most of the respondents do not think the use of the biometrics would be easy but some are positive on the simplicity of the biometrics application when transacting using the normal MPESA set up. A small percentage is not sure on the ease of using MPESA voice biometrics.

The research findings indicated that most respondents 62.5% would prefer using PIN and Voice security together while 31.3% of the respondents would not prefer using PIN and Voice security together. Majority of the respondents would prefer to use the pin and voice as most of them were optimistic of higher security of their money in MPESA accounts.

The research study indicated that 31.3% of the respondents thought use of voice biometrics would slow down the MPESA process, 43.8% of the respondents did not think use of voice biometrics would slow down the MPESA process and 25% were not sure if the use of voice biometrics would slow down the MPESA process. Majority of the respondents expect the voice biometrics to be completely simplified for the purpose of enhancing MPESA security and set up. Therefore, the majority of the respondents view the biometrics as a factor that will not slow down the MPESA (Faulkner, 2017).

6.3.2. Major MPESA Fraud Techniques used in Kenya

The research study indicated that 62.5% of the respondents have never been victims of MPESA fraud whereas 37.5% of the respondents have never been victims of MPESA fraud. Most of the respondents have not been victims of MPESA fraud which suggests
that despite most of the respondents not feeling very safe using the password alone, the somehow had a higher probability of having less instances of fraud.

The research study indicated that majority of the respondents 96.9% did not reveal their PIN numbers while 3.1% of the respondents revealed their MPESA PIN. Majority of the respondents did not reveal their PIN before being victim of a fraud attack. The interpretation here is that the instances of fraud were based on technological scams or measures that were used to identify client information.

The research study indicated that 41.2% of the respondents mentioned that the fraudsters used SMS messages, 41.2% of the respondents mentioned that the fraudsters used phone calls and 5.9% used stolen phones. Half of the respondents are of the opinion that the fraudsters were using SMS to acquire client information which conceals the voice aspect. Half of the respondents think otherwise (fake calls) and an additional 5.9% think that the fraudsters had used stolen phones. The voice biometric application shall be a big step towards the elimination of instances of fraud that occur as a result of these measures.

The research study indicated that 80% of the respondents are aware of the fraud techniques used in their area while 20% of the respondents are not aware of the fraud techniques used in their area. Majority of the respondents are cognisant of the fraud measures used in the area therefore being able to be more receptive to changes proposed that can help or aid in lowering or reducing the incidences of fraud.

The research study indicated that majority of the respondents 80% were aware of the main types of fraud in their area being reversal of erroneous transactions and scam messages, 50% of the respondents had knowledge of the main types of fraud in their area being unauthorized SIM-swap and identity theft and 30% of the respondents had information that the main type of fraud in their area was insider theft. Majority of the respondents think fraud majorly stems from reversal transactions and scam messages which highlight the gap in the MPESA transactions authorization which makes the use of additional biometric features such as voice biometric, a more secure and authentic method of protecting client information and MPESA accounts (Thakkar, 2018).

6.3.3. Impact of Implementing Voice Biometrics Feature on Mobile Transactions

The research study revealed that 31.3% of respondents took less than 10 minutes, 31.3% of respondents took less than 5 minutes, 21.9% of respondents took less than 2 minutes and 15.6% of respondents took more than 10 minutes. Majority of the respondents took
about 10 minutes to register for MPESA services as they had to wait for initialization and verification.

The research study indicated that 59.4% of respondents received assistance on how to register your voice on VMPESA while 40.6% of respondents did not receive assistance on how to register your voice on VMPESA. Most of the respondents got assistance from customer care in getting their voices registered for voice in MPESA.

The research study indicated that 50% of respondents took less than five minutes to perform a transaction using the VMPESA application, 9.4% of respondents took more than ten minutes to perform a transaction using the VMPESA application, 25% of respondents took less than two minutes to perform a transaction using the VMPESA application while 15.6% of respondents took less than ten minutes to perform a transaction using the VMPESA application. Majority of the respondents said the voice security feature did not affect the transaction speed and the transaction was rather fast or instant on trial. This aspect essentially describes the user experience that is enhanced and the simplicity of the incorporating voice biometrics in MPESA (Faulkner, 2017).

The research study indicated that 67.7% of respondents did not encounter any problem when transacting using the VMPESA application, 19.4% of the respondents was not sure if they encountered any problem when transacting using the VMPESA application and 12.9% of respondents encountered any problem when transacting using the VMPESA application. A larger proportion of the respondents mentioned that they had not encountered any problem while transacting with the voice security feature in MPESA. Voice authentication has been designed to make the whole process a lot simpler and easier therefore enabling a higher level of security for user accounts (Premier Technologies, 2018).

