



**UNIVERSITY OF NAIROBI**  
**COLLEGE OF BIOLOGICAL AND HEALTH SCIENCES**  
**SCHOOL OF COMPUTING AND INFORMATICS**

**SECURING MOBILE MONEY PAYMENT AND TRANSFER APPLICATIONS  
AGAINST SMISHING AND VISHING SOCIAL ENGINEERING ATTACKS**

**CHEBII PAMELA JEPKORIR**

**P53/35044/2019**

**Supervisor: DR. CHRISTOPHER KIPCHUMBA CHEPKEN**

**Research Project submitted in partial fulfillment of the requirements for  
the award of Master of Science in Distributed Computing Technology of  
University of Nairobi**

## DECLARATION

### DECLARATION BY THE STUDENT

I declare that this research project is my original work and has never been submitted to or used as part of the award of a degree or any other Certificate in any institution of higher learning or any institution approved by the Ministry of Education, Science and Technology.



22/08/2021

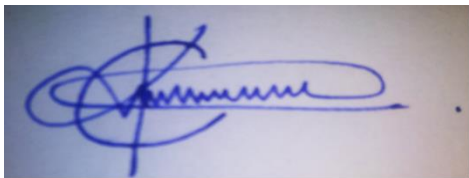
Sign: ..... Date: .....

**CHEBII PAMELA JEPKORIR**

**P53/35044/2019**

### DECLARATION BY THE SUPERVISOR

I declare that Chebii Pamela Jepkorir was under my guidance and supervision all through this research. This research project has been submitted with my approval as the University Supervisor.



Sign: ..... Date: .....23/08/2021.....

**DR. CHRISTOPHER CHEPKEN:**

Senior Lecturer,

University of Nairobi

## **ABSTRACT**

Social Engineering is the science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction, the persuasion, or the request involves a computer-related entity. Social engineering threats are the biggest threats facing cybersecurity because they exploit the natural human tendency to trust. Human-based social engineering requires a person-to-person interaction to achieve an objective. Mobile money users are target to most criminals. Smishing is a form of phishing where someone tries to trick a victim into giving their private information via a text message. A vishing attack is a type of criminal phone fraud that uses voice messages to obtain personal information or money from victims. Consumer-based fraud represents the most prevalent form across all stages of the mobile money services operation, where offending is enabled by a lack of system-based checks and awareness. Current mobile money transfer and payment applications design does not mitigate cybersecurity risks and specifically social engineering. This study establishes the gap and proposes a design that will mitigate these risks. The literature review describes the social engineering frameworks, defensive techniques against social engineering in mobile money, and establishes the knowledge gaps that need to be filled. A descriptive research design with a qualitative approach is employed in this study. Open-ended questionnaires were used to collect the data. Results of the analysis show that 66% of the respondents have experienced social engineering attacks either through phone or SMS. The effects of Social Engineering lead to the inability to recover money once sent. A mobile application prototype called SAFECASH that can analyze and hold unconfirmed transactions, blacklist suspected contacts and lock suspected transactions is implemented and tested.

## **ACKNOWLEDGMENT**

I wish to thank all those who have contributed towards the success of this project in one way or another.

My utmost gratitude goes to my supervisor Dr. Christopher Chepken whose contribution and constructive criticism shaped my academic pursuit and provided guidance to enable the completion of this project. Through him, I have experienced true research. My appreciation also goes to the panel members Dr. Wanjiku, Christine Ronge, Dr. Miriti, and Dr. Mburu whose positive criticism shaped this research.

My sincere appreciation also goes to my parents Joseph Kipsang Chebii and Esther Jepchirchir Chebii who diligently laid the foundation of my education giving it all it takes to ensure I get the best education. I am and will forever be grateful to my dear husband Mark Kimitei for always believing in me and for doing everything possible to ensure that I achieve this feat. May God bless you.

My heartfelt gratitude also goes to my in-laws Mr. and Mrs. Philip Kimaiyo for their encouragement, prayers, and financial support that has enabled me to complete this program. May God bless you.

I also from the bottom of my heart wish to thank my nanny Vivicah for always supporting me and for looking after my daughter Verona even as I spent long hours studying. Thank you for being understanding.

## **DEDICATION**

I dedicate this research to God Almighty my source of inspiration, knowledge, and understanding. I also dedicate this work to my parents and my siblings who have always been supportive throughout my education and especially my father who would sacrifice everything possible to ensure that I achieve the best education. Unfortunately, he passed on in May 2021 when I was going on with this research. I also dedicate this work to my loving husband Mark Kimitei and my lovely daughter Verona Jerop for their love, patience, and understanding. Thank you and may almighty God bless you.

## Table of Contents

<b>DECLARATION</b> .....	ii
<b>ABSTRACT</b> .....	iii
<b>ACKNOWLEDGMENT</b> .....	iv
<b>DEDICATION</b> .....	v
<b>List of Figures</b> .....	ix
<b>List of Tables</b> .....	x
<b>CHAPTER ONE:</b> .....	1
<b>INTRODUCTION</b> .....	1
<b>1.1 Background</b> .....	1
<b>1.2 Problem Statement</b> .....	4
<b>1.3 Aims and objectives of the study</b> .....	4
1.3.1 General objective .....	4
1.3.2 Specific objectives .....	5
<b>1.4 Justification</b> .....	5
<b>CHAPTER TWO:</b> .....	6
<b>LITERATURE REVIEW</b> .....	6
<b>2.1 Introduction</b> .....	6
<b>2.2 Social Engineering Attacks</b> .....	6
2.2.1 Forms of Social Engineering Attacks .....	7
2.2.2 Social Engineering Attack Ontological Model .....	8
2.2.3 Social Engineering Attack Framework .....	9
<b>2.3 Social Engineering Risk Assessment Framework (SERA)</b> .....	10
<b>2.4 The Social Engineering Defensive Framework (SEDF)</b> .....	11
<b>2.5 Defensive Techniques in mobile money</b> .....	13
2.5.1 Hakikisha .....	13
2.5.2 Creating User Awareness .....	13
2.5.3 iVisher: Real-Time Detection of Caller ID Spoofing .....	14

2.5.4 PayProtect .....	14
2.5.5 Blockchain for mobile money traceability .....	14
<b>2.6 The Knowledge Gap .....</b>	<b>15</b>
<b>2.7 Conceptual Design .....</b>	<b>17</b>
<b>2.8 Chapter Summary .....</b>	<b>18</b>
<b>CHAPTER THREE: .....</b>	<b>19</b>
<b>METHODOLOGY .....</b>	<b>19</b>
<b>3.1 Introduction .....</b>	<b>19</b>
<b>3.2 System Development Methodology .....</b>	<b>19</b>
<b>3.3 Research Design .....</b>	<b>22</b>
<b>3.4 Research Approach .....</b>	<b>22</b>
3.4.1 Qualitative Research .....	23
<b>3.5 Population and Sampling .....</b>	<b>23</b>
3.5.1 Study Population .....	24
3.5.2 Sampling .....	25
<b>3.6 Data Collection .....</b>	<b>26</b>
3.6.1 Questionnaires .....	26
<b>3.7 Reliability and Validity of Research Instruments .....</b>	<b>27</b>
<b>3.8 Data Analysis .....</b>	<b>27</b>
<b>3.9 Ethical Consideration .....</b>	<b>28</b>
<b>3.10 Chapter Summary .....</b>	<b>29</b>
<b>CHAPTER FOUR .....</b>	<b>30</b>
<b>RESULTS, FINDINGS, AND DISCUSSIONS .....</b>	<b>30</b>
<b>4.1 Introduction .....</b>	<b>30</b>
<b>4.2 Response Rate .....</b>	<b>30</b>
<b>4.3. Mechanisms used by social engineers to conduct social engineering attacks .....</b>	<b>30</b>
4.3.1 Social Engineering by SMS. ....	30
4.3.2 Social engineering by phone call.....	32

<b>4.4 Challenges in Mobile Money Applications .....</b>	<b>34</b>
<b>4.5 Defensive Techniques against Social engineering attacks .....</b>	<b>35</b>
<b>4.6 Systems Analysis and Requirements Specification.....</b>	<b>36</b>
4.6.1 Requirements specification .....	37
<b>4.7 System Design.....</b>	<b>40</b>
4.7.1 Logical Database Design .....	40
4.7.2 Input design.....	43
4.7.3 Output Design .....	45
4.7.4 Level 0 DFD.....	45
4.7.5 Use Case Narration.....	47
<b>4.8 System implementation .....</b>	<b>50</b>
4.8.1 Testing .....	51
4.8.2 Proof of concept .....	55
<b>4.9 Discussion .....</b>	<b>57</b>
<b>4.10 Chapter Summary .....</b>	<b>58</b>
<b>CHAPTER FIVE: .....</b>	<b>59</b>
<b>CONCLUSION AND RECOMMENDATIONS .....</b>	<b>59</b>
<b>5.1 Introduction.....</b>	<b>59</b>
<b>5.2 Conclusion .....</b>	<b>59</b>
<b>5.3 Limitations of the Study .....</b>	<b>60</b>
<b>5.4 Achievements .....</b>	<b>60</b>
<b>5.5 Recommendations .....</b>	<b>61</b>
<b>REFERENCES .....</b>	<b>62</b>
<b>APPENDICES.....</b>	<b>67</b>
<b>APPENDIX 1: QUESTIONNAIRE .....</b>	<b>67</b>



## **List of Figures**

<b>Figure 1: Classifications of SE Attacks (Salahdine &amp; Kaabouch, 2019) .....</b>	<b>7</b>
<b>Figure 2: Social Engineering Attack Ontological Model (Mouton, Leenen, et al., 2014) .....</b>	<b>9</b>
<b>Figure 3: Social Engineering Attack Framework (Mouton, Malan, et al., 2014) .....</b>	<b>10</b>
<b>Figure 4: SERA and OCTAVE – A (Abeywardana et al., 2016) .....</b>	<b>11</b>
<b>Figure 5: Social Engineering Defensive Framework by Thomas in (Gardner &amp; Thomas, 2014). .....</b>	<b>12</b>
<b>Figure 6: Conceptual Design .....</b>	<b>17</b>
<b>Figure 7: Waterfall model source: (Sparrow, 2011) .....</b>	<b>20</b>
<b>Figure 8: Level 0 DFD .....</b>	<b>46</b>
<b>Figure 9: subscriber use case diagram .....</b>	<b>48</b>
<b>Figure 10: administrator use case diagram .....</b>	<b>49</b>
<b>Figure 11: Agent Use Case diagram .....</b>	<b>50</b>

## **List of Tables**

<b>Table 1: Study population</b> .....	<b>24</b>
<b>Table 2: Functional requirements</b> .....	<b>38</b>
<b>Table 3: non-functional requirements</b> .....	<b>39</b>
<b>Table 4: Members Table- To store subscribers' details</b> .....	<b>40</b>
<b>Table 5: Deposits- To store transaction details</b> .....	<b>41</b>
<b>Table 6: Held time- To store details on the amount of time a transaction is held</b> .....	<b>42</b>
<b>Table 7: Password Resets- To store details on password resets, to provide a new password to the customer</b> ....	<b>43</b>

# **CHAPTER ONE:**

## **INTRODUCTION**

### **1.1 Background**

Cyber security is a term that stands for the steps taken to protect resources in the network from being accessed, modified, or tampered with by unauthorized users. (Edgar & Manz, 2017). It is the act of making cyberspace safe from damage or threat. According to Edgar & Manz (2017), cyberspace is the abstruse construct made from combining digital hardware, data, and people who interrelate with tangible electronic resources and generate and use the processed data the raw data contains. Humans play a major role in cyberspace. Edgar & Manz (2017) further poses that users are usually targeted against their cognitive behavior through social engineering methods and therefore they are the most vulnerable link in security.

The collection of techniques through which people are influenced to give out specific data or forced to behave in a certain manner represents Social Engineering (Serban & Serban, 2014). Human-based and computer-based are the two types of social engineering attacks (Sadiku et al., 2016). To achieve an objective in a human-based social engineering attack, person-to-person interaction is required. This research focused on social engineering in mobile money. The specific social engineering attacks that were focused on in this research are smishing and vishing attacks.

Smishing is a type of phishing attack where a victim is tricked into providing their private information through a text message (Deloitte, 2019). It is a form of social engineering attack that motivates users to act depending on the target for example clicking on a link or behaving accordingly (Soykan & Bagriyanik, 2020). Smishing attacks' success materializes from the reality that victims' mobile phones can be always carried and mechanisms for checking the authenticity of the SMS do not exist (Soykan & Bagriyanik, 2020).

Vishing on the other hand is the perpetrator's act of committing fraud by getting access to the subscribers' information on finances and personal information through the telephone system (RSA, 2015). It refers to phone phishing to manipulate people to provide their sensitive information for verification for example calls from a bank (Salahdine & Kaabouch, 2019). An individual's trust in telephone services is utilized in Vishing.

Mobile money refers to a service in which financial services are accessed with the use of mobile phones (Donovan, 2011; GSMA, 2010). It describes computerized financial services performed using a mobile phone (Subia & Martinez, 2014). The user can deposit, withdraw or send money with the use of a mobile phone. Banks and mobile network operators are already using mobile money to provide a way of storing and accessing money digitally to millions of unbanked consumers.

Mobile banking, mobile payments, and mobile transfers are the three main services provided by mobile money (Subia & Martinez, 2014). This research focused on mobile money transfers and mobile payments. Mobile money transfer is the process of moving values made from a mobile account, accumulates to a mobile account, and/or is started off using a cellphone (GSMA, 2010). A mobile device is involved in executing and confirming payment in the transfer of funds in return for goods or services in mobile payment (Raina, 2015). During the purchase of goods a mobile phone is used to handle the transfer of credit instead of depending on bank cards and cash in mobile payment (Narayan, 2013).

Tremendous development in the use of mobile phone services continues to be witnessed in the Kenya ICT sector. The operational SIM Cards subscriptions count was 59.8 million against 57.0 million customers reported in June 2020 according to the Communications Authority of Kenya statistics report as of the end of September, 30<sup>th</sup> 2020. The subscriptions resulted in SIM usage by 125.8 % between July and September 2020 (Authority-Kenya, 2020). With the increase in mobile

phone usage, the demand for mobile money services by mobile phone users also increases. As of September, 30<sup>th</sup> 2020, there were 31.8 million and 245, 124 active mobile money subscribers and agents respectively (Authority-Kenya, 2020).

Safaricom and Vodafone's MPESA in Kenya initially made mobile money popular in 2007 (Subia & Martinez, 2014). The mobile money industry has increasingly expanded, specifically in developing countries in Africa and South Asia such as India, Bangladesh, and Pakistan since then. The provision of less expensive and reliable services in finance by the growing population who previously did not have bank accounts has been facilitated by services provided by mobile money (Mudiri, 2012). However, the expansion in mobile money comes with a fair share of fraud cases. According to the Financial Analysis Report, 2020, vulnerabilities and impact data indicated that within Africa there is an increase in cases of fraud relating to services provided by mobile money (European Union, 2020). The report further indicated that any of the following stages can be used to exploit mobile money services;

- 1) When money is deposited into an account
- 2) When money is transferred between accounts
- 3) When money is withdrawn from an account, with both customers and agents having opportunities to commit fraud

Potential frauds in mobile money can be classified as either transactional, channel, or internal fraud (Gilman & Joyce, 2012). According to the authors, the main players who need to be examined in mobile fraud risks are the subscriber which translates to transactional risk, the agent which is also referred to as risk associated with the channel, and the internal risks brought about by the employees. This study focused on the customer (transactional risk) and in particular how fraudsters through social engineering methods steal money from mobile money users.

Being a highly dynamic platform, there is a need to understand the human factor when it comes to mobile money payments and transactions. The victory and defeat in securing and protecting information, businesses systems, and services are impacted hugely by the human element (Metalidou et al., 2014). This research established the social engineering methods used by fraudsters to influence unsuspecting mobile money users.

## **1.2 Problem Statement**

Despite the Mobile Network Operators (MNO) working hard to ensure the security of the mobile money application in ensuring financial inclusion for users who cannot access banking services, fraud, and other criminal activities are carried out using mobile money services (Mudiri, 2012). Refusal to refund the money by unintended recipients has led to loss from wrong transfers. Consumer-based fraud represents The most extensive form of fraud across all mobile money services stages is the consumer-based fraud, where lack of authentication by the system and awareness contributes to offenses (European Union, 2020).

Current mobile money transfer and payment applications design does not mitigate cybersecurity risks and specifically social engineering. This study aimed to establish the gap and propose a design that will mitigate these risks.

## **1.3 Aims and objectives of the study**

This part gives the objectives of the study.

### **1.3.1 Main objective**

The study aimed to develop a mobile application prototype for mobile money payment and transfer platforms to mitigate human-based social engineering risks in mobile money.

### **1.3.2 Specific objectives**

- i. To evaluate the effectiveness of existing platforms in use by mobile money and transfer applications that counter the effects of social engineering.
- ii. To identify gaps in the current mobile money applications which facilitate social engineering.
- iii. To design a mobile money application model factoring in the current gaps facilitating social engineering to mitigate human-based social engineering risks in mobile money.
- iv. To implement and test a mobile application model.

### **1.4 Justification**

Humans are the most vulnerable link in information security. Different convincing methods are used to make people perform requests which are sensitive in social engineering attacks by targeting this vulnerability (Salahdine & Kaabouch, 2019). In mitigating fraud in mobile money services, specific steps can be taken by providers to reduce the possibility and monitor the occurrence of some of the more common types of fraud and manage their effects (Mudiri, 2012).

According to GSMA (2019), when funds are fraudulently lost by mobile money users, it can result in loss of confidence in services provided by mobile money, therefore, may undo the achievements in financial inclusion by forcing people to reverse to cash hence sabotaging the realization of global development goals (Farooq, 2019). This study aimed to identify gaps that facilitate social engineering attacks in current mobile money applications and develop a mobile application model for mobile money transfer platforms to mitigate social engineering risks in mobile users.

## **CHAPTER TWO: LITERATURE REVIEW**

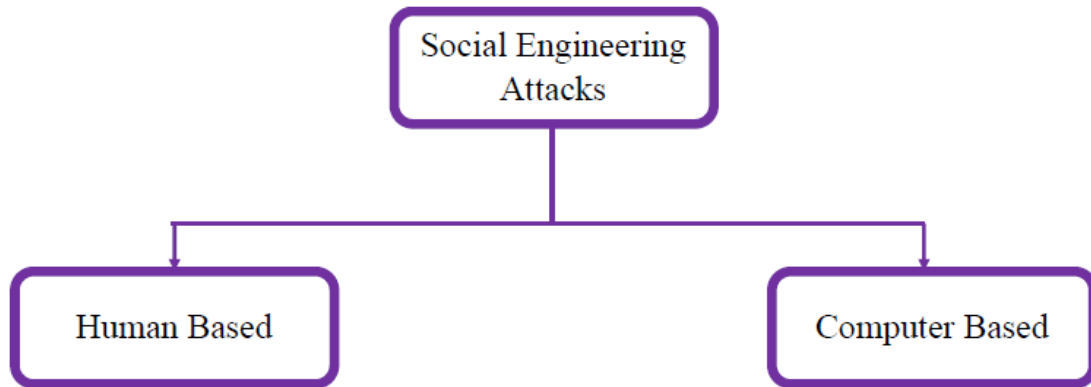
### **2.1 Introduction**

Social Engineering is the act of convincing people or organizations to act as per a specific demand from a perpetrator by use of social interaction where either the social interaction, the manipulation, or the demand concerns an electronic object (Mouton, Leenen, et al., 2014). Influence and persuasion are used in social engineering to deceive people into believing that the social engineer is someone he is not by convincing them (Mitnick, 2002). Social engineering affects cyber security even without considering the presence of strong firewalls, systems for detecting and preventing intrusion or antiviruses (Salahdine & Kaabouch, 2019). Human beings are the most vulnerable connection in the security ecosystem because computers and technologies are less trusted by people compared to other humans (Edgar & Manz, 2017).

### **2.2 Social Engineering Attacks**

The two classifications of attacks in Social Engineering are human and software-based (Salahdine & Kaabouch, 2019). The perpetrator conducts the attack himself by associating with the victim to acquire the information desired in human-based attacks. Computers or mobile phones are used to get information from the targets in order to perform software-based attacks (Sadiku et al., 2016; Salahdine & Kaabouch, 2019).





*Figure 1: Classifications of SE Attacks (Salahdine & Kaabouch, 2019)*

### **2.2.1 Forms of Social Engineering Attacks**

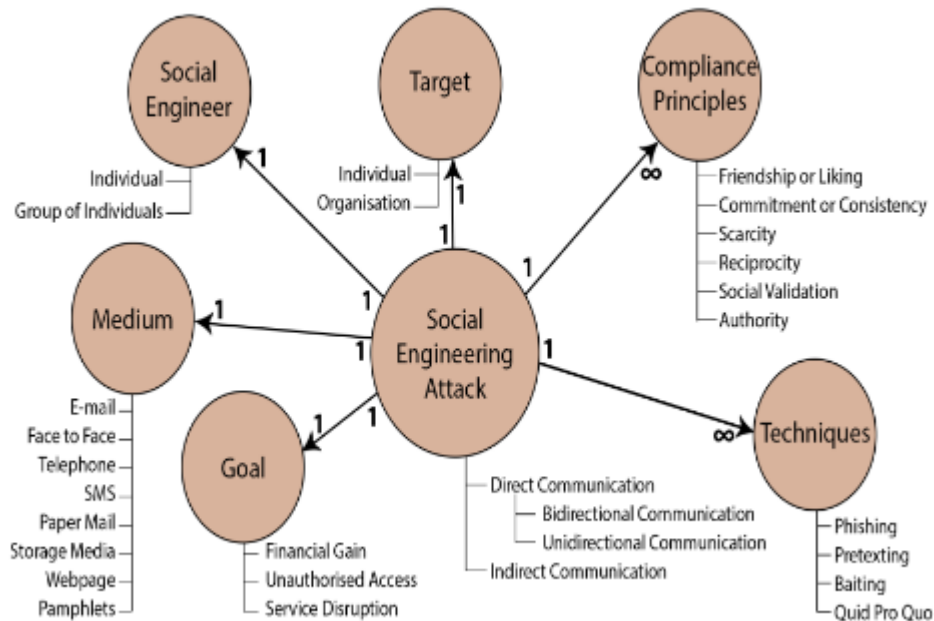
Salahdine & Kaabouch (2019) classify social engineering attacks into the following types:

- 1) Phishing attacks- This type of attack uses phone calls or emails to fraudulently acquire information that is personal and confidential from the victims (Salahdine & Kaabouch, 2019). Sensitive and confidential information is obtained by attackers by misleading victims. The categories of phishing attacks include spear, whaling, vishing, interactive voice response, Smishing, and business email compromise phishing (Grimes, 2017).
- 2) Baiting Attacks - Users are invited to tap on links to acquire priceless items in baiting attacks. Electronic devices which are not secured such as storage devices or USB containing viruses that act like Trojan horses can be exploited in a location where they can be found by victims (Salahdine & Kaabouch, 2019).
- 3) Fake Software attacks – In this type of attack victims are made to believe that fake websites are familiar and legitimate. The perpetrator gets the targets’ details to use in a legitimate website when the victim enters the actual login information into the illegitimate website and can use the information to access other websites such as bank accounts that are online (Salahdine & Kaabouch, 2019).

- 4) Reverse social engineering- a network problem is claimed to be solved by the attacker. It involves making a problem happen for example making the network suddenly fail; publicizing that no one can solve that issue apart from the attacker; fixing the issue and at the same time acquiring the information needed and exiting while leaving no evidence (Salahdine & Kaabouch, 2019).
- 5) Phone or Email Scams Attacks - A phone or email is used by the attacker to contact the victim seeking certain information or assuring the victim stuff for free to manipulate the victim into giving personal information or breaching security (Salahdine & Kaabouch, 2019).
- 6) Pretexting attacks - Victim's personal information is acquired by inventing convincing and fake scenarios in pretexting attacks (Salahdine & Kaabouch, 2019). Allegations that cause the target to have confidence in the perpetrator and trust them are used. Making phone calls, sending emails, or physical electronic devices are used to perform the attack.

### **2.2.2 Social Engineering Attack Ontological Model**

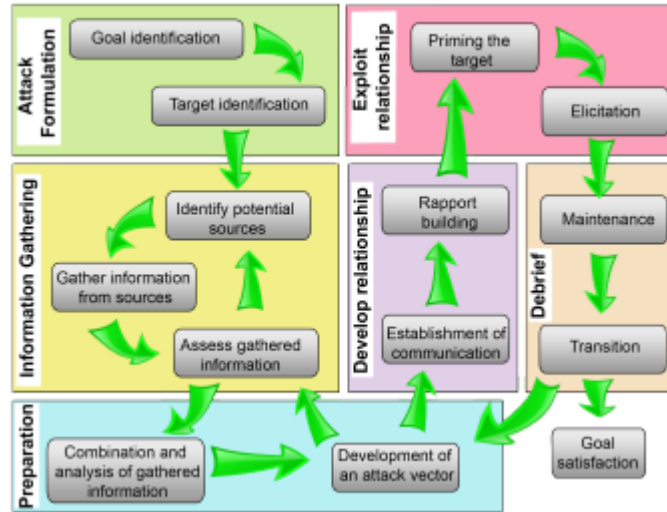
Mouton, Leenen, et al. (2014) proposed an Ontological model made up of the authors' classification of Social Engineering attacks from several other taxonomies. The taxonomies that contributed to the Ontological model include; Harley, Laribee, Ivaturi and Janczewski, Mohd et al., and Tetri and Vuorinen taxonomies (Mouton, Leenen, et al., 2014). The model was based on the argument that taxonomy is too narrow to explain Social Engineering and Social Engineering attacks adequately. The Ontological model was as a result of the authors' description of an attack in social engineering whereby the attack has a single perpetrator; a single victim being targeted; a single or more Compliance Principles; a single or numerous methods; a single Medium; and a single Goal (Mouton, Leenen, et al., 2014).



*Figure 2: Social Engineering Attack Ontological Model (Mouton, Leenen, et al., 2014)*

### 2.2.3 Social Engineering Attack Framework

Kevin Mitnick's original attack cycle for social engineering is used as the background for Social Engineering Attack Framework by (Mouton, Leenen, et al., 2014). The proposed framework for attack reviewed the weaknesses in the attack cycle by Mitnick and enhancement of the weaknesses are mirrored. The phases proposed by Mitnick (Mitnick, 2002) include information gathering, forming a sense of trust, exploiting the victim's trust, and utilizing the obtained information.

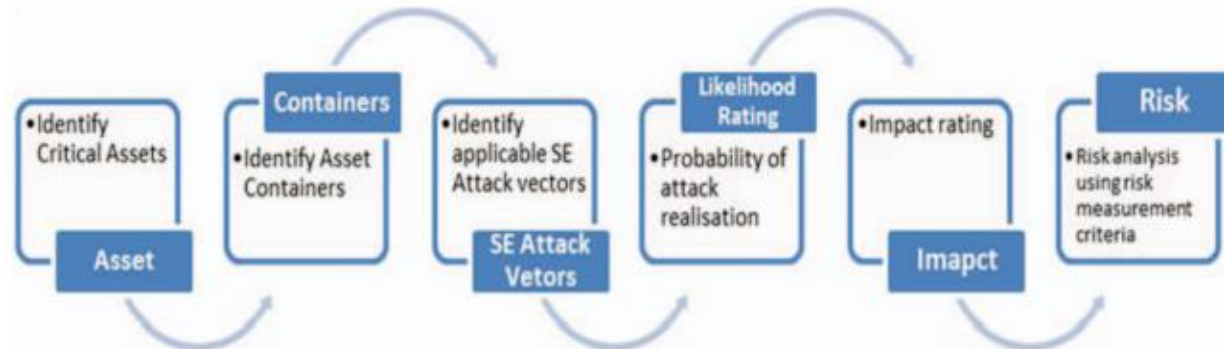


**Figure 3: Social Engineering Attack Framework (Mouton, Malan, et al., 2014)**

An application of the combination of the ontological model (Mouton, Leenen, et al., 2014) proposed previously and attack framework is explored in form of life scenarios. Each proposed attack framework is exhaustively explained.

### 2.3 Social Engineering Risk Assessment Framework (SERA)

Abeywardana et al. (2016) introduced the SERA which can be utilized in supporting security assessment frameworks that exist. The security information acquired previously can be made use of in its employment to give a more detailed risk evaluation of an organization. The matching vector for an attack in social engineering for every container can be pinpointed (though to have social engineering attack vectors all containers are not a must to be available) (Abeywardana et al., 2016).