The research study indicated that 77.3% of respondents’ transactions were successful on the VMPESA application while 22.7% of respondents’ transactions were not successful on the VMPESA application. The majority view is that the voice security feature is ideal for transaction completion as well as security purposes and that the respondents felt safer with their accounts as they could have a higher level of assurance regarding the money in their accounts and the privacy of information in their accounts. Majority of the respondents strongly agree that the security feature has improved MPESA service delivery and that MPESA services have become more secure. The use of a one-time password is the idea brought out by Say Pay Company, voice recognition and biometric
authentication solutions provider. This one time action matches the details of the transactions to the user’s details thus increasing the security of the transaction (PYMNTS, 2016).

Most of the respondents agree that the security feature has made MPESA easy to use and feel that they can make a transaction effectively with increased accuracy. Majority of the respondents also agree feeling quite comfortable when transacting via MPESA through the use of the voice biometric and the ease of learning how to use the system. Research demonstrates that the two factor identification process may be inconvenient; the use of three factor authentication system is a plus for companies using that kind of technology with the institution of voice biometric. Apart from the security associated with the voice biometric feature, the 3FA has minimal disruption with regard to the customer service experience. The research illustrates that globally people are gradually becoming comfortable using their voice for basic commands on mobile handsets thus easy enhancement of the voice biometric on handsets. (Premier Technologies, 2018)

The users or respondents also agree on the error correction ability of the security feature which highlights points of error and guide the user in using MPESA voice biometric with clarity of messages. The respondents also agree that the response information by the voice biometric in MPESA is easily comprehensible thus increasing the user efficiency and accuracy. A greater proportion of the respondents agree that the information is well organized and has an attractive user interface which most of the respondents like.

Most of the respondents are not sure if the voice biometric system has all the functions or capabilities that they require it to have. Majority of the respondents agree that the voice biometric system saves time through voice identification as well as most of them being satisfied with the system. Research into the various uses of biometrics reveals that the end user or the consumer are not required to install specific software to access the voice biometric in the authentication process. Additionally, the voice biometric saves a lot of time through reduction of questions asked by the contact centre persons for verification of persons. Time is also saved through reduced agent-client time on calls and there is overall enhancement of the security that can be modified for multifactor authentication of additional layers of security (for example “who you are” and “what you know” layers) (Bakanay, 2018).
6.4. Conclusion

In light of the discussion of results from the respondents’ data, PIN is not a sufficient security measure when performing mobile transactions and fraudsters are taking advantage of this vulnerability to defraud MPESA subscribers by using techniques such as SIM-swap, reversal transactions and scam messages. Voice biometrics is a factor that can be used to achieve a high degree of benefits and advantages in lowering the risk within mobile financial systems with specific reference to MPESA mobile money transfer system.

A brief demonstration of the conclusive gains and benefits of incorporating a voice biometrics application in the MPESA functionality within Safaricom include the following;

There is a higher level of security of private information through an enhanced authentication system (3FA) which essentially represents and integrated approach of security firewalls per se. In addition to this there is a projection of more secure MPESA accounts through enhanced access and enhanced authentication which is imperative for increasing the efficiency, reliability and increased positive reputation for the Safaricom Company. When it comes to audit, the implementation of the 3FA simplifies the audit trail or follows up therefore increasing the reliability of the MPESA system in financial audit. Three Factor Authentication (3FA) is a unique authentication scheme that increases efficiency and accuracy and is recent in the field of mobile applications globally therefore being less prone to cyber security vulnerabilities. Multifactor authentication system employs uses effective strategies in the protection of customer information which highlights an imperative advantage over single security features. Another benefit is that voice biometrics feature is based on sound identification which means the security feature has been developed for purposes of longevity. Three Factor Authentication is a major boost to authentication and accountability. An addition to this is that low costs incurred in implementation, simplicity in its use, fast enrolment of users and relatively small amount of space to accommodate the voice id.

Shortcomings

For voice biometric system to work as an effective authentication scheme, it requires integration with other authentication systems to optimize its functionality. A major shortcoming is that the human voice changes over significant time periods which may
cause some system error in recognition over long periods of time. Another shortcoming is that the external environmental factors may orchestrate the possibility of voice variation thus the possibility of some error in voice recognition. Lastly, the possibility of inefficiencies generated with the requirement of lengthy details.