*Figure 4: SERA and OCTAVE – A (Abeywardana et al., 2016)*

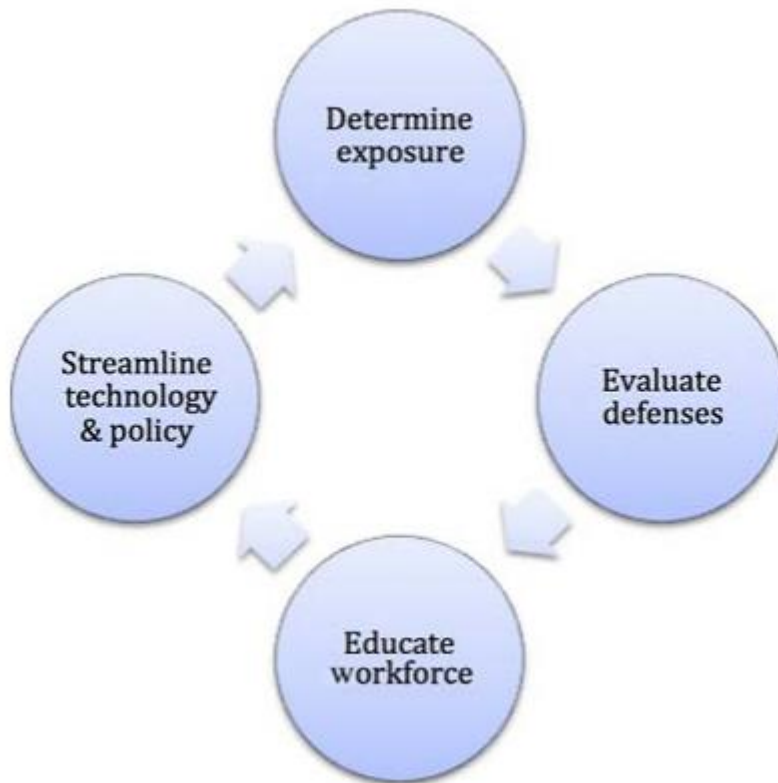
Deriving a risk assessment by identifying applicable social engineering attack vectors is the concept introduced in SERA. The authors describe SERA as a pliable concept that can be easily deployed and can be employed in developing risks in social engineering that present huge threats to an organization.

#### **2.4 The Social Engineering Defensive Framework (SEDF)**

Social Engineering Defensive Framework (SEDF) was created by Valerie Thomas to assist organizations in preventing attacks in social engineering at the business degree (Gardner & Thomas, 2014). The main stages for the protection against an attack are outlined in SEDF. The stages have no relationship with each other and organizations can perform in an order that matches their priorities for instance(Gardner & Thomas, 2014). According to the author, the Social Engineering phases are;

- 1) Determining exposure - Available resources and other websites are viewed through the eyes of a perpetrator in this phase. Technical support forums, social media, and popular hacking websites are other fields to be focused on.
- 2) Examining Defenses - Examining employee resistance and how they react to mimicked attacks is utilized in this stage.

- 3) Educating Employees – Training employees on how attacks are conducted and their repercussions are involved in this stage. Thomas (2014) further poses that in social engineering education disintegrating the scenarios for the attack is an important phase. Moreover, to build a clear understanding of the process it is important to show the listeners the way each element of data was acquired and the way it can be utilized in the attack.
- 4) Improving existing technology and policy –configuration changes are used to improve beneficial technologies for defense that probably exist around you.



*Figure 5: Social Engineering Defensive Framework by Thomas in (Gardner & Thomas, 2014).*

## **2.5 Defensive Techniques in mobile money**

### **2.5.1 Hakikisha**

Hakikisha is a Swahili term meaning “to ascertain, confirm or verify” (Buku, 2015). Hakikisha is a service that enables the confirmation of the intended recipient’s name by the sender of funds before completion of an M-Pesa transaction (Safaricom, 2021b). It also allows the confirmation of the agent’s name when money is being withdrawn from the M-PESA account. Moreover, the service is not only available to transfer but also Payments and M-PESA deposits by the agents. According to Safaricom (2021b), after going to MPESA and sending money a notification containing the recipient's name will be shown on the screen. Any letter or number is sent within 25 seconds in order to stop a wrong transaction. Pressing cancel does NOT abort the transaction.

Safaricom has the advantage of confirming the receiver before sending money but still does not solve fraud in mobile money. According to research done by Otieno in 2020, Hakikisha still facilitates fraud in mobile money. “A perpetrator who wants to con someone will only need to guess random Safaricom numbers, acquire their full names from Hakikisha, and call or text them” (Otieno, 2020). This makes it easier for social engineers to convince users to send them money since they already have the details.

### **2.5.2 Creating User Awareness**

According to Safaricom's (2020) Sustainable Business Report, awareness of the social engineering attacks used by fraudsters to exploit M-PESA users continues to be raised by Safaricom. Safaricom in 2020 was using roadshows and campaigns in local languages in both digital and print media to raise awareness (Peter, 2020). Jitambulisha is a service that allows Safaricom subscribers to register their voice and use it for accessing various services by smoothly calling 100, 234, Or 200 (Safaricom, 2021a).

“Fraud texts or calls will usually ask you to do something like call back a certain number, share your ID number, urgently remind you to send money to a certain number, or send money for an ‘emergency’” (Safaricom, 2021a). Safaricom is promoting awareness by encouraging its users to keep themselves protected by reporting fraudulent messages or call by forwarding the sender's number to 333.

### **2.5.3 iVisher: Detection tool**

iVisher is a tool that checks whether a tool that checks if a phone number has been altered through spoofing and therefore helping in mitigating voice vishing attacks. The caller ID of the approaching calls is verified by iVisher and formally reported caller IDs are blocked by carrying out accessibility examination to show the name of a dubious approaching call (Song et al., 2014). In handling the messages of accessibility examination of the callers that try to authenticate the real caller ID and the name displayed, the examination uses a gateway that understands the real caller ID of the phone call.

### **2.5.4 PayProtect**

PayProtect is an automated escrow system that uses a USSD code (PayProtect, 2021). PayProtect protects both buyers and sellers. The money is stored in an escrow account whereby the buyers' money is safe till they receive items and can reverse payments in case the items are not delivered. Sellers on the other hand are assured of their payments once they deliver. Buyers and sellers can access PayProtect using the USSD code \*483\*151# (Safaricom).

### **2.5.5 Blockchain for mobile money traceability**

Agbezoutsi et al. (2019) show how blockchain can be used to develop trust between mobile money users in the mobile money environment. They propose a model for keeping transactions in blockchain so that data and events that can be traced and are also transparent is created, therefore, a



tool for fewer trust collaborations is yielded to fast developing disruptors of the industry (Agbezoutsu et al., 2019). To get to the blockchain the transaction is carried through USSD and then it is looked into and stored in the blockchain.

## **2.6 The Knowledge Gap**

From the literature, it is evident that social engineers are well organized in their attacks making it difficult for them to be caught and prosecuted. According to Mitnick & Thomas (2002), the social engineer can obtain information from people with or without the use of technology. Research done by Star investigative journalist in Kenya on 20<sup>th</sup> January 2021 showed that the conmen pose as Safaricom staff then make users give out their M-Pesa details through questions that guide them to do so (Vidija, 2021).

The Safaricom Hakikisha does not guarantee security but instead creates a gap for social engineers. Fraudsters can guess a random array of numbers then try sending money to an MPESA user and Hakikisha will provide the full names of the user.

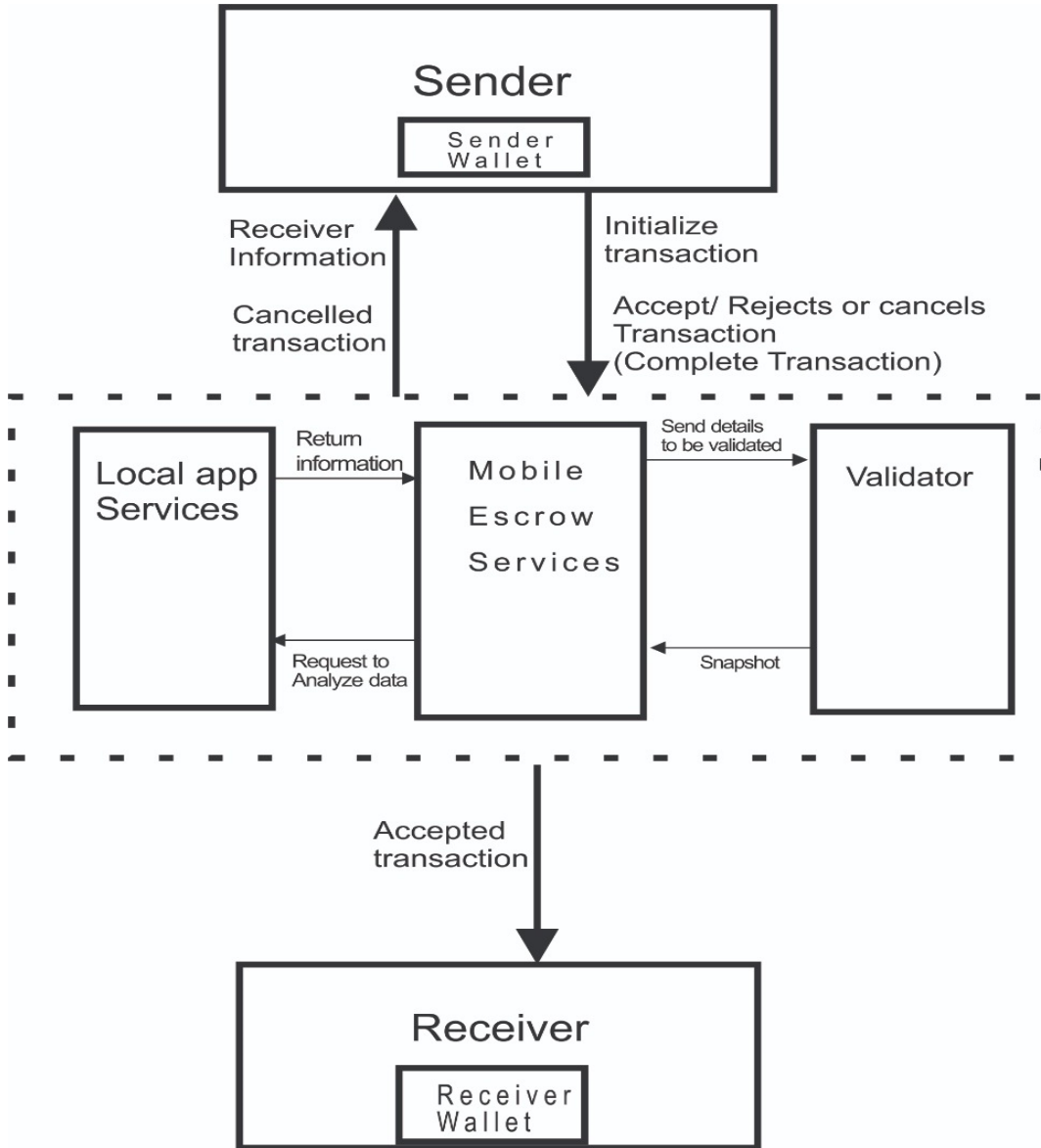
Researchers in the field of security have warned that the success of education on attacks in social engineering and the risks related is largely limited (Song et al., 2014). The awareness created by Safaricom helps the users to understand that fraudsters exist but they can't solve the problem of people accidentally sending money to those numbers. In this case, once the money has been sent and the receiver withdraws the money immediately the sender won't be able to get his/her money back.

iVisher detection tool does not protect users completely even though it was created to reveal the hidden phone numbers by displaying the real name of the caller. The existing system does not provide a trustworthy, efficient, and real authentication for the true locations of the caller (Ankamma & Male, 2019). Research shows that with current technology investigation process needs to be made complex by complicating the calling and receiving process but not concealing the phone number.

The disadvantage of PayProtect is that in case of a disagreement between the buyer and the seller whereby the buyer attempts to reverse payments but the seller rejects a dispute is registered and resolved as per the dispute resolution protocol. The protocol states that a dispute is resolved by suggesting a solution. If it fails, a conference call between the parties is initiated, and if both fail the two parties are invited to a face-to-face discussion at PayProtect offices. Resolving a dispute using PayProtect is a tiresome process.

The attacks in social engineering can neither be put to an end using technology nor training alone (Gardner & Thomas, 2014). Multiple techniques are therefore often implemented to mitigate specific attacks. Based on the above literature it is clear that there are no secure applications to protect mobile money users from social engineers. The researcher aimed to design and develop a mobile application model to protect mobile money users against social engineering.

## 2.7 Conceptual Design



**Figure 6: Conceptual Design**

## **2.8 Chapter Summary**

This chapter gave an introduction to social engineering. Attacks in Social Engineering, social engineering ontological framework, and social engineering attack framework are discussed in this chapter. SERA and SEDF frameworks are also discussed. The defensive techniques against social engineering in mobile money and the knowledge gap are also provided in this chapter. Finally, the conceptual design which guided the implementation of the model is provided in this chapter.

## **CHAPTER THREE:**

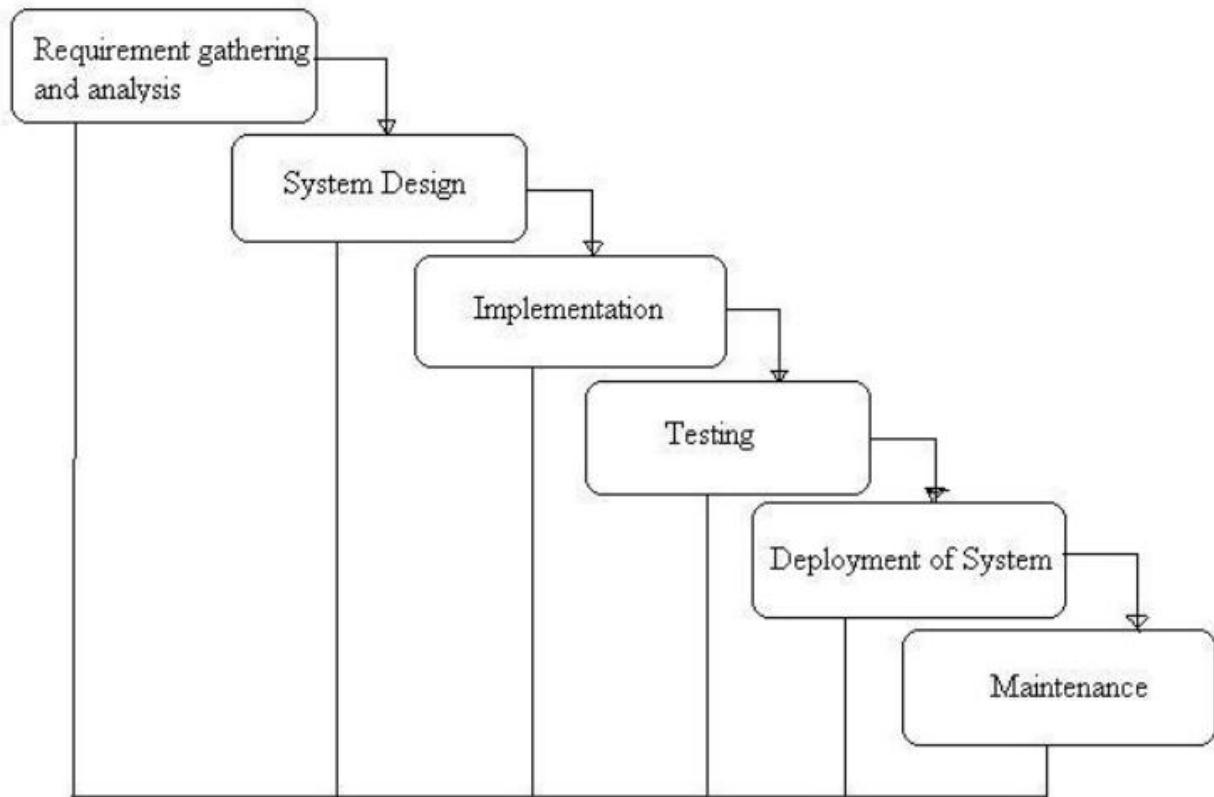
### **METHODOLOGY**

#### **3.1 Introduction**

The methodology for conducting research is exclusively discussed in this chapter. The rules, processes, and practices that control research define methodology (Marczyk et al., 2005). It refers to the techniques used by researchers to ensure that their work can be critiqued, reused, and adapted. Marczyk et al. (2005) further pose that choices made by researchers concerning data collection, sampling, and analysis are guided by these strategies.