In lieu of the benefits and limitations, the benefits of the incorporation of the voice biometric outweigh the costs.

6.4.1. Authentication Schemes Used by Mobile Money Services

The type of authentication scheme adopted by mobile money service providers is critical in protecting users’ information and data. MPESA uses a 4 digit PIN as a security feature while performing transactions. A 4 digit PIN is considered a single factor authentication scheme which has become insufficient when protecting subscriber data.

The research study identified weaknesses in terms of using single factor authentication schemes as a security measure when performing MPESA transactions. The study findings indicated that subscribers’ 4 digit PINS could be easily guessed. The findings also show that other than PIN, subscribers did not remember or hardly used the secret word and 4 digit start key provided during registration of MPESA service.

The study findings also show that adding biometrics as an authentication feature to the MPESA transactions would greatly improve MPESA security. There is need to improve MPESA security by implementing better authentication schemes hence reducing exploitation of the existing single factor authentication weakness by fraudsters.

6.4.2. Major MPESA Fraud Techniques used in Kenya

The research pointed out the major MPESA fraud techniques used in Kenya. These included reversal of unauthorized sim-swap, identity theft, erroneous transactions, scam messages and insider theft. The research study revealed that MPESA subscribers were aware of the fraud techniques used in their area which was mostly unauthorized sim-swap and identity theft. It also revealed that MPESA subscribers were careful not to disclose their PIN meaning that fraud victims were defrauded using information obtained by social engineering. The research also indicated that fraudsters commonly used sms and phone calls to obtain subscriber information.
6.4.3. Impact of Implementing Voice Biometrics Feature on Mobile Transactions
The research study indicated that most subscribers were able to perform transactions on the voice biometrics mobile application. Registration on the voice biometric application took longer than the already existing MPESA registration process. A larger proportion of the respondents mentioned that they had not encountered any problem while transacting with the voice security feature on VMPESA mobile application.

The research study indicated that most that the respondents felt safer with their accounts as they could have a higher level of assurance regarding the money in their accounts and the privacy of information in their accounts while performing transactions.

6.5. Recommendations

6.5.1. Authentication Schemes Used by Mobile Money Services
In reference to objective one on authentication schemes used by mobile money schemes, the recommendation would be for mobile money service providers to concentrate on improving MPESA transactions security by implementing multifactor authentication schemes. They should investigate on better more effective technologies that can be integrated with the existing security feature implemented. Implementing improved security features would greatly reduce the fraud cases reported. Consequently reduce losses incurred to both the subscribers and to the mobile money service providers.

6.5.2. Major MPESA Fraud Techniques used in Kenya
The second recommendation in reference to MPESA fraud can be the actively creating awareness of the fraud techniques used by attackers. In addition to this, Safaricom should create a voice template database that contains voice samples of the fraudsters. The organisation can further investigate on the loopholes fraudsters exploit to carry out fraudulent activities. Safaricom should carry out periodic investigations on the latest fraud techniques used to defraud MPESA subscribers.

6.5.3. Impact of Implementing Voice Biometrics Feature on Mobile Transactions
A variance analysis can be done to compare the new voice biometric application effects and the previous authentication used by MPESA as the three factor authentication system is implemented. The actual difference can be compared on statistical basis to enable conclusive inferences to be highlighted, thus the benefits of the system.

Researchers should do further studies on implementing multifactor authentication using fingerprint technology since most respondents have already interacted with it hence easier
for the subscribers. In addition to this, researchers also should do further studies on voice biometrics and the algorithms used, adding more functionalities to make the entire process more seamless and intelligent in nature.

The recommendation based on the on efficiency is for the firm to invest in high technology to facilitate the development of in-house algorithms as opposed to outsourcing this function to third party APIs. The resultant impact of such a move is lower overall cost incurred in running processes therefore increasing the overall efficiency of the process.

Voice biometrics applications are susceptible to replay attacks and man in the middle attacks. For man in the middle attacks, the recommendation would be to encrypt by using a combination of both RSA encryption and symmetric key encryption. This feature comes in handy in strong data encryption which creates stronger firewalls against fraud by ensuring tougher controls in data accessibility. Regular change of encryption patterns may be a secondary approach for data protection therefore limiting the level of fraud.

For replay attacks, the recommendation would be to use random sentences instead of fixed sentences in voice identification or numerical random codes therefore enabling more accurate recognition of voice and more security authentication. Systems in place should also be featured to be able to distinguish between live voice and recorded voice through unpredictable non sequenced unique questions with unique answers.