#### **3.2 System Development Methodology**

The waterfall model was used to develop the system. The Waterfall methodology is a linear software development methodology, where progress flows gradually toward the conclusion through the different phases of a project (Sparrow, 2011). A straight sequential flow is used to show the system development process in the waterfall model (Bulman, 2017).



*Figure 7: Waterfall model source: (Sparrow, 2011)*

### **System Requirements Specification**

This research phase included no building. A clear understanding of the classification of the enterprise and how the operations are currently being carried out should be met before designing any application. The detailed analysis provides the specific data required during designing to ensure that all the requirements of the users are achieved. The requirements were analyzed and the problem was fully understood. All the necessary system requirements were represented in the systems requirements and Specification phase.

## **Design**

The overall plan of how the system will appear and the requirements for the hardware and the system are defined in the system design(Sparrow, 2011). The functionalities of the system and how it will operate including the layout of the system, data flow diagrams, and other functionalities are pointed out in system design. The developed application was described as an accumulation of different components in the output of the design phase. The problems set out by requirements got a technical solution in this phase.

## **Implementation**

The actual development and installation of a system are done in the Implementation Phase. The inputs from the design phase were first used to develop in small programs known as modules (Sparrow, 2011). The succeeding phase was used to put together the different modules. The development and testing of each module for its functionality were done in the implementation phase.

## **Testing**

The code in the developed application was tested at different stages. Testing is done in different components that make up the system, the whole application, and finally, testing is done to ensure the users are comfortable with the application (Sparrow, 2011). All the components were put together to form a complete application after testing each component separately. A web application called Safecash was developed for managing all the system operations and a mobile application was developed for the user.

## **Deployment**

Changes and improvements of the application are done before it is handed over to the users in the deployment stage(Bulman, 2017). The product will not be deployed since it is a student project.

### **3.3 Research Design**

Research design gives a plan for how data collection, analysis, and reporting in a study (Plano Clark & Creswell, 2015). “It provides the approaches that will be used in carrying out research. Research design is the general outline of how the relevant empirical research and the research problem are connected (Plano Clark & Creswell, 2015). In other words, a research design is a collection of processes logically designed to be used by researchers in the collection, analysis, and presentation of data in a study. The various processes link together systematically and therefore they are considered logical (Plano Clark & Creswell, 2015).

The study adopted a design that is descriptive to explicitly identify the social engineering risks facing mobile money applications in Kenya and the strategies adopted by Mobile Network Operators to address the current threats. The design was appropriate for the research since the study wanted to express the situation exactly the way it is in the industry. Description of how things are currently working in the industry is the main purpose of descriptive research. (Kothari, 2004).

Acquiring information about existing conditions or situations for description and interpretation defines descriptive research. It entails acquiring data describing different events and arranges, code, and explain how data is collected (Marczyk et al., 2005).

### **3.4 Research Approach**

The steps from the general assumption to more detailed techniques for collecting, analyzing, interpreting the data are defined in the research approach (Creswell & Creswell, 2018). Qualitative methods, quantitative methods, and mixed methods are the three major approaches or methods of



carrying out research (Creswell & Creswell, 2018; Marczyk et al., 2005; Plano Clark & Creswell, 2015)., a qualitative approach was used to address the research objectives since the research study involved collecting and examining qualitative data. The description for the choosing of the approach is as follows:

### **3.4.1 Qualitative Research**

Qualitative Research entails inspecting the views of the respondents in the collection, analysis, and presentation of data to answer the research questions (Plano Clark & Creswell, 2015). In this research process, the researcher begins with a problem that needs to be solved and then formulates a question that will help address the problem if answered (Creswell, 2016). This approach is important since it allows a natural setting whereby the researcher addresses the problem under study collecting data from the site where participants have experienced the problem.

Examining documents, observing behavior, or interviewing participants can be used by the researcher in qualitative research (Creswell & Creswell, 2018). The qualitative data in this study was obtained through open-ended questionnaires to understand the general security perspectives of the existing mobile money applications. The researchers focus on understanding the meaning from the respondent's point of view instead of what they understand themselves nor what has been documented by others in the whole process of qualitative research (Kothari, 2004). In this research approach, a sophisticated picture of the problem statement is developed (Creswell & Creswell, 2018). This entails presenting different perspectives, pointing out the different aspects that are involved, and coming up with a bigger picture from the situation.

### **3.5 Study Population and Sampling**

This part discussed the study population and sampling method used in the study

### 3.5.1 Study Population

The entire number of items or elements that can take part in a study is referred to as a population (Gray, 2004). Anything that takes part in a study, whether living or non-living and the researcher wants to derive some features from them is called a population (Creswell & Creswell, 2018).

The population in this research consisted of faculty staff and students from the Technical University of Kenya School of Computing and Information Technology. The relative population size that was involved in the study is shown in Table 1.

*Table 1: Study population*

<b>Participant Category</b>	<b>Population</b>
<b>Students</b>	<b>700</b>
<b>Academic Staff</b>	<b>42</b>
<b>Administrative Staff</b>	<b>12</b>
<b>Total Population</b>	<b>754</b>

Students were chosen in this study because they represent the young population who are mobile money users. In Kenya, the requirement to be registered for mobile money is a possession of a Kenyan Identity card which is issued at the age of 18 years. Students' age, both diploma, and undergraduate, range between 18 to 25 years on average. Apart from age, the students reflected most of the users since they come from different counties.

Faculty staff, both teaching and administrative staff, represented the senior population. Involving the staff in this study assisted the researcher in getting the user experience from the elder population's point of view.

### 3.5.2 Sampling

The choosing of participants who will take part in research from the whole population is called sampling. The decision about the people, the environment, the actions that will take place, the processes that will be observed, and how they will behave is involved in sampling (Plano Clark & Creswell, 2015). A representative of the whole population is chosen by the researcher in form of a sample and the main features of the sample should be similar or identical to those of the population (Marczyk et al., 2005). The selected sample must contain a large proportion of the population if the population itself is relatively small. Kothari (2004) argues that because of the resources involved, it becomes difficult to adopt a complete tally of the whole population if the participants are many.

As indicated in Table 1 the total population of this study was 754 therefore the researcher chose a sample of the population since it could have been expensive to study the whole population. The chosen respondents form a sample and the process of selection is called sampling (Kothari, 2004). A stratified sampling technique was used in this research.

According to Kothari (2004), when the population to be used to choose a representative sample from is different a stratified random method is employed to get the sample. The population is divided into different groups and then the respondents from each group are randomly selected (Plano Clark & Creswell, 2015). The respondents in this research constituted staff and students from the Technical University of Kenya. The population was split in two whereby they were related to each other in a group and then a sample was selected from each group (Kothari, 2004). Strata refer to the different sub-groups that took part in the study. There was correspondence between the sample selected and the size of the strata or group. For instance, if  $P_i$  represents the portion of the population in stratum  $i$  and  $n$  represent the total sample, the number of items chosen from stratum  $i$  is  $n * P_i$  (Kothari, 2004). The researcher selected a sample of size  $n = 100$  from a population of size  $N = 754$  which was split into 2 groups of  $N_1$  (Students) = 700 and  $N_2$  (staff) = 54.

For strata with  $N_1 = 700$ ,  $P_1 = 700/754$

Thus  $n_1 = n * P_1 = 100(700/754) = 93$

For the group with  $N_2 = 54$ , we have

$N_2 = n * P_2 = 100 (54/754) = 7$

The total number of participants that took part in this study constituted 93 students and 7 staff members, therefore, making a total sample size of 100 participants.

### **3.6 Data Collection**

This section outlines the techniques used for the collection of the necessary data to fulfill the objectives of the research. According to Gray (2004), data collection is all about the techniques and tools used when collecting data from the sampled participants. The questionnaire was the primary data collection tool used in data collection.

#### **3.6.1 Questionnaires**

Research instruments that are used to ask people to answer the same collection of questions in a fixed order are called questionnaires (Gray, 2004). Questionnaires were issued to both faculty staff and students at the Technical University of Kenya. According to Gray (2004), Questionnaires have several advantages which include; less resource requirement i.e. money, and time. Questionnaires can be sent to many respondents at a fairly low cost, unlike the interviews. Kothari (2004) opines that answers to a questionnaire are in respondents' own words and therefore free from the bias of the interviewer. Moreover, carefully thought out answers can be given by respondents since they have enough time.

According to Gray (2004), due to various questions that interviewers add to dig into the subject and how they place different emphasis, different interviewers get different answers. Unapproachable respondents can also be conveniently reached through questionnaires (Kothari, 2004).

Questionnaires have two principal forms namely; the numerous choice questions or the short answer and the essay type which are called open-ended in other words (Kothari, 2004). In this study, open-ended questions were employed to include all possible responses.

### **3.7 Reliability and Validity of Research Instruments**

The measure of the level in which the tools of data collection give coherent results even after several trials is called reliability (Kothari, 2004). This is supported by Creswell & Creswell (2015) who states that reliability touches on the stability of a research instrument. Data were checked for consistency and completeness.

Validity is the level at which the obtained results from the examination of the data collected represent the aspect being studied (Plano Clark & Creswell, 2015). A research tool must measure what it is planned to measure to ensure validity (Gray, 2004). To ensure the validity of questionnaires, the designed questionnaires ensured that they had covered the research issues both in content and detail. According to Gray (2004), asking bogus questions which are not relevant to the subject under study makes the questionnaires to be too long and therefore reducing the number of responses. The validity of questionnaires was adhered to by ensuring that the questionnaires designed were specific to the research topic.

### **3.8 Data Analysis**

The steps involved in the process of data analysis include; getting the data ready for examination, examining the data, and deriving a meaning (Marczyk et al., 2005). A Report about the total number of participants, those who returned the questionnaires, and those who never returned was be provided.

In qualitative research design, the data analysis must proceed conjointly with data collection and the results write-up. The first step included organizing and preparing the data for examination. This involves separating the data and organizing them into various forms according to the origin of the information and typing up field notes (Creswell & Creswell, 2018). The next step was to reflect on the overall meaning of the data by reading the entire data to provide a rough idea of the information. The data was then coded by picking the text data acquired during the collection of data, separating the sentences into different groups, and naming each group with a specific title or a term based on the participant's language. Topics known as themes and descriptions were generated in the next step. Themes, that appear as the major outcomes of research in qualitative research and are used as headings in the results section, are normally generated using codes (Creswell & Creswell, 2018).

Eventually, certain conclusions were considered as the outcome of the study grounded on the associations, patterns, and topics that were realized from the data. Results of the examination were conveyed using narrative passages.

### **3.9 Ethical Consideration**

Ethics refers to a code of morality used by people to gauge whether something is wrong or right and also to come up with rules on how to behave (Wallace, 2015). Research ethics deal with the conduct of the researcher with regards to the research subjects and also those who research affect them (Gray, 2004). Information about human beings and how they behave will always be available in cyberspace since cyberspace is greatly a forecast of behaviors in the tangible space (Edgar & Manz, 2017). In data collection, privacy should be maintained by protecting the data that might be sensitive to the participants' lives. Informed consent was obtained from the respondents before questionnaires were issued to them. Also, the researcher made sure that the respondents knew the reason for the research and the information they were required to provide. The anonymity of all participants was maintained in this research.

### **3.10 Chapter Summary**

This chapter discussed the systems development and the data collection methodology. A descriptive study design was adopted in this research. The chapter also explained the qualitative research approach and provided the study population and the sampling technique. Open-ended questionnaires were used in data collection. Furthermore, the reliability and validity of research objects, data analysis, and ethical considerations are provided in this chapter.

## **CHAPTER FOUR**

### **RESULTS, FINDINGS, AND DISCUSSIONS**

#### **4.1 Introduction**

Chapter four gives the results, findings, development of the prototype, and discussions. The findings are presented according to the methodology described and the objectives of the research. The results are from the analysis of the data collected.

#### **4.2 Response Rate**

The total number of questionnaires issued to mobile money users within Nairobi County was 100. Out of the 100, 72 questionnaires were filled and returned. This is equivalent to 72% of the total respondents which was considered good for analysis.

#### **4.3. Mechanisms used by social engineers to conduct social engineering attacks**

The research wanted to find out the methods used by attackers to conduct social engineering attacks. From the research, it was evident that humans are the most vulnerable link in security since computers or technologies are less trusted by humans compared to other humans. 48 out of the 72 respondents have experienced social engineering attacks which is equivalent to 66% of the respondents. social engineers conduct successful SE attacks by playing with the psychology of their victims. Both SMS and phone calls are mechanisms used by social engineering attackers in mobile money.

##### **4.3.1 Social Engineering by SMS.**

A text message is sent to a target's cellphone to make the victim disclose personal information in a Smishing attack, which is also known as SMS phishing (RSA, 2015). The researcher further poses that a smishing attack usually requires an immediate response from the intended victim who is called to action. The methods used by attackers to perform Smishing attacks include;



- a) Social engineers sending messages demanding money for an emergency. In this form of attack, an perpetrator pretends to be a kin who needs urgent help. For example, one of the respondents said that;

*“I received a message claiming that he was one of the siblings in school and he needed money for an emergency.”*

- b) Social engineers sending confirmation messages informing the respondent that they have received money on their mobile phones and immediately calling to inform the victim that they sent money wrongfully so that the victim can reverse the money. This was commented by a respondent who said he received the following message;

*“PG32UYUXFK confirmed. You have received Ksh 4,530 from Peter Simiyu 07...(Phone number hidden for confidentiality) on 3/7/2021. New M-PESA balance is Ksh. (LOCKED). To reverse forward this message to 456”*

Another respondent said that;

*“I received mpesa message and was told the money was meant for another person. I sent the money back later to realize that it was my money that I reversed”*

- c) Social engineers sending messages to victims informing them of job vacancies. In this form of attack, the social engineer takes advantage of the situation that the users are desperately in need of jobs. The attacker pretends to be a caring individual and wants to offer help to the victim. This was confirmed by a respondent who said he received the following message;

*“Hi aunt, tell your friend there are vacancies in accounts and receptionists for new branches. If interested call latest leo noon. Nice time.”*

Another respondent said that;

*“I got a message that claimed I had gotten a job to a position I had applied for. They wanted more details about me. What made me skeptical was the fact that I had not been interviewed yet”*

- d) Social engineering attackers send messages convincing victims to send money to different phone numbers. In this form, the attacker provides a different number from that which was used to send the message. This was confirmed by a respondent who said he received the following message;

*“Hi mum, sanduku yangu ilivunjwa nikaibiwa. Sina chochote, nitumie 1850 kwa number ya teacher EDWARD. No yake ni 07...(phone number hidden for confidentiality). Asante”*

Translation;

*“Hi mother, my box was broken and my items stolen. I have nothing, send me 1850 through teacher Edward’s number. His phone number is 07...(phone number hidden for confidentiality). Thank you.”*

- e) Winning a price SMS - In this type, the attacker manipulates victims into providing access to certain information through promising messages. This was confirmed by a respondent who said;

*“I received an SMS. It was about winning a v8 from a company known as Japan Automobile Manufacturers Association (JAMA). It was all a scam. I almost sent some money. They were talking about the vehicle watermark”*

#### **4.3.2 Social engineering by phone call**

Phone phishing which is also known as vishing is the act of committing fraud using the cellphone to get information about people and their finances (RSA, 2015). In this form of social engineering attack, the perpetrator calls the victim intending to make them disclose information or influence

them into sending money. The methods used by social engineers to perform phishing attacks in mobile money according to this research include;

- a) Posing as Mobile Network operators - In this method, the attacker pretends to be customer care for a mobile network operator and wants to assist the subscriber. The attacker leads the person into disclosing information after winning their trust. This was confirmed by a respondent who said that;

*“I received a phone call. The person said he was from Safaricom and he had seen that I was sharing the same number with another person. He wanted to know my details to check if it was the same”*

- b) Deceitful character - In this method, the attacker calls the victim to exploit them but acts like they are being kind to them. The attacker uses greed as a tool to exploit the victim in this case. This was confirmed by a respondent who said that;

*“Somebody called me. He said he got my phone number from Facebook and after looking at my photos he feels he is in love with me. He promised to send me some jewelry, handbags, and shoes from the US and wanted me to give him my details such as location address. After two days, the person called again and told me the items were already shipped and were held in the port of Mombasa. He took a picture of the parcel showing my name and address and also the items that were in that parcel. He then sent me a number claiming to belong to someone working at the port. He wanted me to send Kshs 10, 000 to that number so that the items could be released since he had not paid the taxes”*

- c) Emotional blackmail - In this method, the attacker triggers the emotions of the victim by instilling stress. The attacker calls the victims and tells them about their kin claiming that they are in danger. This was confirmed by a respondent who said;

*“I was called by an unknown number, telling me that my child was sick. I send them money only to realize later that I was conned”*

- d) Fake promises – In this form of attack, the perpetrator calls the victim informing them of good deals which they have acquired intending to make the victim disclose useful information. This was supported by a respondent who said;

*“Someone called me. I was told I have won a financial offer therefore I was required to provide the PIN to open an account for me to deposit the money.”*

#### **4.4 Challenges in Mobile Money Applications**

The research wanted to establish the challenges experienced by mobile money users when using the application. The challenges that emerged from the data collected are discussed here.

##### **a) Inability to recover money sent to a wrong number after it has been withdrawn**

Mobile money users experience challenges when money is sent to the wrong number. Sometimes if the fraudster withdraws the money immediately the user won't be able to reverse the money. This was supported by a respondent who said that;

*“Reversal of wrongfully sent money is very tedious and takes longer.”*

Another respondent said,

*“There was a time I was sending money to a relative but I made a mistake and I sent it to the wrong person. I wanted to reverse the money but it was already withdrawn. I called Safaricom but they told me they were unable to reverse since the user had already withdrawn the money”*

##### **b) PIN sharing**

Some mobile money users share their Mobile Money applications with their kin which leads to the withdrawal of money with their consent. This was confirmed by a respondent who said;

*“I gave my mpesa PIN to someone I trusted but I came to realize that money was withdrawn from my phone without my consent”*

**c) Sending more money than anticipated**

When a user is in a hurry they can send more money to the receiver than they anticipated. This was supported by a respondent who said that;

*“Somebody wanted to borrow money from me. Initially, I had told him I didn’t have any money but later I decided to send him five hundred shillings. Accidentally, I sent five thousand kshs.”*

**d) Delays in transaction**

When there is a delay in a transaction a subscriber can send money to an individual more than once leading them to send more than what they had planned for. This was supported by a respondent who said

*“Network problems result into sending money twice or many times and there is no funds reversal if someone has withdrawn the money”*

**4.5 Defensive Techniques against Social engineering attacks**

The mobile money service providers can take specific measures to reduce the possibility of fraud occurring and also to observe the occurrence of the prevalent fraud types and work on their effects to mitigate fraud in services provided by mobile money (Mudiri, 2012). The methods to protect against the social engineering attacks in mobile money from the study include; creating public awareness campaigns, providing a secure platform for users, automating spam attacks e.g. true callers, and blacklisting suspected contacts.

A respondent confirmed the above by suggesting that;

*“Mobile network operators should ensure or put in place more secure policies which prevent personal information from being shared to the public”*

From the data collected, it is evident that current mobile money payment and transfer applications design does not mitigate cybersecurity risks and specifically social engineering. Based on the examination of the collected data, the researcher therefore resorted to developing a mobile application. To meet the objective of developing a mobile money application model factoring in the current gaps facilitating social engineering to mitigate human-based social engineering risks in mobile money, the SAFECASH application was designed, developed, and implemented.

#### **4.6 Systems Analysis and Requirements Specification**

The systems analysis and requirements modeling in this study covered various modules that were developed and the requirements of the system both functional and non-functional are provided. A complete system was formed by integrating different components called modules that were put together. The modules include;

##### **a) Registration Module**

This module is concerned with registering the subscribers and agents who will use the system. Once the users have been registered they can access the system using their respective credentials.

- **Register safecash subscriber**

This module is concerned with capturing the subscriber’s details. The details to be captured include names, ID number, date of birth, telephone, gender, and email address.

- **Register agent**

This module is concerned with capturing the details of agents who will use the system. The details include agent name, ID number, address, telephone, email address, agent start date, user occupation, and next of kin personal details.

## **b) Transaction Module**

This module allows subscribers to transact on the platform. The operations include deposits, send money, withdrawals, check balances, and change the PIN.

- **Deposit**

This module is concerned with allowing agents to deposit cash to subscriber accounts.

- **Send Money**

This module is concerned with allowing subscribers to send money to other subscriber accounts

- **Withdraw cash**

This module is concerned with allowing subscribers to withdraw cash from their mobile wallets.

- **Change PIN**

This module is concerned with allowing the subscriber to change the default PIN given during registration. The PIN is verified during the transaction, that is when sending and withdrawing cash.

- **Hold transaction**

This module is concerned with holding incomplete transactions. When a subscriber sends the money he has the option to accept, hold or cancel a transaction.

### **4.6.1 Requirements specification**

The different functional and non-functional requirements of the safecash application are presented in this section.

**Table 2: Functional requirements**

<b>Functional Requirement</b>	<b>Description</b>
SAFECASH Access	The application will be accessed by the user once the application is installed on their phones.
Registration	The system shall enable the administrator to register new subscribers using the registration functionality.
Deposit	The system shall enable cash to be deposited in the subscriber's phone number
Send Money	The system shall enable the subscriber to send money to other registered safecash subscribers.
Hold transaction	The system shall allow the subscriber to hold unconfirmed transactions until the time he/she has specified so that he can release that transaction.
Cancel transaction	The system shall enable the subscriber to cancel unwanted transactions. Once a transaction has been canceled the money will go back to the sender's wallet
Withdraw cash	The system shall enable the subscriber to withdraw money from the mobile wallet



**Table 3: non-functional requirements**

Requirement	Description
Privacy	<p>The system shall ensure data integrity, security, and consistency. The system has various levels of security to protect users' credentials and data.</p> <p><b>Directory Level-</b> Password is used to protect the database. Encryption of passwords is done and details for every user have a security stamp associated with them.</p> <p><b>Application Level-</b> The system has an API key that protects any unauthorized users from accessing it. The system generates a random transaction code used for each transaction.</p>
Turnout	The application shall be accessed by many users concurrently.
Dependability	The application should be full-time operational.
Supportability	The system shall allow frequent and easy changes in the network if connected.
Usability	The system shall be friendly to the user with a favorable interface, navigation links, and minimal training required to use.
Portability	The application shall support various android versions available
Timing constraints	The system shall process data at a higher speed and respond to the user queries as soon as possible
Standards requirement	The system shall adhere to the general IT standards as stated in the ISO software standards

## 4.7 System Design

This section provides the functionality of the system. The logical database design, input design, output design, data flow diagram, and use case description are provided in this section.

### 4.7.1 Logical Database Design

A representation of the software developed was provided in the design. The description of how the customer problems solution was built is provided in the design record.

#### 4.7.1.1 Table Structures

**Table 4: Members Table-** To store subscribers' details

Field Name	Type	Constraint	Explanation
id	Bigint(20)	Primary Key	id
fullnames	Varchar(191)	Not Null	Full names
firstname	Varchar(255)	Not Null	First name
middlename	Varchar(255)	Not Null	Middle name
id_numer	Int(11)	Not Null	Id number
dob	Varchar(191)	Not Null	Date of birth
gender	Varchar(191)	Not Null	gender
telephone	Varchar(191)	Not Null	telephone
email	Varchar(191)	Not Null	email
amount	Varchar(191)	Not Null	amount
reg_number	Varchar(191)	Not Null	Registration number
agent_number	Int(11)	Not Null	Agent number
a_address	Varchar(255)	Not Null	Agent address
a_startdate	Varchar(191)	Not Null	Agent start date

a_occ	text	Not Null	Agent occupation
a_nkin	Varchar(255)	Not Null	Agent next of kin
a_naddress	Varchar(191)	Not Null	Next of kin address
a_ntel	Varchar(191)	Not Null	Next of kin telephone
a_relation	text	Not Null	Agent relationship
password	Varchar(191)	Not Null	password
rawPass	text	Not Null	Raw password
token	text	Not Null	token
status	Varchar(191)	Not Null	status
isActive	Tinyint(4)	Not Null	Is active
isLoggedin	Int(11)	Not Null	Is Logged in
created_at	text	Not Null	Created at
updated_at	timestamp	Not Null	Updated at

**Table 5: Deposits-** To store transaction details

<b>Field Name</b>	<b>Type</b>	<b>Constraints</b>	<b>Explanation</b>
id	Bigint(20)	Primary Key	id
idinitial	Varchar(191)	Not Null	Id initial
TransID	Varchar(191)	Not Null	Transaction ID
Reg_no	Varchar(250)	Not Null	Registration number
Fullnames	Varchar(250)	Not Null	Full names
sender_phn	Varchar(191)	Not Null	Sender Phone number
Amount	Varchar(250)	Not Null	amount
held_amount	Varchar(191)	Not Null	Held amount

initial_time	Varchar(191)	Not Null	Initial time
held_time_interval	Varchar(191)	Not Null	Held time interval
credit	Int(11)	Not Null	credit
debit	Int(11)	Not Null	debit
receiver_name	Varchar(191)	Not Null	Receiver name
receiver_tel	Varchar(191)	Not Null	Receiver telephone
Date	Varchar(250)	Not Null	date
Year	Varchar(250)	Not Null	year
Time	Varchar(250)	Not Null	time
Balance	Varchar(250)	Not Null	balance
rbalance	Varchar(191)	Not Null	Receiver balance
month	Varchar(255)	Not Null	month
status	Varchar(191)	Not Null	status
deleted	Tunyint(2)	Not Null	deleted
created_at	timestamp	Not Null	Created at
updated_at	timestamp	Not Null	Updated at

**Table 6: Held time-** To store details on the amount of time a transaction is held

Field Name	Type	Constraints	Explanation
id	Int(11)	Primary Key	id
time	Varchar(191)	Not Null	time
insec	Varchar(191)	Not Null	Time in seconds

**Table 7: Password Resets-** To store details on password resets, to provide a new password to the customer

Field Name	Type	Constraints	Explanation
email	Varchar(191)	Primary Key	email
token	Varchar(191)	Not Null	token
created_at	timestamp	Not Null	Created at

#### 4.7.2 Input design

The input design describes the various modules implemented for the input process. The design considers the possible errors that may occur during data entry thus mechanisms for ensuring that the data entered is correct and relevant are included. This will enhance database integrity.

##### 4.7.2.1 Layout

- Login
- Registration
- Manage subscribers
- Search master
- Transaction
- Check balance
- Change pin
- Report generation

##### 4.7.2.2 Module Description

###### a) Login

When users enter their user name and password the login module looks for a valid member and directs the user to their actual page or denies the user to log in if the details are incorrect. The module keeps track of the status when a user is logged in and can validate the user id with a password in

different cases. The user can reset their password if they are already registered but are unable to log in.

#### **b) Registration**

The registration module allows the administrator to register new safecash subscribers who will use the system.

#### **c) Manage subscribers**

This module allows the administrator to manage the users of the system. The admin can update the members' details, delete a member, activate, and deactivate a member.

#### **d) Search master**

The admin can look for a specific user using the search function. Different criteria of data can be searched using an improved search tool.

#### **e) Transaction**

Transactions can be managed by the user using the transaction module. With this module, the user can send cash, withdraw cash, hold or cancel a transaction.

#### **f) Check balance**

This module enables the subscriber to check the balance in their mobile wallet.

#### **g) Change PIN**

This module enables the user to change the PIN. When logging in for the first time they use the default password generated by the system which is sent to their phone numbers.