6.5.4 General Recommendation
The following were the recommendations regarding the research study findings. For mobile money service providers to provide safe and secure transactions, they should concentrate on implementing multifactor authentication schemes in their system. They should also identify the major weaknesses of the implementing PIN as a security measure. Improved security will reduce the fraud related cases hence reducing losses incurred to mobile subscribers and to the organisation as a whole. Mobile money service providers should also be aware that fraudsters are employing new techniques everyday therefore continuous upgrade of the security features is imperative. Safeguarding subscriber personal information and account is extremely important and should be top priority to these organisations.

Researchers should do further studies on alternative multifactor authentication schemes which have more functionalities to make the entire process more seamless, convenient for
the subscribers and intelligent in nature. Further studies should be done to identify the advance techniques used by fraudsters to acquire subscribers’ personal information.
References


http://m.myjoyonline.com/articles/opinion/avoiding-fraud-due-to-momo


http://www.globalsecurity.org/security/systems/biometrics-voice.htm


https://premiercontactpoint.com/customer-experience-voice-biometrics/


PYMNTS. (2016, May). Can voice authentication tip the mobile payments scale? Retrieved April 17, 2018, from PYMNTS website:

PYMNTS. (2016, May 12). Can voice authentication tip the mobile payments scale?
PYMNTS .


https://www.safaricom.co.ke/faqs/faq/270
http://www.voicevantage.com/News/industry/practicalguidetobiometrics.html


Appendices

Appendix I: Questionnaire

To Whom It May Concern

Dear Sir/Madam,

I am pleased to inform you that I am a graduate student at United States International University pursuing Masters in Information Systems. As partial fulfilment of the Masters degree, I am conducting a research seeking to investigate the implementation of voice biometrics as an additional security feature in MPESA.

Please note that any information you give will be treated with confidentiality and at no instance will it be used for any other purpose other than for this project. Your assistance will be highly appreciated.

I look forward to your prompt response.

Yours Faithfully,

Lucy Chetalam.
SECTION A: GENERAL INFORMATION

1. What is your age?
   □ 18-24 years old
   □ 25-44 years old
   □ 45-64 years old
   □ 65+ years old

2. What is your gender?
   □ Male
   □ Female
   □ don’t want to indicate

3. Where do you live?
   □ Within Nairobi
   □ Outside Nairobi

4. Where do you work?
   □ Industry or public sector
   □ Self employed
   □ Academia or research
   □ I'm student
   □ I'm unemployed or retired
   □ Housework or childcare

5. Do you study or work in a field related to IT, computer engineering, or computer science?
   □ Yes
   □ No

6. Which phone do you currently use?
   □ Android
   □ BlackBerry
   □ iPhone / iOS
   □ Windows Mobile
   □ Others
   □ I don’t have a smartphone

SECTION B

Authentication Factors used by Mobile Money Services

7. How often do you transact with MPESA in a day?
8. How important is data protection and information security on MPESA for you?
   - Not so important
   - Slightly important
   - Very important
   - Extremely important (I would do every possible thing for this)

9. How much do you trust the following techniques for securing your smartphone and protecting your MPESA data?

<table>
<thead>
<tr>
<th>Technique</th>
<th>I fully trust</th>
<th>I trust</th>
<th>I do not trust</th>
<th>I fully do not trust</th>
<th>I don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iris recognition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(recognizing the iris of your eye and using it to authenticate you and secure your information)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password or PIN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Face recognition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(recognizing your face and using it to authenticate you and secure your information)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(recognizing your fingerprint and using it to)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
authenticate you and secure your information)

<table>
<thead>
<tr>
<th>Ear recognition (recognizing your ear and using it to authenticate you and secure your information)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice recognition (recognizing your voice and using it to authenticate you and secure your information)</td>
</tr>
</tbody>
</table>

10. MPESA uses 4-digit PIN as a security measure. Do you think this is sufficient?
   Yes [ ] No [ ]

11. Are you aware of any security features that MPESA can adopt?
   Yes [ ] No [ ]

12. Which authentication document do you use when transacting with MPESA?
    ________________________________________

13. Do you remember the 4-digit Start Key that you used when registering for MPESA?
    Yes [ ] No [ ]

14. Do you remember the MPESA secret word that you used when registering for MPESA?
    Yes [ ] No [ ]

15. If yes, have you ever used it when calling MPESA Customer Support?
    Yes [ ] No [ ]
    If no, kindly state explain _____________________________________________________________
    _____________________________________________________________
16. Have you ever shared your MPESA PIN or MPESA secret word?
   Yes ☐ No ☐