#### **h) Reports**

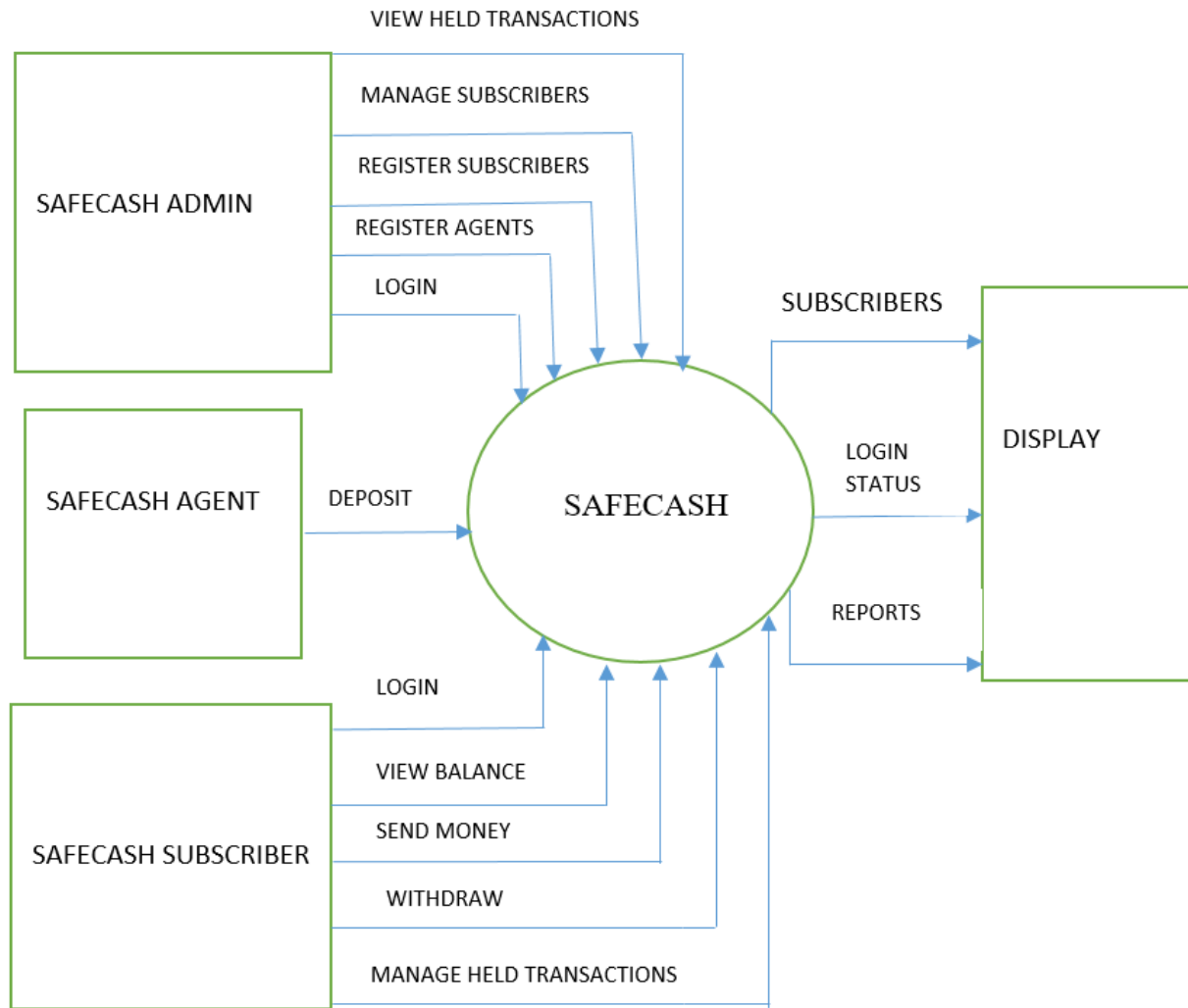
The administrator uses the report module. It enables the system to generate reports such as transactions, registered members, held transactions, and reports of members who logged into the system.

### **4.7.3 Output Design**

The output design was done to ensure that information from the system processes is presented in the best possible format and form. This will enhance the effective utilization of such outputs by users. The output methods considered in this design are the screen displays. Only the requested information will be output in a clear, precise, and accurate way to enhance system credibility, utility, and usability. The reports considered in this study are login reports, members' reports, and transaction reports. The messaging functionality is used to give feedback to the user through SMS at every stage. The messages include; held transactions, successful transactions, and denied transactions.

### **4.7.4 Level 0 DFD**

A system context diagram, also known as Level 0 DFD, presents the complete software application as a single unit by representing all the exterior components that in one way or another may interact with the application (Burge, 2011). The sources and targets of the information are represented as external agents on the context diagram (Ibrahim & Yen, 2010).



**Figure 8: Level 0 DFD**

Figure 9 above shows the context level DFD for SAFECASH. A well drawn diagram used to specify, construct, and visualize a system's model is called a DFD (Ibrahim & Yen, 2010). The components that interact with the system are the admin, agents, and subscribers. Subscribers can log in to the system, view balance, send money, withdraw cash and manage held transactions.



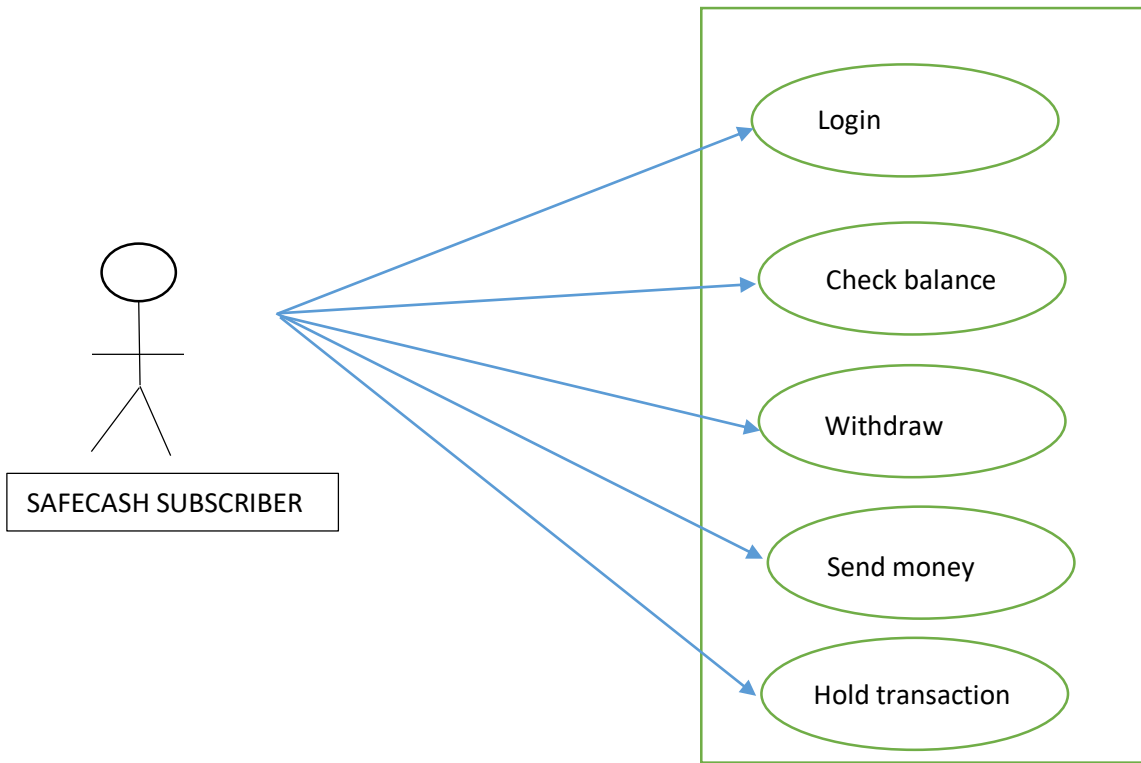
Transactions in this system are held in the subscriber's mobile wallet. When a member initiates a transaction there are three options; to send, to hold, or cancel. When a transaction wants to be held, the member has an option of selecting the amount of time that would want the transaction to be held. After the time chosen elapses, the user gets an SMS notification to remind him/her about the held transaction so that he can decide whether to proceed with sending money or cancel the transaction.

SAFECASH admin on the other hand can log in, register subscribers, register agents, manage subscribers, and view held transactions.

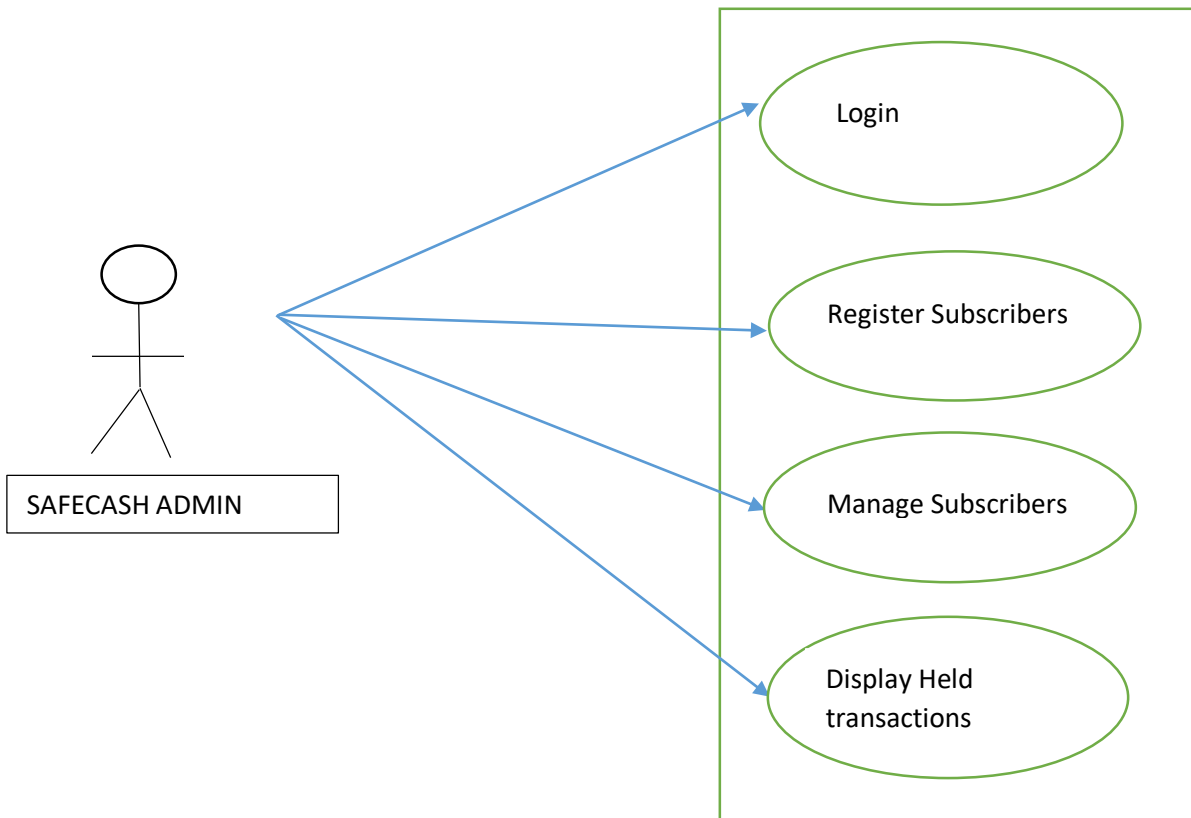
The SAFECASH agent deposits cash to the subscriber's wallet.

#### **4.7.5 Use Case Narration**

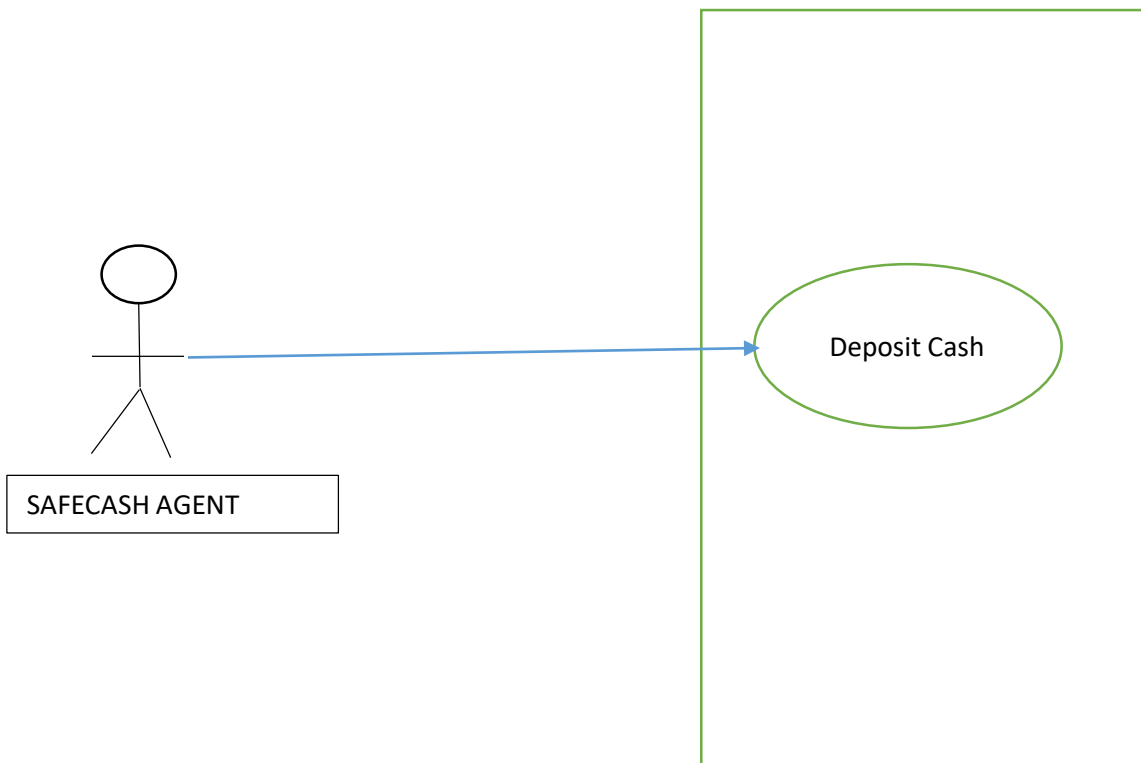
Use case diagrams to show how different components interconnect in the SAFECASH application are provided in this section. The actors involved and the type of interaction is identified in the Use Case Diagrams. Stick figures and named eclipse represent the actors and each class of interaction respectively. All the probable interactions to be represented in the requirement specification are represented in the use cases.



*Figure 9: subscriber use case diagram*



*Figure 10: administrator use case diagram*



*Figure 11: Agent Use Case diagram*

#### **4.8 System implementation**

This section explains how the system was implemented and tested. The system was implemented using Laravel Framework (PHP, CSS, HTML, and JavaScript), Java, and MYSQL database. Android Studio was used to implement the mobile application model.

### 4.8.1 Testing

Testing comprises checking whether the required output is displayed by carrying out a controlled manner execution of the system and inspecting it with data. The researcher comes up with test cases and their expected output and tests the application with data to inspect the output. Testing aimed to ensure that the application could give the correct output, manage normal production, users can relate well with the application and all components can work properly.

#### a) Registration Test Case

PROJECT NAME: SAFECASH APPLICATION					
TEST-CASE 1					
<b>Test-case ID:</b> 1			Designer: Pamela Chebii		
<b>Test component:</b> Subscriber Registration			Test Design Date: 22.07.2021		
<b>Test Title:</b> Registration Test Case			Test execution Date:23.07.2021		
<b>Test Description:</b> Test the subscriber registration page			Test executed by: Pamela Chebii		
<b>Preconditions:</b> The user must have the mobile application installed					
Test	Steps	Data	Expected-Result	Actual-result	Rank (pass/fail)
1.	Go to the Registration-Page		The admin should be able to move to the registration-page	The admin can move to the registration-page	pass
2.	Use registration-page		The admin should be able to use the registration-page	The admin can use the Registration-Page	pass
3.	Provide surname	Saitua	The admin should be able to add Saitua as a surname	The admin can add Saitua as a surname	pass
4.	Provide the first name	Alice	The user should be able to add Alice as the first name	The user can add Alice as the first name	pass
5.	Provide middle name	Nduta	The user should be able to add Nduta as the middle name	The user can add Alice as the middle name	pass
6.	Provide ID number	22989911	The user should be able to provide a valid id number	The user can provide a valid id number	pass
7.	Provide DOB	22-08-1990	User should be able to provide date of birth	The user can provide the date of birth	pass

8.	Provide phone number	0726643349	The user should be able to provide a valid phone number	The user can provide the phone number	pass
9.	Select gender		The user should be able to select gender	The user can select gender	pass
10.	Provide valid email	alicen@gmail.com	The user should be able to provide a valid email address	The user can provide a valid email address	pass
11.	Click on submit button		User should be able to register a new subscriber	The user can register a new subscriber	pass

### b) Sending Money Test Case

PROJECT NAME: SAFECASH APPLICATION					
TEST-CASE 2					
<b>Test-case ID:</b> 2			Designer: Pamela Chebii		
<b>Test component:</b> Sending money			Test Design Date: 22.07.2021		
<b>Test Title:</b> Sending money Test case			Test execution Date:23.07.2021		
<b>Test Description:</b> Test the sending money page			Test executed by: Pamela Chebii		
<b>Preconditions:</b> The user must have the mobile application installed					
Test	Steps	Data	Expected-Result	Actual-result	Status (pass/fail)
1.	Go to the transaction-page		The subscriber should be able to move to the transaction page	The subscriber can navigate to the transaction page	pass
2.	Click on sending money button		The user should be able to click on sending money	The user can access can click on sending money	pass
3.	Select contact or enter the phone number		The subscriber should be able to select a contact	The subscriber can select a contact	pass
4.	Enter amount	500	The subscriber should be able to enter 500 as the amount to send	The subscriber can enter 500 as the amount to send	pass
5.	Enter PIN		The subscriber should be able to enter their safecash PIN	The subscriber can enter safecash PIN	pass
6.	Hold Transaction		The subscriber should be able to hold the transaction	The subscriber can hold a transaction	pass

7.	Check SMS notification message		User should receive an SMS notification informing about held transaction	The user received an SMS notification	pass
----	--------------------------------	--	--	---------------------------------------	------

### c) Cash Deposit Test Case

PROJECT NAME: SAFECASH APPLICATION					
TEST-CASE 3					
<b>Test-case ID:</b> 3			Designer: Pamela Chebii		
<b>Test component:</b> Cash deposit			Test Design Date: 30.07.2021		
<b>Test Title:</b> Cash Deposit Test case			Test execution Date:30.07.2021		
<b>Test Description:</b> Test the Agent Services page			Test executed by: Pamela Chebii		
<b>Preconditions:</b> The user must have the mobile application installed					
Test	Steps	Data	Expected-Result	Actual-Result	Status (pass/fail)
1.	Go to the agent services page		The subscriber should be able to move to the agent services-page	The user can move to the agent services-page	Pass
2.	Click on the deposit cash button		The user should be able to click on deposit cash	The user can access can click on deposit cash	Pass
3.	Select agent number		The subscriber should be able to select agent number	The subscriber can select agent number	Pass
4.	Enter phone number	0726643349	The subscriber should be able to enter 0726643349 as the phone number	The subscriber can enter 0726643349 as the amount to send	Pass
5.	Display Agent Balance		The subscriber should be able to know the balance before choosing the amount to send	The subscriber can see the agent balance which is 1500 ksh	Pass
6.	Enter member ID number	22989911	The ID number should be verified before sending money	The ID number and phone number was verified	Pass
7.	Enter Amount	500	The subscriber should be able to enter 500 as amount	The subscriber can enter 500	Pass
8.	Enter Agent PIN		The subscriber should be able to enter agent pin	The subscriber was able to enter agent pin	Pass

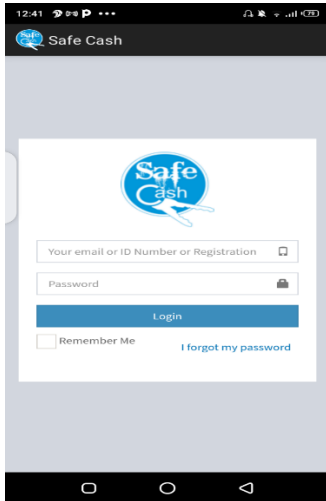
9.	Check SMS notification message		The subscriber should receive an SMS confirmation message	The user received an SMS notification	Pass
----	--------------------------------	--	---	---------------------------------------	------

#### d) Withdraw Cash Test Case

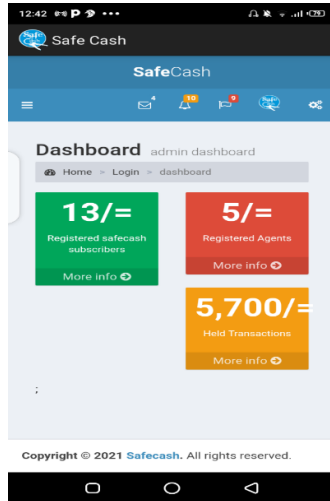
PROJECT NAME: SAFECASH APPLICATION					
TEST-CASE 4					
<b>Test-case ID:</b> 4			Designer: Pamela Chebii		
<b>Test component:</b> Withdraw Cash			Designer: 31.07.2021		
<b>Test Title:</b> Withdraw cash Test case			Test execution Date:31.07.2021		
<b>Test Description:</b> Test the Withdraw Cash page			Test executed by: Pamela Chebii		
<b>Preconditions:</b> The user must have the mobile application installed					
Test	Test steps	Test data	Expected Result	Actual result	Status (pass/fail)
1.	Go to the transaction-page		The subscriber should be able to move to the transaction-page	The subscriber can move to the transaction page	pass
2.	Click on withdraw cash button		The subscriber should be able to click on withdraw cash button	The subscriber can access can click on withdraw cash	pass
1.	Select agent number		The subscriber should be able to select agent number	The user can select agent number	pass
2.	Enter phone number	0726643349	The subscriber should be able to input 0726643349 as the phone number	The subscriber can enter 0726643349 as the amount to send	pass
3.	Enter Amount	500	The user should be able to input 500 as the amount	The user can input 500	pass
4.	Enter PIN		The subscriber should be able to enter their PIN	The subscriber managed to enter PIN	pass
5.	Check SMS notification message		The subscriber should receive an SMS confirmation message	The user received an SMS notification	pass



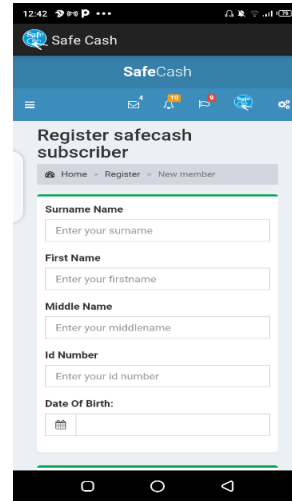
## 4.8.2 Proof of concept



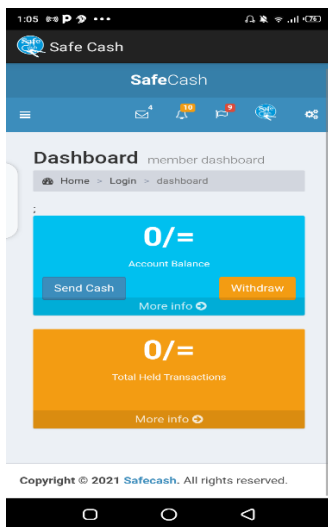
Login Page



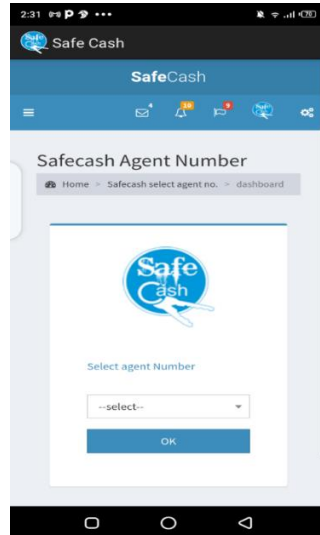
Admin Page



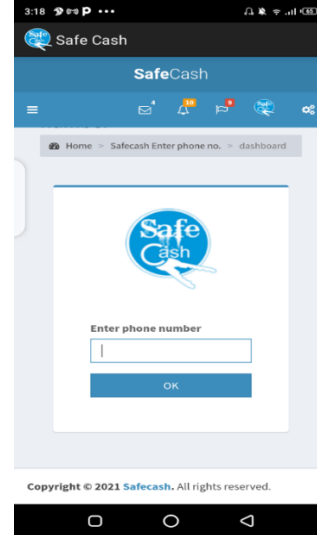
subscriber Registration



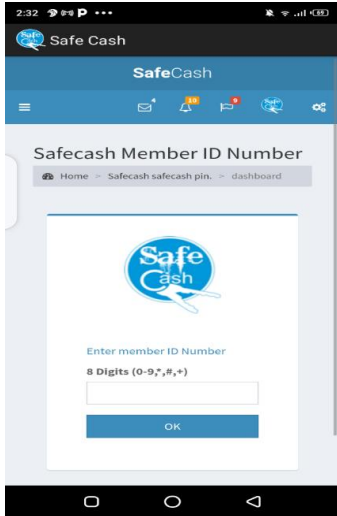
Subscriber landing Page



Cash deposit



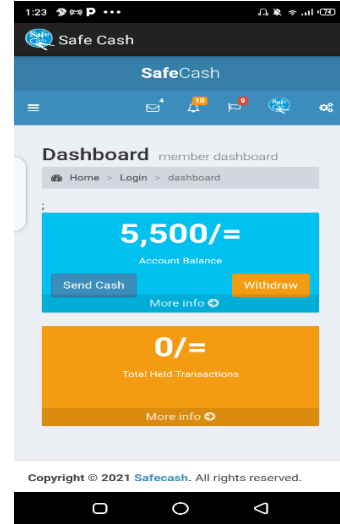
Enter phone number



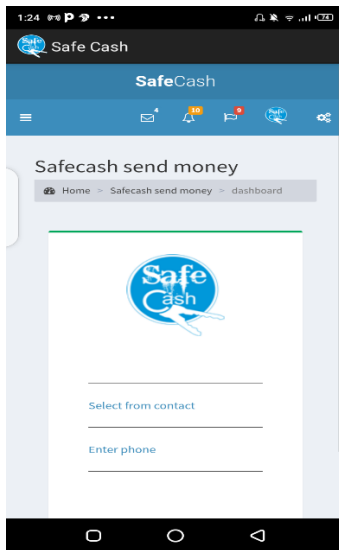
Enter ID Number



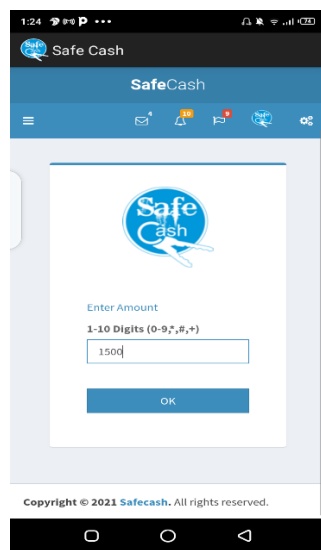
Enter Amount



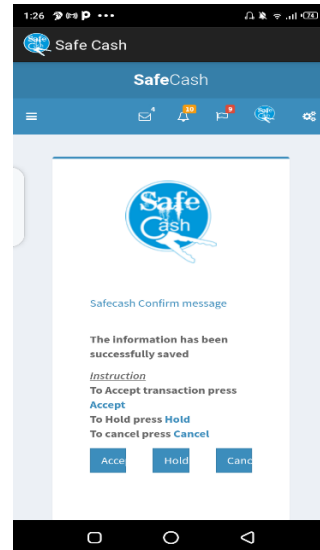
Account Balance



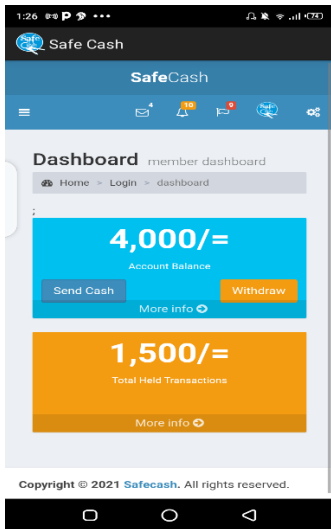
Send money



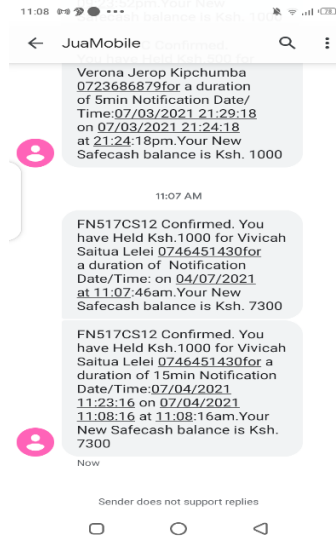
Enter Amount



Confirmation page



Balance after holding transaction



SMS notification for held transaction

#### 4.9 Discussion

To address the issue of social engineering in mobile money, a deactivate functionality was implemented by SAFECASH. If a phone number has been reported to the admin to have been involved in fraud the phone number is deactivated so that the phone user can neither send nor receive cash using the same phone number. This will help eliminate known con men/women who might be using the same number to influence unsuspecting mobile money users to send them money.

The challenges faced by mobile money users such as sending money wrongfully and sending more money than anticipated was addressed by the introduction of a holding functionality in SAFECASH. SAFECASH can lock transactions within the user's wallet up to a specific time as specified by the sender and can send a notification to remind the sender whether to continue holding or accept the transaction. This function gives the sender time to confirm the details of the user at the same time be sure whether he/or she is sending money to the right person and the right amount. If the user

decides to cancel the transaction after holding, the money will go back to the sender's wallet. SAFECASH can hold more than one transaction at the same time.

To address the fraud issues in mobile money, fraud detection functionality was introduced such that if a subscriber is sending so much money in the middle of the night, SAFECASH will automatically lock the transaction until a specified time. Locking of suspected transactions will enable the confirmation of details whether they are correct and also you can track the businesses being conducted by users during the odd hours.

The suggestions provided by the respondents on what they think the mobile network operators can do to protect them from social engineering attacks helped the researcher in the implementation of different functionalities in the SAFECASH application.