   If yes, kindly state the reasons why: ____________________________

17. Do you think your MPESA PIN can be easily guessed?
   Yes ☐ No ☐

18. Do you think adding another security feature to the MPESA PIN will improve MPESA security?
   Yes ☐ No ☐

19. Which combination of authentication systems would you be willing to use for additional MPESA security?
   □ Iris recognition and PIN
   □ Fingerprint and PIN
   □ Ear recognition and PIN
   □ Face recognition and PIN
   □ Iris recognition and fingerprint
   □ Face recognition and iris recognition
   □ I don’t care, as long as it’s not complicated

   b) What are the advantages of the selected choice above?
   __________________________________________________________________________
   __________________________________________________________________________

20. List some of the disadvantages of the biometrics you have identified above?
   __________________________________________________________________________
   __________________________________________________________________________

21. What do you understand by the term biometrics?
   _________________________________________________________________
   _________________________________________________________________

22. Which type of biometrics have you used before?
   □ fingerprint
   □ iris
   □ hand
23. Do you think adding biometrics will improve MPESA security?

Yes ☐ ☐ No ☐ ☐

24. Have you ever used voice biometrics in any system?

Yes ☐ ☐ No ☐ ☐

25. What do you understand by the term Voice biometrics?

________________________________________________________________________

26. Do you think voice biometrics is the most secure type of security for MPESA?

Yes ☐ ☐ No ☐ ☐

27. Would you easily use voice biometrics when transacting using MPESA?

Yes ☐ ☐ No ☐ ☐ Maybe ☐ ☐ Sure ☐ ☐

28. Give reasons to your answer above.

________________________________________________________________________

29. Would you prefer to use PIN and Voice security together?

Yes ☐ ☐ No ☐ ☐

30. Do you think use of voice biometrics would slow down the MPESA process?

Yes ☐ ☐ No ☐ ☐

31. What is your opinion on voice biometrics?

________________________________________________________________________

SECTION B

MPESA Fraud

32. Have you ever been a victim of MPESA fraud?

Yes ☐ ☐ No ☐ ☐

33. Briefly describe the scenario which you were defrauded?

________________________________________________________________________

34. Did you reveal your MPESA PIN before you were defrauded?

Yes ☐ ☐ No ☐ ☐
35. Are you aware of the fraud techniques used in your area?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If yes, which ones

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Reversal of erroneous transactions:
- Scam Messages
- Unauthorized SIM Swap
- Identity Theft
- Insider theft

Mention Others if any:

_________________________________________________________________________________

36. Did you reveal your MPESA PIN before you were defrauded?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

37. If yes, what means did the fraudster use?

- [ ] phone calls
- [ ] SMS messages
- [ ] email

Have you ever been a victim of:

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Reversal of erroneous transactions:
- Scam Messages
- Unauthorized SIM Swap
- Identity Theft
- Insider theft
SECTION C
Impact of Implementing a Voice Biometric Feature on Mobile Transactions

38. How long did it take you to register for MPESA services?

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than two minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Less than five minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Less than ten minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>More than ten minutes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

39. Did you get information or assistance on how to register your voice on MPESA?

Yes ☐ No ☐

40. How many voice samples did you submit?

☐ 1  ☐ 2  ☐ 3  ☐ More than 4

41. How fast did it take for you to perform a MPESA transaction using the voice

security?  ☐ Instant  ☐ not very fast  ☐ slow

42. Have you encountered any problem when transacting with the voice security

feature in MPESA?

Yes ☐ No ☐

43. If yes, kindly describe

______________________________________________________________________

44. What was your general view about this feature?


Using the grid below, please tick in the appropriate column which best expresses your view.

**Strongly Agree 5, Agree 4, Not sure 3, Disagree 2, Strongly disagree 1**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>This feature has improved MPESA service delivery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>MPESA has become more secure with this feature</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Has this feature made MPESA easy to use?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>I can effectively make a transaction with this feature</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>I feel comfortable using my voice when doing MPESA transactions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>It was easy to learn to use this system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>The system gives me error messages that clearly highlight where the mistakes or problem is</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>The information such as alert messages (success, error) provided by the system are clear and understandable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>The information provided by the system is easy to understand, such as what actions I’m to take</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>The organization of information on the screen is clear</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>The system has an attractive user interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>I like using the interface of this system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>This system has all the functions and capabilities I expect it to have</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.</td>
<td>The system saves a lot of time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>Overall, I am satisfied with this system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>