#### **4.10 Chapter Summary**

This chapter discussed data analysis and the development of a prototype for mobile payment and transfer. The results showed that 66% of the respondents have experienced social engineering attacks either through SMS or phone call. Successful SE attacks are achieved by attackers by playing with the psychology of their victims. Systems analysis and requirements specification, design, and implementation of the prototype are provided in this chapter. The system design provided the logical database design, input design, output design, and use case narration. Discussions on the results and findings were also provided in this chapter.

## **CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS**

### **5.1 Introduction**

Chapter five gives the conclusion, limitation of the research, achievements, and recommendations based on the analysis and results from the previous chapters. The recommendation section suggests future work that needs to be done in social engineering and mobile money applications.

### **5.2 Conclusion**

Current mobile money transfer and payment applications design does not mitigate cybersecurity risks and specifically social engineering. This study aimed to establish the gap and propose a design that will mitigate these risks. Threats in Social Engineering are the greatest risks that face cybersecurity because they exploit the natural human tendency to trust”(Salahdine & Kaabouch, 2019). From the research findings, most of the respondents (66%) have experienced Social Engineering attacks either by phone call or by SMS.

Findings showed that smishing and vishing are the mechanisms used by social engineers to conduct social engineering attacks on mobile money. The methods for conducting smishing attacks included; social engineers sending messages demanding money for an emergency, sending false confirmation messages, messages informing victims of job vacancies, attackers sending messages to convince victims to send money to different phone numbers, and winning a price SMS. Vishing attacks on the other hand were conducted by attackers through posing as Mobile Network operators, deceitful characters by acting like they are being kind to the respondent, emotional blackmail, and fake promises.

The social engineering challenges that came from the research include the inability to recover money sent wrongfully and PIN sharing,

The defensive techniques that came out from the research included creating public awareness campaigns, providing a secure platform for users, automating spam attacks, and blacklisting suspected contacts. This is supported by the framework for defense against Social Engineering Defensive (SEDF) by Thomas which states that the organization needs to find out the vulnerability, assess the defense, train employees, and improve on technology and policies to protect against attacks in Social Engineering (Gardner & Thomas, 2014).

### **5.3 Achievements**

The Safecash model was created to serve as a reference point for the detection of social engineering attacks in Mobile money payment and transfer applications. The safe cash application can analyze and hold transactions. Holding of transactions allows the subscriber time to confirm the details of the receiver and whether to proceed with sending money or to abort the transaction. Timing is included so that the application notifies the sender in form of an SMS that there is a held transaction that needs to be released. The cancel functionality allows the transaction to be aborted, unlike the Safaricom hakikisha whereby when a transaction is canceled it automatically sends the money. The application is also able to lock suspected transactions. Suspected contacts are blocked by the safecash application. PIN sharing was solved by allowing the user to change the mobile money PIN. The messaging functionality provides interactive visualization for the subscribers by notifying them of any transaction attempt.

### **5.4 Weaknesses of the Study**

1. The research was limited to smishing and vishing social engineering attacks in mobile money.
2. The study focused on social engineering risks in a transaction. Other risks such as channel risk (agent) and internal risks (employee) were not studied.
3. The implemented application does not authenticate calls and SMS.

## **5.5 Recommendations**

The study recommends expert evaluation of the proposed application to improve it and keep up with current trends in social engineering should be done. A system that monitors and detects social engineering attacks in real-time and provides interactive visualizations for the end-user should be implemented.

The study also recommends further research on social engineering risks on channel risk and internal risks in mobile money payment and transfer applications.

Service providers should invest more in cybersecurity and modern technologies that can detect various social engineering threats. Mobile money payment and transfer applications should be improved to authenticate Calls / SMS.

## REFERENCES

- Abeywardana, K. Y., Pfluegel, E., & Tunnicliffe, M. J. (2016). A layered defense mechanism for a social engineering aware perimeter. *Proceedings of 2016 SAI Computing Conference, SAI 2016*, 1054–1062. <https://doi.org/10.1109/SAI.2016.7556108>
- Agbezouts, K. E., Uriene, P., & Dandjinou, T. M. (2019). Towards Blockchain Services for Mobile Money Traceability and Federation. *2019 3rd Cyber Security in Networking Conference, CSNet 2019*, 14–20. <https://doi.org/10.1109/CSNet47905.2019.9108970>
- Ankamma, V., & Male, R. (2019). *Detection of spoofing attacks in the network over IP calling*. 5(2), 1328–1333. <https://doi.org/https://www.ijariit.com/manuscripts/v5i2/V5I2-1854.pdf>
- Authority-Kenya, C. (2020). *First Quarter Sector Statistics Report for the Financial Year 2020 / 2021. December 2020*, 1–28.
- Buku, M. (2015). *Safaricom Launches Feature to Stop Erroneous Transfers: Hakikisha*. CGAP. <https://www.cgap.org/blog/safaricom-launches-feature-stop-erroneous-transfers-hakikisha>
- Bulman, M. (2017). SDLC - Waterfall Model. *The Independent*, May.
- Burge, S. (2011). Context Diagram (CD). *The Systems Engineering Tool Box, Cd*, 1–17.
- Creswell, J. W. (2016). *30 Essential Skills for the Qualitative Researcher*. SAGE Publications Ltd.
- Creswell, J. W., & Creswell, J. D. (2018). Research Design Qualitative, Quantitative, and Mixed Methods Research Approaches. In *Fast Facts to Loving your Research Project*. <https://doi.org/10.1891/9780826146373.0007>
- Deloitte. (2019). *Understanding phishing techniques Understanding phishing techniques Overview. December*.



- Donovan, K. (2011). Mobile Money for Financial Inclusion. *Information and Communications for Development*, 61(1), 61–74.
- Edgar, T. W., & Manz, D. O. (2017). Research Methods for Cyber Security. In *Research Methods for Cyber Security*. [https://doi.org/10.1016/s1353-4858\(18\)30053-9](https://doi.org/10.1016/s1353-4858(18)30053-9)
- European Union. (2020). *Mobile money and organized crime in Africa*. June.
- Farooq, S. (2019). Mitigating common fraud risks Best practices for the mobile money industry. *GSMA*.
- Gardner, B., & Thomas, V. (2014). Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats. In *Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats* (Issue September). <https://doi.org/10.1016/C2013-0-12654-2>
- Gilman, L., & Joyce, M. (2012). Managing the Risk of Fraud in Mobile Money. *The Microfinance Gateway*, 1–10.
- Gray, D. E. (2004). *Doing Research in the Real World*.
- Grimes, R. A. (2017). Social Engineering Attacks. In *Hacking Multifactor Authentication* (pp. 259–273). <https://doi.org/10.1002/9781119672357.ch12>
- GSMA. (2010). Mobile Money Definitions. *Gsma*, July, 1–4. <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/mobilemoneydefinitionsnomarks56.pdf>
- Ibrahim, R., & Yen, S. Y. (2010). Formalization of the Data Flow Diagram Rules for Consistency Check. *International Journal of Software Engineering & Applications*, 1(4), 95–111. <https://doi.org/10.5121/ijsea.2010.1406>

- Kothari, C. R. (2004). *Research Methodology Methods and Techniques* (Second Rev). New Age International Publishers.
- Marczyk, G., DeMatteo, D., & Festinger, D. (2005). *Essentials of Research Design and Methodology* (A. S. Kaufman & N. L. Kaufman (eds.)). John Wiley & Sons Ltd.  
<https://doi.org/10.1210/endo-69-4-673>
- Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences*, 147, 424–428.  
<https://doi.org/10.1016/j.sbspro.2014.07.133>
- Mitnick, K. D. (2002). *The Art of Deception Controlling The Human Element of Security*. Wiley Publishing, Inc.
- Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014). Towards an Ontological Model Defining the Social Engineering Domain. *IFIP Advances in Information and Communication Technology*, 431. [https://doi.org/10.1007/978-3-662-44208-1\\_22](https://doi.org/10.1007/978-3-662-44208-1_22)
- Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack framework. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference, August*. <https://doi.org/10.1109/ISSA.2014.6950510>
- Mudiri, J. (2012). Fraud in Mobile Financial Services. *A MicroSave Publication*, 48.  
[http://www.microsave.net/files/pdf/RP151\\_Fraud\\_in\\_Mobile\\_Financial\\_Services\\_JMudiri.pdf](http://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf)
- Narayan, S. (2013). *Comparison of Mobile Wallet Concepts*. 55. <http://kth.diva-portal.org/smash/get/diva2:707453/FULLTEXT01.pdf>

- Otieno, D. (2020). *Safaricom needs to fix M-Pesa privacy problems*. Tech-Ish.Com. <https://tech-ish.com/2020/01/20/safaricom-mpesa-privacy/>
- Patrick Vidija. (2021, January 20). Mpesa Fraud: Conmen pose as Safaricom staff to steal from unsuspecting users. *The Star*. <https://www.the-star.co.ke/news/2021-01-20-mpesa-fraud-conmen-pose-as-safaricom-staff-to-steal-from-unsuspecting-users/>
- PayProtect. (2021). *PayProtect*. <https://www.payprotect.co.ke/>
- Peter, J. (2020). Resilience through diversity. *Governing Marine Protected Areas*. <https://doi.org/10.4324/9780203126295-16>
- Plano Clark, V. L., & Creswell, J. W. (2015). Understanding Research: A Consumer's Guide, (2nd Edition). In *Journal of Emergency Nursing* (Vol. 30, Issue 6). <https://doi.org/10.1016/j.measurement.2014.09.004>
- Raina, V. K. (2015). Overview of mobile payment: Technologies and security. In *Banking, Finance, and Accounting: Concepts, Methodologies, Tools, and Applications* (Vols. 1–3, Issue February). <https://doi.org/10.4018/978-1-4666-6268-1.ch011>
- RSA. (2015). Phishing, Vishing, and Smishing : Old Threats Present New Risks How much do you really know about phishing, vishing, and smishing ? *October*.
- Sadiku, M. N. O., Shadare, A. E., & Musa, S. M. (2016). Social Engineering : An Introduction. *Journal of Scientific and Engineering Research, September*, 64–66.
- Safaricom. (2021a). *Jichanue Voice Tips*. <https://www.safaricom.co.ke/personal/get-more/information-services/jichanue-self-service-tips>
- Safaricom. (2021b). *Using M-pesa*. <https://www.safaricom.co.ke/personal/m-pesa/getting-started/using-m-pesa>

- Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4). <https://doi.org/10.3390/FI11040089>
- Serban, V. G., & Serban, O. (2014). Social Engineering A General Approach. *Informatica Economica*, *18*(2/2014), 5–14. <https://doi.org/10.12948/issn14531305/18.2.2014.01>
- Song, J., Kim, H., & Gkelias, A. (2014). iVisher: Real-time detection of caller ID spoofing. *ETRI Journal*, *36*(5), 865–875. <https://doi.org/10.4218/etrij.14.0113.0798>
- Soykan, E. U., & Bagriyanik, M. (2020). *The Effect of SMiShing Attack on Security of Demand Response Programs*.
- Sparrow, P. (2011). *Waterfall Model of SDLC ~ I Answer 4 U*.  
<https://www.ianswer4u.com/2011/11/waterfall-model.html#axzz3Qs5RV0Sb>
- Subia, M. P., & Martinez, N. (2014). Mobile Money Services : “ A bank in Your Pocket”: An Overview of Trends and Opportunities. *ACP Observation on Migration*.
- Wallace, P. (2015). *Introduction to Information Systems* (S. Wall & B. Horan (eds.); 2nd Editio).

## **APPENDICES**

### **APPENDIX 1: QUESTIONNAIRE**

Dear Sir/Madam,

I am a registered Master of Science student at the University of Nairobi, School of Computing and Informatics. As part of the requirements for the award of Master of Science in Distributed Computing Technology (DCT), I am undertaking research titled, “Securing Mobile Money Payment and Transfer Applications against Social Engineering”.

The study aims to evaluate the effectiveness of existing platforms in use by mobile money payment and transfer applications that counter the effects of social engineering and to identify gaps in the current mobile money applications that facilitate social engineering. The study will gather data on Social engineering, mobile money fraud, and defensive techniques in mobile money. The study will then develop a mobile money application model factoring in the current gaps facilitating social engineering to mitigate human-based social engineering risks in mobile money.

The purpose of this communication is to kindly request you to set aside some time to complete the attached questionnaire which will enable me to obtain data that will address the research problem being studied. All the information provided will be treated with absolute confidentiality and used only for the academic purposes of the study.

For any query/clarification about the research, please feel free to contact Ms. Pamela Jepkorir Chebii, +254716318982, [jepkorir.pamela@students.uonbi.ac.ke](mailto:jepkorir.pamela@students.uonbi.ac.ke).

Thank you.

Yours faithfully,

Pamela Chebii

**Demographic Information**

- i. Gender.....
- ii. Age .....
- iii. Highest academic qualification attained .....

**Social Engineering**

- i. Are you aware of a Social engineering attack?  
.....  
.....
- ii. Have you ever experienced money theft via mobile phone? If yes, how did it happen  
.....  
.....  
.....
- iii. Have you ever experienced a social engineering attack before? If yes, kindly explain how it happened  
.....  
.....  
.....  
.....
- iv. What mechanism did the attacker use
  - a) SMS [ ]
  - b) Phone call [ ]
  - c) Physical Approach [ ]

d) Others

.....  
.....

v. Are you able to say something about the attacks you have experienced?

.....  
.....  
.....  
.....

vi. Have you ever experienced a successful attack? If yes, are you able to say something about the attack?

.....  
.....  
.....

**Mobile money Fraud**

i. Have you ever shared your mobile money PIN with anyone? Please give reasons for your answer

.....  
.....  
.....  
.....

ii. Have you received a call or SMS from someone that you suspect was an attempt to get your details for fraudulent purposes? If yes, please elaborate on the situation

.....

.....  
.....  
.....  
.....

iii. Have you received SMS or calls from persons claiming to have sent money wrongfully to your number? How did you respond?

.....  
.....  
.....  
.....

iv. Have you received SMS or Calls from persons demanding money for an emergency? How was your reaction?

.....  
.....  
.....  
.....

v. Has anyone ever transferred money from your mobile wallet without your knowledge?

.....  
.....  
.....

vi. What are some of the challenges you encounter in terms of the security of your mobile money application? Please explain any scenario of encountered

.....  
.....



.....  
.....  
.....

vii. If anyone has your mobile phone do you assume your mobile money is at risk of anyone having access and exploiting it? Please give reasons for your answer

.....  
.....  
.....

**Defensive Techniques**

i. How do you protect yourself against social engineering attacks?

.....  
.....  
.....  
.....

ii. Do you think you encountered social engineering attack because of not being aware of a social engineering attack? Please explain your answer

.....  
.....  
.....  
.....

iii. What do you think the Mobile Network Operators (e.g. Safaricom, Telkom, Airtel) should do in order to protect you as a user against social engineering attacks?

.....

.....  
.....  
iv. Any other comments  
.....  
.....  
.....  
.....

**Thank you for your time and support**